Project S9L5 - Network Traffic Analysis and Indicators of Compromise

Introduction

I present to you the report summarizing my analysis of a network capture file. During the investigation, I examined packets to identify potential **Indicators of Compromise (IOC)**. My goal was to detect signs of suspicious activity, hypothesize possible attack vectors, and propose actionable recommendations to mitigate risks and reduce the impact of potential attacks.

Indicators of Compromise (IOC)

As part of my analysis, I identified several IOC that suggest malicious behavior. Below, I outline the most significant findings:

Port Scanning

- I noticed a large number of TCP SYN requests originating from the IP address **192.168.200.100** and targeting **192.168.200.150**. These requests focused on commonly used service ports, such as:
    - **80 (HTTP):** Web traffic.
    - **443 (HTTPS):** Secure web communications.
    - **23 (Telnet):** Used for remote access.
    - **21 (FTP):** File transfer.
    - **22 (SSH):** Secure shell access.
    - Other less common ports.
- The systematic probing of ports strongly suggests **port scanning activity**, which is a known reconnaissance method used to identify open and exploitable services.

Unexpected Reset Responses

- In several cases, I observed that the target server (192.168.200.150) responded with **RST** (reset) or **RST, ACK** packets. This behavior might indicate:
    - The services being probed are inactive or rejecting unauthorized connection attempts.
    - The server detected the scanning behavior and is terminating the connections.

Suspicious ARP Traffic

- I also found an unusual sequence of **Address Resolution Protocol (ARP)** requests, such as "Who has...?" messages. While ARP traffic is typically normal, this rapid succession could indicate:
    - **ARP spoofing:** An attacker may be trying to manipulate ARP tables to redirect or intercept traffic.
    - This could be a precursor to a **Man-in-the-Middle (MITM)** attack.

These findings collectively indicate reconnaissance activity and potential attempts to exploit vulnerabilities in the network.

Hypotheses on Attack Vectors

Based on the IOC I identified, I hypothesize the following attack vectors:

Port Scanning

- It appears that the attacker (192.168.200.100) is performing a port scan to identify active and potentially vulnerable services on the target machine (192.168.200.150). This reconnaissance phase typically precedes exploitation attempts.

Remote Access Attempts

- The focus on ports such as **23 (Telnet)**, **21 (FTP)**, and **22 (SSH)** leads me to believe the attacker may be attempting to gain unauthorized access. These services are common targets for brute-force attacks, where attackers repeatedly try different username and password combinations.

Man-in-the-Middle (MITM)

- The observed ARP traffic suggests the attacker might be preparing for an MITM attack. By manipulating ARP tables, they could intercept or redirect network traffic, potentially leading to data theft or further exploitation.

Recommended Actions

To address these threats and prevent similar incidents in the future, I recommend the following measures:

Immediate Actions

Block the Attacker's IP Address:

- Configure the firewall to block all traffic from **192.168.200.100**.
- This action would immediately stop the ongoing reconnaissance activity.

Port Filtering:

- Close unused ports to reduce the attack surface.
- Restrict access to critical services like SSH, FTP, and Telnet to authorized IP addresses only.

Verify ARP Tables:

- Inspect the network's ARP tables and remove any unauthorized or suspicious entries.
- This will help counter potential ARP spoofing attacks.

Long-Term Actions

Strengthen Authentication:

- I suggest enforcing strong, complex passwords for services such as SSH, Telnet, and FTP.
- Implementing **two-factor authentication (2FA)** where possible would add another layer of security.

Enable Continuous Monitoring:

- Deploy tools to monitor and log network traffic regularly.
- Review these logs to detect anomalies early and respond proactively.

Implement ARP Spoofing Protections:

- Use static ARP bindings to lock MAC addresses to their corresponding IP addresses.
- Enable dynamic ARP inspection (DAI) on managed switches to prevent spoofing.
-

Raise Security Awareness:

- Educate network administrators and users to recognize signs of compromise and report unusual behavior promptly.

My Approach

To perform this analysis, I used **Wireshark**, a powerful network protocol analyzer. Here are the steps I followed:

- **Traffic Filtering:** I applied specific filters to isolate suspicious traffic:
    - tcp.flags.syn == 1 to capture SYN packets indicating port scans.
    - arp to analyze ARP traffic.
- **Protocol Insights:** I used the **Protocol Hierarchy** tool to review the distribution of protocols in the network traffic.
- **Packet Analysis:** I inspected individual packets to identify patterns consistent with scanning and spoofing.

Conclusion

In conclusion, my analysis of the network capture file revealed evidence of malicious activity, including port scanning, potential unauthorized access attempts, and ARP spoofing. These activities suggest reconnaissance efforts that could lead to further exploitation if left unaddressed.

To mitigate these threats, I recommend blocking the attacker's IP address immediately and securing the network by filtering ports, strengthening authentication, and implementing ARP protections. Additionally, continuous monitoring and periodic vulnerability assessments will improve the network's resilience against future attacks.

By taking these actions, we can significantly reduce the risk of compromise and enhance the overall security posture of the network.