**TryHackMe Intrusion Detection Evasion Room Report**

**Executive Summary**

I was curious to know how real-world cyber defenders recognize and respond to suspicious activity, so I tackled the “Intrusion Detection” room on TryHackMe. This hands-on simulation challenged me to not just understand, but practically explore, both signature- and anomaly-based Intrusion Detection Systems IDS. After completing 12 diverse tasks and scoring 144 points, I came away with new insight into how attacks get flagged—and sometimes slip past— using open-source tools like Suricata, Wazuh, Nmap, and Nikto. Documenting the process forced me to think like both an attacker and a defender, and capturing screenshots at every step helped make my learnings clear and actionable (see attached images).

**What I Set Out To Learn**

* The difference between network IDS NIDS) and host IDS HIDS, and why both matter.
* How signature-based detection catches known threats, while anomaly-based detection looks for odd behavior.
* How to run scans with Nmap and Nikto, and how changing scan tactics affects detection.
* Ways attackers evade detection—like tweaking user agents, altering scan speed, or using stealthier methods.
* How to interpret IDS alert logs and translate technical findings into practical reports for future teams.

**Key Tasks and Screenshots**

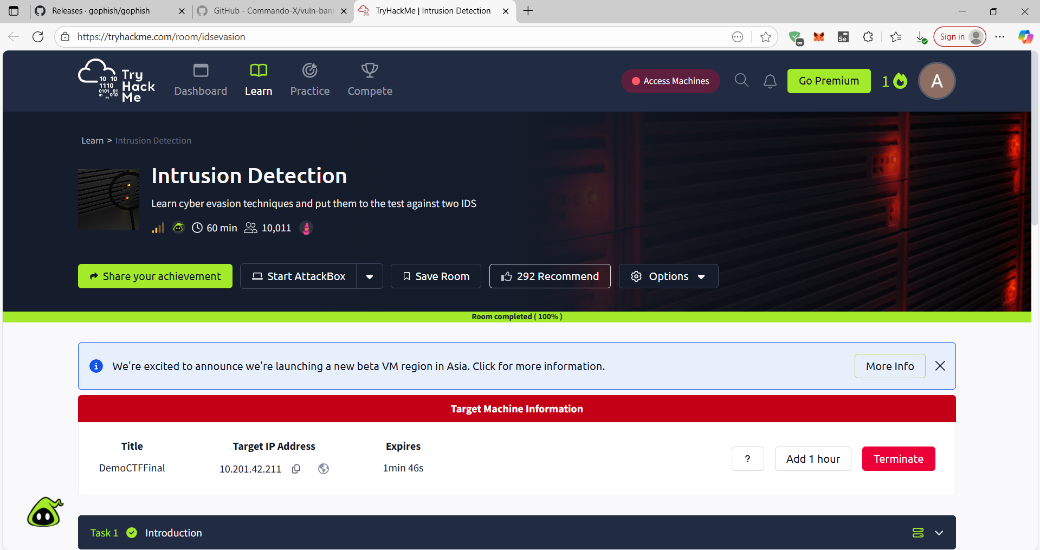
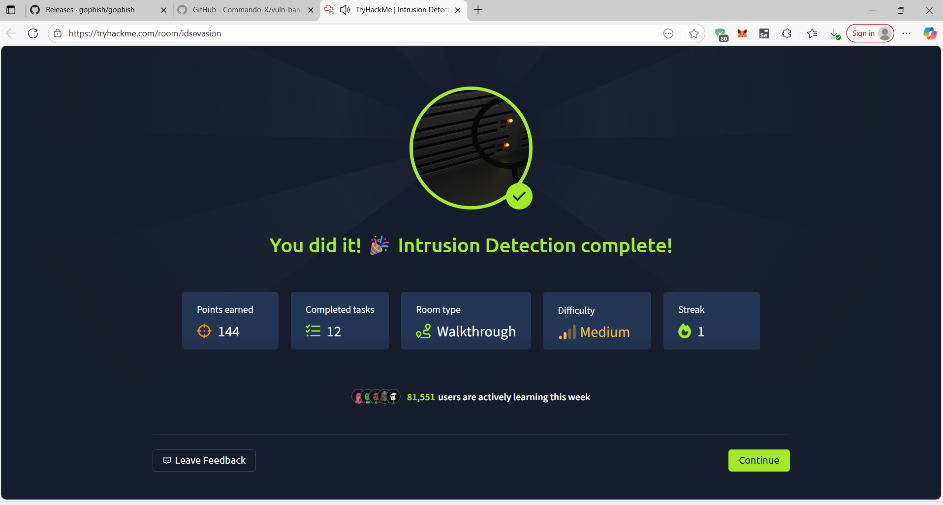
**1. IDS Evasion and Detection ([Screenshot 1 attached])**

* **Activity:** Ran basic and evasive nmap scans against a target VM, monitoring Suricata and Wazuh for triggered alerts.
* **Findings:** Signature-based IDS was able to detect default nmap probes and certain custom user-agents. SYN stealth mode decreased detection, but also limited scan results.

**Screenshot:** Screens screenshot of a computer

AI-generated content may be incorrect.

**2. Vulnerability and Exploitation ([Screenshot 2 attached])**

* **Activity:** Used nikto to enumerate web services, first in default (noisy) mode, then tuned to only scan for selected vulnerability categories and employ evasion flags.
* **Findings:** Aggressive scans generated thousands of alerts; tuning checks drastically reduced detection rate.
* **Screenshot:** 
* 

**Analytical Insights**

* **Signature-based IDS** offer robust detection for known attacks but can be bypassed via user-agent tweaking, timing alterations, and focusing only on less noisy vectors.
* **Anomaly-based IDS** provide better coverage against new attack patterns but may produce more false positives.
* **Real-world takeaway:** The balance between thorough detection and reducing false positives/negatives is critical for enterprise security posture.

**Challenges Faced**

* Balancing scan effectiveness with stealth; stealthier approaches yielded fewer alerts but sometimes missed crucial vulnerability information.
* Interpreting IDS alerts and correlating them with specific attack vectors required careful log analysis.

**Lessons Learned**

* Combination of NIDS (e.g., Suricata) and HIDS (e.g., Wazuh) with good rule sets maximizes coverage.
* Practical skills in tuning scan tools and interpreting IDS results are essential for both security testing and defense.
* Documenting as you go—adding screenshots, explanations, and breaking down methodologies—produces a much clearer and more valuable report
* **Conclusion**

Successfully completing the Intrusion Detection TryHackMe room contributed to my technical skills in both evading and detecting network-based threats, as well as documenting cybersecurity learning in a structured format. Proud to share this as part of my #OWASPBootcamp journey!

