Chapter 12

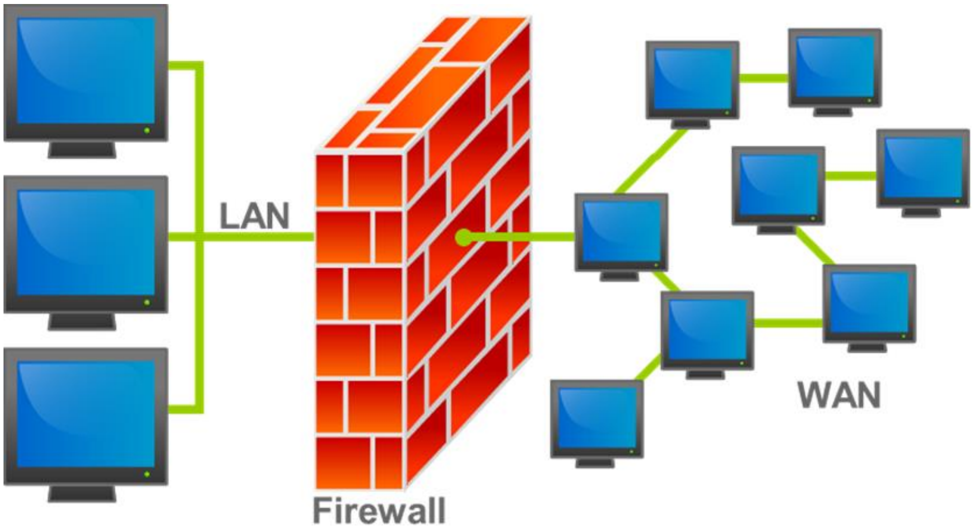
Evading IDS, Firewalls & Honeypots

Theory

Ethical Hacking

Firewall

A firewall is a hardware or software appliance to secure the internal trusted network form the intruders by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and an untrusted external network.



Types of Firewalls

1. Packet filter firewalls
2. Circuit-level gateways
3. Stateful inspection firewalls
4. Application-level gateways

Packet Filter Firewalls

Packet filtering firewall is used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports and this work on IP layer of TCP/IP. The packet filtering firewall examines the header of each packet based on a specific set of rules.

Circuit-level gateways

Circuit level gateways work at the session layer of the OSI model; they monitor TCP handshake to determine whether a requested session is legitimate or not. Information passed to a remote computer through a circuit level gateway firewall appears to be originated at user’s computer. Firewall technology supervises TCP handshaking among packets to confirm that the session is genuine.

Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network. On the other hand, they do not filter individual packets.

Application-level gateways

Application-level gateways can filter packets at the application layer of the OSI model. Application-level gateways examine traffic and filter on application specific commands such as HTTP, POST and GET. This works on the application layer of the TCP/IP Model.

Stateful inspection firewalls

Stateful inspection firewalls combine the aspects of the other three types of firewalls. They filter packets at the network layer, to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer. Traffic is filtered at three layers based on a wide range of the specified application, session, and packet filtering rules

