5. Network Perimeter Security

IT6406 - Network Security and Audit

Level III - Semester 6

Overview

- This section examines the nature of intruders and intrusion detection and prevention systems. Different techniques used for intrusion detection and prevention is also discussed. Additionally, the difference between intrusion detection and intrusion prevention is briefed.

Overview

At the end of this lesson, you will be able to;

- Explain the distinction between intrusion detection and intrusion prevention.
- Describe the techniques for intrusion detection.
- Describe the ways in which and intruder would be identified in an intrusion detection system.

Overview

5.1 Intruders
- 5.1.1. Intruder Behaviour Patterns
- 5.1.2. Intrusion Techniques

5.2 Intrusion Detection
- 5.2.1. Audit Records
- 5.2.2. Statistical Anomaly Detection Rule-Based Intrusion Detection
- 5.2.3. The Base-Rate Fallacy
- 5.2.4. Distributed Intrusion Detection
- 5.2.5. Honeypots

5.3 Intrusion Prevention

5.4. Need for Firewalls

5.5. Firewall Characteristics and Access Policy

5.6. Types of Firewalls

5.7. Firewall Basing

5.8. Firewall Location and Configurations

5.9. Unified Threat Management

5.9.1.Data Leakage Prevention (DLP)

5.9.2.Deep Packet Inspection (DPI)

5.1 Intruders

- Often referred to as a hacker or cracker
- Intruders can be classified into three classes:
  - Masquerader
  - Misfeasor
  - Clandestine user

5.1 Intruders

- 5.1.1. Intruder Behavior Patterns
  - Hackers
  - Some Examples of hacker Patterns of Behavior

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pcAnywhere).
4. Brute force (guess) pcAnywhere password.
5. Install remote administration tool called DameWare.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.

5.1 Intruders

- 5.1.1. Intruder Behavior Patterns
  - Criminal Enterprise
  - Some Examples of Criminal Enterprise Patterns of Behavior

1. Act quickly and precisely to make their activities harder to detect.
2. Exploit perimeter through vulnerable ports.
3. Use Trojan horses (hidden software) to leave back doors for reentry.
4. Use sniffers to capture passwords.
5. Do not stick around until noticed.
6. Make few or no mistakes.

5.1 Intruders

- 5.1.1. Intruder Behavior Patterns
  - Internal Threat
  - Some Examples of Internal Threat Patterns

1. Create network accounts for themselves and their friends.
2. Access accounts and applications they wouldn't normally use for their daily jobs.
3. E-mail former and prospective employers.
4. Conduct furtive instant-messaging chats.
5. Visit Web sites that cater to disgruntled employees, such as f'dcompany.com.
6. Perform large downloads and file copying.
7. Access the network during off hours.

5.1 Intruders

- 5.1.2. Intrusion Techniques
  - The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system
  - Most initial attacks use system or software vulnerabilities that allow a user to execute code that opens a back door into the system
  - Intruder could also attempt to acquire passwords from the system.
    - The password file can be protected in one of two ways
      - One-way function
      - Access control

5.1 Intruders

- 5.1.2. Intrusion Techniques
  - Techniques for learning passwords by crackers/hackers.
    - Try default passwords used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.
    - Exhaustively try all short passwords (those of one to three characters)
    - Try words in the system's online dictionary or a list of likely passwords
    - Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.
    - Try users' phone numbers, Social Security numbers, and room numbers.
    - Try all legitimate license plate numbers for this state.
    - Use a Trojan horse to bypass restrictions on access.
    - Tap the line between a remote user and the host system.

5.2 Intrusion Detection

- Importance of intrusion detection
  - If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.
  - An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
  - Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

5.2 Intrusion Detection

- Approches to intrusion detection
  - Statistical anomaly detection
    - **Threshold detection**: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
    - **Profile based**: A profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts.
  - Rule-based detection
    - **Anomaly detection**: Rules are developed to detect deviation from previous usage patterns.
    - **Penetration identification**: An expert system approach that searches for suspicious behaviour

5.2 Intrusion Detection

- 5.2.1. Audit Records
  - A fundamental tool for intrusion detection is the audit record.
  - Basically, two plans are used
    - Native audit records
      - Virtually all multiuser operating systems include accounting software that collects information on user activity

5.2 Intrusion Detection

- 5.2.1. Audit Records
  - A fundamental tool for intrusion detection is the audit record.
  - Basically, two plans are used
    - Detection-specific audit records
      - A collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system.
      - Each audit record contains the following fields
        - Subject
        - Action
        - Object
        - Exception-Condition
        - Resource-Usage
        - Time-Stamp

5.2 Intrusion Detection

- 5.2.2. Statistical Anomaly Detection
  - As was mentioned, statistical anomaly detection techniques fall into two broad categories: threshold detection and profile-based systems.
  - Threshold analysis, by itself, is a crude and ineffective detector of even moderately sophisticated attacks
  - Profile-based anomaly detection focuses on characterizing the past behaviour of individual users or related groups of users and then detecting significant deviations.
  - The foundation of profile-based anomaly detection approach is an analysis of audit records.

