Owasp x µLearn Bootcamp Task 8

IDS Evasion Techniques Report

Name: Ajay M Nambiar

Date: 03/10/2025

Assessment Type: IDS Evasion Analysis

Objective:

The primary objective of this assessment is to understand the fundamental principles of Intrusion Detection Systems (IDS) and to practically explore various techniques used to evade them. This report documents the process of completing the "IDS Evasion" room on TryHackMe, demonstrating the use of tools like Nmap to bypass network security monitoring.

Information Sources:

- TryHackMe - IDS Evasion Room (https://tryhackme.com/room/idsevasion)
- Nmap Official Documentation
- Snort IDS Documentation

Methodology & Execution

Task 1: Introduction to IDS/IPS

The first step was to understand the core concepts of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). An IDS is a passive monitoring tool that detects malicious activity or policy violations and reports them, whereas an IPS is an active system that can block or prevent detected intrusions. The room covered signature-based detection (matching known attack patterns) and anomaly-based detection (identifying deviations from a normal baseline).

Task 2: Initial Scan & Detection

To establish a baseline, a standard Nmap TCP connect scan was performed against the target machine. This scan is aggressive and easily detectable by most IDS solutions.

Command:

nmap -sT [TARGET_IP]

Observation:

As expected, the IDS (likely a Snort instance) immediately detected this scan. The alert logs on the security system would show multiple connection attempts from my IP address, flagging it as a potential network scan. This confirms the IDS is operational and monitoring traffic.

[Insert Screenshot of the IDS alert log showing the detection of your initial Nmap scan here.]

Caption: Figure 1 - IDS alert triggered by a standard Nmap TCP scan.

Task 3: Evasion Technique - Packet Fragmentation

The first evasion technique explored was packet fragmentation. This method involves splitting the TCP header over several small IP packets. An IDS that isn't configured to reassemble these fragments might not see the full packet and therefore fail to match the malicious signature.

Command:

nmap -f [TARGET_IP]

Observation:

By using the -f flag, Nmap splits the packets into 8-byte fragments. This technique successfully bypassed the basic signature rule that was looking for a standard TCP packet header. The scan completed without triggering an alert in the IDS log. This highlights a common misconfiguration in older or poorly configured IDS systems.

[Insert Screenshot of your successful fragmented scan and the clean IDS log here.]

Caption: Figure 2 - A fragmented scan successfully evades IDS detection.

Task 4: Evasion Technique - Decoys

The decoy technique is used to obscure the true source of a scan by launching it alongside scans from fake, spoofed IP addresses. The IDS logs are flooded with alerts from multiple IPs, making it difficult for an analyst to identify the actual attacker.

Command:

nmap -D RND:10,ME [TARGET_IP]

(This command generates 10 random decoy IPs and includes your real IP (ME) in the scan.)

Observation:

The IDS log was populated with alerts from the 10 random decoy IPs as well as my own. While the scan was still detected, my IP address was hidden among many others. An analyst would have to investigate each IP to determine which was the real source, effectively slowing down the incident response process.

[Insert Screenshot of the IDS log showing alerts from multiple decoy IP addresses.]

Caption: Figure 3 - IDS logs showing multiple decoy IPs, obscuring the attacker's true location.

Task 5: Evasion Technique - Timing Manipulation

Most IDS systems detect scans by looking for a high rate of connection attempts from a single source in a short period. By slowing the scan down, it's possible to fly under the radar. Nmap's timing templates (-T0 to -T5) make this easy.

Command:

nmap -T1 [TARGET_IP]

(The -T1 or "sneaky" template introduces significant delays between probes.)

Observation:

This scan took considerably longer to complete, but it did not trigger an IDS alert. The time between each probe was long enough that the IDS did not recognize the activity as a coordinated scan. This demonstrates the trade-off between speed and stealth in reconnaissance.

[Insert Screenshot of the scan completing without any corresponding IDS alerts.]

Caption: Figure 4 - A slow scan using the -T1 template avoids triggering rate-based IDS rules.

Results and Conclusion

This practical assessment successfully demonstrated several foundational IDS evasion techniques. The key takeaways are:

- **Default configurations are insecure:** A standard, out-of-the-box IDS can often be bypassed with simple techniques like packet fragmentation. Proper configuration, including packet reassembly, is critical.
- **Obscurity is a valid tactic:** While techniques like using decoys don't make a scan invisible, they significantly increase the "noise" for a security analyst, hindering effective incident response.

- **Stealth comes at the cost of speed:** Slowing down scans is a highly effective way to evade detection but is not practical for scanning large networks.
- **Defense-in-Depth:** Relying solely on a network IDS is insufficient. A modern security posture requires multiple layers of defense, including properly configured firewalls, an IPS capable of reassembling packets, and host-based intrusion detection systems (HIDS) to catch what the network sensors miss.