**Content Questions**

**Theoretical questions:**

1. What are the different layers of the OSI model?
2. Describe the role of security operations in the enterprise.
3. What is the difference between a threat, a vulnerability, and a risk?
4. What are Indicators of Compromise?
5. Explain what the SIEM system is and its capabilities.
6. Explain what malware is and give an example for 3 types of malware.
7. Describe how a phishing attack works, how would you conduct a phishing attack? What signs will you be looking for?
8. Give an example of a password attack.
9. What is a DDoS Attack? And what is the difference between DDoS and DoS? How would you mitigate a DDOS attack?
10. What Is the difference between Firewall and WAF?
11. Explain the term 'Ransomware' and give one example.
12. Explain what is SQL Injections and what are the indicators to detect SQLI?
13. What is "Metasploit"?
14. What is Steganography? How can an attacker use it?
15. What is Fileless Malware and how to prevent them?
16. What types of XSS do you know and how and attacker will use this attack?
17. Why is DNS monitoring important?
18. What port does ping work over?
19. How would you defend against a cross-site scripting (XSS) attack?
20. What are the default ports for HTTP and for HTTPS?
21. What are honeypots?
22. What is the difference between a worm and a virus?
23. How does the DNS work? I am browsing into [www.google.com](http://www.google.com) - explain the process
24. What’s the difference between hashing, encryption and encoding?
25. What are the two types of encryption and what is the difference between them?
26. What is a port scanning? How would you identify it?
27. How does an AntiVirus work?
28. Explain the terms of False Positives and False Negative which one is more severe?
29. What is sandbox?
30. What is a virtual machine?
31. What’s the difference between an IP address and MAC address? Which one is used to go over the internet?
32. What is a zero day attack?
33. Explain the term of account take over
34. What is a VPN? Why would an attacker use it?
35. What is the ToR browser?

**Hands-On \ Scenario questions:**

1. Describe the way you will analyze a suspicious IP address.

2. Explain what Firewall is, and how we can use it to prevent suspicious activity?

3. In which online sites will you use to analyze suspicious indicators?

4. Explain what is the risk in this rule on SIEM "Malware Detected on Multiple Systems"?

5. You see a user logging in as root to perform basic functions. Is this a problem?

6. Explain which security products you think that should be implemented in a SOC team?

7. What sorts of anomalies would you look for to identify a compromised system?

8. How would you triage if something is high/med/low severity?

9. How do you keep yourself updated on new attacks and threats?

10. Explain the different methodologies to investigate malware.

שמירת התרגום

**Questions and Answers**

1. **What Is a Public IP Address?**

A public IP address is an outward-facing IP address used to access the Internet. Public IP addresses are provided by an internet service provider (ISP) and assigned to the router. It is a unique IP address on the Internet.

1. **What is a Private IP Address ?**

A private IP address is an IP address that is assigned to devices on a local network, such as a home or business network. Private IP addresses are used to identify devices within the network, but they are not accessible from the internet. Instead, devices on the local network communicate with each other using private IP addresses, and a router or gateway device is used to connect the local network to the internet.

1. **What is IP Address?**

Stands for Internet Protocol address is a series of numbers that identifies any device on a network. Computers use IP addresses to communicate with each other both over the internet as well as on other networks.

an IP address appears as four decimal numbers separated by periods. For example, you might use 204.132. 40.155 as an IP for some device in your network. You probably noticed that the four numbers making up an IP are always between 0 to 255.

1. **can ip address be 8 digits?**

With IPv4, each address consists of four 8-digit binary numbers, called octets. An IPv4 address is 32 bits in total.

1. **can ip address be 4 digits?**

IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 192.0.2.1.

1. **Is it possible to have 2 identical ip addresses for devices in 2 different lan's ?**

Yes, it is possible for two devices in different Local Area Networks (LANs) to have the same IP address, as long as the two LANs are not connected to each other in any way.

1. **What are the 5 types of protocol?**

FTP (20,21) (File Transfer Protocol from server to client based tcp)

SSH (22)

SMTP (25) (The Simple Mail Transfer Protocol (SMTP) is an Internet standard communication protocol for electronic mail transmission.)

DNS (53) (The Domain Name System (DNS) is the phonebook of the Internet.)

HTTP (80)(hypertext transfer protocol - a protocol (utilizing TCP) to transfer hypertext requests and information between servers and browsers)

HTTPS (443) (SSL, more secured)

ARP - translate ip address into MAC address

HTTPS - SSL - Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client (e.g., Outlook).

SSH - The Secure Shell Protocol (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Its most notable applications are remote login and command-line execution.

TCP- The transmission control protocol

UDP - User Datagram Protocol (UDP) is a communications protocol that is primarily used to establish low-latency and loss-tolerating connections between applications on the internet.  
  
