UNIVERSITY OF WESTMINSTER

Defensive Technologies -(Intrusion Detection and Firewalls)

6COSC019W- Cyber Security

Dr Ayman El Hajjar

March 20, 2023

School of Computer Science and Engineering
University of Westminster

OUTLINE

1. intrusion detection

   Classes of Intruders

2. Honeypots

3. Firewalls Systems

4. Intrusion Prevention Systems (IPS)

DEFINITIONS

- Security Intrusion:
    - Unauthorized act of bypassing the security mechanisms of a system
- Intrusion Detection:
    - A hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions

intrusion detection

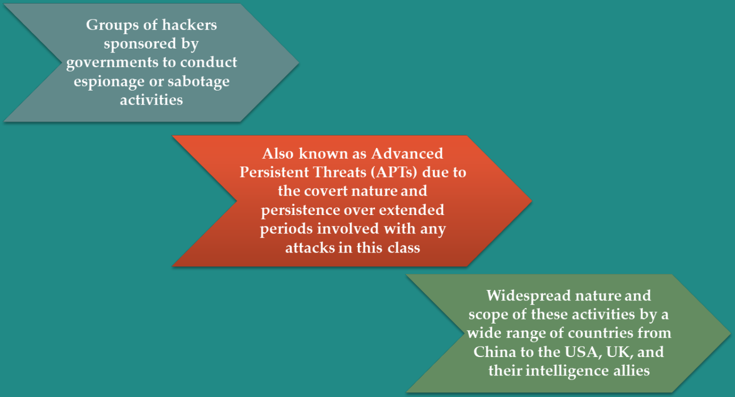
Classes of Intruders- Cyber Criminals

- Individuals or members of an organized crime group with a goal of financial reward
- Their activities may include:
  - ✺Identity theft
  - ✺ Theft of financial credentials
  - ✺ Corporate espionage
  - ✺ Data theft
  - ✺ Data ransoming
- Typically they are young, often Eastern European, Russian, or southeast Asian hackers, who do business on the Web
- They meet in underground forums to trade tips and data and coordinate attacks

Classes of Intruders- Activists

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also know as hacktivists
  - Skill level is often quite low
- Aim of their attacks is often to promote and publicize their cause typically through:
  - Website defacement
  - Denial of service attacks
  - Theft and distribution of data that results in negative publicity or compromise of their targets

Classes of Intruders- State Sponsored Organizations



Groups of hackers sponsored by governments to conduct espionage or sabotage activities

Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class

Widespread nature and scope of these activities by a wide range of countries from China to the USA, UK, and their intelligence allies

Classes of Intruders – Others

- Hackers with motivations other than those previously listed
- Include classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation
- Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class
- Given the wide availability of attack toolkits, there is a pool of “hobby hackers” using them to explore system and network security

Intruder Skill Levels – Apprentice

- Hackers with minimal technical skill who primarily use existing attack toolkits
- They likely comprise the largest number of attackers, including many criminal and activist attackers
- Given their use of existing known tools, these attackers are the easiest to defend against
- Also known as “script-kiddies” due to their use of existing scripts (tools)

Intruder Skill Levels – Journeyman

- Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
- They may be able to locate new vulnerabilities to exploit that are similar to some already known
- Hackers with such skills are likely found in all intruder classes
- Adapt tools for use by others

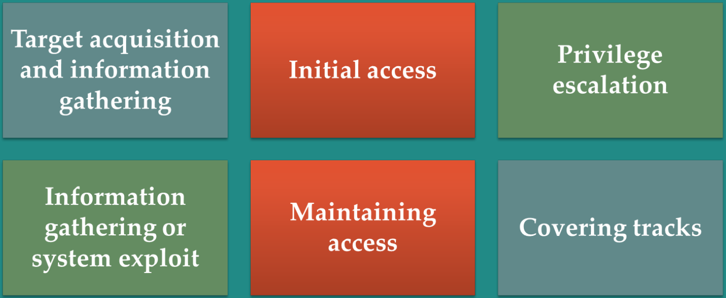
INTRUDER SKILL LEVELS – MASTER

- Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities
- Write new powerful attack toolkits
- Some of the better known classical hackers are of this level
- Some are employed by state-sponsored organizations
- Defending against these attacks is of the highest difficulty