5.2 Intrusion Detection

- 5.2.2. Statistical Anomaly Detection
  - **Profile-based anomaly detection**
  - The audit records provide input to the intrusion detection function in two ways.
  - First, the designer must decide on a number of quantitative metrics that can be used to mea- sure user behaviour. An analysis of audit records over a period of time can be used to determine the activity profile of the average user.
  - Second, current audit records are the input used to detect intrusion. That is, the intrusion detection model analyzes incoming audit records to determine deviation from average behaviour.

5.2 Intrusion Detection

- 5.2.2. Statistical Anomaly Detection
  - **Profile-based anomaly detection**
  - Examples of metrics that are useful for profile-based intrusion detection are
    - Counter
    - Gauge
    - Interval timer
    - Resource utilization
- Given these general metrics, various tests can be performed to determine whether current activity fits within acceptable limits.
    - Mean and standard deviation
    - Multivariate
    - Markov process
    - Time series
    - Operational

5.2 Intrusion Detection

- 5.2.2. Rule-Based Intrusion Detection
  - Rule-based techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious.
  - A simple example of the type of rules that can be used is heuristic rules that can be used to assign degrees of suspicion to activities
    - Users should not read files in other users' personal directories.
    - Users must not write other users' files.
    - Users who login after hours often access the same files they used earlier.
    - Users do not generally open disk devices directly but rely on higher-level operating system utilities.
    - Users should not be logged in more than once to the same system.
    - Users do not make copies of system programs.

5.2 Intrusion Detection

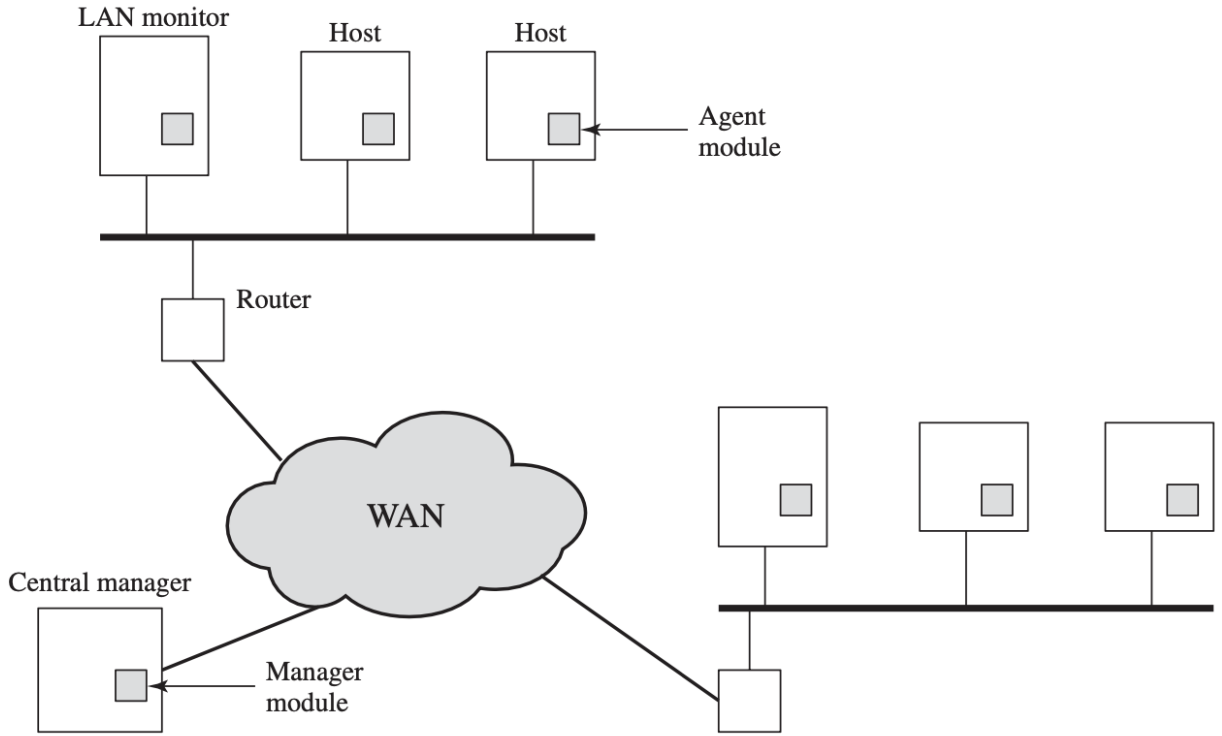
- 5.2.3. The Base-Rate Fallacy
  - To be of practical use, an intrusion detection system should detect a substantial percentage of intrusions while keeping the false alarm rate at an acceptable level.
  - Frequent false alarms will incline system managers to ignore the alarms, or much time will be wasted analyzing the false alarms.

