Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

Title : Detection and Prevention

Lab : 9

Chapter : 19 (Protecting your network)

Exercise 19. 01 :

Step 1 :

Malware	Definition
Virus	It is programmed software with intention of causing damage and deleting the files in the system
Worm	It is a malicious program that replicates into lot like worms and attacks the storage server of the system
Logic Bomb	Its like a bomb when certain conditions are met, it gets executed and affects the user.
Trojan Horse	It seems to be legitimate code or software but has malicious nature in it and enters once users clicks on it.
Rootkit	It has collection of malicious tools and allows unauthorized access to computer system.
Ransomware	It is malware that affects the availability, affects system and encrypts the whole data. Ransom must be provided for the key

Step 2 :

Social Engineering attacks tries to lure the user or creates a legitimate content and add backdoor behind it to fool the user and makes trap to attract the victim, and launches it malicious nature once it gets activated. There are lot of social engineering methods and techniques are there like Backdoors, Keylogging etc.

Step 3 :
Phishing : It is kind of attack that make fool of host and tricks them to give the credentials as it showcases it coming from original source. It is much broader term.

Spear phishing : It is a more refined and targeted way of phishing and is well crafted for a specific person or organization with a purpose.

Whaling : It explains itself in its term, targeting high value people like ceo, chairman or other political people with malicious thought and activity. It may be active or passive.

Step 4 :
Scenario : What if the question asked is “What is your name” and it received as “what is your account name”, it is not the original message and not its intention either. How come this message is modified like this. Somebody must changed something in between and it should be modified, it is called as man in the middle, attacker captures the packet and modifies if it is not encrypted and send the packet to the receiver with little latency. But is seems like normal behavior in both end.

Step 5 :
DOS : Denial of service is attack on availability and it uses single computer and targets a server or website to flood the request or interruption to make it inaccessible.

DDOS : Whereas Distributed Denial of Service is using of botnets and other servers to flood request from different parts of the world, which is hard to detect and mitigate it, and makes it more challenging, also DDOS attack highly disrupts the infrastucture of the company associated with it.

Step 6 :
Open ports : If important ports are closed and not secured properly, it may be the entry point.

Improper or unencrypted data : Not using encryption for sending and receiving the data. Also we should use updated cipher and methodology.

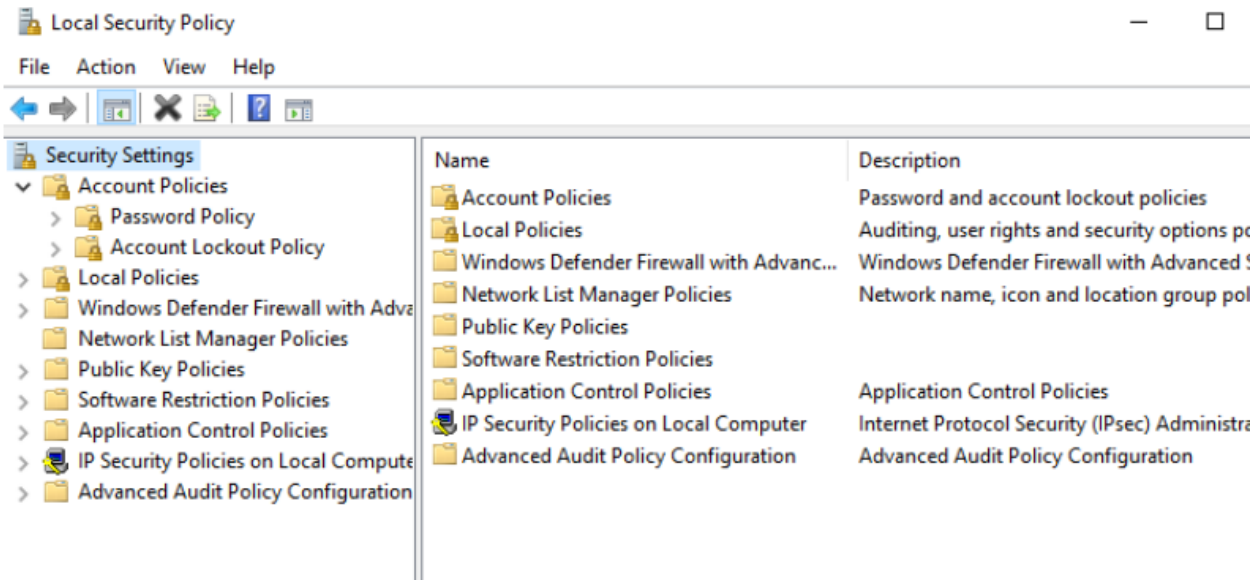
Insider Threats : It is very harmful and regulation of access control and making sure of properly handling the insiders are very important.

Rogue Access points : Access points which are not properly maintained and not secured well are vulnerable.

