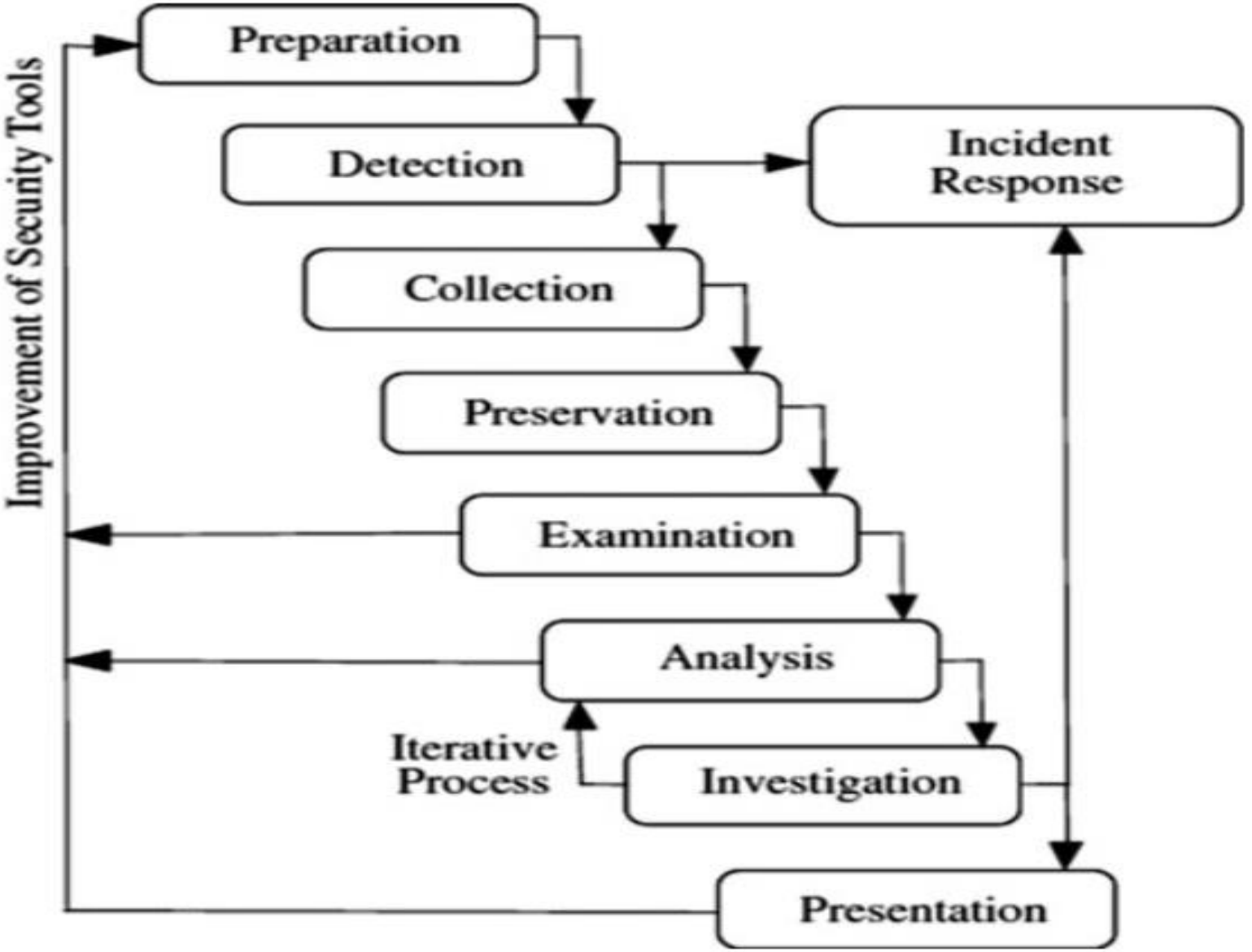
IA 311: Network Forensics

Lecture 2: Generic Process Model and Network Forensic Tools

Generic Process Model for Network Forensics

- Different phases of the Generic Process Model for network forensic framework are preparation, detection, incident response, collection, preservation, examination, analysis, investigation, and presentation.

Generic Process Model for Network Forensics …



Preparation

- In this phase various security tools such as intrusion detection system, firewall, packet analyzer, and traffic flow measure measurement are deployed at various strategic points on the network.
- All necessary legal documents are also acquired so that privacy is not violated.
- A proper training must be given to the staff working in this phase in order to facilitate attribution of the crime.
- The preparation phase reduces the overall cost of investigation.