EXAMPLES OF INTRUSION

- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

INTRUDER BEHAVIOUR



Target acquisition and information gathering

Initial access

Privilege escalation

Information gathering or system exploit

Maintaining access

Covering tracks

Security Intrusion:

Unauthorized act of bypassing the security mechanisms of a system

Intrusion Detection:

A hardware or software function that gathers and analyses information from various areas within a computer or a network to identify possible security intrusions

INTRUSION DETECTION SYSTEM (IDS)

- Host-based IDS (HIDS)
  - ✺ Monitors the characteristics of a single host for suspicious activity
- Network-based IDS (NIDS)
  - ✺ Monitors network traffic and analyses network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
  - ✺ Combines information from a number of sensors, often both host and network based, in a central analyser that is able to better identify and respond to intrusion activity

Comprises three logical components:

- **Sensors collect data**
- **Analysers determine if intrusion has occurred**
- **User interface view output or control system behavior**

IDS Requirements

- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large numbers of systems
- Provide graceful degradation of service
- Allow dynamic reconfiguration

ANALYSIS APPROACH

- Anomaly detection
  - ✺ Involves the collection of data relating to the behaviour of legitimate users over a period of time
  - ✺ Current observed behaviour is analysed to determine whether this behaviour is that of a legitimate user or that of an intruder
- Signature/Heuristic detection
  - ✺ Uses a set of known malicious data patterns or attack rules that are compared with current behaviour
  - ✺ Also known as misuse detection
  - ✺ Can only identify known attacks for which it has patterns or rules

ANOMALY DETECTION

- A variety of classification approaches are used:

1. Statistical
   - ✺ Analysis of the observed behaviour using univariate, multivariate, or time-series models of observed metrics
2. Knowledge based
   - ✺ Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior
3. Machine-learning
   - ✺ Approaches automatically determine a suitable classification model from the training data using data mining techniques

SIGNATURE DETECTION

- Match a large collection of known patterns of malicious data against data stored on a system or in transit over a network
- The signatures need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data
- Widely used in anti-virus products, network traffic scanning proxies, and in NIDS

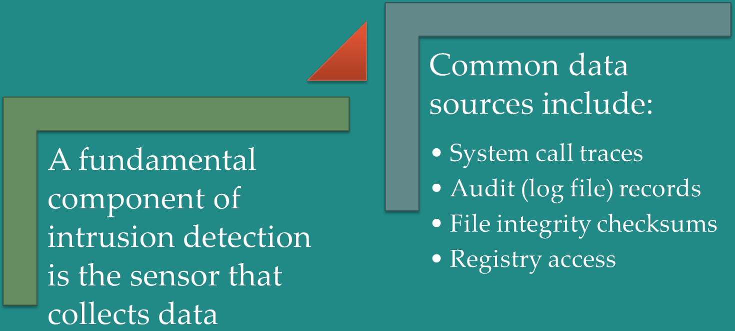
RULE-BASED HEURISTIC IDENTIFICATION

- Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses
- Rules can also be defined that identify suspicious behaviour, even when the behaviour is within the bounds of established patterns of usage
- Typically rules used are specific
- SNORT is an example of a rule-based NIDS

HOST-BASED INTRUSION DETECTION (HIDS)

- Adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- Monitors activity to detect suspicious behaviour
  - Primary purpose is to detect intrusions, log suspicious events, and send alerts
  - Can detect both external and internal intrusions

Data Sources and Sensors



A fundamental component of intrusion detection is the sensor that collects data

Common data sources include:

- System call traces
- Audit (log file) records
- File integrity checksums
- Registry access

NETWORK-BASED IDS (NIDS)

