**BAB III**

**METODE PENELITIAN**

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.

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.

1. **Spesifikasi Objek**

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

1. ***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 |

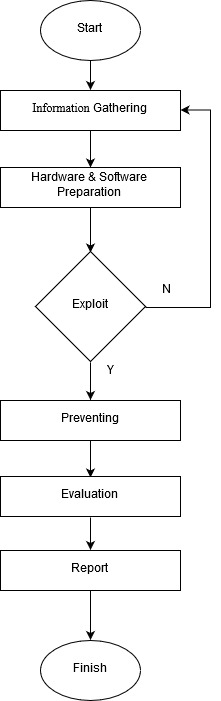
1. ***Client***

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.

1. **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**

1. **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 :

1. ***Information Gathering***

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

1. *Password Wifi* Kantor Desa Citapen

Dalam tahap ini peneliti mencari informasi tentang *password wifi* agar terkoneksi pada jaringan *wifi* tersebut.

1. *Website*

Dalam tahap ini peneliti mencari informasi tentang situs yang sering diakses di lingkup Kantor Desa Citapen untuk keperluan serangan *Dns Spoofing.*

1. ***Create Program***

Dalam tahap ini peneliti membuat program untuk keperluan serangan, yakni program *arp spoof, dns spoof* dan *packet sniffer*. Program ini peneliti tulis menggunakan Bahasa pemograman *python* pada aplikasi *code editor* *pycharm IDE.* Serta memasukan daftar *website* yang sering dikunjungi di lingkup Kantor Desa Citapen yang sudah di

1. ***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 |

1. ***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.

1. ***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*.

1. Asdasda
2. asdada