SOC INTERVIEW Question/Answers: Freshers to Senior Level

➢ Important Fundamental Questions

1. What is an IPS and how does it differ from IDS?
   Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are both parts of the network infrastructure. IDS/IPS compare network packets to a cyber threat database containing known signatures of attacks — and flag any matching packets.

   The main difference between them is that IDS is a monitoring system, while IPS is a control system.

   IDS doesn't alter the network packets in any way, whereas IPS prevents the packet from delivery based on the contents of the packet, much like how a firewall prevents traffic by IP address.

2. Explain risk, vulnerability and threat?
   A threat exploits a vulnerability and can damage or destroy an asset. Vulnerability refers to a weakness in your hardware, software, or procedures. (In other words, it's a way hackers could easily find their way into your system.) And risk refers to the potential for lost, damaged, or destroyed assets

3. What is the difference between Asymmetric and Symmetric encryption and which one is better?
   TIP: Keep the answer simple as this is a vast topic. Symmetric encryption uses the same key for both encryption and decryption, while Asymmetric encryption uses different keys for encryption and decryption. Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel. Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred. Setting up a channel using asymmetric encryption and then sending the data using a symmetric process

4. What is XSS, and how w l you mitigate cross-site site scripting as a JavaScript vulnerability in web applications. The easiest way to explain this is a case when a user enters a script in the client-side input fields and that input gets processed without getting validated. This leads to untrusted data getting saved and executed on the client-side. Countermeasures of XSS are input validation, implementing a CSP (Content security policy), etc.

5. What is the difference between encryption and hashing?

TIP: Keep the answer short and straight.
Point 1: Encryption is reversible whereas hashing is irreversible. Hashing can be cracked using rainbow tables and collision attacks but is not reversible.

Point 2: Encryption ensures confidentiality whereas hashing ensures Integrity

6. What is CSRF?
   Cross-Site Request Forgery is a web application vulnerability in which the server does not check whether the request came from a trusted client or not. The request is just processed directly. It can be further followed by the ways to detect this, examples, and countermeasures.

7. Difference between XSS & CSRF
   Since it doesn't require any user interaction, XSS is believed to be more dangerous
   CSRF is restricted to the actions victims can perform. XSS, on the other hand, works on the execution of malicious scripts enlarging the scope of actions the attacker can perform
   XSS requires only a vulnerability, while CSRF requires a user to access the malicious page or click a link
   CSRF works only one way – it can only send HTTP requests, but cannot view the response. XSS can send and receive HTTP requests and responses to extract the required data

8. Is XSS client side client-server-side attack?
   Client-side attack

9. What is IOC?
   An indicator of compromise in computer forensics is an artefact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion. Ex hash, IP, domain, URL, user-agent etc.

10. Antivirus vs EDR
    DR:
    1. EDR includes real-time monitoring and detection of threats – including those that may not be easily recognized or defined by standard antivirus. Also, EDR is behaviour based, so it can detect unknown threats based on a behaviour that isn't normal.
    2. Data collection and analysis determine real patterns and alerts organizations to threats
    3. Forensic capabilities can assist in determining what has happened during a security event

4. EDR can isolate and quarantine suspicious or infected items. It often uses sandboxing to ensure a file's safety without disrupting the user's system.
5. EDR can include automated remediation or removal of certain threats

Antivirus
1. Antivirus is signature-based, so it only recognizes threats that are known.
2. AV can include scheduled or regular scanning of protected devices to detect known threats
3. Assists in the removal of more basic viruses (worms, trojans, malware, adware, spyware, etc.)
4. Warnings about possibly malicious sites

Do I need both? No EDR is sufficient

11. What is a firewall?
    A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

12. IPS vs Firewall
    The main difference is that firewall performs actions such as blocking and filtering traffic while an IPS/IDS detects and alerts a system administrator or prevents the attack as per configuration. A firewall allows traffic based on a set of rules configured

13. What is a Security Misconfiguration?
    Security misconfiguration is a vulnerability when a device/application/network is configured in a way that can be exploited by an attacker to take advantage of it. This can be as simple as leaving the default username/password unchanged or too simple for device accounts etc.

