EX NO 12   Demonstrate Cyber Evasion Techniques   ROLL NO : 231901014
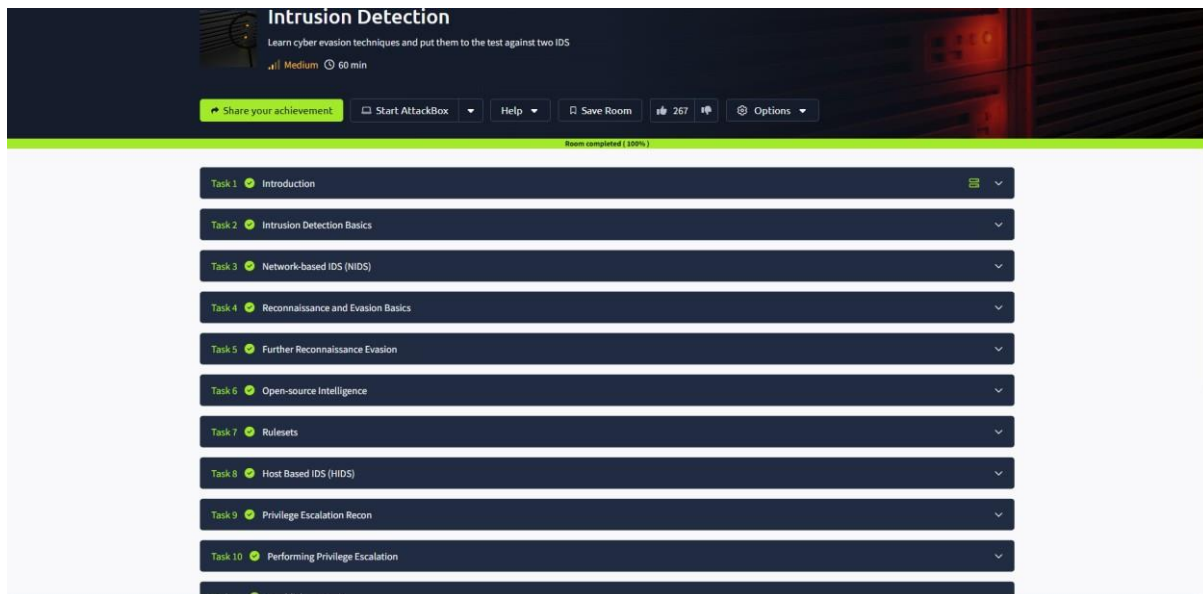
DATE: 30.04.2025   NAME : JASON FREDDY

AIM:

Learn cyber evasion techniques and put them to the test against two IDS

TASK 2 : INTRUSION DETECTION BASICS

What IDS detection methodology relies on rule sets?

signature-based detection   ✓ Correct Answer

TASK 3 : NETWORK-BASED IDS(NIDS)

What widely implemented protocol has an adverse effect on the reliability of NIDS?

TLS   ✓ Correct Answer   ♀ Hint

Experiment by running tools against the target and viewing the resultant alerts. Is there any unexpected activity?

No answer needed   ✓ Correct Answer   ♀ Hint

TASK 4 RECONNAISSANCE AND EVASIOM BASICS

What scale is used to measure alert severity in Suricata? (*-*)

1-3 ✓ Correct Answer ◉ Hint

How many services is nmap able to fully recognise when the service scan (-sV) is performed?

3 ✓ Correct Answer ◉ Hint

TASK 5 : FURTHER RECONNAISSANCE EVASION

Nikto, should find an interesting path when the first scan is performed, what is it called?

/login ✓ Correct Answer

What value is used to toggle denial of service vectors when using scan tuning (-T) in nikto?

6 ✓ Correct Answer ◉ Hint

Which flags are used to modify the request spacing in nikto? Use commas to separate the flags in your answer.

6,A,B ✓ Correct Answer ◉ Hint

TASK 6 : OPEN-SOURCE INTELLIGENCE

What version of Grafana is the server running?

8.2.5 ✓ Correct Answer 💡 Hint

What is the ID of the severe CVE that affects this version of Grafana?

CVE-2021-43798 ✓ Correct Answer 💡 Hint

If this server was publicly available, What site might have information on its services already?

shodan ✓ Correct Answer

How would we search the site "example.com" for pdf files, using advanced Google search tags?

site:example.com filetype:pdf ✓ Correct Answer

TASK 7 : RULESETS

What is the password of the grafana-admin account?

GraphingTheWorld32 ✓ Correct Answer 💡 Hint

Is it possible to gain direct access to the server now that the grafana-admin password is known? (yay/nay)

yay ✓ Correct Answer 💡 Hint

Are any of the attached IDS able to detect the attack if the file /etc/shadow is requested via the exploit, if so what IDS detected it?

Suricata ✓ Correct Answer 💡 Hint

TASK 8 : HOST BASED IDS (HIDS)

What category does Wazuh place HTTP 400 error codes in?

web ✓ Correct Answer ♀ Hint

Play around with some post-exploitation tools and commands and make note of what activity is detected by Wazuh; compare it to the activity that's detected by Suricata.

No answer needed ✓ Correct Answer

TASK 9 : PRIVILEGE ESCALATION RECON

What tool does linPEAS detect as having a potential escalation vector?

docker ✓ Correct Answer ♀ Hint

Is an alert triggered by Wazuh when linPEAS is added to the system, if so what its severity?

5 ✓ Correct Answer ♀ Hint

TASK 10: PERFORMING PRIVILEGE ESCALATION

Perform the privilege escalation and grab the flag in /root/

{SNEAK_ATTACK_CRITICAL} ✓ Correct Answer

RESULT :

Cyber evasion techniques and put them to the test against two IDS is successfully learned