- Monitors traffic at selected points on a network
- Examines traffic packet by packet in real or close to real time
- May examine network, transport, and/or application-level protocol activity
- Comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface
- Analysis of traffic patterns may be done at the sensor, the management server or a combination of the two

INTRUSION DETECTION TECHNIQUES

- Attacks suitable for
- Signature detection

- Attacks suitable for
- Anomaly detection

- Application layer reconnaissance and attacks
- Transport layer reconnaissance and attacks
- Network layer reconnaissance and attacks
- Unexpected application services
- Policy violations

- Denial-of-service (DoS) attacks
- Scanning
- Worms

Stateful Protocol Analysis (SPA)

- Subset of anomaly detection that compares observed network traffic against predetermined universal vendor supplied profiles of benign protocol traffic
    - ✺This distinguishes it from anomaly techniques trained with organization specific traffic protocols
    - ✺Understands and tracks network, transport, and application protocol states to ensure they progress as expected
- A key disadvantage is the high resource use it requires

LOGGING OF ALERTS

- Typical information logged by a NIDS sensor includes:
  - Timestamp
  - Connection or session ID
  - Event or alert type
  - Rating
  - Network, transport, and application layer protocols
  - Source and destination IP addresses
  - Source and destination TCP or UDP ports, or ICMP types and codes
  - Number of bytes transmitted over the connection
  - Decoded payload data, such as application requests and responses
  - State-related information

Honeypots

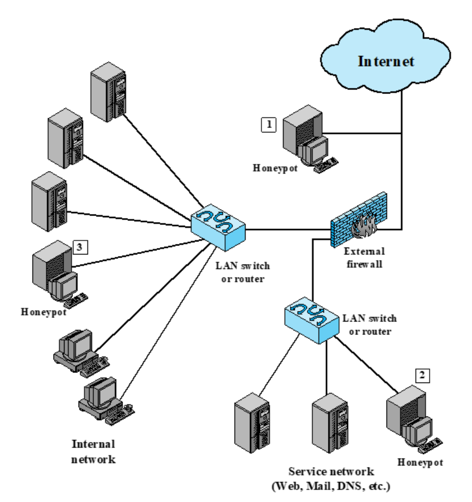
HONEYPOTS

- Decoy systems designed to:
  - Lure a potential attacker 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
- Systems are filled with fabricated information that a legitimate user of the system wouldn’t access
- Resources that have no production value
  - Therefore incoming communication is most likely a probe, scan, or attack
  - Initiated outbound communication suggests that the system has probably been compromised

HONEYPOT CLASSIFICATIONS

- Low interaction honeypot
  - Software package that emulates particular IT services or systems well enough to provide a realistic initial interaction
  - Provides a less realistic target
  - Often sufficient for use as a component of a distributed IDS to warn of imminent attack
- High interaction honeypot
  - A real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers
  - Is a more realistic target that may occupy an attacker for an extended period

HONEYPOT EXAMPLE

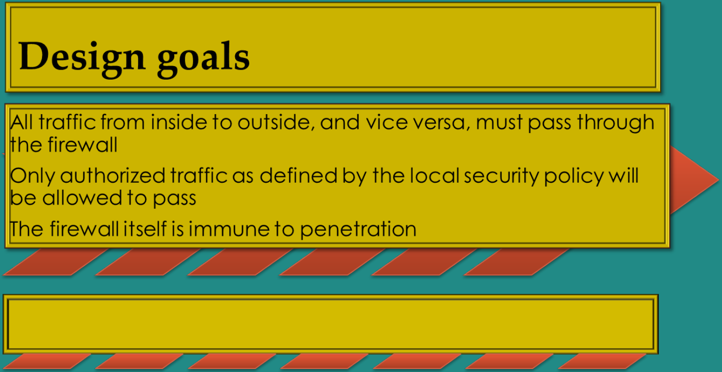


Firewalls Systems

The Need For Firewalls

- Internet connectivity is essential
  - However it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
  - Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defence
  - Single choke point to impose

