| **Course Name:** | **Information Security (116U01L602)** | **Semester:** | **VI** |
| --- | --- | --- | --- |
| **Date of Performance:** | **27/03/2025** | **DIV/ Batch No:** | **C - 3** |
| **Student Name:** | **Romil Lodaya** | **Roll No:** | **16010122096** |

| **Title: Working with sample real life cases related to Network security and**  **forensics using tool – Wireshark and Network Miner.** |
| --- |

| **Objectives:** |
| --- |
| * **Understand Network Forensics Concepts** * **Analyze Packet Captures** * **Identify Malicious Communication Patterns** * **Extract Files and Evidence from Captured Traffic** * **Respond to Network-Based Incidents** |

| **Expected Outcome of Experiment:** |
| --- |
| **CO4:** Illustrate and Compare network security mechanisms |

| **Books/ Journals/ Websites referred:** |
| --- |
| https://forensicscontest.com/2009/09/25/puzzle-1-anns-bad-aim |

| **Pre Lab/ Prior Concepts:** |
| --- |
| **Basic Networking Concepts:**   * OSI Model and TCP/IP layers * IP addressing, subnetting, and MAC addresses * Protocols: TCP, UDP, ARP, HTTP, FTP, etc.   **Packet Capture Basics:**   * Understanding packet structure (Ethernet, IP, TCP/UDP headers) * Concept of packet sniffing and capturing network traffic   **Wireshark Basics:**   * Installation and interface setup * Capturing live traffic * Applying basic filters   **Network Security Fundamentals:**   * Concepts of confidentiality, integrity, and availability (CIA Triad) * Introduction to network attacks (MITM, DoS, DNS Spoofing, etc.) |

| **New Concepts to be learned:** |
| --- |
| **Wireshark Advanced Usage:**   * Applying advanced display filters * Analyzing TCP streams and extracting payloads * Exporting objects (files, conversations)   **Network Forensics Techniques:**   * Identifying suspicious network behavior * Extracting and reconstructing files from traffic * Analyzing protocols used for file transfers and IM conversations   **Using Network Miner:**   * Extracting metadata, files, and credentials from captured traffic * Correlating extracted evidence with events in Wireshark   **Comparing Security Mechanisms:**   * Encryption protocols (TLS/SSL) * Authentication and integrity mechanisms |

| **Abstract:** |
| --- |
| The objective of this experiment is to **analyze real-life network security scenarios** using **Wireshark** and **Network Miner**. The analysis includes identifying suspicious activity, capturing relevant conversations, extracting transferred files, and understanding security vulnerabilities. A captured packet file (.pcap) will be analyzed to detect malicious actions such as unauthorized file transfer or communication, and security mechanisms will be evaluated to mitigate such threats. |

| **Related Theory:** |
| --- |
| **Wireshark Overview:**  Wireshark is a powerful network protocol analyzer that captures and inspects network traffic at a granular level. It allows filtering, reconstructing TCP streams, and exporting objects for forensic analysis.  **Network Miner Overview:**  Network Miner is a network forensic tool that extracts files, metadata, and credentials from packet captures. It helps in identifying critical artifacts for forensic investigation.  **Packet Capture Analysis:**  Packet captures contain raw network traffic, allowing analysts to identify protocol types, examine data payloads, and detect anomalies.  **File Transfer Protocols:**   * **HTTP/HTTPS:** Web-based file transfer * **SMB/FTP:** Internal network file transfers * **IM Conversations:** Detection of file sharing via chat protocols   **Security Mechanisms:**   * **TLS/SSL Encryption:** Securing communications from eavesdropping * **Authentication Protocols:** Validating user identity * **Integrity Checks:** Ensuring data has not been altered |

