

ICS344 Information security

Term Project

Defensive Strategy Proposal

Phase#3

Team

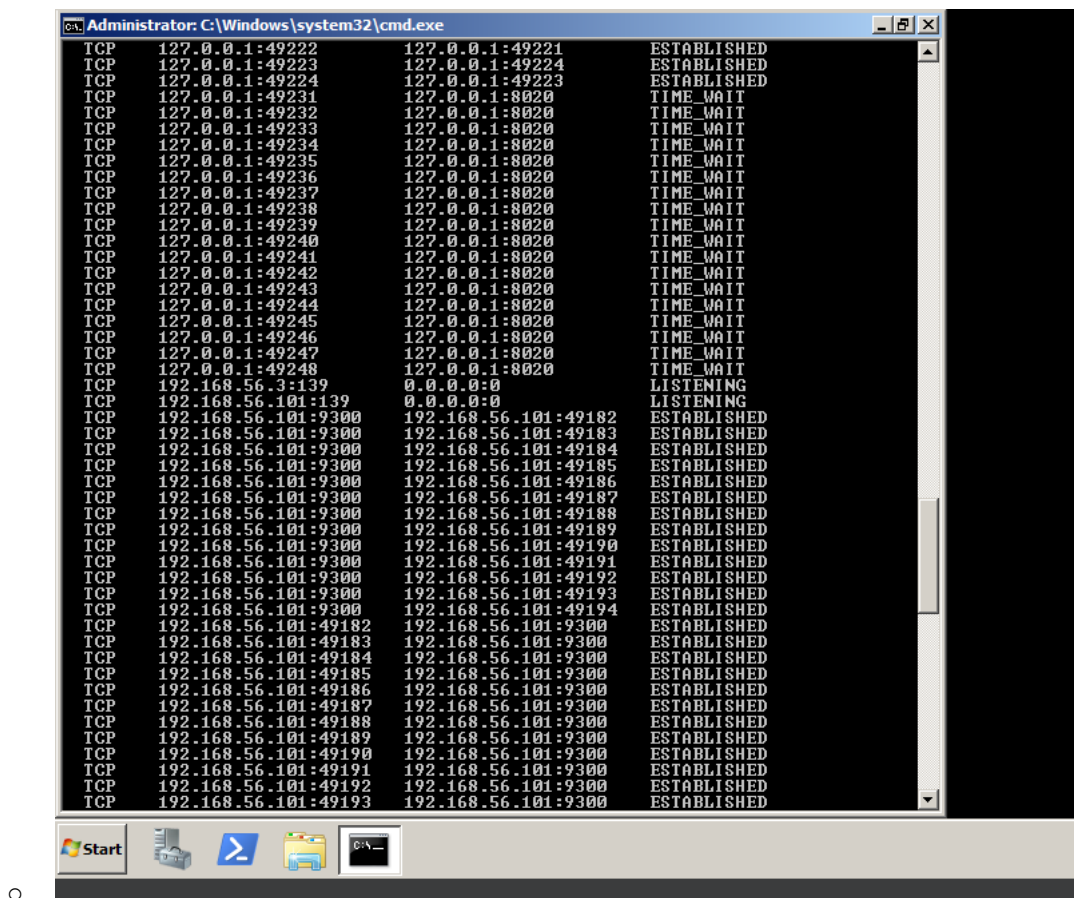
Name	ID
Ismael Arqsosi	202182150
Taha Ali	202045620
Saad Alharbi	201935590

Phase 3: Defense & Remediation

3.1 Simulated Pre-Defense State

Because the attack session was terminated prior to documenting the system's vulnerable state, I simulated the pre-defense state manually by adjusting system settings to represent the same condition.

