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:



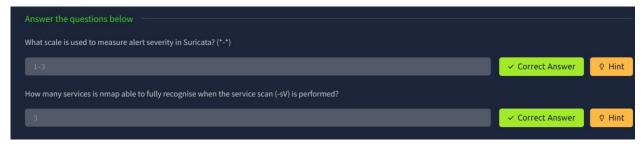
Task 2 Intrusion Detection Basics:



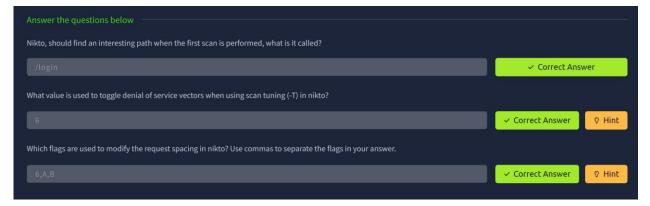
Task 3 Network-based IDS (NIDS):



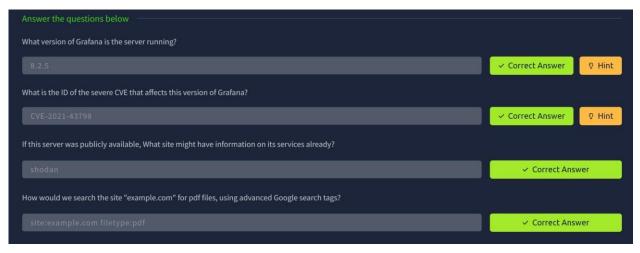
Task 4 Reconnaissance and Evasion Basics:



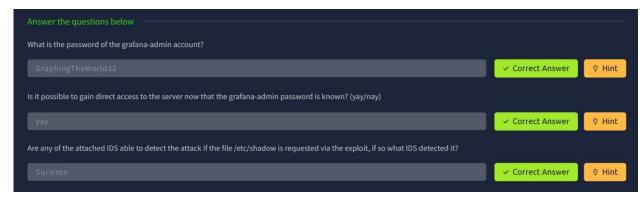
Task 5 Further Reconnaissance Evasion:



Task 6 Open-source Intelligence:



Task 7 Rulesets:



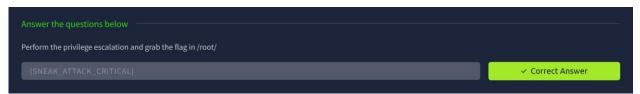
Task 8 Host Based IDS (HIDS):



Task 9 Privilege Escalation Recon:



Task 10 Performing Privilege Escalation:



Task 11 Establishing Persistence:



Task 12 Conclusion:



RESULT:

Thus the Intrusion Detection is completed using tryhackme platform.