ITDO6014
ETHICAL HACKING AND FORENSICS

Module 4: Network Forensics

Network Forensics

- Most attacks move through the network before hitting the target and they leave some trace. According to Locard's exchange principle, "every contact leaves a trace," even in cyberspace.
- Network forensics is a science that centers on the discovery and retrieval of information surrounding a cybercrime within a networked environment. Common forensic activities include the capture, recording and analysis of events that occurred on a network in order to establish the source of cyber attacks.

Network Forensics

- Network forensics can be particularly useful in cases of network leakage, data theft or suspicious network traffic. It focuses predominantly on the investigation and analysis of traffic in a network that is suspected to be compromised by cybercriminals (e.g., DDoS attacks or cyber exploitation).
- Accessing internet networks to perform a thorough investigation may be difficult. Most internet networks are owned and operated outside of the network that has been attacked. Investigation is particularly difficult when the trace leads to a network in a foreign country.

Network Forensics

- Data enters the network en masse but is broken up into smaller pieces called packets before traveling through the network. In order to understand network forensics, one must first understand internet fundamentals like common software for communication and search, which includes emails, VOIP services and browsers. One must also know what ISP, IP addresses and MAC addresses are.

Network Forensics

- Identification of attack patterns requires investigators to understand application and network protocols. Applications and protocols include:
- Web protocols (e.g., http and https)
- File transfer protocols (e.g., Server Message Block/SMB and Network File System/NFS)
- Email protocols, (e.g., Simple Mail Transfer Protocol/SMTP)
- Network protocols (e.g., Ethernet, Wi-Fi and TCP/IP)
- Investigators more easily spot traffic anomalies when a cyberattack starts because the activity deviates from the norm.

Network Forensics

- Methods
- There are two methods of network forensics:
- "Catch it as you can" method: All network traffic is captured. It guarantees that there is no omission of important network events. This process is time-consuming and reduces storage efficiency as storage volume grows
- "Stop, look and listen" method: Administrators watch each data packet that flows across the network but they capture only what is considered suspicious and deserving of an in-depth analysis. While this method does not consume much space, it may require significant processing power

Network Forensics

- Primary sources: Investigators focus on two primary sources:
- Full-packet data capture: This is the direct result of the "Catch it as you can" method. Large enterprises usually have large networks and it can be counterproductive for them to keep full-packet capture for prolonged periods of time anyway
- Log files: These files reside on web servers, proxy servers, Active Directory servers, firewalls, Intrusion Detection Systems (IDS), DNS and Dynamic Host Control Protocols (DHCP). Unlike full-packet capture, logs do not take up so much space

Network Forensics

- Network forensics is also dependent on event logs which show time-sequencing. Investigators determine timelines using information and communications recorded by network control systems. Analysis of network events often reveals the source of the attack.

Network Forensics

- Tools: Free software tools are available for network forensics. Some are equipped with a graphical user interface (GUI). Most though, only have a command-line interface and many only work on Linux systems.
- Here are some tools used in network forensics:
- EMailTrackerPro shows the location of the device from which the email is sent
- Web Historian provides information about the upload/download of files on visited websites
- Wireshark can capture and analyze network traffic between devices

Network Forensics

- According to “Computer Forensics: Network Forensics Analysis and Examination Steps,” other important tools include NetDetector, NetIntercept, OmniPeek, PyFlag and Xplico. The same tools used for network analysis can be used for network forensics.
- It is interesting to note that network monitoring devices are hard to manipulate. For that reason, they provide a more accurate image of an organization’s integrity through the recording of their activities

Network Forensics

- Network forensics is a subset of digital forensics. Compared to digital forensics, network forensics is difficult because of volatile data which is lost once transmitted across the network. Network forensics focuses on dynamic information and computer/disk forensics works with data at rest.
- Similarly to Closed-Circuit Television (CCTV) footage, a copy of the network flow is needed to properly analyze the situation. Due to the dynamic nature of network data, prior arrangements are required to record and store network traffic. The deliberate recording of network traffic differs from conventional digital forensics where information resides on stable storage media. Also, logs are far more important in the context of network forensics than in computer/disk forensics.

