Soc Interview Questions and Answers – CYBER SECURITY ANALYST

By **BalaGanesh** - October 2, 2021

Source/Credits/Written By: Ela Gezerli Ozdemir

Technical:

1. What do you know about the company?

The "company" is one of the global telecommunications technology leaders that deliver innovative IT solutions and offers wireless products and services including cybersecurity operations centers. "The company" is an American company founded in 2000 and headquartered in New York. "The company" has over 135K employees in 150 global locations. "The company" has opened 10th security operation center in Canberra providing SOC services to both public and private sector.

2. What is cybersecurity and why do companies need it?

Cybersecurity is the combination and implementation of security software, hardware, policies, and procedures in computer, network, and information technology systems to protect devices, sensitive data, and services from unauthorized access and modification. Companies need very well-equipped and operated cybersecurity strategies to prevent any damage from occurring to their valuable assets and business.

3. What do you have in your home network?

I set up a very strong user name and password for my router and Wi-Fi, its broadcasting feature is
disabled. I set up MAC address filtering on the router and I use WPA2 (Wi-Fi protected access 2) security encryption technology. It encrypts the traffic on wi-fi networks. I disabled the remote access feature. I use a firewall and configure its security measures and it is always on.

4. What is the CIA triad? (Confidentiality, Integrity, Availability)

CIA is an abbreviation of Confidentiality, Integrity, and Availability. In cybersecurity, these three are the core elements of information security that are kept in place and protected from adverse impacts of incidents such as unauthorized access, disruption, misuse, disclosure, corruption, deletion, modification, etc.

Confidentiality is the term used to describe information/data privacy which means the information is not made available or disclosed to unauthorized entities or individuals.

Integrity is the term used to describe information/data accuracy and completeness throughout its lifecycle. That means that the data cannot be modified by unauthorized entities or individuals.

Availability is the term used to describe information/data being available when needed. Availability systems need to remain available at all times preventing service disruptions due to power outages, hardware failures or system upgrades.

5. Explain the difference between process, guidelines, and policies?

These are the most popular Cyber Security Interview Questions asked in an interview. A process can be defined in this way; it is step-by-step information that helps in specifying what would be the next action and an implementation part. Guidelines are referred to as the recommendation is given to the applications or network, which can be customized and these can be used while creating any procedures. Policies are defined as the criteria for security objectives and the organization’s security framework.

6. What is the meaning of AAA?

AAA stands for Authentication, Authorization, and Accounting.

Authentication is the process of determining if a user is legitimate to use the system and the network. Authentication is usually done using login and password. For example,

you will use a username and password to access your email. The email server authenticates your username and password and provides further access.

Authorization refers to access control rights. This implies every user on the network is allowed access to certain portions of data and information and applications according to his/her level in the organization. **For example**, a marketing person will not be able to record financial transactions. Hence, a user is authorized to perform only certain functions on the network system. These
authorization levels are defined by the system administrator who has access to all the resources and
user policies in the network.

Accounting is known as network accounting which is used to gather all activity on the network for
each use.
Hence, AAA is a framework for network security that is used to control user access, implement
policies, audit usage and keep track of all activities in the network. AAA helps the system administrators and security experts to identify any malicious activity on the network.

7. What is Risk, Threat and Vulnerability in a network?

Risk is any potential loss of, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.

Threat: Anything that can exploit a vulnerability, intentionally or unintentionally, to obtain, damage, or destroying an asset.

Vulnerability: Weaknesses or gaps in a network, software or system that can be exploited by any threats to gain unauthorized access to an asset.

8. What are IDS and IPS and How do you differentiate between IDS and IPS system?

IDS is an Intrusion Detection System that analyses network traffic for signatures of incidents/events that match known cyberattacks.

IPS is Intrusion Prevention System also analyses packets, but can also stop the packet from being delivered.

They are both parts of the network infrastructure. They both compare network packets to cyberthreat databases containing known signatures of cyberattacks and flag any matching packets.

The main difference between them is that IDS is a monitoring system, while IPS is a control system. IDS does not alter the network packets in any way whereas IPS prevents the packet from delivery based on the contents much like how a firewall prevents traffic by IP address. IDS requires a human or another system to look at the results.

Many IDS/IPS systems are integrated with firewalls to create unified threat management technology.IDS and IPS are located in the same area where the firewall is located between the outside world and the internal network.IDS/IPS system covers Automation, compliance, and policy enforcement.

A traditional firewall implements rules that prevent network traffic based on protocol, source/destination address, and/or source/destination port. Firewalls can help you implement access control lists and prevent the use of insecure protocols.IPS works by analyzing the headers and payloads of packets and if suspicious behavior is detected, it can drop the packets. In short, by analyzing the entirety of network packets, IPS can detect potentially malicious behavior that does not inherently violate firewall rules. There are host-based IDS and IPS and also Network-based IPS/IDS anomaly-based detection first creates a baseline of network activity and then compares traffic to that baseline. If network traffic deviates significantly from the baseline, it can be interpreted as a threat.

Security information and event management, SIEMs help make IPS and IDS more scalable and can better enable organizations to achieve compliance, improve reporting, and identify correlations that can indicate a broader threat. In short, SIEMs enable organizations to scale their IDS and IPS data into a more complete security solution.

Some IPS/IDS tools
SolarWinds Security Event Manager

- SNORT
- Security Onion
- WinPatrol
- Osquery
- Splunk
- OSSEC

9. What do you know about cybersecurity frameworks?

An information security framework is a series of documented, agreed, and understood policies, procedures, and processes that define how information is managed in a business to lower risk and vulnerability and increase confidence.

