IA 311: Network Forensics

Lecture 1: Introduction

Network Forensics

- Network forensics involves capturing (fetching) the network traffic, and retrieving the data in reconnaissance from multiple devices, systems, processes, and other resources.
- The information given by network forensics is utilized to strengthen the security tools by understanding the modus operandi of the attacks.
- The available observations can be utilized in the future to prevent a potential threat to network security.

Network forensics …

- Network forensics is a branch of digital forensics that includes host based forensics which is usually crucial to any investigation process. Its importance stems from two observations:
  - Hosts are usually the target of a network attack. Even though an attacker might be interested in attacking a router to disrupt service, the more dangerous attack is the one that involves data theft or vandalism.
  - Hosts are a rich source of forensics data.

Network forensics …

- Broadly speaking, network forensics, in most people's perception, involves the CIA process. In this case, CIA stands for the following:
  - Capture (capture packets)
  - Identify (identify packets based on certain filtering criterion, such as date and time)
  - Analyze (both known and unknown packets to understand what's going on)

What is Network Forensics?

- Network forensics is the process of capturing information that moves over a network and trying to make sense of it in some kind of forensics capacity.
  - Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.
- A network forensics appliance is a device that automates this process.
- Wireless forensics is the process of capturing information that moves over a wireless network and trying to make sense of it in some kind of forensics capacity.

What is Network Forensics?

- Network forensics systems can be one of two kinds:
  - *"Catch-it-as-you-can" systems*, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage.
  - *"Stop, look and listen" systems*, in which each packet is analyzed in a rudimentary way in memory and only certain information saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.

What Purpose Does It Serve ?

- Allows us to find the details of network events after they have happened
- Eliminates the need to reproduce network problems
- Distill data to manageable levels by employing filters and analysis

Why Investigate Network Traffic?

The following are some of the reasons investigators analyze network traffic:

- Locate suspicious network traffic
- Know which network is generating the troublesome traffic and where the traffic is being transmitted to or received from
- Identify network problems

Network Forensics Challenges

- Two attacks make network forensics more challenging:
  - **IP Spoofing**: Change the source IP address in the header to that of a different machine and thus avoid traceback:
    - Traceback by storing some data in the routers
    - Traceback by adding some info in the packets.
  - **Stepping-Stone**: The attack flow may travel through a chain of stepping stones (intermediate hosts) before it reaches the victim:
    - Time-based sampling and matching.

Network vs. Security Forensics

- Network forensics is a superset of security forensics
- Forensics is not just DPI (Deep Packet Inspection)
- Requires the lossless capture, storage, and analysis of extremely large data volumes
- Network forensics: enterprise vs. lawful intercept
  - Concerned with the process of reconstructing a network event
    - Network or infrastructure outage
    - Intrusion such as a “hack” or other penetration
  - Provides a recording of the actual incident
- Based on live IP packet data captures
  - A new way of looking at trace file analysis
  - Continues from where traditional network troubleshooting ends

Computer Forensics vs Network Forensics

❖ Computer Forensics: The main characteristics of computer forensics are as follows:

- It deals with preservation, identification, extraction, documentation, and interpretation of computer-related data.
- It helps to find out the intention behind the attack but is unable to identify the main culprit.
- Handling of computer data is in line with the guidelines of civil procedures.
- The technical expert is always in better position than the attacker.
- It is comparatively easy to find the clues for experts.
- It follows the chronological sequence of custody and analysis of physical evidence and preserves this evidence.
- It acquires, preserves, and interprets the evidences.
- Skills of experts are better than the attacker.
- It helps you to identify all evidences quickly

Computer Forensics vs Network Forensics …

❖Network Forensics: The main characteristics of network forensics are as follows:

- Capturing, recording, and analyzing network clues to investigate the attacks.
- It helps to find out the source of attack and intention of the attack too.
- It is related to investigating through different security tools such as IDs, firewalls, etc.
- The skills of technical experts and the attacker are at the same level.
- To find the clues for experts is comparatively difficult.
- It is all about finding the clues through different tools and techniques.
- It is the incident response of the crime.
- Skills of experts are sometimes lesser than the attacker.
- It takes comparatively more time to identify all evidences than computer forensics.