Collection and Acquisition in Wired Networks:

1. **Packet Capture**: The primary method for collecting data in wired networks is through packet capture. Packet capture involves intercepting and logging network traffic passing through a specific point in the network. Tools like Wireshark, tcpdump, and commercial network monitoring solutions are commonly used for packet capture.
2. **Network Taps**: Network taps are hardware devices installed at strategic points in the network infrastructure to capture and mirror network traffic. Taps provide full visibility into network traffic without introducing latency or affecting network performance.
3. **Port Mirroring (SPAN)**: Switched Port Analyzer (SPAN) or port mirroring is a feature available on managed switches that allows the traffic from one or more ports to be mirrored to a designated monitoring port. This enables the collection of network traffic for analysis and forensic investigation.
4. **Network Forensic Appliances**: Specialized network forensic appliances are available that are designed to capture and store network traffic for forensic analysis. These appliances often include advanced features for real-time monitoring, traffic analysis, and incident response.

Collection and Acquisition in Wireless Networks:

1. **Wireless Packet Capture**: Similar to wired networks, wireless packet capture involves intercepting and logging wireless network traffic. Tools like Wireshark with compatible wireless adapters or specialized wireless monitoring devices can be used to capture wireless packets.
2. **Wireless Intrusion Detection Systems (WIDS)**: Wireless intrusion detection systems are deployed to monitor wireless networks for unauthorized access, rogue devices, and security threats. WIDS sensors capture and analyze wireless traffic to detect and respond to security incidents in real-time.
3. **Wireless Access Points (WAPs)**: Wireless access points can be configured to log wireless client activity, association and disassociation events, authentication attempts, and other wireless network activities. These logs can provide valuable insights into wireless network usage and security incidents.
4. **Probe Requests and Responses**: Mobile devices and wireless clients regularly broadcast probe requests to discover available wireless networks. Monitoring and analyzing probe requests and responses can help identify nearby wireless networks and potential security risks.

Examinations of Network Forensics

- **Examinations of Network Forensics**
- The steps of a network forensics investigation are as follows:
- **Recognition**
- Because this step is the path to the case's conclusion, the identification process has a significant effect on the subsequent steps. The process of identifying and assessing an incident based on network indicators is included in this step.

Examinations of Network Forensics

- **Safeguarding**
- In the second step, the examiner would isolate the data for preservation and security purposes, preventing others from accessing the digital device and tampering with the digital evidence. Many software tools, such as Autopsy and Encase, are available for data preservation.
- **Accumulating**
- The act of documenting the physical scene and duplicating digital evidence using standardized processes and procedures is known as accumulating.

Examinations of Network Forensics

- **Observation**
- This procedure entails keeping track of all visible data. Many pieces of metadata from data may be discovered by the examiner, which may be useful in court.
- **Investigation**
- The investigation agents can reconstruct data fragments after recognizing and safeguarding the evidence (data). The agent draws a conclusion based on the evidence after analyzing the data. SIEM (Security Information and Event Management) software keeps track of what happens in the IT environment. With security information management (SIM), which gathers, analyses, and reports on log data, SIEM tools analyze log and event data in real-time to provide threat monitoring, event correlation, and incident response.

Examinations of Network Forensics

- **Documentation**
- Forensic is a legal term that means "to bring to the court". The procedure for summarizing and explaining conclusions has been completed. This should be written in layman's terms with abstracted terminologies, with all abstract terminologies referring to precise details.
- **Incident Response**
- The information gathered to validate and assess the incident led to the detection of an intrusion.

