Network Security Activities

Network Threats and Vulnerabilities D/618/5218 **AC 3.2:** Plan procedures to secure a network in line with organisational requirements. **AC 4.1:** Configure a device or software to improve network security.			
Learner Name	O. Folarin	**Tutor Name**	Shamim Khan

Scenario

"Pentest Ground" *are a security services company based in New York and have employed you as their Network Administrator. You have recently undertaken some network management activities for them, and now they ask you to undertake some network security activities on the same network. Prior to commencing with these activities, you must create a list of procedures to plan how Pentest Ground can secure their network in line with their organisational requirements (3.2).*

Organisational Requirements

- *Secure the server by applying a firewall and only allow access by trusted networked devices (4.1).*
- *Apply UAC on the server (802.1x) (4.1).*
- *Ensure passwords on the email server account that meet policy standards (4.1).*
- *Test the servers for functionality and performance to ensure security measures do not slow down system functions (4.1).*

Task 1: Create a list of procedures to plan how Pentest Ground can secure their network in line with their organisational requirements (3.2).

This could include…

- **Planned procedures to configure a firewall, define trusted devices, implement network segmentation.**
- **Planned procedures to apply UAC on the server, enable 802.1x network access control, enforce role-based access control, regularly review and update user access.**
- **Planned procedures to implement strong password policies, enable MFA, monitor and log email server access.**
- **Planned procedures to test server functionality and performance to maintain security – this could include conducting performance and security testing, monitoring system performance, backup and disaster plan, regular updates to software.**

The following procedures are to be executed as instructed.

Check that all PCs are configured properly.

Allow access to authorised devices on the server.

Deny access to unauthorised devices on the server.

Set up a security layer on the server by applying ''802.1X Security''.

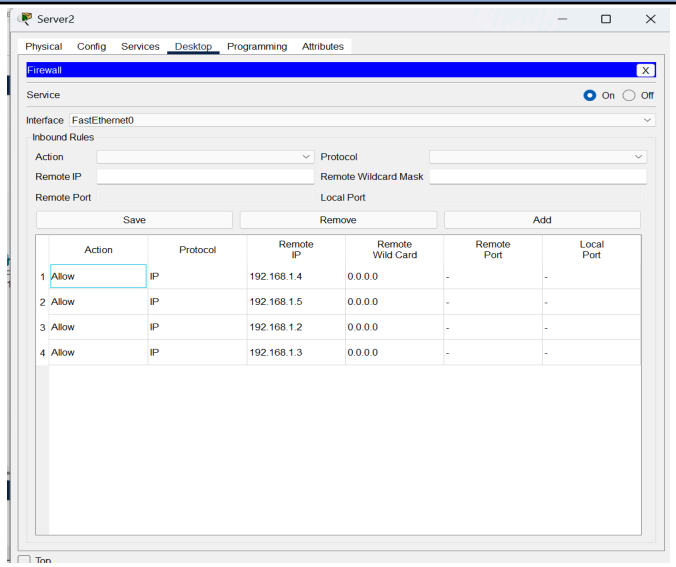
Change password for user1 to meet company's security policy standards.

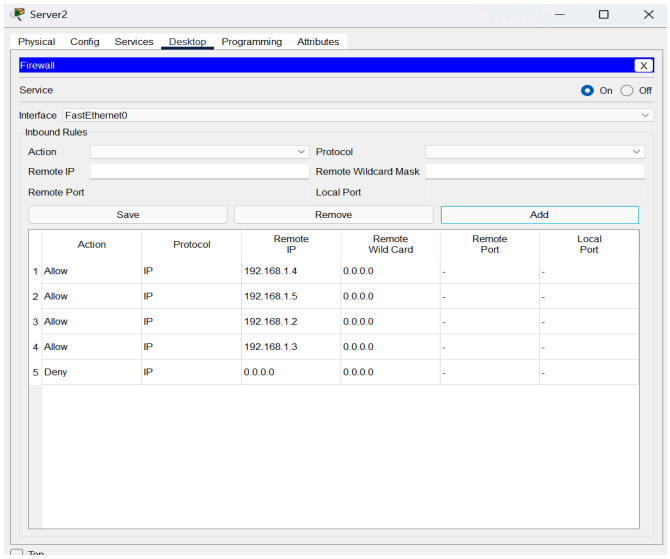
Change password for user2 to meet company's security policy standards.

