Cybersecurity Questions:

1. **What is the difference between Vulnerability Assessment and Penetration Testing?**
   Vulnerability Assessment identifies potential security weaknesses, while Penetration Testing exploits those vulnerabilities to determine the level of risk.

2. **What are the key steps of a penetration test?**
   Answer: Planning and reconnaissance, scanning, gaining access, maintaining access, and analysis/reporting.

3. **What tools do you use for VAPT?**
   Answer: Burp Suite, Nmap, OWASP ZAP, Nessus, Nikto, SQLmap, Metasploit, Qualys, and custom scripts.

4. **What is SIEM and why is it important?**
   Answer: SIEM (Security Information and Event Management) helps collect, monitor, and analyze log data to detect and respond to security incidents.

5. **Explain Firewall and IDS/IPS difference.**
   Answer: Firewalls filter traffic based on rules; IDS/IPS detect and block malicious network activities based on signatures or behavior.

6. **What are the common web application vulnerabilities?**
   Answer: SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Broken Authentication, and Sensitive Data Exposure.

7. **What steps would you take if you detect a cyberattack in the bank's system?**
   Answer: Isolate affected systems, collect evidence, identify the attack vector, mitigate, report to management, and implement post-incident improvements.

8. **What is your experience with SIEM tools?**
   Answer: I have practiced using tools like Splunk and Graylog to monitor, correlate, and investigate alerts from network and endpoint logs.

9. **What is the purpose of log monitoring in banks?**
   Answer: To detect suspicious activities, identify insider threats, and meet regulatory compliance (e.g., ISO 27001, PCI DSS).

10. **How would you secure a banking web application?**
    Answer: Use input validation, encryption (TLS/SSL), authentication control, patch management, and regular security assessments.

11. **What is network segmentation and why is it important?**
    Answer: It divides a network into zones to limit access, reduce breach impact, and improve security monitoring.

12. **What are DLP solutions and how do they work?**
    Answer: Data Loss Prevention (DLP) tools detect and prevent unauthorized data transfer outside the organization.

13. **What is phishing and how can banks prevent it?**
    Answer: A social engineering attack to steal sensitive data. Banks prevent it using awareness training, email filters, and domain monitoring.

14. **How would you respond to a ransomware incident in the bank?**
    Answer: Disconnect infected systems, identify the ransomware type, restore from backups, notify management, and strengthen security policies.

15. **What is Cybersecurity, and why is it important?**
    Answer**:** The critical importance of cybersecurity is mainly to protect computer systems, networks, and programs from cyber-attacks whose aim is access, alter, or destroy sensitive user data. In this case, it also helps in ensuring confidentiality of information, as well as preventing privacy breaches or financial losses.

16. **Define the terms virus, malware, and ransomware.**
    Answer: By infecting files and programs on computers, the virus moves across the internet. Among other things, malware is designed to harm computer systems, networks, and servers. The program named ransomware encrypts user files and asks for money to give out decryption keys."

17. **How can a firewall protect a network?**

    Answer: A network firewall safeguard data traffic entering and leaving a system according to specified security rules. It acts as a barrier between safe and unsafe sections of a network. Without it, the way a network operates would change and its security lessened compared to if there were no wall at all. Its main task is monitoring ongoing activities to prevent malicious entities from accessing the system. There are threats lurking around which make a firewall necessary as it protects against them.

18. **What is social engineering? Give an example.**

    Answer: Tricking people into giving away personal sensitive information is what it's all about. For example, one could impersonate the CEO and call or email a staff member to request that they provide information regarding company portal passwords.

19. **How can you prevent a Man-In-The-Middle attack?**

    Answer: To prevent MitM Attacks, the simple measures can be taken:

    - Encrypting the communication using proper encryption
    - Voice communication through secured channels
    - Verification of authenticity of digital signature
    - Implementing 2FA before login
    - Deploying VPNs
    - Keeping systems updated and well patched.

24. 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.

25. 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 always remain available preventing service disruptions due to power outages, hardware failures or system upgrades.

26. 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.

27. 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.

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

Risk is any potential loss of, damage, or destruction of an asset because 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.

29 . 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 do 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 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

30. 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)

31. **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

32. **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 organization is unable to prove that employees reviewed and understood the content of the policy.

33. **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

34. **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.

35. **What is a DDOS attack and how is it mitigated?**

DDOS (Distributed Denial of Service) is when a network is flooded with many 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.

36. **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.

To avoid such attacks-password best practices should be followed, mainly on critical resources like servers, routers.