14. What is a Black hat, white hat, and Grey hat hacker?
    Black hat hackers are those who hack without authority. White hat hackers are authorized to perform a hacking attempt under a signed NDA. Grey hat hackers are white hat hackers who sometimes perform unauthorized activities

15. How do you keep yourself updated with the information security news?
    By following blogs such as Trendmicro blogs, hacker news, gbhackers etc.

16. Name some recent attacks and explain in brief?
    Example: log4j Vulnerability, spring4shell vulnerability

17. What is the CIA?

Confidentiality: Keeping the information secret.

Integrity: Keeping the information unaltered.

Availability: Information is available to the authorized parties at all times.

18. HIDS vs NIDS which one is better and why?
    HIDS is a host intrusion detection system and NIDS is a network intrusion detection system. Both the systems work on similar lines. It's just that the placement is different. HIDS is placed on each host whereas NIDS is placed in the network. For an enterprise, NIDS is preferred as HIDS is difficult to manage, plus it consumes the processing power of the host as well.

19. What is port scanning?
    Port scanning is the process of sending messages to gather information about the network, system, etc. by analyzing the response received.

20. What is the difference between VA and PT?
    Vulnerability Assessment is an approach used to find flaws in an application/network whereas Penetration testing is the practice of finding exploitable vulnerabilities like a real attacker will do. VA is like travelling on the surface whereas PT is digging it for gold.

21. Can you name some response codes from a web application?
    1xx – Informational responses
    2xx – Success
    3xx – Redirection
    4xx – Client-side error
    5xx – Server side error

22. When do you use tracert/traceroute?
    In case you can't ping the final destination, tracert will help to identify where the connection stops or gets broken, whether it is the firewall, ISP, router, etc.

23. DDoS and its mitigation?
    DDoS stands for distributed denial of service. When a network/server/application is flooded with a large number of requests that it is not designed to handle making the server unavailable to legitimate requests. The requests can come from different not related sources hence it is a distributed denial-of-service attack. It can be mitigated by analyzing and filtering the traffic in the scrubbing centres. The scrubbing centres are

centralized data cleansing stations wherein the traffic to a website is analyzed and the malicious traffic is removed.

24. What is a WAF and what are its types?
    WAF stands for web application firewall. It is used to protect the application by filtering legitimate traffic from malicious traffic. WAF can be either a box type or cloud-based.

25. How do you handle AntiVirus alerts?
    Check the policy for the AV and then the alert. If the alert is for a legitimate file then it can be whitelisted and if this is a malicious file then it can be quarantined/deleted. The hash of the file can be checked for reputation on various websites like virustotal, malwares.com, etc. AV needs to be fine-tuned so that the alerts can be reduced.

26. Blue teaming vs Red teaming
    A red team is an attacker and a blue team is a defender. Being on the red team seems fun but being in the blue team is difficult as you need to understand the attacks and methodologies the red team may follow.

27. What is a false positive and false negative in the case of IDS? Which one is more acceptable?
    When the device generated an alert for an intrusion that has not happened: this is a false positive and if the device has not generated any alert and the intrusion has happened, this is the case of a false negative
    False positives are more acceptable. False negatives will lead to intrusions happening without getting noticed.

28. What is data leakage? How will you detect and prevent it?
    Data leak is when data gets out of the organization in an unauthorized way. Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorized upload of data to public portals, removable drives, photographs, etc. There are various controls which can be placed to ensure that the data does not get leaked, a few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the mails to the internal network, restriction printing of confidential data, etc.