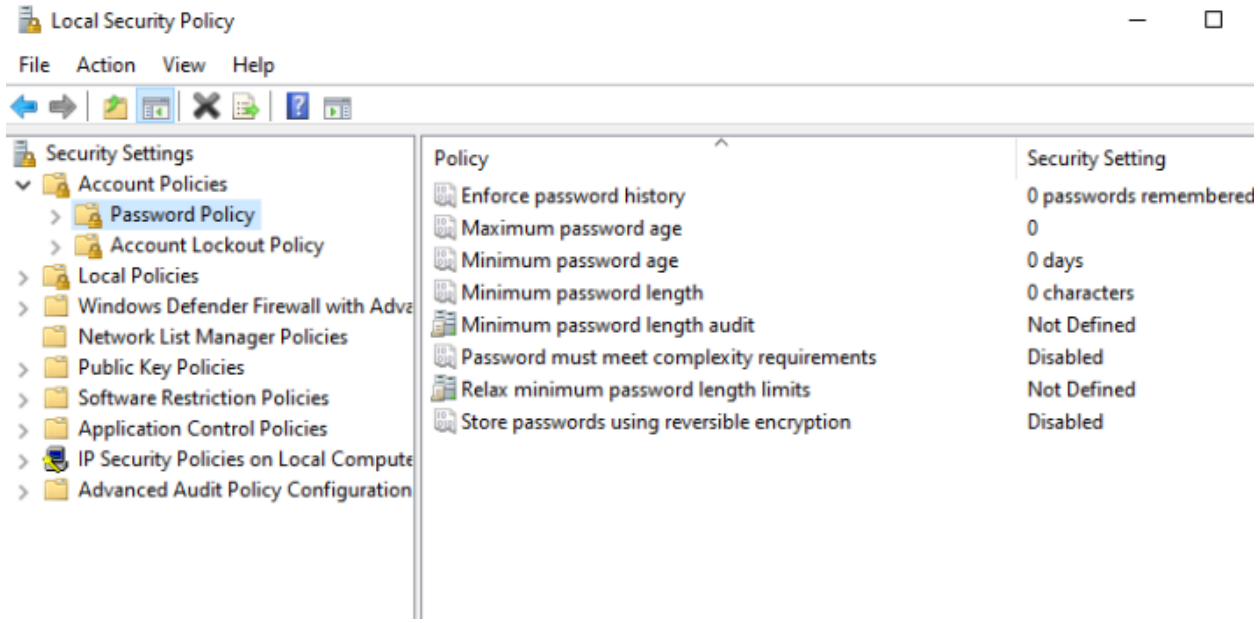
Step 7 :
I never faced any, but my friend got scammed through social engineering, where he got webpage looks same like facebook and asked to update the credentials, as to maintain the account and he trapped into it, finally his account was completely hacked and made him to delete the account. And lot of scams occur around people through social engineering which is hard to detect.

Step 8 :
I think the human error, which will be always present and we can't determine it, because based on our convenience we may do some mistake and let our access point or passwords weak. So this is the main weakest link I think.

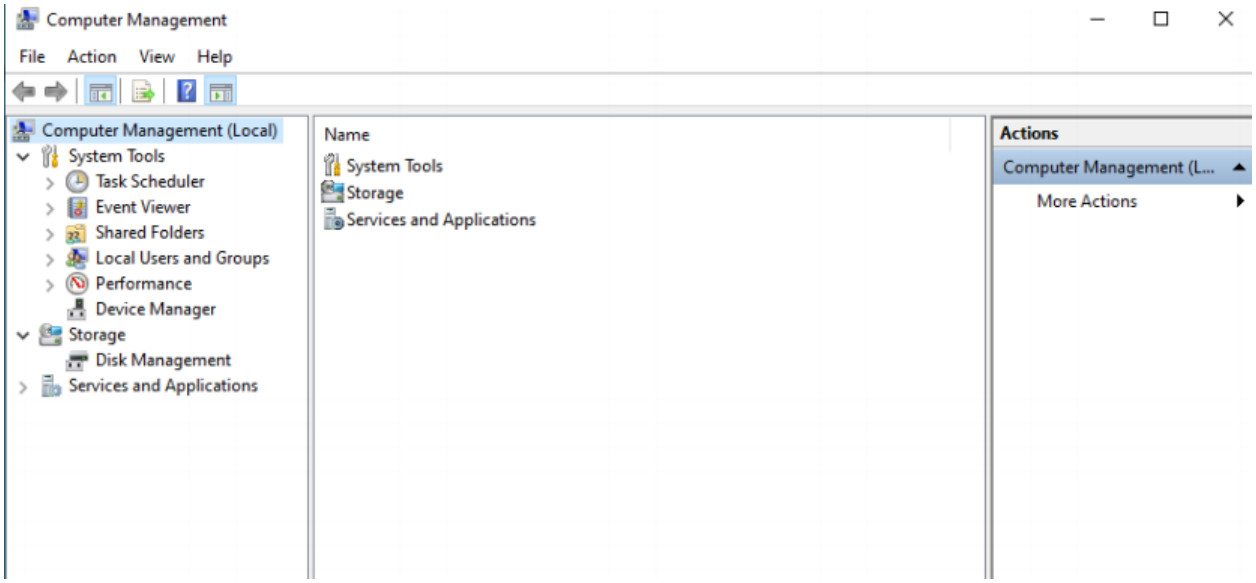
Exercise 19. 02
Step 1 :