37. **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.

38. 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.

39. 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.

41. 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.

42. **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".

43. **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

44. 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.

45. 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.

48. 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

49. 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.

50. 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.

56. 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.

57. 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.

58. 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.

59. 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.

61. What is DHCP?

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

62. 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 workstations 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.

63. 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.

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

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

65. What is a three-way handshake?

A method in TCP/IP networks to establish a connection between client and server in three steps:

(a) Client sends SYN packet to server.
(b) Server responds with SYN-ACK.
(c) Client replies with ACK, completing the connection.

66. What is Cryptography?

Cryptography is the practice and study of techniques for securing information and communication mainly to protect the data from third parties that the data is not intended for.

67. What is the difference between Symmetric and Asymmetric encryption?

Symmetric Encryption	Asymmetric Encryption
Same key for encryption & decryption.	Different keys for encryption & decryption
Encryption is fast but more vulnerable.	Encryption is slow due to high computation
DES, 3DES, AES, RC4	Diffie-Hellman, RSA
Used for bulk data transmission	Often used for securely exchanging secret keys

68. What is the difference between IDS and IPS?

IDS (Intrusion Detection System) only detect intrusions; the administrator must prevent them. IPS (Intrusion Prevention System) detects intrusions **and** takes actions to prevent them.

69. Explain CIA triad.

CIA stands for Confidentiality, Integrity, and Availability, a model to guide information security policies.

- **Confidentiality:** Data is accessible only to authorized personnel. Encryption protects against unauthorized access.
- **Integrity:** Ensures data is not modified or corrupted by unauthorized entities. Failed changes by authorized entities should be reversible.
- **Availability:** Data must be accessible whenever required. Hardware maintenance, upgrades, backups, and network management ensure availability.

70. How is Encryption different from Hashing?

- **Encryption:** Converts readable data to unreadable format; can be decrypted back to original data.
- **Hashing:** Converts data to a fixed-size hash; cannot be reversed.

71. What is a Firewall and why is it used?

A firewall is a network security system that monitors and controls incoming and outgoing traffic. It protects against viruses, malware, unauthorized access, and can filter content.

72. What is the difference between VA (Vulnerability Assessment) and PT (Penetration Testing)?

- **Vulnerability Assessment:** Identifies and prioritizes system flaws; organization is aware of weaknesses.
- **Penetration Testing:** Tests security measures by simulating attacks to find unknown vulnerabilities

73. What is a three-way handshake?

A method in TCP/IP networks to establish a connection between client and server in three steps:

a. Client sends SYN packet to server.
b. Server responds with SYN-ACK.
c. Client replies with ACK, completing the connection.

74. **What are the response codes received from a Web Application?**

- 1xx – Informational
- 2xx – Success
- 3xx – Redirection
- 4xx – Client-side error
- 5xx – Server-side error

75. What is traceroute? Why is it used?

Traceroute lists the path of a packet through routers. It helps identify where a connection fails.

76. Difference between HIDS and NIDS**:**

- **HIDS (Host IDS):** Monitors traffic on a particular host.
- **NIDS (Network IDS):** Monitors traffic across the entire network.

77. Steps to set up a firewall:

1. Change default username/password.
2. Disable remote administration.
3. Configure port forwarding for specific applications.
4. Disable DHCP if conflicting.
5. Enable logging.
6. Configure firewall policies.

78. Explain SSL Encryption:

SSL (Secure Sockets Layer) encrypts communication between a web server and browser. Steps:

a. Browser requests SSL connection.
b. Browser sends SSL certificate.
c. Certificate verification.
d. Server acknowledges.
e. Encrypted communication begins.

79. Steps to secure a server:

a. Secure root/admin passwords.
b. Create separate system users.
c. Remove remote access from default accounts.
d. Configure firewall rules.

80. Explain Data Leakage:

Data Leakage occurs when sensitive data is transmitted to unauthorized entities, intentionally or accidentally. Prevention uses DLP (Data Leakage Prevention) tools.

82. What is a Brute Force Attack? How to prevent it?

- Automated attempts to guess credentials.

Prevention: Strong and complex passwords, minimum length, limit login attempts.

83. What is Port Scanning?

Detects open ports and services on hosts; used by hackers and administrators. Techniques include Ping Scan, TCP Connect, TCP Half-Open, UDP, Stealth Scanning.

85. What is VPN?

Virtual Private Network creates a secure and encrypted connection between client and server.

86. Patch management frequency:

Apply patches immediately; not later than one month for Windows or network devices.

