1. **How to enable the password complexity requirement?**

* Minimum length (such as 8 characters): this helps ensure that passwords not too short and easily guessable.
* Complexity rules: Specify rules for password complexity, such as requiring a combination of uppercase and lowercase letters, numbers, and special characters.
* Avoid common password: Implement checks to prevent users from using commonly used password or passwords that are easily guessable
* Password expiry and history: Consider implementing password expiration policies; maintain a password history to prevent users from reusing their previous passwords.
* Password strength meter: include a password strength meter on registration or password change
* Educate users: provide guidance to users on creating strong password and the important of password security

1. **How to set the inbound and outbound rules in windows firewall?**
2. Press the Windows key, type “Windows Defender Firewall” and open the “Windows Defender Firewall” app
3. Click in “Advanced settings” on the left-hand side
4. In the “Window Defender Firewall with Advanced Security” window, choose either “Inbound Rules” or “Outbound Rules” in the left-hand pane
5. Right-click on the chosen rule types (inbound or outbound) and select “New Rule”
6. Select the rule type: program, port, predefined, or custom rules
7. Follow the wizard steps to provide necessary details like program path, port number, or criteria
8. Specify the action: allow or block the traffic that matches the rule
9. Name and describe the rule for identification purposes
10. Complete the wizard by reviewing the setting and click “Finish” to create the rule
11. **How to apply the IP security?**
12. Press the Windows key, type “Windows Defender Firewall” and open the “Windows Defender Firewall” app
13. Click in “Advanced settings” on the left-hand side
14. Select “IP Security Policies on Local Computer”
15. Right-click and choose “Create IP Security Policy”
16. Follow the IP Security Policy Wizard by providing a name, description, and activation option
17. Configure policy properties by editing rules, filter lists, filter actions, and authentication methods
18. Save the changes and close the “Windows Defender Firewall with Advanced Security” window
19. **How to apply the encryption?**

* Identify the data that needs to be encrypted
* Choose an appropriate encryption algorithm such as AES, RSA, or Blowfish
* Implement encryption in your code using encryption libraries or function specific to your programming language and platform
* Generate strong encryption keys using random number generators or cryptographic libraries
* Encrypt the data using the chosen encryption algorithm and generated encryption keys
* Store or transmit the encrypted data securely, employing secure storage methods or secure communication channels
* When accessing the encrypted data, decrypt it using the appropriate decryption algorithm and keys

1. **How to apply the security on the folder, full access for simple users?**
2. Right-click on the folder you want to secure and select “Properties”
3. Go to the “Security” tab
4. Click on “Edit” to modify the folder’s security settings
5. Click on “Add” to add the simple users you want to grant access to
6. Type the name of the user or click on “Advanced” to browse and select the users
7. Click “OK” to close the dialog box
8. Select the added users from the list
9. Check the box next to “Full Control” to grant full access
10. Click “Apply” and then “OK” to save the changes
11. **What is the use of netstat command as well as two switches?**

* The netstat command is a useful network utility that displays active network connections, listening ports, and network statistics on a system. It provides information about network connection, routing tables, and network interface statistic. The command is available in various operating systems, including Windows, Linux and MacOS
* Two commonly used switches with the “netstat”:
  + ‘-a’ or ‘--all’: this switch displays all active connections and listening ports. Including both TCP and UDP connections
  + ‘-n’ or ‘--numeric’: this switch displays IP addresses and port numbers in numeric form, rather than resolving them to hostnames and services names

1. **Hot to find out the information regarding domain name?**

* WHOIS Lookup: a protocol used to retrieve domain name registration information, including owner information, registration date, and more
* DNS Lookup: DNS (Domain Name System): using tools like ‘nslookup’ or ‘dig’ to gather IP address(es) associated with the domain and other DNS records like MX and TXT
* Website Analysis Tools: provide comprehensive information about a domain. There tools analyze various aspects of a website, including domain authority, hosting provider, IP address, SSL certificate details, website performance…
* Web Search Engines: you can search for the domain name in popular engines like Gooogle.