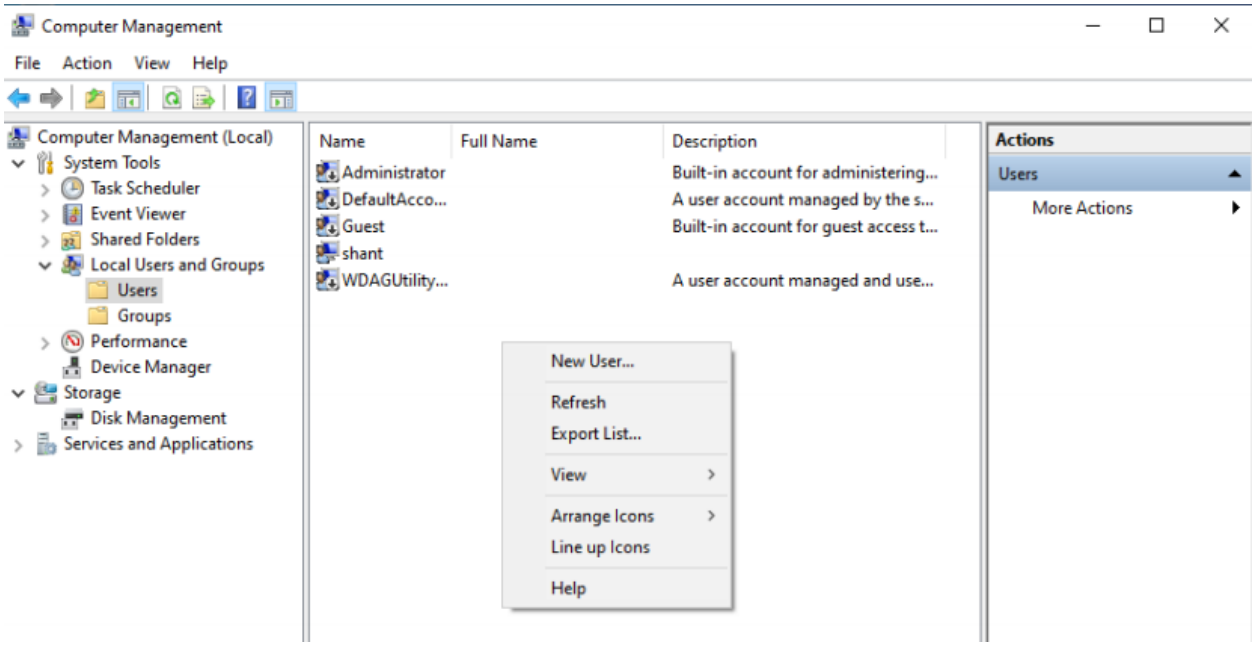
Step 2 :

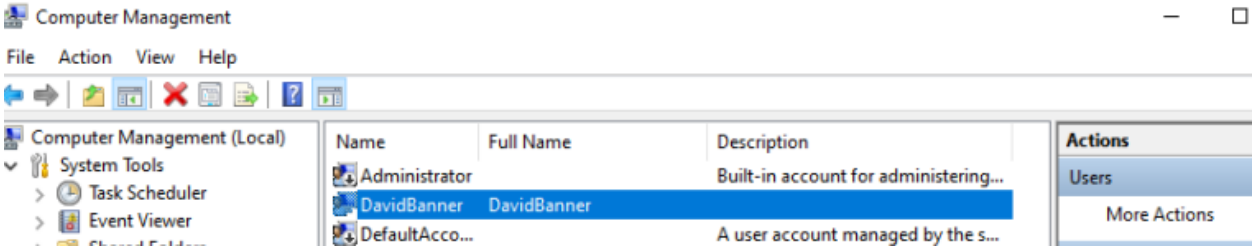

Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
0
Minimum password age
0 days
Minimum password length
0 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Disabled
Relax minimum password length limits
Not Defined
Store passwords using reversible encryption
Disabled

Step 3 :

