IDS, Firewalls And Honeypots

IDS → Intrusion Detection System

→ Security Software or Hardware device which monitor all Inbound and Outbound Network Traffic for suspicious pattern that may indicate a network or system Breach.

→ IDS check traffic for signature that match known intrusion pattern and signals an alarm when a match is found.

→ IDS can be placed Outside / Inside the firewall, Depending on traffic.

Main Function of IDS

→ Gather and Analyze info from Computer/network.

→ Identify possible violations of security policy, including unauthorized access, as well as misuse.

→ Signal an Alarm after Detection.

Where IDS should be placed, with Firewall

-> Inside -> Ideal if it is near DMZ

-> Outside -> If most of the traffic is generated from outside the network, And we have more chance of getting malicious traffic from outside Network.

-> The Best practice is to use a layered defence by deploying one IDS in front of the firewall and one behind the firewall in the network.

Working of IDS

-> IDS have sensors to detect malicious signatures in data packets.

-> Advance IDS have Behavious based Detection as well.

-> If signature match IDS perform predefined action such as terminating connection, blocking IP, Drop Packets, Alert Admin.

How IDS Detect Intrusion

⇒ Signature Recognition → Tries to identify events that indicate an abuse of a system/network.

⇒ Anomaly Detection → Behaviour based detection. Detect fixed behavioural characteristics of the user and components of computer sys.

⇒ Protocol Anomaly Detection → In this, models are built to explore anomalies in the way vendors deploy the TCP/IP specifications.

Signature Based IDS

⇒ Compares incoming and outgoing packets with the binary signatures of known attacks using simple pattern matching techniques.

→ Only detect known attacks and can produce false positive alerts.

→ The number of sig. required is huge.

→ Comparision of sig. to huge database may slow network traffic.

Anomaly Based IDS

-> Consist of a database of Anomalies.
-> An Anomaly occur when an event occurs outside the tolerence threshold of normal traffic.
-> Any Deviation from regular use is attack.
-> There is some unpredictability in network traffic, and there are too many statistical variation, thus making these models imprecise
-> Some Anomly might only be irregularity in network usage.

Protocol Anomaly Detection

-> Works on protocol Design according to RFC specification, which dictate standard Handshake to permit universal communication.
-> Can detect New Attacks.
-> The best way to present alarm is to explain which part of the state system compromises.

General Indication of Intrusions

⇒ File System Intrusion
- → Presence of new, unfamiliar file or program.
- → Changes in file System.
- → Unexplained change in file Size.
- → missing files.

⇒ Network Intrusion
- → Repeated Probes of the availble service on your machine.
- → Connections from unusual locations
- → Repeted Login Attempts.

⇒ ⇒ System Intrusions
- → Incomplete or Modification in logs.
- → Unusual slow system performance.
- → Modification to System software or config files.
- → System Crashes or reboots.
- → Unfamiliar Process

Types of Intrusion Detection System

→ Network Based IDS ⇒ Typically consist of a black box that is placed on the network in a promiscuous mode, listening for patterns indicative of an intrusion.

→ Detect Activities such as DOS, Port Scanning and even a attempt to crack into system/computer.

→ Host Based IDS → Usually include auditing for events that occur on a specific Host.

→ Not commonly used because of overhead they incure by having to monitor each system events.

Type of IDS Alearts :-

⇒ True-Positive = Attack → Alert

⇒ False-Positive = No-Attack → Alert

⇒ False-Negative = Attack → No Alert

⇒ True-Negative = No Attack - No Alert

Firewall

→ Hardware or Software designed to prevent unauthorized access to or from private netw.
→ Placed at the junction or Gateway b/w 2 network, usually Private and Public Networks.
→ Examine all packets and block those that do not meet security criteria.

