Tech Fusionist

CYBER SECURITY

QUICK GUIDE

FOR INTERVIEWS

Cyber Security

Services Covered

1. Firewalls
2. Intrusion Detection System (IDS)
3. Intrusion Prevention System (IPS)
4. VPN (Virtual Private Network)
5. Access Control Lists (ACL)
6. Encryption
7. Decryption
8. Malware Analysis
9. Penetration Testing
10. Vulnerability Assessment
11. Risk Assessment
12. Incident Response
13. Security Information and Event Management (SIEM)
14. Two-Factor Authentication (2FA)
15. Public Key Infrastructure (PKI)
16. Digital Certificates
17. Secure Sockets Layer (SSL)
18. Transport Layer Security (TLS)
19. Network Security
20. Endpoint Security
21. Data Loss Prevention (DLP)
22. Identity and Access Management (IAM)
23. Security Operations Center (SOC)
24. Phishing
25. Spoofing
26. Zero-Day Attack
27. Social Engineering
28. Distributed Denial of Service (DDoS)
29. Ransomware
30. Man-in-the-Middle Attack (MITM)
31. Brute Force Attack
32. Buffer Overflow
33. SQL Injection
34. Cross-Site Scripting (XSS)
35. Cyber Threat Intelligence
36. Cyber Kill Chain
37. Defense in Depth
38. Least Privilege Principle
39. Principle of Least Astonishment
40. Hardening
41. Patch Management
42. Incident Handling
43. Threat Modeling
44. Rootkit
45. Botnet
46. Trojan Horse
47. Payload
48. Backdoor
49. White Hat Hacker
50. Black Hat Hacker
51. Gray Hat Hacker
52. Red Team
53. Blue Team
54. Purple Team
55. Security Audit
56. Security Policy
57. Risk Management
58. Security Controls
59. Security Compliance
60. Data Classification
61. Network Segmentation
62. Cloud Security
63. Application Security
64. Mobile Device Management (MDM)
65. Container Security
66. Digital Forensics
67. Cybersecurity Frameworks (e.g., NIST, ISO/IEC 27001)
68. Threat Hunting
69. Web Application Firewall (WAF)
70. Network Access Control (NAC)
71. Security Orchestration, Automation, and Response (SOAR)
72. Secure Development Lifecycle (SDL)
73. Cyber Insurance
74. Security Awareness Training
75. Incident Classification
76. Data Breach
77. Security Architecture
78. Security as a Service (SECaaS)
79. Data Masking
80. Risk Register
81. Single Sign-On (SSO)
82. Honeypot
83. Security Operations (SecOps)
84. Digital Rights Management (DRM)
85. Threat Intelligence Platform (TIP)
86. Adaptive Security
87. Software Defined Security (SDS)
88. Next-Generation Firewall (NGFW)
89. Network Behavior Analysis (NBA)
90. Cyber Hygiene
91. Behavioral Analytics
92. Secure Coding
93. Security Testing
94. Password Management
95. Supply Chain Security
96. Incident Containment
97. Network Forensics
98. Application Whitelisting
99. Risk Mitigation
100. Cyber Resilience

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

1 Firewall

A security system that monitors and controls incoming and outgoing network traffic, allowing only authorized communication. Imagine it as a bouncer at a club, only letting in guests with valid IDs.

- Purpose: Protects against unauthorized access, malware, and data breaches by filtering traffic based on pre-defined rules.
- When to use: Always, on any device or network with internet access.
- How to use: Configured with specific rules and policies to allow legitimate traffic and block threats. Can be hardware, software, or cloud-based.
- Type of Threat Address: Network-based attacks, unauthorized access, data exfiltration.

2 Intrusion Detection System (IDS)

A security system that monitors network traffic for suspicious activities and anomalies, alerting administrators to potential threats. Think of it as a security guard noticing unusual behavior in a building.

- Purpose: Detects and reports potential intrusions before they cause damage, providing early warning and actionable intelligence.
- When to use: In critical networks and systems with sensitive data.
- How to use: Installed and configured to monitor specific traffic patterns and trigger alerts based on pre-defined rules.
- Type of Threat Address: Malware, network attacks, unauthorized access attempts.

3 Intrusion Prevention System (IPS)

Similar to IDS, but goes beyond detection and actively blocks identified threats. Think of it as a security guard who can stop suspicious individuals at the entrance.

- Purpose: Prevents intrusions in real-time, offering proactive defense against known threats and zero-day attacks.
- When to use: In high-risk environments where immediate response is critical.
- How to use: Deployed alongside IDS for proactive threat mitigation. Requires careful configuration to avoid blocking legitimate traffic.
- Type of Threat Address: Same as IDS, but with real-time prevention capabilities

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

4 VPN (Virtual Private Network)

Creates a secure tunnel over a public network, encrypting data communication between devices and a private server. Think of it as a secret passage for your data to travel safely.

- Purpose: Protects data privacy and security while connecting to public Wi-Fi or accessing sensitive information remotely.
- When to use: When using public Wi-Fi, accessing corporate networks remotely, or protecting sensitive data transmission.
- How to use: Install and configure a VPN client on your device, connect to a trusted VPN server, and enjoy secure communication.
- Type of Threat Address: Data interception, eavesdropping, and man-in-the-middle attacks.

5 Access Control Lists (ACL)

Rule-based system that defines who can access specific resources within a network. Think of it as a guest list for different areas in a building.

