TOP 100 Interview Questions

PART 2

TOP 100 INTERVIEW QUESTIONS PART 2

51. What are the phases of an incident response process?

The incident response process typically includes:

1. **Preparation:** Establishing systems, policies, and procedures.
2. **Identification:** Detecting and confirming incidents.
3. **Containment:** Limiting the damage.
4. **Eradication:** Eliminating the root cause.
5. **Recovery:** Restoring systems and services.
6. **Lessons Learned:** Reviewing the incident to improve future responses.

---

52. How would you manage a data breach?

Managing a data breach involves identifying the source, containing the issue to prevent further impact, notifying affected individuals and relevant authorities, investigating the breach to understand its scope, and implementing measures to prevent recurrence.

---

53. Which tools are commonly used in digital forensics?

Popular digital forensics tools include EnCase, FTK Imager, Autopsy, Sleuth Kit, and X1 Search. These tools assist in collecting, analysing, and preserving evidence during investigations.

---

54. What is the difference between proactive and reactive incident management?

- **Proactive management:** Focuses on preventing incidents through regular security assessments and monitoring.
- **Reactive management:** Involves responding to incidents after they occur to minimize damage.

---

55. How is the chain of custody maintained during a forensic investigation?

The chain of custody is preserved by documenting every individual who handles the evidence, recording timestamps for each transfer, and securely storing evidence to prevent tampering.

TOP 100 INTERVIEW QUESTIONS PART 2

---

56. How would you address a phishing email reported by an employee?

Analyze the email for signs of phishing, such as fake links or unusual sender addresses. Educate the employee on recognizing phishing attempts, block the sender, isolate affected systems, and investigate to ensure no additional threats exist.

---

57. What distinguishes a security incident from a security event?

A **security incident** is a verified breach or attempted breach of security, while a **security event** is an observable action or occurrence that might or might not pose a threat.

---

58. How do you detect and respond to Advanced Persistent Threats (APTs)?

Detecting APTs involves monitoring for prolonged unusual activity, analyzing network traffic, and identifying Indicators of Compromise (IOCs). Response includes isolating affected systems, removing attacker access, and improving detection mechanisms.

---

59. What are the key phases of the Cyber Kill Chain?

The Cyber Kill Chain includes:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Action on Objectives

---

60. What are Indicators of Compromise (IOCs), and how are they used?

IOCs are signs that a system has been breached, such as unusual network traffic, rogue processes, or malicious files. They help identify, investigate, and respond to security incidents.

TOP 100 INTERVIEW QUESTIONS PART 2

---

61. What is the goal of GDPR or similar data protection regulations?

Regulations like GDPR (General Data Protection Regulation) aim to protect individuals' personal data, ensure privacy rights, and provide guidelines for organizations to securely manage data.

---

62. How do ISO 27001 and NIST frameworks differ?

- **ISO 27001:** A global standard for establishing and maintaining an Information Security Management System (ISMS).
- **NIST Frameworks:** Provide technical guidelines for managing cybersecurity risks.

ISO 27001 focuses on management processes, while NIST offers detailed technical recommendations.

---

63. What are the primary controls in PCI DSS compliance?

Key PCI DSS controls include:

- Protecting cardholder data using encryption and secure storage.
- Implementing firewalls and access controls.
- Conducting vulnerability scans and penetration testing.
- Logging and monitoring all network activity.

---

64. How do you ensure adherence to security policies?

Security policy compliance is achieved through regular monitoring, periodic audits, employee training, and automating enforcement with tools and technologies.

---

65. Why are security audits important?

Security audits evaluate the effectiveness of security controls, identify vulnerabilities, ensure regulatory compliance, and provide actionable recommendations for enhancing security.

TOP 100 INTERVIEW QUESTIONS PART 2

---

66. What is the purpose of a security baseline?

A security baseline defines the minimum required security settings and configurations for systems to meet organizational standards and minimize risks.

---

67. How are risk assessment and risk management different?

- **Risk assessment:** Identifies and evaluates risks.
- **Risk management:** Encompasses mitigating, monitoring, and addressing identified risks.

---

68. What is an Information Security Management System (ISMS)?

An ISMS is a framework of policies, procedures, and controls designed to manage an organization's information security risks systematically.

---

69. How does a Business Continuity Plan (BCP) differ from a Disaster Recovery Plan (DRP)?

- **BCP:** Focuses on maintaining essential business operations during disruptions.
- **DRP:** Specifically addresses the restoration of IT systems and data after a disaster.

---

70. What is the difference between qualitative and quantitative risk assessments?

- **Qualitative:** Evaluates risks based on subjective criteria like likelihood and impact.
- **Quantitative:** Uses numerical data, such as financial implications, to assess risks

71. How do symmetric and asymmetric encryption differ?

- **Symmetric encryption:** Uses the same key for both encryption and decryption, making it faster but less secure for key exchange.
- **Asymmetric encryption:** Employs a pair of keys—public and private—offering better security but slower performance due to its computational complexity.

TOP 100 INTERVIEW QUESTIONS PART 2

---

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

MFA requires users to verify their identity using two or more factors, such as:

- **Something you know:** Password.
- **Something you have:** Security token or smartphone.
- **Something you are:** Biometric data like a fingerprint.

It enhances security by adding layers of protection.

---

73. How does hashing differ from encryption?

Hashing is a one-way process that converts data into a fixed-length hash value, primarily for verifying integrity. Encryption, on the other hand, is a reversible process that transforms data into an unreadable format to ensure confidentiality.

---

74. What role does a firewall play in network security?

A firewall acts as a protective barrier between internal and external networks, filtering traffic based on predefined rules to block unauthorized access and reduce security risks.

