BAB III

METODE PENELITIAN

3.1 Objek Penelitan

Objek penelitian yang diteliti ini bertempat di Kantor Desa Citapen Kabupaten Bandung Barat dengan memiliki SSID publik *wifi* KANTORDESA. Kemudian target serangan yang diuji yaitu perangkat Laptop dan perangkat Android yang terhubung pada jaringan Kantor Desa. Peneliti mengambil objek penelitian ini dikarenakan perangkat –perangkat tersebut selalu terhubung dengan koneksi internet untuk kegiatan sehari-hari, baik dalam hal pekerjaan maupun kegiatan pribadi.

Para pengguna *wifi* publik kadang hanya memikirkan dapat mengakses internet dengan gratis tanpa memikirkan kemanan data-data yang terkirim pada jaringan tersebut. Sehingga menimbulkan kerentanan data-data tersebut tercuri tanpa sepengetahuan pengguna.

3.1.1 Profil Secara Umum

Kantor Desa Citapen adalah salah satu tempat aparatur desa untuk melakukan tugas dan fungsinya di desa Citapen. Kantor desa ini beralamatkan di Jalan Cihampelas no 12, Kabupaten Bandung Barat, Jawa Barat, Indonesia.

Berdasarkan metode pengumpulan data yaitu dengan melakukan observasi berkaitan dengan penelitian, didapatkan *access point* yang digunakan oleh pihak Kantor Desa Citapen.

3.1.2 Spesifikasi Objek

Adapun spesifikasi dari objek penelitian yang akan dilakukan pengujia adalah sebagai berikut :

a. *Access Point*

Untuk media pengujian dengan serangan *arp spoofing, dns spoofing* dan *packet sniffer* dibutuhkan *access point* yang berfungsi mengatur transmisi data sehingga dapat menghubungkan *client* dengan jaringan internet. Spesifikasi dari *access point* dengan SSID KANTORDESA adalah sebagai berikut :

Tabel 3.1 Spesifikasi *access point* SSID KANTORDESA

Nama	Merk	Model	SSID
Access Point	Huawei	EchoLife HG8245H	KANTORDESA

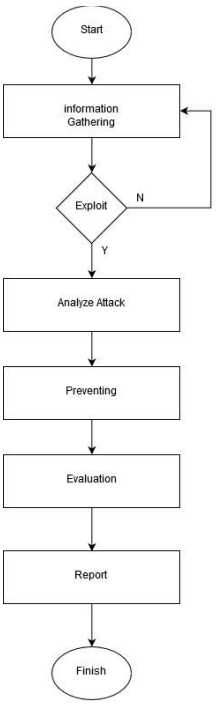
b. *Client*

Objek penelitian yang digunakan sebagai media mendapatkan informasi secara pribadi dan juga simulasi untuk melakukan pengujian dengan metode *penetration testing* sebagai target/*client* adalah perangakat Laptop dan *Smartphone* Android yang terkoneksi pada jaringan *wifi* dengan SSID KANTORDESA.

3.2 Metode Pengujian

Metode pengujian yang peneliti gunakan adalah *penetration testing*. *Penetration Testing* (Pentest) adalah sebuah metode untuk melakukan evaluasi terhadap keamanan dari sebuah system dan jaringan komputer. Evaluasi dilakukan dengan cara melakukan serangan.

Hasil dari pengujian *Penetration testing* ini sangatlah penting bagi pengelola sistem sebagai tolak ukur untuk meningkatkan keamanan dari sisi komputer maupun jaringannya. Laporan hasil dari pentest ini memberikan masukan terhadap kerentanan yg terdapat pada sistem, sehingga memberikan kemudahan untuk melakukan evaluasi pada sistem keamanan yang sedang berjalan. Berikut alur pentest yang peneliti lakukan :



Gambar 3.1 Alur *Penetration Testing* Peneliti

3.3 Metode *Penetration Testing*

Disini peneliti akan menjelaskan setiap tahap dari *penetration testing* yang telah ditunjukkan pada gambar di atas. Untuk penjelasan metode pengujian adalah sebagai berikut :

3.4.1 *Information Gathering*

Dalam tahap ini peneliti mencari informasi tentang kebutuhan untuk melakukan tes penetrasi, seperti :