29. Open source software and licensed software, which one you will prefer?
    Licensed software as the licensed version is updated and easy to track in an organization

30. What is DNS?
    The Domain Name System (DNS) turns domain names into IP addresses, which browsers use to load internet pages

31. Hodoes w DNS Wordoes ks?
    Please search another the r cybersec live youtube channel

32. What is TLD?
    A TLD (top-level domain) is the most generic domain in the Internet's hierarchical DNS (domain name system). A TLD is the final component of a domain name, for example, "org" in developer[.]mozila[.]org . ICANN (Internet Corporation for Assigned Names and Numbers) designates organizations to manage each TLDare
33. What is Naare servers?
    Name servers translate the domain name into an IP address, connecting information that's easy for humans to understand with information that's easy for computers to understand

34. Canonical Name
    A canonical name (CNAME) is a type of Domain Name System (DNS) database record that indicates that a domain name is a nickname or alias for another domain name. Also referred to as the "true name," the CNAME is especially important when multiple services run from a single IP address

35. What details did you dididiandnd when you searched IP/Domain for DNS Lookup?
    A, AAAA, SOA, Name server etc.

36. What is DHCP?
    The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using clients-serverrver architecture.
    DORA is the main concept behind the working of DHCP

37. What is CVE? Which authority generate CVE?
    CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. CVEs are assigned by a CVE Numbering Authority (CNA).

38. What is the loopback address?
    The IP address is 127.0. 0.1 is called a loopback address. Packets sent to this address never reach the network but are looped through the network interface card only. This can be used for diagnostic purposes to verify that the internal path through the TCP/IP protocols is working.

39. Difference between thread & process?

A process is a program under execution i.e an active program. A thread is a lightweight process that can be managed independently by a scheduler. Processes require more time for context switching as they are heavier. Threads require less time for context switching as they are lighter than processes.

40. Difference between thread & services?
    Service: is a component of android which perform the ms long-ruoperationsration in the backmost without having UI. Thread is aanO.S level feat that allowswsw you to do some operations in the background

41. What is Kerberos?
    Kerberos is a computernetworkkk authentication protocol that works based on tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

42. What is 0x18 andarex12 in Kerberos authentication?
    0x12Clients' credentials have been revoked. Account didisabledexpired, locked out, logon hours
    The failure code 0x18 means that the account was already disabled or locked out when the client attempted to authenticate

43. What is kernel?
    The kernel is the essential centre of a computer operating system (OS). It is the core that provides basic services for all other parts of the OS. It is the main layer between the OS and hardware, and it helps with process and memory management, file systems, device control and networking.

44. LDAP use & Port number
    LDAP is a tool for extracting and editing data stored in Active Directory and other compatible directory service providers. Each user account in an AD has several attributes, such as the user's full name and email address. Extracting this information in a usable format requires LDAP. Port 389

45. What are salted hashes?
    Password hash salting is when random data – a salt – is used as an additional input to a hash function that hashes a password. The goal of salting is to defend against dictionary attacks or attacks against hashed passwords using a rainbow table.

46. What is a brute force attack? How you will mitigate it?
    It tries various combinations of usernames and passwords repeatedly until it gets in. This repetitive action is like an army attacking a fort.

Mitigation: Limit the login attempts, enable 2FA, use captchas to block malicious IP etc.

