Deakin University

Computer Networks and Security

OnTrack Submission

Protocols, Vulnerabilities, and Attacks

Submitted By:
Gloria Chemutai Kiplagat
s223452112
2024/06/04 08:07

Tutor:
Juhar Abdella

June 4, 2024

1. Identify the Protocol and Cyberattack

Protocol: Simple Mail Transfer Protocol (SMTP)
Cyberattack: SMTP Spoofing

2. Describe the Selected Protocol

Simple Mail Transfer Protocol (SMTP):

Layer in TCP/IP Model: Application Layer

Functionality: SMTP is a protocol used to send emails from one server to another. It facilitates the transmission of electronic mail across Internet Protocol (IP) networks.

3. Normal Operation of the Protocol Relevant to the Cyberattack

In normal operation, SMTP works as follows:

Client-Server Communication: An email client connects to an SMTP server using TCP (typically on port 25, 587, or 465).

Handshake: The client sends a HELO or EHLO command to the server to identify itself.

Mail Transactions:

The client specifies the sender's email address using the MAIL FROM command.

The client specifies the recipient's email address using the RCPT TO command.

The client sends the email data, including headers and body, using the DATA command.

Transmission: The SMTP server processes the email and forwards it to the recipient's email server if it is not the destination.

Delivery: The recipient's email server delivers the email to the recipient's mailbox.

4. Vulnerabilities in the Protocol

The primary vulnerability in SMTP that allows spoofing involves its lack of authentication mechanisms in its basic form:

No Sender Verification: SMTP does not inherently verify the sender's email address. The MAIL FROM command can be easily forged.

Plain Text Transmission: SMTP transmits data in plain text, making it susceptible to interception and manipulation.

5. Describe the Selected Cyberattack

SMTP Spoofing:

Mechanism: SMTP spoofing exploits the lack of sender verification in the SMTP protocol. An attacker sends an email with a forged sender address, making it appear as if it came from a legitimate source.

Vulnerability Exploitation: The attacker connects to an SMTP server and issues commands to send an email. By forging the sender's address in the MAIL FROM command, the email appears to come from a trusted source.

Potential Damage/Impacts:

Phishing Attacks: Spoofed emails can trick recipients into revealing sensitive information, such as login credentials or financial information.

Spread of Malware: Spoofed emails can contain malicious attachments or links, leading to the spread of malware.

Reputation Damage: Organizations can suffer reputational harm if their domain is used for spoofing attacks.

Financial Loss: Both individuals and organizations can incur financial losses due to fraudulent activities enabled by spoofed emails.