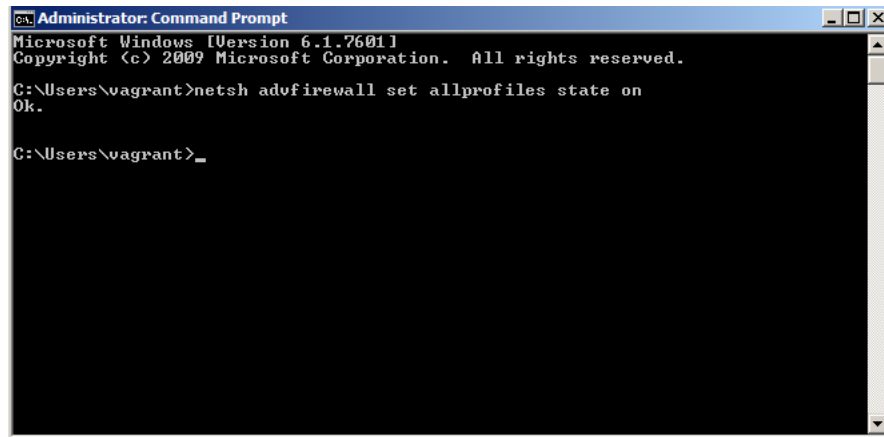
- Disabled firewall, enabled SMBv1, lowered password policy settings temporarily
- Screenshots:



3.2 Remediation Actions

- Deleted any unnecessary user accounts:
- net user backdoor /delete
- Deleted suspicious scheduled tasks:
- schtasks /query /fo LIST /v
- schtasks /delete /tn "TaskName"

- Re-enabled Windows Firewall: also, we can see after enabling the firewall Nmap couldn't scan the port 445 (SMB) and it shows that the port is filtered and the eavesdropper couldn't see the port status which would protect from the attack.



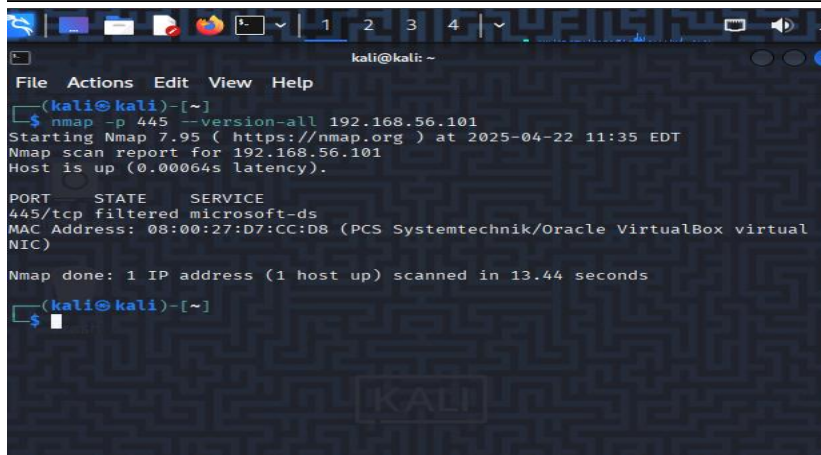
```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\vagrant>netsh advfirewall set allprofiles state on
Ok.

C:\Users\vagrant>_