- Purpose: Controls access to network resources, preventing unauthorized users and activities.
- When to use: On all network devices and systems with sensitive data.
- How to use: Defined and applied on specific devices and resources, specifying who can access what and under what conditions.
- Type of Threat Address: Unauthorized access, data breaches, privilege escalation.

6 Encryption

The process of converting plain text data into a scrambled format that can only be decrypted with a specific key. Think of it as locking your data in a safe with a unique password.

- Purpose: Protects data confidentiality by ensuring it can only be accessed by authorized individuals with the decryption key.
- When to use: For storing and transmitting sensitive data, like financial information, personal data, or intellectual property.
- How to use: Various encryption algorithms and tools are available, depending on the data type and security requirements.
- Type of Threat Address: Data breaches, unauthorized access, data theft.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

7 Decryption

The reverse process of encryption, converting scrambled data back into its original plain text format using the correct decryption key. Think of it as unlocking your data safe with the right password.

- Purpose: Allows authorized users to access and process encrypted data for legitimate purposes.
- When to use: After receiving or retrieving encrypted data, when authorized access is required for analysis, processing, or use.
- How to use: Decryption tools and algorithms are specific to the encryption method used. Requires the correct decryption key to successfully access the data.
- Type of Threat Address: None directly, but supports secure access and processing of encrypted data.

8 Malware Analysis

The process of examining and understanding malicious software to identify its functionality, vulnerabilities, and potential threats. Think of it as dissecting a virus to understand its workings and develop countermeasures.

- Purpose: Helps security professionals detect new malware strains, develop effective defenses, and mitigate potential damage from existing malware.
- When to use: When suspicious activity or malware infections are detected, to understand the threat and develop appropriate response strategies.
- How to use: Specialized tools and techniques are used to analyze malware samples in controlled environments.
- Type of Threat Address: Malware detection, threat intelligence, vulnerability research, incident response.

9 Penetration Testing

Simulated cyberattacks conducted by authorized professionals to identify vulnerabilities and weaknesses in systems and networks. Think of it as ethical hacking to identify security flaws before attackers exploit them.

- Purpose: Identifies exploitable vulnerabilities before malicious actors can, allowing organizations to patch and strengthen their defenses.
- When to use: Regularly, on critical systems and networks, before major IT changes, or after significant modifications to infrastructure.
- How to use: Pen testers use various tools and techniques to attempt unauthorized access and identify vulnerabilities. Organizations can then address these vulnerabilities before real attacks occur.
- Type of Threat Address: Vulnerabilities, security weaknesses, potential attack vectors, incident response preparedness.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

10 Vulnerability Assessment

A systematic process of identifying, classifying, and prioritizing vulnerabilities within systems and networks. Think of it as a security audit to identify potential security gaps.

- Purpose: Provides a comprehensive understanding of an organization's security posture, highlighting critical vulnerabilities that require immediate attention.
- When to use: Regularly, as part of a proactive security strategy, after significant infrastructure changes, or before deploying new systems.
- How to use: Vulnerability scanners and assessment tools identify vulnerabilities, which are then prioritized and addressed based on their severity and potential impact.
- Type of Threat Address: Vulnerabilities, security gaps, prioritization of risks, vulnerability management.

11 Risk Assessment

A systematic process of identifying, analyzing, and evaluating potential threats and vulnerabilities within an organization's IT infrastructure. Think of it as proactively mapping potential security risks.

- Purpose: Helps prioritize security investments, allocate resources effectively, and develop a comprehensive security strategy to mitigate identified risks.
- When to use: Regularly, as part of a proactive security posture, before major IT changes, or after significant infrastructure modifications.
- How to use: Risk assessment methodologies vary, but typically involve threat modeling, vulnerability scanning, and penetration testing to identify and assess risks.
- Type of Threat Address: All types of threats, vulnerabilities, and security risks.

12 Incident Response

The process of identifying, containing, mitigating, and recovering from security incidents such as data breaches, malware infections, or cyberattacks. Think of it as a well-rehearsed emergency response plan for cybersecurity events.

- Purpose: Minimizes damage from security incidents, protects sensitive data, and restores normal operations as quickly as possible.
- When to use: Whenever a security incident is suspected or confirmed, such as unauthorized access attempts, data breaches, or system outages.
- How to use: Develop a comprehensive incident response plan outlining roles, responsibilities, communication protocols, and recovery procedures. Regularly test and update the plan to ensure readiness.
- Type of Threat Address: All types of security incidents, including data breaches, malware infections, cyberattacks, and system outages.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

13 Security Information and Event Management (SIEM)

A centralized platform that collects and analyzes security data from various sources across an organization's IT infrastructure. Think of it as a security command center that monitors and analyzes all security-related events.

- Purpose: Provides real-time visibility into security events, identifies potential threats, and helps security teams respond to incidents quickly and effectively.
- When to use: In organizations with complex IT infrastructure and large amounts of security data to manage.
- How to use: Implement SIEM software and configure it to collect data from various sources, such as firewalls, intrusion detection systems, and endpoint security tools. Analyze data for anomalies and suspicious activities to identify potential threats.
- Type of Threat Address: All types of security threats, including malware infections, unauthorized access attempts, and data breaches.

14 Two-Factor Authentication (2FA)

An additional layer of security that adds a second verification step beyond passwords, often involving a code sent via SMS or a dedicated app. Think of it as an extra lock on your door requiring a key and fingerprint.

- Purpose: Makes it significantly harder for attackers to gain access even if they steal your password, reducing the risk of unauthorized access and account compromise.
- When to use: On all accounts containing sensitive information, especially financial accounts, email, social media, and critical applications.
- How to use: Enable 2FA on supported accounts and choose a secure method like time-based one-time passwords or hardware authentication tokens.
- Type of Threat Address: Account takeover, password breaches, phishing attacks.