Analysis of network evidences

1. Analyzing network evidence from various sources such as Intrusion Detection Systems (IDS), routers, firewalls, and other network devices is a critical aspect of network forensics. These devices generate logs and alerts that provide valuable information about network activities, security incidents, and potential threats.

- **Intrusion Detection Systems (IDS):**

1. **Alert Logs**: IDS systems monitor network traffic for suspicious activity and generate alerts when predefined signatures or anomalous behavior are detected. Analyzing IDS alert logs involves reviewing the alerts, understanding the severity, impact, and context of each alert, and determining whether it indicates a security incident.
2. **Packet Capture**: Some IDS systems can capture and store packet-level data associated with detected alerts. Analyzing packet captures allows forensic analysts to reconstruct network sessions, examine packet payloads, and identify the source and nature of the detected intrusion attempts.
3. **Correlation with Other Logs**: Correlating IDS alerts with logs from other network devices, such as firewalls, routers, and authentication servers, can

Analysis of network evidences

- **Routers and Switches:**

1. **Syslog and SNMP Traps**: Routers and switches generate syslog messages and SNMP traps that provide information about network events, interface status changes, routing updates, and traffic statistics. Analyzing router and switch logs involves identifying abnormal behavior, routing issues, network errors, and potential security threats.
2. **NetFlow and sFlow**: NetFlow and sFlow are protocols used to collect and export network traffic flow data from routers and switches. Analyzing NetFlow and sFlow data allows forensic analysts to identify patterns, anomalies, and trends in network traffic, including top talkers, bandwidth utilization, and communication patterns between hosts.

Analysis of network evidences

- **Firewalls:**

1. **Firewall Logs**: Firewalls log information about allowed and denied traffic, rule violations, intrusion attempts, and firewall policy changes. Analyzing firewall logs involves reviewing firewall rules, identifying unauthorized access attempts, analyzing traffic patterns, and assessing the effectiveness of firewall policies in enforcing security controls.
2. **Packet Filtering**: Firewalls can be configured to capture and log packet-level data associated with specific firewall rules or security events. Analyzing packet filtering logs allows forensic analysts to examine packet headers, source and destination addresses, ports, protocols, and payload contents to identify malicious activities and security breaches.

Analysis of network evidences

- **Network Traffic Analysis:**

1. **Traffic Patterns and Anomalies**: Analyzing network traffic patterns and anomalies involves monitoring network traffic in real-time or retrospectively, identifying abnormal behaviors, identifying trends, and detecting indicators of compromise (IOCs) such as unusual communication patterns, spikes in traffic volume, and unauthorized access attempts.
2. **Protocol Analysis**: Analyzing network protocols involves dissecting protocol headers, examining protocol-specific behavior, and identifying protocol violations and anomalies that may indicate malicious activities or security incidents.
3. **Payload Analysis**: Analyzing packet payloads involves examining the contents of network packets, including data, commands, and file transfers, to identify malicious code, malware, data exfiltration attempts, and unauthorized access to sensitive information.

