Incident Response Report

Executive Summary

This report documents the analysis and response to a simulated cybersecurity incident involving a Denial-of-Service (DoS) attack on a web server hosted on a Metasploitable 2 Oracle VM VirtualBox environment. The attack was performed using the Slowloris tool, targeting the port 80 (HTTP) of Metasploitable 2. Wireshark was utilized to capture and analyze the network traffic generated during the attack. The root cause of the incident, mitigation steps, and recommendations to prevent future occurrences are detailed below.

Incident Details

Location: Oracle VM VirtualBox
Target: Web server hosted on port 80 (HTTP)
Threat Actor: Simulated attack using the Slowloris tool
Attack Type: Denial-of-Service (DoS) attack

Root Cause Analysis

Summary of Events:

1. A web server was configured and hosted on a virtual machine using Oracle VM (Metasploitable 2), accessible via port 80 (HTTP).
2. A DoS attack was launched using the Slowloris tool, which exhausts a server's connection pool by sending incomplete HTTP requests.
3. Network traffic during the attack was captured using Wireshark.

Evidence Collected:

- **Wireshark Capture Analysis:**
  - Traffic logs showed numerous incomplete HTTP GET requests from the attacker’s IP.
  - The connection requests had long timeouts and minimal data transmission, characteristic of a Slowloris attack.

- Network logs indicated a significant increase in resource consumption on the target server, leading to degraded performance.

Root Cause:

The vulnerability exploited in this attack is the web server's inability to handle numerous incomplete connections. The Slowloris tool exploited the lack of a timeout mechanism for idle connections, causing the server's connection pool to be overwhelmed.

Steps Taken to Mitigate the Incident

1. **Immediate Actions:**
   - Stopped the Slowloris attack by terminating the attacker's connection to the server.
   - Restarted the web server to restore normal functionality.
2. **Investigation:**
   - Analyzed network traffic using Wireshark to confirm the nature of the attack.
   - Reviewed server logs to identify patterns consistent with Slowloris.
3. **Temporary Measures:**
   - Blocked the attacker's IP address using the firewall.
   - Enabled rate limiting on the server to reduce the impact of potential future attacks.
4. **Mitigation and Prevention**
   - On the target system run:
   - **iptables -A INPUT -p tcp --dport 80 --syn -m limit --limit 10/s --limit-burst 20 -j ACCEPT**
   - This limits SYN packets to prevent flooding.

Recommendations to Prevent Future Occurrences

Technical Recommendations:

1. **Configure Timeout Settings:**

    - Implement a timeout mechanism to close idle or incomplete connections.
2. **Install a Web Application Firewall (WAF):**
    - Deploy a WAF to detect and block malicious traffic patterns, including Slowloris attacks.
3. **Enable Rate Limiting:**
    - Limit the number of simultaneous connections per IP address to reduce the impact of resource exhaustion attacks.
4. **Use a Reverse Proxy:**
    - Deploy a reverse proxy, such as Nginx, to handle incoming requests and filter malicious traffic.
5. **Apply Load Balancing:**
    - Use a load balancer to distribute traffic across multiple servers, mitigating the risk of a single server being overwhelmed.
6. **Monitor Network Traffic:**
    - Continuously monitor network traffic for anomalies using tools like Wireshark, Splunk, or Kibana.

Administrative Recommendations:

1. **Incident Response Plan:**
    - Develop and implement a formal incident response plan.
2. **Security Awareness Training:**
    - Train staff on recognizing and responding to potential DoS attacks.
3. **Regular Updates and Patching:**
    - Keep the web server and related software up-to-date with security patches.
4. **Periodic Penetration Testing:**
    - Conduct regular penetration tests to identify and mitigate vulnerabilities.

