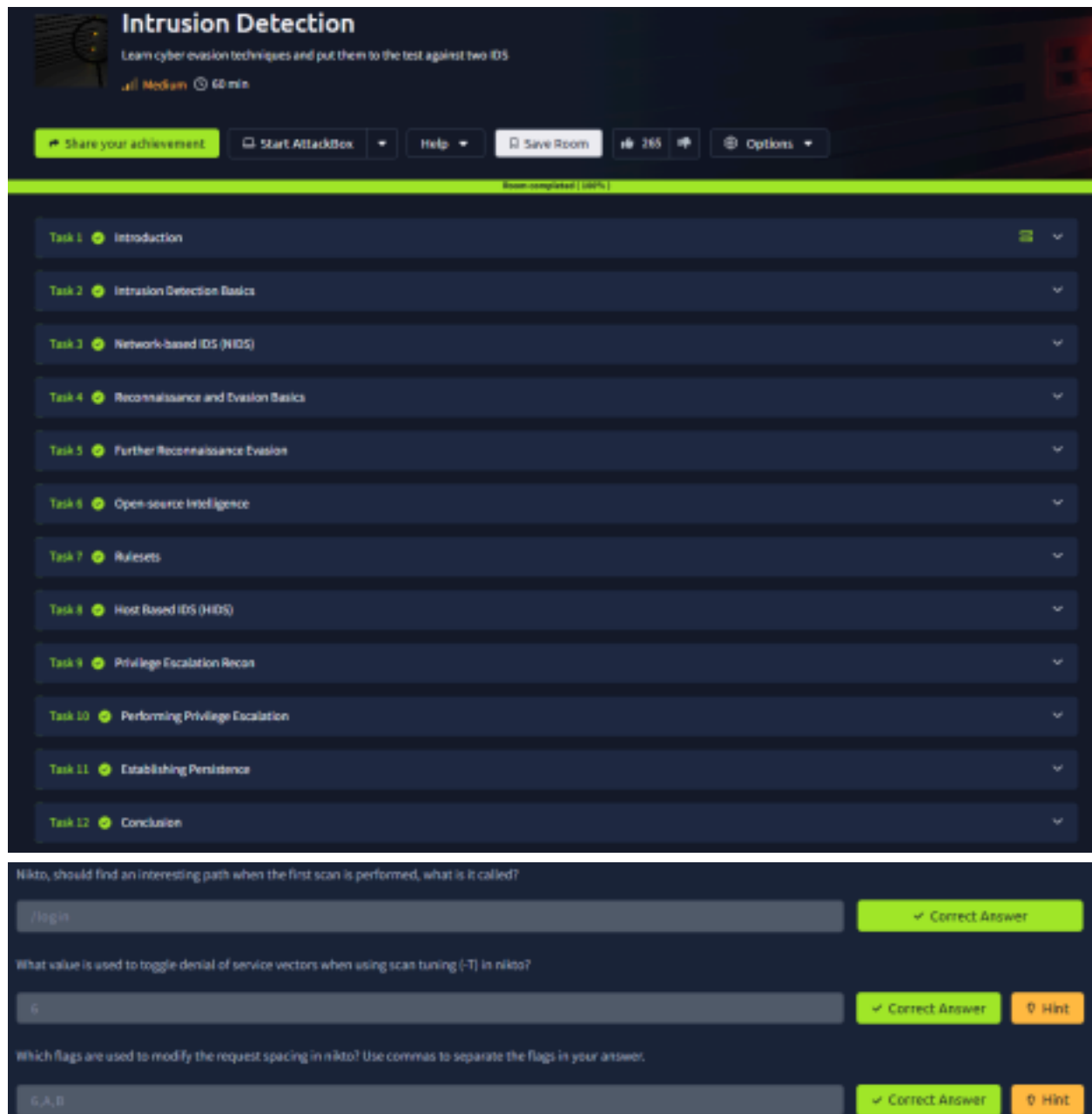**Vishwanath M 231901062**

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).

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.