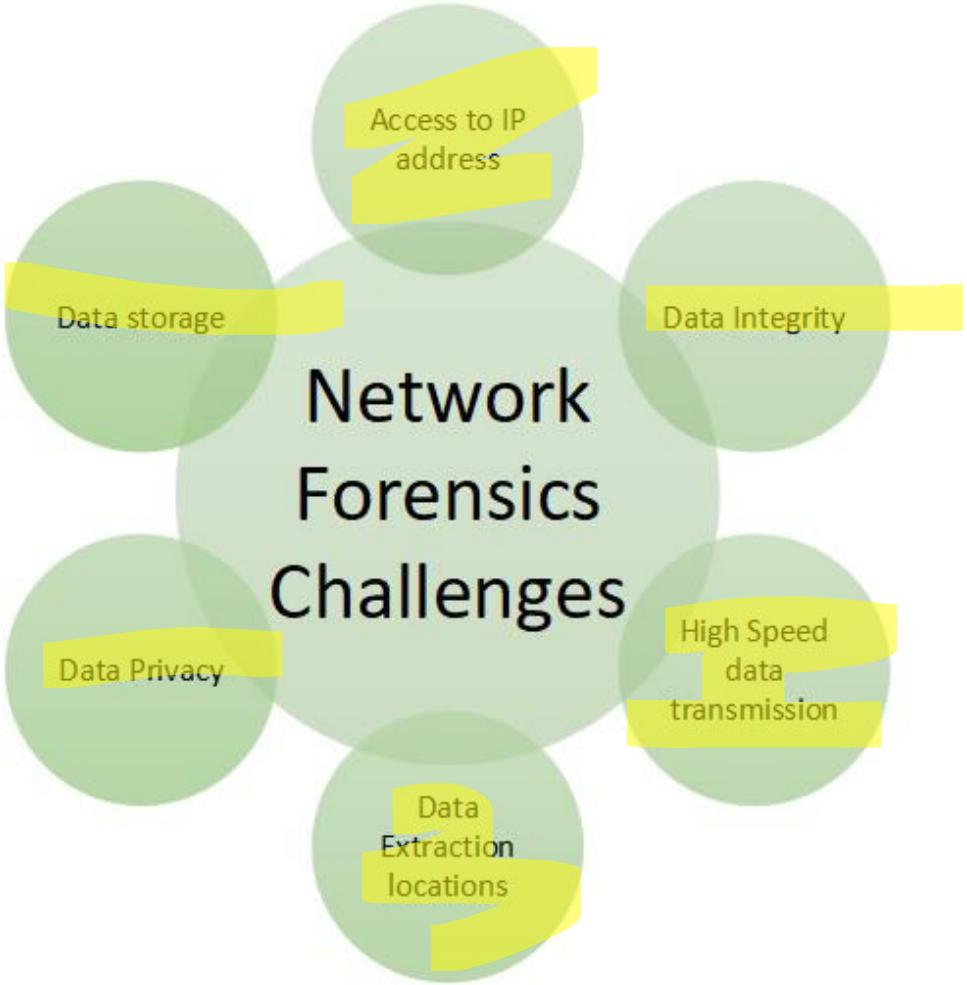
Challenges and Considerations:

1. **Encryption**: Encrypted traffic, such as SSL/TLS, can pose challenges for network forensic analysis, as the contents of encrypted packets are not readily readable without decryption keys.
2. **Legal and Privacy Concerns**: Adhering to legal and privacy regulations is essential when collecting and analyzing network traffic, especially when dealing with personally identifiable information (PII) or sensitive data.
3. **Packet Loss and Fragmentation**: In wireless networks, packet loss and fragmentation are common due to environmental factors, interference, and network congestion. Dealing with packet loss and reassembly of fragmented packets is a challenge in wireless packet capture and analysis.
4. **Data Integrity and Chain of Custody**: Maintaining data integrity and establishing a chain of custody is critical to ensure the admissibility and reliability of evidence collected during network forensic investigations.

Challenges in Network Forensics:

- **Challenges in Network Forensics:**
- The biggest challenge is to manage the data generated during the process.
- Intrinsic anonymity of the IP.
- Address Spoofing.

Challenges in Network Forensics:



Network Forensics

- **Advantages:**
- Network forensics helps in identifying security threats and vulnerabilities.
- It analyzes and monitors network performance demands.
- Network forensics helps in reducing downtime.
- Network resources can be used in a better way by reporting and better planning.
- It helps in a detailed network search for any trace of evidence left on the network.
- **Disadvantage:**
- The only disadvantage of network forensics is that It is difficult to implement.