88. MITM Attack & prevention:

Man-in-the-Middle attack intercepts communication.

Prevention: VPN, strong encryption, HTTPS, Intrusion Detection, public-key authentication.

89. DDoS Attack & prevention:

Distributed attack flooding servers or exploiting bugs.

Prevention: Anti-DDoS, firewalls, load balancing, front-end hardware.

90. XSS Attack & prevention:

Injects malicious scripts into web pages.

Prevention: Input validation, sanitization, encoding, anti-XSS tools.

90. What is ARP?

Maps IP addresses to MAC addresses in a local network. Uses ARP cache or broadcasts to locate addresses.

91. Protocols under TCP/IP Internet Layer:

Layer	*Protocol Examples*
Application	NFS, DNS, FTP, Telnet, etc.
Transport	TCP, UDP
Internet	IP, ARP, ICMP
Data Link	PPP, IEEE 802.2
Physical	Ethernet, Token Ring, RS-232

92. What is a Botnet?

Network of devices with malware/bots used for spam, data theft, DDoS.

93. What are salted hashes?

Random salt added to hashed passwords to prevent dictionary attacks.

94. SSL vs TLS:

SSL – verifies sender identity.

TLS – stronger, additional data protection. Often used together.

95. What's the difference between a threat, a vulnerability, and a risk?

These three terms form the foundation of every risk assessment, incident report, and triage decision you'll make as an analyst.

- **Threat:** Anything that could cause harm to your systems, data, or operations. Examples include a malicious actor, ransomware, or even non-human events like a power outage.
- **Vulnerability:** A weakness that a threat can exploit, such as unpatched software, open ports, overly permissive IAM roles, or poor password hygiene.
- **Risk:** The potential for loss or damage when a threat successfully exploits a vulnerability. Risk represents the intersection of likelihood and impact and what teams are constantly trying to identify, reduce, or accept.

Example: If a phishing email targets your organization (threat), and someone reuses a weak password (vulnerability), there's a real risk of account compromise and lateral movement.

96. What are the most common types of cyber-attacks?

- **Phishing:** Tricks users into revealing sensitive information through fake emails or login pages. Targets people rather than systems.
- **Malware:** Malicious software like ransomware, viruses, or spyware that steals data, damages systems, or gives attackers remote access.
- **Man-in-the-middle (MITM) attacks:** Intercept communication between two parties, often to steal data in transit.
- **Denial-of-service (DoS) attacks:** Overwhelm a system with traffic, causing downtime without necessarily stealing data.
- **SQL injection:** Inserts malicious code into input fields to access or tamper with backend databases.
- **Password attacks:** Steal or guess user credentials through brute force, dumps, or reused passwords.
- **Zero-day exploits:** Exploit software bugs that have no patches yet. Hard to detect and very dangerous.

97. How does a firewall work?

A firewall acts like a security guard between your internal network and the outside world. It monitors traffic and blocks anything that doesn't follow defined rules.

- **Network firewalls:** Protect the entire network.
- **Host-based firewalls:** Protect individual machines.

Firewalls can be:

- **Stateless:** Treat each packet independently.
- **Stateful:** Track active connections to make more informed decisions.

98. What is the CIA triad, and why is it important?

The **CIA triad** stands for **Confidentiality, Integrity, and Availability**, forming the foundation of cybersecurity decisions.

- **Confidentiality:** Ensures data is private. Tools: encryption, role-based access, physical security.
- **Integrity:** Ensures data isn't altered or tampered with. Tools: cryptographic hashes, digital signatures, file integrity monitoring.
- **Availability:** Ensures systems and data are accessible when needed. Tools: backups, load balancing, DDoS mitigation.

Example: Encrypting all data improves confidentiality but may reduce availability. Balancing tradeoffs is key.

99. What's the difference between symmetric and asymmetric encryption?

- **Symmetric encryption:** Uses the same key for encryption and decryption. Fast and efficient for large data but key distribution is a challenge.
- **Asymmetric encryption:** Uses a public key to encrypt and a private key to decrypt. Slower but essential for secure communications like HTTPS and digital signatures.

Example: HTTPS uses asymmetric encryption to exchange a session key, then symmetric encryption for the rest of the session.

100. What is multi-factor authentication (MFA) and why is it important?

MFA requires more than one form of authentication:

- Something you **know** (password/PIN)
- Something you **have** (phone, token)
- Something you **are** (fingerprint, face scan)

Example: Password + face recognition + push notification approval drastically reduces account compromise risk.

