**Module 12: Evading IDS, Firewalls, and Honeypots**

**IDS:**

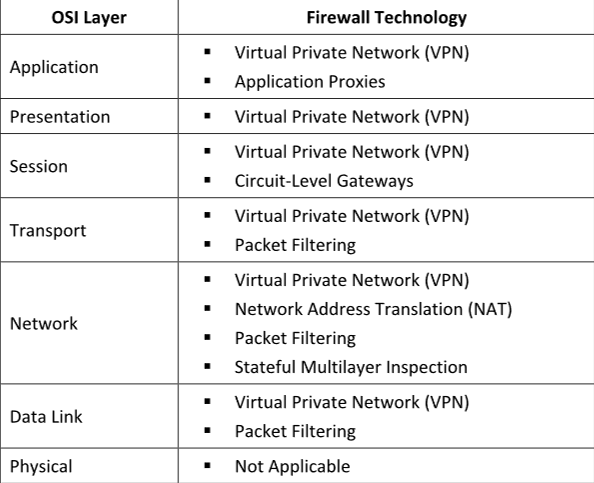
* Also referred to as a packet sniffer, which intercepts packets traveling via various communication media and protocols
* Check traffic for signatures that match known intrusion patterns and signals an alaram when a match is found
* Placed outside/inside the firewall
* How an IDS detects an Intrusion?
  + **Signature Recongnition:** Misuse detection, tries to identify events that indicate an abuse of a system or network resource.
  + **Anomaly Detection:** Not-use detection, base on the fixed behaviroal characteristics of the users and components in a computer system
  + **Protocol Anomaly Detection:** Models are built to explore anomalies in the way in which vendors deploy the TCP/IP specification
* **Types of IDS**
  + **Network-Based IDS:** Consist of a black box that is placed on the network in a promiscuous mode, listening for patterns indicative of an instrusion.
  + **Host-Based IDS:** Usually include auditing for events that occur on a specific host
* **Types of IDS Alerts**
  + TP: Attack->Alert
  + FP: No Attack -> Alert
  + FN: Attack -> No Alert
  + TN: No Attack -> No Alert

**IPS**

* Also considered as an **active IDS** since it is capable of not only detecting..but also preventing..
* Unlike an IDS, which is passive, an IPS is placed **inline in the network**, between the src and dst to **actively analyze the network traffic** and to automatically take decisions
* Types of IDS: Network-based IPS, Host-based IPS
* **Adv over IDS**
  + IPS can block as well as drop illegal packets
  + Be used to monitor activities occurting in a single org
  + Can prevent the occurrence of direct attacks in the network by controlling the amount of network traffic

**Firewall**

* Hardware or software designed to prevent **unauthorized access** to or from a private network.
* Placed at the junction or **gateway** between two networks, which is usually between a private network and a public network such as the Internet
* **Architecture**
  + **Bastion Host:** A computer system designed and configured to protect network resources from attacks.
  + **Screened Subnet:** The screened subnet or DMZ contains hosts that offer public services.
  + **Multi-homed Firewall:** A firewall with two or more interfaces is present that allows further subdivision of the network based on the specific security objectives of the org
* Technologies operating at each OSI layer



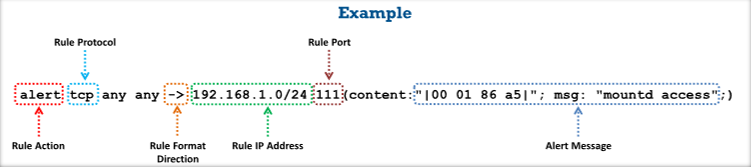
* **Technologies**
  + **Packet Filtering**
    - Work at the **network layer** of OSI (or Internet layer of TCP/IP), usually form part of a router
    - Each packet is compared to a set of criteria before it is forwarded
  + **Circuit Level Gateways**
    - **Session** layer of OSI (**Transport** layer of TCP/IP)
    - Info passed to a remote computer through a circuit-level gateway
    - Monitor requests to create sessions and determine if those sessions will be allowed
    - Allow or prevent data stream, not individual packets
  + **Application Level Firewall**
    - Application-level gateways (Proxies) can filter packets at the **application** layer of OSI (**Application** Layer of TCP/IP)
    - Traffic is **restricted to services** supported by the proxy
    - Configured as a web proxy prohibit FTP, gopher, telnet, or other traffic
    - Examine traffic and filter on **application-specific commands** such as http:post and get
  + **Stateful Multilayer Inspection**
    - **Combine the aspects of the other three types** of firewalls
    - Filter packets at the network layer of OSI or the Internet layer of TCP/IP, and evaluate the contents of packets at the application layer
  + **Application Proxies**
    - Work as a proxy server and filter connection for specific services
    - Filter connections based on the services and protocols appropriate to that application
  + **NAT**
    - Work with a router, similar to packet filtering. Modify the packet the router sends simultaneously
    - Have the ability to change the address of the packet and make it appear to have arrived from a valid address
    - It can act as a firewall filtering techniques
  + **VPN**
    - **A private network** constructed using public networks
    - Used for **secure tranmission**, using **encapsulation and encryption**
    - Establish a virtual p2p connection through the **used of dedicated connections**
* Limitations
  + Does not protect the network from new **viruses, backdoors, insider attacks**
  + Do nothing if the network design or configuration is faulty
  + Not an alternative to AV or antimalware protection
  + Do not prevent password misuse
  + Do not block attacks from a **higher level of the protocol stack**
  + Do not protect against attacks from **dial-in connections** or attacks originating from **common ports** and applications
  + Unable to understand **tunneled traffic**

