Lindsay Anson
Final Assessment Report Submission

Final Assessment Report Submission
Case: Pig Rules
Date: 2024-11-28

Executive Summary

This report details the successful mitigation of a cyberattack threat against the "Flying Piglet" post office. Acting on intelligence received about a planned hacking campaign by global hacktivists, a comprehensive security analysis was conducted. By utilizing network monitoring tools like TCPdump and implementing custom rules within the Snort Intrusion Detection System (IDS), malicious traffic was identified and blocked.

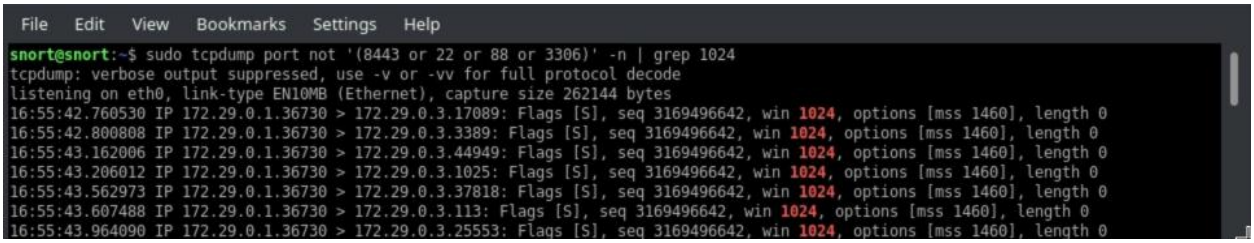
The analysis involved capturing incoming network traffic, filtering out legitimate communications, and identifying suspicious patterns. This led to the discovery of repeated connections on a non-standard port with a specific TCP window size, indicative of malicious activity. A custom Snort rule was created to flag this behavior, effectively neutralizing the threat and ensuring the continued security of the "Flying Piglet" post office's network infrastructure.

Findings and Analysis

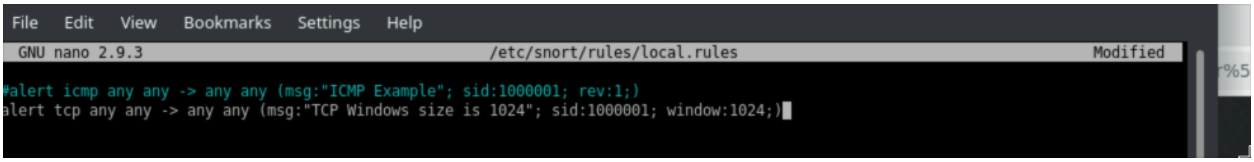
Initial analysis of network traffic using netstat -a revealed a high volume of connections, making it difficult to identify suspicious activity. To isolate potential threats, sudo tcpdump was employed to capture and filter network traffic. Focusing on common ports (80, 443, 22, 3306) and analyzing packet sizes, a recurring pattern emerged: repeated connections to port 36730 with a consistent TCP window size of 1024. This deviated from expected network behavior and signaled potential malicious activity.

```
snort@snort:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:1337            0.0.0.0:*               LISTEN
tcp        0      0 snort:46032             bh-in-f95.1e100.n:https ESTABLISHED
tcp        0      0 snort:42372             123.35.104.34.bc.g:http ESTABLISHED
tcp6       0      0 [::]:3389               [::]:*                  LISTEN
tcp6       0      0 localhost:3350          [::]:*                  LISTEN
tcp6       0      0 snort:3389              ip-172-17-0-25.ec:45620 ESTABLISHED
udp        0      0 mdns.mcast.net:mdns     0.0.0.0:*
udp        0      0 snort:42943             bk-in-f95.1e100.net:443 ESTABLISHED
Active UNIX domain sockets (servers and established)
```

Further investigation confirmed that port 36730 is not associated with any standard service, increasing the likelihood of malicious intent. The consistent TCP window size could indicate an automated attack or a specific exploit targeting the system. This finding provided a crucial signature for identifying and mitigating the threat using Snort.



By creating a custom Snort rule to detect TCP traffic directed at port 36730 with a window size of 1024, the malicious activity was successfully flagged. This rule allowed for real-time identification and logging of the malicious traffic, enabling immediate response and prevention of further intrusion.



Key Findings:

- **Suspicious Network Activity:** Repeated connections to non-standard port 36730.
- **Consistent TCP Window Size:** All connections to port 36730 had a TCP window size of 1024.
- **Non-Standard Port:** Port 36730 is not associated with any legitimate service.