Detection

- This phase is related to generating alerts for detected threats.
- The anomalies and illegitimate events are analyzed based on various parameters, and attacks are detected.
- By a quick validation the suspected attack is confirmed.
- Accordingly an important decision is taken whether to continue the investigation and generate the alert or ignore the alert.
- Various tools are used such as TcpDump, Wireshark, PADS, Sebek, Ntop, p0f, Bro, Snort, etc.
- This phase branches in two directions, incident response and collection.

Incident Response

- The response to the crime is dependent on the gathered information to validate and assess the incidents.
- An organization policy is kept in place while responding to attack.
- The response also depends on the type of the attack identified.
- Meanwhile, a decision is taken whether to continue with the investigation or gather more information.
- An important criterion to respond to an incident while performing network forensic analysis is to ensure that data being collected as evidence is neither tampered nor obstructed.

Collection

- Data are acquired from the sensors used to collect the traffic data.
- The sensors used must be secure, must be fault tolerant, must have limited access, and must be able to avoid compromise.
- A well-defined procedure using reliable hardware and software tools must be in place to gather maximum evidence causing minimum impact to the victim.
- The network must be monitored to identify future attacks.
- The integrity of data logged and network events recorded must be ensured.
- This phase is very significant as the traffic data change at a rapid pace, and it is not possible to generate the same trace at a later time.
- Due to the enormous amount of data logged, huge memory space is required, and the system must be versatile in nature and able to handle different log data formats appropriately.
- Various tools used in this phase are TCPDump, Wireshark, PADS, Sebek, LiLK, TCPReplay, Snort, Bro, etc.

Preservation

- The collected traces and logs are stored on a backup device like read-only media.
- A hash of all the traces is preserved.
- The analysis is carried out over the copied data, and the original data is kept untouched.
- This step is carried out to prove the investigation when the process is repeated on original data to facilitate the legal requirements.
- Various tools used in this phase are TCPDump, Wireshark, PADS, Sebek, LiLK, TCPReplay, Snort, Bro, etc.

Examination

- Traces are integrated and fused as a large data set on which the analysis is performed.
- There can be some issues like redundant information and overlapping time zones which need appropriation.
- Alerts from various sources may be contradictory.
- However, this process needs to be done in such a manner so that crucial information from important sources is not lost.
- The collected data is classified and clustered into groups so that the volume of data to be stored may be reduced to manageable chunks.
- It is easy to analyze large groups of organized data.
- The collected evidence is searched methodically to extract specific indicators of the crime.
- Minimum attack attributes selected must be so credible that the least information recorded, contains the highest probable evidence.
- Feedback is given to improve the security tools.
- Various tools used are TCPDump, Wireshark, TCPFlow, Flow-tools, NfDump, PADS, Argus, Nessus, Sebek, TCPTrace, Ntop, TCPStat, NetFlow, TCPDstat, ngrep, TCPXtract, SiLK, TCPReplay, P0f, Nmap, Bro, Snort, etc.

Analysis

- This phase performs analysis on data using various approaches like data mining such as ANN, fuzzy, and genetic algorithm (GA) and statistical computing to search of attack patterns in the data.
- Some of the critical parameters are related to network connection establishment, DNS queries, packet fragmentation, protocol, and operating system fingerprinting.
- The attack patterns are reconstructed and replayed to understand the intention and methodology of the attacker.
- Feedback is given to improve the security tools.
- The tools include TCPDump, Wireshark, TCPFlow, Flow-tools, NfDump, PADS, Argus, Nessus, Sebek, TCPTrace, Ntop, TCPStat, NetFlow, TCPDstat, ngrep, TCPXtract, SiLK, TCPReplay, P0f, Nmap, Bro, Snort, etc.

Investigation

- Investigation is performed to determine the path from a victim network or system through any intermediate systems and communication pathways back to the point of attack origination.
- Packet statistics are obtained for attribution of the attack.
- This phase may require some additional features from the analysis phase, and hence these two phases are iteratively performed to arrive at the conclusion.
- Attribution is establishing the identity of the attacker and is the most difficult of network forensics.
- The investigation phase provides data for incident response and prosecution of the attacker.