FIREWALL CHARACTERISTICS



Design goals

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

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

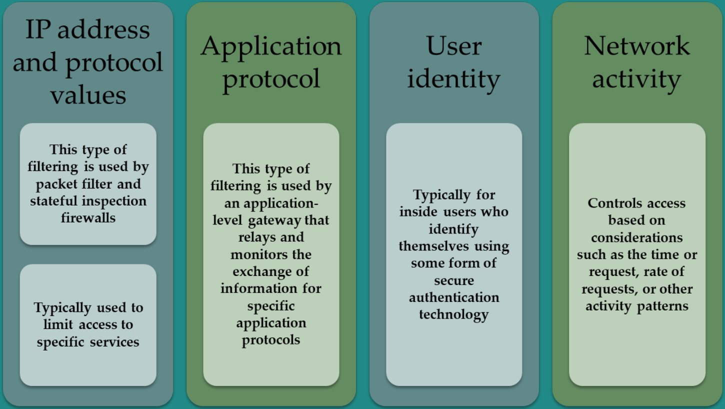
The firewall itself is immune to penetration

FIREWALL ACCESS POLICY

- A critical component in the planning and implementation of a firewall is specifying a suitable access policy
  - This lists the types of traffic authorized to pass through the firewall
  - Includes address ranges, protocols, applications and content types
- This policy should be developed from the organization’s information security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support
  - Then refined to detail the filter elements which can then be implemented within an appropriate firewall topology

FIREWALL FILTER CHARACTERISTICS

- Characteristics that a firewall access policy could use to filter traffic include:



IP address and protocol values

This type of filtering is used by packet filter and stateful inspection firewalls

Typically used to limit access to specific services

Application protocol

This type of filtering is 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

Firewall Capabilities And Limits

Capabilities:

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as the platform for IPSec

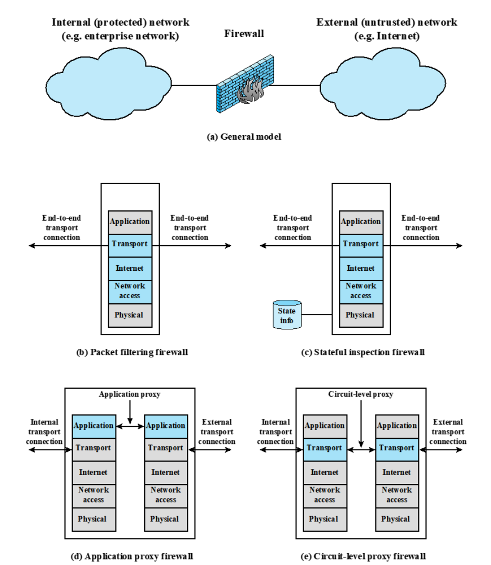
Limitations:

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organization
- Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

TYPES OF FIREWALL

- A firewall can monitor network traffic at a number of levels from **low-level network packets**, either individually or as part of a flow, to **all traffic** within a transport connection, up to **inspecting details of application protocols**.
- The choice of which level is appropriate is determined by the desired firewall access policy.

TYPES OF FIREWALL


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
State info
Application proxy
Circuit-level proxy
Internal transport connection
External transport connection

(a) General model

(b) Packet filtering firewall

(c) Stateful inspection firewall

(d) Application proxy firewall

(e) Circuit-level proxy firewall

Packet Filtering Firewall

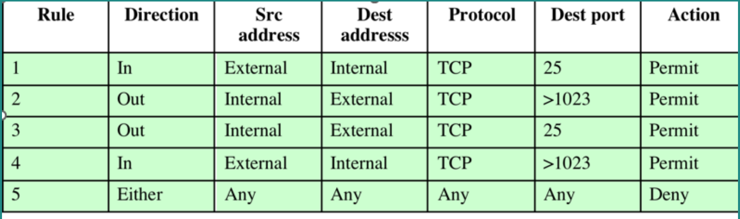
- Applies rules to each incoming and outgoing IP packet
  - ✺ Typically a list of rules based on matches in the IP or TCP header
  - ✺ Forwards or discards the packet based on rules match