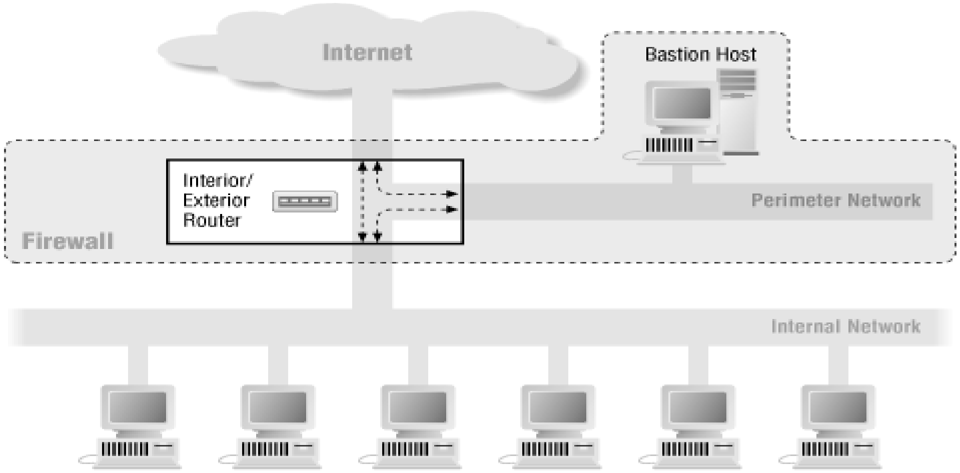
Types of Firewall Architectures

The different types of firewall architectures are

1. Bastion Host
2. Screened Subnet (DMZ - Demilitarized Zone)
3. Dual-Homed Firewall

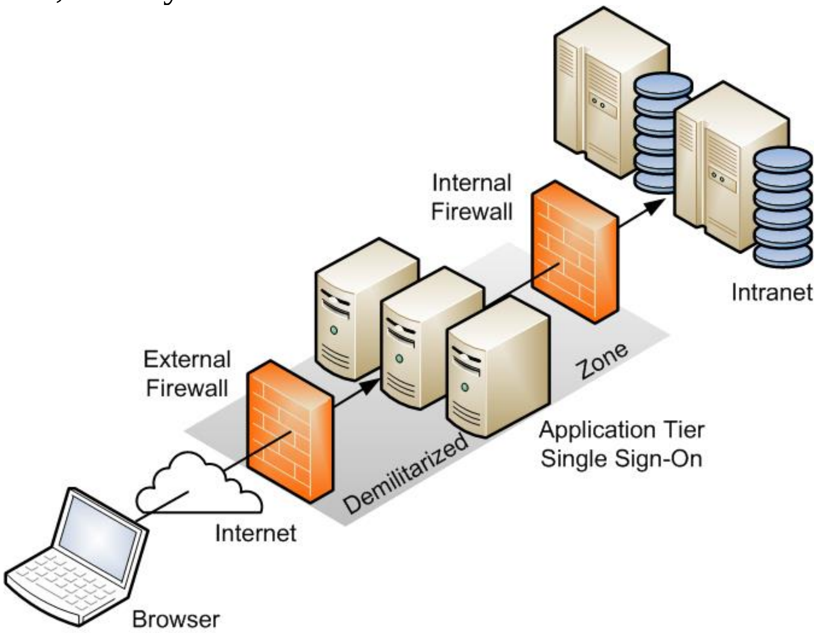
Bastion Host

A Bastion host is a computer that is fully exposed to attack. The system is on the public side of the demilitarized zone, unprotected by a firewall or filtering router. Frequently the roles of these systems are critical to the network security system.



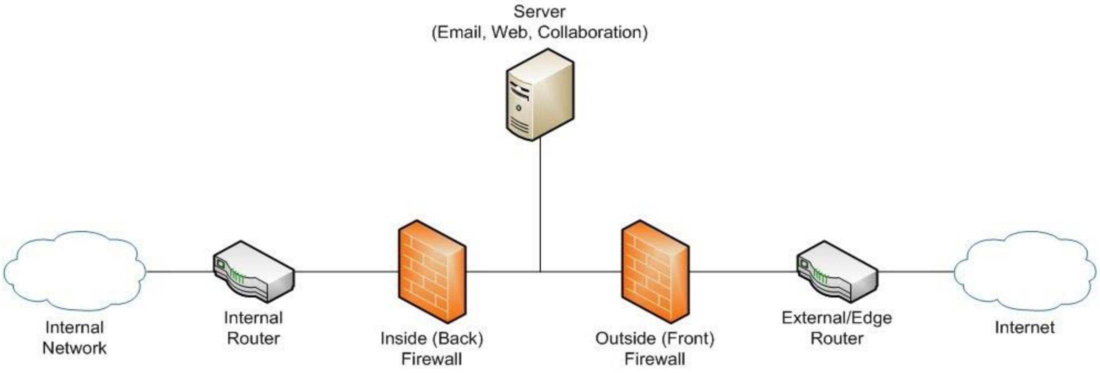
Screened Subnet (DMZ)

A screened subnet (also known as a "triple-homed firewall") is a network architecture that uses a single firewall with three network interfaces. In computer security, a DMZ or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.



