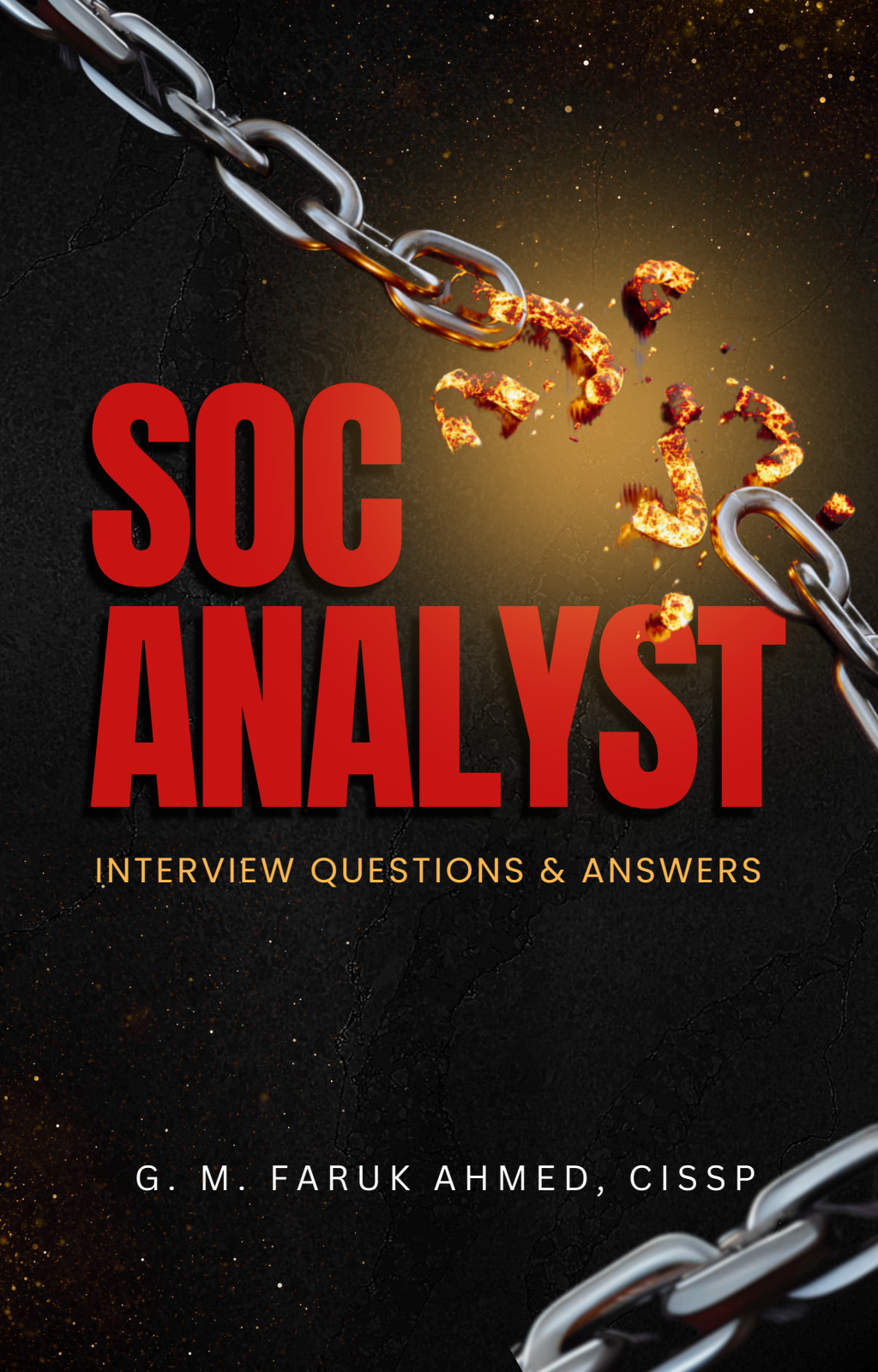
SOC
ANALYST
INTERVIEW QUESTIONS & ANSWERS
G. M. FARUK AHMED, CISSP

SOC ANALYST

INTERVIEW QUESTIONS & ANSWERS

Category - Cyber Attacks

Prepared by: G. M. Faruk Ahmed, CISSP

What are TTPs?