Ping the server from all connected devices for functionality and performance to ensure security measures do not slow down system functions.

Network Security Activities

Task 2: Secure the server by applying a firewall and only allow access by trusted networked devices (4.1).





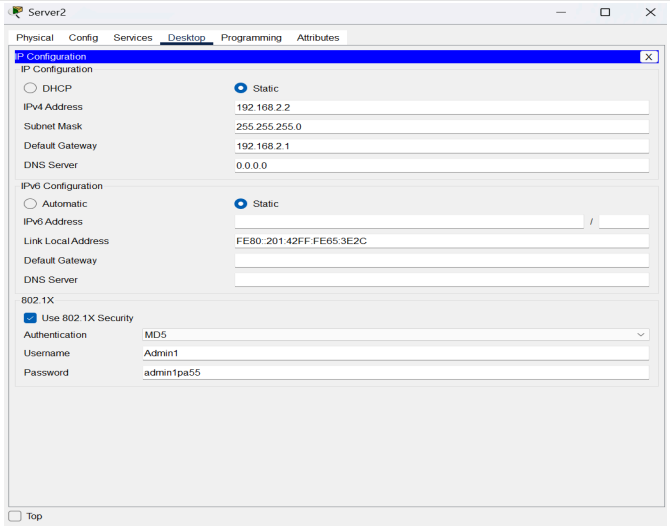
Annotation:

I clicked on Server2, selected Desktop followed by IPv4. PC-1 and PC-2 were already allowed access from my previous network project so I went on to allow PC-3 and PC-4 access on the server and deny access to any other IP.

As shown in the screenshot, all PCs have been allowed access to the server.

As shown in the screenshot, access to any other IP on the server has been denied. This can be seen as a security layer knowing for sure that the server will reject any access to any other devices apart from the 4 PCs that are allowed access.

Task 3: Apply UAC on the server (802.1x) (4.1).

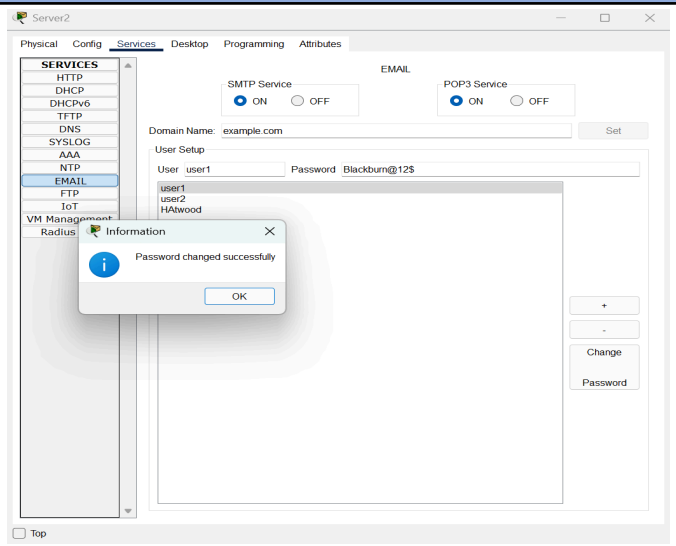


To apple UAC (802.1X), I clicked on Server2, on the Desktop, I clicked IP Configuration, I went down the IP Config page, checked "Use 802.1X Security", then input username: Admin1 and password: admin1pa55 for authentication as shown in this screenshot.

802.1X adds an extra layer of security to the network. It does not allow any device to enter the main network unless the device has passed authentication properly. I set up 802.1X authentication using RADIUS server that verifies device identity. I used MD5 for the credential authentication part to make sure only authorized devices can connect.

