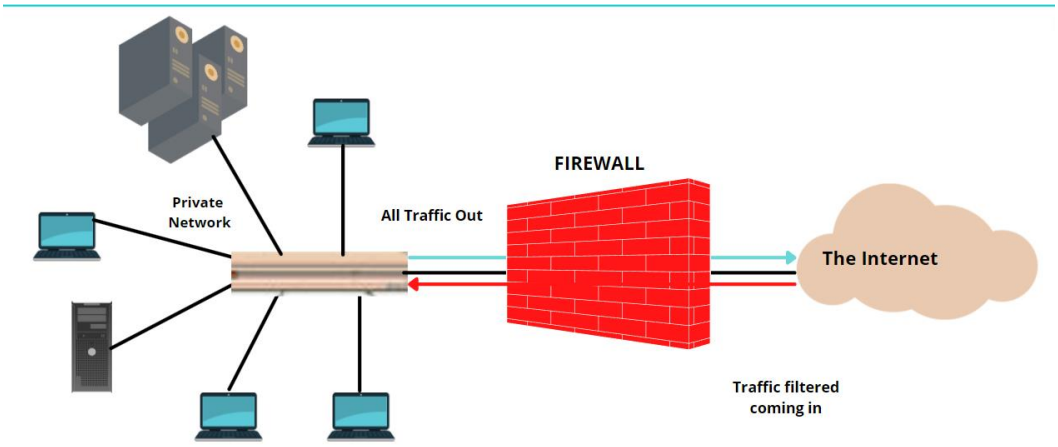
UTS Keamanan Informasi

Juan Pahlevy Sutrisno

20190801219

a. Keamanan Jaringan




Penjelasan: Pada tahap pengujian sistem keamanan yang telah dibangun, disini saya akan menjelaskan mengenai hasil laporan pengujian PC Router sebagai Firewall menggunakan 2 aplikasi, yaitu :

1. NMap

2. Hping3

1. Nmap (Network Mapper)

Nmap digunakan untuk melakukan port scan/port sweep yang bertujuan untuk mengumpulkan informasi/reconnaissance terhadap komputer target yaitu layanan apa saja yang disediakan oleh komputer target atau web server Private Cloud.

Pada pengujian sistem keamanannya dilakukan dua kali percobaan (percobaan 1 dan 2) yang masing-masing percobaan menggunakan fitur Nmap TCP Connect () Scan, yang dimana scan ini mengirim paket TCP utuh (SYNSYN_ACK-ACK) pada komputer target kemudian periksa hasil data log sistem keamanan terhadap scan tersebut. Untuk dapat melakukan Nmap TCP Connect () Scan, ketikkan perintah berikut pada terminal: Nmap –sT 192.168.10

2. Hping3

Hping3 digunakan untuk melakukan serangan DOS (Denial Of Service) yang berupa ICMP Flood yang dimana bertujuan untuk membanjiri komputer target dengan paket ICMP_ECHO_REQUEST yang berjumlah sangat banyak sehingga dapat menghabiskan resource (CPU Usage) yang dimiliki komputer target.

Untuk dapat melakukan Hping3, ketikkan perintah di bawah ini pada terminal:

*hping3-p 8o --flood--icmp 19.168.1.10*

Agar proses analisa data log dari setiap keadaan pengujian lebih efisien dan mudah dianalisa, maka untuk setiap pengujian file log akan dihapus kemudian dibuat kembali, serta log daemon serta sistem keamanan yang digunakan direstart. Efeknya agar setiap pengujian paket yang di-log oleh Iptables/Psad dapat berjumlah hingga ribuan paket sehingga dapat menyebabkan kesulitan dalam menganalisa data log dari setiap keadaan pengujian pada PC Router. Serta sampel log yang diambil adalah paket yang berada diurutan terakhir agar lebih efisien dalam menganalisa paket tersebut.

Paket yang di log merupakan paket yang memiliki prefix sebagaimana berikut :

“INVALID PKT “ Paket yang termasuk/memiliki prefix ini adalah paket yang tidak sesuai/invalid dengan state yang ada. Artinya tidak termasuk kedalam koneksi apapun yang berjalan/ada pada server.

“SPOOFED IP “ Paket yang memiliki prefix ini adalah paket yang berasal dari LAN 1 yang memiliki alamat sumber sama dengan alamat IP dari LAN 2.

“DROP PKT “ Paket yang memiliki prefix ini adalah paket yang tidak sesuai dengan rules yang ada pada firewall.

“ICMP FLOOD “ Paket yang memiliki prefix ini adalah paket yang terdeteksi sebagai paket DOS ICMP Flood.

Pengujian PC Router sebagai Firewall

Pada pengujian PC Router sebagai Firewall, fitur keamanan firewall yang digunakan yaitu Iptables. Dimana firewall Iptables sudah terkonfigurasi dan diatur paket-paket apa saja kah yang diijinkan masuk kedalam jaringan/web server dan 38 mana yang tidak (rules and policy). Paket yang tidak sesuai dengan rules/policy yang diterapkan akan di log dan data log tersebut akan dianalisis.

Pengujian Menggunakan Nmap : Digunakan Nmap TCP Connect Scan () untuk melakukan port scan/sweep terhadap web server cloud dan melihat hasilnya apakah firewall berfungsi dengan baik. Berikut merupakan hasil tampilan dari Nmap ketika firewall diterapkan.

Pengujian Menggunakan Hping3 : Untuk melakukan serangan DOS, digunakan tools hping3 yang dimana tipe DOS yang dilakukan adalah ICMP Flood. Ketikkan perintah berikut pada terminal dan perhatikan hasil nya pada server dan data log sistem keamanan ketika firewall Iptables diterapkan.

b. Untuk Syntak nya:

```
<?php
$mysqli = mysqli_connect("localhost", "root", "", "keamananinformasi");
if ($mysqli){
    echo "" . mysqli_connect_error();
```

```
}

$name = "Juan";
$password = "";

$name = $mysqli->real_escape_string($name);
$password = $mysqli->real_escape_string($password);

$sql = "SELECT * FROM user WHERE name='$name' AND password='$password'";

if ($result = $mysqli->query($sql)){
    print_r($result->fetch_object());
}
```

c. Untuk bagian C saya sudah menjelaskan di youtube
   https://youtu.be/f-H1hl2lTts
d. Untuk step step bagian D seperti ini:
   Step 1 : mkdir rsa_key_pair
   Step 2 : cd rsa_key_pair/
   Step 3 : openssl genrsa -des3 -out private.pem 2048
   Step 4 : Input pass pharse (isi bebas)
   Step 5 : generate public key
   Step 6 : openssl rsa -in private.pem -outform PEM -pubout -out public.pem
   Step 7 : Input pass pharse lagi (isi pass bebas)
   Step 8 : code . (redirect ke visual studio code)

   dan penjelasanya:
   https://youtu.be/Sd4-ANDIy4U