15 Public Key Infrastructure (PKI)

A system for secure digital identities and encryption using public and private key pairs. Think of it as a secure system of digital passports and keys for online interactions.

- Purpose: Enables secure communication, digital signatures, and authentication by verifying identities and encrypting data transmission.
- When to use: For online transactions, email encryption, website security (SSL/TLS), and secure communication between devices and applications.
- How to use: Obtain digital certificates from trusted certificate authorities and configure applications and systems to use PKI for secure communication and authentication.
- Type of Threat Address: Man-in-the-middle attacks, data breaches, identity theft, insecure communication.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

16 Digital Certificates

Electronic documents that verify the identity of a person or organization, issued by trusted certificate authorities. Think of it as a digital ID card for online entities.

- Purpose: Verify the identity of websites and applications, encrypt communication, and ensure secure transactions.
- When to use: For websites, email servers, VPN connections, and any online interaction requiring identity verification and secure communication.
- How to use: Obtain and install digital certificates on websites, servers, and applications to enable secure communication and identity verification.
- Type of Threat Address: Phishing attacks, spoofing, identity theft, insecure communication.

17 Secure Sockets Layer (SSL)

Encryption protocols that secure communication between devices and applications over the internet. Think of it as a secure tunnel for data transmission.

- Purpose: Protect data in transit from eavesdropping, tampering, and unauthorized access.
- When to use: On websites, email, online transactions, and any communication requiring data confidentiality and integrity.
- How to use: Most websites and applications automatically use SSL/TLS. Look for the padlock symbol in your browser address bar and "https://" to confirm secure connections.
- Type of Threat Address: Man-in-the-middle attacks, data interception, eavesdropping, and tampering.

18 Transport Layer Security (TLS)

TLS, or Transport Layer Security, is a cryptographic protocol that encrypts communication between devices and applications over the internet.

- Purpose: TLS serves several critical purposes like Confidentiality, Integrity, Authentication
- When to use: TLS should be used in various scenarios to safeguard your data for Websites, Emails and Online Transactions.
- How to use: TLS is often implemented automatically by websites, applications, and communication protocols.
- Type of Threat Address: Man-in-the-middle attacks, Eavesdropping, Data tampering, Identity theft.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

19 Network Security

A broad category of security measures and technologies designed to protect computer networks from unauthorized access, attacks, and malware.

- Purpose: Safeguard the integrity, confidentiality, and availability of network resources.
- When to use: All organizations, regardless of size, should implement network security measures.
- How to use: Implement various security tools and techniques like firewalls, intrusion detection/prevention systems, access control lists, network segmentation, and vulnerability management.
- Type of Threat Address: Network attacks, unauthorized access, malware infections, data breaches, network outages.

20 Endpoint Security

Security software and techniques installed on individual devices like laptops, desktops, and mobile phones to protect them from malware, unauthorized access, and data breaches.

- Purpose: Secure endpoints as critical entry points for cyberattacks.
- When to use: On all devices used to access organizational data, especially laptops, desktops, and mobile phones.
- How to use: Install and configure endpoint security software, including antivirus, anti-malware, and personal firewalls. Keep software updated and educate users on safe computing practices.
- Type of Threat Address: Malware infections, phishing attacks, data breaches, unauthorized access from compromised devices.

21 Data Loss Prevention (DLP)

A set of tools and processes that prevent sensitive data from being leaked or exfiltrated from an organization. Think of it as a security perimeter around your valuable information.

- Purpose: Protects sensitive data like financial records, personal data, and intellectual property from unauthorized access, theft, or accidental loss.
- When to use: In organizations with sensitive data, especially regulated industries like healthcare, finance, and government.
- How to use: Implement DLP policies, classify sensitive data, and use DLP tools to monitor and control data movement across endpoints, networks, and cloud environments.
- Type of Threat Address: Data breaches, unauthorized data sharing, insider threats, data exfiltration.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

22 Identity and Access Management (IAM)

A framework for managing user identities, access rights, and permissions across various systems and applications. Think of it as a secure key system for accessing digital resources.

- Purpose: Ensures only authorized users have access to specific resources based on their roles and permissions, preventing unauthorized access and privilege escalation.
- When to use: In organizations with multiple users and applications requiring granular access control.
- How to use: Implement IAM systems, define user roles and permissions, and enforce strong authentication and authorization mechanisms.
- Type of Threat Address: Unauthorized access, account takeover, identity theft, privilege escalation.

23 Security Operations Center (SOC)

A centralized hub for security monitoring, analysis, and incident response. Think of it as a security command center monitoring all security activities.

- Purpose: Provides real-time visibility into security events, detects and analyzes threats, and coordinates incident response activities.
- When to use: In organizations with complex IT infrastructure and high security requirements.
- How to use: Implement a SOC with SIEM, threat intelligence tools, and incident response protocols. Train personnel and ensure effective communication between the SOC and other security teams.
- Type of Threat Address: All types of security incidents, including cyberattacks, data breaches, malware infections, and system outages.

24 Phishing

A deceptive tactic luring victims into revealing sensitive information or clicking malicious links in emails, text messages, or websites. Think of it as a digital fishing lure to steal information.