101. What's the difference between a virus, a worm, and a Trojan horse?

- **Virus:** Malicious code that attaches to files; requires user action to execute.
- **Worm:** Self-replicates through networks without user action.
- **Trojan horse:** Disguised as legitimate software; contains hidden malicious code.

102. What's a SIEM, and how do analysts use it?

SIEM (Security Information and Event Management) collects, analyzes, and correlates security data.

- **Log aggregation:** Stores logs for historical analysis.
- **Real-time monitoring:** Detects anomalies and alerts analysts.

Popular SIEMs: Splunk, IBM QRadar, LogRhythm, Microsoft Sentinel, Wazuh.

103. How would you respond to a phishing email incident?

Steps:

1. Preserve evidence (headers, links, attachments).
2. Assess impact (check for malware or suspicious processes).
3. Isolate affected device.
4. Remove threat, clean systems, reset credentials.
5. Report and communicate findings.

104. What's the difference between IDS and IPS?

- **IDS (Intrusion Detection System):** Passive; alerts but doesn't block.
- **IPS (Intrusion Prevention System):** Active; blocks malicious traffic.

Detection methods:

- **Signature-based:** Known patterns.
- **Anomaly-based:** Deviations from normal behavior.

105. Can you walk me through how SSL/TLS works?

- **Handshake:** Client and server negotiate protocol version, algorithms, and exchange certificates.
- **Certificate validation:** Confirms server identity.
- **Key exchange:** Establish shared session key via asymmetric encryption.
- **Secure communication:** Encrypts all data with symmetric encryption.

106. How do you stay current with security news and emerging threats?

- **News sources:** Krebs on Security, The Hacker News, Dark Reading.
- **Threat intelligence feeds:** AlienVault OTX, Recorded Future, CISA advisories.
- **Podcasts/YouTube:** Malicious Life, CyberWire Daily, John Hammond.
- **Social media:** Twitter/X, LinkedIn for real-time alerts.
- **Hands-on labs:** TryHackMe, Hack The Box, Immersive Labs.

107. What's the difference between encoding, encryption, and hashing?

- **Encoding:** Transform data for safe transmission. Reversible, not secure. Example: Base64.
- **Encryption:** Protects data confidentiality. Reversible with a key.
- **Hashing:** Verifies data integrity. One-way, irreversible. Example: SHA-256.

108. What steps would you take if you saw unusual outbound traffic from a user's machine?

Steps:

1. Validate the alert.
2. Correlate with other logs.
3. Check for known threats.
4. Isolate the host if needed.
5. Investigate root cause.
6. Remediate and monitor.

109. How would you perform a root cause analysis after a security incident?

Steps:

1. Confirm the timeline.
2. Trace initial access point.
3. Map the attack path.
4. Identify failures (root cause).
5. Document findings.
6. Recommend corrective actions.

110. Describe a threat-hunting approach you would use in a large network

Steps:

1. Form a hypothesis using threat intel.
2. Identify relevant data sources.
3. Hunt for attacker patterns (e.g., unusual RDP sessions).
4. Sort and analyze data.
5. Investigate anomalies.
6. Document findings and improve detection.

111. What steps would you take to reduce false positives in IDS alerts?

Steps:

i. Prioritize noisy rules.
ii. Understand traffic/business context.
iii. Tune rules (exceptions, specificity, thresholds).
iv. Layer in contextual detection.
v. Test, monitor, and iterate.
vi. Document all changes.

112. How would you secure an AWS-hosted web app from common vulnerabilities?

Steps:

1. **Application security:** Input validation, modern auth, password hashing, HTTPS, rate limiting.
2. **AWS services:** WAF, Shield, CloudFront, Secrets Manager.
3. **Storage:** Restrict S3 access, enable encryption, enable logging.
4. **EC2/Lambda hardening:** Patching, least privilege, secure network rules.
5. **IAM:** Avoid wildcards, enable MFA, audit policies.
6. **Monitoring:** CloudTrail, GuardDuty, CloudWatch alerts.

112. What's your approach to creating a layered security strategy?

Principles:

- Understand assets and priorities.
- Build layers across network, endpoint, application, data, identity, monitoring, and response.
- Apply least privilege everywhere.
- Assume breach; focus on detection and containment.
- Regularly test and validate.
- Balance usability and maintainability.