1. **What is the use of an advantage scanner?**

* Security Assessment: Identifies vulnerabilities and weaknesses in systems for improved security
* Risk Mitigation: Helps address vulnerabilities before they can be exploited by attackers
* Compliance: Assists in meeting regulatory and compliance requirements
* Continuous Monitoring: Offers ongoing vulnerability detection and protection
* Time and Cost Efficiency: Automates scanning, saving time and resources
* Reporting and Prioritization: Generates reports to prioritize and plan remediation efforts

1. **How to create the HTTPS website?**
2. Obtain and SSL/TS certificate form a trusted Certificate Authority (CA) or use free option like Let’s Encrypt
3. Install the certificate on your web server
4. Update your website’s URL to use HTTPS instead of HTTP
5. Implement redirects from HTTP to HTTPS
6. Test and verify the functionality of your HTTPS website
7. Renew the certificate before it expires
8. **What is the function of baseline security analysis?**

* Security Benchmarking: help establish a benchmark or reference point to measure the effectiveness of security controls and identify areas for improvement. It provides a comparison against established security standards or frameworks
* Vulnerability Identification: by conduct a baseline security analysis, vulnerabilities and weaknesses in systems and networks can be identified. This includes: misconfigurations, outdated software versions, weak access controls, and other security gaps
* Risk Assessment: helps in assessing the potential risks and impacts associated with identified vulnerabilities. It allows organizations to prioritize their security efforts based on the severity and potential impact of vulnerabilities
* Compliance and Regulatory Requirements: help organization ensure compliance with relevant laws, regulations, and industry standards
* Security Improvement Planning: based on the finding of the analysis, organization can develop a roadmap for improving their security posture. This may include implementing additional security controls, updating configurations, enhancing security policies, or providing employee training
* Security Awareness: raise awareness among stakeholders about importance of security and potential risks

1. **How many types of hackers and objectives of hackers as well as phases?**

* Type of hacker:
  + White Hat Hackers: Ethical hackers who identify vulnerabilities and help improve security
  + Black Hat Hackers: Malicious (hiem doc, co ac tam) hackers who exploit vulnerabilities for personal gain or illegal activities
  + Grey Hat Hackers: Hacker who operate without permission but may not have malicious intent
* Objectives of hackers
  + Unauthorized Access: Gain unauthorized access to systems or networks
  + Data Theft: Steal sensitive information for financial gain or espionage
  + Disruption or Damage: Cause disruption or damage to systems or networks
  + Financial Gain: Engage in fraud or extortion benefit
  + Espionage: Conduct cyber espionage for intelligence gathering
* Phases of hacking:
  + Reconnaissance: Gather information about the target
  + Scanning: Identify vulnerabilities and potential entry points
  + Gaining Access: Exploit vulnerabilities to gain unauthorized access
  + Maintaining Access: Establish persistence within the compromised system or network
  + Covering Tracks: Erase evidence of activities to avoid detection

1. **What is the use of NS lookup?**

* IP Address Resolution: NS Lookup helps in resolving domain names to their corresponding IP address associated with a given domain name
* DNS Record Retrieval: NS Lookup can retrieve various types of DNS records (IPv4 addresses), AAAA records (IPv6 addresses), MX records (mail server information), CNAME records (canonical name aliases),…
* Reverse DNS Lookup: This is particularly useful when investigating suspicious or unwanted network activities, identifying the origin of network traffic, or verifying the legitimacy of an IP address
* DNS Zone Information: provides information about the authoritative name servers for a particular domain
* Troubleshooting and Network Analysis: is a valuable tool for a troubleshooting DNS-related issues, verifying DNS configurations, and analyzing to validate DNS setting, verify DNS propagation and gather information about domain names and their associated IP addresses

