

Executive Summary

A comprehensive analysis of a simulated cybersecurity incident involving a Denial-of-Service (DoS) attack on a web server hosted in a VMware (Metasploitable 2) environment. The attack was executed using the Slow Loris tool, targeting port 80 (HTTP) to exhaust the server's connection pool. Wireshark was utilized to capture and analyze network traffic, revealing key indicators of the attack. This document outlines the root cause, mitigation measures, and preventive strategies to enhance system resilience against future threats.

Incident Details

- Environment: VMware Virtual Machine (Metasploitable 2)
 - Target: Web Server (Port 80 - HTTP)
 - Attack Type: Denial-of-Service (DoS)
 - Threat Actor: Simulated attack using Slowloris
-

Root Cause Analysis

Summary of Events:

1. A web server was deployed on a virtual machine and made accessible via port 80 (HTTP).
2. The Slowloris attack was initiated, sending multiple incomplete HTTP requests to exhaust the server's connection pool.
3. Wireshark was used to capture network traffic and analyze attack patterns.

Evidence Collected:

- Wireshark Packet Capture:

- Multiple incomplete HTTP GET requests from a single IP address.
- Long timeouts with minimal data transfer—hallmarks of Slowloris.
- Increased server resource consumption, leading to degraded performance.

Root Cause:

The web server lacked an efficient timeout mechanism, allowing the Slowloris tool to keep connections open indefinitely, exhausting available connections.

Steps Taken to Mitigate the Incident

Immediate Actions:

- ✓ Blocked the attacker's IP.
- ✓ Restarted the web server to restore normal operations.

Investigation Process:

- 🔍 Analyzed Wireshark traffic logs to confirm the attack pattern.
- 🔍 Reviewed server logs to identify anomalies and slow connections.

Temporary Measures:

- ◆ Implemented firewall rules to block the attacker's IP.
- ◆ Enabled rate limiting to reduce excessive connection attempts.

Mitigation & Prevention:

- ◆ Applied the following iptables rule to mitigate future SYN flood attacks:

```
iptables -A INPUT -p tcp --dport 80 --syn -m limit --limit 10/s  
--limit-burst 20 -j ACCEPT
```

- ◆ Configured timeouts to drop idle connections.
-

Recommendations to Prevent Future Attacks

Technical Measures:

1. **Configure Connection Timeouts:** Implement a timeout mechanism to close idle/incomplete connections.
2. **Deploy a Web Application Firewall (WAF):** Use ModSecurity or Cloudflare WAF to filter malicious traffic.
3. **Enable Rate Limiting:** Limit simultaneous connections per IP to prevent resource exhaustion.
4. **Use a Reverse Proxy:** Deploy Nginx or Apache mod_proxy to filter incoming requests.
5. **Apply Load Balancing:** Distribute traffic across multiple servers to mitigate overload risks.
6. **Continuous Network Monitoring:** Utilize Wireshark, Splunk, or Kibana to detect anomalies.

Administrative Measures:






1. **Develop an Incident Response Plan:** Define roles, responsibilities, and escalation procedures.
2. **Security Awareness Training:** Educate employees on recognizing and responding to DoS attacks.
3. **Regular System Updates & Patching:** Keep the web server and security tools up to date.
4. **Periodic Penetration Testing:** Conduct regular vulnerability assessments to identify weaknesses.

Conclusion

This incident demonstrated how Slowloris DoS attacks exploit poor connection management in web servers. Wireshark analysis confirmed the attack pattern, and mitigation steps were successfully implemented to restore functionality. By adopting stronger security

configurations, continuous network monitoring, and robust firewall rules, the risk of similar attacks can be significantly reduced.

Attachments:

-  Before Attack: Screenshot of a fully accessible website.
-  Slowloris Tool Output: Evidence of attack initiation.
-  Wireshark Logs: Packet capture demonstrating attack pattern.
-  After Attack: Screenshot showing website buffering due to attack.
-  Proactive security measures are essential in preventing cyber threats!