1. Choose the most appropriate explanation of a "Rainbow Table Attack." (5 Points) *
   - o A Rainbow Table Attack encrypts data to protect it from unauthorized access.
   - o A Rainbow Table Attack involves using brute force to guess passwords by trying all possible combinations.
   - o A Rainbow Table Attack is a method of securing passwords by adding random salt to them before hashing.
   - o **A Rainbow Table Attack uses precomputed tables of hash values to quickly find the original text of hashed passwords.**

2. Choose the most appropriate explanation of "Salt" in the context of cybersecurity. (5 Points) *
   - o **Salt is a process of adding random data to passwords before hashing to prevent precomputed attacks.**
   - o Salt is a technique for encrypting passwords to ensure they are not stored in plain text.
   - o Salt is a method used to store hashed passwords securely in a database.
   - o Salt is a cryptographic technique used to generate secure keys for data encryption.

3. Choose the most appropriate explanation of the "Challenge-Response Authentication" flow. (5 Points) *
   - o The client and server exchange public keys to create a secure communication channel.
   - o The server sends a random challenge to the client, and the client must encrypt it with a secret key before sending it back.
   - o **The server sends a random challenge to the client, and the client must hash it with their password before sending it back.**
   - o The client sends a random challenge to the server, and the server must decrypt it using a public key.

4. Choose the most appropriate explanation of the "Pass-the-Hash Attack." (5 Points) *
   - o An attack where the attacker intercepts and decrypts encrypted communications between two parties.
   - o **An attack where the attacker uses a captured hash of a password to authenticate without knowing the actual password.**
   - o An attack where the attacker modifies the hash function to generate collisions, allowing unauthorized access.
   - o An attack where the attacker injects malicious code into a hashed value to compromise a system.

5. Choose the most appropriate explanation of the "MFA Fatigue Attack." (5 Points) *
   - o An attack where the attacker exploits software vulnerabilities in the multi-factor authentication system to disable its security measures and gain unauthorized access.
   - o An attack where the attacker, after bypassing password authentication, intercepts and decrypts the multi-factor authentication tokens to gain access.
   - o **An attack where the attacker, having already obtained the victim's password, repeatedly sends multi-factor authentication (MFA) requests to the victim, hoping the victim will eventually approve one out of fatigue.**
   - o An attack where the attacker, using social engineering techniques, tricks the victim into revealing their multi-factor authentication codes.

6. Choose the most appropriate explanation of what "Nmap" is. (5 Points) *
   - o A security tool used for scanning and preventing unauthorized access to a network by monitoring for suspicious activity.
   - o A tool used for scanning network communications to detect vulnerabilities and ensure data security.
   - o **A network scanning tool used to discover hosts and services on a computer network by sending packets and analyzing the responses.**
   - o A scanning tool designed to manage and monitor network traffic for performance optimization.

7. Choose the most appropriate explanation of "Well-Known Ports" including their port range. (5 Points) *
   - o Ports that are dynamically assigned by the system and have a range of 49152-65535.
   - o Ports that are assigned to specific services and applications, ranging from 1024-49151.
   - o **Ports that are used for common, standardized services and applications, ranging from 0-1023.**
   - o Ports that are used for internal network communications and have a range of 1024-65535.

8. Choose the correct combination of port numbers and protocols for "Well-Known Ports." (5 Points)
   - o FTP: 25, HTTP: 443, DINS: 22
   - o **HTTP: 80, FTP: 21, SMTP: 25**
   - o HTTPS: 21, DNS: 53, Telnet: 80
   - o SMTP: 53, Telnet: 443, HTTPS: 25

9. Choose the most appropriate explanation of "LDAP" protocol. (5 Points) *
   - o A protocol used for transferring files between clients and servers.
   - o A protocol used for sending and receiving emails over the internet.
   - o **A protocol used for managing and accessing directories over a network.**
   - o A protocol used for encrypting data transmissions over the internet.

10. Choose the most appropriate explanation of "SMB" protocol. (5 Points) *
    - o A protocol used for managing and accessing directories over a network, typically using port 389.
    - o A protocol used for sending and receiving emails over the internet, typically using port 25.
    - o A protocol used for transferring files between clients and servers, typically using port 21.
    - o **A protocol used for accessing and sharing files, printers, and other resources over a network, typically using port 445.**

11. Please answer the following questions. Please also assume that continuous communication to the same URL is occurring.

- **Question1**

alertContents_totalCount: 1
Date and time of occurrence: 2024-05-08 14:35:21 +00 0(JST)
Action: Blocked
Event Name: Reputation block outbound request: malicious URL
Risk Name: None
Risk Score: 100
User Name: yurie.rikiishi@techone.co.jR
Source Local IP Address: 10.38.135.102
Source Grobal IP Address: XXX.XXX.XXX.XXX(undefined)
Destination IP: 180.163.207[.]111
Traffic forwarding method: ZscalerClientConnector
URL: saas.fancyapi[.Jcom:80
Protocol:0.0.0.0
Status Code:403
User Agent:iOS/Version17.0.3(Build21A360)Ztunnel/1.0
Referer: None
URL Category: Malicious Content
File Type: None
File Name: None
Malware Class: None
Malware Category: None
Sandbox Hash Value (MD5): None
Policy Name: NA
Cloud Application Name: General Browsing Cloud Application Class:General Browsing

Analyst Comment (Description problem) (25 Points) *

12. Please answer the following questions. Please also assume that continuous communication to the same URL is occurring.

- **Question2**

alertContents_totalCount:1
Date and time of occurrence:2024-05-08 14:35:21 +0900(JST)
Action: Allowed
Event Name: Allowed
Risk Name: suspicious
Risk Score:66
User Name: yurie.rikiishi@techone.co.jp
Source Local IP Address:192.168.11.33
Source Grobal IP Address: XXX.XXX.XXX.XXX(undefined)
Destination IP: XXXXXX.XXX.XXX(undefined)
Traffic forwarding method: ZscalerClientConnector
URL: download.wondershare[-ljp/inst/uniconverter15_setup_full14225.exe
Protocol: 23.208.85.152
Status Code:200
User Agent: Mozilla/5.0(Windows NT 10.0; Win64; ×64) AppleWebkit/537.36(KHTML, like Gecko) Chrome/123.0.0.0 5 Safari/537.36 Edg/123.0.0.0
Referer: uniconverter.wondershare[-ljp/picture-convert/heic-to-jpg.html?
URL Category: Corporate Marketing
File Type: Windows Executable (exe, exe64,scr)
File Name: uniconverter 15_ setup._full14225.exe
Malware Class: Behaivior Analysis
Malware Category: Sandbox Suspicious
Sandbox Hash Value (MD5): 144d741be2da0ce054d08f8452febb77
Policy Name: None
Cloud Application Name: Wondershare Japan
Cloud Application Class: Business

Analyst Comment (Description problem) (25 Points) *