

Intrusion Detection

EX-NO-12

AIM:

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

PROCEDURE:

- Task 1 Introduction
- Task 2 Intrusion Detection Basics
- Task 3 Network-based IDS (NIDS)
- Task 4 Reconnaissance and Evasion Basics
- Task 5 Further Reconnaissance Evasion
- Task 6 Open-source Intelligence
- Task 7 Rulesets
- Task 8 Host Based IDS (HIDS)
- Task 9 Privilege Escalation Recon
- Task 10 Performing Privilege Escalation
- Task 11 Establishing Persistence
- Task 12 Conclusion

Task 1 Introduction :

Answer the questions below

Deploy the target machine and create an account and log into the system at `http://MACHINE_IP:8000`, in preparation for future tasks.

Task 2 Intrusion Detection Basics :

Answer the questions below

What IDS detection methodology relies on rule sets?

Task 3 Network-based IDS (NIDS) :

Answer the questions below

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

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

Task 4 Reconnaissance and Evasion Basics :

Answer the questions below

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 :

Answer the questions below

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 :

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-2021-43798

✓ 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 :

Answer the questions below

What is the password of the grafana-admin account?

✓ Correct Answer 🔍 Hint

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

✓ 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?

✓ Correct Answer 🔍 Hint

Task 8 Host Based IDS (HIDS) :

Answer the questions below

What category does Wazuh place HTTP 400 error codes in?

✓ 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.

✓ Correct Answer

Task 9 Privilege Escalation Recon :

Answer the questions below

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

✓ Correct Answer 🔍 Hint

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

✓ Correct Answer 🔍 Hint

Task 10 Performing Privilege Escalation :

Answer the questions below

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

✓ Correct Answer

Task 11 Establishing Persistence :

Answer the questions below

Abuse docker to establish a backdoor on the host system

✓ Correct Answer

Task 12 Conclusion :

Answer the questions below

Read the above

No answer needed

✓ Correct Answer

RESULT:

Thus the Intrusion Detection is completed using tryhackme platform.