- Purpose: Steals passwords, credit card details, personal information, or infects devices with malware.
- When to be aware: Always! Be cautious about unsolicited messages, suspicious attachments, and unexpected requests for information.
- How to protect yourself: Verify sender legitimacy, avoid clicking suspicious links, check website URLs, and use strong passwords with multi-factor authentication.
- Threat Address: Data breaches, identity theft, malware infections, financial loss.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

25 Spoofing

The act of impersonating another entity, like a legitimate website or person, to deceive victims. Think of it as a digital mask to hide true identity and gain trust.

- Purpose: Can be used for phishing attacks, email scams, malware distribution, or credit card fraud.
- When to be aware: Be cautious about unexpected contacts claiming to be from familiar entities. Verify sender details, check website URLs, and use caution with unsolicited calls or messages.
- How to protect yourself: Don't rely solely on email addresses or phone numbers for verification, check domain names and website certificates, and avoid sharing sensitive information over unverified channels.
- Threat Address: Identity theft, data breaches, financial loss, malware infections.

26 Zero-Day Attack

An exploit targeting a software vulnerability unknown to security vendors, making it difficult to detect and defend against. Think of it as a surprise attack using an unexpected vulnerability.

- Purpose: Gains unauthorized access, steals data, or disrupts systems before a patch is available.
- When to be vigilant: Always! Update software regularly and promptly apply security patches.
- How to protect yourself: Use layered security solutions, including firewalls, intrusion detection systems, and endpoint protection, alongside strong patching practices.
- Threat Address: Data breaches, system compromise, loss of control, financial damage.

27 Social Engineering

The manipulation of human emotions and psychology to trick victims into revealing information or taking actions that compromise security. Think of it as using persuasion and deception to gain access.

- Purpose: Steals data, gains unauthorized access, or spreads malware through deception and manipulation.
- When to be aware: Always! Be cautious about unsolicited requests, emotional appeals, and pressure tactics.
- How to protect yourself: Be skeptical of unexpected requests, verify information independently, and avoid making emotional decisions about security. Educate yourself about common social engineering tactics.
- Threat Address: Data breaches, identity theft, malware infections, financial loss.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

28 Distributed Denial of Service (DDoS)

An attack that overwhelms a website or server with traffic from multiple sources, making it unavailable to legitimate users. Think of it as a digital flood to overwhelm and shut down a website.

- Purpose: Disrupts websites, applications, or online services, causing financial loss and reputational damage.
- When to be prepared: If your organization relies heavily on online services or websites.
- How to protect yourself: Implement DDoS mitigation strategies like traffic filtering, rate limiting, and redundant infrastructure. Consider DDoS protection services from security providers.
- Threat Address: Website outages, service disruptions, financial loss, reputational damage.

29 Ransomware

Malicious software that encrypts files and demands payment for decryption. Think of it as a digital hostage situation for your data.

- Purpose: Extorts money from victims by making their data inaccessible.
- When to be aware: Always! Backup data regularly and keep backups offline to avoid ransomware attacks.
- How to protect yourself: Use anti-malware software, keep software updated, avoid suspicious attachments and links, and implement strong data backup and recovery procedures.
- Threat Address: Data loss, financial extortion, operational disruption, reputational damage.

30 Man-in-the-Middle Attack (MITM)

An attack where an attacker intercepts communication between two parties, eavesdropping or altering data in transit. Think of it as a hidden listener on a phone call.

- Purpose: Steals sensitive information, redirects users to malicious websites, or modifies data for fraudulent purposes.
- When to be aware: Always! Use secure connections (HTTPS) on websites and avoid public Wi-Fi for sensitive communication.
- How to protect yourself: Use VPNs on public Wi-Fi, verify website certificates, and avoid insecure connections like HTTP.
- Threat Address: Data interception, eavesdropping, data manipulation, identity theft, financial loss

CYBER SECURITY

QUICK GUIDE

REMAINING SERVICES WILL UPDATED IN COUPLE OF DAYS AND WILL BE SHARED WITH YOU!

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Beginners

1. What is a firewall?
A firewall is a network security device that monitors and controls incoming and outgoing traffic, acting as a barrier between trusted and untrusted networks. It filters traffic based on predefined rules, allowing legitimate traffic and blocking malicious activity. Think of it as a security guard at the entrance to your network, checking credentials and access permissions.

2. How does an Intrusion Detection System (IDS) differ from an Intrusion Prevention System (IPS)?
An IDS monitors network traffic for suspicious activity, but it doesn't actively block it. It raises an alarm when it detects potential threats, allowing security teams to investigate and take action. An IPS, on the other hand, actively prevents threats by blocking malicious traffic before it can harm the network. It's like an IDS with a built-in bouncer, stopping attackers in their tracks.

3. Explain the purpose of a VPN (Virtual Private Network).
A VPN creates a secure tunnel over the public internet, encrypting data transmitted between your device and a remote server. This protects your online activity from eavesdropping and ensures privacy when using public Wi-Fi, for example. Think of it as a secret passageway through a crowded marketplace, shielding your communications from prying eyes.

4. What are Access Control Lists (ACLs) used for?
ACLs are sets of rules that define who can access what resources on a network. They specify the type of traffic allowed (e.g., ports, protocols), the source and destination addresses, and the permitted actions (e.g., read, write, execute). Imagine ACLs as VIP passes for your network, granting access only to authorized users and activities.

5. Define encryption and its importance in cybersecurity.
Encryption scrambles data into an unreadable format, requiring a decryption key to access it. This protects sensitive information like passwords, financial data, and personal files from unauthorized access even if intercepted. In cybersecurity, encryption is like a locked vault, safeguarding valuable data from prying hands.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Beginners

6. What is malware analysis and why is it crucial?
Malware analysis involves examining and understanding malicious software to identify its capabilities, vulnerabilities, and potential targets. This knowledge is crucial for developing effective defenses, detecting future attacks, and mitigating damage caused by malware. Think of it as dissecting a virus to understand its weaknesses and develop a cure.

