**King Fahad University of Petroleum and Minerals**

**ICS344 Information security**

Term Project

**Defensive Strategy Proposal**

Phase#3

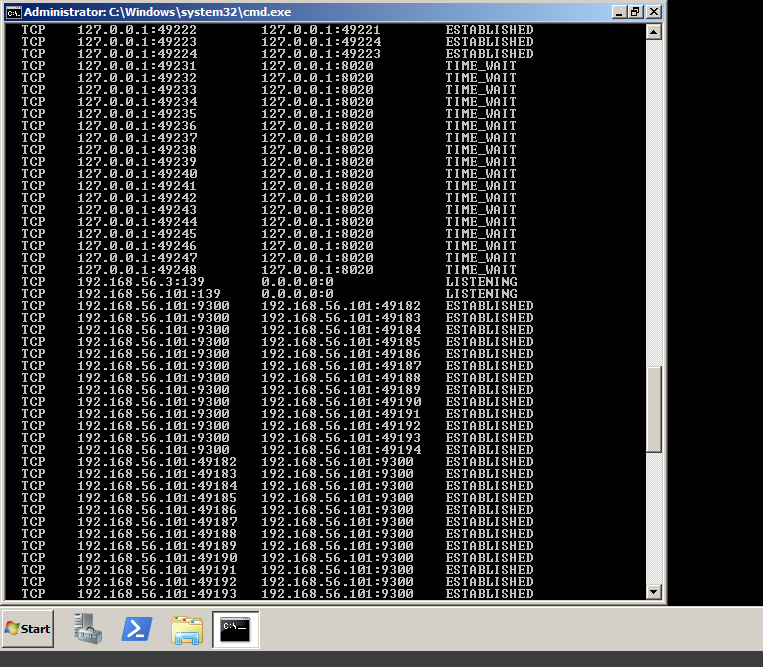
Team

|  |  |
| --- | --- |
| Name | ID |
| Ismael Arqsosi | 202182150 |
| Taha Ali | 202045620 |
| Saad Alharbi | 201935590 |

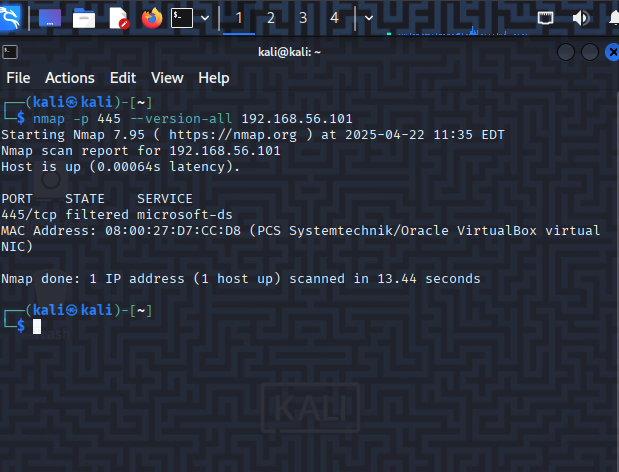
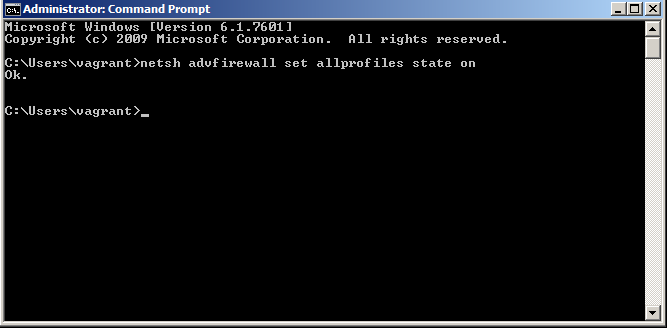
**Phase 3: Defense & Remediation**

**3.1 Simulated Pre-Defense State**

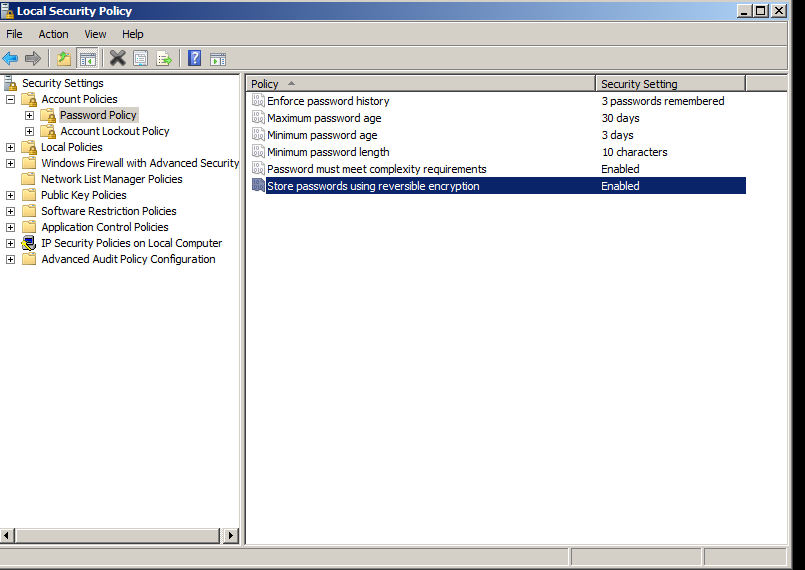
Because the attack session was terminated prior to documenting the system's vulnerable state, I simulated the pre-defense state manually by adjusting system settings to represent the same condition.