Dual-Homed Firewall

A dual-homed host (or dual-homed gateway) is a system fitted with two network interfaces (NICs) that sits between an untrusted network (like the Internet) and trusted network (such as a corporate network) to provide secure access. Dual-homed is a general term for proxies, gateways, firewalls, or any server running security applications or providing security services directly to an untrusted network.



Dual-homed hosts can be seen as a special case of bastion hosts and multi-homed hosts. They fall into the category of application-based firewalls. Dual-homed hosts can act as firewalls provided that they do not forward IP datagrams unconditionally.

List of Firewall Products

Software firewalls

- Lavasoft Personal Firewall
- NetLimiter
- Windows Firewall
- ZoneAlarm
- Nftables
- Netfilter/iptables
- IPFilter
- Norton 360
- PeerBlock
- Shorewall

Hardware firewalls

- Clavister
- FortiGate
- Sophos
- Juniper SSG
- Sonicwall
- Barracuda Firewall
- WinGate
- Endian Firewall
- Cisco ASA Firepower
- Cisco PI

Honeypot

In computer terminology, a honeypot is a computer security mechanism set to detect or deflect attempts at unauthorized access to the information systems. In other words, it is a simple trap to catch the hackers. In honeypots, we will emulate the required devices in an environment, and we will let attackers come there and try to perform attacks. But meanwhile, we will get the identity of the attacker. So that we can take action against attacks. Honeypots are of two types

Low Interaction Honeypot

Low interaction honeypots allow only limited interaction for an attacker. All services offered by a low interaction honeypot are emulated. Thus, these are not themselves vulnerable and will not become infected by the exploit attempted against the vulnerability.

High interaction honeypot

High interaction honeypots make use of the actual vulnerable service or software. These are usually complex as they involve real vulnerable operating systems and applications. In this type of Honeypots, nothing is emulated everything is real and provide a far more detailed picture of how an attack or intrusion progresses or how a particular malware executes in real-time.

List of honeypots

Database Honeypots

- Elastic honey - A simple elastic search honeypot
- NoSQL Honeypot Framework - A framework for NoSQL databases
- ESPot - elasticsearch honeypot

Anti-honeypot stuff

- Kippo detect - This is not a honeypot, but it detects kippo.

ICS/SCADA honeypots

- Conpot - ICS/SCADA honeypot
- Scada-honeynet - Mimics many of the services from a popular PLC and better helps SCADA researchers understand the potential risks of exposed control system devices

Service Honeypots

- Honey NTP - NTP logger/honeypot
- Honeypot camera - Observation camera honeypot
- Troje - A honeypot built around lxc containers. It will run each connection with the service within a separate lxc container.
- Slipm honeypot - A simple low-interaction port monitoring honeypot

Web honeypots

- Glastopf - Web Application Honeypot
- PhpMyAdmin honeypot - A simple and effective phpMyAdmin honeypot
- Servlet pot - Web Application Honeypot
- Node pot - A Nodejs web app NoSQL honeypot framework application
- Basic Auth Pot - HTTP basic authentication honeypot
- Shadow Daemon - A modular Web Application Firewall / High-Interaction Honeypot for PHP, Perl & Python apps
- Google Hack Honeypot - designed to provide reconnaissance against attackers that use search engines as a hacking tool against your resources.
- Smart Honeypot - PHP script demonstrating a smart honeypot
- WP Smart Honeypot - WordPress plugin to reduce comment spam with a smarter honeypot
- Word pot - A WordPress Honeypot
- Bukkit Honeypot - A honeypot plugin for Bukkit
- Laravel Application Honeypot - Simple spam prevention package for Laravel applications
- Stack Honeypot - Inserts a trap for spambots into responses
- Eos Honeypot Bundle - Honeypot type for Symfony2 forms
- Shock pot - WebApp Honeypot for detecting Shell Shock exploit attempts

Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a device or software application that monitors network or computer system operations for malicious activities, policy violations and reports to a controlling station.

