Module 12 Firewall,IDS AND HONEYPOTS

DT by Durgesh Thakare

Firewalls

A firewall is a critical component used to filter incoming and outgoing traffic in a network based on predefined rules. It acts as a barrier between a trusted internal network and untrusted external networks, safeguarding against unauthorized access and potential threats. Firewalls employ a database of signatures for data packets, enabling them to identify and block malicious content in accordance with established rules.

For a more visual explanation, you can watch this video: **Firewalls Explained**.

Types of Firewalls

1. **Software-Based Firewalls:** These firewalls exist in the form of applications or software with rulesets for managing inbound and outbound traffic. Examples include Windows Firewalls and Linux Firewalls (e.g., IP Tables).
2. **Hardware-Based Firewalls:** Hardware-based firewalls are physical devices equipped with a processor, configuration panel, and advanced features beyond software-based firewalls. Examples include Juniper, Sophos, and Endian.
3. **Proxy Firewalls:** Acts as an intermediary between internal and external systems. Handles requests on behalf of clients and forwards the results.

Functions of a Firewall:

1. **Packet Filtering:**
   - Analyzes data packets based on predefined rules.
   - Determines whether to allow or block packets based on criteria such as source and destination IP addresses, ports, and protocols.
2. **Stateful Inspection:**
   - Keeps track of the state of active connections.
   - Makes decisions based on the context of the traffic, allowing or blocking packets based on the connection's current state.
3. **Proxying and Network Address Translation (NAT):**
   - Acts as an intermediary between internal and external systems.
   - Can provide proxy services, hiding internal network details, and perform NAT to conceal internal IP addresses.
4. **Access Control Lists (ACLs):**
   - Implements access control lists to specify what types of traffic are allowed or denied.
   - Defines rules for allowing or blocking traffic based on various criteria.
5. **Virtual Private Network (VPN) Support:**
   - Facilitates secure communication over the internet by supporting VPNs.
   - Allows the establishment of encrypted connections for remote users or branch offices.
6. **Intrusion Prevention and Detection:**
   - Some advanced firewalls include intrusion prevention and detection capabilities.
   - Can detect and block known attack patterns, providing an additional layer of security.
7. **Logging and Auditing:**
   - Maintains logs of network traffic and firewall activities.
   - Enables administrators to review and analyze events for security monitoring and compliance purposes.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is either a software or hardware-based program designed to identify suspicious activities within a network. It generates logs of such activities and can immediately alert network administrators to potential intrusions. Different types of IDS include Network IDS (NIDS), Host IDS (HIDS), and Wireless IDS (WIDS).

Types of IDS

Network IDS (NIDS):

Monitors network traffic in real-time. Analyzes packets flowing through the network to detect unusual patterns or behaviors. Positioned at strategic points within the network to capture and analyze traffic.

Host IDS (HIDS):

Monitors activities on individual devices or hosts. Examines system logs, configuration files, and critical system files for signs of intrusion. Provides a more comprehensive view of activities occurring on a specific device.

Wireless IDS (WIDS):

Specialized in monitoring wireless networks for potential security threats. Analyzes wireless traffic to detect unauthorized access points or suspicious activities. Essential for securing Wi-Fi networks and preventing unauthorized access.

How IDS Works

1. **Packet Analysis:**
   - Inspects data packets flowing through the network.
   - Utilizes predefined rules and signatures to identify known attack patterns.
2. **Anomaly Detection:**
   - Establishes a baseline of normal network behavior.
   - Raises alerts when deviations from the baseline are detected, indicating potential security issues.
3. **Log Analysis:**
   - Examines system logs and records for irregularities.
   - Correlates information from different sources to identify complex security incidents.
4. **Alert Generation:**
   - Generates alerts or notifications when suspicious activities are detected.
   - Alerts may include details such as the type of intrusion, severity, and potential impact.
5. **Response Mechanisms:**
   - Depending on the configuration, IDS can take automated actions or notify administrators for manual intervention.
   - Responses may include blocking specific IP addresses, isolating affected devices, or altering firewall rules.