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

PACKET FILTERING FIREWALL

- Two default policies:
  - ✺ Discard (Deny) prohibit unless expressly permitted
    - ✍ More conservative, controlled, visible to users
  - ✺ Forward (Permit) permit unless expressly prohibited
    - ✍ Easier to manage and use but less secure



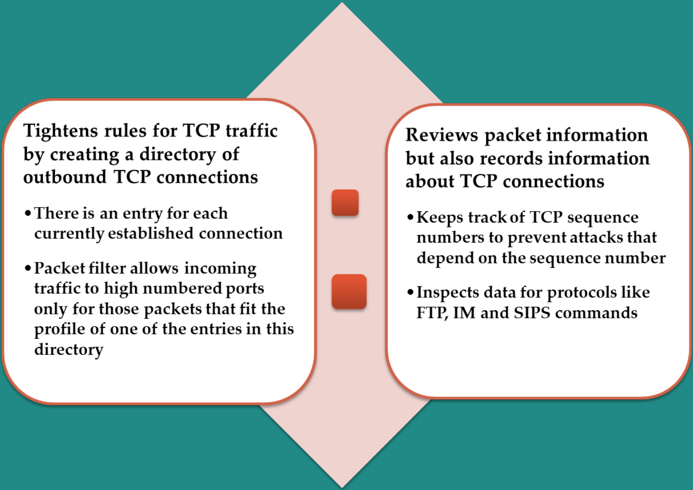
Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet-Filtering Examples

PACKET FILTER ADVANTAGES AND WEAKNESSES

- Advantages
  - Simplicity
  - Typically transparent to users and are very fast
- Weaknesses
  - Cannot prevent attacks that employ application specific vulnerabilities or functions
  - Limited logging functionality
  - Do not support advanced user authentication
  - Vulnerable to attacks on TCP/IP protocol bugs
  - Improper configuration can lead to breaches

Stateful Inspection Firewall



Tightens rules for TCP traffic by creating a directory of outbound TCP connections

- There is an entry for each currently established connection
- Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory

Reviews packet information but also records information about TCP connections

- Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
- Inspects data for protocols like FTP, IM and SIPS commands

APPLICATION-LEVEL GATEWAY

- Also called an application proxy
- 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
  - May restrict application features supported
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection

Circuit-Level Gateway

Circuit level proxy

- 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

BASTION HOSTS

- System identified as a critical strong point in the network's security
- Serves as a platform for an application-level or circuit-level gateway
- Common characteristics:
  - Runs secure O/S, only essential services
  - May require user authentication to access proxy or host
  - Each proxy can restrict features, hosts accessed
  - Each proxy is small, simple, checked for security
  - Each proxy is independent, non-privileged
  - Limited disk use, hence read-only code

Host-Based Firewalls

- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Filter and restrict packet flows
- Common location is a server

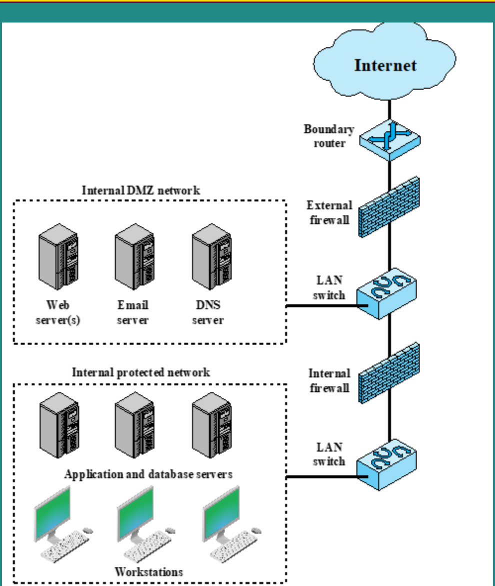
Advantages

- ✺ Filtering rules can be tailored to the host environment
- ✺ Protection is provided independent of topology
- ✺ Provides an additional layer of protection