Some of the most common frameworks are:

- International Standards Organisation (ISO) 27K

- Australian Signal Directorate (ASD) Essential 8 -> ASD agency is responsible for cyber welfare
  and information security. The ASD’s cyber division is known as the Australian Cyber Security
  Centre (ACSC). The ACSC provides information, advice, and assistance to prevent and combat cybersecurity threats in public and private sectors.

- US National Institute of Standards and Technology (NIST)-> US agency for industry standardisation and measurements.
- Industry-Specific Standards
- CIS (Critical Security Controls)

10. What is a SIEM?

SIEM is Security Information and Event Management software that provides a holistic view of what is happening on a network in real-time and help cybersecurity analyst to be more proactive in the fight against security threats.

SEM security event management carries out analysis of the event and logs data in real-time to provide event correlation, threat monitoring, and incident response

SIM security information management retrieves and analyses log data and generate a report. For the organization that wants complete visibility and control over what is happening on their network in real-time, SIEM solutions are critical.

How Does SIEM work?

SIEM collects log and event data that is generated by host systems, security devices, and applications throughout an organization's network infrastructure and collating it on a centralized platform. From antivirus events to firewall logs, SIEM software identifies this data and sorts it into categories, such as malware activity, failed and successful logins, and other potentially malicious activity.

When software identifies activity that could signify a threat, alerts are generated to indicate a potential security issue. These alerts can be set either low or high priority using pre-defined rules.

SIEM solutions provide a powerful method of threat detection, real-time reporting, and monitoring, long term analytics of security logs and events.

A single alert from an antivirus filter may not be a cause of panic on its own, but if traffic anomaly alerts are received from the firewall at the same time, this could signify that a severe breach is in progress. SIEM collects all of these alerts in a centralized console, allowing fast and thorough analysis.

- Splunk
- SIEMonster
- AlienVault
- IBM QRadar
- SolarWinds

11. What is weak information security policy?

An information security policy must be strong in terms of distribution, review, comprehension, compliance, and uniformity. Information security considered weak if:

- The policy has not made readily available for review by all employees.
- An organisation is unable to prove that employees reviewed and understood the content of the policy.

12. How can identity theft be prevented?

- Ensure strong password
- Avoid sharing confidential information online on social media
- Shop from known and trusted websites
- Use the latest version of browsers
- Install advanced malware and spyware protection tools
- Update your system and software

13. How can you prevent Man-in-the-middle-attack?

MITM attack happens when a communication between two parties is intruded or intercepted by an outside entity.

- Use encryption (public-key encryption) between both parties
- Avoid using open wi-fi networks.
- Use HTTPS, forced TLS or VPN.

14. What is a DDOS attack and how is it mitigated?

DDOS (Distributed Denial of Service) is when a network is flooded with a large number of requests which is not recognized to handle and making the server unavailable to the legitimate requests.

DDOS can be mitigated by analyzing and filtering the traffic in the scrubbing centers. The scrubbing centers are centralized data cleansing stations wherein the traffic to a website is analyzed and the malicious traffic is removed.

15. What is a brute-force attack and how is it mitigated?

In a brute force attack, the attacker tries to determine the password for a target through permutation or fuzzing process. As it is a lengthy task, attackers usually employ software such as fuzzer or hydra, to automate the process of creating numerous passwords to be tested against a target.

In order to avoid such attacks-password best practices should be followed, mainly on critical

resources like servers, routers.

16. Why do you need DNS (Domain Name System) monitoring?

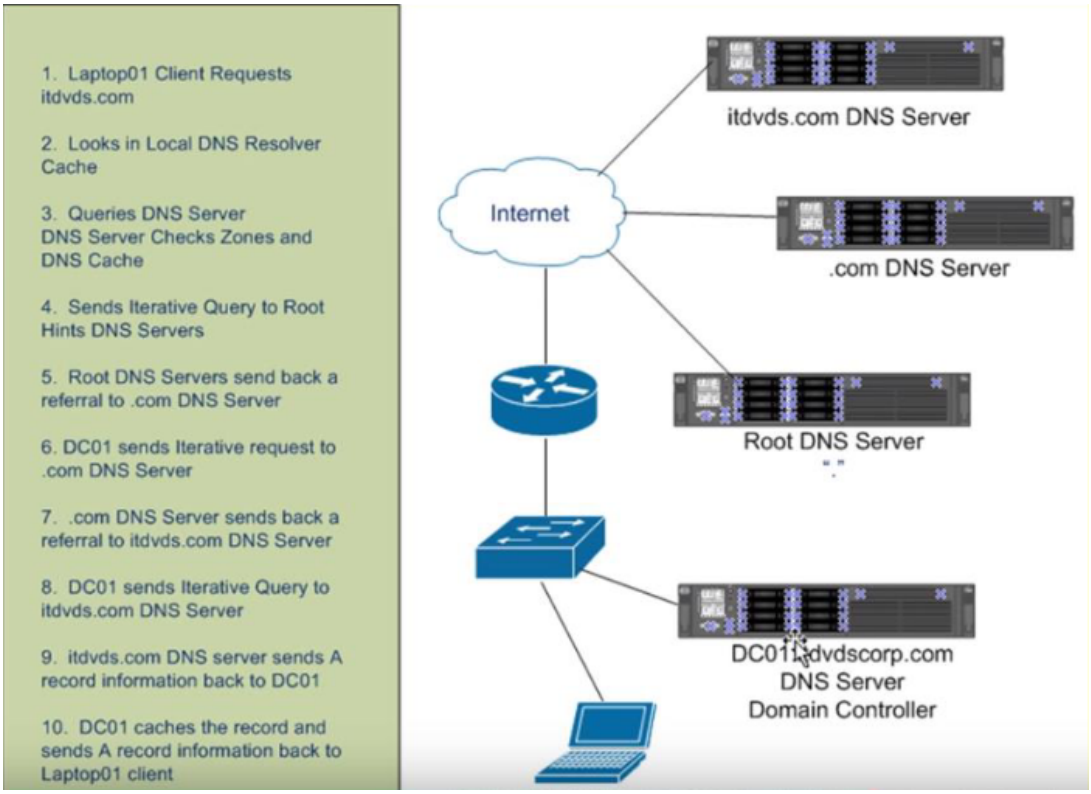
When you add your domain(s) to a DNS provider's name servers, you are making those name servers authoritative for answering your domain's incoming queries. DNS is the first point of contact between you and your clients, so it is crucial to keep an eye on the service you trust to manage it.