Presentation

- The observations are presented in an understandable language for legal personnel while providing an explanation of the various procedures used to arrive at the conclusion.
- Legal requirements must be fulfilled, and systematic documentation is presented to authorities.
- The findings are also presented using visualization so that they can be easily grasped.
- The statistical data is interpreted in support of the conclusions arrived.
- A thorough review of the incident is done, and countermeasures are recommended to prevent similar incidents in the future.
- The entire case is documented to influence future investigations and to provide feedback to guide the deployment and improvement of security products.
- This process concludes the network forensic analysis as the information presented results in the prosecution of the attacker.

Network Forensic Analysis Tools (NFAT)

❖NetDetector

- NetDetector integrates signature-based IDS with statistical anomaly detection with full-application reconstruction, packet level decoding, etc.
- NetDetector informs the user about the security breaches and can take preventive measures such as blocking the malicious traffic from entering the system.
- Some key features of the NetDetector are as follows:
  - Big data security and intelligence
  - Reconstruction of applications and sessions
  - Integrated signature-based IDS and anomaly detection
  - Traffic capture and multi-timescale analysis
  - Ad hoc and scheduled reporting

NetIntercept

- ❖NetIntercept is available as a complete system, with hardware and pre-installed software, ready to deploy forensic solution.
- NetIntercept can be placed in the machine room or at the firewall.
- NetIntercept records the traffic in hard disk; hence, traffic from the last hours, days, or weeks is available for the analysis.
- The analysis is generally analyzed in batch mode.
- NetIntercept correlates user sessions and reconstructs transmitted or received files, providing immediate proof of the misbehavior.
- NetIntercept aims to answer following basic questions:
  - Who sent what information where
  - Why information isn’t moving
  - How the system was attacked

OmniPeek

- OmniPeek provides real-time visibility into every part of the network.
- It has high capture capabilities, centralized console, distributed engines, and expert analysis.
- OmniPeek supports Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n/ac wireless, VoIP, video, MPLS, and VLAN.
- OmniPeek is available in four versions: basic, professional, enterprise, and connect.
- Each version provides some unique features and supports different types of networks.

Python Forensic Log Analysis GUI (PyFLAG)

- PyFLAG is a Web-based, database-backed forensic and log analysis tool written in python.
- PyFlag analyzes captured packets in libpcap format while supporting a number of network protocols.
- It has the ability to recursively examine data at multiple levels and is ideally suited for network protocols which are typically layered.
- PyFlag parses the pcap files, extracts the packets, and dissects them at lowlevel protocols (IP, TCP, or UDP).
- Related packets are collected into streams using a reassembler.
- These streams are then dissected with higher-level protocol dissectors such as HTTP, IRC, etc.

Xplico

- Xplico is an open-source forensic analysis tool for UNIX-like systems.
- Xplico is capable of reconstructing a protocol's application data from captured packets.
- Xplico was specifically created for reconstruction of protocol data.
- It employs as technique named Port Independent Protocol Identification (PIPI) for recognizing the protocols.
- Xplico dissects data at the protocol level and reconstructs and normalizes it for use in manipulators.
- The manipulators then transcode, correlate, and aggregate data for analysis and present the results in a visualized form.

Vulnerability Assessment Tools

❖Metasploit

- Metasploit is basically a penetration testing framework.
- It provides a platform for developing, testing, and using “exploits” to take advantage of a system’s vulnerabilities.
- Originally Metasploit was open source but Rapid7 acquired it in 2009.
- It is available for Windows, Linux, and MAC in GUI and a CLI-based interface.

Nessus

- Nessus is a vulnerability-scanning tool for Windows, Linux, Solaris, FreeBSD, and MAC.
- Nessus is owned by Tenable Network Security.
- It is available in four versions, Nessus evaluation, Nessus, Nessus Perimeter Service, and Nessus Home.
- Nessus offers new vulnerability checks in a form of “plug-in” on a daily basis.
- It is also used for DoS attack scan, port scan, password vulnerabilities.
- The vulnerability checks are available for free for home users and written in Nessus Attack Scripting Language (NASL).

Nikto

- Nikto is an open-source (GPL) Web server vulnerability scanner.
- Nikto scans the server for dangerous files/CGIs, outdated server softwares, and version-specific bugs.
- It also checks for server configuration items such as index files, server options, etc.
- Nikto presently scans for over 6700 dangerous files/CGIs, version-specific bugs on over 270 servers, and outdated version of over 1250 servers.

Yersinia

- Yersinia is a network security tool for performing layer 2 attacks. It is designed to take advantage of weaknesses of layer 2 protocols for UNIX-like systems.
- Yersinia is still under development and supports only a limited number of protocols, such as Dynamic Host Configuration Protocol (DHCP), Dynamic Trunking Protocol (DTP), Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), Cisco Inter-Switch Link (ISL), VLAN Trunking Protocol (VTP), Hot Standby Router Protocol (HSRP), IEEE 802.1Q, and IEEE 802.1X.