1. **What is the Function of wire shark and perform the practical?**

* Functions include:
  + Network troubleshooting: it helps in identifying packet-level problems, analyzing network latency, detecting network errors, and understanding the flow of data between devices
  + Security analysis: It helps security professionals in identifying security vulnerabilities, analyzing network behavior, and investigating security incidents
  + Protocol analysis: Provides a deep analysis of various network protocol, allowing to inspect packet headers, payloads, and protocol behavior
  + Network performance optimization: helps in optimizing network performance. It allows you to identify bottlenecks, monitor bandwidth usage, analyze network latency, and optimize network configurations for better performance
  + Protocol development and testing: it helps in debugging protocols, validating protocol behaviors and identifying interoperability issue
* To performance a practical with Wireshark:
  + Install and launch Wireshark
  + Select the network interface (e.g.,Ethernet, Wi Fi)
  + Start capturing packets by click “Start” or “Capture” button
  + Stop the capture and analyze the packets
  + Use Wireshark’s features to filter and dissect packets
  + Interpret the date for insights into network behavior, performance, or security

1. **What is the Mac Address Scanning and Practical?**

* MAC address scanning refers to the process of discovering and identifying the Media Access Control (MAC) addresses associated with network devices. MAC addresses are unique identifiers assigned to network interfaces, and they are used for communication within a local network.
* The practical use of MAC address scanning includes:
  + Network Device Inventory: MAC address scanning helps in building an inventory of network devices connected to a network.
  + Network Security: MAC address scanning can be used for security purposes. It allows you to identify unauthorized devices on the network by comparing the discovered MAC addresses with a list of approved devices.
  + Network Troubleshooting: MAC address scanning can assist in troubleshooting network connectivity issues. By scanning for MAC addresses, you can verify if the expected devices are present on the network and check for any conflicts or misconfigurations that may be causing connectivity problems.
  + MAC Filtering: MAC address scanning is used in MAC filtering, a technique that allows or denies network access based on the MAC address of the device.
* To perform a practical MAC address scanning:
  + Use a network scanning tool or utility that supports MAC address scanning, such as Nmap, Advanced IP Scanner, or Angry IP Scanner.
  + Specify the IP range or subnet you want to scan for MAC addresses.
  + Start the scanning process and wait for the tool to discover and retrieve
  + Analyze the results and identify the MAC addresses of the devices.
  + Cross-reference the MAC addresses with your records or approved device list to determine the authorized and unauthorized devices on the network.
  + Take appropriate actions based on the results, such as adding or removing devices from the network, updating access control lists, or investigating any unauthorized devices.

1. **What is the Function of IP configure and perform the thru switch?**

* The "IP configure" command, also known as "ipconfig" on Windows or "ifconfig" on Linux/Unix, is a command-line utility used to view and configure IP network interfaces on a computer. It provides information about the IP configuration of the network interfaces and allows for various network-related operations.
* The function of IP configure includes:
  + Displaying IP Configuration: The IP configure command displays the IP address, subnet mask, default gateway, and other network configuration details of each network interface on the computer.
  + Releasing and Renewing IP Addresses: IP configure allows you to release and renew the IP address assigned to a network interface. This is useful when troubleshooting network connectivity issues or when a new IP address is required from the DHCP (Dynamic Host Configuration Protocol) server.
  + Changing IP Configuration: IP configure enables you to change the IP address, subnet mask, default gateway, and other network settings of a network interface. This can be helpful when manually configuring a static IP address or modifying the network configuration to adapt to specific network requirements.
  + Flushing DNS Cache: IP configure can be used to flush the DNS (Domain Name System) cache, which clears any stored DNS records on the computer. This is useful when troubleshooting DNS-related problems or when you need to ensure that the latest DNS information is retrieved.
* Performing the IP configure command through a switch depends on the specific switch or router configuration. Generally, the switch should be accessed through a command-line interface (CLI) or a web-based management interface. The steps to perform IP configuration through a switch may include:
  + Connect to the switch: Use a terminal emulator program or a web browser to establish a connection to the switch. This typically involves providing the switch's IP address, username, and password.
  + Access the configuration interface: Depending on the switch, navigate to the appropriate configuration section or enter the appropriate command to access the IP configuration settings.
  + Configure IP settings: Within the switch's configuration interface, you can modify the IP address, subnet mask, default gateway, and other relevant network settings. Follow the switch's documentation or interface prompts to make the desired changes.
  + Save the configuration: After making the IP configuration changes, save the configuration on the switch to ensure that the settings persist after a reboot or power cycle.

