Lampiran

Tabel 4. 7 Pengujian Hasil Tahapan ENFGP

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
1	**Preparation**		Preparation merupakan tahapan awal di mana berisi tentang langkah -langkah maupun kebutuhan baik *tools software* ataupun *hardware* yang akan digunakan pada awal investigasi	• Identifikasi kebutuhan • *Lireture Review*
2		**Indentifikasi Kebutuhan**	*Literatur review* akan membahas tentang uraian dari teori, temuan-temuan maupun rangkuman – rangkuman dari penelitian sebelumnya yang nanti dapat digunakan sebagai landasan atau acuan dalam melakukan kegiatan penelitian	• *Software* • *Hardware*
3		**Study literature**	*Identification* kebutuhan akan disesuaikan dengan kondisi pada kasus seperti kebutuhan perangkat keras maupun perangkat lunak	• *Network* Forensik • Penelitian Sebelumnya • konsep dasar deteksi MITM base *Evil Twin*
4	**Detection Evil twin**		*Detection* merupakan salah tahapan awal dimana, investigator melakukan prosess *scanning* untuk menemukan adanya kemungkinan AP palsu	• *Detection* menggunakan Chellam
5		**Scanning**	Scanning merupakan tahapan prosess *scanning population* AP yang di lakukan di suatu *public Area*	• *Scanning* ditemukan adanya ancaman serangan *Evil Twin*
6		**Notification**	*Notification* merupakan pemberi informasi apabila ditemukanadanya serangan *Evil Twin/Rogue* AP.	• Notifikasi serangan *Evil Twin*, untuk Lebih jelasnya dapat di lihat pada Gambar 4.5

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
7	**Collection Evil Twin**		*Collection Evil Twin* merupakan tahapan pengumpulan data dan informasi terkait AP yang mencurigakan.	
8		**Scanning AP & Capture wifi Traffik**	*Scanning* AP di lakukan dengan menggunakan aplikasi Chellam dan Acrlyric-wifi, dengan bertujuan untuk menggumpulkan data data AP	• *Scanning* detail info menggunakan Chellam • *Capture* Traffik menggunakan Acrlyric-
9		**Data Scanning Population**	data *scanning* berupa tabel informasi hasil *capture* traffik *wfii*	• Tabel info detail • file Pcap
10	**Approach Strategy**	**Entry into the network evil twin AP**	Masuk ke dalam jaringan Evil Twin ketika ditemukan adanya Notifikasi serangan *Evil twin* dengan Tujuan Untuk mengumpulkan informasi lebih lanjut	• Masuk ke dalam jangkaun *Evil twin* untuk melakukan proses *caprture* Traffik
11	**Detection MITM**		Proses *detection* MITM di lakukan Untuk menidentifikasi adanya kemungkan serangan MITM.	• Deteksi Arp attack menggunkan Xarp
12		**Scan Arp Attack**	Proses *Scanning* Arp Attack menggunakan Aplikasi Xarp, untuk menemukan adanya serangan ARP	• Dari hasil *scan* ditemukan adanya serangan ARP *attack*, dimana terlihat

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
13		**Notification**	*Notication* di berikan apabila ditemukan adanya serangan ARP.	• Notifikasi serangan dapat di lihat pada Gambar 4.12
14	**Collection MITM**		*Collection* MITM, merupakan tahapan penggumpulan informasi terkait dengan serangan MITM	• Proses *collection* di lakukan menggunakan aplikasi Wireshark, dan
15		**Capture wifi Traffik**	*Capture* Traffik dilakukan dengan mengamati laluntas data di dalam jaringan *Evil Twin* , dengan menggunkan aplikasi Wireshark	• File Pcap dengan nama : Mitm analisa.Pcap
16		**File Pcap**	File Pcap merupakan file hasil capture traffik yang di simpan dalam bentuk pcap. File Pcap berisitentang informasi laluntas data yang teriadi di dalam jaringan	• Hasi *capture* file dapat dilihat pada tabel 4.1
17	**Preservation**		*Preservation* adalah tahapan pengamann informasi yang ditemukan dalam prosses *collection*	• Dari hasil *scan* ditemukan adanya serangan ARP *attack*, dimana terlihat *source* IP 10.0.0.1 melakukan recquest pada