TCP AND UDP are two commonly used protocols for transmitting data over the internet.

1. **What is the difference between tcp and udp protocols? (The transmission control protocol)**

TCP is ideal for applications such as file transfer, email, and web browsing where data accuracy and reliability are crucial.

UDP, on the other hand, is a connectionless protocol that does not establish a dedicated communication channel between two applications. Instead, it sends data packets as quickly as possible without any confirmation that the data has been received. UDP is used for applications such as video streaming and online gaming where speed and efficiency are more important than data accuracy and reliability.

1. **The main differences between TCP and UDP are:**

* TCP is connection-oriented, while UDP is connectionless.
* TCP ensures reliable data transmission, while UDP does not guarantee data integrity.
* TCP is slower than UDP due to the additional overhead required for establishing and maintaining the connection, while UDP is faster due to its lightweight nature.

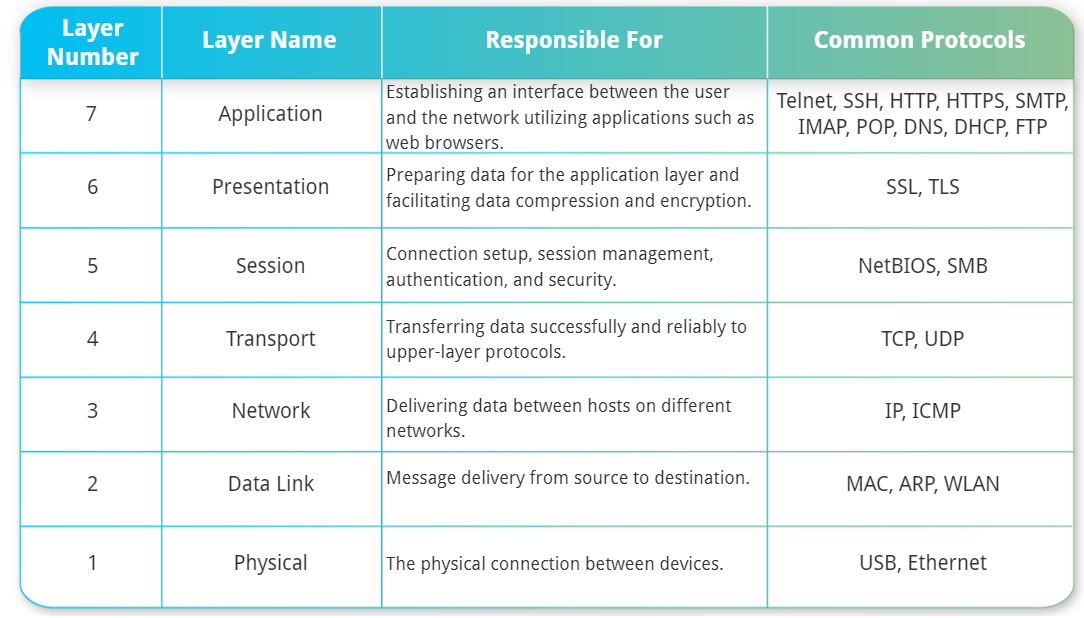
1. **What is the difference between HTTP and HTTPS protocols?**

The main difference between HTTP and HTTPS is that HTTPS is a secure version of HTTP that uses encryption to protect the data transmitted between the web server and client from unauthorized access.

1. **Explain the OSI Model.**

The OSI (Open Systems Interconnection) model is a conceptual framework for understanding how network communication occurs between computers. It is divided into seven layers, each of which performs a specific set of functions that are necessary for communication to occur.

1. Starting from the bottom, the seven layers are:
2. Physical Layer: concerned with the physical aspects of data transmission, such as electrical signals, cables, and connectors.
3. Data Link Layer: responsible for transferring data between adjacent network nodes and error detection.
4. Network Layer: manages the movement of data across networks, including routing, addressing, and fragmentation.
5. Transport Layer: ensures reliable data transmission between end devices, including flow control, error recovery, and segmentation.
6. Session Layer: establishes and manages connections between applications on different devices, including synchronization and checkpointing.
7. Presentation Layer: translates data from one format to another, including encryption and compression.
8. Application Layer: provides services to end-user applications, such as email, file transfer, and remote login.



**12. what is soc?**

A SOC (Security Operations Center) team is responsible for monitoring and defending an organization's information systems and infrastructure from potential security threats.

The primary purpose of a SOC team is to detect, analyze, and respond to security incidents or breaches in real-time.

