IA 311: Network Forensics

Lecture 4: Sources of Network-Based Evidence

Introduction

- It worth noting that every environment is unique.
  - Compare large financial institutions Vs. Local government agencies or small health care offices.
    - They are different in terms of equipment (probably even in terms of configuration), staff, network topologies.

Introduction …

- There are many sources of network-based evidence in any networking environment.
  - The question is: How useful is the evidence on each device?
    - The answer varies depending on the type of investigation, the configuration of the specific device and the topology of the environment.
- NOTE:
  - Sometimes there may be an overlap of data from different sources – this is useful for correlation.
  - Sometimes the data sources are only complementary, each containing portions of evidence not found elsewhere.

Introduction …

- Here, we take a look at the commonly encountered types of network equipment as well as the types of evidence that can be recovered from them. These (sources of network-based evidence) include:
  - On the Wire
  - In the Air
  - Switches
  - Routers
  - DHCP Servers
  - Name Servers
  - Authentication Servers
  - Network Intrusion Detection/Prevention Systems
  - Firewalls
  - Web Proxies
  - Application Servers
  - Central Log Servers

On the Wire

- This refers to physical cabling
  - This provides connectivity between devices on a LAN and local switches as well as between switches and routers.
  - The cabling consists of:
    - Copper cables – in the form of either twisted pair (TP) or coaxial cable.
    - Fiber-optic cables
- Forensic value
  - The network forensics investigator can tap into the physical cabling to copy and preserve network traffic as it is transmitted across the cable.
    - There are commercial tools for tapping the transmitted data by replicating the data to a passive machine without degrading the original data.

In the Air

- Data transmits station-to-station signals is via “wireless” networking,
- It consists of radio frequency (RF) and (less commonly) infrared (IR) waves.
- Wireless networks can easily be deployed even without “line-of-sight”.
- RF waves can and do travel through air, wood, and brick, no se of cables.

In the Air …

- Forensics value
  - Wireless access points act as hubs, broadcasting all signals so that any station within range can receive them.
  - As a result, it is often trivial for investigators to gain access to traffic traversing a wireless network.

Switches

- Used to hold our LAN together and connect multiple stations.
- Switches connected to other switches and connect to other switches and form a complex switched network environment.
- Two types of switches
  - CORE aggregate traffic from many different segments.
  - EDGE aggregate stations on individual segments.

Switches …

- Forensics value
  - Switches contain a “content addressable memory” (CAM) table, which stores mappings between physical ports and each network card’s MAC address.
  - Using mac address investigator determine switches and corresponding port.
  - It also provide VLAN to capture traffic from the mirroring port with a packet sniffer.

Routers

- It connect different subnets or networks together and facilitate transmission of packets between different network segments.
- It allows LAN, MAN, WAN and GAN connections.
- Forensics value
  - Switches have CAM tables, routers have routing tables.
  - Tables map ports on the router to the networks that they connect.
  - This allows a forensic investigator to trace the path that network traffic takes to traverse multiple networks.

DHCP Servers

- Dynamic Host Configuration Protocol (DHCP) is widely used as the mechanism for assigning IP addresses to LAN stations which could change dynamically as needed.
- Forensic Value
  - —When DHCP servers assign (or “lease”) IP addresses, they typically create a log of the event, which includes the assigned IP address, the MAC address of the device receiving the IP address, and the time the lease was provided or renewed.
  - —Other details, such as the requesting system’s hostname, may be logged as well.

Name Servers

- Mechanism to map MAC addresses to IP addresses.
- Enterprises typically use the Domain Name System (DNS), in which individual hosts query central DNS servers when they need to map an IP address to a hostname, or vice versa.

Name Servers …

- Forensic Value
  - DNS servers can be configured to log queries for IP address and hostname resolutions.
  - DNS servers can log not only queries, but also the corresponding times.
    - —Therefore, forensic investigators can leverage DNS logs to build a timeline of a suspect's activities

Authentication Servers

- Theses servers are designed to provide centralized authentication services to users throughout an organization so that user accounts can be managed in one place, rather than on hundreds or thousands of individual computers.
- This allows enterprises to streamline account provisioning and audit tasks.

Authentication Servers …

- Forensic Value
  - Authentication servers typically log successful and/or failed login attempts and other related events.
  - Investigators can analyze authentication logs to identify brute-force password-guessing attacks, account logins at suspicious hours or unusual locations, or unexpected privileged logins, which may indicate questionable activities.

Network Intrusion Detection/Prevention Systems (NIDS/NIPS)

- NIDS/NIPS specifically designed to provide security analysts and forensic investigators with information about network security–related events.
- It monitors network traffic in real time for indication of any adverse events.
- When indications are detected they alert the security personals.