Network Security vs Network Forensics

- Network Security: The main characteristics of network security are as follows:
  - Network security requires in real time.
  - It mitigates the probable risk to come inside of network.
  - It works round the clock to watch the network.
  - It is a continuous process.
  - It is a well-established field in computer science.

Network Security vs Network Forensics …

- Network Forensics: The main characteristics of network forensics are as follows:
  - Network forensics works after crime happens.
  - It is a post-mortem of an attack.
  - It works when it is required, i.e., when a crime is notified.
  - It is a time-bounded activity.
  - It is a nascent science.

Digital Forensics vs. Network Forensics

❖ Digital Forensics:

- Data is static and preserved even if power is cut.
- Evidence is contained within the file system.
- Making a forensically sound image is straightforward.
- Seizing a computer to obtain evidence might involve disruption to the existing file, storage and logs.
- Legal precedence in place and derived evidence is routinely admitted into court.

Digital Forensics vs. Network Forensics …

❖ Network Forensics:

- Data is changing constantly (dynamic).
- Pinpointing exact location of required evidence is problematic since this may involve direct evidence that can be obtained directly from single network device and some evidences can indirectly obtained from several network devices.
- Physical access to network devices can be difficult to obtain due to some geographical and legal constraints.
- Most network devices do not have persistent data storage.
- Investigators must minimize investigation impact on live business networks.
- Conflicting precedence and lack of standardization means courtroom admissibility is not guaranteed.
- Network Forensics requires deep understanding of network protocols and routing protocols such as Border Gateway Protocol (BGP), Interior Gateway Routing Protocol (IGRP) Routing Information Protocol (RIP), Ethernet, ARP, IP, TCP/UDP and a myriad of application layer protocols

Network Forensic Data

- Network-based forensic data is data residing on network devices or passing through a transmission medium (either wired or wireless).

Network Forensic Data …

❖Network forensic data is typically grouped into three main data types based on the associated tools and analysis techniques used:

- Full packet capture (PCAP)
  - A full copy of packets travelling over the network is captured.
  - Supports The most complete form of monitoring possible.
  - Requires considerable storage capacity. . Packet Brokering may be used to come up with scalable architecture for the data.
- Flow data (netflow)
  - Records summary data of conversations on the network.
  - Stores information such as time, duration, number of packets, total bytes sent, received, etc.
  - No application layer data recorded.
  - Suitable for gaining a quick understanding of how data flows on the network .
- Log / alert data (giant text files)
  - Text records are written to a file and the file is monitored .
  - Records of varying importance with high priority alerts generated by firewalls, IDs, IPs, etc.
  - There are a lot of log sources, so a management interface is required. Tools (e.g. Splunk) to explore large files of text records will also aid the investigative process and the data management task. .

