Nama: Limas Baginta

NPM:1306368690

Jurusan: Teknik Komputer

Praktikum: Keamanan Jaringan Komputer

Case Study Modul 8

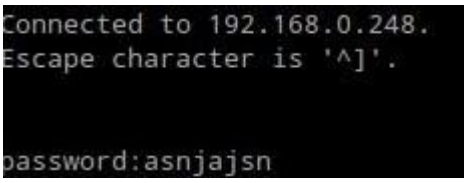
**Tugas 1**

Commmand nmap scanning:

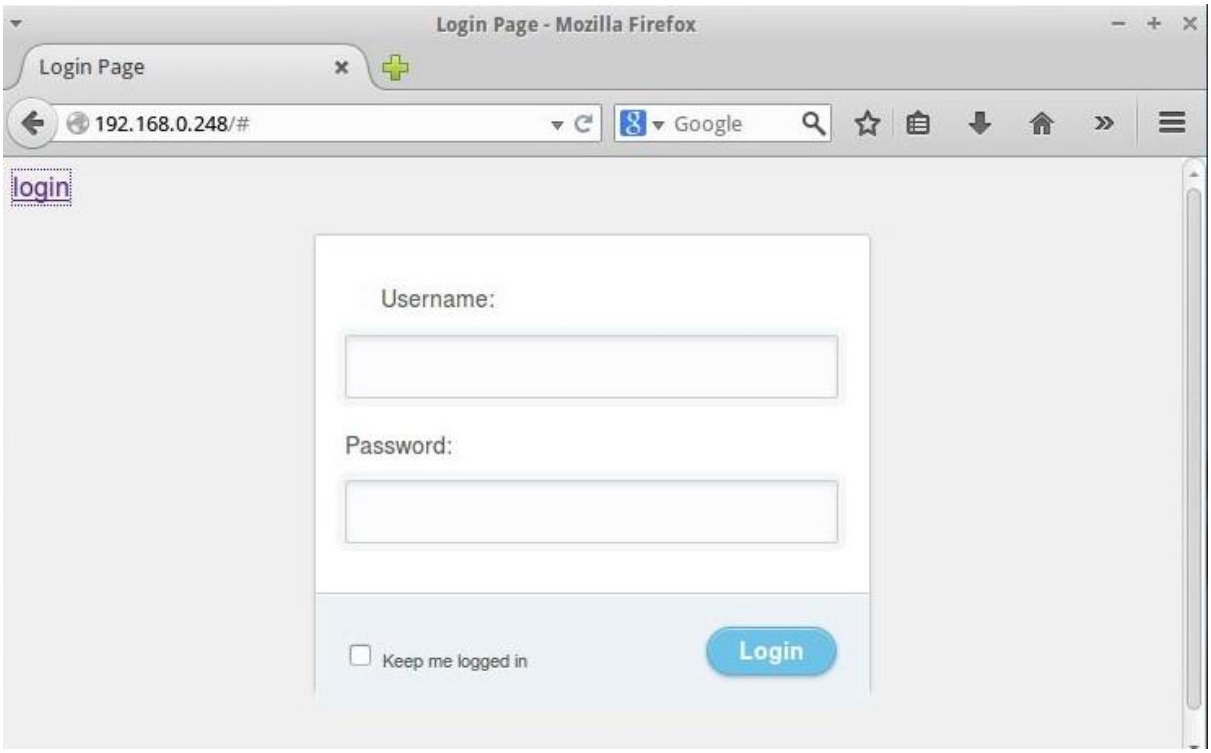
**nmap –sP [target address]**

maka nmap akan mulai melakukan scan


Hasil Telnet



**Tugas 2**




Analisa hasil:

Pada dasarnya, praktikum Honepot ini termasuk Low-Interaction Honeypot yang merupakan metode pengelabuhan hacker yang paling mudah diinstal dan dipelihara karena desainnya yang sederhana dan fungsionalitas dasar. Normalnya teknologi ini hanya meniru berbagai macam service.

Contohnya, honeypot dapat meniru server Linux dengan beberapa service yang berjalan, seperti Telnet dan FTP. Penyerang dapat melakukan Telnet ke honeypot, mendapatkan identitas system operasi, dan bahkan mendapatkan prompt **login**.

Penyerang dapat melakukan login dengan metode brute force ataumenebak password. Honeypot akan merekam dan mengumpulkan percobaan login yang dilakukan oleh penyerang.