DNS monitoring uses network monitoring tools to test connectivity between your authoritative name servers and local recursive servers. The queries have to ask multiple servers for the DNS information until they finally reach the name server authoritative for the domain. We can also monitor the connection between actual clients and the authoritative name servers.

What you can control is actually the most important part of the DNS process, the performance of your authoritative name server answering the recursive name server on the return trip.

Sonar offers an automated monitoring service that checks your domain as often as every 30 seconds for performance changes. You can also set up instant alerts to email or text you when there are any
significant deviations.

Inspecting DNS traffic between the client's devices and your local recursive resolver could be revealing a wealth of information for forensic analysis. DNS queries can reveal bot botnets and malware is connecting to the C&C server, so this is why DNS monitoring is very essential.



17. What are encoding, hashing and encryption?

Encoding: Converts the data in the desired format required for exchange between different systems.

Hashing: Maintains the integrity of a message or data. Any change did any day could be noticed.

Encryption: Ensures that the data is secure and one needs a digital verification code or image in order to open it or access it.

18. What steps will you take to secure a server?

Secure servers use the SSL (Secure Sockets Layer) protocol for data encryption and decryption to protect data.

- Have a secure password for the root and administrator users.
- Make new users that you use to manage the system.
- Remove remote access from default.
- Configure firewall rules for remote access.

19. What is black hat, white hat and grey hat hackers?

Black hat hackers: are those who hack without authority

White hat hackers: are authorized to perform a hacking attempt under signed NDA (non-disclosure agreement)

Grey hat hackers: are white hat hackers who sometimes perform unauthorized activities.

20. What do you know about application security?

It is the practice of improving the security of applications using software, hardware, and other procedural methods.

Countermeasures are taken to ensure application security, the most common one is an application firewall that limits the execution of files or the handling of data by specific installed programs.

21. Can you tell me about common cyber-attacks?

Malware: Malicious software that infects your computer, such as computer viruses, worms, Trojan horses, spyware, and adware.

DDOS: A distributed denial-of-service (DDoS) attack — or DDoS attack — is when a malicious

the user gets a network of zombie computers to sabotage a specific website or server.

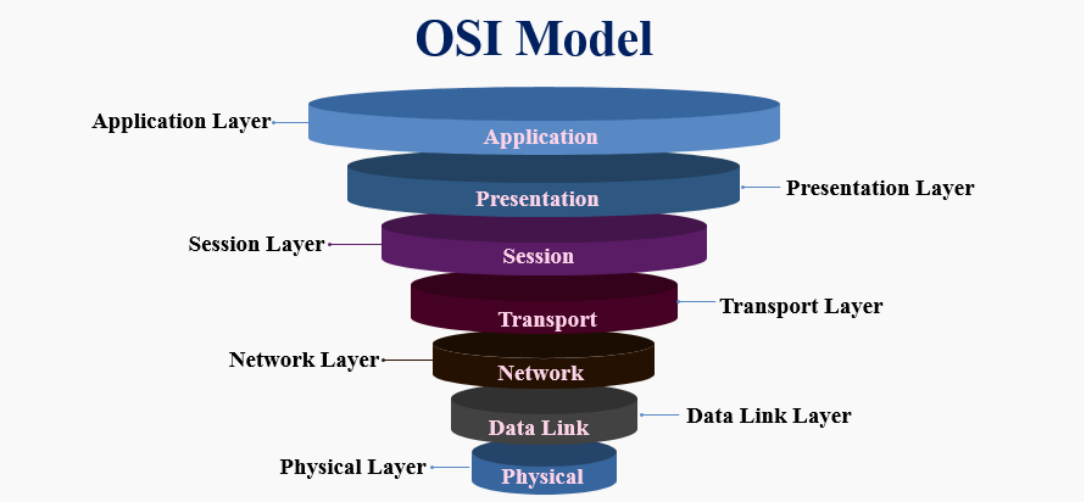
Hacking: Hacking is a term used to describe actions taken by someone to gain unauthorized
access to a computer.

Phishing: Fake emails, text messages, and websites created to look like they're from authentic companies. They're sent by criminals to steal personal and financial information from you. This is also known as "spoofing".