Maintain the confidentiality, integrity, and availability of an organization's sensitive data and critical systems

**13. Explain to me shortly about siem?**

Splunk SIEM (Security Information and Event Management) is a software solution that helps organizations collect and analyze security events and incidents in real time. It allows security teams to aggregate data from multiple sources, such as logs, network traffic, and endpoints, and apply advanced analytics to detect and investigate security threats.

Splunk SIEM uses a combination of machine learning, behavioral analytics, and threat intelligence to identify anomalous activity, correlate events across different systems, and prioritize security incidents based on their severity. It also provides customizable dashboards, reports, and alerts to help security teams quickly identify and respond to threats.

EDR(sentinal one, checkpoint, palo alto) - generates alerts and responds to them based on predefined rules and detects, analyzes, and responds to abnormalities.

Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is a cybersecurity solution that continuously detects and mitigates cyber threats on endpoint devices.

**14. The principal roles of an EDR are as follows:**

1. Monitor and gather endpoint behavior and activities that could indicate malicious activity or actual attack.
2. Analyze the received data to discover potential threat indicators and patterns.
3. Respond to recognized threats automatically, depending on defined response plans, eliminate or restrict them, and alert the security analysts.

**15. What is Wireshark ?**

Wireshark is a popular network protocol analyzer that allows users to capture and inspect the traffic flowing on a network. It is open source software that runs on multiple platforms, including Windows, macOS, and Linux.

Using Wireshark, you can capture packets transmitted over a network and view the contents of those packets in a human-readable format. Wireshark supports a wide range of network protocols, including Ethernet, Wi-Fi, TCP, UDP, HTTP, DNS, and many others.

In addition to capturing and analyzing network traffic, Wireshark includes many powerful features for filtering, searching, and exporting packet data. It also provides a detailed view of the individual packets that make up network traffic, allowing you to understand the behavior of a network and troubleshoot issues that may arise.

**16. What is DLP ?**

DLP stands for "Data Loss Prevention." It refers to a set of technologies and processes designed to protect sensitive data from being lost, stolen, or leaked. DLP solutions are used to identify and monitor sensitive data in use, in motion, and at rest, and to prevent unauthorized access to or transmission of that data.

IDS/IPS How do they work? Both analyze network traffic and compare it to a database of known threats, however, they function in different ways.

* Intrusion detection system: An IDS is intended to identify a suspected incident and generate an alert without taking any action to prevent the incident from occurri ng. Assume malicious traffic is detected on an attacker's website. In that case, the IDS will generate an alert and notify the analyst, allowing the analyst to take any necessary actions.
* Intrusion prevention system: An IPS, on the other hand, is intended to take action when an event occurs to prevent anything from posing a threat to the network. Since malware attacks have become relatively quick and more complicated, an IPS reduces the significant impact these attacks may pose.

**17. What is the CIA triad?**

The CIA Triad is a widely recognized model that represents the three key principles of information security: confidentiality, integrity, and availability.

Confidentiality - refers to the protection of sensitive information from unauthorized access or disclosure. This includes ensuring that only authorized individuals have access to the information and that it is not disclosed to those who should not have access to it.

Integrity - refers to the protection of the accuracy and completeness of the information. This includes ensuring that information has not been tampered with or modified in any way and that it can be trusted to be accurate and complete.

Availability - refers to the assurance that information is available and accessible to authorized individuals when needed. This includes ensuring that information is not lost or destroyed and that systems and networks are available and functioning as required.

**18. How to handle an incident?**

SOC (Security Operations Center) teams handle events using a structured process that involves the following steps:

Event Collection: SOC teams collect security event data from various sources, including security devices, endpoints, applications, and network traffic.

Event Analysis: SOC teams analyze the collected data to identify any suspicious or anomalous activities that may indicate a security threat. This analysis may involve correlating events across multiple sources, applying threat intelligence, and using machine learning algorithms to detect patterns.

Incident Investigation: If a security threat is identified, SOC teams investigate the incident to determine the scope and severity of the attack. This may involve gathering additional data, conducting interviews, and analyzing system logs and other artifacts.

Incident Response: SOC teams develop and execute a response plan to contain and remediate the incident. This may include isolating affected systems, blocking network traffic, and applying patches or updates to affected software.

Incident Reporting: SOC teams document the incident and provide reports to management and other stakeholders. These reports may include details on the incident's impact, the response actions taken, and recommendations for improving the organization's security posture.

Throughout the event handling process, SOC teams work closely with other IT and security teams, such as network engineers, system administrators, and incident response teams

**19. Different Types of Cyber Attacks**

1. Malware-based attacks (Ransomware, Trojans, etc.) (What is WannaCry? WannaCry is a ransomware worm that spread rapidly across a number of computer networks in May of 2017. After infecting a Windows computer, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin in order to decrypt them)
2. Phishing attacks (spear phishing, whaling, etc.)
3. Man-in-the-middle attacks
4. Denial of Service attacks (DOS and Distributed DoS/ddos)
5. SQL Injection attacks ( What is SQL injection attack with example?

