

Daftar Isi

Lembar Pengesahan Pembimbing.....	i
Lembar Pengesahan Penguji	ii
Abstrak	iii
Abstract	iv
Pernyataan keaslian tulisan	v
Publikasi selama masa studi.....	vi
Kontribusi yang diberikan oleh pihak lain dalam tesis ini.....	vii
Halaman Persembahan.....	viii
Kata Pengantar.....	ix
Daftar Isi	x
Daftar Tabel.....	xiv
Daftar Gambar.....	xv
Glosarium.....	xvii
BAB 1 Pendahuluan.....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah.....	4
1.3 Rumusan Masalah.....	4
1.4 Batasan Masalah	4
1.5 Tujuan Penelitian	5
1.6 Manfaat Penelitian	5
1.7 Metode Penelitian	5
1.8 Sistematika Penulisan Penelitian.....	7
BAB 2 Tinjauan Pustaka.....	8
2.1 Gambaran Umum Dinas Komunikasi dan Informatika Kota Tegal	8
2.1.1 Gambaran Topologi Jaringan Kota Tegal.....	9
2.2 Studi Pustaka	10
2.2.1 Penelitian Terdahulux.....	10
2.3 Landasan Teori	15
2.3.1 Keamanan Informasi (<i>Information Security</i>)	15
2.3.2 <i>Network Threat</i>	17
2.3.3 <i>IT Security Risk Management</i>	19

2.3.4	<i>Risk Assesment</i>	19
2.3.5	<i>Security Strategy Defence in Depth</i>	20
2.3.6	Sistem Manajemen Keamanan Informasi (SKMI).....	21
2.3.7	Indeks Keamanan Informasi (KAMI).....	22
2.3.8	Pengukuran indeks Keamanan Informasi (KAMI)	24
2.3.9	<i>SIEM</i>	27
2.3.10	<i>Digital Forensic</i>	30
2.3.11	<i>Network Forensic</i>	31
BAB 3	Metode Penelitian	33
3.1	Studi Literatur.....	33
3.2	<i>Pre-Assesment</i> Indeks KAMI Dinas Komunikasi dan Informatika Kota Tegal	33
3.3	Pembuatan <i>Network Environment</i>	34
3.4	Penyerangan <i>Network Environment</i>	36
3.4.1	Skenario Penyerangan	37
3.5	Network Forensik	38
3.6	<i>Post-Assesment</i> Indeks KAMI Dinas Komunikasi dan Informatika Kota Tegal	40
3.7	Analisa Serangan	40
3.8	Hipotesa.....	41
Bab 4	Analisis dan Pembahasan	42
4.1	<i>Pre-assesment</i> Indeks KAMI Dinas Komunikasi dan Informatika Kota Tegal	42
4.2	Pembuatan <i>Network Environment</i>	44
4.3	Penyerangan <i>Network Environment</i>	47
4.3.1	<i>Link Layer Attack</i>	48
	a. Simulasi Serangan <i>Mac Flooding</i>	48
	b. Simulasi Serangan <i>Arp Poisoning</i>	49
	c. Simulasi Serangan <i>CDP Flooding</i>	51
4.3.2	<i>Internet Layer Attack</i>	51
	a. Simulasi Serangan DHCP Starvation.....	51
	b. Simulasi Serangan DHCP <i>Rogue</i>	52
4.3.3	<i>Transport Layer Attack</i>	53

	a. Simulasi Serangan SYN flooding	53
	4.3.4 <i>Application Layer Attack</i>	53
	a. Simulasi Serangan <i>Brute Force Ssh</i>	53
	b. Simulasi Serangan <i>Brute Force Ftp</i>	54
	4.4 <i>Network Forensic</i>	54
	4.4.1 <i>Link Layer Attack</i>	55
	a. <i>Network Forensic Mac Flooding</i>	55
	b. <i>Network Forensic Arp Poisoning</i>	55
	c. <i>Network Forensic CDP Flooding</i>	56
	4.4.2 <i>Network Layer Attack</i>	56
	a. <i>Network Forensic DHCP Starvation</i>	56
	b. <i>Network Forensic DHCP Rogue</i>	57
	4.4.3 <i>Transport Layer Attack</i>	57
	4.4.4 <i>Application Layer Attack</i>	58
	a. <i>Network Forensic SSH Brute Force</i>	58
	b. <i>Network Forensic FTP Brute Force</i>	58
	4.5 <i>Post-assesment Indeks KAMI Dinas Komunikasi dan Informatika Kota</i> <i>Tegal</i>	59
	4.6 <i>Analisa Data</i>	61
	4.6.1 <i>Serangan dan SIEM</i>	61
	4.6.2 <i>Indeks Kami</i>	62
Bab 5	<i>Kesimpulan dan Saran</i>	64
	5.1 <i>Kesimpulan</i>	64
	5.2 <i>Saran</i>	64
	Daftar Pustaka	66
	Lampiran	69
	1. <i>Script konfigurasi Mikrotik</i>	69
	2. <i>Network forensic Mac Flooding</i>	70
	3. <i>Network forensic Arp Poisoning</i>	71
	4. <i>Network forensic CDP Flooding</i>	72
	5. <i>Network forensic DHCP Starvation</i>	73
	6. <i>Network forensic DHCP Rogue</i>	74
	7. <i>Network forensic SYN Flooding</i>	75

