THE UNIVERSITY OF DODOMA

COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)

GROUP ASSIGNMENT 6.

COURSE NAME: NETWORK FORENSIC

COURSE CODE: IA 311

PROGRAM: Bsc.CNISE

GROUP PARTICIPANTS

NAMES	REGISTRATION NUMBER
GABRIEL MBETI	T22-03-02516
HENRY SELEMAN	T22-03-00295
PUDENCIANA PETER	T22-03-11584
AMANI MLIMANDOLA	T22-03-05155
IBRAHIMU BONIFACE	T22-03-05565
JIMSON MAHENGE	T22-03-08372
PETRO MOHERE	T22-03-02116
GEORGE KALAMU	T22-03-08400
NASSIBU ALLY	T22-03-01214
EMMANUEL WOLFGANG	T22-03-09178

THESE ARE SOME NETWORK LAYER ATTACKS

1. **Denial of Service (DoS) Attack**

A Denial of Service (DoS) attack aims to make a network resource unavailable to legitimate users by overwhelming it with malicious traffic or exploiting vulnerabilities.

Types of DoS Attacks:

- **Flood Attacks:** Overwhelm the target with excessive requests, e.g., Ping Flood, SYN .
- **Application Layer Attacks:** Target specific applications or services, e.g., HTTP Flood.
- **Exploitation of Vulnerabilities:** Exploit protocol weaknesses to cause disruption, e.g., Ping of Death, Teardrop Attack.

Distributed Denial of Service (DDoS):

A more severe variant where multiple compromised systems, often part of a botnet, attack a single target simultaneously.

2. **Corrupt Packet**

A corrupt packet occurs when data packets transmitted over a network become altered, damaged, or tampered with during transmission. Corruption can happen due to various reasons:

- **Physical layer issues:** Poor cabling, interference, or faulty hardware.
- **Transmission errors:** Signal degradation, bit flips, or electromagnetic interference.
- **Deliberate tampering**: Attackers may intentionally corrupt packets to disrupt network communications.

Detection :

- Error-Detection Mechanisms: Protocols like TCP/IP use error-checking mechanisms, such as checksums and cyclic redundancy checks (CRC), to detect and discard corrupt packets.
- Retransmission: If a corrupt packet is detected, protocols like TCP will request retransmission to ensure data integrity.

3. **IP address spoofing.**

Spoofing is the act of disguising a communication or identity so that it appears to be associated with a trusted, authorized source. Ip address spoofing occurs if the IP header fields and lengths are known, the IP address in the IP datagram can be easily discovered and spoofed.

Detection :

- **Packet filtering:** Uses ingress and egress filtering to examine incoming and outgoing packets for suspicious activity:
    - **Ingress filtering:** Checks incoming packets to see if the source IP header matches a permitted source address.
    - **Egress filtering:** Checks outgoing packets to see if the source IP address matches those on the organization's network.
- **Network monitoring:** Monitors networks for suspicious activity.
- **Traffic analysis:** Uses traffic analysis and filtering techniques to identify and divert suspicious traffic.
- **Spoofing detection software:** Uses spoofing detection software to prevent spoofing network attacks.

4. **Man in the Middle Attack.**

   This attack occurs when a hacker places himself or herself between the source and destination computer in such a way that neither notices his or her existence. Meanwhile, the attacker can modify packets or simply view their contents.

Detection :

- Check the URL: Look for a lack of "S" in HTTPS or any other unusual address.
- Watch for disconnections: Look for frequent disconnections or connections to unfamiliar locations.
- Be careful on public Wi-Fi: Avoid public Wi-Fi networks and choose your network to "public" to disable network discovery .

5. **Incorrect reassembly of fragmented datagrams.**

   For fragmented datagrams, the Offset field is used with packet reassembly. If the offset is changed, the datagram is reformed incorrectly. This could allow a datagram that would typically not pass through a firewall to gain access to your internal network, and could disrupt the C-I-A triad.