Capabilities of IDS

- Monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyber attacks.
- Including an extensive attack signature database against which information from the system can be matched.
- Recognizing and reporting when the IDS detects that data files have been altered.
- Generating an alarm and notifying the security operations team when there is a security breach.

IDS detection methods

Signature-based

Signature-based IDS performs detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. Signature-based IDS is very helpful for detecting already known attacks, but it fails in detecting new attacks, for which no pattern is available. Signatures fall into two categories

Attack signatures - They describe action patterns that may pose a security threat. Typically, they are presented as a time-dependent relationship between a series of activities.

Selected text strings - Signatures to match text strings which look for suspicious action (for example - calling /etc./passwd)

Anomaly-based

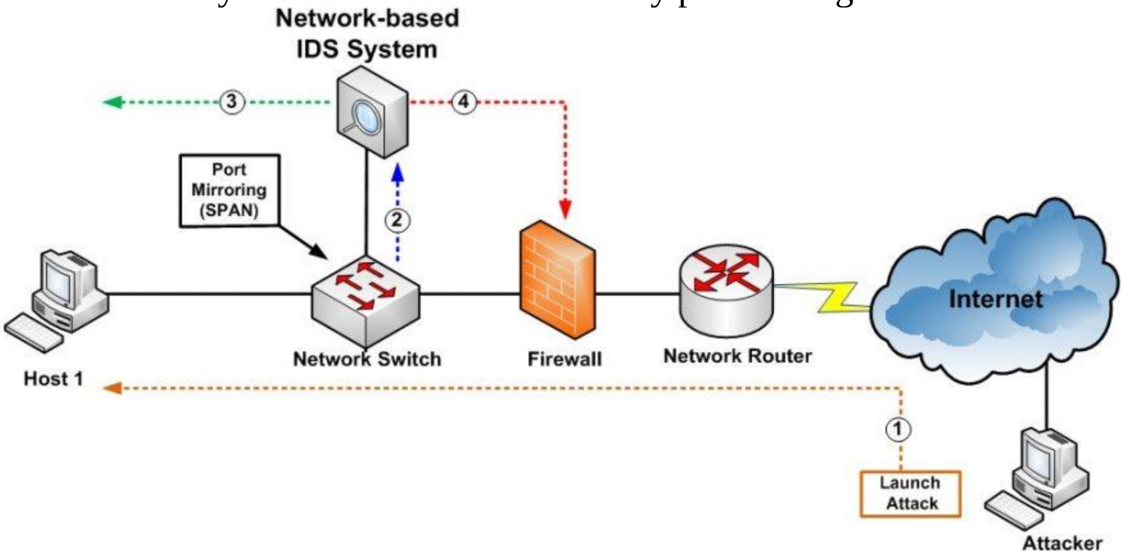
Anomaly detectors construct profiles that represent normal usage and then use current behavior data to detect a possible mismatch between profiles and recognize possible attack attempts. In order to match event profiles, the system is required to produce initial user profiles to train the system about legitimate user behaviors, which is a difficult and time-consuming task. Everything that does not match the stored profile is considered to be a suspicious action.