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
18	**Acquisitions**		Akuisisi data serangan merupakan hasil pengakuisisian data network traffik dengan menggunakan beberapa metode seperti filterisasi maupun memanfaatkan modul modul pada wireshark lainnya	• Proses akuisisi dengan menggunkan *tools* Wireshark, Networkminer, Chellam dan Acrlyric-wifi
19		**Tabel informasi Evil Twin attack**	Tabel informasi merupakan data dari tabel scanning dan file pcap, hasil dari prosses Capture Traffik	• Tabel dan informasi *Evil Twin Attack* merupakan informasi yang dikumpulakan pada tahapan *collection*
20		**Tools Chellam & Acrlyric-wifi**	Chellam digunakan untuk menaganalisa data *scanning* AP dan Acrlyric digunakan untuk melakukan *capture* traffik	• Hasil analisa dapat dilihat pada Gambar 4.7, 4.8, 4.9, 4.10
21		**MITM attack .pcap**	File Pcap hasil capture traffik lalulintas data dalam jaringan *Evil Twin*	• Akuisisi file pcap • Akuisisi menggunkan modul hirarki
22		**Tools wireshark & network miner**	Prosses akuisisi dilakukan menggunkan aplikasi Wireshark dan Networkminer	• Dari hasil *scan* ditemukan adanya serangan ARP *attack*, dimana terlihat *source* IP 10.0.0.1

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
23	**Analysis And Investigation**		Merupakan tahapan proses analisis dan investigasi forensik	• Proses analisa daninvestigasi menggunakan Metode *live* forensik
24		**Analisa data scanning AP**	Merupakan tahapan dalam menganalisa data scanning dan file Pcap	• Analisa di lakukan dari data yang terlihat pada Gambar 4.7, 4.8, 4.9, 4.10
25		**Hasli analisa wifi**	Merupakan proses akhir dan menemukan hasil analisa dari proses sebelumnya.	• Dari hasil scanning ditemukan adanya dua AP yang menggunakan SSID "PUSFID", dengan Mac "e4:8d:8c:ca:80:c0, dengan kode vendor : "Routerboard.com,

Tabel Hasil Tahapan ENFGP Lanjutan

NO	TAHAPAN INVESTIGASI		KETERANGAN	HASIL PENGUJIAN
26		**Bukti evil twin attack/rouge AP**	Proses penemuan barang bukti *digital Evil Twin* Ap yang ditemukan melalui prosses analisa sebelumnya.	• Notifikasi dari Chellam • SSID dengan Mac: f4:f2:6d:1c:76:15, dengan kode Vendor : "Tp-Link technologies.co.ltd", kekuatan
27		**Analisa File pcap**	Merupakan tahapan tahapan untuk menganalisa file Pcap dari hasil *capture* traffik pada jaringan *Evil Twin* .	• Deteksi IP • Analisa Port ARP
28		**Hasil analisa Trafik**	Merupakan tahapan akhir dari proses analisa *capture* trafik.	• hasil analisa dapat dilihat pada Gambar 4.14, 4.15, 4.16 dan 4.7
29		**Bukti digital MITM attck**	Proses penemuan barang bukti *digital* MITM *Attcak* yang ditemukan melalui prosses analisa sebelumnya.	• IP dan Mac pelaku : 10.0.0.1/Tp-link_89:7a:15
30	**Reporting**		merupakan proses akhir, yaitu penyusunnan laporan dari hasil informasi barang bukti yang ditemukan dari beberapa tahapan analisa sebelumnya	• Hasil laporan di buat berdasarkan evaluasi dan hasil dari tahapan analisa

ISLAM
UNIVERSITAS
INDONESIA

ISLAM
UNIVERSITAS
INDONESIA