SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IoT Including CS & BCT

COURSE NAME :19SB701 PATTERN RECOGNITION TECHNIQUES IN CYBER CRIME

IV YEAR / VII SEMESTER

Unit IV- **MALWARE ANALYSIS AND NETWORK TRAFFIC ANALYSIS**

Topic :Network Traffic Analysis.

Network Traffic Analysis involves monitoring, capturing, and analyzing network traffic to understand the behavior of data transmitted across a network.

This process is crucial for identifying security threats, diagnosing network issues, and optimizing performance.

Key Concepts in Network Traffic Analysis

Traffic Capture: The process of collecting data packets as they travel across a network. Tools like Wireshark, tcpdump, and Snort are commonly used for this purpose.

Packet Sniffing: Involves capturing the data packets to analyze their content and metadata.

Packet Analysis:

Header Analysis: Examining the headers of packets (such as IP, TCP/UDP, etc.) to understand the source, destination, protocol, and other attributes.

Payload Analysis: Analyzing the data portion of packets to detect malicious content, extract useful information, or understand the data being transmitted.

Flow Analysis:

NetFlow/SFlow: Protocols used to summarize traffic flows on a network. A flow represents a sequence of packets between a source and destination.

Traffic Profiling: Understanding normal traffic patterns to detect anomalies or deviations that may indicate security threats.

Protocol Analysis:

Understanding the behavior of specific protocols (like HTTP, DNS, FTP) in the network traffic. Protocol analyzers can be used to decode and analyze the data specific to a protocol.

Anomaly Detection:

Signature-Based Detection: Identifies threats by comparing traffic against a database of known attack signatures.

Heuristic/Behavioral Analysis: Detects anomalies by identifying traffic patterns that deviate from the norm.

Security Applications:

Intrusion Detection Systems (IDS): Tools that monitor network traffic for suspicious activity and known threats.

Firewall Logs: Analyzing logs from firewalls to understand allowed and blocked traffic.

Performance Monitoring:

Bandwidth Usage: Monitoring the amount of data transmitted across the network to prevent congestion and ensure optimal performance.

Latency: Measuring the time it takes for data to travel from source to destination to detect slow connections or network bottlenecks.

Common Tools for Network Traffic Analysis

Wireshark: A powerful network protocol analyzer for deep inspection of hundreds of protocols.

Tcpdump: A command-line packet analyzer that allows users to capture and display packet headers.

Snort: An open-source network intrusion detection system (NIDS) capable of real-time traffic analysis and packet logging.

Solar Winds Network Performance Monitor: A tool for real-time network monitoring, fault detection, and performance analysis.

Challenges in Network Traffic Analysis

Encryption: With the widespread use of encryption (HTTPS, VPNs), analyzing the payload of network traffic becomes challenging.

High Volume: Analyzing large volumes of network data in real-time requires significant computational resources.

False Positives: Detecting real threats while minimizing false alarms is a critical challenge in network security.

Network Traffic Analysis is an essential practice for maintaining the security, reliability, and performance of a network.

By understanding and analyzing network traffic, administrators can detect and mitigate security threats, troubleshoot network issues, and ensure efficient data transmission.

1. Which tool is commonly used for deep inspection of network protocols and packet analysis?

A) Tcpdump

B) NetFlow

C) Wireshark

D) SolarWinds

Answer: C) Wireshark

2. What is the primary challenge of analyzing encrypted network traffic?

A) High volume of data

B) Real-time monitoring

C) False positives

D) Inability to inspect the payload content

Answer: D) Inability to inspect the payload content

3. Which method of anomaly detection involves comparing network traffic against a database of known attack signatures?

- A) Heuristic Analysis
- B) Flow Analysis
- C) Signature-Based Detection
- D) Protocol Analysis

Answer: C) Signature-Based Detection

Any Query????

Thank you……