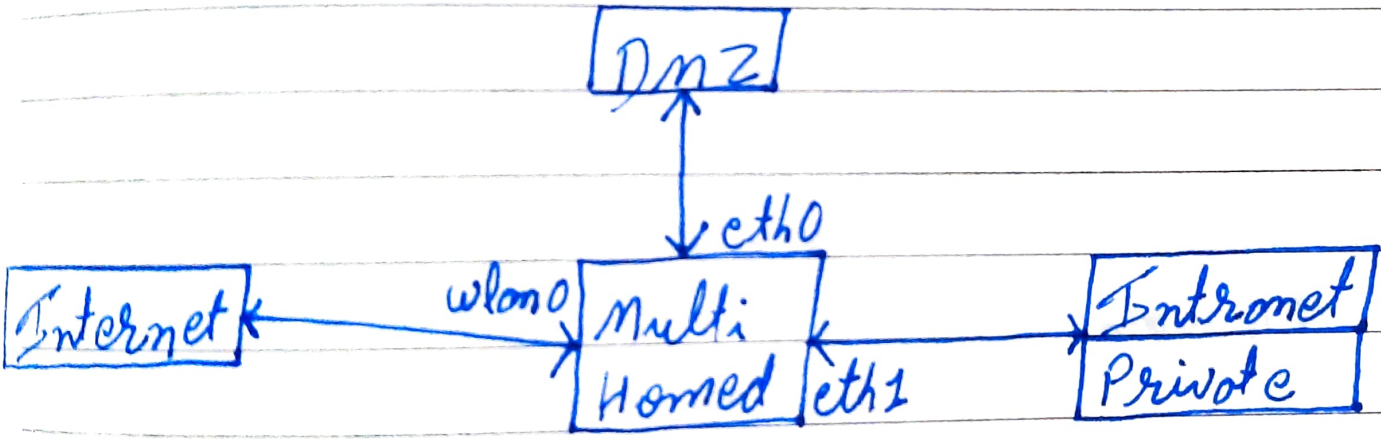
Firewall Architecture

→ Baston Host
  ↳ A computer system designed and configured to protect network resources.
  :- Public Interface → Connected to internet.
  :- Private Interface → " " intranet.

→ Screened Subnet, (DMZ)
  :- Contain Hosts that offer public services.
  :- Responds to public requests.
  :- Private Zone can not be accessed by internet user.

→ Multi-Homed Firewall

:- A firewall device or host system that has 2 or more network interface. One interface is connected to the untrusted network and another is connected to the trusted Network.



DMZ (Demilitarized Zone)

→ DMZ is a network that serves as a buffer b/w the internal secure network and insecure internet.

→ It can be created with Firewalls with 3 or more interfaces.

Types of Firewall

→ Hardware Firewall → Dedicated Hardware resources.

:- Advantages → High security level
→ Faster Analysis
→ Better Management

: Disadvantages → Expensive
→ Hard to implement & Config.
→ Consume more space and Cabling.

→ Software Firewall → Application Software.

: Advantages → Cheap
→ Ideal for personal & Home use.
→ Easier to config and reconfig.

: Disadvantages → Consume System Resources.
→ Difficult to un-install firewall
→ Slow Response Time.

Technologies used for creating firewall service:-

⇒ Packet Filtering
⇒ Circuit Level Firewall
⇒ Application Level Firewall
⇒ Stateful Multilayer Inspection
⇒ Application Proxies
⇒ Virtual Private Network (VPN)

Packet Filtering ⇒ Each Packet is compared to a set of criteria before it is forwarded.

⇒ Decision is made on following info. in packet

:- Source IP
:- Destination IP
:- Source Port
:- Destination Port
:- TCP Flag Bits
:- Protocol
:- Direction - Incoming or Outgoing

Circuit Level Gateway Firewall

→ Info. is passed to a remote computer through a circuit level gateway appears to have originated from the Gateway.

→ They monitor sessions, and determine if those sessions will be allowed or not.

→ Only allow or prevent Data Stream; they do not filter individual packet.

Application Level Firewall

→ ~~Anal~~ Analyze Application info. to make decisions ~~with~~ whether to permit traffic.

→ Being proxy based, they can permit or deny traffic According to authenticity of the user or process involved.

Stateful Multilayer Inspection Firewall

→ Combination of Packet Filtering, Circuit Level Gateway and Application Level Firewall.

→ This type of firewall can remember the packets that passed through it earlier and make decisions about future packets based on the stated in the conversation.

Application Proxy Firewall

→ Works as a proxy server and filter connections for specific services

→ It filter connections based on services and protocol, when acting as proxy.

→ Ex → FTP proxy will only allow FTP traffic.

VPN - Virtual Private Network

-> A VPN is private network constructed using public Network.

-> Used for secure transmission of sensitive info. over internet, using encapsulation and encryption.

-> A virtual Point-to-Point connection is established through the use of dedicated connection.

-> Only computers running VPN software can access VPN.

Firewall Limitations :-

→ Does not Prevent Network from new Viruses, Backdoor and insider Attack.
→ Firewall fails, if networks design and config. is faulty.
→ Not a alternative to Antivirus or Antimalware.
→ A Firewall cannot prevent social engineering Attacks.
→ A Firewall does not prevent Password Misuse.
→ A Firewall does not block attacks from Higher level of the protocol stack.
→ A Firewall is unable to understood tunneled traffic.

Honeypots

An info. security resource configured/set up to attract and trap peoples/Hackers. who attempt to penetrate on orgnization network.

-> It has no authorized activity, no production value and any traffic to it is like probe, attack or compromise.

-> Honeypot can log port Access attempts, or monitor on attackers keystrokes. These could be an early warning of a more powerful attack.

Types of Honeypots :-

-> Low-Interaction Honeypot -> Limited services

-> Medium-Interaction Honeypot -> Simulate a real O.S

-> High-Interaction Honeypot -> Full " and Comp. Records.

-> Production Honeypots -> Collect internal Flaw, Mal-Insider.

-> Research Honeypots -> High interaction Honeypots, deployed at Research Institute, Government, Military Organizations.