TYPES OF IDS ALERT

High Priority Alerts:

Description: Indicates a critical security incident or a potential major breach. Examples: Multiple failed login attempts from a single IP address. Anomalies indicating a potential system compromise.

Medium Priority Alerts:

Description: Highlights suspicious activities that require attention but may not pose an immediate, severe threat. Examples: Unusual network traffic patterns. Suspicious file modifications.

Low Priority Alerts:

Description: Informs about activities that are less critical but still warrant investigation. Examples: Unusual but non-malicious user behavior. Minor policy violations.

False Positive Alerts:

Description: Alerts triggered by the IDS but are not indicative of a genuine security threat. Examples: Legitimate software updates mistaken for malicious activities. Authorized penetration testing activities.

False Negative Alerts:

Description: Fails to generate an alert when a genuine security incident occurs. Examples: A zero-day exploit not covered by the IDS signatures. Advanced persistent threats (APTs) that go undetected.

Threshold Alerts:

Description: Triggered when a predefined threshold of a specific metric is exceeded. Examples: Unusually high network traffic volume. Numerous failed login attempts within a short timeframe.

Pattern-Matching Alerts:

Description: Alerts generated based on predefined attack patterns or signatures. Examples: Detection of a known malware signature in network traffic. Identification of a well-documented hacking technique.

Behavioral Anomaly Alerts:

Description: Alerts resulting from deviations in user or system behavior from established baselines. Examples: Unusual access patterns indicating a compromised user account. Abnormal system resource usage.

Correlation Alerts:

Description: Generated when the IDS correlates information from multiple sources to identify a complex security incident. Examples: Detection of a coordinated attack involving multiple vectors. Correlation of events indicating a potential data exfiltration attempt.

Compliance Violation Alerts:

Description: Alerts triggered when activities violate established security policies or compliance standards. Examples: Unauthorized access to sensitive data. Violation of data retention policies.

Informational Alerts:

Description: Provides information about normal activities or system status. Examples: Routine system updates. Scheduled network maintenance.

IDS DETECTION TOOLS

Snort

AlienVault

Wifi Inspector

Zips

Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a critical component of network security that goes beyond the detection capabilities of an Intrusion Detection System (IDS) by actively preventing and blocking potential security threats. IPS works to analyze network and/or system activities, identify malicious behavior, and take automated actions to stop or mitigate the impact of security incidents. Here's an overview of key aspects related to Intrusion Prevention Systems:

Functionality

Real-Time Monitoring:

IPS continuously monitors network and/or system activities in real-time. Analyzes traffic patterns, packet contents, and behaviors to identify potential threats.

Signature-Based Detection:

Utilizes predefined signatures to identify known patterns of malicious activities. Blocks or allows traffic based on matches with these signatures.

Anomaly-Based Detection:

Detects abnormal behaviors that may indicate new or unknown threats. Establishes baselines for normal network behavior and raises alerts or takes action when deviations occur. Protocol Analysis:

Analyzes network protocols to identify and block malicious activities. Ensures adherence to protocol standards and prevents protocol-based attacks.

Blocking and Mitigation:

Takes immediate automated actions to block or mitigate identified threats. Can include blocking specific IP addresses, closing ports, or modifying firewall rules.

Deployment Models

Network-Based IPS (NIPS):

Monitors and analyzes network traffic at the network layer. Placed at strategic points within the network to inspect and block malicious traffic.

Host-Based IPS (HIPS):

Installed on individual devices or hosts. Monitors activities on the host and can take actions to block malicious processes or activities.

Inline and Passive Modes:

Inline IPS: Actively participates in the network traffic flow, allowing it to block malicious content in real-time.

Passive IPS: Operates in a non-blocking mode, monitoring and analyzing traffic without actively blocking content.

IPS Features

Deep Packet Inspection:

Analyzes packet contents at a granular level to identify threats. Examines not only header information but also payload content.

SSL/TLS Decryption:

Decrypts encrypted traffic to inspect contents for potential threats. Ensures comprehensive analysis of both encrypted and unencrypted traffic.

Policy Enforcement:

Enforces security policies to ensure compliance with organizational rules. Blocks activities that violate security policies or pose a threat.

