



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Course Name:** | | **Information Security (116U01L602)** | **Semester:** | **VI** | |
| **Date of**  **Performance:** | | **16 / 04 / 2025** | **DIV/ Batch No:** | **A-3** | |
| **Student Name:** | | **Kashish Mamania** | **Roll No:** | **16010122104** | |
|  | | | | | |
|  | **Title: Illustrate and Compare network security mechanisms** | | | |  |

**Working with sample real life cases related to Network security and forensics using tools like NMAP and Network Miner.**

**Objectives:**

**Expected Outcome of Experiment:**

**Books/ Journals/ Websites referred:**

**Pre Lab/ Prior Concepts:**

Wireshark

**New Concepts to be learned:**

|  |
| --- |
| **Related Theory:** |
| **1. Network-Based Attacks**  Network-based attacks are cyber threats that target vulnerabilities in network infrastructure to compromise data integrity, confidentiality, and availability. Some common types of network-based attacks include:   * **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks** – Overwhelm network resources to disrupt services. * **Man-in-the-Middle (MITM) Attacks** – Intercept communications between two parties to steal or manipulate data. * **IP Spoofing** – Mask the attacker’s IP address to impersonate a legitimate user. * **Packet Sniffing** – Capture network traffic to extract sensitive information. * **SQL Injection and Cross-Site Scripting (XSS)** – Exploit vulnerabilities in web applications to gain unauthorized access. * **Malware and Ransomware Attacks** – Deploy malicious software to compromise devices and demand ransom.   **2. Network Security Tools**  Network security tools are essential for monitoring, analyzing, and protecting network infrastructure from cyber threats. Some commonly used network security tools include:   * **Firewalls** – Block unauthorized access to networks. * **Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS)** – Detect and mitigate suspicious activities. * **Wireshark** – Analyze network traffic in real-time. * **Network Miner** – Perform network forensic analysis to identify potential threats. * **Nmap (Network Mapper)** – Scan networks for vulnerabilities. * **Snort** – Open-source IDS that detects malicious activities. * **Metasploit** – Penetration testing tool for simulating attacks.   **3. Wireshark – Purpose and Importance in Network Security**  Wireshark is a powerful open-source network protocol analyzer used for real-time packet capturing and deep network traffic inspection. Its significance in network security includes:   * **Packet Analysis** – Examines network traffic to detect anomalies and potential security threats. * **Network Troubleshooting** – Identifies bottlenecks, misconfigurations, and connectivity issues. * **Forensic Investigations** – Helps cybersecurity professionals analyze cyber attacks by reconstructing traffic. * **Performance Monitoring** – Evaluates network performance to optimize data flow. * **Intrusion Detection** – Detects suspicious activities by analyzing abnormal traffic patterns. * **Protocol Analysis** – Identifies vulnerabilities in network protocols that could be exploited.   **4. Network Miner – Purpose and Importance in Network Security**  Network Miner is a network forensic analysis tool (NFAT) designed to extract information from captured network traffic. It is widely used for passive network monitoring and forensic investigations. Key functionalities include:   * **Network Traffic Analysis** – Helps analyze network packets to detect security incidents. * **File Extraction** – Recovers files transferred over the network, aiding forensic investigations. * **User Identification** – Identifies active users and their communication details. * **Host Discovery** – Gathers information about connected devices, including IP addresses and operating systems. * **Malware Detection** – Detects malicious activity by analyzing network behavior. * **Passive Analysis** – Unlike Wireshark, Network Miner does not send traffic, making it a stealthy analysis tool. |

|  |
| --- |
| **Implementation Details:** |
| Username is Sec558user1    1st message :  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 &gt;:-)    Name of file : recipe.docx    Magic Number (1st 4 bytes): 50 4b 03 04        Hence MD5sum is 8350582774EID4DBEID61D64C89EOEA1  This is the secret recipe |

|  |
| --- |
| **Post Lab Questions:** |
| 8.1 Explain the different challenges in handling network based incidents.  Ans:  Handling network-based incidents presents several key challenges:   * Anonymity of Attackers: Attackers can launch attacks from remote locations, often masking their identities, making attribution and response difficult. * Multiple Points of Attack: Large and complex networks have numerous potential entry points, increasing the difficulty of monitoring and securing every access vector. * System Complexity: Networks often consist of diverse systems with different operating systems, configurations, and vulnerabilities, complicating coordinated incident response. * Unknown Perimeter and Paths: The dynamic nature of networks, with devices and connections constantly changing, makes it hard to define clear security perimeters and trusted paths.   8.2 Discuss the tools used for monitoring the network traffic.  Ans:  Several tools and systems are commonly used to monitor network traffic and detect incidents:   * Intrusion Detection Systems (IDS): These systems monitor network traffic for suspicious patterns and alert administrators to potential threats. * Intrusion Prevention Systems (IPS): Similar to IDS, but can also take automated actions to block or mitigate detected threats. * Firewalls: Monitor and filter incoming and outgoing network traffic based on predefined security rules. * Packet Sniffers (e.g., Wireshark): Capture and analyze network packets in real time, allowing detailed inspection of traffic for troubleshooting or forensic purposes. * Network Analyzers: Provide comprehensive views of network performance and security, often integrating with other monitoring tools. * Security Information and Event Management (SIEM) Systems: Aggregate and analyze logs and alerts from various sources to provide a unified view of network security events. * Port Scanners: Scan network devices for open ports and services, helping identify potential vulnerabilities.   8.3 What do you understand by packet sniffing?  Ans:  Packet sniffing is the process of capturing and analyzing packets of data as they travel across a network. A packet sniffer (or network analyzer) intercepts network traffic, allowing an observer to view the contents of data packets, including headers and payloads. This technique can be used for legitimate purposes, such as network troubleshooting and performance analysis, but it can also be exploited by attackers to eavesdrop on sensitive communications, steal credentials, or gather intelligence for further attacks. |

|  |
| --- |
| **Conclusion:** |
| If the goal is to monitor live network traffic and perform in-depth analysis, Wireshark is the better choice.  If the goal is to extract forensic evidence quickly from captured network data, Network Miner is more efficient.  A combination of both tools provides the most comprehensive results for network forensic investigations.  Hence, we have implemented the Working with sample real life cases related to Network security and forensics using tool Wireshark and Network Miner |