5.2 Intrusion Detection

- 5.2.4. Distributed Intrusion Detection
  - Design issues of Distributed Intrusion Detection
    - A distributed intrusion detection system may need to deal with different audit record formats.
    - One or more nodes in the network will serve as collection and analysis points for the data from the systems on the network. Thus, either raw audit data or summary data must be transmitted across the network. Therefore, there is a requirement to assure the integrity and confidentiality of these data.
    - Either a centralized or decentralized architecture can be used but choosing one of the architecture needs careful consideration.

5.2 Intrusion Detection

- 5.2.4. Distributed Intrusion Detection
  - Architecture of Distributed Intrusion Detection



5.2 Intrusion Detection

- 5.2.5. Honeypots
  - Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.
  - Honeypots are designed to:
    - divert an attacker from accessing critical systems
    - collect information about the attacker's activity
    - encourage the attacker to stay on the system long enough for administrators to respond
- These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honeypot is suspect.

5.3 Intrusion Prevention

- While Intrusion Detection Systems can be used as passive systems/devices Intrusion Prevention Systems should be installed and implemented as active inline systems/devices.
- In addition to the functions by Intrusion Detection Systems, Intrusion Prevention Systems would do the following to prevent an attack.
  - Dropping the malicious packets
  - Blacklisting malicious sources
  - Resetting malicious network connections
  - Configuring firewalls to prevent future attack

5.4. Need for Firewalls

- Organizations need an Internet connectivity to perform the operations and provide the services available within the oraganization.
- Internet connection provides lot of benefits to the organization.
- But it allows outside world to reach and interact with the local network assets, which is a treat to the oraganization.
- Firewall can be inserted between the premises network and the Internet to establish a controlled link and establish an outer security wall or perimeter.

5.5. Firewall Characteristics and Access Policy

- Design Goals of Firewalls
  - All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.
  - Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this chapter.
  - The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

Ref1: Online Chapter 22.2

5.5. Firewall Characteristics and Access Policy…(2)

- Techniques used by firewalls to control access
  - Service control
  - Direction control
  - User control
  - Behavior control

Ref1: Online Chapter 22.2

5.6. Types of Firewalls

- Packet Filtering Firewall - applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. Filtering rules are based on, Source IP address, Destination IP address, Source and destination transport-level address, IP protocol field, and Interface.
- Stateful Inspection Firewalls - reviews the same packet information as a packet filtering firewall, but also records information about TCP connections. Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking.
- Application-Level Gateway - acts as a relay of application level traffic. They tend to be more secure than packet filters.
- Circuit-Level Gateway - a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.