113. Difference Between HIDS and NIDS

Parameter	HIDS	NIDS
Usage	Monitors host for intrusions	Monitors entire network traffic
Monitoring	Specific device activities	All network devices
Installation	On each host	On network nodes
Performance	Slower, per host	Can monitor multiple hosts

114. What types of information can be used for authentication?

- Type 1 – *Something You Know* – includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.
- Type 2 – *Something You Have* – includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.).
- Type 3 – *Something You Are* – includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

115. Why is DNS monitoring important?

- DNS plays an important role in connecting end users to the internet. Each connection made to a domain by the client devices is recorded in the DNS logs. Inspecting DNS traffic between client devices and your local resolver could reveal information for forensic analysis as well as discovering malicious activity/connections on your network such as:
    botnets
    DDOS attack detections
    malicious domains
    dynamic domains

116. What is an IT security audit?

- At its root, an IT security audit includes two different assessments. The manual assessment occurs when an internal or external IT security auditor interviews employees, reviews access controls, analyzes physical access to hardware, and performs vulnerability scans. These reviews should occur, at a minimum, annually. Some organizations, however, prefer to do them more frequently.
- While some apply broadly to the IT industry, many are more sector-specific, pertaining directly, for instance, to healthcare or financial institutions. Below is a short list of some of the most-discussed IT security standards in existence today.
    ISO Compliance: The International Organization for Standardization (ISO) develops and publishes an array of guidelines designed to ensure quality, reliability, and safety. The ISO/IEC 27000 family of standards are some of the most relevant to system administrators, as these standards focus on keeping information assets secure. The ISO/IEC 27001 is known for its information security management system requirements.
    HIPAA Security Rule: The HIPAA Security Rule outlines specific guidelines pertaining to exactly how organizations should protect patients' electronic personal health information.
    PCI DSS Compliance: The PCI DSS compliance standard applies directly to companies dealing with any sort of customer payment. Think of this standard as the requirement responsible for making sure your credit card information is protected every time you conduct a transaction.

SOX Compliance: The SOX Act, known more formally as the Sarbanes-Oxley Act after its sponsors Senator Paul Sarbanes (D-MD) and Representative Michael G. Oxley (R-OOH-4), was passed in 2002 following the highly publicized Enron scandal. The goal was to protect investors by requiring all public companies to provide accurate, reliable financial disclosures on an annual basis.

117. What is incident management?

- IT incident management is an area of IT service management (ITSM) wherein the IT team returns a service to normal as quickly as possible after a disruption, in a way that aims to create as little negative impact on the business as possible.
- Security incident management focuses heavily on resolving incidents quickly to ensure that employees and users alike aren't hit with too much downtime. By identifying, managing, recording and analyzing security threats or incidents in real-time, security incident management provides a robust and comprehensive view of any security issues within an IT infrastructure.

118. What is the difference between logical and physical security? Can you give an example of both?

- Protecting the people involves a combination of physical and logical security. Physical security keeps them safe by allowing only authorized individuals into the building. Logical security protects their computers and data from unauthorized access.
- Logical security protects computer software by discouraging user access by implementing user identifications, passwords, authentication,and biometrics. Physical security prevents and discourages attackers from entering a building by installing fences, alarms, cameras, security guards, electronic access control, intrusion detection and administration access controls. The difference between logical security and physical security is logical security protects access to computer systems and physical security protects the site and everything located within the site.

119. Can you explain the difference between a packet filtering firewall and a application layer firewall?

- Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.
- In computing, a stateful firewall (any firewall that performs stateful packet inspection (SPI) or stateful inspection) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it.
- A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.

120. Can you explain how you would approach a security incident?

When it comes to approaching a security incident, my priority is to quickly contain the threat to prevent any further damage. This involves identifying the source of the breach and isolating the affected systems or data.

Once the threat has been contained, I move on to investigating the incident to determine the extent of the damage and collect any evidence that can help prevent similar incidents in the future. This includes analyzing system logs, reviewing security policies and protocols, and working with any other relevant teams.

During this process, I document everything thoroughly to ensure that all parties involved have a clear understanding of what occurred and how it was handled. This documentation can also prove useful in the event of any legal or compliance issues that may arise.

After the investigation is complete, I use the information gathered to implement any necessary improvements or updates to our security protocols. This may involve updating software and hardware or providing additional training for employees to prevent similar incidents from occurring in the future.

To give you an example, in a previous role I was the lead on a team that responded to a ransomware attack. Our first step was to disconnect the affected devices to prevent the malware from spreading. We then performed a full analysis of our network logs to determine the scope of the attack and identify any other potential vulnerabilities. Based on this analysis, we made improvements to our software security policies and provided additional training to our employees to prevent similar attacks in the future. As a result of our swift response and thorough investigation, we were able to prevent any further damage and ensure that our systems were secured going forward.