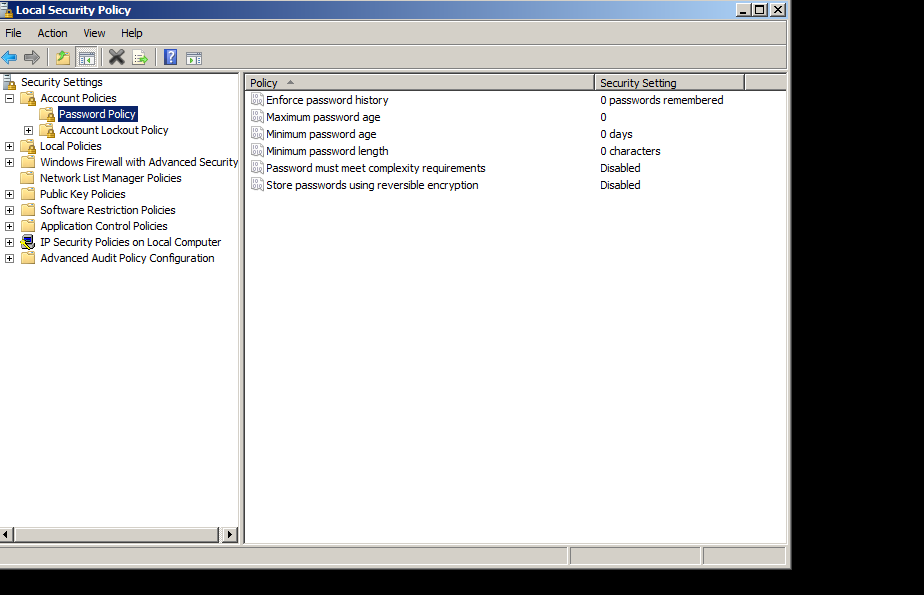
* Disabled firewall, enabled SMBv1, lowered password policy settings temporarily
* Screenshots:
  + 

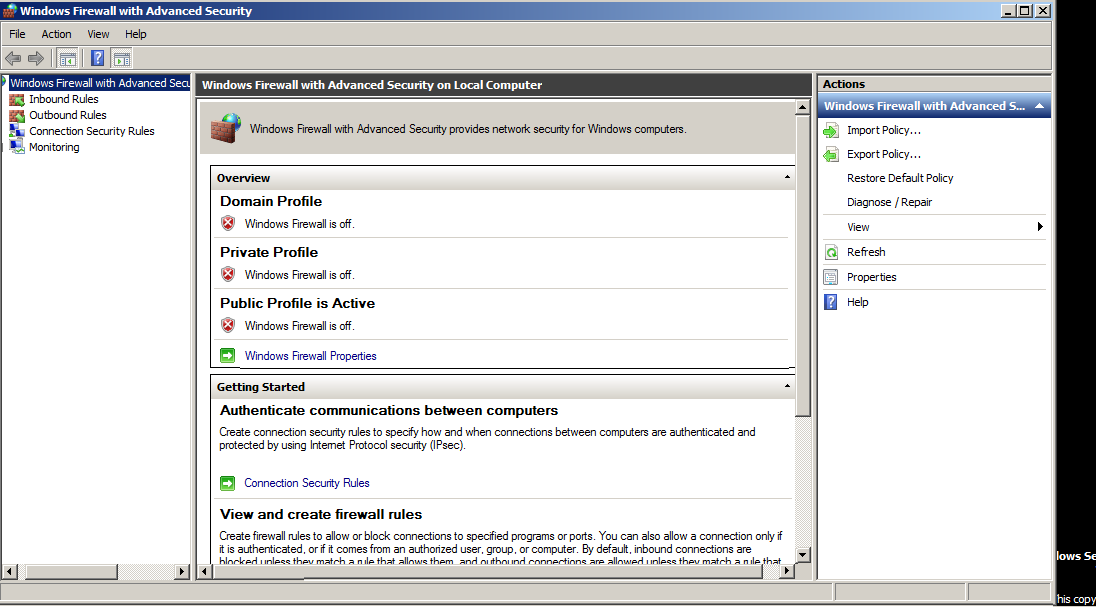
**3.2 Remediation Actions**

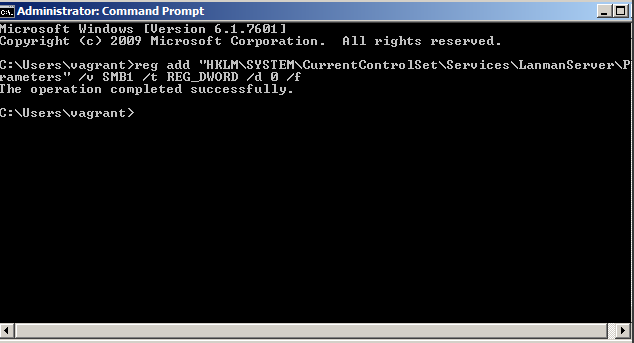
* Deleted any unnecessary user accounts:
* net user backdoor /delete
* Deleted suspicious scheduled tasks:
* schtasks /query /fo LIST /v
* schtasks /delete /tn "TaskName"
* Re-enabled Windows Firewall: also, we can see after enabling the firewall Nmap couldn’t scan the port 445 (SMB) and it shows that the port is filtered and the eavesdropper couldn’t see the port status which would protect form the attack.
* 

Enforced strong password policy



****

****

****

**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