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details)

1. Zero-day exploits and attacks
2. Password attacks (A brute force attack involves 'guessing' usernames and passwords to gain unauthorized access to a system. Brute force is a simple attack method and has a high success rate. Some attackers use applications and scripts as brute force tools.)
3. Cross-site scripting (XSS) attacks (to manipulate the database, gain access, the code injected into the url or submitted into any variability the site has)
4. URL manipulation
5. Inside threats

**20. What is IBM® QRadar?**

It's a siem similar to Splunk but more advanced

is a network security management platform that provides situational awareness and compliance support. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

**21. What is a subnet?**

A subnet, or subnetwork, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments.

The purpose of subnetting is to improve network performance and security in the organization.

**22. How to prevent brute force?**

Brute force attacks are a type of cyber attack where an attacker attempts to gain access to a system or account by repeatedly guessing usernames and passwords until they succeed. There are several measures that can be taken to prevent brute force attacks, including:

1. Implement strong password policies: Encourage users to create strong passwords that are difficult to guess or brute force. This includes using a combination of uppercase and lowercase letters, numbers, and symbols.
2. Use multi-factor authentication (MFA): MFA is an additional layer of security that requires users to provide more than one form of identification before being granted access. This can include biometric authentication, such as a fingerprint or facial recognition, or a one-time code sent to the user's mobile device.
3. Implement account lockout policies: After a certain number of unsuccessful login attempts, lock the account for a specified period of time. This will prevent the attacker from continuing to guess passwords and will give the system administrator time to investigate the attack.
4. Implement rate limiting: Limit the number of login attempts that can be made within a certain period of time. This can help prevent brute force attacks by slowing down the rate at which the attacker can guess passwords.
5. Use intrusion detection/prevention systems (IDS/IPS): These systems can monitor network traffic for patterns that indicate a brute force attack is in progress and can take actions to prevent the attack from continuing.
6. Keep software and systems up to date: Brute force attacks can often exploit vulnerabilities in software or systems. Keeping these up to date with the latest security patches and updates can help prevent these types of attacks.

**23. What is the difference between ping and trace commands?**

Ping is a simple tool that sends an Internet Control Message Protocol (ICMP) echo request to a remote device and waits for an ICMP echo reply. The time it takes for the request and reply to complete is measured in milliseconds, which is known as the "ping time" or "latency." Ping is often used to check if a device is reachable and how fast it responds. It also provides information about packet loss and network congestion.

Trace, on the other hand, is a tool that traces the route that packets take from a local device to a remote device over the network. It does this by sending packets with a Time-to-Live (TTL) field that gradually increases, forcing each network hop to respond with an ICMP "time exceeded" message. By analyzing these responses, trace can identify the path that packets take and measure the latency and packet loss at each hop. Trace is often used to diagnose network routing problems, identify network bottlenecks, and troubleshoot slow network performance.

while ping measures the response time of a remote device, trace maps the network path taken by packets between two devices. Both tools are useful for network troubleshooting, and they complement each other when it comes to identifying and resolving network issues.

### **24. What does a Phishing Email look like?**

One of the reasons phishing emails are so sinister — and unfortunately often successful — is that they're crafted to look legitimate. Generally, the following features are common among phishing emails and should raise red flags:

* Attachments or links
* Spelling errors
* Poor grammar
* Unprofessional graphics
* Unnecessary urgency about verifying your email address or other personal information immediately
* Generic greetings like "Dear Customer" instead of your name.

**25. How to deal with phishing?**

Employ common sense before handing over sensitive information. When you get an alert from your bank or other major institution, never click the link in the email. Instead, open your browser window and type the address directly into the URL field so you can make sure the site is real.

Never trust alarming messages. Most reputable companies will not request personally identifiable information or account details, via email. This includes your bank, insurance company, and any company you do business with. If you ever receive an email asking for any type of account information, immediately delete it and then call the company to confirm that your account is OK.

Do not open attachments in these suspicious or strange emails — especially Word, Excel, PowerPoint or PDF attachments.

Avoid clicking embedded links in emails at all times, because these can be seeded with malware. Be cautious when receiving messages from vendors or third parties; never click on embedded URLs in the original message. Instead, visit the site directly by typing in the correct URL address to verify the request, and review the vendor's contact policies and procedures for requesting information.

Keep your software and operating system up to date. Windows OS products are often targets of phishing and other malicious attacks, so be sure you're secure and up to date. Especially for those still running anything older than Windows 10.