ECMM464: Security Assessment and Validation

Continuous Assessment

Saif Alzubi

Due date: Wednesday 6th March 2024

CA Mark: This CA weights 40% of your final mark.

Format of Submission: Please submit your answers in a single PDF file via ELE by **Wednesday 6th of March 2024 at 12 pm (midday)**

Referencing and Academic Conduct: This CA is an individual assessment and must be completed independently. Any discussions about the CA answers or methods for obtaining them are not allowed. You are required to cite any sources used in your solution and include a list of references. Additionally, you must avoid plagiarism, collusion and any academic misconduct behaviours.

Guidance for Report Content: The answers should include a comprehensive technical analysis and detailed explanations.

Question 1

You are the lead cybersecurity analyst at ABC, a software development company that holds personal client data. Recently, you have been informed of unusual network activity. Initial investigations suggest a combination of packet sniffing and spoofing attacks. The attackers are believed to be using packet sniffing to intercept and analyse network traffic, gathering information about network protocols and data flow. Concurrently, the attackers appear to be employing IP spoofing to masquerade as legitimate network entities, bypassing security measures to gain unauthorised access to the clients' data.

The network infrastructure at ABC is designed to balance functionality with security. It encompasses a blend of wired and wireless connections across various access points, facilitated through a sophisticated arrangement of routers (Cisco ISR 4000 Series), switches (Cisco Catalyst 3650 Series for distribution layers and Cisco Catalyst 1000 Series at access points), and a diverse array of end-point devices. These include servers running on Red Hat Linux 7 for critical web services, a PostgreSQL database hosted on a Red Hat Linux 5 server for storing sensitive client information, and a MySQL database for operational data. Employee workstations predominantly run on Windows 10 and macOS for development teams, all connecting through a network that supports both Ethernet and Wi-Fi (802.11ac standard) technologies.

For remote connections, the company employs OpenVPN solutions, ensuring that employees working from outside the office maintain secure access to the internal network. Despite these precautions, the existing security measures, including firewalls configured to allow FTP traffic and remote desktop services via TCP port 3389, and network monitoring through Intrusion Detection Systems (IDS), have proven insufficient against the current sophisticated attack vectors. Notably, the firewall's rule to allow FTP traffic and the reliance on single-factor authentication for remote desktop (RDP), SSH, and Telnet logins have exposed vulnerabilities in the system.

Your task is to understand the depth and impact of these attacks, strengthen network security, and develop strategies to prevent future incidents.

(a) Given the complexity of the attack, how would you accurately identify and examine the combination of packet sniffing and IP spoofing activities? Consider the tools, methodologies, and specific network data you would examine.

(8 marks)

(b) What immediate mitigation strategies would you implement to counter the current attack, and what long-term prevention measures would you advise to defend against similar threats in the future?

(8 marks)

(c) How would you assess the impact of these combined attacks on ABC's operations and sensitive data?

(6 marks)

(Total 22 marks)

Question 2

(a) You're leading the Cybersecurity Incident Response Team at GlobalTech Solutions, a big company that specialises in software development and data analysis. The company has a large and complex computer network that supports many essential tasks, from managing money transactions to keeping client information safe and developing and designing new software. This network is spread out across the world, including headquarters in London, research facilities in Paris and Berlin, and multiple offices worldwide, making it a prime target for cyber attacks.

Infrastructure Overview

Servers and Operating Systems: At the core of GlobalTech's operations are servers running Windows Server 2019, responsible for managing critical applications like the company's custom financial transaction processing system and client data management platform. Complementing these are Linux servers (Ubuntu 20.04 and Red Hat Enterprise Linux 8), hosting web services that include the company's customer portal, internal databases utilising PostgreSQL for transaction records, and MongoDB for data analytics workloads. These Linux servers also facilitate cloud connectivity and are integrated with AWS for additional compute resources and data storage solutions.

Workstations and User Environment: Employees mainly use Windows 10 OS, provided with Microsoft Office for day-to-day work, Linux for the development teams featuring tools like Git and Docker, and macOS for the marketing departments.