121. How would you handle a security breach that involves personal data or sensitive company information?

Handling a security breach involving personal data or sensitive company information is a critical concern for any organization. In the event of a breach, I would follow a predefined incident response plan to ensure an efficient and timely response. This plan should include the following steps:

(a) **Containment:** Identify the affected systems and isolate them from the rest of the network to prevent further damage.
(b) **Evaluation:** Evaluate the scope and impact of the breach, including the type of data compromised, and the potential harm caused to individuals or the organization.
(c) **Notification:** Notify the appropriate authorities and stakeholders about the incident, including the IT team, legal department, and affected individuals. Compliance with GDPR and other regulations is an essential part of this process.
(d) **Investigation:** Conduct a detailed investigation to determine the root cause of the breach, understanding whether it's an internal or external threat.
(e) **Remediation:** Implement corrective actions to address the root cause of the issue and prevent future occurrences. This might include patching systems, revising policies, and updating employee training.
(f) **Monitoring:** Continuously monitor the systems for any further suspicious activity to prevent future attacks. As part of this phase, we can use intrusion detection systems and other specialized tools dedicated for this purpose.

122. How do you ensure data integrity and confidentiality?

As a Cyber Security Engineer, ensuring data integrity and confidentiality is top priority. To guarantee integrity, I use cryptographic algorithms such as SHA-2 and SHA-3 to generate hashes for data validation. In addition, I make use of digital signatures for non-repudiation purposes.

When it comes to data confidentiality, I use encryption techniques. I implement symmetric encryption methods such as AES and Twofish for secure communication over insecure channels. Furthermore, I utilize asymmetric encryption methods such as RSA and Elliptic Curve Cryptography (ECC) for secure key exchange and message authentication.

One example of my successful implementation of data integrity and confidentiality was in my previous job as a Security Engineer at XYZ Corp. I performed a security audit and found that the company's financial data was being transmitted over an unsecured network. I immediately implemented AES encryption and SHA-2 hashing to ensure data confidentiality and integrity. As a result, the company received an A+ rating in their next security audit.

123. List and explain the different types of cybersecurity.

a. Network security. This security type protects a computer network against intruders, unauthorized access, disruption, attacks, and misuse of hardware and software. Network security helps protect the organization’s assets from external and internal threats like. Example: firewalls.
b. Application security. Application security involves safeguarding devices and software against malicious attacks. This is accomplished by regularly updating the apps to ensure they are secure and safe against threats.

c. Data security. It entails establishing a solid data storage system that delivers data integrity and privacy when the data is in storage or in transit.

d. Management. Identity management involves identifying each individual's level of access within the organization. For example, restricting data access to data as dictated by the individual's job role.

e. Operational security. It entails analyzing and deciding how to handle and secure data assets. For example, storing data in an encrypted form within the database.

f. Mobile security. It protects organizational and personal data stored on mobile devices like cell phones, PCs, tablets, and similar devices against hostile attacks. These dangers include unauthorized access, device loss or theft, malware, and other threats.

g. Cloud security. It refers to safeguarding data stored in a digital environment or cloud infrastructures. Cloud security employs a variety of cloud service platforms, such as AWS, Azure, Google, and others, to assure protection against various threats.

Part-C: Critical and Logical Cybersecurity Questions with Detailed Answers

1. **Unusual outbound traffic to unknown IP overseas:** Investigate by checking server and firewall logs for abnormal activity, analyzing traffic patterns over time, performing IP reputation checks to see if the IP is blacklisted, isolating the affected server from the network, and conducting a thorough malware scan. Document findings and apply patches or block suspicious traffic.

2. **Vulnerability prioritization (high probability, low impact vs. low probability, high impact):** Evaluate vulnerabilities based on both probability of exploitation and potential impact. Even low probability vulnerabilities should be prioritized if their impact could cause catastrophic damage, such as data loss or system shutdown. Consider business risk tolerance and regulatory requirements in decision-making.

3. **Network slowdown with failed logins and DNS spikes:** Likely caused by brute force attacks or DDoS activity. Steps include monitoring traffic with IDS/IPS, implementing rate limiting and account lockouts, investigating authentication logs, and verifying if any accounts were compromised. Adjust firewall rules and employ additional monitoring as needed.

4. **Sensitive data copied to USBs:** Deploy Data Loss Prevention (DLP) tools to monitor and restrict USB activity, review endpoint logs, enforce strict access policies, and educate users on secure handling of data. Investigate past incidents to determine if any unauthorized transfers occurred.