```



```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -p 445 --version-all 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-22 11:35 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00064s latency).

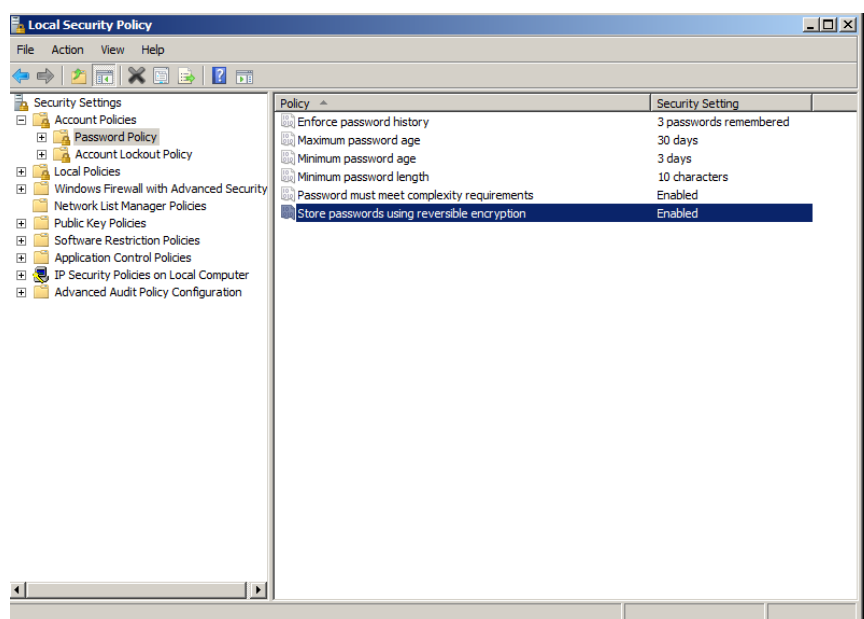
PORT      STATE SERVICE
445/tcp    filtered microsoft-ds
MAC Address: 08:00:27:D7:CC:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

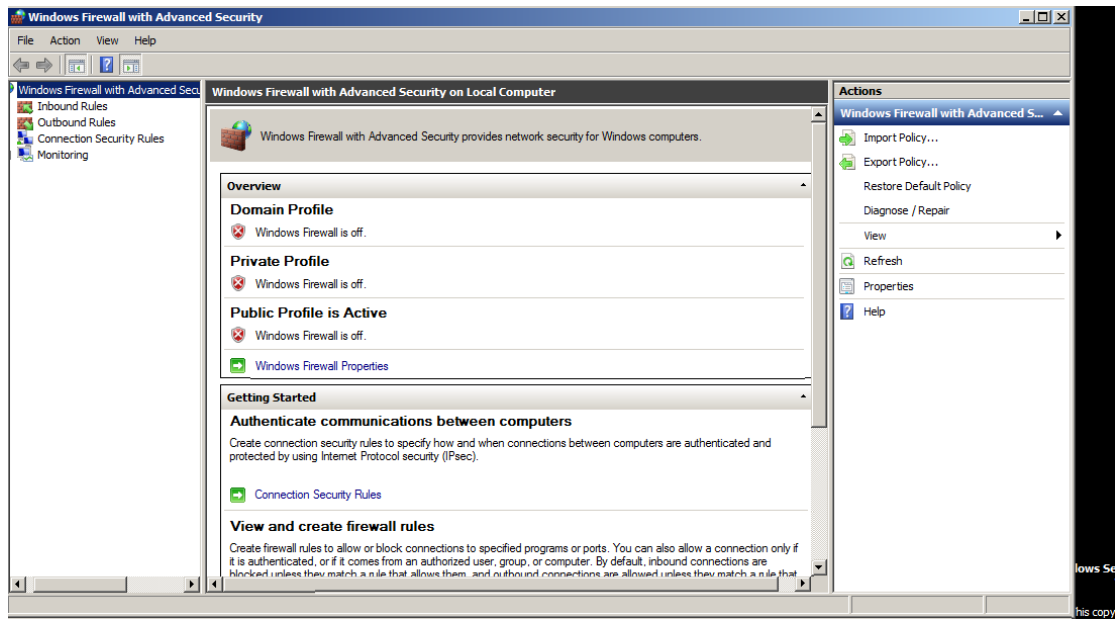
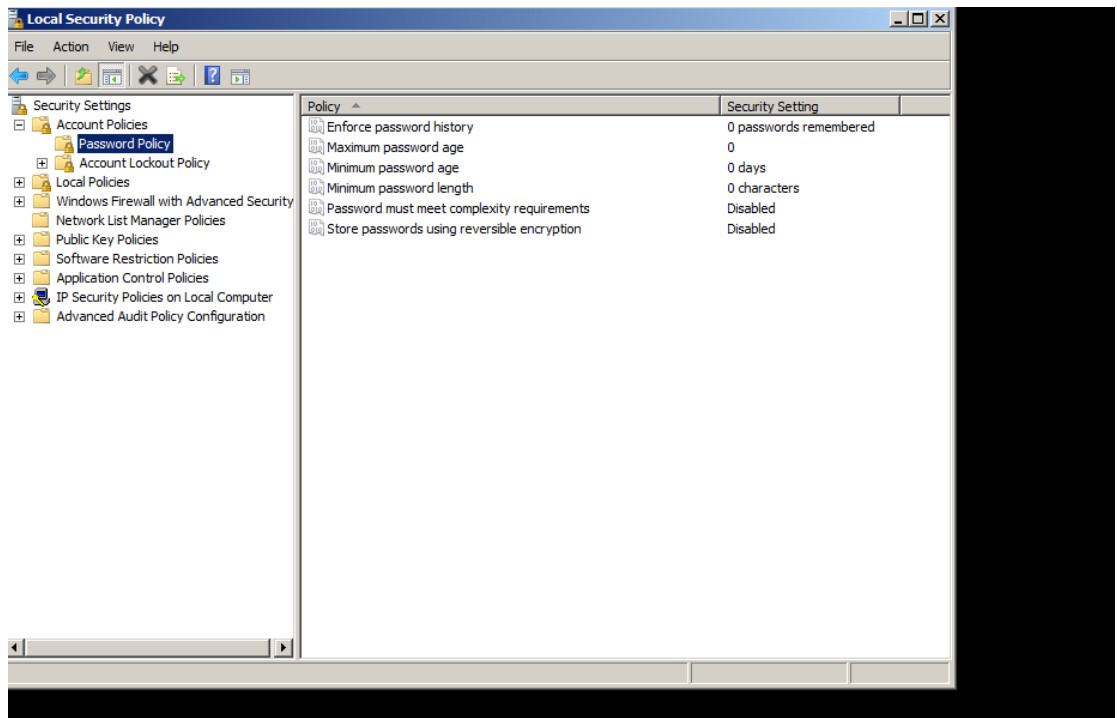
Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds

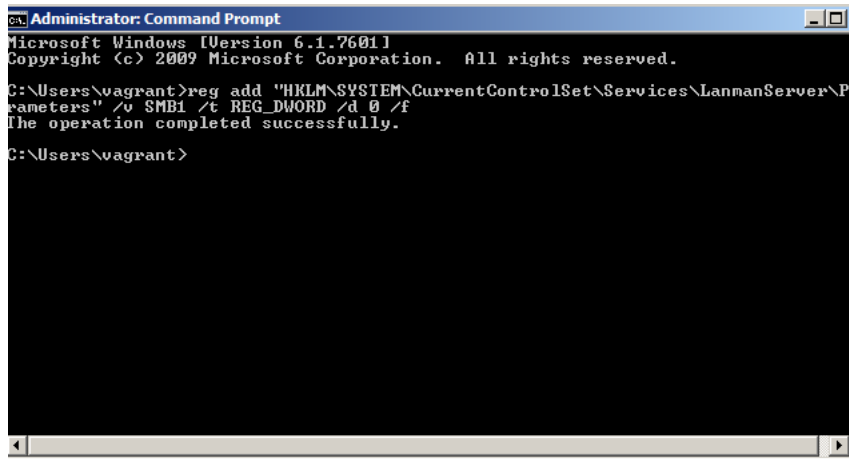
(kali@kali)-[~]
$

```

Enforced strong password policy







```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\vagrant>reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v SMB1 /t REG_DWORD /d 0 /f
The operation completed successfully.

C:\Users\vagrant>
```

Final Notes

- All logs, screenshots, code files, and Splunk artifacts have been stored in the GitHub repository under appropriate phase folders.
- I simulated some steps responsibly in line with the learning objectives of this project.
- All required documentation and visuals are complete except for Kali log collection.
- Simulated the pre-defense state since the original attack session was terminated
- Used netstat and task manager to verify open connections and backdoors
- Removed suspicious user accounts and scheduled tasks
- Re-enabled Windows Firewall and configured to block unused ports
- Enforced password complexity through Local Security Policy
- Disabled SMBv1 to prevent exploitation through EternalBlue
- Captured all defense actions in screenshots before and after