22. What are the OSI layers and what is the job of network layer?

It is Open System Interconnection is a reference model for how applications communicate over a network. There 7 layers in OSI which are:

- Application layer->Data -> network process and apps -> SMTP, telnet, HTTP, FTP, etc.
- Presentation Layer->Data -> Data formatting and encryption -> JPG, HTTPS, SSL
- Session layer->Data -> establishes/ends connections between two hosts -> NetBIOS, PPTP
- Transport layer->Segments -> end-to-end connections and reliability -> TCP, UDP
- Network layer-> Packets -> Path determination and IP (logical addressing) -> routers and layer3 switches
- Data link layer-> Frames -> Physical addressing – > switches
- Physical layer -> Bits -> Send data on to the physical wire -> Hubs, NICS, cables



23. How would you reset a password-protected BIOS configuration?

Pop-out the CMOS or set the factory by using the default password.

24. What is 2FA and how can it be implemented for the public websites?

2FA (two-factor authentication) is an extra layer of security that requires not the only username and password but also something that only the user knows or have (knowledge, possession, inherence)

Authenticator apps replace the need to obtain a verification code via text, voice call or email.

25. What are the three main transmission modes between devices in computer network?

Simplex mode: data can be sent only in one direction i.e. communication is unidirectional. We cannot send a message back to the sender.

Half-duplex mode: data can be transmitted in both directions on a signal carrier, but not at the same time.

Full duplex mode: we can send data in both directions as it is bidirectional at the same time, in other words, data can be sent in both directions simultaneously.

26. What are the network types?

LAN, WAN, personal area, WLAN, Metropolitan, Storage area network, System area network.

27. What is data centre multi-tier model design?

This design consists primarily of the web, application, and database server tiers running on various platforms including blade servers, one rack unit (1RU) servers, and mainframes. Core, aggregation, and access.

28. What are TCP header flags and what they do?

Source port: Sending port (16 bits)

Destination Port (16 bits): receiving port

Flags:

- SYN
- URG
- ACK
- PSH
- RST
- FIN

29. What is SSDP?

Simple service discovery protocol: The Simple Service Discovery Protocol (SSDP) is a network protocol based on the Internet protocol suite for the advertisement and discovery of network services and presence information.

A Simple Service Discovery Protocol (SSDP) attack is a reflection-based distributed denial-of-service (DDoS) the attack that exploits Universal Plug and Play (UPnP) networking protocols in order to send an amplified amount of traffic to a targeted victim, overwhelming the target's infrastructure and taking their web resource offline.

Source port, destination port, length, checksum, data.

30. What are intrusion detection methods? Explain them

The intrusion detection system is a device or software that monitors a network or systems for malicious activity any violation is reported to the SIEM system. IDS types can be host-based and network-based. IDS can detect a malicious activity based on a signature-based approach or anomaly-based approach or a combination of both.

31. What is SNMP?

SNMP (Simple network management protocol) is an internet standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. It is an application layer protocol

32. What are sniffing attacks? Explain them

A sniffer attack corresponds to theft or interception of data by capturing the network traffic using a sniffer. When data is transmitted across the network, if the data is not encrypted the data within the network packet can be read using a sniffer such as Wireshark.

33. What is MAC spoofing? Explain

MAC address is virtually etched to the hardware by the manufacturer. Users are not able to change or rewrite the MAC address but it is possible to mask it on the software side.

This masking is what is referred to as MAC spoofing.

Hackers use this method of attack to conceal their own identity and imitate another.

34. What is ARP and ARP poisoning (Flooding)?

ARP (Address resolution protocol) is a protocol for mapping an IP address to a physical machine address (MAC address) that is recognized in the local network.

When an incoming packet destined for a host machine on a particular local area network arrives ar a gateway, the gateway asks ARP program to find a physical host or MAC address that matches the IP address.

The ARP program looks in the ARP cache and If it finds the address in the ARP cache it provides the MAC address so that the packet can be converted to the right packet length and format and sent to the destination machine. If no IP address is found, ARP broadcasts the request in a special format to all the machines on the LAN to see if one machine knows that IP address associated with it.

ARP poisoning is ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.

35. What are three main data transmission methods in layer 2?

Unicast, Broadcast, Multicast (Explain each one)

36. What is DHCP?

DHCP is a dynamic host configuration protocol. When it is activated, DHCP assigns IP addresses to devices on the network.

37. What is VLAN? What is the difference between VPN and VLAN?

VPN: it is related to remote access to a network with a secured and encrypted tunnel. Saves the data from prying eye while in transit and no one on the net can capture the packets.

VLAN: Helps to group work stations that are not within the same locations into the same broadcast domain. Logically segregates networks without physical segregation with switches. Does not involve any encryption.

38. What is port blocking within LAN?

Restricting users from accessing a set of services within the local area network is called port blocking.

Stopping the source not to access the destination node via port as the application works on the ports are blocked to restrict access.

39. What tools are commonly used to secure a standard network?

Firewalls, end-point antiviruses, security policies and procedures, IDS/IPS, password managers.

40. How do you keep up-to-date outside the normal working hours?

I follow security professionals on LinkedIn and read their articles

- Browse security-related social media topics
- Follow the SANS page
- Browse National vulnerability database and CVE (common vulnerabilities and exposures)
  websites
- ACCC website
- CISCO security blog
- twitter