Wikto

- Wikto is a Web server assessment tool that checks for flaws in Web servers.
- Wikto scans the Web server to find directories and files stored on that server.
- It looks for known vulnerabilities and other scripts that can be abused or exploited in the server implementation.
- Wikto can be seen as Nikto for Windows, only with some extra added features such as a fuzzy logic-based error code checking, back-end mining capabilities, Google-assisted directory mining, real-time HTTP request/response monitoring, etc.

Acunetix Web Vulnerability Scanner

- Acunetix Web vulnerability scanner is an application that automatically checks an entire Web site or Web application for security vulnerabilities.
- Acunetix Web vulnerability scanner is capable of scanning the entire code and scripts for possible vulnerabilities that can be exploited.
- It also includes some penetration testing tools to automate the whole process.
- It creates fake attacks and checks the response of the Web site against the attack.
- After scanning it displays a detailed report of what it has found and how to improve the security.
- Some features of Acunetix WVS are testing for SQL injection and cross site scripting testing, support for CAPTCHA pages, multithreaded scanning, port scans a Web server and runs security checks against network services running on the server, and advanced penetration testing tools, (e.g., HTTP Editor and the HTTP Fuzzer).

Network Sniffing and Packet Analyzing Tools

❖Wireshark

- Wireshark is an open-source packet and protocol analyzer.
- Wireshark is cross platform and runs on GNU/Linux, Windows, OS X, BSD, and other UNIX-like operating systems.
- Wireshark uses “libpcap” to capture packets from the network hence works only on networks that supports libpcap.
- Data from an already captured packet can also be read as an input for the analysis.
- The main features of Wireshark include:
  - Support for Ethernet, IEEE 802.11, PPP, and loopback.
  - Live capture and offline analysis.
  - Interactive GUI as well as command line version.
  - Plug-ins can be created for analyzing new protocols.
  - Provides rich VoIP analysis.
  - Output can be exported to a number of file formats such as XML, CSV, plain text, and PostScript.

Aircrack-ng

- Aircrack-ng is a network software suite for IEEE 802.11 wireless local area networks.
- Primarily it consists of a detector, packet sniffer, WPA/WPA2-PSK, and WEP cracking and analysis tool.
- Aircrack-ng is available for Windows and Linux and works with any wireless network interface card (NIC) which supports monitoring mode.

WebScarab

- WebScarab is written in Java and analyzes applications that use HTTP and HTTPS protocols for communication.
- WebScarab operates as an intermediate proxy between the Internet and the application, allowing to review and modify the outgoing requests and incoming responses.
- WebScarab has several features in form of plug-ins such as:
  - Proxy: To observe the traffic between the application and the Web.
  - Manual Intercept: Allows user to modify and requests and responses (HTTP and HTTPS) before they reach to the server.
  - Manual Request: Allows manual editing or replaying of previous request or to create entirely new requests.
  - Bandwidth Emulator: Allows user to emulate a slower network.

ngrep

- “ngrep” is an open-source network packet analyzer for Linux and can be imported to other UNIX-like operating systems.
- ngrep can look for traffic originating from a specific port and can search for a regular expression in the payload of the packet.
- ngrep allows user to see all the unencrypted traffic on the network.
- It supports a wide number of protocols: IPv4 and IPv6, TCP, UDP, ICMPv4 and ICMPv6, IGMP, SLIP, PPP, FDDI, Ethernet, etc.

NetworkMiner

- NetworkMiner is a forensic network sniffing tool for Windows and can detect IPs, host names, Operating Systems, and open ports.
- It can also extract files transmitted over the network.
- NetworkMiner collects data about the hosts rather than collecting data about the traffic.
- The main user interface is host centric information grouped per host.

Kismet

- Kismet is a wireless network detector and sniffer.
- Kismet works with any wireless adapter which supports raw monitoring mode (rfmon).
- Kismet is capable of detecting standard-named (SSID) networks as well as hidden and non-beaconing networks.
- Kismet passively collects packets without interfering in the network traffic.

eMailTrackerPro

- eMailTrackerPro offers the ability to trace an e-mail using the e-mail header and the e-mail id itself to its originating location.
- The advanced version of the eMailTrackerPro also comes with a spam filter, which scans each incoming e-mail for their suspected spam nature.
- eMailTrackerPro can trace multiple IPs and domains at the same time.