TTPs stand for Tactics, Techniques, and Procedures. These are patterns of activities or methods associated with a specific threat actor or group of threat actors.

Explain Brute-force attack.

Brute-force is a password guessing attack that tries various combinations of user names and passwords repeatedly until successful.

Mitigation:

- Encourage users to use complex passwords.
- Lock accounts after a limited number of failed attempts.
- Use Captcha to slow down brute-force attempts.
- Implement multifactor authentication.

Explain Dictionary attack.

A Dictionary attack is a type of brute-force attack that uses a pre-defined list of potential passwords (a "dictionary"). It can be personalized using target-specific information like date of birth or names.

Mitigation:

- Advise users against using simple, easily identifiable passwords.
- Lock accounts after a set number of attempts.
- Implement multifactor authentication.

Explain Rainbow attack.

A Rainbow attack uses precomputed password hashes instead of trying plaintext passwords.

Mitigation:

- Use salt techniques (add random data to the hash function).
- Lock accounts after a certain number of failed attempts.
- Implement multifactor authentication.

What is Pass-the-hash attack?

This technique allows an attacker to authenticate to a server using a password hash instead of the plaintext password.

Mitigation:

- Restrict and protect high-privileged domain accounts.
- Limit local accounts with administrative privileges.
- Restrict inbound traffic using firewalls.

What is Scanning?

Scanning is a method for discovering exploitable communication channels, such as open ports or known vulnerabilities.

Mitigation:

- Use firewalls and intrusion prevention systems (IPS).
- Perform OS hardening.
- Deploy honey pots to detect scanning activities.

Explain Sniffing Attack.

Sniffing involves intercepting data by capturing network traffic as it flows through a computer network.

Mitigation:

- Avoid insecure protocols like HTTP; use HTTPS, SFTP, or SSH.
- Encrypt data during transmission.

Explain Phishing.

Phishing is a cyber attack that uses disguised emails to trick users in to revealing sensitive information or downloading malware.

Mitigation:

- Educate users.
- Implement email security solutions.
- Use DMARC for email authentication.

Explain Spear Phishing and Whaling.

- Spear Phishing: A targeted email scam personalized for a specific individual or organization.
- Whaling: A phishing attack targeting high-level executives or important individuals.

What is an exploit and payload?

- Exploit: A tool or method that takes advantage of vulnerability.
- Payload: The part of the malware that causes harm, such as deleting files or encrypting data.

Explain Vishing.

Vishing is similar to phishing but conducted over the phone to trick victims into divulging sensitive information.

What is Spoofing?

Spoofing deceives systems or users by impersonating another entity, such as IP, MAC address, or email.

Mitigation:

- Deploy IPS.
- Educate users.
- Enable port-level security.

Explain DOS and DDOS attack.

- DOS: Denial-of-Service attack disrupts services by overwhelming a machine or network.
- DDOS: Distributed Denial-of-Service involves multiple systems launching a DOS attack simultaneously.

Mitigation:

- Use anti-DDOS technology.
- Deploy load balancers.
- Limit connection rates.

Explain ARP poisoning.

Also known as ARP spoofing, this attack links the attacker's MAC address to a legitimate IP address.

Mitigation:

- Use static ARP.

- Detect ARP poisoning with tools like XARP.

Explain MITM attack.

A Man-in-the-Middle attack intercepts and alters communications between two parties.

Mitigation:

- Use encryption.

- Deploy IPS.

For a complete guide with more questions and answers, contact:

G. M. Faruk Ahmed, CISSP

Cybersecurity Careers for Everyone

farukiu@gmail.com | +8801985269902 | www.gmfaruk.com