Unit 1: History of Network Security, Vulnerabilities and Approaches

1. Explain the origins of a number of common attacks.

The history of cybersecurity can be traced back to the seventies. In 1971, Bob Thomas created the first-ever computer worm. Robert Morris launched the first DoS attack in 1988. The first ransomware attack took place in 1989. 1990, the Computer Misuse Act was passed, making unauthorised attempts to access computer systems illegal. In 1999, Windows 98 brought accessibility to non-specialists. The ILOVEYOU worm caused damage in the new millennium. The Department of Homeland Security was created in 2002. Anonymous, the most iconic group of hackers worldwide, was started in 2003 (Townsend, 2019).

Today, enhancing network security is a crucial objective for businesses and organisations. The significance of network security was realised in the 1950s when the value of data was acknowledged. The rise of digital storage in the late 1960s and early 1970s allowed access to data through direct plugging into the mainframe or accessing it from terminals within the building. However, data emerged as a valuable commodity within a decade, and security measures were adapted to protect it. These early stages marked the beginning of network security's future as the data revolution continued to drive changes in security strategies (Avast, N.D.).

Moreover, network security has been a concern since networked computers' advent, as Radware (N.D.) highlighted. During the '70s and '80s, researchers exposed security flaws in the ARPANET, the predecessor of the present-day internet. With the surge of network usage in the late '80s, the need for security increased rapidly. The first automated worm surfaced on the ARPANET in 1988, exposing the vulnerabilities of networked computers and causing influential leaders in the network to develop security methods to counter network threats.

Cybercrime is a rapidly growing industry, with organisations offering technical leadership and step-by-step instructions via ransomware-as-a-service. Its history goes back to 1834 and has evolved. Notable cyber-attacks include the MIT computer network breach in 1962, the first computer virus in 1971, and the first significant cyber-attack on the internet in 1988. Cybercrime increased in the 1990s with the birth of the internet, and in the new millennium, APTs sponsored by nation-states caused significant damage. Major cyber-attacks include Operation Aurora in 2010, Sony's PlayStation Network hack in 2011, and the Snowden revelations in 2013. From 2020 to 2022, several high-profile cyberattacks resulted in billions of dollars in losses (Wolf, 2020).

Cyber-attacks have been around for a long time, and many of them have their roots in the past. An example of this is the Denial-of-service (DoS) attacks, which date back to the early days of the Internet. In a DoS attack, an attacker floods a target with traffic, making it unavailable to legitimate users. One of the most premature documented DoS attacks occurred in 1988 when a hacker launched a worm that caused thousands of computers on the internet to crash (Townsend, 2019).

SQL injection attacks are another common type of attack. In an SQL injection attack, an attacker exploits vulnerabilities in a web application's database to insert malicious code. This code can then steal, modify, or even control the database. The first known SQL injection attack was in 1998 (Yasar et al. N.D).

Cross-site scripting (XSS) attacks are also widespread. In an XSS attack, an attacker injects malicious code into a web page. When a victim visits the page, the code is executed in their browser, which can give the attacker control of the victim's session (Kirsten, 2020).

Phishing attacks are a type of social engineering attack. In a phishing attack, an attacker sends an email or text message that appears to be from a legitimate source, such as a bank or credit card company. The email or text message often links to a malicious website or asks the victim to enter their personal information. The first known phishing attack was in 1996 (Spiceworks, N.D.).

2. Recommend a best practice approach to mitigate attacks.

Internet access poses many risks to business activities. Creating a security policy requires balancing services with controlling access to functions and data. Security is more difficult with networking computers, as the communication channel is open to attack. Understanding the risks imposed by each service you use or provide is critical to determining clear security objectives. Some typical security risks include passive and active attacks, which can be challenging to detect. Active attacks may consist of system access attempts, spoofing attacks, denial of service attacks, and cryptographic attacks (IBM, 2021).