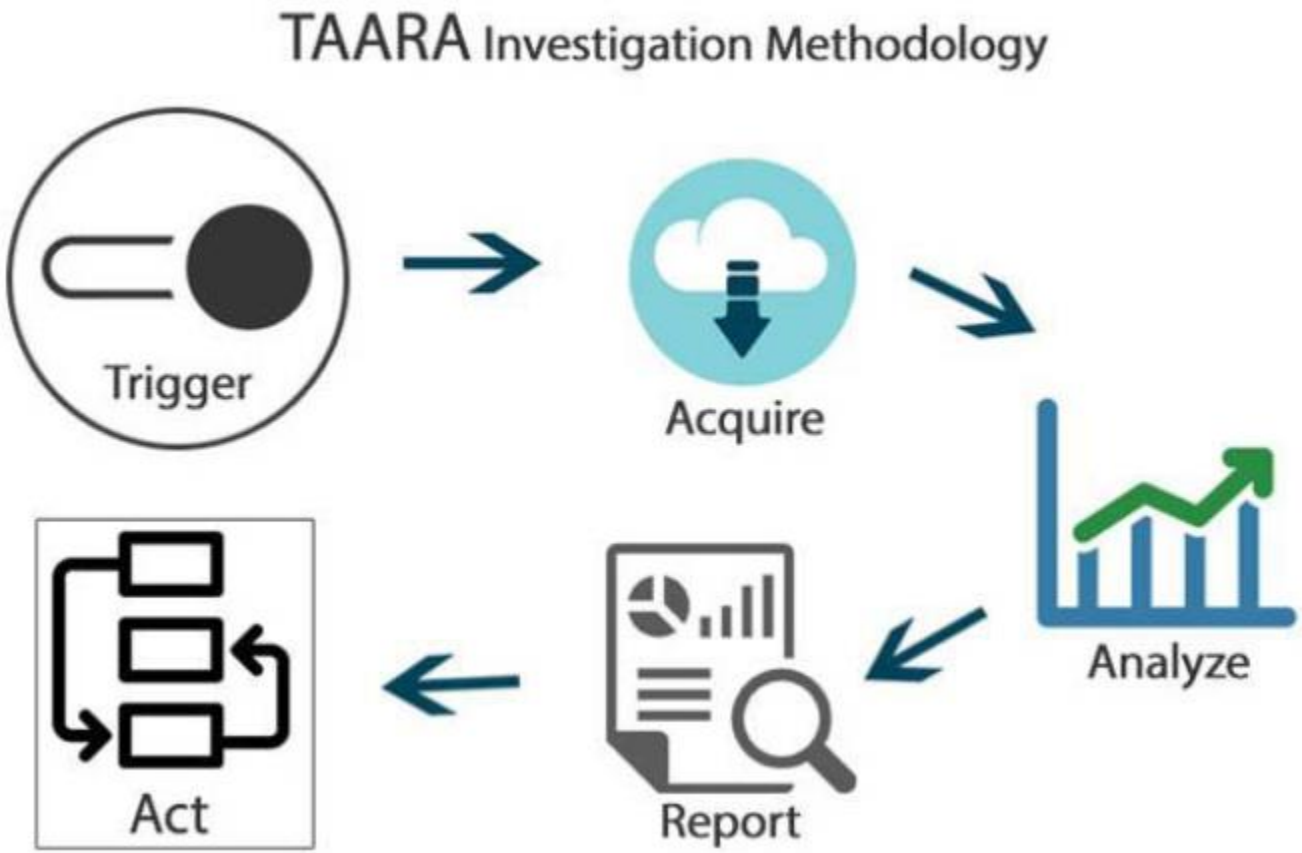
The TAARA methodology for network forensics

- To help simplify the understanding of the process, there is an easy-to-remember TAARA framework:
- Trigger: This is the incident that leads to the investigation.
- Acquire: This is the process that is set in motion by the trigger—this is predefined as a part of the incident response plan—and it involves identifying, acquiring, and collecting information and evidence relating to the incident.
  - This includes getting information related to the triggers, reasons for suspecting an incident, and identifying and acquiring sources of evidence for subsequent analysis.

The TAARA methodology for network forensics …

- Analysis: All the evidence that is collected so far is collated, correlated, and analyzed.
  - The sequence of events is identified. Pertinent questions such as whether the incident actually occurred or not; if it did, what exactly happened; how it happened; who was involved; what is the extent of the compromise; and so on are answered.
  - Based on the information that is gathered during this stage, it may be necessary to go back to the acquire stage in order to gather additional evidence.
  - Analysis is then initiated on the newly acquired evidence.
- Report: Based on the preceding analysis, a report is produced before the stakeholders in order to determine the next course of action.
- Action: The action recommended in the report is usually implemented during this stage.

The TAARA methodology for network forensics …



Best Practices for Network Forensics

- Capturing Network Traffic
  - Capture traffic continuously
  - Deploy a solution that captures traffic reliably
  - Set up filters to catch anomalies
- Storing Traffic
  - Allocate sufficient storage for the volume of data being collected
  - Adjust file sizes for the desired performance optimization
- Analyzing Traffic
  - Select a network forensics solution that supports filters and searches that are fast, flexible, and precise
  - Record baseline measurements of network performance
  - Use filters to zoom in on the problem at hand