Network Intrusion Detection/Prevention Systems (NIDS/NIPS) …

- Forensic Value
  - Designed to provide for timely data pertaining to adverse event on the network.
  - Forensic investigators can request that network staff tune the NIDS to gather more granular data (source and destination IP addresses, the TCP/UDP ports, and the time the event occurred) for specific events of interest or specific sources and destinations

Firewalls

- Firewalls are specialized routers designed to perform deeper inspection of network traffic in order to make more intelligent decisions as to what traffic should be forwarded and what traffic should be logged or dropped.

Firewalls …

- Forensic Value
  - —They were most definitely designed to implement security policies to prevent violations.
  - —Firewalls can be configured to produce alerts and log allowed or denied traffic, system configuration changes, errors, and a variety of other events.

Web Proxies

- Web proxies are commonly used within enterprises for two purposes:
  - first, to improve performance by locally caching web pages and
  - second, to log, inspect, and filter web surfing traffic.
- End clients send their traffic through an anonymous web proxy so that the remote web server only sees the proxy's IP address rather than the end-user's IP address.

Web Proxies …

- Forensic Value
  - Web proxies are configured to retain granular logs for an extended period of time.
  - Investigator can produce the web surfing history for users of a single device.
  - It finds user's inappropriate web surfing habits, or identify the source of web-based malware.

Central Log Servers

- Central log servers aggregate event logs from a wide variety of sources, such as authentication servers, web proxies, firewalls, and more.
- Individuals servers send logs to central log servers, where they time stamped analyze and correlated.

Central Log Servers …

- Forensic Value: Devices such as routers, which typically have very limited storage space, may retain logs for very short periods of time, but the same logs may be sent in real time to a central log server and preserved for months or years.

Network Forensics Examination Steps

- A generic Network forensic examination includes the following steps:
  - **Identification**

    Identifying and investigating an incident originated from network indicators. This step is crucial as it impacts the following steps.
  - **Preservation**

    Shielding and isolating the state of physical and logical evidences in order to protect them from getting tampered due to external interference.
  - **Collection**

    Documenting the physical evidence and making copies of digital evidence using standardized methods and procedures.

Network Forensics Examination Steps …

– **Examination**

Comprehensive and exhaustive exploration of evidence pertaining to the network attack. It involves digging and inspecting potential evidence and assembling elaborate documentation for analysis.

– **Analysis**

This step involves rebuilding packets belonging to network traffic data and deduce significance based on evidence found.

– **Presentation**

Provide a brief summary and description of drawn conclusions.

– **Incident Response**

Craft a response to the intrusion detected curated based on details and evidence collected to substantiate and evaluate the incident.

Basic classes of network information

- There are four basic classes of network information that might be collected by the forensics examiner:
  - Full content data: Collect every bit of information, including packet headers, on the network.
  - Session data: Collect only the information pertinent to a particular investigation.
  - Alert data: Collect only data that includes particular items of interest.
  - Statistical data: Information that individually might not be suspicious but that, taken in the context of the overall network activity, indicates something remarkable.

Network Forensics with Network Protocol

- Network forensics methods can be applied within the different network protocols or layers:
  - Ethernet
  - TCP/IP
  - Internet
  - Wireless

Data-link and physical layer examined (Ethernet)

- Methods are achieved with eavesdropping bit streams on the Ethernet layer of the OSI model.
- This can be done using monitoring tools or sniffers such as Wireshark or Tcpdump
- Those tools allow investigator to filter traffic and reconstruct attachments transmitted over the network.
- Protocols can be consulted and analyzed, such as the ARP or any higher level protocols.
- The disadvantage of this method is that it requires a large storage capacity.

Transport and network layer Examined (TCP/IP)

- The network layer provides router information based on the routing table present on all routers
- It also provides authentication log evidence.
- Investigating this information helps determine compromised packets, identifying source, and reverse routing and tracking data.
- Network device logs provide detailed information about network activities.
- Multiple logs recorded from different network devices can be correlated together to reconstruct the attack scenario.
- Network devices have a limited storage capacity.
- Network administrators configure the devices to send logs to a server and store them for a period of time.

Traffic examined based on the use case (Internet)

- The internet provides numerous services such as WWW, email, chat, file transfer, etc. which makes it rich with digital evidence.
- This is achieved by identifying the logs of servers deployed on the internet.
- Servers include web servers, email servers, internet relay chat (IRC), and other types of traffic and communication.
- These servers collect useful log information, such as browsing history, email accounts (except when email headers are faked), user account information, etc.

Wireless

- This is achieved by collecting and analyzing traffic from wireless networks and devices, such as mobile phones.
- This extends normal traffic data to include voice communications.
- Phone location can be also determined.
- The Analysis methods of wireless traffic are similar to wired network traffic but different security issues should be taken into consideration.

Functions of a Network Forensics Analysis Tools

- Network traffic capturing and analysis
- Evaluation of network performance
- Detection of anomalies and misuse of resources
- Determination of network protocols in use
- Aggregating data from multiple sources
- Security investigations and incident response
- Protection of intellectual property