5. **Complex passwords vs usability:** Strike a balance by enforcing passphrases rather than overly complex passwords, implementing multi-factor authentication, educating users on password hygiene, and using password managers to maintain security without compromising usability.

6. **Multiple alerts (ransomware, foreign login, firewall misconfiguration):** Prioritize alerts based on potential damage. Address ransomware first due to immediate threat to system integrity, investigate foreign logins for potential compromised accounts, and rectify firewall misconfigurations. Correlate alerts for contextual understanding.

7. **IDS false positives:** Use threat intelligence feeds, historical alert data, and correlation with other security events to prioritize alerts. Adjust IDS rules periodically and perform tuning to reduce unnecessary noise while ensuring real threats are detected.

8. **Healthcare system security with tight budget:** Focus on high-impact controls first: encrypt sensitive patient data, enforce strong access control policies, regularly patch systems, and segment networks to isolate critical components. Implement cost-effective monitoring and incident response strategies.

9. **After-hours file access:** Investigate by reviewing audit logs, analyzing user behavior for anomalies, interviewing the employee if appropriate, and monitoring for further unusual activity. Establish alerting for out-of-hours access.

10. **Secure emails/files with limited resources:** Use symmetric encryption for performance efficiency and secure key management, while employing asymmetric encryption for key exchange when necessary. Encourage use of secure communication channels and educate staff.

11. **SQL injection prevention:** Implement parameterized queries and prepared statements, validate and sanitize user inputs, enforce least privilege on database accounts, and conduct regular code reviews and automated security testing.

12. **Zero-day discovered:** Immediately isolate affected systems, apply virtual patches or mitigations if available, monitor systems for exploitation, notify vendors and stakeholders, and document response actions for post-incident analysis.
13. **Suspicious emails from HR:** Educate employees not to click links, report phishing attempts, analyze email headers for origin verification, and deploy email filtering tools. Conduct simulated phishing tests to strengthen awareness.

14. **Network segmentation:** Divide networks based on sensitivity and function, isolating critical assets from less sensitive systems. Use firewalls and VLANs to enforce boundaries, reducing the attack surface and minimizing lateral movement opportunities.

15. **Correlating multiple alerts:** Employ SIEM systems to aggregate, normalize, and correlate security events. Analyze patterns to distinguish true incidents from noise, prioritize alerts based on risk, and respond accordingly.

16. **Defend against brute force attacks:** Implement account lockout policies, CAPTCHAs, enforce strong password policies, and deploy multi-factor authentication to prevent automated attacks.

17. **Defend against MITM attacks:** Use TLS/SSL encryption, VPNs for secure communications, certificate pinning in applications, and secure authentication protocols. Regularly update cryptographic libraries and monitor for anomalies.

18. **Forward secrecy importance:** Ensures each session has a unique key. Even if long-term keys are compromised, past communications remain secure. Widely used in HTTPS and secure messaging.

19. **Virus vs Worm:** Viruses attach to executable files and require user action to spread, modifying or corrupting data. Worms replicate independently across networks, consuming bandwidth and system resources, often exploiting vulnerabilities without user intervention.

20. **SQL injection:** Malicious SQL input modifies database queries. Prevent through input validation, parameterized queries, stored procedures, and least privilege access policies.

21. **Network sniffing:** Captures packets traversing a network. Detect via anomaly detection systems, monitor ARP tables for spoofing, use encrypted communication, and segment sensitive networks.

22. **Detect data exfiltration:** Monitor outbound traffic, employ DLP solutions, track file access patterns, and investigate unusual transfers. Correlate with user behavior and system logs.

23. **Prioritize risks:** Assess risk based on likelihood and potential impact. Prioritize high-impact, high-likelihood vulnerabilities first, and maintain a dynamic risk register to adjust priorities as threat landscape evolves.

24. **Business continuity during cyberattacks:** Follow an incident response plan, maintain recent backups, activate alternate operations sites, and communicate clearly with stakeholders. Conduct post-incident analysis to prevent recurrence.

25. **Secure remote work:** Implement VPNs, endpoint security software, multi-factor authentication, and limit remote access to necessary systems. Educate staff on secure practices.

26. **Detect insider threat:** Monitor access logs, implement behavioral analytics, set alerts for anomalous activity, and conduct regular audits of privileged accounts.