Ref1: Online Chapter 22.3

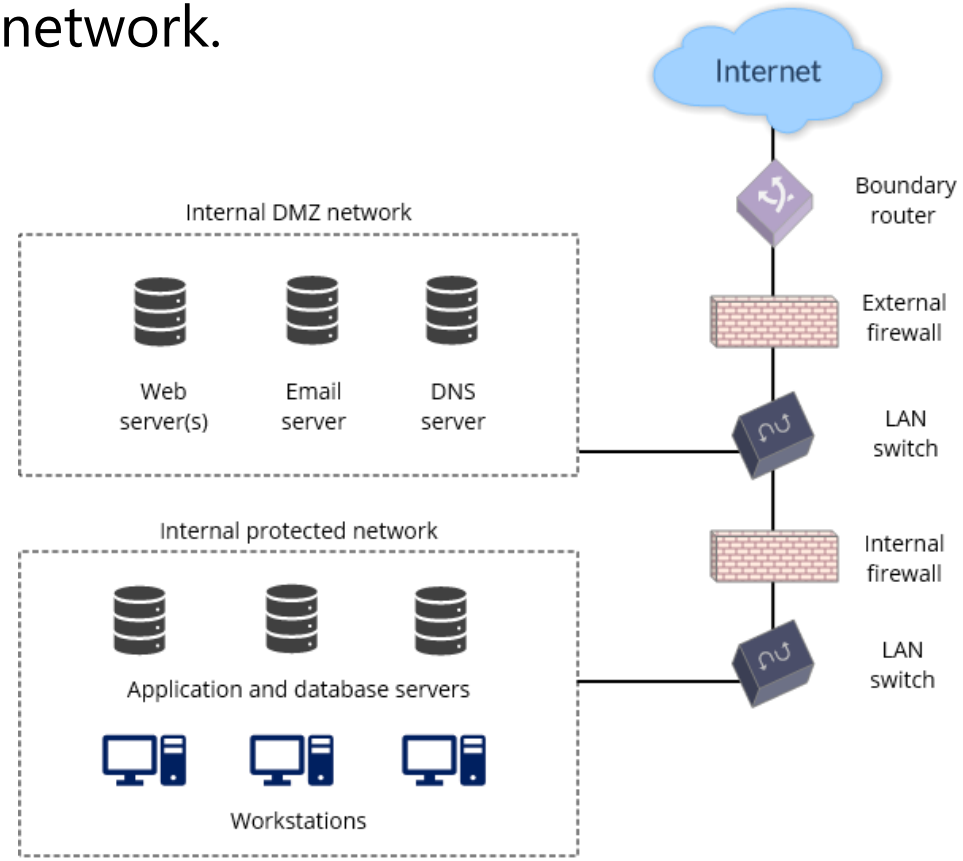
5.7. Firewall Basing

- Bastion Host - A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. The bastion host serves as a platform for an application-level or circuit-level gateway.
- Host-Based Firewall - is a software module used to secure an individual host. Available in many operating systems or can be provided as an add-on package.
- Personal Firewall - A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side.

Ref1: Online Chapter 22.4

5.8. Firewall Location and Configurations

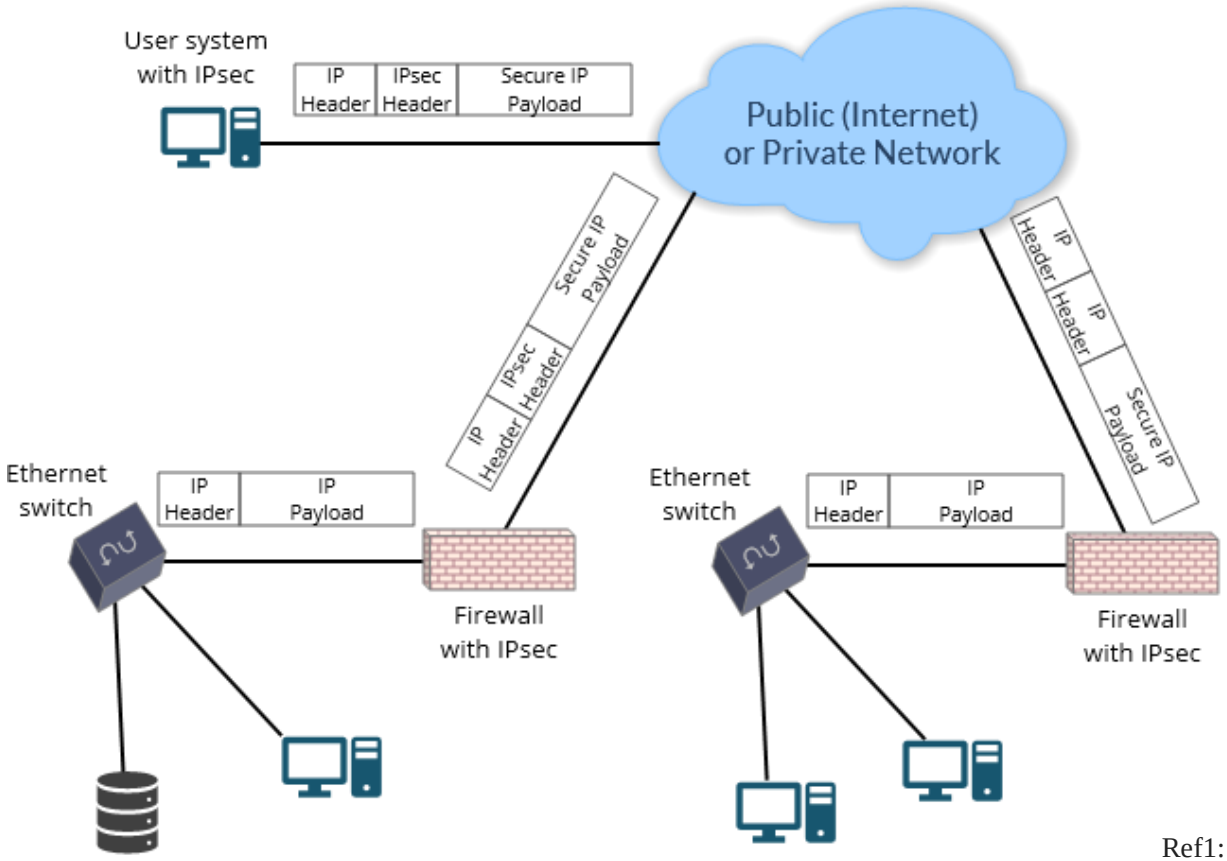
- DMZ Networks - An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network.