8. <i>Network forensic SSH Brute Force</i>	76
9. <i>Network forensic FTP Brute Force</i>	77
10. Kuisisioner Pre-Assessment Indeks KAMI Diskominfo Kota Tegal.....	79
11. Kuisisioner Post-Assessment Indeks KAMI Diskominfo Kota Tegal	95



Daftar Tabel

Tabel 2.1: <i>Literature Review</i>	12
Tabel 3.1: Tipe serangan di <i>Network</i> dan <i>Tools</i>	36
Tabel 3.2: Rangkuman <i>Network Forensic</i> Serangan	39
Tabel 3.3: Kolerasi Serangan dan <i>SIEM</i>	40
Tabel 4.1: Pelaporan <i>Network Forensic</i> serangan <i>Mac flooding</i>	55
Tabel 4.2: Pelaporan <i>Network Forensic</i> serangan <i>Arp Poisoning</i>	55
Tabel 4.3: Pelaporan <i>Network Forensic</i> serangan <i>CDP flooding</i>	56
Tabel 4.4: Pelaporan <i>Network Forensic</i> serangan <i>DHCP Starvation</i>	56
Tabel 4.5: Pelaporan <i>Network Forensic</i> serangan <i>Dhcp Rogue</i>	57
Tabel 4.6: Pelaporan <i>Network Forensic</i> serangan <i>SYN flooding</i>	57
Tabel 4.7: Pelaporan <i>Network Forensic</i> serangan <i>Ssh Bruteforce</i>	58
Tabel 4.8: Pelaporan <i>Network Forensic</i> serangan <i>Ftp bruteforce</i>	58
Tabel 4.9: Aspek Teknologi yang dipengaruhi Diskominfo Kota Tegal.....	60
Tabel 4.10: Rangkuman <i>Network Forensic</i> Simulasi Serangan	61



Daftar Gambar

Gambar 1.1 <i>Top Network Security Attack</i>	2
Gambar 1.2 <i>Mikrotik Training 2014-2016 (Source:Inixindo Jogja Internal Data)</i>	2
Gambar 2.1 Struktur Organisasi Dinas Komunikasi dan Informatika Kota Tegal.....	8
Gambar 2.2 Gambaran Umum Jaringan Kota Tegal	9
Gambar 2.3 <i>Information Security (CIA)</i>	15
Gambar 2.4 <i>Defence in Depth Strategy</i>	21
Gambar 2.5 Contoh Grafik Indeks KAMI	23
Gambar 2.6 Tabel Skoring Peran IT dan Status Kesiapan.....	25
Gambar 2.7 Tabel Nilai Kategori Penilaian.....	25
Gambar 2.8 Tingkat Kematangan dan Kesiapain ISO 27001	26
Gambar 2.9 <i>SIEM Feature List</i>	27
Gambar 2.10 Metodologi <i>OSCAR (Source: A Road Map for Digital Forensic Research)</i> .	31
Gambar 3.1 Metodologi Penelitian.....	33
Gambar 3.2 Topologi <i>Network Environment</i>	35
Gambar 3.3 Topologi <i>Network Environment with Attack</i>	36
Gambar 3.4 Skenario Simulasi Serangan.....	37
Gambar 3.5 Proses Analisis Serangan dan <i>SIEM</i>	39
Gambar 4.1 Nilai Indeks (KAMI) <i>Pre-Assessment</i> Diskominfo Kota Tegal.....	42
Gambar 4.2 Grafik nilai per-Aspek indeks (KAMI) Diskominfo Kota Tegal.....	43
Gambar 4.3 Konfigurasi <i>Ip Router Mikrotik</i>	44
Gambar 4.4 Konfigurasi Topik <i>Logging Router Mikrotik</i>	44
Gambar 4.5 Konfigurasi <i>Remote Logging router Mikrotik</i>	45
Gambar 4.6 Konfigurasi <i>Mirroring Port Switch A</i>	45
Gambar 4.7 Konfigurasi <i>Mirroring Port Switch B</i>	46
Gambar 4.8 <i>Mac Flooding</i> dengan <i>Macof</i>	48
Gambar 4.9 Tabel <i>Arp End User Windows</i> Jaringan Yang di <i>Mac Flooding</i>	49
Gambar 4.10 Proses Pemilihan Target Aset <i>router Mikrotik</i> dan End User.....	50
Gambar 4.11 <i>Ettercap</i> Melakukan <i>Arp Poisioning</i> ke <i>router Mikrotik</i>	50
Gambar 4.12 <i>CDP Flooding</i> dengan <i>Yersinia</i>	51
Gambar 4.13 <i>DHCP Starvation</i> dengan <i>Yersinia</i>	52
Gambar 4.14 <i>DHCP Rogue</i> dengan <i>Yersinia</i>	52

Gambar 4.15 <i>Syn Flooding</i> dengan <i>Hping3</i>	53
Gambar 4.16 <i>Bruteforce SSH</i> dengan <i>Hydra</i>	54
Gambar 4.17 <i>Bruteforce FTP</i> dengan <i>Hydra</i>	54
Gambar 4.18 Nilai <i>Post-assessment</i> indeks KAMI Diskominfo Kota Tegal.....	59
Gambar 4.19 Nilai Indeks (KAMI) <i>Pre-Assessment</i> Diskominfo Kota Tegal.....	60
Gambar 4.20 Nilai indeks (KAMI) <i>Pre</i> dan <i>Post-assessment</i> Diskominfo Kota Tegal.....	62

