


## EXERCISE 12

### Demonstrate Cyber Evasion Techniques

**Aim:** To learn various cyber evasion techniques and apply them to test the effectiveness of two Intrusion Detection Systems (IDS).



### Intrusion Detection

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

Medium 60 min

Share your achievement Start AttackBox Help Save Room 265 Options

Room completed ( 100% )

- 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

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

What is the password of the grafana-admin account?

GraphingTheWorld32 ✓ Correct Answer Hint

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

{SNEAK\_ATTACK\_CRITICAL} ✓ Correct Answer

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

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

**Result:** Successfully executed multiple evasion techniques and evaluated their impact, identifying the strengths and weaknesses of both IDS setups against stealthy attack patterns.