Professional Certificate in Digital Forensics Fundamentals

Network Forensics

Analysis: The process of interpreting and making sense of data in order to draw conclusions or support decision-making. In the context of network forensics, analysis involves examining network traffic and logs to identify suspicious or malicious activity.

Capturing Packets: The process of intercepting and recording data packets as they travel across a network. This is often done using a network tap or a tool like Wireshark.

Computer Network: A group of interconnected devices, such as computers, servers, and routers, that are able to communicate with each other and share resources.

Digital Forensics: The process of collecting, analyzing, and preserving digital evidence in order to investigate cybercrimes or other security incidents.

Evidence: Any data or information that can be used to support a claim or argument. In the context of network forensics, evidence may include network logs, packet captures, and other data that can be used to investigate security incidents.

Firewall: A security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Honeypot: A security resource whose value lies in being probed, attacked, or compromised. Honeypots are used to detect, deflect, or study attempts to access a computer or network system for malicious purposes.

Intrusion Detection System (IDS): A system that monitors network traffic for suspicious activity and sends alerts when such activity is detected.

Logs: Records of events or transactions that have occurred on a computer or network. Logs can provide valuable information for network forensics investigations.

Network Forensics: The process of collecting, analyzing, and preserving evidence from a computer network in order to investigate security incidents.

Network Tap: A device that allows network traffic to be passively monitored without interfering with the normal flow of data.

Packet: A small unit of data that is sent over a network. Packets contain a header, which includes information about the source and destination of the data, and a payload, which contains the actual data being sent.

Payload: The actual data that is contained in a packet.

Sniffing: The process of intercepting and analyzing data packets as they travel across a network. This is often done using a network tap or a tool like Wireshark.

Traffic Analysis: The process of examining and interpreting network traffic in order to understand the behavior and patterns of network users and devices.

Wireshark: A popular open-source tool for capturing, analyzing, and displaying network traffic.

Zero Day Exploit: A security vulnerability that is unknown to the software vendor and for which no patch is available. Zero day exploits are often used by attackers to gain unauthorized access to a system or network.

Address Resolution Protocol (ARP): A protocol used to maps an IP address to a physical (MAC) address on a local area network (LAN).

Denial of Service (DoS) Attack: An attack that floods a network or server with traffic in order to make it unavailable to legitimate users.

Domain Name System (DNS): A system that translates domain names (such as www.example.com) into IP addresses (such as 192.0.2.1).

Ethernet: A standard for wired local area networks (LANs) that specifies the physical and data link layers of the network protocol stack.

Firewall Rules: The set of rules that determine what traffic is allowed to pass through a firewall.

Header: The portion of a packet that contains information about the source and destination of the data, as well as other metadata.

Hashing: A one-way function that maps data of arbitrary size to a fixed size. Hashing is often used for data integrity checks.

Hypertext Transfer Protocol (HTTP): The protocol used for transmitting hypertext requests and information between servers and browsers.

Hypertext Transfer Protocol Secure (HTTPS): A secure version of HTTP that uses encryption to protect the data being transmitted.

Initial Sequence Number (ISN): A number used in the TCP protocol to ensure that each data packet is uniquely identified and can be reassembled in the correct order.

Intrusion Prevention System (IPS): A system that monitors network traffic for suspicious activity and takes action to prevent or mitigate potential attacks.

Internet Control Message Protocol (ICMP): A protocol used for error reporting and diagnostic functions in the Internet protocol suite.

Internet Message Access Protocol (IMAP): A protocol used for accessing and managing email messages on

a remote server.

Internet Relay Chat (IRC): A protocol for real-time communication in the form of text messages.

Internet Service Provider (ISP): A company that provides access to the internet.

Internet of Things (IoT): A network of interconnected devices, such as sensors, appliances, and vehicles, that are able to collect and exchange data.

IP Address: A unique numerical label assigned to every device connected to the internet.

IP Spoofing: The act of disguising the true origin of an IP packet by falsifying the source IP address.

IPv4: The fourth version of the Internet Protocol (IP), which uses 32-bit addresses.

IPv6: The sixth version of the Internet Protocol (IP), which uses 128-bit addresses.

Jitter: The variation in the delay of packets as they travel across a network.

Latency: The delay between the request for a piece of data and the response.

Link Layer Discovery Protocol (LLDP): A standard protocol used for discovering and sharing information about devices on a local area network (LAN).

Log Files: Files that contain records of events or transactions that have occurred on a computer or network.

Man-in-the-Middle (MitM) Attack: An attack in which an attacker intercepts and alters the communication between two parties in order to eavesdrop or inject malicious data.

Media Access Control (MAC) Address: A unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

Network Address Translation (NAT): A method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit.

Network Interface Card (NIC): A computer hardware component that connects a computer to a network.

Network Layer: The third layer of the OSI model, responsible for the delivery of packets from the source host to the destination host.

Network Layer Protocols: Protocols that operate at the network layer of the OSI model, such as IP and ICMP.

Network Sniffer: A tool used for capturing and analyzing network traffic.

Open Systems Interconnection (OSI) Model: A conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.

Payload: The actual data that is contained in a packet.

Port: A numerical label assigned to a specific process or service running on a host.

Promiscuous Mode: A mode in which a network interface card (NIC) is able to receive and process all packets on a network, rather than just those addressed to its own MAC address.

Protocol: A set of rules governing the format of data sent over a network and the steps needed for two devices to communicate.

Proxy Server: An intermediary server that forwards requests from clients to other servers and returns the responses.

Quality of Service (QoS): The description or measurement of the overall performance of a service, such as a telephony or computer network.

<