Week 11:

**FIREWALLS**

Placed between the premises network and the Internet to establish a controlled link.

Used as a perimeter defence.

**FIREWALL CHARACTERISTICS**

All traffic from inside to outside, and vice versa, must pass through the firewall.

Only authorised traffic as defined by the local security policy will be allowed to pass.

The firewall itself is immune to penetration.

**TYPES OF FIREWALLS**

❐ \_Packet filtering firewall

❐ \_Stateful filtering firewall

❐ \_Application proxy firewall

❐ \_Circuit level proxy firewall

**IP address and protocol values** Used by packet filter and stateful inspection firewalls, used to limit access to specific services.

**Application protocol** Used by an application-level gateway that relays and monitors the exchange of information for specific application protocols.

**User identity** Typically for inside users who identify themselves using some form of secure authentication technology.

**Network activity** Controls access based on considerations such as the time or request, rate of requests, or other activity patterns.

**PACKET FILTERING FIREWALL -** Also called Stateless filtering Firewall.

Applies rules to each incoming and outgoing IP packet.

Typically, a list of rules based on matches in the IP or TCP header.

Two default policies:

Discard (Deny) prohibit unless expressly permitted.

Forward (Permit) permit unless expressly prohibited.

**Filtering rules are based on information contained in a network packet.**

Source IP address.

Destination IP address

Source and destination transport-level address.

IP protocol field

Interface

**STATEFUL FILTERING FIREWALL.**

Creates a directory of outbound TCP connections, with an entry for each currently established connection.

Allows incoming traffic to high-numbered ports only for packets that match the profile of an entry in the connection directory.

Examines packet details and records information about TCP connections, such as TCP sequence numbers.

Keeps track of TCP sequence numbers to thwart attacks that rely on sequence number manipulation.

**APPLICATION PROXY FIREWALL**

Application-Level Gateway - Act as an intermediary

❏ Acts as a relay of application-level traffic

❐ User contacts gateway using a TCP/IP application

❐ User is authenticated

❐ Gateway contacts application on remote host and relays TCP segments between server and user

Must have proxy code for each application.

Tend to be more secure than packet filters.

Disadvantage is the additional processing overhead on each connection.

**CIRCUIT-LEVEL GATEWAY**

Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host.

Relays TCP segments from one connection to the other without examining contents.

Security function consists of determining which connections will be allowed.

Typically used when inside users are trusted.

May use application-level gateway inbound and circuit-level gateway outbound.

Lower overheads

**HOST-BASED FIREWALLS/ PERSONAL FIREWALL**

Used to secure an individual host.

Available in operating systems

Can be housed in a router that connects all the home computers to the Internet.

Filter and restrict packet flows. Primary role is to deny unauthorised remote access.

May also monitor outgoing traffic to detect and block worms and malware activity.

**Advantages** Filtering rules can be tailored to the host environment.

Protection is provided independent of topology.

Provides an additional layer of protection.

**A yellow and green background with white text

Description automatically generated**

**INTRUSION DETECTION SYSTEM (IDS):**

Components:

- Sensors: Core component responsible for collecting data related to potential intrusions.

- Data Sources: Include system call traces, audit records (log files), file integrity checksums, and registry access.

- Analysers: Assess collected data to determine if an intrusion has occurred.

- User Interface: Provides an interface for viewing output or controlling system behaviours.

IDS utilizes either the Anomaly detection or the Signature/Heuristic detection approach to identify intrusions.

Types of IDS:

- Host-based IDS (HIDS): Monitors and analyses the internals of a computing system, typically focusing on individual hosts or servers.

- Network-based IDS (NIDS): Examines network traffic to detect suspicious patterns or behaviours indicative of intrusions.

- Distributed or Hybrid IDS: Combines characteristics of both HIDS and NIDS, providing comprehensive intrusion detection capabilities across networks and hosts.

A blue background with white text

Description automatically generatedAnalysis Approaches:

**- Anomaly Detection:**

- Involves collecting data on the behaviours of legitimate users over time.

- Analyses current observed behaviours to distinguish between legitimate users and potential intruders.

**- Signature/Heuristic Detection:**

- Utilizes a predefined set of known malicious data patterns or attack rules.

- Compares current behaviours against these patterns or rules to identify potential threats.

- Also referred to as misuse detection.

- Limited to identifying known attacks for which patterns or rules exist.

**HOST-BASED INTRUSION DETECTION SYSTEM (HIDS):**

- Adds a specialized layer of security software to vulnerable or sensitive systems.

- Can employ either anomaly or signature/heuristic approaches.

- Monitors system activity to identify suspicious behaviours.

- Primarily aims to detect intrusions, log suspicious events, and issue alerts.

- Capable of detecting both external and internal intrusions.

**NETWORK-BASED INTRUSION DETECTION SYSTEM (NIDS):**

- Monitors traffic at specific points within a network.

- Analyses network traffic packet by packet in real or near-real time.

- May inspect network, transport, and/or application-level protocol activity.