41. Tell us about some cyber-attacks happened

WannaCry ransomware attack in 2017

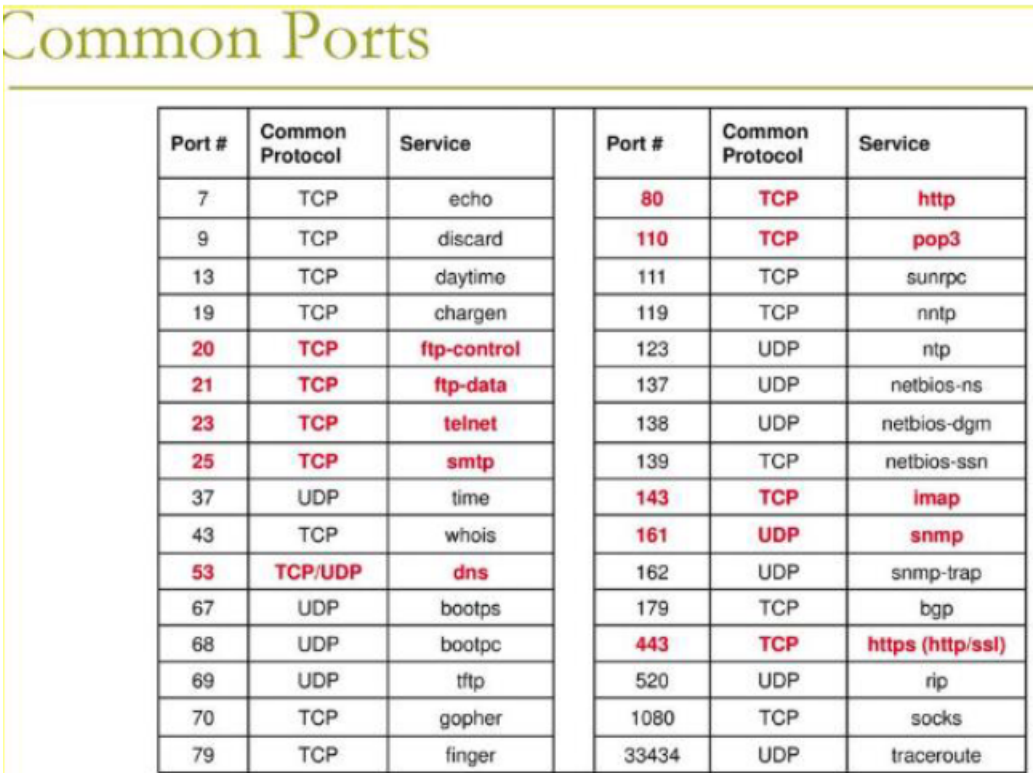
- Stuxnet a malicious computer worm infected by means of a thumb drive
- ANU Hack happened on November 9, 2018 the hackers sent an email to a senior staffmember at the ANU. Another staff member who had access to their colleague's account previewed the email without clicking on it. Even though the email was deleted, it was too late to stop the hackers, who had already accessed the senior staff member's username,password and calendar.
- The world's biggest currency exchange company was hacked and the data is being held hostage for $6 million. The company's exchange services have been offline since the hack was detected on December 31, 2019. On Tuesday, December 31st, Travelex detected a
  software virus which had compromised some of its services," the company said in astatement. "On discovering the virus, and as a precautionary measure, Travelex immediately took all its systems offline to prevent the spread of the virus further across the network."
  The virus in question is reportedly the Sodinokibi ransomware, also known as REvil. The virus, in its broadest function, is used to encrypt data and demand a ransom in order to unlock said data.
  Ransom.Sodinokibi is Malwarebytes' detection name for a family of Ransomware that targets Windows systems. Ransom.Sodinokibi encrypts important files and asks for a ransom to decrypt them.

42. How exactly does traceroute work?

Tracert or traceroute is a command that records the route (the specific gateway computers at each hop) through the internet between your computer and a specified destination computer. It also calculates and displays the amount of time each hop took. Traceroute determines when the packet has reached the destination by including a port number that is outside the normal range.

When it's received, a Port Unreachable message is returned, enabling the traceroute to measure the time length of the final hop. Traceroute is a handy tool both for understanding where problems are in the Internet network and for getting a detailed sense of the Internet itself. Traceroute helps to identify where the connection stops or gets broken, whether it is a firewall, ISP, router, etc.

43. What are some common port numbers and their services?


Common Ports

Port #	Common Protocol	Service	Port #	Common Protocol	Service
7	TCP	echo	80	TCP	http
9	TCP	discard	110	TCP	pop3
13	TCP	daytime	111	TCP	sunrpc
19	TCP	chargen	119	TCP	nntp
20	TCP	ftp-control	123	UDP	ntp
21	TCP	ftp-data	137	UDP	netbios-ns
23	TCP	telnet	138	UDP	netbios-dgm
25	TCP	smtp	139	TCP	netbios-ssn
37	UDP	time	143	TCP	imap
43	TCP	whois	161	UDP	snmp
53	TCP/UDP	dns	162	UDP	snmp-trap
67	UDP	bootps	179	TCP	bgp
68	UDP	bootpc	443	TCP	https (http/ssl)
69	UDP	tftp	520	UDP	rip
70	TCP	gopher	1080	TCP	socks
79	TCP	finger	33434	UDP	traceroute

44. How does a firewall work? What is the better approach of setting up a firewall?

A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. The purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communication. In most server infrastructure, firewalls provide an essential layer of security that combined with other measures, prevent attackers from accessing the servers.

There are packet filtering (stateless), stateful, and application layer network firewall types. Firewall functionalities can be provided as software and also hardware devices such as routers or firewall appliances.

Some firewall rules that can be configured:

- Accept new and established incoming traffic to the public network interface on port 80 and 443(HTTP and HTTPS web traffic)
- Drop incoming traffic from IP addresses of the non-technical employees in your office to port 22(SSH)
- Accept new and established incoming traffic from your office IP range to the private network interface on port 22(SSH)

The firewall has accepted, reject and drop options when configuring.