1. **Explain the task manager?**

* The Task Manager is a built-in utility in Windows operating systems that provides an in-depth view of the processes, performance, and resource usage on a computer. It offers a range of features and functions to help users manage their system effectively. Here are some additional details about the Task Manager:
  + Process Tab: The Process tab displays a list of all running processes on the computer. It provides information about each process, including the process name, ID, CPU usage, memory consumption, and user associated with the process.
  + Performance Tab: The Performance tab presents real-time graphical and numerical data about the system's performance. It includes details about CPU usage, memory usage, disk activity, and network activity.
  + Application Tab: The Application tab lists all the currently open applications on the system.
  + Startup Tab: The Startup tab displays a list of programs configured to launch automatically when the computer starts. Users can enable or disable specific programs from starting at boot, helping to improve the system's startup time and overall performance.
  + Services Tab: The Services tab lists all the services running on the computer. It provides information about each service, such as the service name, description, and status.
  + Performance Analysis: The Task Manager includes tools for performance analysis.
  + Resource Monitor: The Task Manager integrates with Resource Monitor, a more advanced tool for monitoring system resources.

1. **What is the Function of Microsoft Network Monitor?**

* The function of Microsoft Network Monitor, also known as Microsoft Message Analyzer, is to capture, analyze, and troubleshoot network traffic in Windows environments. It is a powerful network protocol analyzer tool developed by Microsoft that allows users to monitor and analyze network packets to gain insights into network behavior, diagnose network issues, and troubleshoot network-related problems. Some key functions of Microsoft Network Monitor include:
  + Network Traffic Capture: Microsoft Network Monitor captures network traffic flowing through a network interface, allowing users to capture packets for analysis. It supports capturing traffic from multiple network interfaces simultaneously, providing a comprehensive view of network activity.
  + Packet Analysis: Once network traffic is captured, Microsoft Network Monitor provides advanced packet analysis capabilities. Users can dissect individual network packets, examine protocol headers, inspect payload data, and interpret network protocols to understand the communication between network devices.
  + Protocol Decoding: Microsoft Network Monitor supports a wide range of network protocols and can decode various protocols at different layers of the network stack. It can interpret and analyze protocols such as Ethernet, IP, TCP, UDP, HTTP, DNS, and many others. This allows users to understand the structure and behavior of network protocols within captured packets.
  + Real-Time Monitoring: Microsoft Network Monitor can operate in real-time mode, displaying captured packets as they are captured. This feature is useful for monitoring live network traffic and quickly identifying network issues or anomalies as they occur.
  + Filtering and Search: The tool provides powerful filtering and search capabilities, allowing users to focus on specific packets or specific criteria of interest. Users can apply filters based on protocols, source or destination IP addresses, port numbers, packet content, and other criteria to narrow down the packet set and focus on relevant information.
  + Statistics and Performance Analysis: Microsoft Network Monitor generates statistics and performance metrics based on the captured packets. Users can analyze network utilization, packet loss, latency, throughput, and other performance-related metrics to identify network bottlenecks and optimize network performance.
  + Troubleshooting Network Issues: With its comprehensive packet analysis capabilities, Microsoft Network Monitor is a valuable tool for troubleshooting network issues. Users can examine packet-level details, identify packet-level errors or anomalies, and diagnose problems related to network connectivity, performance, security, and application behavior.

