Page No.
Date

Devanshu Surana
PC-23, 10322210755
Panel C, Batch C1

(A) 4½
30/11/23

ICS Lab Assignment 9

Aim: Implement intrusion detection system using Snort IDs tool

FAQ's

1) What are various types of IDs system?
→ Network IDs - Monitor network traffic for malicious activity
Host IDs - Installed on hosts monitor system logs, file, etc.
Wireless IDs - Monitor wireless network traffic.
Network Behaviour Analysis - Detect anomalies in traffic patterns.

2) What are the popular tools based on IDs systems?
→ Snort - open source network IDs.
Suricata - Utilizes GPU processing for high performance
OSSEC - Host based IDs with emphasis on log analysis.
Alien Vault - Unified security management with IDs built in.

3) What are the features of snort software of IDs?
→ Rules based detection using signature of known attacks.

Page No.
Date

Real time traffic analysis and packet logging.
Support for detecting protocol anomalies
Flexible deployment option - sniffers, packet logger or NIDS mods.
Customizable alerting and logging option.
Open Source with community support.

Q4) What are detection methods of IDs?
→ Signature based - Recognize attack pattern
Anomaly based - Identify deviation from normal behaviour
Stateful protocol analysis - Understand context of protocol states.
Machine learning - Train models to detect new attacks

Q5) What are the intrusion prevention systems?
→ Intrusion prevention systems (IPs) are network security devices that monitor traffic just like IDs but can also actively prevent / block detected threats in real time. IPS solutions leverage various detection techniques used by IDs as well.