PERSONAL FIREWALL

- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- For both home or corporate use
- Typically is a software module on a personal computer
- Can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically much less complex than server-based or stand-alone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity

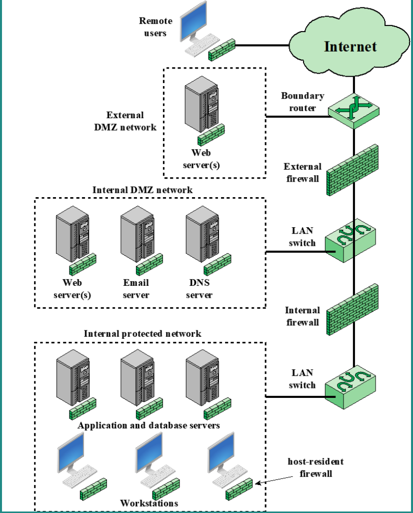
FIREWALL CONFIGURATION EXAMPLE



FIREWALL TOPOLOGIES

Host-resident firewall	• Includes personal firewall software and firewall software on servers
Screening router	• Single router between internal and external networks with stateless or full packet filtering
Single bastion inline	• Single firewall device between an internal and external router
Single bastion T	• Has a third network interface on bastion to a DMZ where externally visible servers are placed
Double bastion inline	• DMZ is sandwiched between bastion firewalls
Double bastion T	• DMZ is on a separate network interface on the bastion firewall
Distributed firewall configuration	• Used by large businesses and government organizations

DISTRIBUTED FIREWALL CONFIGURATION EXAMPLE



Intrusion Prevention Systems (IPS)

INTRUSION PREVENTION SYSTEMS (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

HOST-BASED IPS (HIPS)

- Can make use of either signature/heuristic or anomaly detection techniques to identify attacks
  - ✺ Signature: focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious
  - ✺ Anomaly: IPS is looking for behaviour patterns that indicate malware
- Examples of the types of malicious behaviour addressed by a HIPS are Modification of system resources, Privilege-escalation exploits, Buffer-overflow exploits, Access to e-mail contact list, Directory traversal

HIPS

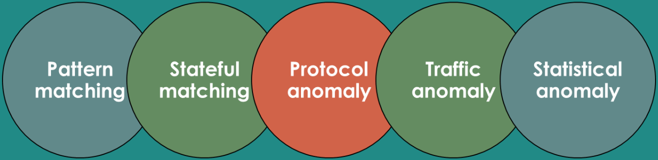
- Capability can be tailored to the specific platform
- A set of general purpose tools may be used for a desktop or server system.
- Some packages are designed to protect specific types of servers, such as Web servers and database servers
- Can use a sandbox approach
  - ✺ Sandboxes are especially suited to mobile code such as Java applets and scripting languages
  - ✺ HIPS quarantines such code in an isolated system area then runs the code and monitors its behavior
  - ✺ Areas for which a HIPS typically offers desktop protection such as System calls, File system access.

THE ROLE OF HIPS

- Many industry observers see the enterprise endpoint, including desktop and laptop systems, as now the main target for hackers and criminals
  - Endpoint security is provided by a collection of products, such as antivirus, and firewalls.
- Approach is an effort to provide an integrated, single-product suite of functions
- HIPS can be used as a defence-in-depth strategy that involves network-level devices, such as network-based IPSs

Network-Based IPS (NIPS)

- Inline NIDS with the authority to modify or discard packets and tear down TCP connections
- Makes use of signature/heuristic and anomaly detection
- May provide flow data protection
  - Requires that the application payload in a sequence of packets be reassembled
- Methods used to identify malicious packets:



References

REFERENCES

- Figures and tables are from the recommended books
- Chapter 8,9 Computer Security: Principles and Practice, , William Stallings and Lawrie Brown