| **Implementation Details:** |
| --- |
| What is the name of Ann’s IM buddy? **Sec558user10**      Where were they to meet?  **see you in hawaii!**      What was the first comment in the captured IM conversation?  **Here’s the secret recipe… I just downloaded it from the file server. Just copy to a thumb drive and you’re good to go**      What is the name of the file Ann transferred?  **recipe.docx**    What is the magic number of the file you want to extract (first four bytes)?  **0x504B0304**      What was the MD5sum of the file? **8350582774e1d4dbe1d61d64c89e0ea1**    What is the secret recipe? **Recipe for Disaster:**  **1 serving**  **Ingredients:**  **4 cups sugar**  **2 cups water**  **In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.** |

| **Conclusion:** |
| --- |
| In conclusion, this lab will help develop a practical understanding of network security and forensic analysis. By using Wireshark and Network Miner, we will learn how to capture and analyze network traffic, identify vulnerabilities, and detect malicious activities. The tools offer powerful capabilities for deep traffic inspection and session reconstruction, which are essential for effective forensic investigations. |

| **Post-Lab Questions:** |
| --- |
| Explain the Different Challenges in Handling Network-Based Incidents:  1. **Volume of Data:**  Large enterprises generate terabytes of data daily, making it difficult to analyze and filter out relevant information. 2. **Real-Time Detection:**  Identifying malicious activity in real-time is challenging due to sophisticated attack techniques like zero-day exploits and polymorphic malware. 3. **Encryption and Obfuscation:**  Attackers often use encrypted channels (SSL/TLS) to exfiltrate data, making it harder to analyze network traffic. 4. **False Positives and Negatives:**  Security tools may generate numerous false positives, while some attacks might bypass detection mechanisms (false negatives), leading to delays in incident response. 5. **Lack of Context and Correlation:**  Without correlating multiple sources of data (firewall logs, intrusion detection logs, system events), identifying patterns of attack or compromise is difficult. 6. **Insider Threats:**  Malicious insiders or compromised internal systems can evade traditional security monitoring tools. 7. **Advanced Persistent Threats (APTs):**  APTs stay undetected in networks for long periods, making it difficult to trace their origin and impact.  Discuss the Tools Used for Monitoring Network Traffic:  1. **Wireshark:**     * Captures and analyzes packets on a network.    * Identifies suspicious traffic patterns and reconstructs TCP streams. 2. **Network Miner:**     * Extracts files, metadata, and credentials from captured traffic.    * Useful for forensic analysis and incident response. 3. **Snort:**     * Open-source intrusion detection and prevention system (IDS/IPS).    * Analyzes network traffic and identifies malicious patterns using rule-based detection. 4. **Suricata:**     * Advanced network IDS/IPS capable of deep packet inspection.    * Supports automatic signature updates and integrates with SIEM solutions. 5. **Zeek (formerly Bro):**     * Monitors network traffic and generates detailed log data.    * Used for security monitoring and incident analysis. 6. **Tshark:**     * Command-line version of Wireshark, useful for automated packet analysis. 7. **SolarWinds Network Performance Monitor:**     * Monitors network devices and traffic for performance and security insights. 8. **Splunk:**     * Aggregates, analyzes, and visualizes data from multiple network sources.    * Helps in identifying anomalies and generating security alerts.  What Do You Understand by Packet Sniffing? **Packet Sniffing** is the process of capturing and analyzing packets transmitted across a network to monitor, diagnose, and secure network communications. It involves inspecting the raw data at the network level to identify protocols, source and destination addresses, payload data, and possible anomalies. Types of Packet Sniffing:  1. **Passive Sniffing:**     * Listens to network traffic without altering data.    * Typically used in wired networks with hubs or wireless networks. 2. **Active Sniffing:**     * Involves injecting traffic or manipulating data to capture packets.    * Used in switched networks where traffic is segregated.  Uses of Packet Sniffing:  * **Network Troubleshooting:** Identifying performance issues and misconfigurations. * **Security Analysis:** Detecting intrusions, malicious activities, and data exfiltration. * **Forensic Investigations:** Reconstructing communication sessions for incident response. * **Protocol Analysis:** Ensuring proper protocol implementation and adherence.  Common Packet Sniffing Tools:  * Wireshark * Tcpdump * Tshark * Ettercap * Cain & Abel |