

EX.NO:12

NAME:KALAIYARASI.M

DATE:16/4/25

ROLLNO:231901503

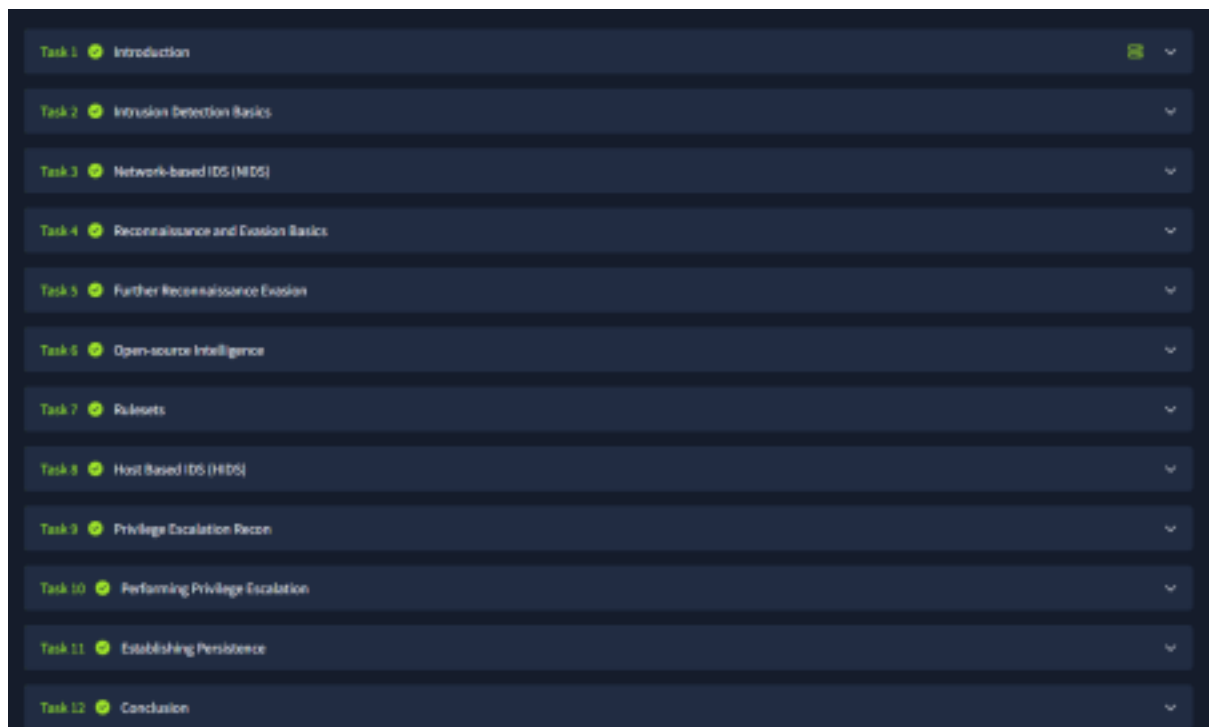
Intrusion Detection

AIM:

To learn cyber evasion techniques and put them to the test against two

IDS. PROCEDURE:

Complete the given task as per the instructions.



Task 1:Introduction



Task 2:Intrusion Detection Basics



Task 3:Network-based IDS (NIDS)

Answer the questions below

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 Evasion Basics

Answer the questions below

What scale is used to measure alert severity in Sericata? (1-5)

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

Answer the questions below

Mikto, 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 mikto?

S ✓ Correct Answer Hint

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

S,A,B ✓ Correct Answer Hint

Task 6: Open-source Intelligence

Answer the questions below

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-2021-43793 ✓ 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

Answer the questions below

What is the password of the grafana-admin account?

GraphingTheWorld32 ✓ Correct Answer 0 Hint

Is it possible to gain direct access to the server now that the grafana-admin password is known? (yes/no)

yes ✓ Correct Answer 0 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 0 Hint

Task 8:Host Based IDS (HIDS)

Answer the questions below

What category does Wazuh place HTTP 400 error codes in?

web ✓ Correct Answer 0 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

Answer the questions below

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

docker ✓ Correct Answer 0 Hint

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

5 ✓ Correct Answer 0 Hint

Task 10:Performing Privilege Escalation

Answer the questions below

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

[SNEAK_ATTACK_CRITICAL] ✓ Correct Answer

Task 11:Establishing Persistence

Answer the questions below

Abuse docker to establish a backdoor on the host system

No answer needed ✓ Correct Answer

Task 12:Conclusion

Answer the questions below

Read the above

No answer needed ✓ Correct Answer

RESULT:

Thus, the experiment is completed successfully in try hack me platform.