Task 1 : Measures to Protect from Cyber Crimes:

Use of Strong, Unique Passwords: I use complex passwords for different accounts and regularly update them. I avoid reusing the same password across multiple services.

Two-Factor Authentication (2FA): I have enabled 2FA on all major accounts to add an extra layer of security.

Regular Software Updates: I ensure that my devices, operating systems, and software are updated to patch any vulnerabilities.

Antivirus & Anti-Malware Protection: I use reputable antivirus software to scan for potential threats and malware. In my case it is

Email Vigilance: I avoid clicking on suspicious links or opening attachments in unsolicited emails, and I verify email senders.

Secure Wi-Fi Usage: I use a VPN when accessing public Wi-Fi and ensure my home network has strong encryption.

Experience with Cyber Crimes:

I have not been a victim of any major cybercrimes, but I have received phishing emails. I can adapt the habit of continuously staying informed about the latest cyber threats and reviewing account activities regularly.

Task 2 : Company Security Policy

- **Password Policy**

Purpose:

To ensure that strong passwords are used to safeguard access to the company's digital resources and sensitive information.

Scope:

This policy applies to all employees, contractors, and third-party users who have access to company systems.

Guidelines:

Password Length and Complexity:

Passwords must be at least 12 characters long and include a mix of uppercase letters, lowercase letters, numbers, and special characters.

Password Expiration:

Passwords should be changed every 90 days, and users will be notified before expiration.

Prohibited Practices:

Do not share passwords with anyone.

Avoid writing passwords down or storing them in unsecured places.

Reusing passwords across multiple platforms is prohibited.

Password Storage:

Passwords must be stored using encryption in approved password management systems only.

Failed Login Attempts:

After 5 unsuccessful login attempts, the account will be locked for 15 minutes to prevent unauthorized access.

Enforcement:

Violations of this policy may result in disciplinary actions, including warning of access.

- **Cloud Usage/Security Policy**

Purpose:

To provide guidelines for secure cloud usage to protect sensitive company data and prevent unauthorized access.

Scope:

This policy applies to all employees, contractors, and third-party partners using cloud services to access, store, or process company data.

Guidelines:

Data Classification:

Employees must categorize data based on sensitivity (public, internal, confidential, restricted) and apply appropriate security measures when storing data on cloud platforms.

Authentication and Access Control:

Strong authentication mechanisms, such as multi-factor authentication (MFA), must be used for accessing cloud services.

Encryption:

All sensitive data must be encrypted both in transit and at rest when stored in the cloud.

Third-Party Cloud Providers:

Cloud providers must comply with industry standards and regulatory requirements, and contracts should outline security measures to be followed.

Monitoring and Logging:

Continuous monitoring of cloud services should be in place to detect suspicious activity. All access logs should be reviewed regularly.

Data Backup:

Critical data stored in the cloud should be backed up periodically in secure offsite locations.

Task 4

Did you find any devices you did not know were in your network?

Based on the scan results, the following devices were detected:

IP 10.0.2.2 and 10.0.2.3 with multiple open ports such as msrpc, iss-realsecure, apex-mesh, webpush, and EtherNetIP-1.

IP 10.0.2.15 only has SSH (port 22) open.

I am unfamiliar with devices hosting services like apex-mesh or iss-realsecure, these may be the devices I didn't expect to see on my network.

Were there any open ports that should have been closed?

The scan results show multiple open ports that are typically used for specific services:

135/tcp (msrpc) and 445/tcp (microsoft-ds) are often targeted by malware or hackers, so these should ideally be closed unless specifically required.

Ports like 2222/tcp (EtherNetIP-1) and 27000/tcp (flexlm0) may also need review based on my specific network configuration and security needs.

It is recommended to close these ports for security reasons.

Did nmap find any vulnerabilities?

Nmap didn't flag any explicit vulnerabilities in the output, but open ports such as SSH (22), MSRPC, and others could expose potential entry points if not properly secured. I should ensure services running on these ports are updated and properly configured to prevent unauthorized access.