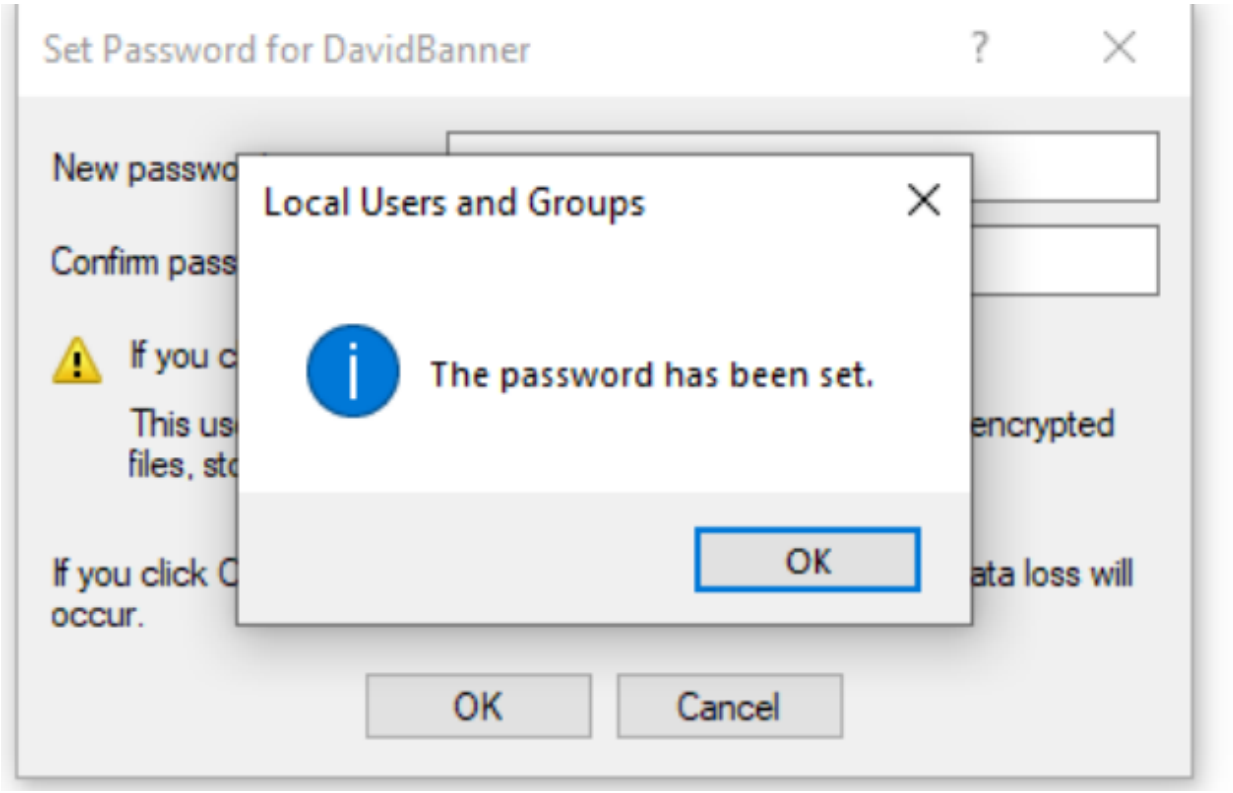

Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
System Tools
Storage
Services and Applications
Actions
Computer Management (L...
More Actions

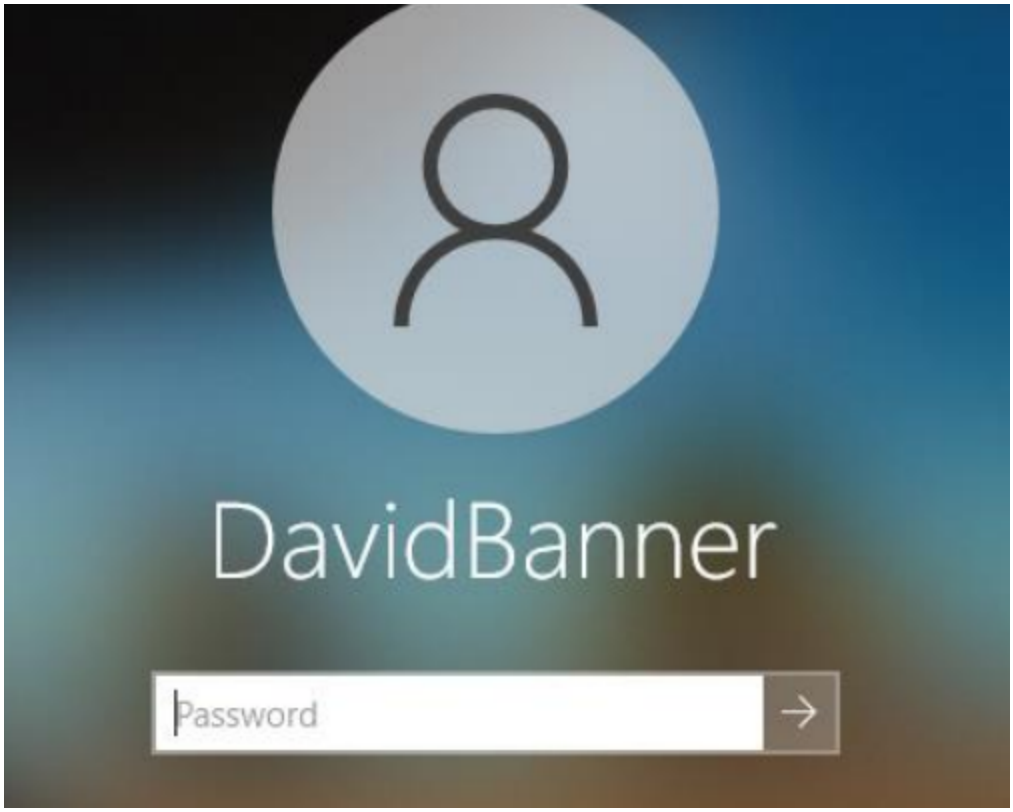
:


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
DefaultAcco...
A user account managed by the s...
Guest
Built-in account for guest access t...
shant
WDAGUtility...
A user account managed and use...
New User...
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help
Actions
Users
More Actions