Following are the steps you should take to configure the firewall:

- Strong username/Password
- Disable remote administration
- For certain applications to work properly, such as Web server or ftp server, you need to configure appropriate port forwarding (**Port forwarding** is a technique that is used to allow external devices access to computers services on private networks. if you want, for example, to host a website on your internal network and that website needs to be accessible to external clients then you will need to use a standard port (**port 80 for http**) as the external client expects this. To do this you statically map the **external IP address + port 80** to the **Internal IP address** of the **web server + port 80 – This is port forwarding.**
- Installing a firewall on a network with an existing DHCP server will cause conflicts unless the firewall's DHCP server is disabled
- In order to troubleshoot firewall issues or potential attacks, you want to make sure to enable logging and understand how to view the logs.
- Firewalls needs to be configured to enforce security policies.

45. If there was a possible attack from a specific IP address, what would you do to defend the network?

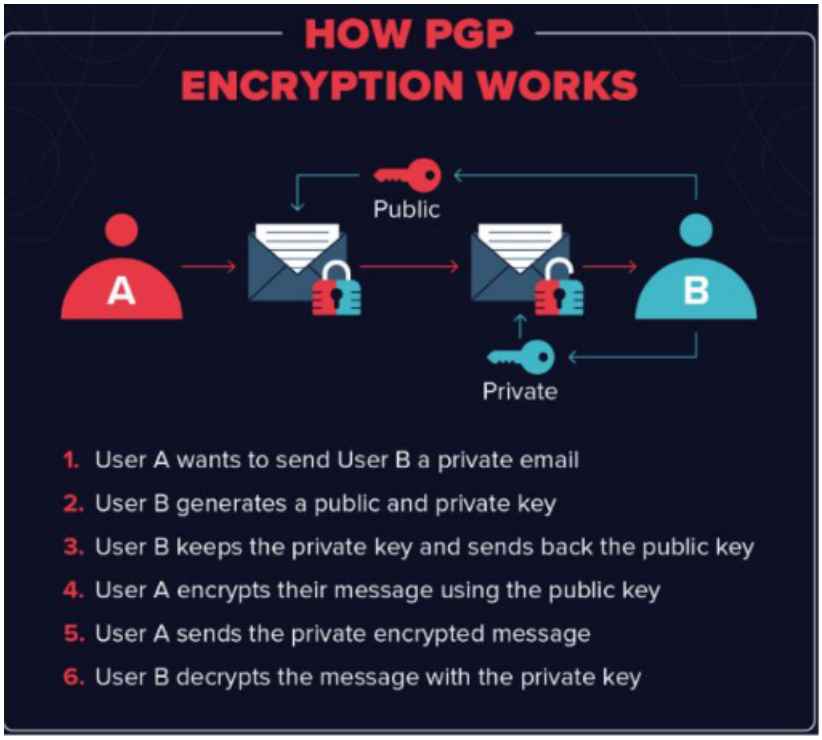
Block the IP address on the firewall

46. How does encryption work? Why is it important?

Encryption is a process that encodes a message or file so that it can only be read by certain people. Encryption uses an algorithm to scramble or encrypt data and then uses a key for the receiving party to unscramble or decrypt the information. Keys are usually generated with random number generators or computer algorithms that mimic random number generators.

Key: Random string of bits created specifically for scrambling and unscrambling data. These are used to encrypt and/or decrypt data. Each key is unique and created via an algorithm to make sure it is unpredictable. Longer keys are harder to crack. Common key lengths are 128 bits for symmetric key algorithms and 2048 bits for public-key algorithms.

- **Private Key (or Symmetric Key)**: This means that the encryption and decryption keys are the same. The two parties must have the same key before they can achieve secure communication.
- **Public Key**: This means that the encryption key is published and available for anyone to use. Only the receiving party has access to the decryption key that enables them to read the message.



47. What are salted hashes?

Salt is random data. When a properly protected password system receives a new password, it creates a hash value of that password, a random salt value, and then the combined value is stored in its database. This helps defend against dictionary attacks and known hash attacks.

48. Can you explain TCP three-way handshake method?

The TCP three-way handshake is the method used in a TCP/IP network to create a connection between a local host/client and server. It is a three-step method that requires both the client and server to exchange SYN and ACK packets before actual data communication begins.

• A client node sends an SYN data packet over an IP network to a server on the same or an external network. The objective of this packet is to ask/infer if the server is open for new connections.

• The target server must have open ports that can accept and initiate new connections. When the server receives the SYN packet from the client node, it responds and returns a confirmation receipt – the ACK packet or SYN/ACK packet.

• The client node receives the SYN/ACK from the server and responds with an ACK packet. Upon completion of this process, the connection is created and the host and server can communicate.

49. Can you explain the SSL (Secure socket layer) encryption and handshake? Which one is more secure SSL or TLS (Transport layer security)?

SSL is a Secure Socket Layer. It is a protocol that enables safe conversation between two or more parties. It is designed to identify and verify that the person you are talking to on the other end is who they say they are. For example, HTTPS (Hypertext Transfer Protocol Secure) is HTTP combined with SSL which provides safe browsing with encryption.

TLS is Transport Layer Security is another cryptographic protocol that provides authentication and data encryption between servers, machines, and applications. SSL is the predecessor to TLS and they can be
used together.

SSL handshake process
1. The client contacts the server and requests a secure connection. The server replies with the list of cipher suites-Algorithmic toolkits of creating encrypted connection-that it knows how to use. The client compares this against its own list of supported cipher suites, selects one, and lets the server know that they will both be using it.

