Unit 3 - DIGITAL DEVICES SECURITY Assignment Questions.

Syllabus:

Device and Mobile Security: End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third-party software, Device security policy.

Tools and Technologies for Cyber Security: Authentication tools, firewalls, intrusion detection systems, and antivirus and encryption software.

Cyber Security Best Practices: Cyber Security best practices, Significance of host firewall and Anti-virus, Managementof host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.

Device and Mobile Security:

1Q. Essay Question:

Explore the importance of device and mobile security in today's digital landscape. Discuss the various threats and vulnerabilities faced by mobile devices, including malware, phishing attacks, and data breaches. Explain the significance of implementing security measures such as encryption, biometric authentication, and secure boot processes to protect against these threats. Additionally, analyze the role of user education and awareness in enhancing device security. Provide examples of best practices and case studies to illustrate effective strategies for mitigating risks to mobile and IoT devices.

(OR)

Research Question:

Conduct a comparative analysis of different mobile operating systems (e.g., Android, iOS) in terms of their security features and vulnerabilities. Investigate the security architectures, patching mechanisms, and app permission models employed by each operating system to protect user data and privacy. Evaluate the effectiveness of these security measures in mitigating common threats such as malware, unauthorized access, and data leakage. Furthermore, examine the impact of device fragmentation and software update practices on the overall security posture of mobile ecosystems. Based on your analysis, propose recommendations for improving the security of mobile devices across different platforms.

Tools and Technologies for Cyber Security:

1Q. Case Study Question:

Select a recent cyberattack incident and analyze the tools and technologies that were utilized by the attackers. Describe the attack vector, the tools employed (e.g., malware, penetration testing frameworks, exploit kits), and the techniques used to exploit vulnerabilities. Evaluate the effectiveness of the defensive measures in place at the targeted organization and assess the lessons learned from the incident. Based on your analysis, propose recommendations for enhancing the organization's cybersecurity posture, including the adoption of specific tools and technologies to prevent similar attacks in the future.

(OR)

Research Question:

Investigate and compare different categories of cybersecurity tools and technologies used for threat detection, prevention, and incident response. Choose three categories (e.g., antivirus software, intrusion detection systems, threat intelligence platforms) and analyze the key features, functionalities, and deployment considerations for each category. Evaluate the strengths and limitations of popular tools within each category, considering factors such as scalability, ease of use, and integration capabilities. Finally, discuss emerging trends in cybersecurity technology, such

as artificial intelligence and machine learning, and their potential impact on the effectiveness of cyber defense strategies.

Cyber Security Best Practices:

1Q. Policy Development Question:

Imagine you are tasked with developing a comprehensive cyber security policy for a medium-sized organization. Outline the key components that should be included in the policy, such as access control, data protection, incident response, and employee training. Discuss the importance of each component and provide examples of specific policies or procedures that could be implemented to mitigate cyber security risks. Additionally, address the challenges of policy enforcement and compliance monitoring within the organization. Finally, propose strategies for ensuring the ongoing effectiveness of the cyber security policy in the face of evolving threats and technologies.

(OR)

Scenario-Based Analysis Question:

Analyze a hypothetical cyber security incident scenario and develop a set of best practices for preventing, detecting, and responding to such incidents. Describe the incident scenario, including the type of attack, the target system or data, and the potential impact on the organization. Based on the scenario, identify the key steps that should be taken by the organization to mitigate the immediate threat and minimize the impact on operations. Additionally, outline proactive measures that could have been implemented beforehand to prevent or mitigate the incident. Finally, discuss the importance of continuous monitoring, incident response planning, and post-incident analysis in improving cyber security resilience.