**Honeypot**

* An info system resource that is expressly set up to **attract and trap** attackers
* Log port access attempts or monitor an **attacker’s keystrokes**
* **Types of Honeyports**
  + Low-interaction Honeypots
  + Medium-interaction Honeypots
  + High-interaction Honeypots
  + Pure Honeypots
* **Classfication of honeypots based on strategy**
  + Production Honeypots
  + Research Honeypots
* **Classfication of honeypots based on deception technology**
  + Malware Honeypots
  + Database Honeypots
  + Spam Honeypots
  + Email Honeypots
  + Spider Honeypots
  + Honeynets

**Intrusion Detection Tools**

* **Snort** 
  + Can perform protocol analysis and content searching/matching, and is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, and OS fingerprinting attempts
  + Use a flexible rules language to describe traffic
  + Uses of Snort
    - Straight packet sniffer like tcpdump
    - Packet logger
    - Network IPS
  + **Rules:** rule action+rule protocol+rule format direction+rule ip+rule port+alert message



* + Rule Actions
    - Alert
    - Log
    - Pass: Drop (Ignore) the packet
  + IP Protocols
    - TCP
    - UDP
    - ICMP
* **Suricata**
* **AlienBault OSSIM**

**IPS Tools**

* **AlienVault Unified Security Management (USM)**
* **Firewalls: ZoneAlarm Free Firewall 2019**
* **ManageEngine Firewall Analyzer**

**Honeypot Tools**

* **KFSensor:** A host-based IDS that acts as a honeypot
* **SPECTER**

**IDS Evasion Techniques**

* **Insertion Attack**
  + The process by which the **attacker confuses the IDS** by forcing it to read invalid packets
  + An IDS blindly believes and accepts a packet that an end system rejects, and an attacker exploit this condition and **inserts data into the IDS**
  + Occurs when the NIDS is less strict in processing packets than the internal network
  + Obscure extra traffic and the IDS concludes the traffic is safe. The **IDS gets more packets** than the destination.
* **Evasion**
  + An end system **accepts a packet** that an IDS rejects.
  + An attacker **exploits the host computer** without the IDS realizing it,
  + The attacker sends **portions of the request i**n packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the IDS
* **DoS Attack**
  + Many IDSs use a centralized server for logging alerts
  + Attackers can perform DoS on the centralized server
  + The attackers’ intrusion attempts will not be loggeg
* **Obfuscating**
  + Attacker who **encode the attack packet payload** that only the des host can decode it.
  + Attackers manipulate the **path referenced in the signature** to fool the HIDS
  + **Encode attack patterns in unicode** to bypass IDS filters, but be understood by an IIS web server
  + **Polymorphic code** is another means to circumvent **signatured-based** IDSs by creating different attack patterns
  + Attacks on **encrypted protocol** are obfuscated
* **FP generation**
  + Craft malicious packets just to generate alerts
  + Use these FP alerts to hide the real attack traffic
* **Session Splicing**
  + **Split the attack traffic** into many packets such no single packet triggers the IDS
  + IDSs stop reassembly if they **do not receive packets within a certain time**
  + The IDS will stop working if the target host keeps the session active for a time longer than the **IDS reassembly time**
* **Unicode Evasion**
  + All the code points are treated differently but it is possible that there could be multiple representations of a single char in the Unicode code space
  + IDS handle unicode improperly as Unicode allows multiple interpretations of the same char
* **Fragmentation Attack**
  + Fragmentation timeouts vary between the IDS and the host
* **Overlapping Fragments**
  + **Generate a series of tiny fragments** with overlapping TCP seq numbers
* **TTL Attacks**
  + The attacker has to have a prior knowledge of the topology of the victim’s network
  + The info can be obtained using tools such as craceroute
* **Invalid RST Packets**
  + TCP uses a 16-bits checksum field for error-checking of the header and data
  + The attack makes the IDS think the communication has ended
* **Urgency Flag**
  + Many IDSs **do not consider the urgent pointer** and process all the packets in the traffic, wheras the taraget processes the urgent data only
  + Result in the IDS and the target system having **dfferent sets of packets**, which can be exploited by attackers
* **Polymorphic Shellcode**
  + Include **multiple signatures**
  + **Encode the payload**
  + The **shellcode is completely rewritten** each time it is sent
  + **Evade the ommonly used shellcode strings**
* **ASCII Shellcode**
  + Bypass the IDS signature as the **pattern matching** does not work effectively with the ASCII values
* **Application-layer Attacks**
  + IDS cannot verify the **signature of the compressed file format**
* **Desynchronization**
  + **Pre-Connection SYN:** Send an initial SYN before the real connection is established, but with an invalid TCP checksum
  + **Post-Connection SYN:** Send a post connection SYN packet which will have divergent seq numbers.
* **Encryption**
* **Flooding:** Produce noise