1. Mengaktifkan mode monitor pada *interface wireless* yang dapat mendukung aktifitas monitoring *wireless.*
2. Memonitor keberadaan dan informasi *Access Point* yang berada di sekitar.
3. Informasi ini berupa *BSSID, SSID, Channel,* jenis enkripsi, dan *WPA Handshake.*
4. Melakukan *Crack password wifi* menggunakan *tools ariodump-ng, aireplay* dan *hashcat.* guna mendapatkan informasi *password access point* menggunakan informasi yang sudah didapatkan sebelumnya.
5. Melakukan pencarian informasi *ipaddress client* yang terhubung pada jaringan menggunakan *tools nmap.*

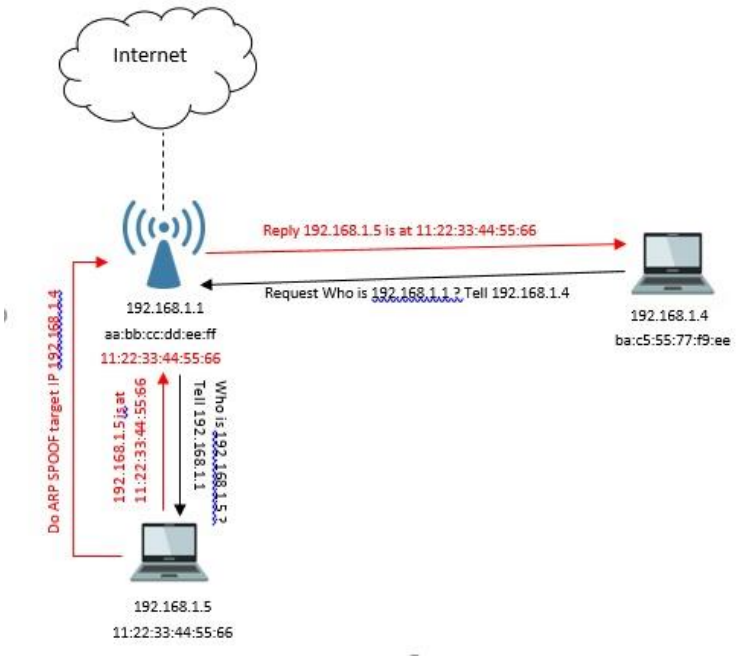
3.4.2 *Exploit*

Pada tahap ini merupakan proses pengujian dengan penyerangan sesuai dengan judul yang peneliti ambil yaitu *arp spoofing, dns spoofing* dan *packet sniffer*. Serangan tersebut bertujuan untuk mengambil data-data pada *client* yang terhubung pada jaringan secara diam-diam atau tanpa sepengetahuan

client. Untuk penjelasan tentang masing-masing serangan akan dijelaskan sebagai berikut :

a. *Arp Spoofing*

Serangan yang dipakai peneliti disini adalah *arp spoofing* dengan menggunakan program yang peneliti dapatkan pada situs *github.com*. Dengan target serangan berupa *Access point* yang memiliki SSID KANTORDESA serta *client* yang terhubung pada jaringan tersebut. Berikut alur kerja / scenario dari serangan *arp spoofing* :



