UNIVERSITY OF WESTMINSTER

Defensive Technologies -(Intrusion Detection and Firewalls)

6COSC019W- Cyber Security

Dr Ayman El Hajjar

April 02, 2024

School of Computer Science and Engineering
University of Westminster

OUTLINE

Firewall Systems

THE NEED FOR FIREWALLS

- Internet connectivity is essential however it brings threats to our information system enrolment.
- Placed 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 security and auditing
  - separates the internal systems from external networks

Firewall Characteristics

Design goals

- 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 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.
- Firewall levels are:
  - Packet filtering firewall
  - Stateful filtering firewall
  - Application proxy firewall
  - Circuit level proxy firewall

What do they Filter!

IP address and protocol values

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

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

- 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

APPLICATION PROXY FIREWALL

- Also called ”Application-Level Gateway”
- 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

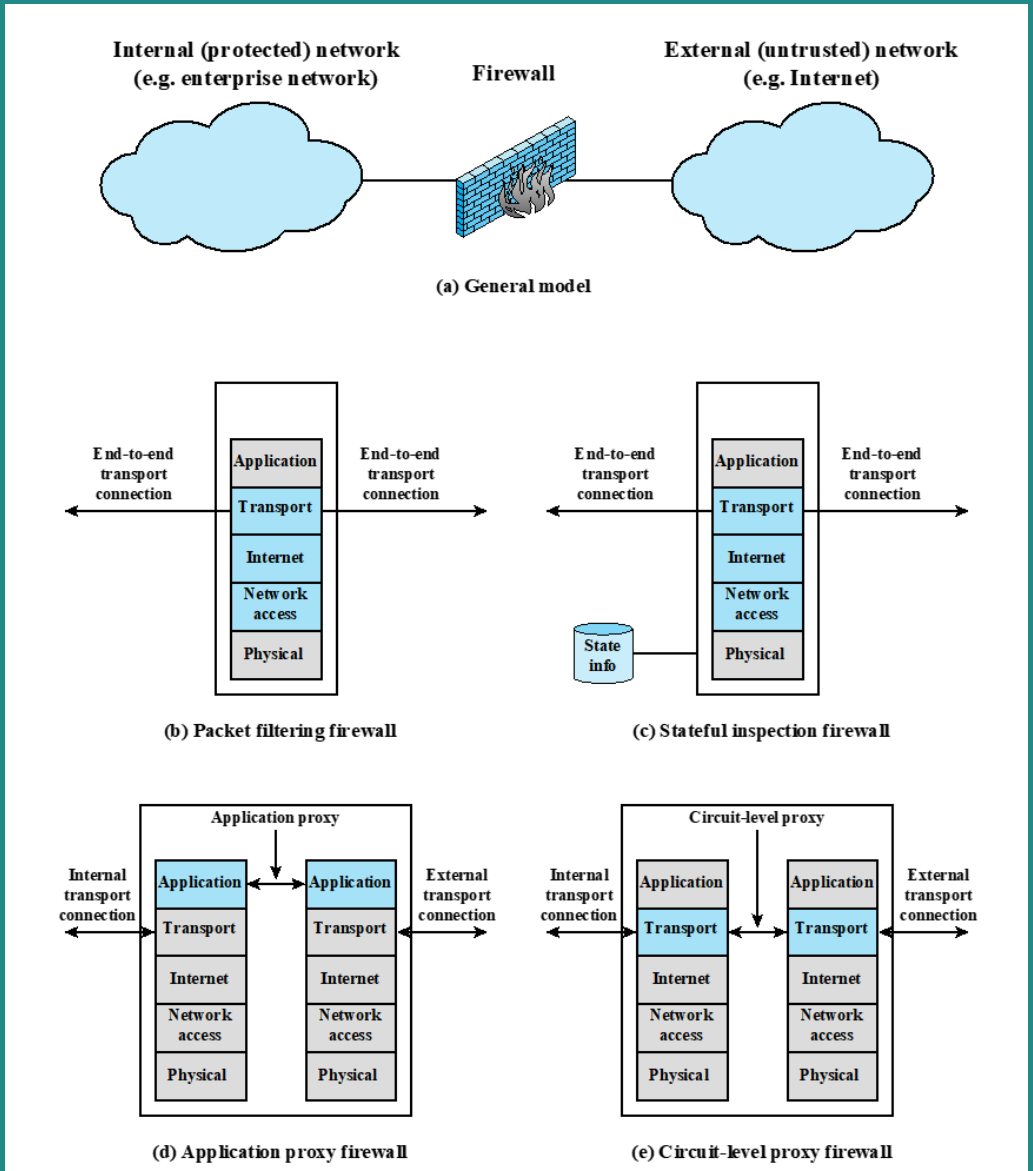

Figure 1: Types of Firewall

HOST-BASED FIREWALLS/ PERSONAL FIREWALL

- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Can be housed in a router that connects all of 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