Network Scanning Tools

❖Nmap

- Nmap (“Network Mapper”) is an open-source, cross platform free network discovery and port scanning tool.
- It is also useful for mapping an IP to its relative host information. Nmap also offers details about services the hosts’ are providing and answers to questions like – what OS is being used? Or what types of packet filter/firewall is being used? etc.
- Nmap comes with the following options: Zenmap (a GUI result viewer), Ncat (a data transfer and debugging tool), Ndiff (a utility for comparing the scan results), and Nping (packet generation and response analysis tool).

Angry IP Scanner

- Angry IP Scanner (or IPScan) is an open-source IP address and port scanner.
- It can scan IP address in any range by pinging them and then resolving its host name, MAC address, scan ports, etc.
- It is lightweight and works on cross platform.
- It does not need to be installed as it can be run from a browser, the only prerequisite being Java Runtime Environment (JRE).
- The scanning results can be saved in various file formats such as CSV, TXT, XML, and IP-Port list file.
- IP Scanner uses multithreaded approach to speed up the scanning process.
- For each IP address, a separate thread is created.
- The functionality of IP Scanner can be extended using plug-ins.

Wireless Network Watcher

- Wireless network watcher is a small utility by NirSoft, Inc.
- It scans the wireless network and displays a list of all the nodes and devices that are currently connected to the network.
- The scan results can also be exported in HTML, CSV, XML, or text format.
- For every device connected to the network, the following information is displayed: IP address, MAC address, NIC manufacturer, device name, first detection date, and active status.

Network Monitoring Tools

❖IPTraf

- IPTraf is an open-source console-based network statistics utility for UNIX-like systems.
- It collects a variety of network traffic-related figures such as TCP and UDP packet counts, byte counts, host activities, and interface statistics.
- IPTraf supports a number of interfaces such as Ethernet, FDDI, ISDN, SLIP, PPP, etc.
- IPTraf supports a wide number of packet types: IP, TCP, UDP, IGMP, ICMP, OSPF, IGP, ARP, and RARP.

VisualRoute

- VisualRoute is a connectivity diagnostic tool that displays ping and traceroute results in an effective visual form.
- VisualRoute is primarily used for troubleshooting connectivity issues, performance evaluation of a link on the basis of packet loss, and latency.
- VisualRoute generates an interactive ping and whois information with time graphs.
- The results of VisualRoute trace can be exported to a text, HTML reports, or JPG screenshots.
- The main features of VisualRoute are as follows: IP location reporting, whois lookup, multipath discovery, port testing, port probing, DNS performance testing, traceroute and reverse tracing, etc.

Ntop

- Ntop is a network probe that shows network statistics.
- It has two modes, interactive mode and web mode.
- In interactive mode, it shows the network status on the terminal.
- In web mode, it acts as a web server and creates an HTML dump of network status and shows it in the form of Web pages, with graphs and other statistical figures.
- Ntop can sort traffic according to many protocols, analyze IP traffic, and sort according to the source or destination.
- It can also geo-locate the hosts.

TCPStat

- TCPStat reports TCP-related statistics by reading a TCPDump file or by monitoring an interface.
- It shows statistics like bandwidth, number of packets, average packet size, interface load, standard deviation of packet size, etc.
- TCPStat is capable of handling a large number of packets per second and has a compact interface.

Intrusion Detection Systems (IDS)

❖Snort

- Snort is a network intrusion detection system (NIDS) designed for IP-based networks.
- Snort analyzes the network traffic and packets to detect worms, vulnerability exploits, port scan, and other suspicious behavior.
- Snort primarily works in three modes: in sniffer mode, it just reads the network packets and displays on a console; in logger mode, it logs and saves the packets to the disk; and in intrusion detection mode, it analyzes the network traffic against defined rule sets.
- Snort rules can also be defined by users and checks various attributes of packets whether the traffic should be allowed or blocked.

Bro

- Bro is an open-source, passive NIDS for UNIX-like systems.
- Bro is primarily a network monitor that scans for suspicious link traffic in depth.
- Bro records the network activities in log files in high-level terms.
- Bro can log all HTTP requests along with their requested URI, headers, MIME types, DNS request-responses, SSL certificates, SMTP sessions, and much more.
- Bro can be viewed as a platform for traffic analysis.
- Bro is fully customizable, and new analysis task can easily be added by the means of scripts.
- Bro comes with a predefined standard library and supports a wide range of features for detecting intrusions.