**Tugas 3**

Hydra  ftp bruteforce

```
Hydra (http://www.thc.org/thc-hydra) starting at 2015-11-18 10:43:16
[DATA] 16 tasks, 1 server, 500 login tries (l:1/p:500), ~31 tries per task
[DATA] attacking service ftp on port 21
```

```
Hydra (http://www.thc.org/thc-hydra) starting at 2015-11-18 10:43:16
[DATA] 16 tasks, 1 server, 500 login tries (l:1/p:500), ~31 tries per task
[DATA] attacking service ftp on port 21
Process 2843: Can not connect [timeout], process exiting
Process 2847: Can not connect [timeout], process exiting
Process 2853: Can not connect [timeout], process exiting
Process 2844: Can not connect [timeout], process exiting
Process 2845: Can not connect [timeout], process exiting
Process 2855: Can not connect [timeout], process exiting
Process 2846: Can not connect [timeout], process exiting
Process 2848: Can not connect [timeout], process exiting
Process 2849: Can not connect [timeout], process exiting
Process 2850: Can not connect [timeout], process exiting
Process 2851: Can not connect [timeout], process exiting
Process 2852: Can not connect [timeout], process exiting
Process 2854: Can not connect [timeout], process exiting
Process 2856: Can not connect [timeout], process exiting
Process 2857: Can not connect [timeout], process exiting
Process 2858: Can not connect [timeout], process exiting
```

Analisa log:

Pada gambar screenshot terlihat bahwa terdapat 16 task yang melakukan serangan pada servis FTP pada port 21. Walaupun demikian,beberapa proses serangan tidak mampu menembus port,  seperti yang terihat pada gambar terbaca,

Process <Number>: Can not connect [timeout], process exiting

Ini  mengindikasikan bahwa beberapa proses dari serangan Bruteforce menjadi timeout dan proses dikeluarkan secara langsung sehingga attacker tidak dapat membaca informasi port 21 untuk UDP seluruhnya.

Dalam hal penggunaan ftp, perlu ada pembatasan remote user untuk mengakses file. Ini dikarenakan file /etc/ftpusers sendiri sering digunakan untuk membuat daftar user yang tidak diizinkan untuk dapat mengakses file apapun menggunakan FTP.

**Tugas 4**

Command yang digunakan:

```
/home/honeydrive# nmap -O 192.168.0.248
```

Selanjutnya, nmap akan memulai scan

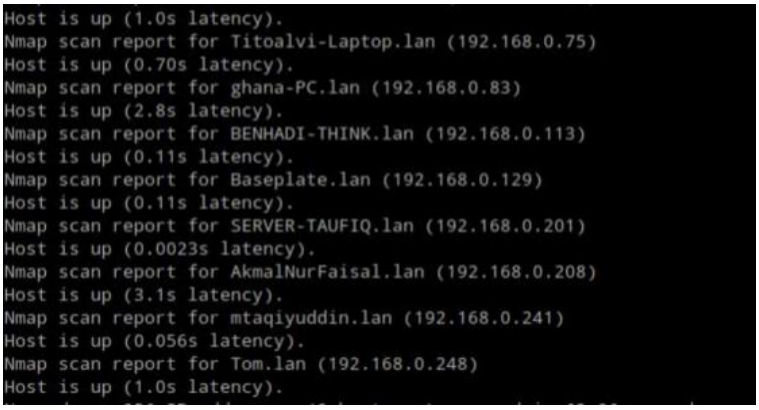
```
Starting Nmap 5.21 ( http://nmap.org ) at 2015-11-18 10:48 GMT
Nmap scan report for Tom.lan (192.168.0.248)
Host is up (0.0092s latency).
Not shown: 752 filtered ports
```

Lalu didapatkan  OS dari target yakni, Windows 7

```
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING) : Microsoft Windows Vista|2008|7 (93%), FreeBSD 6.X (86%
)
Aggressive OS guesses: Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or W
indows 7 (93%), Microsoft Windows Vista Business SP1 (89%), Microsoft Windows Vi
sta Home Premium SP1 or Windows 7 (87%), FreeBSD 6.2-RELEASE (86%), Microsoft Wi
ndows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

Scanning terhadap semua port yang terbuka




Yang harus dilakukan agar honeypot tersebut lebih baik adalah melakukan instalasi Honeyd dan menggunakannya, dimana Honeyd adalah low interaction honeypot client yang menciptakan virtual host (Honeypots) dalam jaringan sehingga dapat mengelabuhi attacker bahwa ip server up.

Honeypot ini dapat dikonfigurasi untuk bertindak seperti sebuah sistem operasi yang nyata. Pada saat yang sama kita dapat mengkonfigurasi sistem-sistem operasi untuk mengaktifkan layanan seperti FTP, HTTP, Telnet, dan lain-lain.