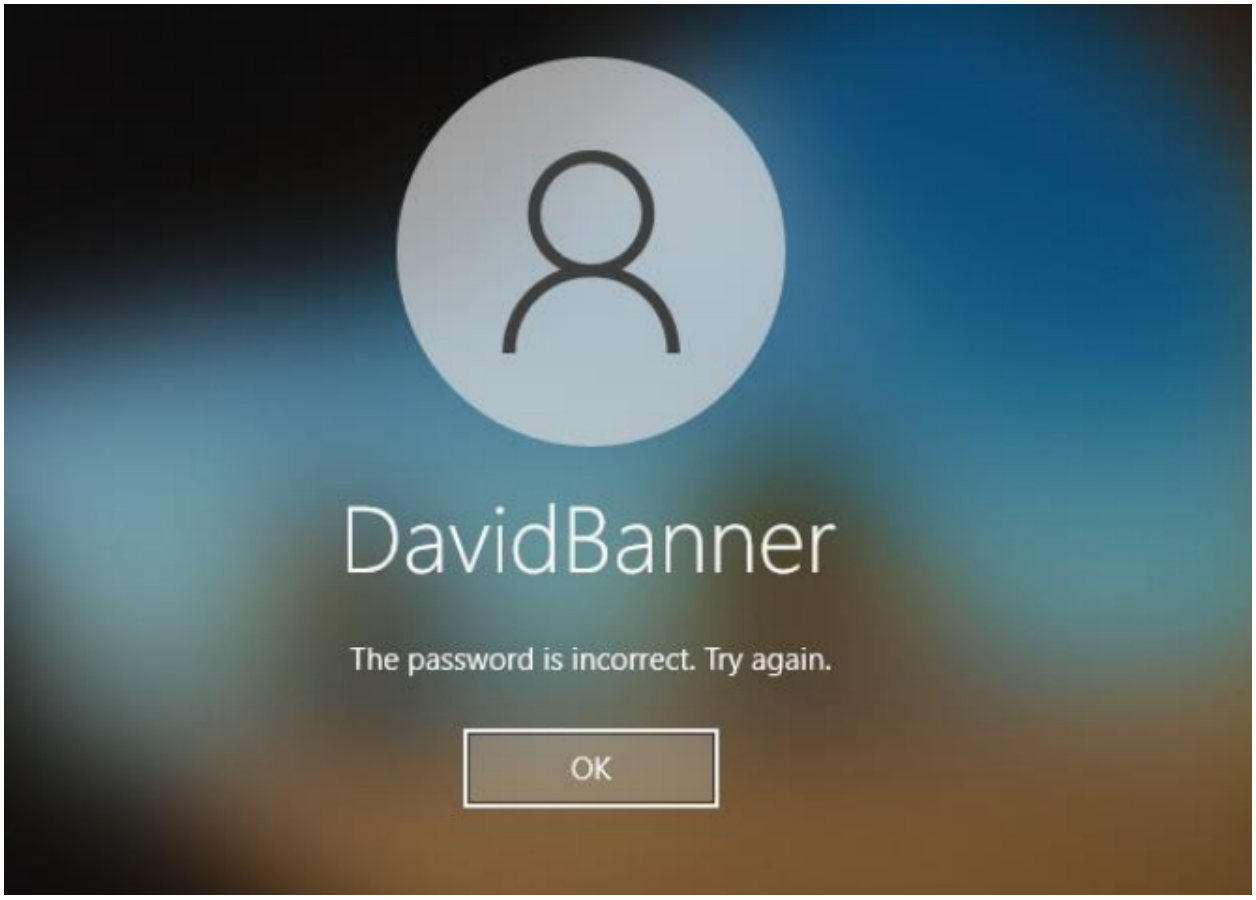

Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Name
Full Name
Description
Administrator
Built-in account for administering...
DavidBanner
DavidBanner
DefaultAcco...
A user account managed by the s...
Actions
Users
More Actions

Step 4 :
Password has been set for david banner :




