Unit 4: Breach Analysis and Mitigation

1. Describe a typical breach attack.

The cyber kill chain is a fundamental framework that delineates the distinct stages of a cyberattack, ranging from the initial reconnaissance phase to the final data exfiltration step. This framework is especially vital when thwarting complex cybersecurity threats such as APTs, ransomware, and security breaches. While initially based on a military model, the cyber kill chain has since evolved significantly to account for a broad spectrum of risks, including insider threats, social engineering, advanced ransomware, and novel attack vectors (Hospelhorn, 2016).

Huang et al. (2023) state that cybersecurity breaches are prevalent in today's digital landscape, and their impact can devastate organisations.

A typical breach attack follows a sequential pattern involving surveillance, intrusion, exploitation, privilege escalation, lateral movement, obfuscation / anti-forensics, denial of service, and exfiltration, as highlighted by Hospelhorn (2016).

Below is a resume of a typical breach attack:

- **Reconnaissance:** Attackers gather information about the target organisation's networks, systems, and vulnerabilities to identify potential entry points. This may involve scanning for open ports, identifying commonly used software, and searching for public data leaks.

- **Intrusion:** Once the attacker has identified a vulnerability, they attempt to access the target network. Standard methods include exploiting known software vulnerabilities, using phishing emails to distribute malware, or brute-forcing weak passwords.

- **Lateral Movement:** Once inside the network, attackers seek to expand their access by moving laterally to other systems and gaining privileges. This allows them to steal sensitive data, install additional malware, and disrupt operations.

- **Exfiltration:** The ultimate goal of an attack is to exfiltrate sensitive data, such as financial information, customer records, or intellectual property. This data may be encrypted or compressed for secure transfer to the attacker's control.

2. Suggest suitable mitigations against typical attacks.

All individuals, including IT staff and end users, must take part in preventing data breaches. A system's weakest link is its security, and every user who engages with it has the potential to introduce weakness. It is advised to adhere to best practices to prevent data breaches, including software patching and updates, the use of high-grade encryption, device upgrades, enforcement of Bring Your Own Device (BYOD) security policies, implementation of multi-factor authentication and strong credentials, and training of staff on best security practices (Kaspersky, 2022).

To effectively protect against cyberattacks, organisations should implement a comprehensive cybersecurity strategy, as the National Cyber Security Centre (2018) suggests that includes:

- **Vulnerability Management:** Apply patches or mitigations as soon as possible after regularly scanning systems and networks for known vulnerabilities.
- **Access Controls:** Apply strict access controls, such as minor privilege guidelines, user authentication, and authorisation.
- **Data Security:** Safeguard confidential information when used, transferred, and at rest. Implement access controls, encryption, and data loss prevention (DLP) strategies.
- **Phishing Awareness:** Inform staff members about phishing attempts and train them to see and steer clear of them.

3. Evaluate and select appropriate tools from the Kali Linux distribution.

Devlesaver, J. C. (2023) notes that Kali Linux is a Linux distribution for Security Auditing and Penetration Testing. With over 600 penetration tools, it is highly customisable and free. It offers multi-language support and extensive wireless device support. Developed in a secure environment, it is an indispensable tool for security professionals.

Kali Linux offers a range of powerful tools for network security assessment (Mohammed, 2023). Some of the ten most commonly used Kali Linux tools for breach analysis and mitigation include:

- **Fluxion** identifies Wi-Fi vulnerabilities using social engineering tactics.
- **John the Ripper** cracks hashed passwords.
- **Lynis** scans Linux-based systems for vulnerabilities and security issues.
- **Metasploit** exploits system vulnerabilities and conducts penetration testing.
- **Nikto** scans web servers for potential vulnerabilities.
- **Nmap** identifies hosts and services on a network.
- **Skipfish** focuses on web application security.
- **Social Engineering Toolkit (SET)** facilitates ethical hacking engagements that involve social engineering tactics.
- **OpenVAS** identifies security weaknesses in systems, applications, and networks.
- **Snort** analyses network traffic for malicious activities.

References:

- Hospelhorn, S. (2016). *What is The Cyber Kill Chain and How to Use it Effectively | Varonis*. [online] www.varonis.com. Available at: https://www.varonis.com/blog/cyber-kill-chain.
- Huang, K., Wang, X., Wei, W. & Madnick, S. (2023). *The Devastating Business Impacts of a Cyber Breach*. [online] Harvard Business Review. Available at: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.
- Kaspersky (2022). *How Data Breaches Happen*. [online] Kaspersky. Available at: https://www.kaspersky.com/resource-center/definitions/data-breach.
- National Cyber Security Centre (2018). *Phishing attacks: defending your organisation*. [online] NCSC.gov.uk. Available at: https://www.ncsc.gov.uk/guidance/phishing.
- Devlesaver, J. C. (2023). *Kali Linux | Digital Skills and Jobs Platform*. [online] Available at: https://digital-skills-jobs.europa.eu/en/inspiration/resources/kali-linux-most-advanced-penetration-testing-distribution [Accessed 16 Dec. 2023].
- Mohammed (2023). *Understanding the Benefits of Using Kali Linux for Penetration Testing*. [online] Medium. Available at: https://medium.com/@techlatest.net/understanding-the-benefits-of-using-kali-linux-for-penetration-testing-bfc89b8fab39.