Network device evidence

- There are a number of log sources that can provide CSIRT personnel and incident responders with good information. A range of manufacturers provides each of these network devices. As a preparation task, CSIRT personnel should become familiar on how to access these devices and obtain the necessary evidence:
- **Switches**
- **Routers**
- **Firewalls**
- **Web Proxy Servers**
- **Domain Controllers / Authentication Servers**
- **DHCP Server**
- **Application Servers**

Network device evidence

- **Network Intrusion Detection and Prevention systems:** An Intrusion Detection System (IDS) is a technology solution that monitors inbound and outbound traffic in your network for suspicious activity and policy breaches. As the name suggests, the primary purpose of an IDS is to detect and prevent intrusions within your IT infrastructure, then alert the relevant people. These solutions can be either hardware devices or software applications.
- Typically, an IDS will be part of a larger Security Information and Event Management (SIEM) system. When implemented as part of a holistic system, your IDS is your first line of defense. It works to proactively detect unusual behavior and cut down your *mean time to detect* (MTTD). Ultimately, the earlier you recognize an attempted or successful intrusion, the sooner you can take action and secure your network.

Network device evidence

- 5 DIFFERENT TYPES OF INTRUSION DETECTION SYSTEMS
- 1. NETWORK INTRUSION DETECTION SYSTEM
- 2. NETWORK NODE INTRUSION DETECTION SYSTEM
- 3. HOST INTRUSION DETECTION SYSTEM
- 4. PROTOCOL-BASED INTRUSION DETECTION SYSTEM
- 5. APPLICATION PROTOCOL-BASED INTRUSION DETECTION SYSTEM
-

Tools used in network forensics

1. **Wireshark**: Wireshark is a popular open-source packet analyzer that allows users to capture and interactively browse the contents of network traffic. It supports a wide range of protocols and provides detailed packet-level analysis, filtering, and packet reconstruction capabilities.
2. **tcpdump**: tcpdump is a command-line packet analyzer for Unix-like operating systems. It captures network packets and displays them in real-time or saves them to a file for offline analysis. tcpdump is often used in conjunction with other tools for network troubleshooting and forensic investigation.
3. **Zeek (formerly known as Bro)**: Zeek is an open-source network security monitoring tool that captures and analyzes network traffic in real-time. It generates high-level protocol logs and metadata, which can be used for network traffic analysis, intrusion detection, and forensic investigation.

Tools used in network forensics

1. **Snort**: Snort is an open-source network intrusion detection and prevention system (NIDS/NIPS). It analyzes network traffic in real-time and detects and responds to suspicious activities, malware infections, and security threats based on predefined rules and signatures.
2. **Security Information and Event Management (SIEM) Systems**: SIEM systems like Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), and QRadar are used to collect, correlate, and analyze logs and events from various sources, including network devices, servers, applications, and security appliances. They provide centralized visibility into network activities, security incidents, and compliance violations.
3. **Network Forensic Appliances**: Commercial network forensic appliances like NetworkMiner, Security Onion, and RSA NetWitness provide comprehensive capabilities for capturing, analyzing, and reconstructing network traffic, performing full-packet capture, and conducting forensic investigations.

Tools used in network forensics

1. **Nmap**: Nmap (Network Mapper) is a powerful open-source network scanning tool used for network discovery, host enumeration, service detection, and vulnerability assessment. It provides detailed information about network hosts, open ports, and running services, which can be useful for network reconnaissance and forensic analysis.
2. **NetWitness Investigator**: NetWitness Investigator is a free network forensic analysis tool provided by RSA Security. It allows users to conduct deep-packet inspection, search, and analysis of network traffic captured from various sources, including packet captures, logs, and network appliances.
3. **Tshark**: Tshark is a command-line version of Wireshark, designed for capturing and analyzing network traffic from the terminal. It provides similar functionality to Wireshark, including packet capture, filtering, and analysis, but without the graphical user interface.
4. **Volatility**: Volatility is an open-source memory forensics framework used for analyzing volatile memory (RAM) dumps from live systems. It allows forensic analysts to extract and analyze process memory, system artifacts, network connections, and other volatile data to investigate security incidents and