Vulnerability Protection:

Identifies and blocks known vulnerabilities in applications and systems. Protects against exploits targeting known weaknesses.

Rate Limiting and Threshold Controls:

Implements rate limiting to prevent abuse or attacks based on unusual traffic patterns. Sets thresholds for various activities to trigger alerts or preventive actions.

Honeypots

Honeypots are a deceptive technique used to attract and trap hackers, attackers, or other malicious entities. They can take the form of web applications, network systems, or access points, appearing normal but created with the sole purpose of luring and identifying potential threats. A tool like Pentbox can be employed to

Types of Honeypots:

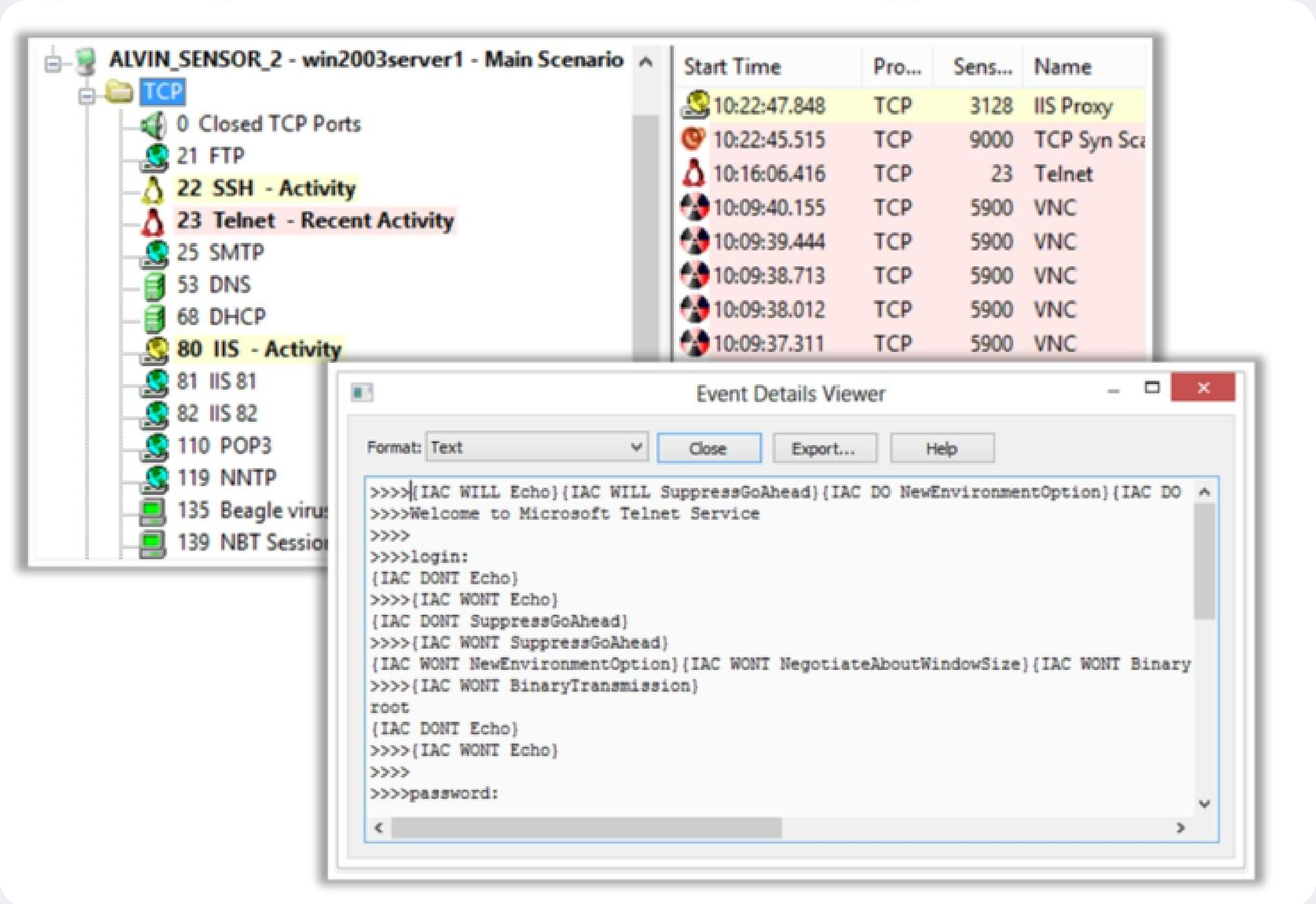
1. **Low-Interaction Honeypots:**
    - Emulate only the services and applications commonly targeted by attackers.
    - Require minimal resources and are less complex.
    - Suitable for early detection and analysis.
2. **High-Interaction Honeypots:**
    - Fully emulate real operating systems and applications.
    - Provide a more realistic environment for attackers.
    - Capture a broader range of attacker behaviors.
3. **Production Honeypots:**
    - Integrated into the production network to identify and monitor real threats.
    - Mimic the organization's actual systems and services.
    - Useful for detecting attacks targeting specific resources.
4. **Research Honeypots:**
    - Deployed in a controlled research environment.
    - Gather extensive data on attackers and their techniques.
    - Often used for academic or industry research purposes