47. What is encoding, hashing and encryption?

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

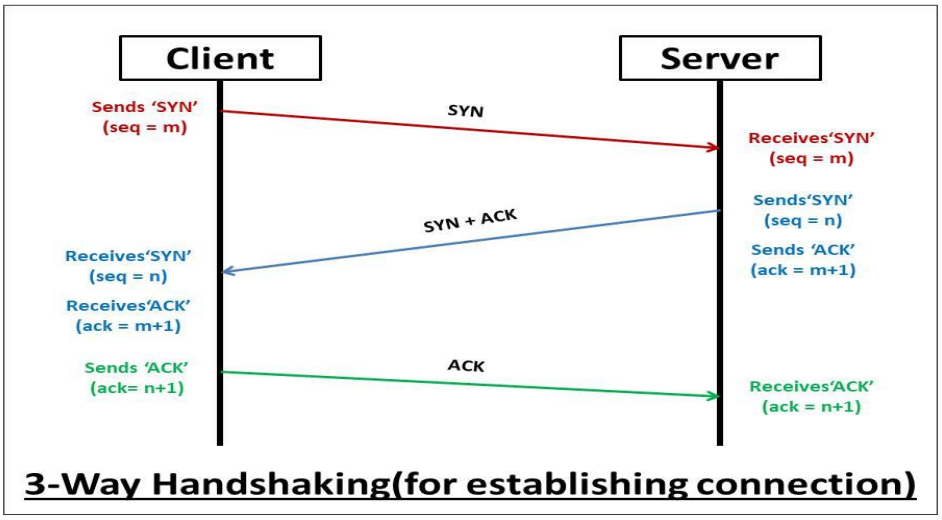
Hashing: Maintains the integrity of a message or data. Any change did any day could be noticed.

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

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

- SYdo N
- URG
- ACK
- PSHRSS
- RST
- FIN

49. What is 3-way/TCP handshaking?



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

VPN is related to remote access to a network with a secured and encrypted tunnel. Saves the data fra om pryineyesye 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.

51. Difference between proxy and VPN?
    A VPN secures all your network traffic, while a proxy works on an application level. They both hide your IP address, but only a VPN redirects your internet data through an encrypted tunnel. A proxy is suitable for browsing the internet, but it's not as safe and secure as a VPN.

52. Difference between reverse proxy and forward proxy?
    The main difference between the two is that forward proxy is used by the client such as a web browser whereas reverse proxy is used by the server such as a web server.

53. SSL vs TLS? How do the es the workforce? Which one is better?

    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 ciphecypheres-Algorithmic toolkits for creating an encrypted connection that it knows how to use. The client compares this against its list of supported ciphcyphertes, 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.

TLS is better than SSL

54. Difference betwevirusesrus, Wovirusesnd Trojan Malware

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 operatsimilarlyon. 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.

55. What is the chain of custody y?
For legal cases the data/device (evidence) needs to be integrated, hence any access needs to be documented – who, what when, and why. Compromise in this process can cause legal issues for the parties involved.

OSI Model Layer Questions:

56. What is OSI Model Layer?
It is Open System Interconnection is a reference model for how applications communicate over a network.

57. Can you tell OSlayer'srsnamese and at least 1 protocol for each layer?

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

58. Do you know the attack on every OSI layer? If yes then what vulnerabilities/attacks were found on which layer. Elaborate layer wise with its attack?
    Application Layer: HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks.

    Presentation Layer: SSL hijacking, encryption downgrade attacks, decryption attacks, encoding attacks
    Session Layer: Session hijacking attack, Man-in-the-Middle (MITM), Blind attack, Man-in-the-browser, SSH Sniffing

    Transport Layer: TCP Sequence prediction, SYN flood attack, TCP Session hijacking, UDP flood attack, UDP-based amplification attacks

    Network Layer: IP Spoofing and jamming, ICMP attack, Smurf attack, Worm-hole, Blackhole attacks, Sybil attack, Packet sniffing, and selective forwarding attacks.

    Data Link Layer: ARP Spoofing, MAC cloning, DoS, Spanning tree attack, VLAN hopping, DHCP attacks

    Physical Layer: Unauthorised access, data sniffing, physical damage

59. On which layer does HTTP protocol work?
    Application Layer

60. What is MITM? How can you prevent Man-in-the-middle-attack?

    MITM attack happens when a communication between two parties is intruded on 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

61. What is sniffing? Do you have ou any tool for sniffing?
    A sniffer attack corresponds to the theft or interception of data by capturing the network traffic using a sniffer. When data is transmitted across the network, the data within the network packet can be read using a sniffer such as Wireshark if the data is not encrypted.

    Ransomware & Server Questions:
62. On which port mainly wannacry ransomware attacks?
    445 (SMB) & Netbios (137, 138, 139)

63. How you can prevent your organization from ransomware attacks?
    By using 2 techniques: Network segregation and Network segmentation

    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.