27. **Ransomware response:** Immediately isolate infected systems, restore from backups, notify relevant parties, analyze attack vector, and implement additional security measures to prevent recurrence.
28. **Evaluate cloud provider security:** Review compliance certifications (ISO 27001, SOC2), assess encryption and access control practices, examine incident response protocols, and audit reports regularly to ensure data security.

29. **Test for phishing vulnerabilities:** Conduct simulated phishing campaigns, analyze employee responses, provide training on safe practices, and refine controls based on findings.

30. **Analyze alerts logically:** Always consider context, correlate with other system events, verify sources, and evaluate potential business impact before responding. Document findings and improve monitoring rules.

31. What is Cross-Site Request Forgery?

When an attacker gets a victim's browser to make requests, ideally with their credentials included, without their knowing. A solid example of this is when an IMG tag points to a URL associated with an action, e.g. http://foo.com/logout/. A victim just loading that page could potentially get logged out from foo.com, and their browser would have made the action, not them (since browsers load all IMG tags automatically).

32. What is the COBIT framework used for?

COBIT (Control Objectives for Information and Related Technologies) is used for **IT governance and management**. It helps align business goals with IT processes, ensuring effective risk management and regulatory compliance.

33. What is a cybersecurity framework?

A cybersecurity framework is a structured set of guidelines and best practices designed to help organizations manage and reduce cybersecurity risk. It provides a systematic approach to identifying, protecting, detecting, responding to, and recovering from cyber threats. Examples include NIST CSF, ISO 27001, and CIS Controls.

34. What are the core functions of the NIST Cybersecurity Framework?

The NIST CSF consists of **five core functions**:

a. **Identify** – Understand assets, risks, and business context.
b. **Protect** – Develop safeguards (access control, awareness, data protection).
c. **Detect** – Identify cybersecurity incidents quickly.
d. **Respond** – Take action to contain and mitigate threats.
e. **Recover** – Restore normal operations and improve processes.

35. What is SSL/TLS, and how does it secure communication?

SSL (Secure Sockets Layer) and **TLS (Transport Layer Security)** secure data transmission between a client and server using **encryption and certificates**.

- Data confidentiality
- Server authenticity (via certificates)
- Data integrity (via hashing)

36. What is Active Directory (AD)?

Active Directory (AD) is a **directory service developed by Microsoft** for Windows domain networks. It stores information about users, computers, and other resources, and manages authentication, authorization, and centralized administration.

37. What are the main components of Active Directory?

Domain: Logical group of network objects (users, computers).
Tree: Collection of domains in a hierarchical structure.
Forest: Collection of trees sharing a common schema.
Organizational Unit (OU): Container for organizing users/computers.
Objects: Actual items like users, groups, or printers.

38. What is a Domain Controller (DC)?

A Domain Controller is a **server that runs Active Directory Domain Services (AD DS)**. It authenticates and authorizes all users and computers in a domain and enforces security policies.

39. What is LDAP, and how does it relate to AD?

LDAP (Lightweight Directory Access Protocol) is used to query and modify items in directory services like AD.

AD is **Microsoft's implementation** of LDAP with Kerberos authentication.

40. What is Kerberos authentication in AD?

Kerberos is the **default authentication protocol** used by AD.

It uses **tickets** and symmetric key cryptography to verify identities securely, reducing password exposure on the network.

41. Define Buffer Overflow?

Buffer Overflow is a type of vulnerability that occurs when more data is written to buffer than it can hold allowing an attacker to execute malicious code.

42. A server is exposing a http server at port 8080 vulnerable to a directory traversal, you must use this vulnerability to leak the RSA key of one the user within the machine to get inside the server.

A. Find the endpoint

- Look for parameters that accept filenames/paths (examples: download, file, path).
- Confirm by requesting a known public file to ensure the endpoint returns expected content.

B. Verify traversal safely

- Probe with a harmless file outside webroot (example: /etc/hosts) using ../ sequences.
- Confirm the response contains the harmless file contents before attempting anything sensitive.

C. Check likely key locations (lab-only)

- Common paths to test: /home/<user>/.ssh/id_rsa, /home/<user>/.ssh/id_rsa.pub, /home/<user>/.ssh/authorized_keys, /root/.ssh/id_rsa, /etc/ssh/ssh_host_rsa_key.
- Look for PEM header -----BEGIN RSA PRIVATE KEY-----.

D. Validate the key (lab-only)

- Save retrieved content as id_rsa and confirm PEM format.
- Derive and fingerprint the public key to confirm identity (example: ssh-keygen -y -f id_rsa > id_rsa.pub and ssh-keygen -lf id_rsa.pub).