DavidBanner
Password

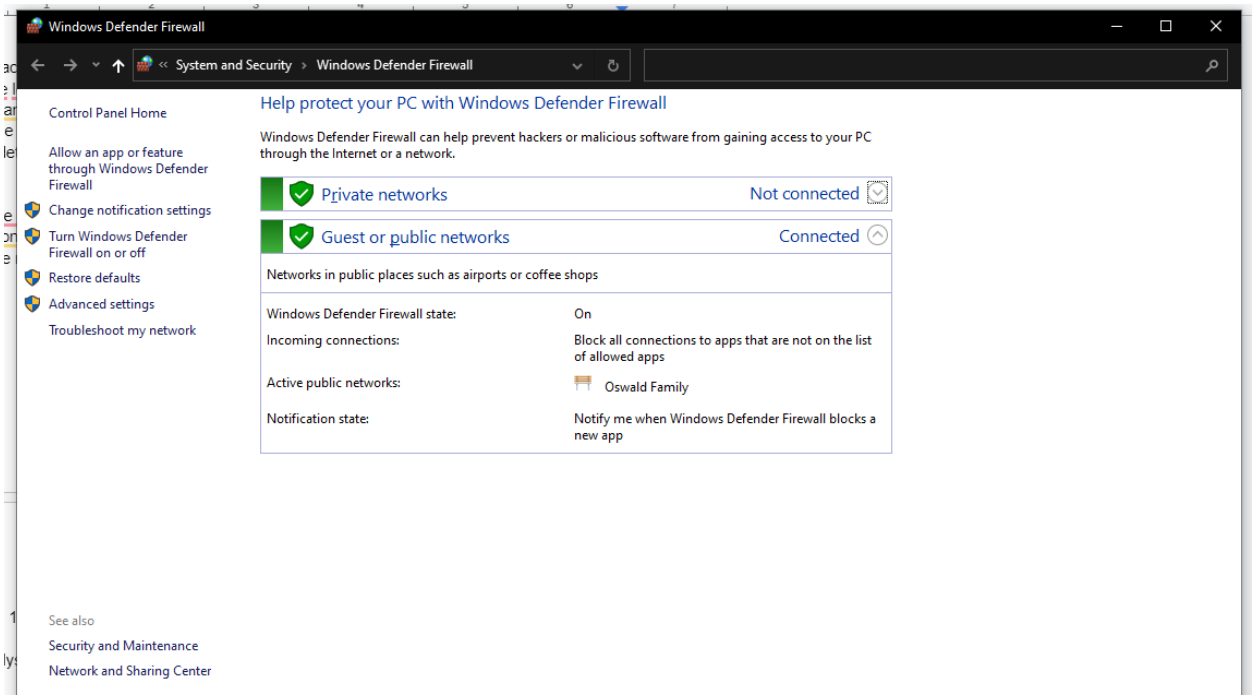
Step 5 :



While changing the password we have to opt for new password, old password can’t be reused, that why it failed the password.

Step 6 :
The new password must have the length minimum of 10 characters with the mixture of alphabets, symbols, and other characters to ensure the strength and reliability of the password.

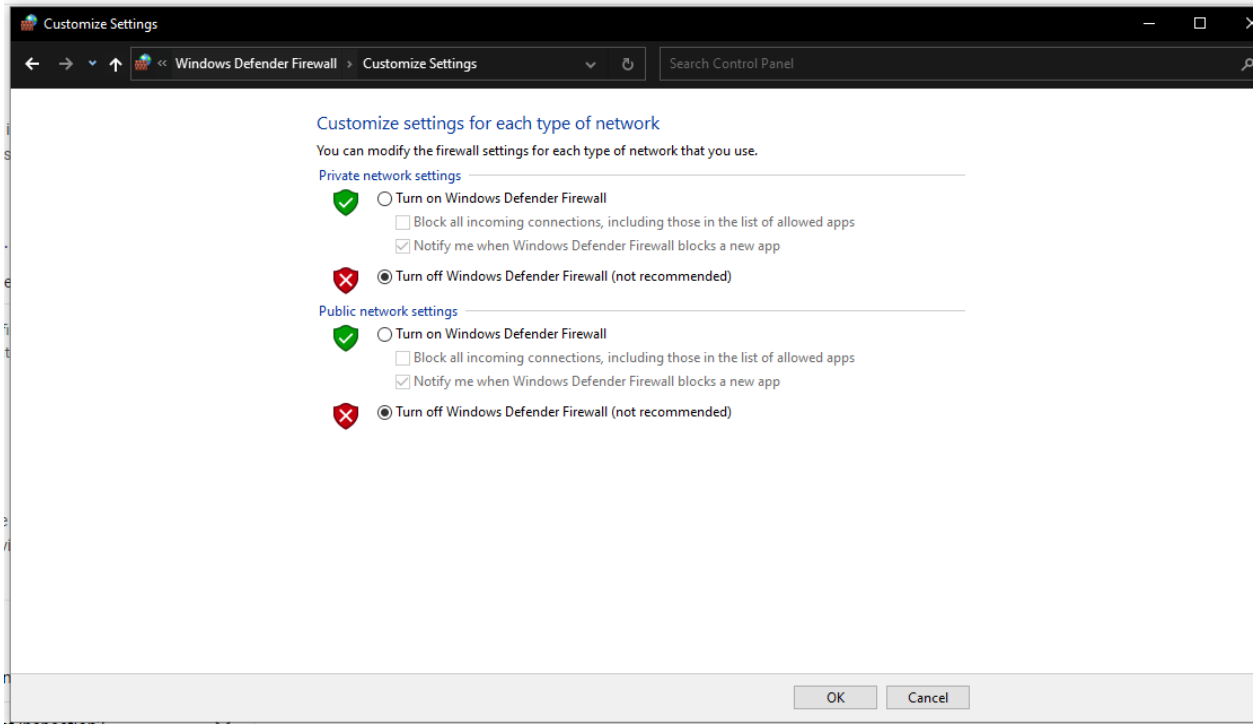
Exercise 19. 03 :
Step 1 :



Step 2 :
From the web, I found Windows Firewall indeed uses some features of SPI.

Stateful packet inspection maintains the network security of the system by maintaining the state tables and analyzing packets based on those predetermined rules and data.

