**Executive Summary**

This report details the analysis and response to a simulated cybersecurity incident involving a **Denial-of-Service (DoS) attack** on a web server hosted in a **VMware (Metasploitable 2) environment**. The attack, executed using the **Slowloris tool**, targeted **port 80 (HTTP)** to exhaust the server’s connection pool. **Wireshark** was employed to capture and analyze network traffic, revealing key indicators of the attack. This report outlines the root cause, mitigation measures, and preventive strategies to fortify the system 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 set up on a virtual machine and made accessible via **port 80 (HTTP)**.
2. The **Slowloris attack** was launched, sending multiple **incomplete HTTP requests** to consume the server’s connection pool.
3. **Wireshark** captured network traffic to analyze the attack pattern.

**Evidence Collected:**

* **Wireshark Packet Capture:**
  + Numerous **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, thereby **exhausting available connections**.

**Steps Taken to Mitigate the Incident**

**Immediate Actions:**

✅ **Terminated the attack** by blocking the attacker's IP. ✅ **Restarted the web server** to restore normal operations.

**Investigation Process:**

🔍 **Used Wireshark** to confirm the attack pattern. 🔍 **Reviewed server logs** to identify anomalies and slow connections.

**Temporary Measures:**

🔹 **Blocked the attacker’s IP** using firewall rules. 🔹 **Enabled rate limiting** to reduce excessive connection attempts.

**Mitigation & Prevention:**

🔹 Implemented 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:**
   * Implement **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**, **network monitoring**, and **firewall rules**, the risk of similar attacks can be significantly reduced.

**Attachments:**

📌 **Before Attack:** Screenshot of 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!**