Network Security Activities

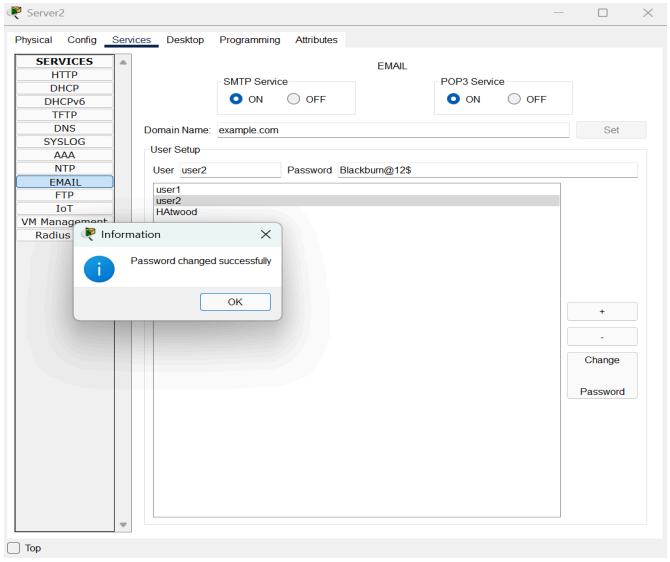
Task 4: Ensure passwords on the email server account meet policy standards (4.1).



Annotation:

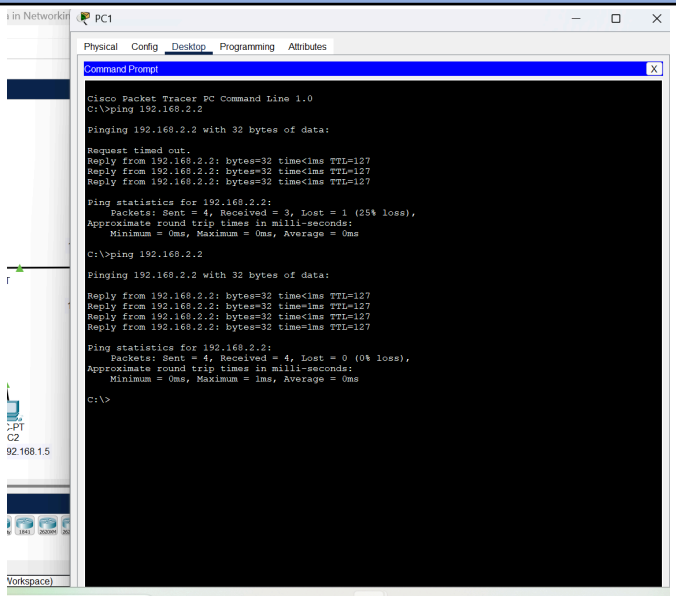
To ensure passwords on the email server account meet policy standards;

I clicked on Server2, on the Desktop page, I selected Services followed by Email. Then I clicked on user1, selected ''Change Password'' typed in my new password which meets the policy standard ''Blackburn@12$''. As shown in the screenshot, password for user1 was changed successfully.



I repeated the same steps for user2. Updated the password to ''Blackburn@12$''. As shown in the screenshot, password for user2 was changed successfully.

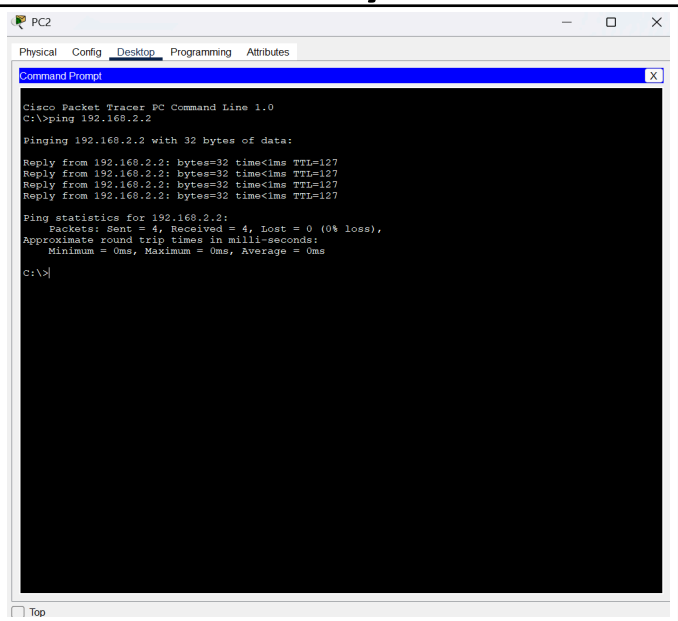
Task 5: Test the servers for functionality and performance to ensure security measures do not slow down system functions (4.1).