    MITRE Attack & Cyber Kill Chain Questions:

64. What is MITRE ATT&CK?
    MITRE ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behaviour, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target

65. What is TTP?

Tactics, Techniques, and Procedures (TTP) are behaviours, methods, or patterns of activity used by a threat actor or group of threat actors.

66. Can you explain tactics and technique?
    Tactics are movements with difficulty stratagem cand running action to achisomethinghing. A manoeuvre was used against the enemy. The army trains tactics aagainnsnotnemy. The technique I skill and knowledge of a given art or occupation.

67. Which one you will prefer more TTP or IOC and why?
    Both are preferable but TTP can be more preferable as IOC is static whereas through TTP we can get that type of attack and more indicators.

68. Have you remembered all tactics of the mitre attack?
    Yes 14 tactics (Mention all tactics)

69. Whatdefenceense evasion, name some techniques for it?
    The adversary is trying to avoid being detected. Defence Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defence evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts

70. What is persistence in Mitre? Can you name some paths where they train to have their foothold?
    The adversary is trying to maintain its foothold.
    Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. It can be found in the registry, startup folder etc.

71. Can you recognize some Persistence techniques?
    BootLoginogon Auto start Execution etc.

72. What is lateral movement?
    The adversary is trying to move through your environment.
    Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

73. What is the difference between cyber kill chain & Mitre ATT&CK?
    ATT&CK Tactics are unordered and may not all occur in a single intrusion because adversary tactical goals change throughout an operation, whereas the Cyber Kill Chain uses ordered phases to describe high-level adversary objectives.

74. Can you explain all steps of cyber kithe ll chain?
    RECONNAISSANCE. Harvesting email addresses, conference information, etc.
    WEAPONIZATION.
    DELIVERY.
    EXPLOITATION.
    INSTALLATION. ...
    COMMAND AND CONTROL
    Actions on Objectives.

75. Can you please elaborate on ate worked incident/case in the form of cyber kill chain? For example, if you worked on an alert/phish which was related to malware you can relate that malware in the form cyber kill chain step by step with its 7 stages.

Scenario-Based Questions:

76. What you will do to stop the DDOS attack?
    Document your DDoS resiliency plan
    Recognize DDoS attack activity.
    Don’t assume that only large-scale, volumetric attacks are the problem
    Don’t rely on traffic monitoring or thresholds
    Don’t rely on an IPS or firewall
    Engage with a mitigation provider
    Pair time-to-mitigation with successful attack protection

    Apart from that, you can make a scrubbing centre to mitigate the DDOS attack.
    A scrubbing server is a dedicated machine that receives all network traffic destined for an IP address and attempts to filter good traffic from bad. Ideally, the scrubbing server will only forward non-DDoS packets to the Internet application being attacked

77. Suppose a Server is compromised with malware? 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.

78. Suppose there is no usecasuse caseittorrent, then how you will analyze the traffic of bit torrent?
    An analyst can get to know with firewall, SIEM logs & can filter on port 6881. Bit torrent usually works on ports 6881-6889.
    In addition, the domain can be seen in the payload, which can also a sign for it.

79. Data Breach on the network- What is the first thing you do when an attack occurs on the network? what is 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, a successful email phishing attack, outdated antivirus software, or an employee that unknowingly divulged confidential data?
    - Isolate the affected 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.

80. How do you keep company devices secure if they're on public/hotel wifi?
    Aware of the user that does connect with their mobile hotspot.
    If in case not possible then the user should use VPN for secure communication.

    Roles & Responsibilities, SIEM Questions:
81. What is SIEM?
    Security information and event management is a field within the field of computer security, where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.

82. Which SIEM you were using in your organization? What were the sources from where SIEMcollectedg the logs were?
    Here the Interviewer is asking from where the SIEM is collecting the logs. It contains your NIDS, HIDS, Server, routers, Virtual machines etc. For this question you should aware of your organization's architecture.