Step 3 :



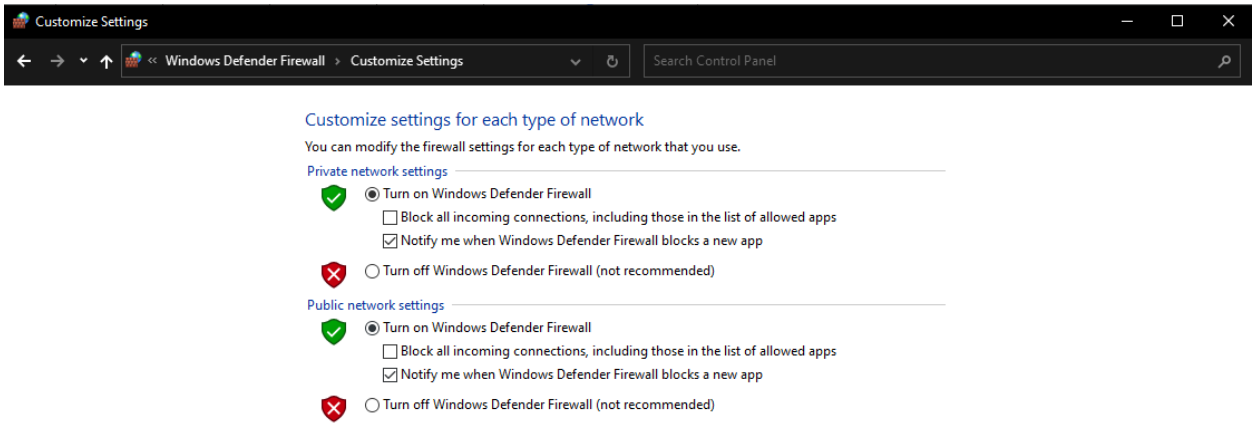
Step 4 :

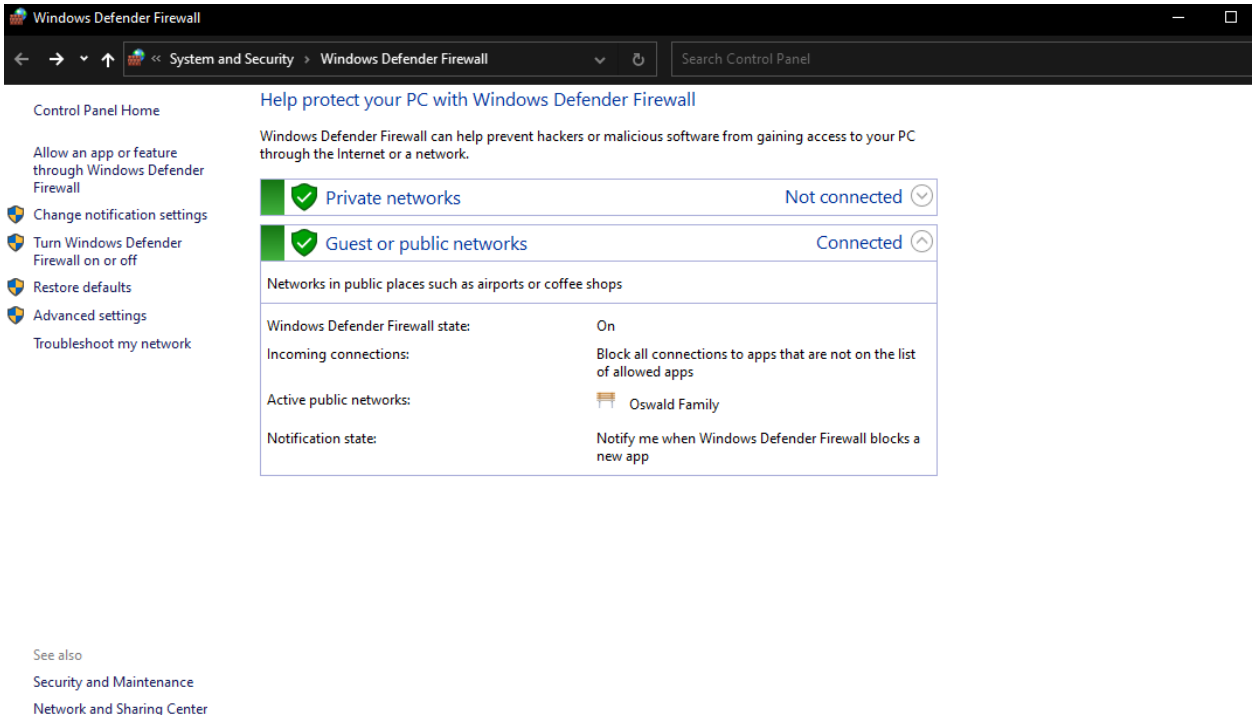
```
C:\Users\dinot>ping 192.168.173.1

Pinging 192.168.173.1 with 32 bytes of data:
Reply from 192.168.173.1: bytes=32 time<1ms TTL=128
Reply from 192.168.173.1: bytes=32 time<1ms TTL=128
Reply from 192.168.173.1: bytes=32 time<1ms TTL=128
Reply from 192.168.173.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.173.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

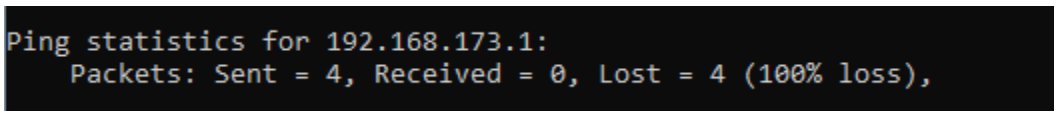
Step 5 :



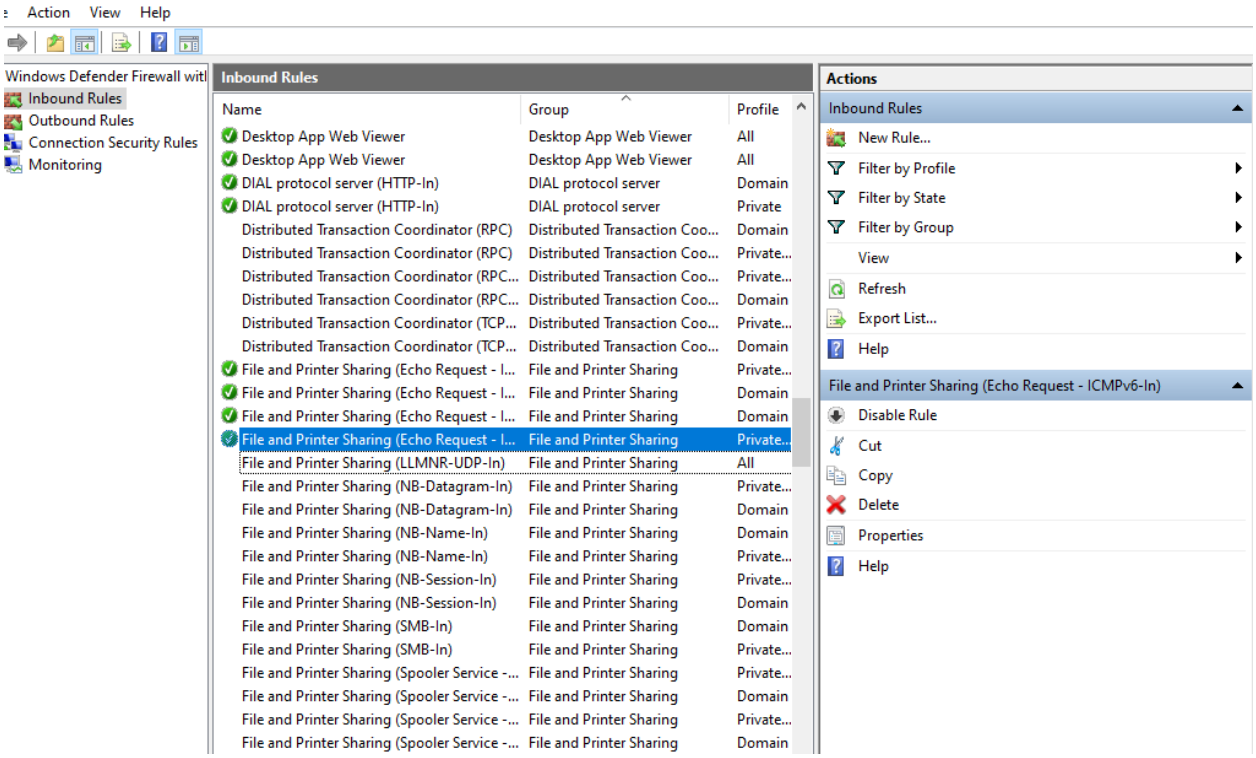


Step 6 :

After pinging with firewall on



Step 7 :



Step 8 :