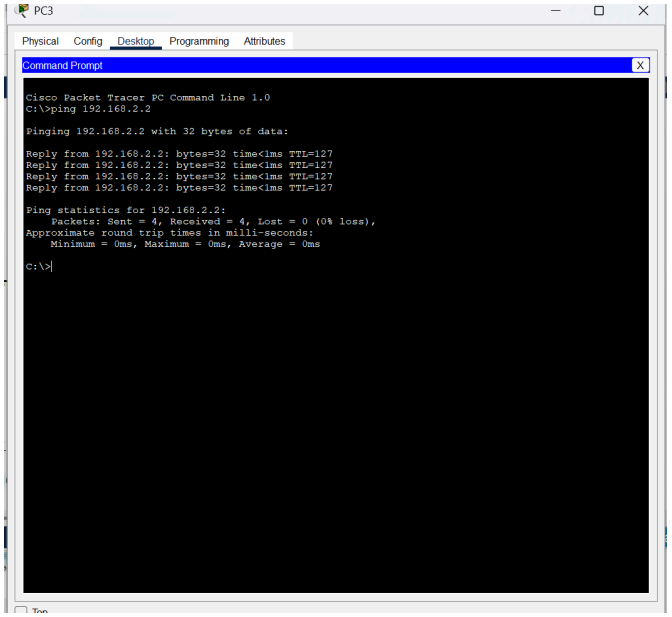
Annotation:

I clicked on PC-1, selected Desktop followed by Command Prompt then input ''ping 192.168.2.2'' to ping the server from PC-1. At first attempt, out of 4 packets sent, 1 was lost and 3 was received by the server. I pinged again and this time all 4 packets were successfully delivered and received with no delay or time out.

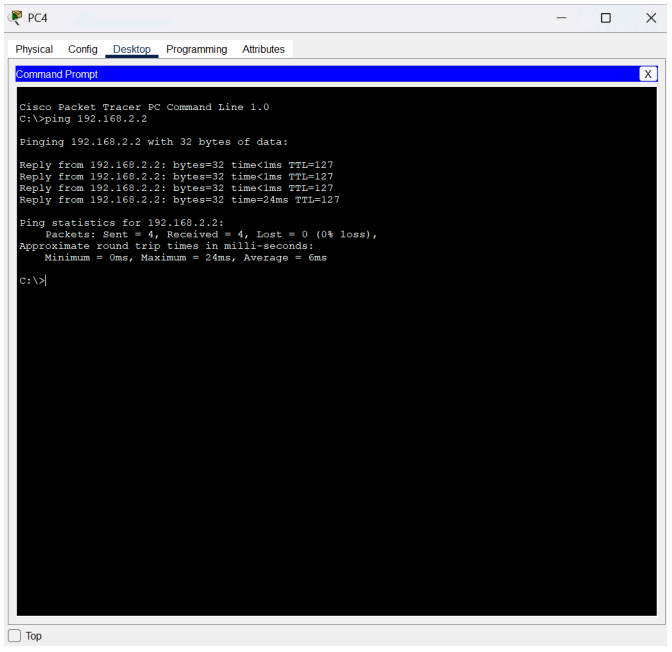
Network Security Activities



I clicked on PC-2, selected Desktop followed by Command Prompt then input "ping 192.168.2.2" to ping the server from PC-2. Network connection works fine. All 4 packets were successfully delivered and received with no delay or time out.



I clicked on PC-3, selected Desktop followed by Command Prompt then input "ping 192.168.2.2" to ping the server from PC-3. Network connection works fine. All 4 packets were successfully delivered and received with no delay or time out.



I clicked on PC-4, selected Desktop followed by Command Prompt then input "ping 192.168.2.2" to ping the server from PC-4. Network connection works fine. All 4 packets were successfully delivered and received with no delay or time out.

Network Security Activities