**Evading Firewalls**

* **Firewalking:** Use TTL value to determine gatyeway ACL filters and it maps networks
* **Banner Grabbing:** Fingerprinting method to detect the vendor of a firewall and its firmware version.
* **IP Address Spoofing**
* **Source Routing:** Allow the sender of a packet to partially or completely specify the route
* **Tiny Fragments:** Create tiny fragments of outgoing packets forcing some of the TCP packet’s header info into the next fragment
* **Using an IP Address in Place of a URL**
* **Using a Proxy Server**
* **ICMP Tunneling:** Allow tunneling a backdoor shell in the data portion of ICMP Echo packets. By using **Loki ICMP tunneling** to execute cmds of choice by tunneling them inside the payload of the ICMP echo packets
* **ACK Tunneling:** Allow tunneling a backdoor application with **TCP packets with the ACK bit set**. Tool such as **AckCmd** can be used to…
* **HTTP Tunneling:** Allow attackers to perform various Internet tasks desipte the restrictions imposed by firewall. Encapsulates data inside HTTP traffic. Can use tools such as **HTTPort and HTTHost**, **Super Network Tunnel**
* **SSH**: Tools such as **OpenSSH, Bitvise,** and **Secure Pipes**
* **DNS Tunneling:** Small size constraint on external queries allow the DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Tools such as **NSTX, Heyoka**, and **Lodine** use this technique of tunneling traffic aross DNS port 53.
* **Through External Systems:** Attackers sniff the user traffic and steal the SID and cookie. Redirect users’ web browser to the attacker’s web server. Download and execute…
* **Through MITM Attack:** Make use of DNS server and routing techniques. DNS poisoning, redirect, download and execute.
* **Through Content:** Send content containing malicious code and trick a user to open it.
* **Through XSS**

**Evasion Tools**

* **Traffic IQ Professional:** Generate custom attack traffic
* **Packet Fragment Generator Tools:** Colasoft Packet Builider

**Detect Honeypots**

* Layer7 : Observe the latency of the response.
* Layer4: Analyze the TCP window size
* Tools: **Send-Safe Honeypot Hunter**, checking lists of HTTPS and SOCKS proxies for honey pots.

**IDS Evasion Countermeasures**

* Shut down switch ports associated with known attack hosts.
* Perform an in-depth analysis of ambiguous network traffic for all possible threats.
* Use TCP FIN or Reset (RST) packet to terminate malicious TCP sessions.
* Look for the nop opcode other than 0x90 to defend against the polymorphic shellcode problem.
* Train users to identify attack patterns and regularly update/patch all the systems and network devices.
* Deploy IDS after a thorough analysis of the network topology, nature of network traffic, and number of hosts to monitor.
* Use a traffic normalizer to remove potential ambiguity from the packet stream before it reaches the IDS.
* Ensure that IDS normalize fragmented packets and allow those packets to be reassembled in the proper order.
* Define DNS server for client resolver in routers or similar network devices.
* Harden the security of all communication devices such as modems, routers, etc.
* If possible, block ICMP TTL expired packets at the external interface level and change the TTL field to a considerable value, ensuring that the end host always receives the packets.
* Regularly update the antivirus signature database.
* Use a traffic normalization solution at the IDS to protect the system from evasions.
* Store the attack information (attacker IP, victim IP, timestamp) for future analysis.

**Defend against Firewall Evasoin**

* The firewall should be configured such that the IP address of an intruder should be filtered out.
* Set the firewall rule set to deny all traffic and enable only the services required.
* If possible, create a unique user ID to run the firewall services instead of running the services using the administrator or root ID.
* Configure a remote syslog server and adopt strict measures to protect it from malicious users.
* Monitor firewall logs at regular intervals and investigate all suspicious log entries found.
* By default, disable all FTP connections to or from the network.
* Catalog and review all inbound and outbound traffic allowed through the firewall.
* Run regular risk queries to identify vulnerable firewall rules.
* Monitor user access to firewalls and control who can modify the firewall configuration.
* Specify the source and destination IP addresses as well as the ports.
* Notify the security policy administrator about firewall changes and document them.
* Control physical access to the firewall.
* Take regular backups of the firewall rule set and configuration files.
* Schedule regular firewall security audits.