2. The server then provides its digital certificate, an electronic document issued by a third-party authority confirming the server's identity. This digital certificate contains the server's public cryptographic key. Once the client receives the certificates, it confirms the certificate's authenticity.

3. Using the server's public key, the client and server establish a session key that both will use for the rest of the session to encrypt communication.

50. Can you name 5 common ports and their services?

- 21-FTP- File transport protocol
- 22- SSH- secure shall protocol that secure the communication between hosts and services.
- 80- HTTP- Hypertext transport protocol- HTTP gives users a way to interact with web resources such as HTML files by transmitting hypertext messages between clients and servers.
- 67-68 – DHCP
- 110- POP
- 53- DNS
- 443- HTTPS

51. How can you defend against ransomware? (They wanted to hear antivirus and segmented VLAN's)

Network Segregation, Segmentation Can Stop Ransomware Attacks. Network segregation is the separation of critical networks from the Internet and other internal, less sensitive networks.

Network segmentation, which involves splitting the larger network into smaller network segments, can be accomplished through firewalls, virtual local area networks, and other separation techniques.

Both strategies have the potential to prevent ransomware attacks that encrypt files on the network, block access to those files, and then direct the victim to a webpage with instructions on how to pay a ransom in bitcoin to unlock the files.

52. What are three types of malware and then explain them in more detail?

Virus – A computer virus can automatically create and install a copy of itself on a computer's files, and – like a virus in humans – it can spread from computer to computer. Viruses require a host program to exist, and they are initiated when the user opens or runs this host file. Typically, this type of malware is designed only to destroy a particular computer's files, and the extent of its damage can vary. Some viruses are simply annoying, while others can cause more serious damage that requires the attention
of a Maryland virus removal professional.

Worm – Much like viruses, worms can automatically replicate and infect multiple files. Unlike viruses, they can operate within a computer without a host file and without attaching to an existing file. Many times, worms gain access to a computer via email, while other times they enter the network through a vulnerability. Instead of targeting a single computer, worms typically seek to harm an entire network or open a backdoor for other malware.

Trojan -Named after the famed wooden gift horse Greek soldiers used to invade the city of Troy, Trojans operate in a similar fashion. They are disguised as legitimate or even beneficial programs, and once a user enables them, they infect the computer. They are not self-replicating and can only be spread by user interaction, typically through email attachments or internet downloads.

53. What is XSS? how do you defend a system from XSS?

XSS (cross-site scripting) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject malicious client-side scripts into web pages viewed by other users. XSS vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

XSS vulnerability attacks can steal data, take control of a user's session, run malicious code, or be used for a phishing scam. they attack an application's users, not the application or server. XSS

attacks is to gather cookie data, as cookies are commonly and regularly used incorrectly to store information such as session IDs, user preferences, or login information.

How to reduce the risk of XSS attacks?

security development lifecycle (SDL). I will look at SDLs in more detail in a future article, but their aim is to reduce the number of security-related design and coding errors in an application and reduce the severity of any errors that remain undetected.

A critical rule you'll learn when developing secure applications is to assume that all data received by the application is from an untrusted source. This applies to any data received by the application — data, cookies, emails, files, or images — even if the data is from users who have logged into their account and authenticated themselves.

Not trusting user input means validating it for type, length, format, and range whenever data passes through a trust boundary, say from a Web form to an application script, and then encoding it prior to redisplay in a dynamic page.

In practice, this means that you need to review every point on your site where user-supplied data is handled and processed and ensure that, before being passed back to the user, any values accepted from the client side are checked, filtered, and encoded.

54. What is a DMZ and what would you most likely find in it?

In computer security, a DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.

The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network and, if its design is effective, allows the
organization extra time to detect and address breaches before they would further penetrate into the internal networks.

55. What is Splunk?

Splunk is a SIEM tool that performs near real-time data and logs analyses, visualization, alerting, reporting, and investigation of computer and network systems. Splunk can make machine data (scrambled, meaningless characters) readable because we can train Splunk to tag characters with a meaningful item.

Splunk components:

Indexer: Indexer takes raw data from forwarders, turns it into events, and places results into
an index that is stored in a bucket (categorizes and applies metadata to the data)

Search heads: Search heads act as the user interface and allow users to create dashboards,
alerts and reports related to analyzed logs and data.

Forwarder: Forwards raw data to other parts of the deployment (indexer, search head & indexer) universal forwarder requires very little configuration and heavy forwarder which you can configure it according to your needs.

Splunk has a data pipeline that includes 4 phases:

- Input
- Parsing
- Indexing
- Searching

56. What is Cyber Kill chain?

Kill Chain is a term related to the structure of a cyber-attack consisting of target identification, force dispatch to target, decision and order to attack the target, and finally the destruction of the target.

Attacks may occur in phases and can be disrupted through controls established at each phase.

The kill chain can also be used as a management tool to help continuously improve network defense.
Threats progress through several phases in the model, including:

1. Reconnaissance: The intruder selects a target, researches it, and attempts to identify
vulnerabilities in the target network.

2. Weaponization: Intruder creates remote access malware weapon, such as a virus or worm,
tailored to one or more vulnerabilities.

3. Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB
drives)

4. Exploitation: Malware weapon’s program code triggers, which takes action on target network to exploit the vulnerability.

5. Installation: Malware weapon installs access point (e.g., "backdoor") usable by an intruder.

6. Command and Control: Malware enables intruders to have "hands on the keyboard" persistent access to the target network.

7. Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration,
data destruction, or encryption for ransom.