83. What is Qradar/Splunk?
    Both are SIEM

84. What is the architecture of Qradar/Splunk (whatever SIEM on which you worked)?
    You should know the architecture of you SIEM on which you are working.
    Here is the link for Qradar and Splunk architecture:
    Please take the link from the video or search on Google directly

85. What are the components of Qradar/Splunk?
    Please take the link from the video or search on Google directly

86. Brief us about your career.
    Starting with your academics will give a good impression. Explain the learning and positive things which you learn in your career.

87. Please explain your roles and responsibilities at your previous organization.
    Through this question, they want to see what you have done in your organization. If you have done something good apart from roles and responsibilities you can also mention it.

88. Have you handled any big Incident/Phishing email/case in your career? Brief it systematically.
    For example, A candidate handled a remote malware campaign so he will explain each and everything that how he detected, investigated and how he mitigated.

89. Explain this incident in the form of a cyber kill chain.
    Already discussed in the cyber kill chain video

90. What are the stages of the Incident management process?
    - Incident Identification, Logging, and Categorization
    - Incident Notification & Escalation
    - Investigation and Diagnosis
    - Resolution and Recovery
    - Incident Closure

91. How do you handle any alerts? Please explain the process.
    They are talking about incidents or any ticket which you handled in your organization. Explain the process here

92. What is the event code for success and failure logins?
    4624 & 4625. They can ask for more event codes which are important.
93. Which certification you have done? The interviewer can ask many questions based on your certification.
    Name the certification, which you have done. Brush up your certification course once they can ask a question related to that course.
94. What is NMAP?
    Nmap stands for Network Mapper and is used to scan a system and understand what weaknesses exist that a hacker could potentially exploit. As the program is open-source and free, it is one of the more common tools used for scanning networks for open ports and other weaknesses.

95. What is the difference between IOC & IOA?
    IOCs are Static but IOAs are Dynamic
    Indicators of attack (IOA) focus on detecting the intent of what an attacker is trying to accomplish, regardless of the malware or exploit used in an attack. Just like AV signatures, an IOC-based detection approach cannot detect the increasing threats from malware-free intrusions and zero-day exploits

96. What is spear phishing?
    Spear phishing is the act of extracting sensitive information or money from a specific target using personalized, authentic-looking emails. Spear phishing is defined as a form of phishing wherein attackers research specific targets and uses the acquired information to forge authentic-looking emails.

97. How you will do the analyses of a phishing email?
    Take this free course to learn about the Phishing email investigation.
    Free course: Ultimate way to analyse phishing email

98. What is Header analysis?
    Free course: Ultimate way to analyse phishing email

99. Can you name some port numbers?
    They are asking about important port numbers such as22, 25, 137, 445, 80, 443, 389 etc. you should know the important port number on which you are working daily.

100. What is DLP?

Data lose prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use, in motion, and at rest. The terms "data loss" and "data leak" are related and are often used interchangeably

101. What is DMARC, SPF & DKIM?

DMARC: Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol.

SPF: Sender Policy Framework (SPF) is an authentication protocol that lists IP addresses in a DNS TXT record that are authorized to send an email on behalf of domains.

DKIM: DKIM (Domain Keys Identified Mail) is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain. This is done by giving the email a digital signature

Free course: Ultimate way to analyse phishing email

102. How you will decide on which alert you have to work on first if there are 100 alerts in the queue?

Based on priority and severity i.e. critical, high, medium and then low
First, we will work on critical severity/priority

103. Why do you want to leave your company?

You can think of your answer
I have learned a lot of things in my previous organization and explored as much as I can. Now I feel that I should move to a challenging and a new responsibility so that I can grow more.

104. What motivated you to come to this organization?

Learning, challenges and new responsibility

105. Do you have any questions for us?

If you have any good questions, you can ask. However, I recommend do not ask any questions just say thank you if you are not sure that your question will be good for you and give a good impression to the interviewer.