Intrusion Detection Systems (IDS)

Security Intrusion:

unauthorised 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)

- An IDS Comprises of three logical components
  - **Sensors** A fundamental component of intrusion detection that collects data.
  - Common data sources include System call traces, Audit (log file) records,File integrity checksums, Registry access.
  - **Analysers** determine if intrusion has occurred
  - **User interface** view output or control system behaviour
- An IDS uses either the Anomaly detection or the Signature/Heuristic detection approach.
- There are three type of Intrusion Detection systems, a **Host-based IDS (HIDS)** a **Network-based IDS (NIDS)** and a **Distributed or hybrid IDS** that combines both characteristics

Analysis Approaches

- 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

Signature or Anomaly?

- Attacks suitable for Signature detection
  - Application layer reconnaissance and attacks
  - Transport layer reconnaissance and attacks
  - Network layer reconnaissance and attacks
  - Unexpected application services
  - Policy violations
- Attacks suitable for Anomaly detection
  - Denial-of-service (DoS) attacks
  - Scanning
  - Worms

HOST-BASED INTRUSION DETECTION SYSTEM (HIDS)

- Adds a specialised 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

NETWORK-BASED INTRUSION DETECTION SYSTEM (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

AN INTRUSION DETECTION SYSTEM MUST BE ABLE TO

- Run continually with minimal human supervision.
- Be fault tolerant Must be able to recover from system crashes and reinitialisations.
- Resist subversion. The IDS must be able to monitor itself and detect if it has been modified by an attacker.
- Impose a minimal overhead on the system where it is running.
- Be able to be configured according to the security policies of the system that is being monitored.
- Be able to adapt to changes in system and user behaviour over time.
- Be able to scale to monitor a large number of hosts.
- Provide graceful degradation of service in the sense that if some components of the IDS stop working for any reason, the rest of them should be affected as little as possible.
- Allow dynamic reconfiguration; that is, the ability to reconfigure the IDS without having to restart it.

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

HOST-BASED IPS (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

IPS METHODS TO IDENTIFY MALICIOUS PACKETS

- **Signature-based** : This method involves comparing network traffic against a database of known attack patterns or signatures.
- **Anomaly-based** : Anomaly detection involves establishing a baseline of normal network behaviour and then identifying deviations from this baseline.
- **Heuristic-based** : Heuristic analysis involves using rules and algorithms to identify potentially malicious behaviour. This method is less specific than signature-based method but can detect previously unknown threats such as Zero-Day attacks based on certain characteristics.
- **Protocol Analysis**: IPS devices may analyse network protocols to detect abnormalities or violations. For example, if a protocol is not adhering to its standard specifications, it may be flagged as suspicious.

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
- A collection of honeypots is called HoneyNets.

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

Requirements of Honeypots/Honeynets

- Isolation
  - They should be isolated from the production system and network are typically
  - They should contain and study any malicious activity without putting actual production systems at risk.
- Continuous monitoring
  - They should be monitored continuously analyse potential threats on the company and the behaviour of attackers.
- Deception
  - They should be as realistic as possible as they rely on the principle of deception.
  - By presenting an attractive target to potential attackers, security experts can observe and learn from their activities without exposing real assets

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **The lecture notes are very detailed. If you attend the lecture, you should be able to understand the topics.**
- **You can use any of the recommended readings! You do not need to read all the chapters!**
- **Recommended Readings note:** Focus on what was covered in the class.
  - Chapter 3, Security Foundations , CEH v11 Certified Ethical Hacker Study Guide
  - Chapter 5 ,Networks and Telecommunications, Fundamentals of Information Systems Security
  - Chapter 19, Network Security, The Cyber Security Body of Knowledge