```
C:\Users\dinot>ping 192.168.173.1

Pinging 192.168.173.1 with 32 bytes of data:
Reply from 192.168.173.1: bytes=32 time<1ms TTL=128
Reply from 192.168.173.1: bytes=32 time<1ms TTL=128
Reply from 192.168.173.1: bytes=32 time<1ms TTL=128
Reply from 192.168.173.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.173.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Lab Analysis :

1. For Step 4 we turn off the windows defender and this allows the other system to ping the computer which is not protected by the firewall. So that we can ping successfully on step 4. Whereas Step 6, we turn the firewall on again, then we try to ping, the firewall will not allow the ping to send and receive the packets, so it should fail. Finally for step 8 we configured and changed the In-rules of the firewall, so the ping should work again now. This is what happening in each steps.

2. Chany should only share her username and password after she verifies about the network administrator by asking for the employee ID and some company related security question, and let him know that she will mail the details through organizational mail rather than on the phone. These measures will safeguard her from spam attacks.

3. It seems like a logic bomb attack as the attack is established after 1 week he resigned and only he can detonate it, as he only knows about the trigger. These are hard to detect in advance, as they only established when the conditions met and got triggered.

4. Because it makes user to reuse the part of the old password to remember it, makes it vulnerable, also sometimes using of complex letters make users to forget the password too. They should focus on the length of the password rather than the complexity of it and using added layer of security enhances the protection.

5. A stateful firewall is a type of network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Stateful firewalls are effective in providing an added layer of security as they can analyze the context of network traffic, making them more adept at identifying and blocking suspicious or unauthorized activity.

Quiz :

1. Ransomware
2. Social Engineering
3. Longer
4. Firewall
5. Humans