- Consists of multiple sensors, one or more servers for NIDS management functions, and one or more management consoles for human interface.

- Traffic pattern analysis can occur at the sensor, the management server, or a combination of both.

**AN INTRUSION DETECTION SYSTEM (IDS) MUST POSSESS THE FOLLOWING CAPABILITIES:**

* Operate continuously with minimal human supervision.
* Capable of recovering from system crashes and reinitializations.
* Resist subversion by monitoring itself and detecting modifications made by attackers.
* Impose minimal overhead on the system where it is deployed.
* Configurable according to the security policies of the monitored system.
* Adapt to changes in system and user behaviours over time.
* Scale to monitor many hosts effectively.
* Provide graceful degradation of service, minimizing the impact of component failures on overall functionality.
* Allow dynamic reconfiguration without requiring system restarts.

**INTRUSION PREVENTION SYSTEMS (IPS)**

Also known as Intrusion Detection and Prevention System (IDPS).

Includes capabilities to not only detect but also attempt to block or prevent detected malicious activities.

Types:

- Can be host-based, network-based, or distributed/hybrid, depending on deployment requirements.

Detection Approaches:

- Utilizes anomaly detection to identify abnormal behaviours not typical of legitimate users.

- Also employs signature/heuristic detection to identify known malicious behaviours.

- Can block traffic like a firewall but uses algorithms developed for IDS to determine when to do so.

**HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS):**

Detection Techniques:

- Signature Detection: Focuses on specific content of application network traffic or sequences of system calls to identify known malicious patterns.

- Anomaly Detection: Identifies behaviours patterns indicating malware.

Examples of Malicious Behaviour:

- Modification of system resources, privilege escalation exploits, buffer overflow exploits, access to email contact lists, directory traversal, etc.

- Capability can be tailored to specific platforms, utilizing general-purpose tools for desktop or server systems or specialized packages for web servers and database servers.

- Utilizes a sandbox approach, particularly suited for mobile code such as Java applets and scripting languages.

- Quarantines code in an isolated system area, then monitors its behaviours.

**ROLE OF HIPS:**

- Recognizes the enterprise endpoint, including desktop and laptop systems, as the primary target for hackers and criminals.

- Complements existing endpoint security measures like antivirus and firewalls.

Integrated Security Suite:

- Offers an integrated, single-product suite of functions to provide comprehensive endpoint security.

Defence-in-Depth Strategy:

- Can be employed as part of a defence-in-depth strategy alongside network-level devices like network-based IPSs.

**NETWORK-BASED INTRUSION PREVENTION SYSTEM (NIPS):**

- Operates inline, positioned strategically within the network architecture, with the authority to modify or discard packets and terminate TCP connections.

- Utilizes both signature/heuristic and anomaly detection techniques to identify potential threats.

- May offer flow data protection, safeguarding against various types of network attacks.

- Requires the reassembly of application payload in a sequence of packets to provide comprehensive protection.

**INTRUSION PREVENTION SYSTEM (IPS) METHODS TO IDENTIFY MALICIOUS PACKETS:**

Signature-based:

- Method: Compares network traffic against a database of known attack patterns or signatures.

- Functionality: Efficient for detecting known threats based on predefined signatures.

Anomaly-based:

- Method: Establishes a baseline of normal network behaviours and identifies deviations from this baseline.

- Functionality: Effective for detecting previously unseen or novel threats by flagging unusual behaviours.

Heuristic-based:

- Method: Uses rules and algorithms to identify potentially malicious behaviours.

- Functionality: Less specific than signature-based methods but can detect previously unknown threats such as Zero-Day attacks based on certain characteristics.

Protocol Analysis:

- Method: Analyses network protocols to detect abnormalities or violations.

- Functionality: Flags suspicious behaviours if a protocol does not adhere to its standard specifications.

**HONEYPOTS:**

- Decoy systems designed to:

- Lure potential attackers away from critical systems.

- Collect information about the attacker’s activity.

- Encourage the attacker to stay on the system long enough for administrators to respond.

- Filled with fabricated information that legitimate users wouldn’t access.

- Resources have no production value, making incoming communication likely a probe, scan, or attack.

- Outbound communication suggests the system may have been compromised.

- A collection of honeypots is called honey nets

**HONEYPOT CLASSIFICATIONS:**

Low Interaction Honeypot:

- Emulates specific IT services or systems to provide a realistic initial interaction.

- Provides a less realistic target but is sufficient for use as a component of a distributed IDS to warn of imminent attacks.

High Interaction Honeypot:

- A real system with a full operating system, services, and applications.

- More realistic target that may occupy an attacker for an extended period.

**REQUIREMENTS OF HONEYPOTS/HONEYNETS:**

Isolation:

- Should be isolated from production systems and networks to contain and study malicious activity without risking actual production systems.

Continuous Monitoring:

- Should be continuously monitored to analyse potential threats and attacker behaviours.

Deception:

- Should be as realistic as possible to deceive potential attackers and observe and learn from their activities without exposing real assets.