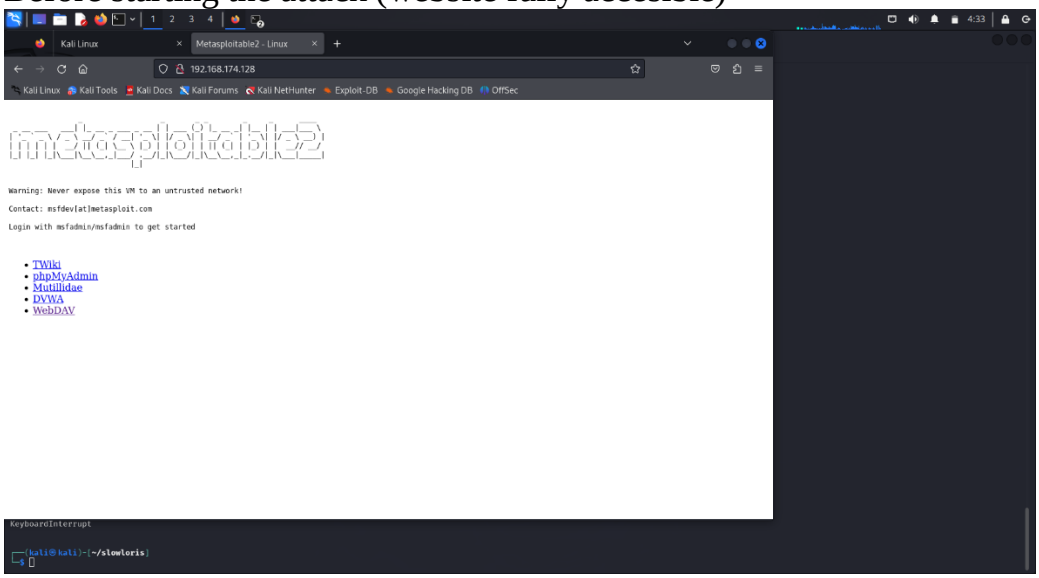
Conclusion

The simulated cybersecurity incident highlighted the vulnerabilities of a web server to a Slowloris-based DoS attack. Through Wireshark analysis, the root cause was identified as inadequate timeout and connection management mechanisms. Immediate mitigation steps restored functionality, and detailed

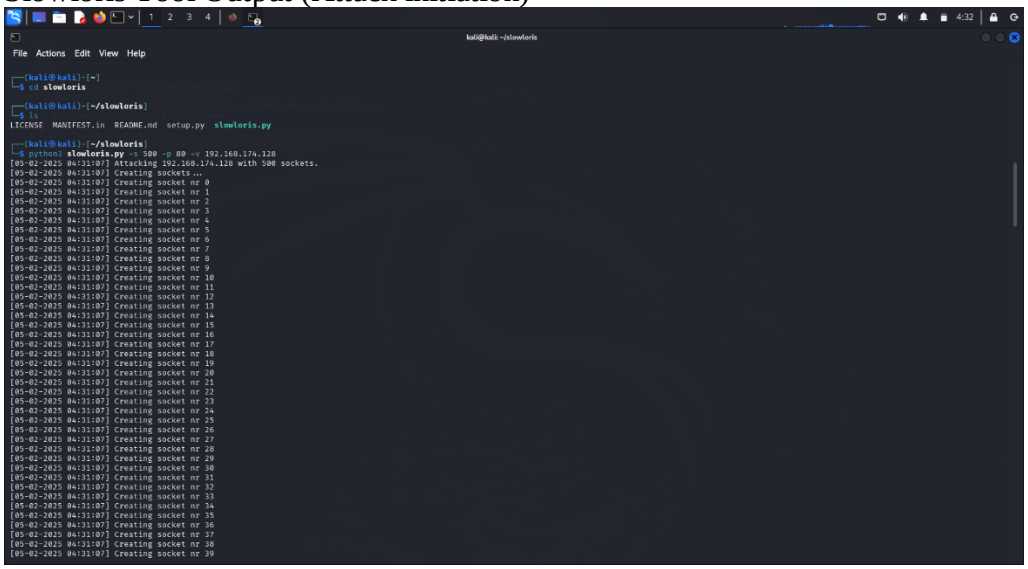
recommendations have been provided to enhance the server's resilience against similar attacks in the future.

Attachments:

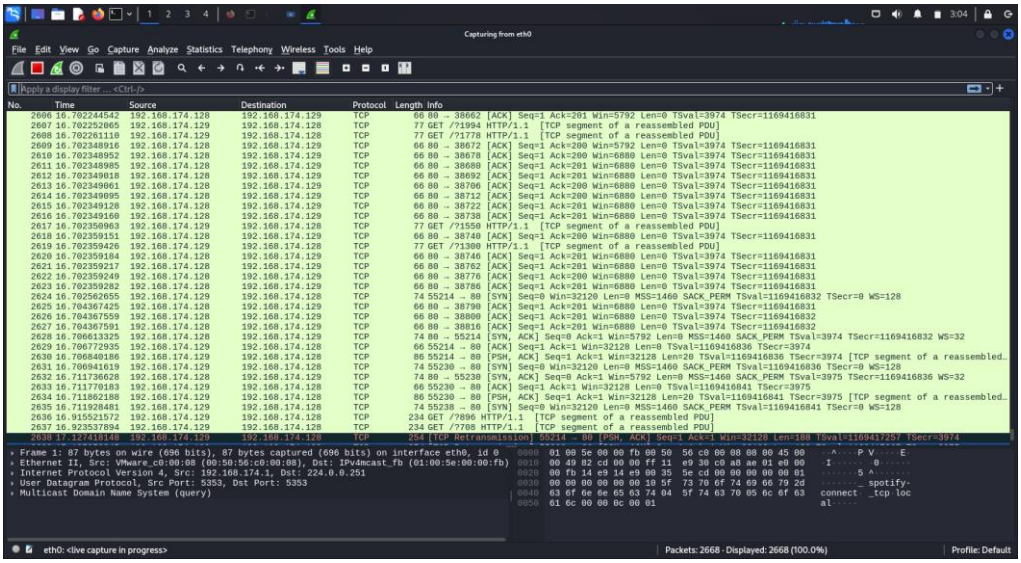
- Before starting the attack (website fully accesible)



- Slowloris Tool Output (Attack initiation)



- Wireshark Packet Capture Logs (network traffic)



- After Attack(Website buffering), user can’t able to open website