7. What is penetration testing?
Penetration testing, also known as pen testing, simulates real-world cyberattacks to identify vulnerabilities in an organization's systems and networks. Ethical hackers attempt to exploit these vulnerabilities, providing valuable insights for patching weaknesses and improving security posture. Imagine pen testing as a controlled fire drill, exposing vulnerabilities before real attackers can exploit them.

8. How does vulnerability assessment differ from risk assessment?
Vulnerability assessment identifies weaknesses in systems and networks, while risk assessment evaluates the potential impact and likelihood of those vulnerabilities being exploited. Combining these assessments provides a comprehensive understanding of the security risks faced by an organization, allowing them to prioritize and address the most critical issues. Think of it as mapping out potential potholes on a road (vulnerability assessment) and then prioritizing repairs based on their severity and potential damage (risk assessment).

9. Explain the concept of incident response.
Incident response is a planned approach to identifying, containing, and recovering from security incidents. It involves a set of procedures for investigating suspicious activity, minimizing damage, eradicating threats, and preventing future incidents. Imagine incident response as a well-rehearsed emergency plan for your network, ensuring a swift and effective response to security breaches.

10. What is Security Information and Event Management (SIEM)?
A SIEM is a platform that collects and analyzes security data from various sources across an organization's network. It provides real-time insights into security events, allowing security teams to detect threats, investigate incidents, and respond effectively. Think of SIEM as a central hub for your security information, offering a holistic view of your network's health and potential threats.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Beginners

11. Define Two-Factor Authentication (2FA) and its advantages.
Two-Factor Authentication (2FA) adds an extra layer of security by requiring two forms of verification for access, typically a password and a one-time code (SMS, app, etc.). This significantly reduces the risk of unauthorized access even if a password is compromised.

12. What is Public Key Infrastructure (PKI) used for?
PKI provides secure encryption and authentication for online communication. It uses paired public and private keys to scramble and unscramble messages, ensuring only authorized parties can read them and verify their identity.

13. Describe the function of Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
SSL and TLS are protocols that encrypt communication between your device and a server, protecting data from eavesdropping during online activities like banking and e-commerce. Both achieve similar goals, but TLS is the newer and more secure version of SSL.

14. What is meant by endpoint security?
Endpoint security focuses on protecting individual devices (laptops, phones, etc.) from malware, unauthorized access, and data breaches. It includes antivirus software, firewalls, encryption, and patching vulnerabilities to harden endpoints against cyberattacks.

15. Explain the purpose of Data Loss Prevention (DLP).
DLP systems prevent sensitive data from being leaked or accessed by unauthorized individuals. They monitor user activities, data transfers, and content, identifying and blocking attempts to share confidential information outside authorized channels.

16. What is Identity and Access Management (IAM)?
IAM manages user identities, access permissions, and authentication processes within an organization. It controls who can access what resources, ensuring only authorized users have the necessary privileges to perform specific tasks.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Beginners

17. Define a Security Operations Center (SOC).
A SOC is a centralized hub for monitoring, analyzing, and responding to security threats across an organization's network. It gathers data from various sources, detects suspicious activity, and coordinates incident response efforts.

18. Explain phishing and its potential impact.
Phishing scams attempt to trick users into revealing personal information or clicking malicious links through deceptive emails, texts, or websites. This can lead to identity theft, financial losses, and malware infections.

19. What is a DDoS (Distributed Denial of Service) attack?
A DDoS attack floods a server with overwhelming traffic from compromised devices worldwide, aiming to overload it and make it unavailable to legitimate users. This can disrupt critical services, damage reputation, and cause financial losses.

20. Define ransomware and how it operates.
Ransomware encrypts a victim's files, making them inaccessible, and demands a ransom payment for decryption. It can target individuals, organizations, and critical infrastructure, causing significant data loss and financial disruption.

Questions: Intermediate

21. How can Cross-Site Scripting (XSS) vulnerabilities be exploited?
XSS vulnerabilities allow attackers to inject malicious scripts into web pages, potentially stealing user data, hijacking sessions, or redirecting users to phishing sites. Attackers can exploit XSS through various methods, such as:

- **Reflected XSS:** Injecting malicious code in inputs like search bars or comments, reflected back to users.
- **Stored XSS:** Inserting scripts in database fields like usernames, later displayed to other users.
- **DOM-based XSS:** Exploiting vulnerabilities in JavaScript code to manipulate the web page dynamically.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

22. Discuss the layers involved in Defense in Depth strategy.
Defense in Depth is a layered security approach where multiple controls are implemented at different levels to create overlapping barriers against threats. Key layers include:

- **Network Security:** Firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation to control traffic flow.
- **Endpoint Security:** Antivirus software, endpoint detection and response (EDR), and application whitelisting to protect devices.
- **Application Security:** Code reviews, vulnerability scanning, and secure coding practices to prevent vulnerabilities in software.
- **Data Security:** Encryption, access controls, and data loss prevention (DLP) to protect sensitive information.
- **Physical Security:** Physical access controls, security cameras, and monitoring systems to safeguard physical infrastructure.