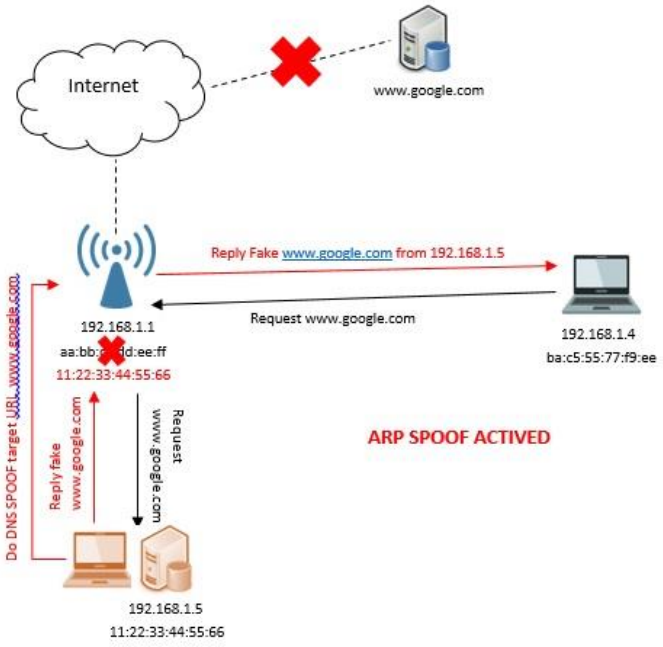
Gambar 3.2 Skenario *ARP Spoofing*

Tabel 3.2 Skenario Serangan *Arp Spoofing*

No	Proses Serangan	Keterangan
1	Information Gathering	1. Melakukan *scanning ip address client* terhadap jaringan *wifi* KANTORDESA menggunakan *tools nmap*.
2	*spoofing*	1. Mengetikkan *command* dan memasukan *ip taget* dan *ip gateway* untuk menjalankan program. 2. Melakukan *spoofing* terhadap *router.* Mengganti *mac address router* menjadi *mac address* peneliti. 3. Mengaktifkan *ipforward* agar target yang diserang masih bisa melakukan akses ke *internet*.
3	*Man In The Middle*	1. *Mac Address* router sudah terganti dengan *Mac Address* peneliti. 2. Setiap *packet* yang terkirim dari perangkat *cliet* akan diteruskan terlebih dahulu ke perangkat *peneliti* kemudian diteruskan kembali ke *router*.

b. *Dns Spoofing*

Serangan yang dipakai peneliti disini adalah serangan *Dns Spoofing* dengan menggunakan program yang peneliti dapatkan pada situs *github.com.* Serangan ini bisa dilakukan apabila peneliti sudah berada di tengah-tengah komunikasi antara target dengan *gateway*, yang berarti peneliti harus sudah berhasil melakukan *Arp Spoofing* terlebih dahulu. Berikut alur kerja / scenario dari serangan *dns spoofing* :



Gambar 3.3 Skenario Dns Spoofing

Tabel 3.3 Skenario Serang Dns Spoofing

No	Proses Serangan	Keterangan
1	Membuat *Fake Website*	1. *Download file html* yang menyerupai tampilan situs aslinya. Kemudian diterapkan pada *file html index.html* peneliti yang berada di */var/www/html/index.html.*
2	Aktifkan *Apache2*	1. Mengaktifkan *Apache2* sebagai *DNS Server local* peneliti, sehingga dapat diakses dari luar perangkat peneliti.
3	*Spoofing*	1. Menjalankan program serangan *DNS Spoofing* dengan mengetikkan *command*. Serta menambahkan parameter situs yang akan di *spoof* dan *ip address* peneliti.
4	Mendapatkan data *login Client*	1. Jika *client* tidak sadar akan serangan *DNS Spoof* dan memasukan *username & password*nya maka data tersebut akan didapatkan oleh peneliti. 2. *Client* akan disambungkan lagi ke *google.com* yang asli.

c. *Packet Sniffer*

d. *Sdfsdfsd*

3.4.3 *Setting Iptables and Ip Forward Rules*

Dalam tahap ini peneliti melakukan konfigurasi terhadap *iptables* dan *ip forward* pada laptop penguji di sistem operasi *Kali Linux 2019.2*. Berikut perintahnya :

Tabel 3.1 Beberapa Rules Yang Digunakan Pada *Iptables*

Nama	Jenis Rules	Rules
Iptables	INPUT	$iptables –I INPUT –j NFQUEUE ACCEPT $iptables –I INPUT –j DROP $iptables –I INPUT –j NFQUEUE –queue-num [number]
	OUTPUT	$iptables –I OUTPUT –j ACCEPT $iptables –I OUTPUT –j DROP

		$iptables –I OUTPUT –j NFQUEUE –queue-num [number]
	FORWARD	$iptables –I FORWARD –j ACCEPT $iptables –I FORWARD –j DROP $iptables –I FORWARD –j NFQUEUE –queue-num [number]

Tabel 3.2 Rules Yang Digunakan Pada *IP Forward*

Nama	Jenis Rules	Rules
Ip Forward	Forward	$echo 1 > /proc/sys/net/ipv4/ip_forward $echo 0 > /proc/sys/net/ipv4/ip_forward

3.4.4 *Exploit*

Dalam tahap ini peneliti melakukan *exploit* dengan cara mengeksekusi semua program yang telah dibuat menggunakan python. Program tersebut

bertujuan menjadi *Man In The Middle* antara komunikasi target dengan router. Serta mengambil informasi target secara diam-diam.

3.4.5 *Final Analysis*

Dalam tahap ini peneliti melakukan analisis paket data pada jaringan tersebut menggunakan *wireshark*. Guna mengetahui perilaku serangan *arp spoof*, *dns spoof* dan *packet sniffer*.

3.4.6

3.4.7 Asdasda

3.4.8 asdada