1. **How to Access the registry in a remote location?**

To access the registry in a remote location, you can follow these steps:

1. Open the Registry Editor: On your local computer, open the Registry Editor by pressing "Windows Key + R" to open the Run dialog box, then type "regedit" and press Enter.

2. Connect to the Remote Registry: In the Registry Editor, go to the "File" menu and select "Connect Network Registry." This will open a dialog box to specify the remote computer's name or IP address.

3. Enter Remote Computer Name: In the dialog box, enter the name or IP address of the remote computer whose registry you want to access. Make sure you have the necessary permissions to access the remote computer's registry.

4. Establish Connection: Click the "OK" button to establish a connection to the remote computer's registry. The Registry Editor will attempt to connect to the specified remote computer.

5. Provide Credentials (if required): If the remote computer requires credentials to access its registry, you will be prompted to enter a username and password with sufficient privileges on the remote computer. Enter the credentials and click "OK" to proceed.

6. Access the Remote Registry: Once the connection is established, you will see the remote computer's registry structure in the Registry Editor. You can navigate through the registry keys and access or modify the values as needed.

1. **How to Block cmd?**

* To block the Command Prompt (cmd) on a Windows computer, you can follow these steps:

1. Open the Group Policy Editor: Press "Windows Key + R" to open the Run dialog box, then type "gpedit.msc" and press Enter. This will open the Group Policy Editor.

2. Navigate to the AppLocker Settings: In the Group Policy Editor, navigate to "Computer Configuration" -> "Windows Settings" -> "Security Settings" -> "Application Control Policies" -> "AppLocker".

3. Create a New Executable Rule: Right-click on "Executable Rules" and select "Create New Rule". This will open the "Create Executable Rule" wizard.

4. Select Action and Conditions: In the wizard, select "Deny" for the action and choose the conditions to match the Command Prompt executable (cmd.exe). You can specify the file path or use wildcards to match all instances of cmd.exe.

5. Apply the Rule: Complete the wizard and apply the rule. This will block the execution of the Command Prompt on the computer.

1. **How to block network Connection?**

To block network connections on a Windows computer:

1. Open Windows Firewall Settings: Press "Windows Key + R" to open the Run dialog box, then type "control firewall.cpl" and press Enter. This will open the Windows Firewall settings.

2. Open Advanced Settings: In the Windows Firewall settings window, click on "Advanced settings" on the left-hand side. This will open the Windows Firewall with Advanced Security.

3. Create an Outbound Rule: In the Windows Firewall with Advanced Security window, click on "Outbound Rules" on the left-hand side. Then, click on "New Rule" in the Actions pane on the right-hand side. This will open the New Outbound Rule Wizard.

4. Configure the Rule: In the New Outbound Rule Wizard, select the rule type based on your requirement. For example, you can choose to block a specific program, block a port, or block a predefined rule. Follow the wizard to set the necessary parameters for the rule, such as specifying the program or port to block.

5. Apply the Rule: Complete the wizard, and the outbound rule will be created and applied to block the specified network connection.

To block network connections on Mac

1. Open System Preferences: Click on the Apple menu in the top-left corner of the screen and select "System Preferences" from the drop-down menu.

2. Open Security & Privacy: In the System Preferences window, click on "Security & Privacy."

3. Navigate to Firewall Settings: In the Security & Privacy window, select the "Firewall" tab.

4. Unlock Firewall Settings: If the padlock icon at the bottom left of the window is locked, click on it and enter your administrator password to unlock the settings.

5. Turn on Firewall: Click on the "Turn On Firewall" button to enable the firewall.

6. Customize Firewall Options: Click on the "Firewall Options" button to customize the firewall settings.

7. Block Incoming Connections: In the Firewall Options window, check the box next to "Block all incoming connections" to block all incoming network connections.

8. Add Specific Connections (Optional): If you want to allow specific apps or services to receive incoming connections, click on the "+" button and select the desired apps or services from the list.

9. Apply Changes: Click on the "OK" button to apply the changes and close the Firewall Options window.