Network Security and Segmentation: The network is architecturally designed for resilience and security, segmented into VLANs to isolate sensitive information — financial operations are conducted in a VLAN with enhanced security protocols, R&D activities in another with restricted access controls, and client data storage in yet another, safeguarded by encryption. The segmentation is reinforced by robust Cisco ASA firewalls, complemented by Palo Alto Networks NGFWs, providing intrusion prevention and malware detection capabilities.

Monitoring and Incident Detection: Snort-based IDS/IPS systems monitor network traffic for signs of intrusion within these VLANs, with anomalies flagged and escalated through a sophisticated SIEM (Security Information and Event Management) system. This system gathers logs from across the infrastructure, providing real-time alerting for rapid response.

Incident Overview

Recently, the team noticed some unusual activity in the network that looked like a hybrid malware attack. The attack was a combination of a virus, rootkit

and a worm.

Infection Vector: The entry point identified was a spear-phishing email sent to an employee in the finance department, which bypassed security defences to deliver a payload that exploits zero-day vulnerabilities within the network's software environment.

The complexity of the hybrid malware encountered presents a unique set of challenges:

Evasion Techniques: The malware's ability to bypass traditional antivirus solutions suggests the use of polymorphic code, making it difficult to detect based on signatures alone.

Propagation Mechanism: The worm component seeks out other hosts on the network, leveraging protocols such as SMB for lateral movement.

Persistence and Stealth: The rootkit component employs kernel-level hooks to hide its presence from system monitoring tools, complicating its detection and removal.

Data Corruption: The virus component actively targets and corrupts files related to critical applications and databases, employing ransomware-like tactics to encrypt data for potential financial extortion.

As the Incident Response Team Lead, your primary objectives are to stop further propagation of the hybrid malware and mitigate its ongoing impact. Following this, locate and eliminate the malware from your systems. Next, address and fix any disruptions or damages incurred as a result of the attack. Finally, a critical evaluation of the incident's origins and analysis of exploited vulnerabilities, including the development and implementation of enhanced defensive measures, ensuring the organisation's cybersecurity measures are strengthened against future incidents.

(i) What are the (immediate) steps you would take upon identifying this malware infection?

(6 marks)

(ii) How would you go about identifying and removing each component (Virus, Worm, Rootkit) of the malware?

(6 marks)

(iii) What steps would you take for post-incident analysis and to prevent future infections of a similar nature?

(6 marks)

(b) Researchers have identified a new security risk that takes advantage of remote learning to launch an attack from a teacher's computer. The attack was initiated by a group named "employer21". They email a fake assignment to a teacher. The assignment contains macros that, when activated, will download and run malicious software. This software encrypts files on the victim's computer. A notice then opens up demanding £500 in Bitcoin.

Name two social engineering attacks used here. Briefly provide the reasons behind your answer.

(10 marks)

(Total 28 marks)

Question 3

You are the Chief Network Security Officer at a multinational corporation with a complex network infrastructure across several locations. The network comprises both legacy and modern systems, crucial for real-time data exchanges between departments such as finance, R&D, and production.

The network architecture includes Linux servers for high-volume computational tasks in R&D, while the production department uses legacy systems on outdated Windows versions due to specific legacy application dependencies. The finance department relies on high-speed, fault-tolerant UNIX servers, ensuring maximum uptime and secure transactions.

The underlying network infrastructure includes a number of high-capacity Cisco routers and switches. These devices are configured to manage VLANs and enhance security and performance. The routers, operating on IOS-XE, employ advanced routing protocols to ensure data packets find the most efficient path across international offices.

The network security system consists of next-gen firewalls and intrusion detection systems (IDS) that monitor traffic for malicious activity, with their logs analysed by a centralised Security Information and Event Management (SIEM) system. Despite these security measures, the network's diversity introduces unique challenges in detecting and mitigating sophisticated attacks.

Recently, you were notified of network disruptions emerging across different departments. The finance department encounters delays in processing transactions, R&D complains of access issues to their data servers, and the production line experiences unusual system behaviour. Further investigation revealed abnormal network traffic patterns, including suspicious ARP (Address Resolution Protocol) broadcasts. This raises your suspicion of a potential ARP cache poisoning attack.

The investigation showed that the attack originated across multiple network segments, indicating the attackers' knowledge of the network layout and systems. The attackers exploited specific ports open for inter-departmental communications, such as Port 22 for SSH access to Linux servers in R&D and Port 445 for SMB traffic to Windows servers in the production department, to launch their attack.