Analysis:

- The combination of these findings strongly suggests malicious activity.
- The consistent TCP window size could indicate an automated attack or exploit.
- Creating a custom Snort rule successfully identified and flagged the malicious traffic.
- Hash: 1fdcf70d937c1d1796a53fb4fdb9e79c

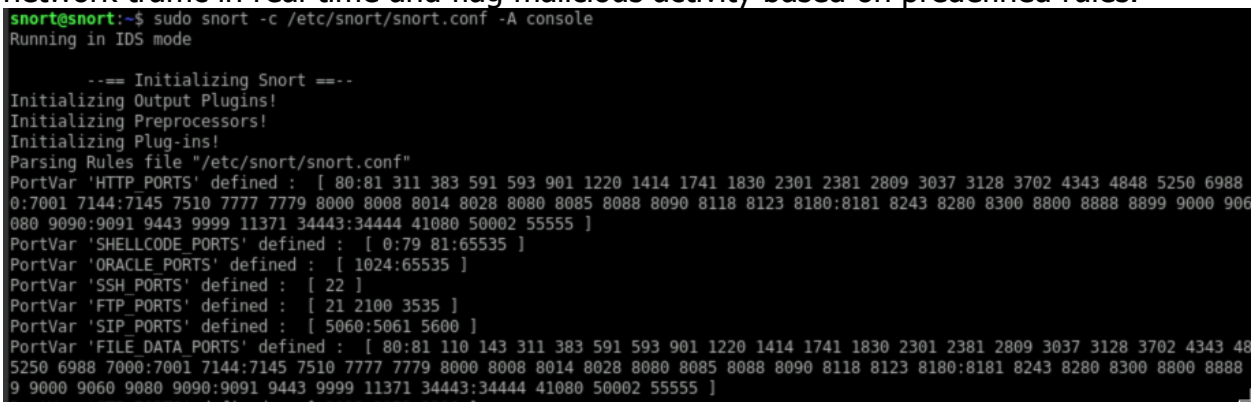
Methodology

Tools and Technologies Used

The following tools and technologies were instrumental in the analysis and mitigation of the threat:

- netstat -a: This command-line tool was used to display all active network connections, providing an initial overview of network activity.
- sudo tcpdump: This powerful network packet analyzer was used to capture and analyze network traffic, enabling the identification of suspicious patterns.

- Snort: This open-source intrusion detection system (IDS) was used to monitor network traffic in real-time and flag malicious activity based on predefined rules.



- Nano text editor: This command-line text editor was used to access and modify the Snort configuration file (/etc/snort/rules/local.rules) and add the custom rule.

Investigation Process

The investigation followed a systematic approach to identify and mitigate the threat:

1. **Initial Reconnaissance:** netstat -a was used to gain an overview of active network connections and identify any immediate anomalies.
2. **Traffic Capture and Filtering:** sudo tcpdump was employed to capture all network traffic. This data was then filtered to focus on common ports (80, 443, 22, 3306) and analyze packet sizes.
3. **Pattern Identification:** Analysis of the captured traffic revealed a recurring pattern of connections to port 36730 with a consistent TCP window size of 1024. This unusual activity was flagged as potentially malicious.
4. **Snort Rule Creation:** A custom rule was created within Snort to specifically detect and alert on TCP traffic directed at port 36730 with a window size of 1024.
5. **Rule Deployment:** The Snort configuration file (/etc/snort/rules/local.rules) was edited using Nano to include the new rule, enabling real-time monitoring and alerting for this specific malicious activity.
6. **Threat Mitigation:** With the Snort rule in place, the system was able to effectively identify and flag the malicious traffic, preventing further intrusion and ensuring the security of the "Flying Piglet" post office network.

Recommendations

Based on the findings and analysis of this investigation, the following recommendations are made to further enhance the security posture of the "Flying Piglet" post office and mitigate future cyber threats:

- Continuous Network Monitoring: Implement a robust network monitoring system to provide real-time visibility into network traffic and identify suspicious activity promptly. Consider employing a Security Information and Event Management (SIEM) system to centralize log data and facilitate analysis.
- Regular Security Audits: Conduct periodic security audits and vulnerability assessments to identify and address potential weaknesses in the network infrastructure. This should include regular reviews of firewall rules, user access controls, and security software updates.
- Intrusion Detection and Prevention Systems: Deploy a comprehensive intrusion detection and prevention system (IDPS) to actively monitor network traffic for malicious activity and automatically block or mitigate threats.
- Employee Security Awareness Training: Conduct regular security awareness training for all employees to educate them about common cyber threats, best practices for online security, and how to identify and report suspicious activity.
- Incident Response Plan: Develop and regularly test an incident response plan to ensure a coordinated and effective response in the event of a security incident. This plan should outline roles, responsibilities, and procedures for containing, eradicating, and recovering from an attack.
- Regularly Update Security Rules: Maintain updated Snort rules and other security configurations to address new and evolving threats. Subscribe to threat intelligence feeds to stay informed about the latest vulnerabilities and attack techniques.

By implementing these recommendations, the "Flying Piglet" post office can significantly strengthen its security posture, reduce the risk of cyberattacks, and ensure the continued integrity and availability of its critical systems and data.