Name: Tejas Redkar
PRN: 1032210937
Panel- C, Batch -C2
Roll NO: PC-44

ICS Lab A9

A+ 1/12/23

* FAQ's

Q1) What are various types of IDS system?

Ans → 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 Anamolies in traffic patterns.

Q2) What are the popular tools based on IDS systems?

Ans → Snort - Open source network IDS

→ Suricata- Utilizes GPU processing for high performance

→ OSSEC - Host based IDS with emphasis on log analysis

→ AlienVault - Unified security management with IDS built in.

Q3) What are the features of snort software of IDS?

Ans → Rules based detection using signature of known attacks

→ Real time traffic analysis & packet logging.

→ Support for detecting protocol anamolies

→ flexible deployment option- sniffer, packet logger or NIDs mode.

→ Customizable alerting & logging option

→ open Source with community support.

Q4) What are detection methods of IDs?

Ans → signature based- recognize attack patterns

→ Anamoly based - Identify deviations 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 system?

Ans Intrusion Prevention System (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 detections techniques used by IDS as well.

A+ 11/12/23