Given the critical nature of the affected systems and the sophistication of the attack, you must approach this situation with a comprehensive strategy that encompasses immediate response, in-depth forensic analysis, and long-term prevention measures. Based on the given scenario, answer the below questions:

(a) Considering the complexity and scale of the network, outline the forensic analysis steps you would take to trace the source(s) of the ARP cache poisoning. How would you go about attributing the attack to specific actors or devices within such a mixed network?

(8 marks)

(b) What immediate response and containment strategies would you deploy, considering the network's mix of legacy and modern systems? How would you ensure that these strategies are effective across such a mixed technological landscape without causing further operational disruptions?

(8 marks)

(c) What long-term strategic changes would you recommend to the company's network infrastructure and policies to strengthen security against similar future attacks?

(6 marks)

(Total 22 marks)

Question 4

ECMM464 Inc., a leading technology corporation with a vast global presence specialising in cloud computing services, international e-commerce, and a suite of internal communication tools, recently suffered from a Domain Name System (DNS) infrastructure disruption

The problem surfaced when the company's primary DNS servers became the target of sophisticated Distributed Denial of Service (DDoS) attacks. The attacks caused periodic and significant downtimes, particularly impacting the e-commerce platform and leading to substantial financial losses and reputational damage. The DDoS attacks not only consumed the network resources but also exposed the inadequacy of existing security mechanisms to such attacks.

Following the attack, There were reports from users across different international branches who encountered abnormal website redirections when attempting to access internal web resources. These redirections led to either phishing websites or dead links. Therefore, ECMM464 Inc. hired your cybersecurity firm to investigate and resolve the issues.

The Cyber Security team started an investigation and observed a surge in DNS traffic characterised by unusually high query rates and strange query patterns, indicating of a DNS amplification attack.

The Security team's further investigation also uncovered multiple other issues affecting their DNS infrastructure. Firstly, DNS hijacking was identified, where several DNS records had been maliciously altered to redirect traffic to malicious websites, which indicated that there was a breach of the DNS management system settings. Simultaneously, instances of DNS cache poisoning were detected across several servers, which led to users receiving incorrect domain resolution results, guiding them to potentially malicious websites.

The investigation also revealed significant misconfigurations in multiple internal DNS servers. These misconfigurations contributed to resolution delays and occasional failures.

Based on the complex DNS attack at ECMM464 Inc., answer the below questions

(a) Considering the DDoS attacks and the need for a resilient DNS infrastructure, what should be ECMM464 Inc.'s long-term strategy for DNS resilience?

(6 marks)

(b) Given the DNS hijacking that occurred, what specific countermeasures should ECMM464 Inc. implement to prevent future hijacking incidents?

(8 marks)

(c) In light of the DNS cache poisoning, what strategies should ECMM464 Inc. adopt to mitigate such attacks?

(8 marks)

(d) How should ECMM464 Inc. address the internal DNS misconfigurations to improve the reliability and security of their DNS infrastructure?

(6 marks)

(Total 28 marks)

Table 1: Marking Scheme

Marking Scheme	Description	Mark
Theoretical Knowledge	- Demonstrates a comprehensive understanding of core cybersecurity concepts, principles, and theories. - Shows an ability to interpret and relate these concepts accurately to real-world scenarios. - Demonstrates an understanding of the evolving nature of cybersecurity threats and defences. Including emerging threats and the latest defence mechanisms.	15%
Scenario Analysis	- Applies theoretical knowledge to analyse the given cybersecurity scenario effectively. - Identifies potential threats, vulnerabilities, and the broader implications of cybersecurity measures.	20%
Solution Design	- Focuses on conceptualising and justifying cybersecurity solutions derived from scenario analysis. - Emphasises the feasibility and practicality of proposed solutions in addressing identified issues.	25%
Technical Solution	- Demonstrates proficiency in implementing proposed cybersecurity solutions. - Provides detailed insights into the technical aspects and methodologies utilised for solution execution.	25%
Clarity and Structure of Writing	- Presents ideas in a clear, structured, and coherent manner. - Ensures the report is well-organised, facilitating easy comprehension. - Technical information is presented in an accessible manner to the intended audience. - Employs evidence and logical reasoning to support arguments.	15%