   Detection :

- Overlapping offset detection: Blocks fragments that contain overlapping offsets
- NIDS sensor: If the NIDS sensor doesn't reassemble IP fragments in the same way as the target host, it won't be able to match the packet to its signature database

TOOLS USED FOR DETECTING AND ANALYZING NETWORK LAYER ATTACKS.

1. **Tools for Detecting and Analyzing DoS Attacks**

✓ **Wireshark**

Used for deep packet inspection where by it capture traffic, filter using TCP Flags (tcp.flags.syn==1 && tcp.flags.ack==0), and visualize anomalies.

Features:

- Real-time packet capturing.
- Ability to filter SYN flood attacks by checking excessive SYN requests without corresponding ACKs.
- Can detect ICMP, UDP, and TCP flood patterns.

✓ **Snort**

It is used for Intrusion Detection System(IDS) with forensic capabilities. Also configure specific rules for identifying DoS patterns(eg. Excessive pings or SYN request).

Features :

- Detects known DoS patterns through rules sets.
- Generates alert based on DoS signatures.

✓ **Moloch(Arkime)**

It is full-packet capture, analysis platform and Ideal for post-attack investigations of large-scale DoS incidents.

Features :

- Captures high volumes of traffic for large-scale DoS investigation.
- Provide advanced search and tagging for forensic analysis.

2. **Tools for Analyzing Corrupt Packets**

✓ **Tcpdump**

It is a command-line packet sniffer for capturing network traffic. It capture and filter corrupted packets with specific flags, such as bash, tcpdump -vv -i eth0 'ip[6] & 0x40 != 0'(to detect fragmented packets).

Features:

- Can detect malformed packets and specific patterns.
- Lightweight and effective for quick captures.

✓ **NetworkMiner**

It is used for debugging and testing also import PCAP files for reconstructing corrupted sessions.

Features :

- Extracts metadata, files and session data from corrupted traffic.
- Visualizes packets corruption by showing missing or malformed segments.

✓ **Colasoft Caspa**

It is a Network analyzer with visual forensic capabilities and used its error detection features to isolate corrupt packets and their source.

Features :

- Detects abnormal packet structures.
- Provides detailed protocol breakdown.

3. **Tools for Analyzing** IP address spoofing.

✓ **Ettercap**

It is a network analysis and attack tool and used for Network security assessments and penetration testing.

Features:

- Includes features for ARP poisoning and IP spoofing.

✓ **Snort**

A popular open-source IDS/IPS that can detect spoofing attempts using predefined rules.

Features :

- It uses predefined and custom rules to analyze traffic. Rules can match specific patterns, such as spoofed source IPs or anomalies in headers.
- Deploy Snort inline (IPS mode) to block spoofed packets in real-time.

✓ **Suricata**

Another robust IDS/IPS that identifies suspicious activity, including IP spoofing, based on deep packet inspection and protocol analysis.

Features :

- It offers additional capabilities like multi-threading and advanced protocol parsing.
- Use Suricata's advanced detection engine to alert or block spoofing attempts dynamically.

4. Tools for Analyzing Man in the Middle Attack.

✓ **Wireshark**

It is a powerful network protocol analyzer that captures and inspects traffic in real-time. It offers detailed packet-level visibility and supports extensive protocol analysis.

Features:

- Look for anomalies like duplicate ARP replies, unexpected DNS responses, or unusual SSL/TLS traffic.

✓ **tcpdump**

Features :

- Captures and analyzes low-level packet headers.
- Flags unexpected traffic routing or IP address mismatches.

✓ **Snort**

Features :

- Uses rules to identify malicious ARP responses or rogue DHCP servers.
- Detects anomalies in SSL/TLS sessions, such as self-signed certificates.

5. Tools for Analyzing Incorrect reassembly of fragmented datagrams.

✓ **Network Miner**

It is a passive network analysis tool that can help in reconstructing fragmented datagrams during analysis.

Features :

- Visualizes reassembled data.
- Useful in forensic investigations.