GROUP TASK :2
OS LAYER 5

A Brief Overview

2

1:Nikki Mariya Wilson
2:Swathi

Analyze a real-world case study of an attack on Layer 5 (session Layer) of the OSI model

SESSION LAYER

The session layer establishes communication channels between devices, known as sessions. It starts sessions, keeps them open and effective while data is transferred, and closes them after communication is completed. Hijacking is one of the common security attacks that occurs in this layer.

Attack: Hijacking

Hijacking in the session layer occurs when an attacker intercepts and takes control of an established communication session between two parties. This can be carried out by exploiting vulnerabilities in the protocol used to establish the session or using the tools to intercept and manipulate network traffic. Once the attackers hijack the session, they can access sensitive information or gain unauthorized access.

two types of session hijacking:

□ Active session hijacking: In this, the attacker takes control of an active user session on a network and intercepts and alters network traffic in real time.

□ Passive session hijacking: In this, attackers monitor network traffic and wait for users to log into a website; at that point, the attackers take over the session.

CASE STUDY

News about CircleCI being a target of a cybersecurity hack surfaced in the first week of January, warning customers to rotate their secrets and review internal system logs for suspicious activities. CircleCI said it was detected after a customer reported unauthorised system access in their GitHub OAuth token.

After the initial investigation, the software company revealed that one of their engineers was infected by an infostealer malware, resulting in the theft of a corporate session cookie. This stolen session allowed the hacker to access the engineer’s corporate computer without having to authenticate via 2FA.

The CircleCI hack was completed after the threat actors abused the stolen session cookie and escalated their access inside the corporate network.

According to the latest released incident report of CircleCI concerning the hack, they explained that the threat actors had escalated their admin access to a subset of the company’s production systems after successfully leveraging the hijacked session cookie.
On December 22, the hackers started collecting valuable data from CircleCI’s databases, including customers’ tokens, keys, and environment variables. Moreover,

the hackers also stole encryption keys that allowed them to decrypt several encrypted corporate data.
Thus, all customers are immediately warned and instructed to rotate their secrets and tokens, especially if they logged in to their accounts between December 21, 2022, and January 4, 2023. CircleCI also automatically rotated all customer-associated tokens and teamed up with Atlassian and AWS to alert their respective clients of possible BitBucket and AWS tokens compromise..

As a part of the software company’s abundance of caution, they implemented additional detection mechanisms against infostealer malware, restricted access to production systems to a smaller group of authorised personnel, and heightened their 2FA implementation security.

Security researchers are concerned about the increasing attacks involving MFAs. These MFA bypassing campaigns are mostly geared towards corporate credential theft, whether launched through malware or phishing.

While MFA implementation is crucial for a company’s cybersecurity, hackers have somehow acquired methods to bypass them. Stealing session cookies and MFA Fatigue attacks are two of the most common tactics hackers use to gain access to corporate systems. Some notable breach incidents related to this campaign were launched on Microsoft, Uber, Cisco, and CircleCI.

Analysts believe that even if MFA is activated in a corporate system, it still needs to be properly configured to detect malicious access on a session cookie. Requesting additional MFA validation is also recommended.

Impact and Consequences:

- Data Breach: The attacker gains access to sensitive information transmitted during active sessions, including confidential documents, trade secrets, and customer data. This breach leads to compromised privacy, potential legal ramifications, and damage to the company's reputation.

- Disruption of Operations: By hijacking sessions, the attacker disrupts critical communication channels. This can lead to delays in decision-making, breakdowns in collaboration, and a loss of productivity for the affected employees.

- Malicious Activities: The attacker may abuse the compromised sessions to impersonate employees or inject malicious content, leading to further security incidents within the company's network environment.

Consequences of the attack:

The consequences of the undersea cable cut incident were widespread and varied. Some of the
major consequences include:

A)Unauthorized Access: Attackers may gain unauthorized access to active user sessions, allowing them to impersonate legitimate users and perform actions on their behalf. This can lead to unauthorized data access, manipulation, or unauthorized transactions.

B) Data Disclosure: If session encryption or other security measures are compromised, attackers may gain access to sensitive data transmitted during the session. This can result in data breaches, exposing confidential information such as personal data, financial details, or sensitive business information.

C) Data Manipulation: In some cases, attackers may manipulate the data transmitted within sessions. This can involve modifying or injecting malicious content, leading to unauthorized changes in data, unauthorized transactions, or the introduction of malware into the system. Service Disruption: Attacks targeting session-related functions can disrupt communication channels, leading to service disruptions or denial of service for legitimate users. This can impact productivity, interrupt critical business operations, and result in financial losses.

.

Countermeasures:

- Strong Session Authentication: Implement robust authentication mechanisms for session establishment, such as using strong passwords, multi-factor authentication, and certificate-based authentication. This ensures that only authorized individuals can initiate and participate in sessions.

- Encryption: Apply encryption techniques, such as SSL/TLS, to protect session data during transmission. This safeguards the confidentiality and integrity of the information exchanged, making it harder for attackers to intercept or manipulate session content.

- Session Monitoring: Employ session monitoring tools and intrusion detection systems to identify suspicious activity or abnormal behavior within sessions. This enables the timely detection and response to potential attacks, minimizing their impact.

- Session Timeout and Termination: Implement session timeout mechanisms to automatically terminate inactive sessions. This prevents unauthorized individuals from exploiting idle sessions and reduces the window of opportunity for session hijacking attacks.

- Intrusion Prevention Systems (IPS): Deploy IPS solutions that can analyze session traffic in real-time, detecting and blocking suspicious activities or known attack patterns. IPS can help identify session-based attacks and take proactive measures to mitigate them.

- Employee Awareness and Training: Conduct regular security awareness programs and training sessions to educate employees about the importance of session security, safe communication practices, and how to recognize and report potential session-related threats.

THANK YOU