23. Explain the Principle of Least Privilege in detail.
The Principle of Least Privilege states that users and systems should only have the minimum permissions necessary to perform their intended tasks. This minimizes the potential damage caused by compromised accounts or systems. Implementing least privilege involves:

- Assigning roles and permissions based on specific needs and responsibilities.
- Granting temporary access for specific tasks, not permanent privileges.
- Regularly reviewing and adjusting access levels to ensure they remain appropriate.

24. Discuss the concept of hardening in cybersecurity.
Hardening refers to strengthening systems and networks to make them more resistant to cyberattacks. This involves a range of measures, including:

- Patching vulnerabilities promptly to close security holes.
- Disabling unnecessary services and applications to reduce attack surface.
- Configuring systems securely with strong passwords, encryption, and access controls.

Implementing intrusion detection and prevention systems to monitor for suspicious activity.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

25. Describe the steps involved in efficient patch management.
Efficient patch management involves a systematic approach to identifying, testing, and deploying security patches across systems:

- Vulnerability Scanning: Regularly scan systems for vulnerabilities to identify patching priorities.
- Patch Evaluation: Test patches in a controlled environment before deploying them to production systems.
- Deployment Planning: Develop a plan for rolling out patches with minimal disruption.
- Monitoring and Validation: Monitor systems after patching for potential issues and verify successful implementation.

26. Discuss the Incident Handling process in detail.
Incident handling involves a structured approach to identifying, containing, eradicating, and recovering from security incidents:

- Identification: Detect and analyze suspicious activity to identify potential incidents.
- Containment: Limit the impact of the incident by isolating affected systems and users.
- Eradication: Eliminate the threat by removing malware, patching vulnerabilities, or restoring backups.
- Recovery: Restore affected systems and data to their previous state.
- Post-mortem: Analyze the incident to identify root causes and improve future response procedures.

27. How is threat modeling conducted in cybersecurity?
Threat modeling identifies and analyzes potential threats to systems and applications. This involves:

- Identifying assets: Defining critical systems and data needing protection.
- Mapping threats: Identifying potential attack vectors and vulnerabilities.
- Analyzing risks: Evaluating the likelihood and impact of each threat.
- Implementing controls: Defining security measures to mitigate identified risks.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

28. Explain the characteristics of a botnet and how to mitigate its impact.
A botnet is a network of compromised devices controlled by an attacker. Characteristics include:

- **Centralized command and control:** The attacker controls the botnet through a server.
- **Large-scale attacks:** Botnets can be used for DDoS attacks, spam campaigns, or data theft.
- **Difficulties in detection:** Individual botnet nodes may be difficult to identify.

Mitigation involves:

- **Patching vulnerabilities:** Closing security holes used to compromise devices.
- **Network segmentation:** Isolating critical systems from potential botnet infection.
- **Anti-botnet software:** Deploying tools to detect and remove botnet malware.

29. Discuss the ethical implications of White Hat Hacking.
White Hat Hackers identify and disclose vulnerabilities to organizations responsibly, helping them improve their security posture. However, ethical considerations arise regarding the methods used, potential for misuse, and vulnerability disclosure practices. Transparency and responsible vulnerability disclosure are crucial to ensure ethical and beneficial white hat hacking.

30. Explain the motivations behind Black Hat Hacking.
Black Hat Hackers engage in illegal or malicious activities for personal gain or disruption. Their motivations can include:

- **Financial gain:** Stealing data, extorting money through ransomware, or selling stolen information.
- **Power and control:** Defacing websites, disrupting critical infrastructure, or causing widespread damage.
- **Challenge and recognition:** Demonstrating technical skills or proving their ability to exploit vulnerabilities.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

31. Discuss the importance of a Risk Management Framework.
A Risk Management Framework defines a structured approach to identifying, analyzing, prioritizing, and mitigating security risks. It provides a roadmap for organizations to proactively address threats, allocate resources effectively, and make informed security decisions. By proactively managing risks, organizations can minimize potential losses, ensure business continuity, and build a more resilient security posture.

32. Describe the elements of a robust Security Compliance program.
A robust Security Compliance program ensures adherence to relevant regulations and industry standards. Key elements include:

- **Policy and Procedure Development:** Defining clear policies and procedures for all aspects of security.
- **Risk Assessment and Management:** Identifying, analyzing, and mitigating security risks.
- **Control Implementation:** Implementing and maintaining appropriate security controls.
- **Training and Awareness:** Training employees on security policies and procedures.
- **Monitoring and Auditing:** Monitoring compliance and conducting regular audits.
- **Incident Response:** Defining and rehearsing a plan for handling security incidents.

33. How does Data Classification aid in securing information?
Data Classification categorizes information based on its sensitivity and criticality. This helps organizations prioritize security controls, restrict access, and implement appropriate data protection measures. By understanding the value and risk associated with different types of data, organizations can focus their security efforts on protecting the most sensitive information.

34. Explain the role of network segmentation in enhancing security.
Network segmentation divides a network into smaller, isolated segments, limiting the spread of malware and lateral movement of attackers. This can confine damage to specific segments, minimizing the impact of security incidents. Additionally, it facilitates granular control over access and simplifies security management.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

35. Discuss the key challenges in Cloud Security.
Cloud security challenges include:

- **Shared responsibility model:** Dividing security responsibilities between cloud provider and customer can lead to confusion and gaps in coverage.
- **Data residency and privacy:** Ensuring data is stored and processed in compliance with regulations and user expectations.
- **Visibility and control:** Maintaining visibility into cloud environments and ensuring adequate control over security configurations.
- **Evolving threats:** Keeping pace with the evolving landscape of cloud-specific threats and vulnerabilities.

