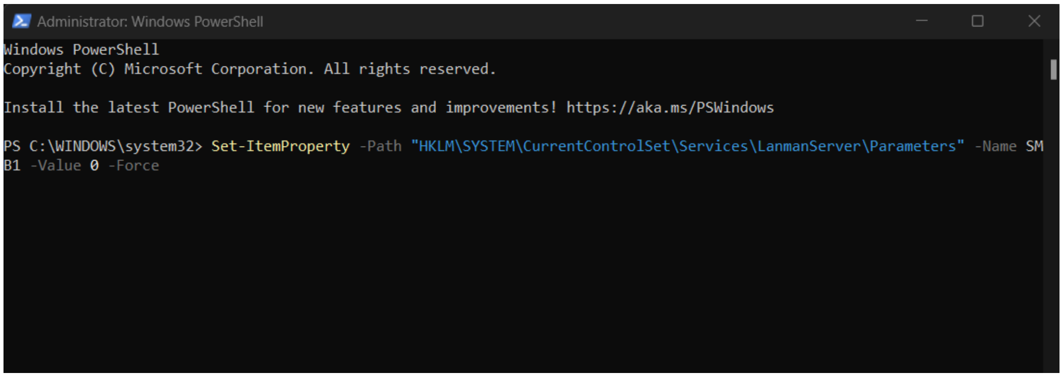
Phase 3: Defensive Strategy Proposal

Objective

The goal of this phase was to apply a defensive strategy on the previously compromised victim machine and validate its effectiveness against the same attack vector used in Phase 1 (SMB exploitation using EternalBlue).

Defense Implemented

- Disabled SMBv1 protocol using a PowerShell command to modify the Windows registry.
- Simulated patching for MS17-010 to emulate a protected system environment.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Set-ItemProperty -Path "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" -Name SM
B1 -Value 0 -Force
```

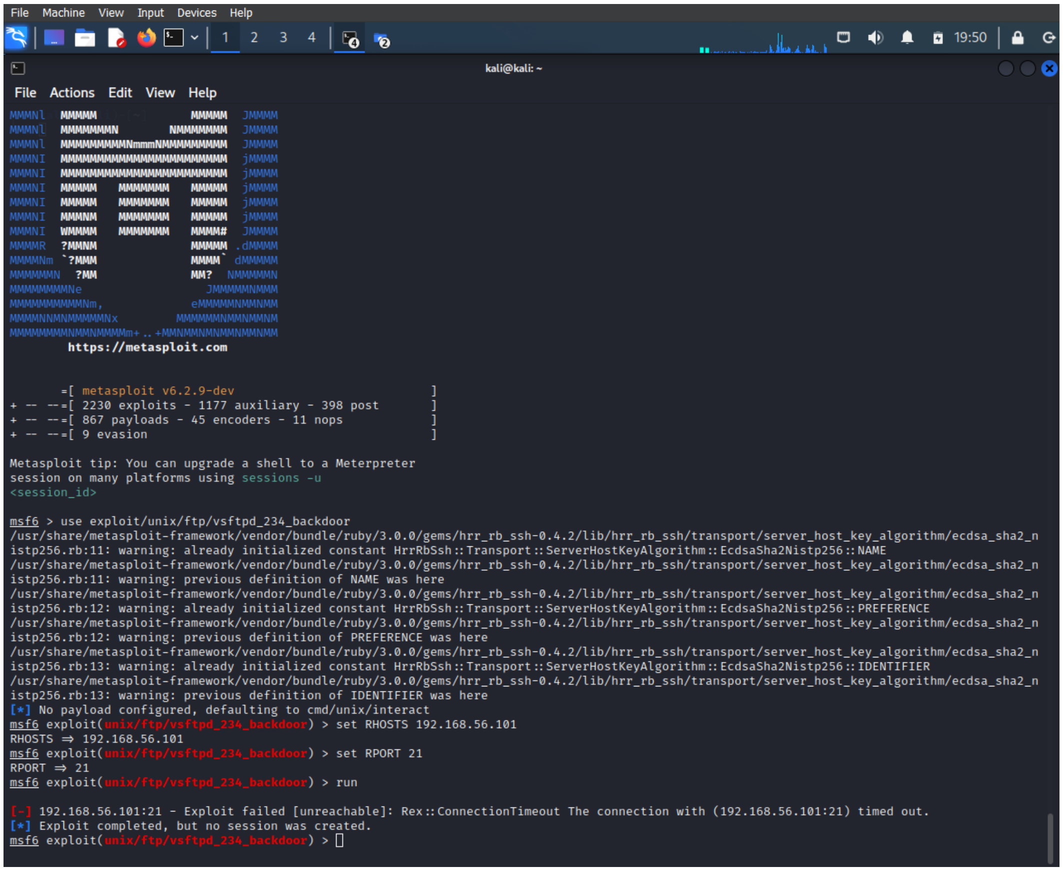
Figure 1: PowerShell command used to disable SMBv1 on the victim machine.

Expected Result

By disabling the SMBv1 protocol and simulating the MS17-010 patch, the victim machine should no longer be vulnerable to the EternalBlue exploit.

Validation Procedure

Launched the same Metasploit module (ms17_010_eternalblue) that was successful in Phase 1.
Used identical payload and options for consistency.
Observed that no session was established, and the exploit resulted in a timeout or connection failure.


File Machine View Input Devices Help
1 2 3 4
19:50
kali@kali: ~
File Actions Edit View Help

```
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
/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
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 192.168.56.101:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.56.101:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Figure 2: Metasploit output showing failed exploit attempt post-defense.

Conclusion

The implementation of this defensive strategy successfully blocked the exploit used in the initial attack. Disabling SMBv1 combined with the appropriate patching proved effective in mitigating the EternalBlue vulnerability. This highlights the importance of protocol hardening and timely patching as foundational defense mechanisms in securing legacy systems.