Advantages of Honeypots:

1. **Early Threat Detection:**
    - Identifies attacks in their early stages before they can impact critical systems.
2. **Behavior Analysis:**
    - Allows security professionals to study and understand attacker behavior and tactics.
3. **Misdirection of Attackers:**
    - Diverts attackers away from critical systems, reducing the potential for real damage.
4. **Research and Intelligence Gathering:**
    - Provides valuable insights into the latest attack techniques and trends.
5. **Legal and Ethical Use:**
    - Can be legally and ethically deployed within a controlled environment for security research and education.

Honepot Tools:

KFSensor



ALVIN_SENSOR_2 - win2003server1 - Main Scenario

TCP
- 0 Closed TCP Ports
- 21 FTP
- 22 SSH - Activity
- 23 Telnet - Recent Activity
- 25 SMTP
- 53 DNS
- 68 DHCP
- 80 IIS - Activity
- 81 IIS 81
- 82 IIS 82
- 110 POP3
- 119 NNTP
- 135 Beagle viru
- 139 NBT Sessio

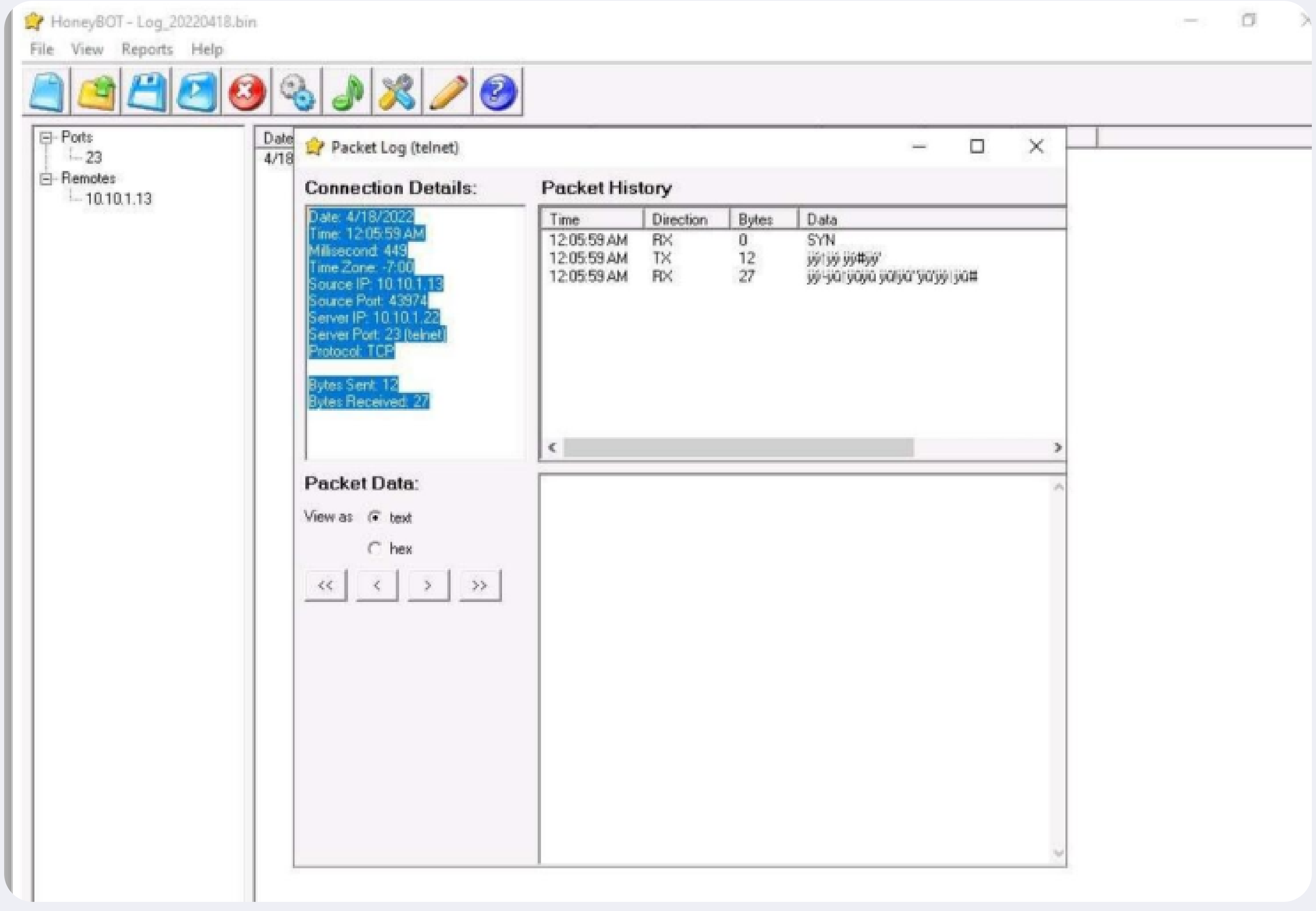
Start Time	Pro...	Sens...	Name
10:22:47.848	TCP	3128	IIS Proxy
10:22:45.515	TCP	9000	TCP Syn Sca
10:16:06.416	TCP	23	Telnet