36. What are the common vulnerabilities in application security?
Common application security vulnerabilities include:

- **Injection vulnerabilities (SQL injection, XSS):** Exploiting user input to inject malicious code.
- **Broken authentication and authorization:** Weak password policies, insecure session management, and unauthorized access to resources.
- **Cross-site scripting (XSS):** Injecting malicious scripts into web applications to steal user data or hijack sessions.
- **Insecure direct object references:** Accessing unauthorized objects due to flawed design or implementation.
- **Insufficient logging and monitoring:** Lack of visibility into application activity, making it difficult to detect and respond to attacks.

37. Explain the components of a Mobile Device Management (MDM) system.
An MDM system manages mobile devices used within an organization. Key components include:

- **Device enrollment and provisioning:** Securely registering and configuring devices.
- **Policy enforcement:** Implementing security policies like password requirements, application restrictions, and encryption.
- **Remote device management:** Pushing updates, troubleshooting issues, and wiping lost or stolen devices.
- **Application management:** Deploying and controlling applications on devices.
- **Data security:** Protecting corporate data on mobile devices.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

38. Discuss the methodologies involved in Digital Forensics.
Digital forensics investigates cybercrime through the analysis of digital evidence. Methodologies involve:

- **Identification and preservation:** Identifying relevant evidence and ensuring its integrity.
- **Acquisition and collection:** Securely collecting evidence from various sources.
- **Analysis and examination:** Examining evidence to uncover artifacts and reconstruct events.
- **Reporting and presentation:** Documenting findings and presenting them in a court-admissible format.

39. Compare and contrast NIST and ISO/IEC 27001 frameworks.

- **NIST Cybersecurity Framework:** Voluntary framework providing a flexible approach to managing cybersecurity risks.
- **ISO/IEC 27001:** Prescriptive standard with detailed controls and requirements for implementing an information security management system (ISMS).

Similarities: Both frameworks focus on identifying, assessing, and managing security risks.

Differences: NIST is more flexible and adaptable, while ISO/IEC 27001 is more prescriptive and compliance-oriented.

40. How does Threat Hunting enhance cybersecurity?
Threat hunting proactively seeks out and identifies potential threats before they materialize into incidents. This proactive approach can:

- **Detect advanced threats:** Uncover threats that evade traditional security measures.
- **Reduce dwell time:** Identify threats early and minimize potential damage.
- **Improve incident response:** Provide valuable insights for faster and more effective response.
- **Strengthen overall security posture:** Increase the organization's overall security posture.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

41. Explain the functionality of a Web Application Firewall (WAF).
A WAF sits between a website and the internet, monitoring traffic for malicious patterns. It acts like a security guard, filtering out attacks like SQL injection, XSS, and bot attacks before they reach the web application, protecting it from vulnerabilities.

42. What are the key features of Network Access Control (NAC)?
NAC verifies the identity and health of devices before granting access to the network. It can:

- **Authenticate devices:** Ensures only authorized devices connect.
- **Enforce security policies:** Implements device posture checks and configuration compliance.
- **Quarantine or block unauthorized devices:** Limits potential attack vectors.

43. Discuss the advantages of Security Orchestration, Automation, and Response (SOAR) systems.
SOAR automates and integrates various security tools, streamlining incident response and threat detection. Benefits include:

- **Faster response times:** Automating routine tasks frees up analysts for complex investigations.
- **Improved efficiency:** Centralized platform reduces manual workload and coordination efforts.
- **Enhanced visibility:** Correlating data from different tools provides a holistic view of security posture.

44. Describe the stages of a Secure Development Lifecycle (SDL).
SDL integrates security practices throughout the software development process. Stages typically include:

- **Threat modeling:** Identifying potential threats and vulnerabilities early.
- **Secure coding practices:** Implementing secure coding techniques to minimize vulnerabilities.
- **Security testing:** Regularly testing applications for vulnerabilities.
- **Incident response planning:** Preparing for and addressing security incidents effectively.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

45. Explain the role of Cyber Insurance in risk management.
Cyber Insurance financially protects organizations from cyberattacks and their consequences. It can:

- **Offset financial losses:** Cover costs associated with data breaches, business disruptions, and legal fees.
- **Improve risk management:** Encourage organizations to invest in stronger security controls.
- **Provide access to expertise:** Insurance providers may offer incident response assistance and security consulting services.

46. Discuss the strategies for effective Security Awareness Training.
Effective training engages employees and promotes a culture of security. Strategies include:

- **Interactive and engaging content:** Use real-world scenarios, quizzes, and phishing simulations.
- **Tailored training:** Address specific roles and responsibilities within the organization.
- **Continuous learning:** Encourage ongoing awareness through regular updates and refresher courses.
- **Measurement and feedback:** Track training effectiveness and adapt programs based on results.

47. How are incidents classified based on severity in cybersecurity?
Incidents are often classified based on factors like:

- **Impact:** Potential damage caused to data, systems, or operations.
- **Scope:** Extent of affected users, systems, or data.
- **Likelihood:** Probability of further harm or escalation.

Common severity levels include:

- **Low:** Minimal impact, minimal urgency.
- **Medium:** Moderate impact, needs prompt attention.
- **High:** Significant impact, requires immediate action.
- **Critical:** Severe impact, necessitates full-scale response.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Intermediate

48. Explain the design considerations in Security Architecture.
Security Architecture defines the overall security posture of an organization. Design considerations include:

- **Defense in depth:** Implementing layered security controls to mitigate various threats.
- **Least privilege:** Granting users only necessary access to minimize attack surface.
- **Scalability and flexibility:** Adapting security to evolving threats and business needs.
- **Integration and automation:** Combining various security tools for efficient management.