Defensive courses of action can be taken against these phases:

1. **Detect**: determine whether an attacker is poking around

2. **Deny**: prevent information disclosure and unauthorized access

3. **Disrupt**: stop or change outbound traffic (to the attacker)

4. **Degrade**: counter-attack command and control

5. **Deceive**: interfere with command and control

6. **Contain**: network segmentation changes

57. What is MITRE ATT&CK?

MITRE ATT&CK™ is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. has been around for five years and is a living,
growing document of threat tactics and techniques that have been observed from millions of attacks on enterprise networks.

A custom XML configuration is set up with Windows agents to translate process activity to MITRE ATT&CK vectors, so specific events can be easily queried.

Dashboards are also provided for forensic analysis of MITRE ATT&CK correlations. It can be integrated with Malware information sharing platform (MISP), OpenCTI

Also Read: **What is the MITRE ATT&CK Framework? How Is It Useful**

Scenario Based Interview Questions

58. Password and Other suspicious Request- Cybercriminals can pose as employees, contractors or third-party vendors to bait employees into divulging sensitive passwords or other access controls, how do you recognize a suspicious request?

Cybercriminals use the phishing technique to gain passwords, credentials, and sensitive information of users by means of e-mails and messages.

They ask you to download attachments or click on a link to update or change your password or user credentials. They then seize your user name and password to use create a new account for themselves.

- Legit companies do not request your sensitive information via e-mail or message.
- Legit companies call you by your name. Some hackers avoid the salutation altogether
- Legit companies have domain emails, so check the name as well as the email address of the a person who sent you the email.
- Check if there are spelling errors and bad grammar.
- Legit companies do not force you to their website and do not send unsolicited attachments.

59. Unauthorized Computers and Devices on Network- Computers and devices that haven't gone through proper authentication processes before joining your corporate network are perfect targets for attackers. How does your response team not only identify attempts to connect to your network but also block them?

- Authenticate the user and the device before joining them to network.
- Implement access control process to recognize each user and each device and enforce security policies. With access control method we can also block noncompliant endpoint devices or give them only limited access. Network access controls implement a defined security policy for access which is supported by a network access server that performs the authentication and authorization. dynamic network access control works on specific computers that are connected to a local area network and are considered to be trusted systems. When an unauthorized user attempts to access the network, the trusted systems will restrict access and then communicate the action to the main policy server.
- Mobile device management should be in place to control and configure which devices can access your network.

60. Data Breach on the network- What is the first thing you do when attack occurs on the network? what are the incident response plan in place in your organization? Describe the six steps for incident response

- Investigate the incident. Gathering information on the incident is important in validating that an incident has occurred (i.e., who, what, where, and when the incident occurred)
- If the breach is valid, inform management with a summary of the incident
- Identify the suspected cause of the incident. For example, was the breach caused by a firewall with an open port, malware on the system, successful email phishing attack, outdated antivirus software, or an employee that unknowingly divulged confidential data?
- Isolate the effected system and eradicate the cause of the breach
- Implement policy, procedures, and technology if necessary, to prevent a recurrence
- Perform period technology audit or risk assessments combined with network penetration testing to identify weaknesses in the system.

61. How do you stay on top of cybersecurity news and developments?

- The Computer Emergency Readiness Team Coordination Center (CERT/CC) has up-to-date vulnerability information for the most popular products. The vulnerability database is searchable, and you can sort the entries by severity or date published.
- SecurityFocus has a feed with recent advisories for almost every product. The specific feeds are not frequently updated.
- The National Vulnerability Database has two feeds: One covers all the recent CVE vulnerabilities, while the other focuses on fully analyzed CVE vulnerabilities. I only follow the feed with the fully analyzed vulnerabilities because it provides the information that’s important to me: the vulnerable product names.
- US-CERT and the Industrial Control Systems CERT (ICS-CERT) publish regularly updated summaries of the most frequent, high-impact security incidents. The information is similar to CERT/CC. The content from ICS-CERT is especially useful if you have to protect critical infrastructure.
- The feed at Full Disclosure, now part of SecLists.org, is one of the oldest available. It can b rather chatty, but it gives access to information on vulnerabilities that is not immediately covered via other channels.
- Most vendors have their own feed of advisories, as well. With the use of good asset management, you should be able to compile a list of key products and vendors to follow.
- SANS, the hacker news, reddit news

62. What types of security breaches have you dealt with? How did you deal with them and what did you learn from them?

Theft or loss:

- Computers and laptops, portable electronic devices, electronic media, paper files.
- Laptops should be secured at all times. Keep it with you or lock it up securely before you step
  away — and make sure it is locked to or in something permanent.
- Use extra security measures for portable devices (including laptop computers) and portable electronic media containing sensitive or critical info:
- Encryption
- Extra physical security
- Securely delete personal identity information (PII) and other sensitive data when it is no longer needed for business purposes.
- Report suspected theft of ACCC-related computing equipment to **Password hacked or revealed**
- Use good, cryptic passwords that are difficult to guess
- Never share or reveal your passwords
- Use different passwords for work and non-work accounts
- Have a unique password for each account

Protect Your Company Against A Data Breach by Applying Following Key Measures

- Train your employees
- Protect sensitive data
- Enforce strong passwords
- Monitor data and its traffic
- Limit access
- Patch vulnerabilities
- Encrypt devices and data
- Two-factor authentication
- Breach recovery plan
- IR plan in place and exercised

BalaGanesh

https://www.socinvestigation.com

Balaganesh is a Incident Responder. Certified Ethical Hacker, Penetration Tester, Security blogger, Founder & Author of Soc Investigation.