10:09:40.155	TCP	5900	VNC
10:09:39.444	TCP	5900	VNC
10:09:38.713	TCP	5900	VNC
10:09:38.012	TCP	5900	VNC
10:09:37.311	TCP	5900	VNC

Event Details Viewer

Format: Text

```
>>>>{IAC WILL Echo}{IAC WILL SuppressGoAhead}{IAC DO NewEnvironmentOption}{IAC DO
>>>>Welcome to Microsoft Telnet Service
>>>>
>>>>login:
{IAC DONT Echo}
>>>>{IAC WONT Echo}
{IAC DONT SuppressGoAhead}
>>>>{IAC WONT SuppressGoAhead}
{IAC WONT NewEnvironmentOption}{IAC WONT NegotiateAboutWindowSize}{IAC WONT Binary
>>>>{IAC WONT BinaryTransmission}
root
{IAC DONT Echo}
>>>>{IAC WONT Echo}
>>>>
>>>>password:
```

Honeybot



HoneyBOT - Log_20220418.bin

- Ports
    - 23
- Remotes
    - 10.10.1.13

Date
4/18

Packet Log (telnet)

Connection Details:

Date: 4/18/2022
Time: 12:05:59 AM
Millisecond: 449
Time Zone: -7:00
Source IP: 10.10.1.13
Source Port: 43974
Server IP: 10.10.1.22
Server Port: 23 (telnet)
Protocol: TCP

Bytes Sent: 12
Bytes Received: 27

Packet History

Time	Direction	Bytes	Data
12:05:59 AM	RX	0	SYN
12:05:59 AM	TX	12	ÿÿ ÿÿ ÿÿ#ÿÿ'
12:05:59 AM	RX	27	ÿÿ-ÿú ÿúÿú ÿúÿú'ÿúÿÿ ÿú#

Packet Data:

View as ● text ○ hex

Pentbox