Ref1: Online Chapter 22.5

5.8. Firewall Location and Configurations…(2)

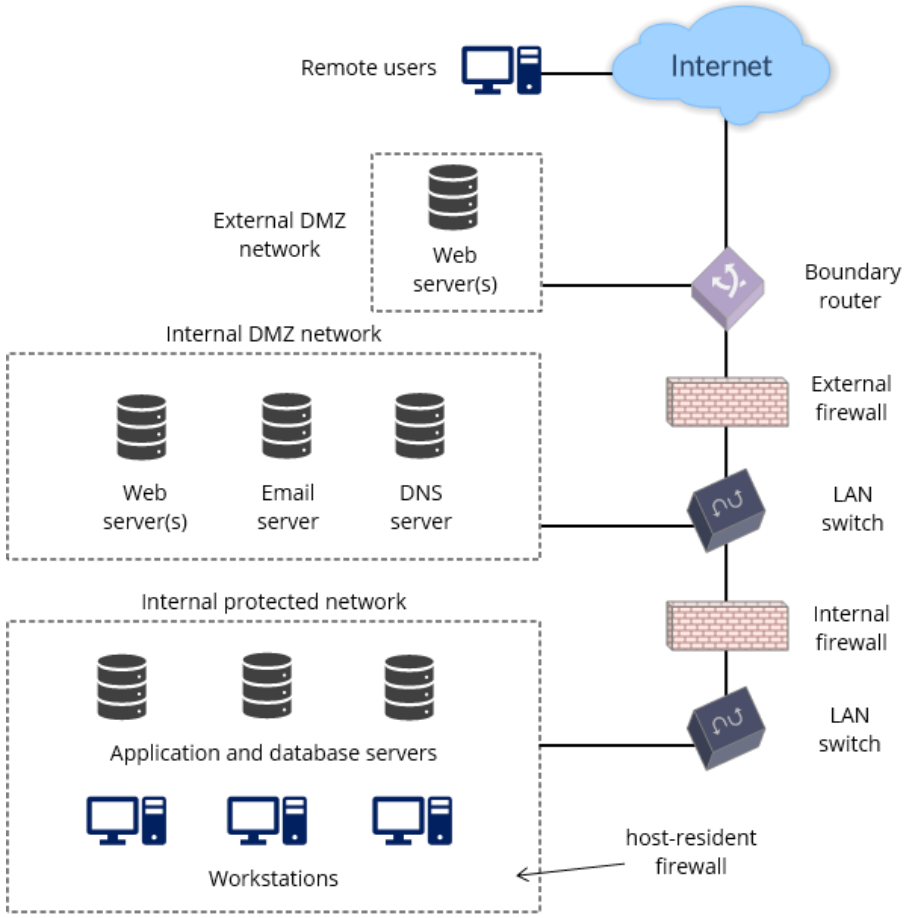
- Virtual Private Networks - a VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security for the content.



Ref1: Online Chapter 22.5

5.8. Firewall Location and Configurations…(3)

- Distributed Firewalls - A distributed firewall configuration involves stand-alone firewall devices plus host- based firewalls working together under a central administrative control



Ref1: Online Chapter 22.5

5.9. Unified Threat Management

- Unified Threat Management (UTM) is a single device or a service which provides multiple security features and services on the network.
- It protects the users of the network from numerous security threats.
- It is also known as Next-Generation Firewalls.
- It includes features such as anti-virus, anti-spam, content filtering, web filtering and so on.

5.9. Unified Threat Management...(2)

- Data Leakage Prevention (DLP) - it is the process of detection and prevention of data breaches and leakages. Companies used this mechanisms to protect and secure their valuable data.
- Deep Packet Inspection (DPI) - it can be a hardware or software system. It uses known intrusion signatures to detect abnormal network traffic.

Reference

- Ref1: Cryptography and Network Security, Principles and Practice, 7th Edition, William Stallings. Online Chapter 23.2