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

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.

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.

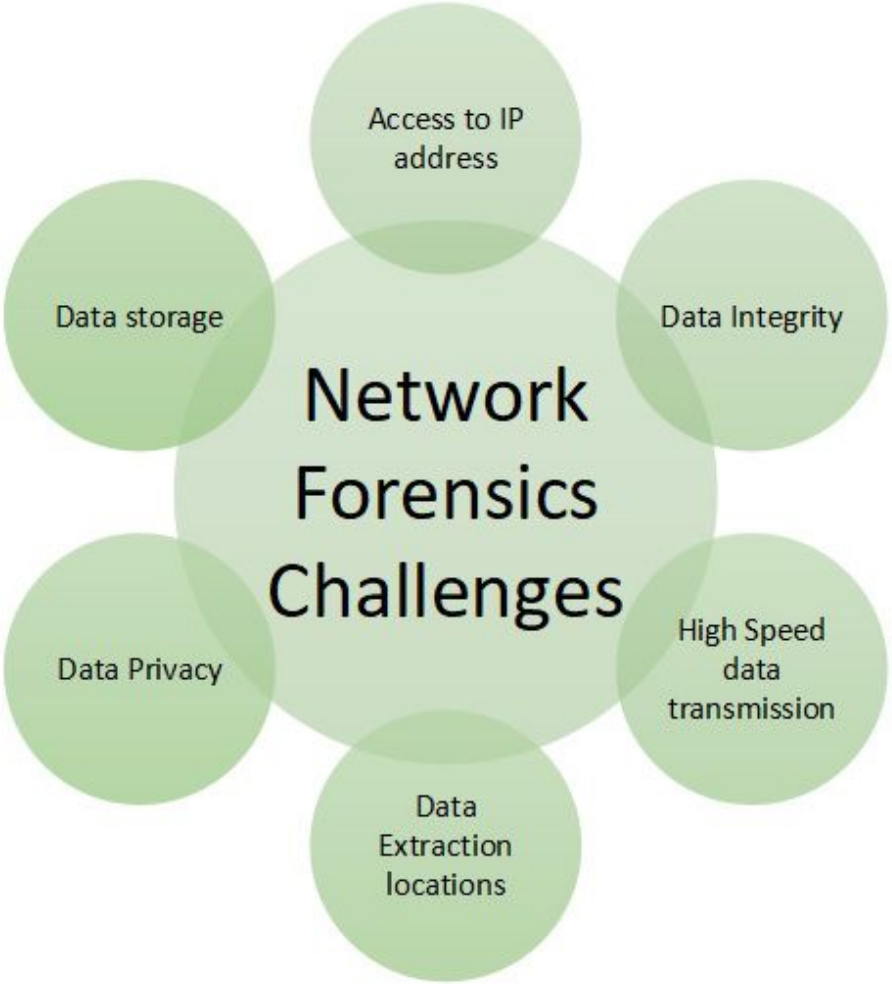
Examinations of Network Forensics

- **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.

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**

Network Forensics Tools

- **tcpdump**
- **Wireshark**
- **Network Miner**
- **Splunk**
- **Snort**