According to IMI (2023), implementing a layered security approach is considered best practice to mitigate attacks. This approach employs multiple security measures within a system or network at different levels, providing extra protection and addressing various threats. By implementing multiple layers of security, organisations can create a more secure environment for their assets, data, and systems, ultimately reducing the risk of a successful cyber-attack or security breach. In a security breach, a layered security model provides additional layers of defence to help contain the damage and limit the attack's impact. This model allows organisations to select control measures based on their needs, risks, and budgets. Standard security controls include firewalls,

intrusion detection and prevention systems, anti-virus software, web application firewalls, endpoint security solutions, and security awareness training.

By implementing a layered security approach, organisations can effectively control network access, detect and remove malicious activity, and safeguard their devices against malware and other threats. Additionally, providing security awareness training to employees can help them recognise and avoid phishing attacks and other social engineering scams.

3. Discuss a number of modern protection techniques.

Effectively managing IT risks is crucial for every organisation. It requires careful identification of potential adverse outcomes from IT failure or misuse, a thorough cybersecurity risk assessment, and a comprehensive plan to guide risk response strategies. Additionally, constant monitoring of the IT environment is critical to ensure that internal controls remain aligned with IT risks. As we all know, change is a constant in today's world, and it is imperative to maintain continuous vigilance in monitoring the environment (Knowles, 2021).

According to the National Cyber Security Centre (2021), prioritising system security is vital to protect sensitive data. It is essential to keep software up-to-date, opt for managed services from reputable vendors, and establish a vulnerability management process. A layered approach with secure product configuration, planning for DoS attacks, and seeking independent validation for critical controls is necessary. To reduce the impact of compromise, lateral movement should be prevented, and recovery processes should be made more accessible. Detecting and investigating settlements should be easy by using clearly defined communication methods,

restricting flows, and collecting logs. Lastly, secure development and deployment processes, restricting administrative interface access, and protecting sensitive data with encryption and backups are crucial.

In addition to traditional security controls, modern protection techniques include micro-segmentation, zero-trust security, security automation, and orchestration solutions.

References:

- Avast (N.D.). *The history and evolution of network security | Avast*. [online] Available at: https://www.avast.com/en-gb/business/resources/future-of-network-security [Accessed 9 Nov. 2023].
- Radware (N.D.). *History of Network Security Methods | Radware Security*. [online] Available at: https://www.radware.com/resources/network_security_history.aspx/.
- Wolf, A. (2020). *The Fascinating Decade in Cybercrime: 2010-2020*. [online] Arctic Wolf. Available at: https://arcticwolf.com/resources/blog/decade-of-cybercrime/.
- Townsend, C. (2019). *Cyber Security Summit New York 2019*. [online] United States Cybersecurity Magazine. Available at: https://www.uscybersecurity.net/history/.
- Yasar, K., Terrell, H. & Lewis, S. (N.D.). *What is SQL injection?* [online] Available at: https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.
- Kirsten, S. (2020). *Cross Site Scripting (XSS) | OWASP*. [online] Owasp.org. Available at: https://owasp.org/www-community/attacks/xss/.
- Spiceworks (N.D.). *What Is a Spear Phishing Attack? Definition, Process, and Prevention Best Practices*. [online] Available at: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-a-spear-phishing-attack/.
- IBM (2021). *The layered defense approach to security*. [online] www.ibm.com. Available at: https://www.ibm.com/docs/en/i/7.3?topic=security-layered-defense-approach.
- IMI (2023). *Layered Security Model*. [online] Identity Management Institute®. Available at: https://identitymanagementinstitute.org/layered-security-model [Accessed 9 Nov. 2023].
- Knowles, M. (2021). *Cybersecurity Risk Management: Frameworks, Plans, & Best Practices*. [online] Hyperproof. Available at: https://hyperproof.io/resource/cybersecurity-risk-management-process/.
- National Cyber Security Centre (2021). *10 Steps to Cyber Security*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/collection/10-steps.