49. Discuss the benefits and limitations of Security as a Service (SECaaS).
SECaaS offers managed security solutions delivered on a cloud platform. Benefits include:

- **Reduced costs:** Eliminates need for expensive hardware and in-house expertise.
- **Scalability and flexibility:** Easily adapts to changing security needs.
- **Access to advanced technologies:** Leverages provider's expertise and resources.

Limitations include:

- **Vendor dependence:** Relies on provider's security posture and infrastructure.
- **Potential data privacy concerns:** Sharing sensitive data with the provider.
- **Limited customization:** May not fully meet specific security requirements.

50. How does Data Masking contribute to privacy protection?
Data masking replaces sensitive information with realistic but non-identifiable data, protecting privacy while enabling essential activities like testing and training. It can:

- **Meet compliance requirements:** Fulfill regulations regarding data privacy and security.
- **Reduce risk of data breaches:** Minimize potential harm if sensitive data is compromised.
- **Enable data sharing and collaboration:** Facilitate secure data sharing without exposing personally identifiable information.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Expert

1. You're a cybersecurity analyst in a financial institution. Describe how you'd respond to a potential ransomware attack targeting critical systems.

Action need to taken as below to a Potential Ransomware Attack:

1. **Immediate Containment:** Isolate affected systems, disconnect network access, and activate backup protocols.
2. **Incident Response:** Assemble response team, notify relevant authorities, and initiate investigation.
3. **Identify and Evaluate:** Analyze attack vectors, determine data encrypted, and assess potential damage.
4. **Decision Point:** Consider decryption options (paying ransom, leveraging backups, utilizing decryption tools) based on risk-benefit analysis.
5. **Recovery and Post-Incident:** Restore systems from backups, patch vulnerabilities, and conduct comprehensive review to prevent future attacks.

2. You've discovered a persistent Man-in-the-Middle attack within your organization's network. Detail the steps you'd take to mitigate this threat.

Step need to taken to mitigate a persistent Man-in-the-Middle Attack:

1. **Isolate and Contain:** Identify compromised devices and isolate them from the network to prevent further interception.
2. **Investigate and Trace:** Analyze network logs to identify attack origin, attack methods, and potentially compromised systems.
3. **Eradicate Malware:** Remove malicious software from affected devices and ensure clean installation of operating systems.
4. **Remediate Vulnerabilities:** Patch security holes exploited in the attack and implement network segmentation to limit attack vectors.
5. **Review and Monitor:** Conduct a post-incident review to identify root cause and implement improved security measures. Continuously monitor network for suspicious activity.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Expert

3. A major e-commerce platform you're overseeing has experienced a DDoS attack. Outline your plan to handle this situation.

We can take below steps to handle DDoS Attack on E-Commerce Platform:

1. **DDoS Mitigation Service:** Activate pre-configured DDoS mitigation service to absorb and distribute attack traffic.
2. **Identify and Block Attackers:** Analyze attack patterns and utilize traffic filtering mechanisms to block malicious IP addresses and traffic.
3. **Communication and Scalability:** Communicate with customers and stakeholders about the attack, ensuring transparency and minimizing disruption.
4. **Scale Resources:** Consider scaling up cloud infrastructure or activating additional servers to handle increased traffic volume.
5. **Post-Incident Analysis and Prevention:** Analyze attack logs and vulnerabilities exploited, implement improved DDoS mitigation strategies, and consider diversifying traffic routing.

4. Discuss a comprehensive strategy to defend against evolving phishing techniques within a corporate environment.

Strategy for Defending Against Evolving Phishing:

1. **Security Awareness Training:** Train employees on phishing techniques, social engineering tactics, and red flags to identify suspicious emails.
2. **Email Filtering and Security Tools:** Implement robust email filtering solutions and utilize advanced security tools to detect and block malicious emails.
3. **Simulated Phishing Exercises:** Conduct regular phishing simulations to test employee awareness, identify vulnerabilities in training, and promote continuous learning.
4. **Phishing Reporting Mechanisms:** Establish clear reporting channels for employees to report suspicious emails and provide timely feedback for analysis and updates.
5. **Multi-layered Security Approach:** Combine technical solutions with employee awareness to create a comprehensive defense against evolving phishing threats.

CYBER SECURITY - QUICK GUIDE FOR **INTERVIEWS**

Questions: Expert

5. In a scenario where your company's database has been compromised due to an SQL injection, how would you conduct a forensic investigation?

Forensic investigation against SQL Injection Database Compromise:

1. **Immediate Containment:** Isolate the compromised database server and restrict access to prevent further data manipulation or exfiltration.
2. **Forensic Data Acquisition:** Secure and acquire forensic copies of logs, database files, and related evidence for investigation.
3. **Incident Response Team:** Assemble a qualified incident response team with expertise in forensics and database security.
4. **Analyze Attack Vector and Scope:** Identify the specific SQL injection exploit used, determine the extent of data accessed or compromised, and assess potential damage.
5. **Remediate Vulnerabilities:** Patch the SQL injection vulnerability and implement additional security measures to prevent future exploitation.
6. **Data Recovery and Restoration:** Restore the database from backups or implement data recovery techniques if backups are unavailable.
7. **Post-Incident Review and Reporting:** Conduct a thorough review to identify root causes, implement corrective actions, and report findings to relevant authorities.

CYBER SECURITY

QUICK GUIDE

THANK YOU!

Tech Fusionist