Types of IDS

1. Network-based Intrusion Detection System
2. Host-based Intrusion Detection System

Network-based IDS

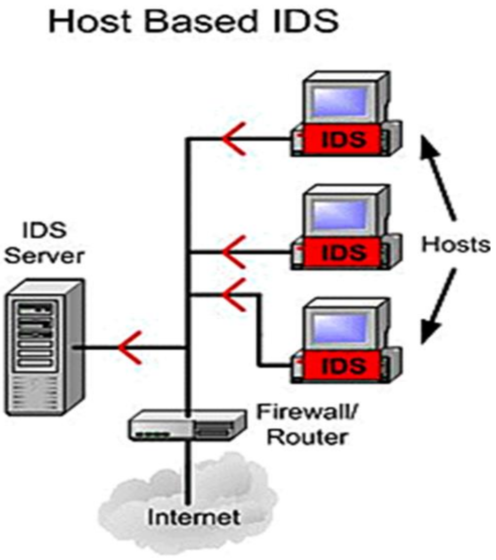
NIDS is an IDS which can be configured on a network to monitor intrusions. This will notify the administrators about any possible signature match of attacks.



Host-based IDS

HIDS are the IDS systems which will be configured on the standalone machines and will only detect intrusions for that particular machine.

HIDS might detect which program accesses what resources and discover malicious attempts, for example, a word-processor has suddenly started modifying the system password database, which can be considered as a malicious attempt on sensitive data stored on the host machine.



List of Intrusion detection systems

- Snort IDS
- SonicWall
- Juniper
- McAfee Security Agent
- Palo Alto
- Cisco ASA Security Agent

Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.

The IPS often sits directly behind the firewall and provides a complementary layer of analysis for dangerous content detection. The Intrusion Detection System (IDS) which is a passive system that scans traffic and reports back on threats but the Intrusion Prevention System (IPS) is placed in the direct communication path between source and destination, that can actively analyze and take automated actions on all traffic that enter the network. These actions include:

- Sending an alarm to the administrator
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection

Types of IPS

Host-based intrusion prevention systems

Host-based intrusion prevention systems are used to protect both servers and workstations through software that runs between your system's applications and OS kernel. The software is preconfigured to determine the protection rules based on intrusion and attack signatures. The HIPS will catch suspicious activity on the system and then, depend on the predefined rules; it will either block or allow the event to happen. HIPS monitor activities such as application or data requests, network connection attempts, and read or write attempts.

Network-based intrusion prevention systems

Network-based intrusion prevention system is a solution for network-based security. NIPS will intercept all network traffic and monitor it for suspicious activity and events, either blocking the requests or passing it. One interesting aspect of NIPS is that if the system finds an offending packet of information it can rewrite the packet so that attempt for the attack will fail, but the organization can mark this event to gather evidence against the intruder, without their knowledge.

Countermeasures

- Shut down switch ports associated with the known attack hosts.
- Perform an in-depth analysis of network traffic to detect all possible threats.
- Use a traffic normalizer to remove potential ambiguity from the packet stream before it reaches to the IDS.
- Harden the security of all communication devices such as modems, routers, switches, etc.

References:

1. Beal, V. (n.d.). Intrusion Detection (IDS) and Prevention (IPS) Systems. Retrieved from https://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp
2. WHAT IS AN INTRUSION PREVENTION SYSTEM? (n.d.). Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
3. Firewall image reference: Firewall (computing). (2018, July 03). Retrieved from https://en.wikipedia.org/wiki/Firewall_(computing)
4. Recommended Deployment Configurations. (n.d.). Retrieved from https://irmbor.co.rs/~dspalovic/assets/docsOracle/E36387/html/ol_recdepcfg_sec.html
5. Wilkins, S. (2015, August 25). A Guide To DMZs And Screened Subnets - DMZs And Screened Subnets. Retrieved from http://www.tomsitpro.com/articles/dmz-screen-subnets-guide,2-919.html
6. Intrusion Detection Systems. (n.d.). Retrieved from http://www.anses.net.in/index.php/network-and-data-security/technology-for-internet-security/intrusion-detection-systems/