---

75. How does a Virtual Private Network (VPN) work?

A VPN creates a secure, encrypted tunnel for data transmission between a user's device and a remote network. It ensures privacy by hiding the user's IP address and encrypting all communication.

---

76. What is the principle of least privilege, and why is it important?

The principle of least privilege restricts users, systems, and applications to the minimum access necessary to perform their tasks. This reduces the risk of accidental or malicious misuse.

TOP 100 INTERVIEW QUESTIONS PART 2

77. How can you secure a web application effectively?

Securing a web application involves:

- Input validation and output encoding.
- Implementing secure authentication methods like MFA.
- Using HTTPS and strong access controls.
- Regularly testing for vulnerabilities such as SQL injection and XSS.

---

78. What is the difference between IDS and IPS?

- **Intrusion Detection Systems (IDS):** Monitor network traffic for suspicious activities and generate alerts.
- **Intrusion Prevention Systems (IPS):** Detect and actively block threats in real time.

---

79. How does HTTPS improve upon HTTP?

HTTPS encrypts data exchanged between a user's browser and the server using SSL/TLS protocols, ensuring confidentiality and protection from interception, unlike HTTP, which transmits data in plaintext.

---

80. What is a man-in-the-middle (MITM) attack?

A MITM attack occurs when an attacker intercepts communication between two parties, potentially altering or stealing sensitive information without their knowledge.

---

81. What is Wireshark, and how is it used?

Wireshark is a network analysis tool that captures and inspects packets of data in real-time. It's commonly used to troubleshoot network issues, detect security threats, and analyze protocols.

---

82. What is a Security Information and Event Management (SIEM) system?

TOP 100 INTERVIEW QUESTIONS PART 2

A SIEM system collects, aggregates, and analyzes log data from various sources to detect and respond to security threats in real time, providing valuable insights into security events and anomalies.

---

83. How does a port scanner differ from a vulnerability scanner?

- **Port scanner:** Identifies open ports and running services on a network.
- **Vulnerability scanner:** Detects known security weaknesses in systems or networks.

---

84. What is a honeypot, and how is it used in cybersecurity?

A honeypot is a decoy system designed to attract attackers by mimicking vulnerabilities. It's used to study attack techniques and protect actual systems by diverting malicious activity.

---

85. What is a sandbox in cybersecurity?

A sandbox is a controlled, isolated environment where suspicious files or programs can be tested for malicious behavior without risking harm to production systems.

---

86. What role does a proxy server play in security?

A proxy server acts as an intermediary between clients and servers, enhancing security by filtering traffic, masking client IP addresses, and caching content for improved performance.

---

87. Why is penetration testing important?

Penetration testing, or ethical hacking, simulates cyberattacks to uncover security weaknesses before they can be exploited by malicious actors, helping organizations improve their defenses.

TOP 100 INTERVIEW QUESTIONS PART 2

88. What is a reverse shell, and how does it work?

A reverse shell allows an attacker to gain control of a victim's system by initiating an outbound connection to the attacker's server, often bypassing firewall restrictions.

---

89. What are the common types of malware?

- **Viruses:** Attach to files and require user action to spread.
- **Worms:** Replicate independently across networks.
- **Trojans:** Disguise themselves as legitimate software.
- **Ransomware:** Encrypts files and demands payment for decryption.
- **Spyware:** Monitors user activities without consent.
- **Adware:** Delivers unwanted advertisements.

---

90. How do you prevent cross-site scripting (XSS) attacks?

Prevent XSS by:

- Validating and sanitizing user inputs.
- Encoding outputs.
- Using Content Security Policy (CSP) headers.
- Avoiding inline JavaScript.

---

91. What is the Shared Responsibility Model in cloud computing?

The Shared Responsibility Model divides security responsibilities between the cloud provider (managing infrastructure security) and the customer (securing data, applications, and access controls).

---

92. How do public, private, and hybrid clouds differ?

- **Public cloud:** Shared infrastructure managed by a third party.
- **Private cloud:** Exclusive infrastructure for a single organization.
- **Hybrid cloud:** Combines public and private clouds for flexibility.

TOP 100 INTERVIEW QUESTIONS PART 2

93. What are common cloud security risks?

Common risks include data breaches, misconfigurations, insecure APIs, insufficient access controls, and lack of visibility into cloud environments.

---

94. How does encryption contribute to cloud security?

Encryption protects data in the cloud by converting it into an unreadable format, ensuring that only authorized parties with the decryption key can access it.

---

95. What is a Cloud Access Security Broker (CASB)?

A CASB acts as a security intermediary between users and cloud services, enforcing policies, monitoring activities, and protecting sensitive data in cloud environments.

---

96. What is the Zero Trust security model?

Zero Trust assumes no user or device is trusted by default, requiring continuous verification of identities and strict access controls regardless of location.

---

97. What are the principles of cloud security?

Cloud security principles include identity and access management, data protection, continuous monitoring, compliance, and risk management.

---

98. Why is container security important?

Container security protects containerized applications by securing container images, monitoring runtime activities, and enforcing security policies, preventing exploitation of vulnerabilities.

TOP 100 INTERVIEW QUESTIONS PART 2

99. How do you secure APIs in the cloud?

Secure APIs by implementing encryption (SSL/TLS), authentication (OAuth, API keys), input validation, rate limiting, and logging, along with regular testing for vulnerabilities.

---

100. What is cloud incident response, and how does it differ from traditional incident response?

Cloud incident response focuses on addressing security incidents in cloud environments, requiring collaboration with cloud providers and managing incidents across virtualized, distributed systems.

DID YOU FIND THIS DOCUMENT USEFUL

WWW.MINISTRYOFSECURITY.CO

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS