Evading IDS, Firewalls, and Honeypots
Module - 10

 # Indicators of File System Intrusion :

- Have unfamiliar files or programs been introduced to the environment ?
- Have Privileges been escalated above normal ?
- Have File permissions changed in an unusal Fashion ?
- Have file changed size in an unexpected fashion ?

 # Indicators of Network Intrusion :

- Are unusually high volumes of traffic leaving the network ?
- Is there unexplained traffic on unusual ports or over unusual protocols ?
- Are there an unusually high number of failed logins ?
- Are there connection requests from unusual IP address ?

 # Firewalls :

A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and another outside network.

 # Firwall Implementations :

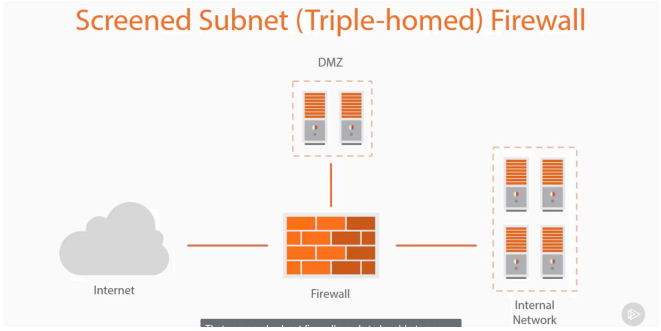
1. Software Firewall
2. Hardware Firewall
3. Firewall as a Service : CloudFlare

 # Firewall Architectures :

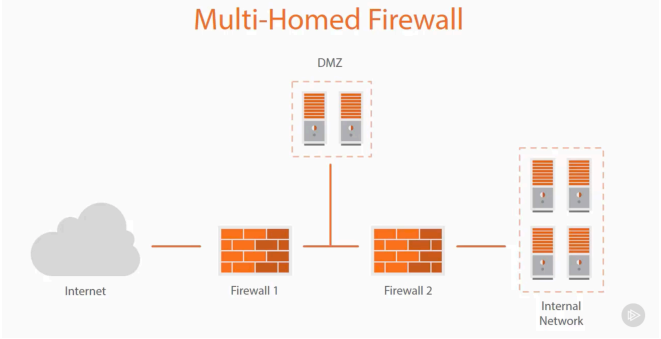
1. **Bastion Host** : A computer that is fully exposed to attack. The system is on the public side of the demilitarized zone, unprotected by the firewall or filtering router. Frequently the role of these system are critical to the network security system.

2. **Screened Subnet** (Triple Homed) Firewall : It divide network into three logical segments

DMZ : Demilitarized Zone network : it is the different subnet in a internal network, it contain assets that you want publicly exposed so that it need to be accessible by the internet. And this subnet is also accessible by the internal network.



Multi Homed Firewall :

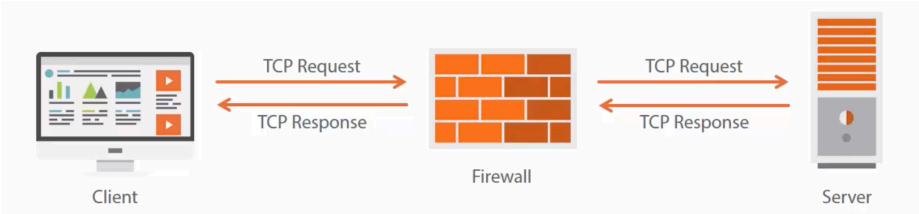


 # Packet Filtering firewall :

Packet Filtering Firewall do not looks at data and the packet filtering firewall will allow the malicious payload to come in Because it is not looking at the Headers and other infos

 # Circuit-level Gateway Firewalls :

The circuit level gateway firewall create two connection one with the public internet and one with the internal network , It also match response with the request.



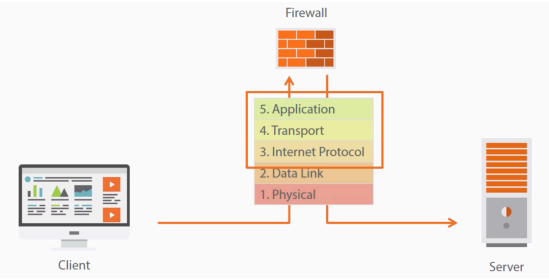
 # Application-Level Gateway Firewalls :

It sits at layer - 7 at the top of the stack it check all the protocol no only http, it has the ability to intercept the traffic contents. It can block sites similar to cloudflare

 # Stateful Multilayer Inspection firewall :

It will combine the aspects of above 3 firewalls :

1. Packet
2. Circuit
3. Application



 # Identifying the Firewall :

- Fingerprinting based on Open Ports and Protocols
  Typically by port scanning with nmap
- Banner Grabbing
  The system being connected to simply announces itself via banner or connection
- Open ports behind the firewall may be discovered by “Firewalking”
- PHASE 1 : “Hopcount Ramping” they just keep bumping up the TTL until they reach the destination host
- PHASE 2 : FIREWALKING : **Firewalking** uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device

 # Evasion Techniques :

1. IP address Spoofing : Change the Source IP address and take that one which can bypass the firewall
2. Source Routing : In computer networking, source routing, also called path addressing, allows a sender of a packet to partially or completely specify the route the packet takes through the network.
3. Tiny Fragment Attack : A TCP Level Attack which attempt to evade a firewall by splitting a packet into multiple fragments, the first of which does not contain port information and is not blocked. The second fragment contains the port and may be allowed trough.
4. ICMP, ACK and HTTP Tunneling : ICMP via Ping or traceroutes, ACK for three way handshake or simply via HTTP.
Malicious Payload Wrapped in Protocol.
Target unwraps, executes, Re-Wraps and Send
5. Firewall Bypass channels : By using proxy, using VPNs (Creates a encrypted tunnel) , TOR (can obfuscate the nature of the target’s website that an attacker is looking to connect to.)

 # Evasion Tools :

- **Nessus** - Also a vulnerability scanner
- **ADMmutate** - Creates scripts not recognizable by signature files
- **NIDSbench** - Older tool for fragmenting bits
- **Inundator** - Flooding tool
- **Gtunnels -** works as a local HTTP or SOCKs proxy server
- **HTTPTunnel :** Tunneling over HTTP
- **Nmap :**

 # Intrusion Detection System :

An IDS is a Device or software application that monitors network or system activities for malicious activities or policy violation and procedure electronic reports to the management Station.

 # Role of an IDS :

1. Frequently referred to as a “Packet Sniffer”
2. They’re not just about preventing intrusions like a firewall, they also alert administrator
3. They Typically record events for later review
4. They may simply detect and report (intrusion detection or “Passive” system)…
5. Or actually block (Intrusion Protection, IPS or “reactive” system)

 # Intrusion Protection System :

A system that terminates connections is called an IPS and is another form of an application layer firewall

 # Signature Based IDS : It contains the Signature Database and matches the traffic to detect any malicious activity

 # Statistical Anomaly Based IDS : An IDS which is anomaly based will monitor network traffic and compare it against an established baseline.

-> Training, Testing and Maintenance

 # Protocol Anomaly Detection : Protocol anomaly detection identifies deviations from protocol norms. This may include duplicate or spoofed ip address or MAC, invalid URI characters or non-contiguous TCP Sequence numbers, among others.

 # Understanding Anomalous Traffic :
- Detection can involve artificial intelligence that attempts to identify norms
- It may also adhere to a strict mathematical model known as “Strict Anomaly detection”
- There remains a risk of false positive - legitimate traffic being classed as malicious
- But also a risk of an atttack being delivered via “correctly” formed traffic

 # Network Based IDS :

A network intrusion detection system is placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.

 # Understanding NIDS :
- Typically monitors passing traffic on a subnet
- A NIDS implementation may be configured to scan all inbound and outbound traffic
- but that may also create a bottleneck in a the traffic flow
- May be implemented in one of two fashions:
  - Online: monitors the network in real time
  - Offline: reviews previously captured packets

 # Host Intrusion Detection system (HIDS) :

A host intrusion detection system runs on individual hosts or devices on the network and monitors the inbound and outbound packets from the device only.

 # Understanding HIDS :

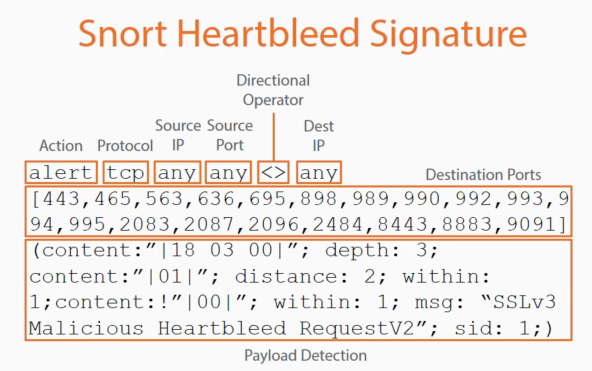
- Can be tailored specifically to the behavioural norms of the host
- May monitor changes to files in the system and raise alerts based on suspicious patterns
- A HIDS is much more effective at identifying insider abuse
- Configuration changes are a perfect example of required monitoring
  - A change is something an administrator should know about

 # Other Classes of IDS :

1. Log File Monitoring
2. File Integrity Checking
3. System Integrity Verifier

 # Snort :

Snort Modes :
1. Sniffer
2. Packet Logger
3. Network Intrusion Detection



 # Evasion by Obfuscation

: Polymorphic Code : Code that uses a polymorphic engine to mutate while keeping the original algorithm intact. **The code changes itself each time it runs**, but the function of the code will not change at all.

: ASCII Shellcode : Shellcode is a smal piece of code used as the payload in the exploitation of a software vulnerability. Encoding the payload into ASCII can bypass **character restrictions** in some IDS.

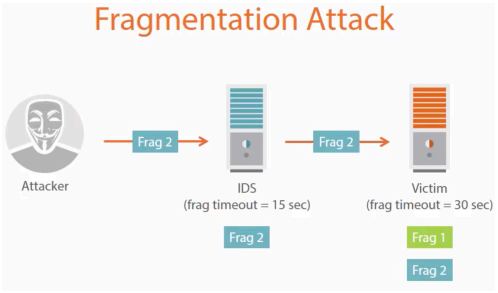
: Unicode

: Encrypted or compressed Payload

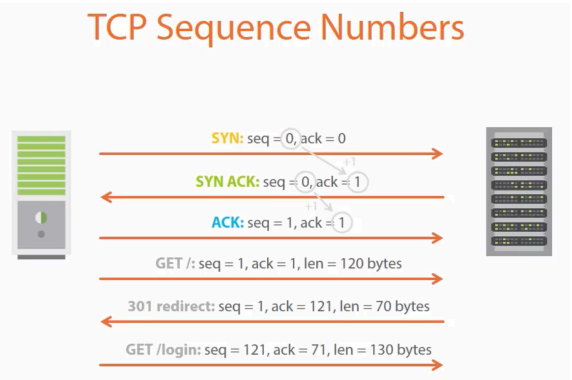
: Session Splicing : Some IDS don't reconstruct the session before pattern matching is done

Ex : If an attacker can deliver packets with enough delay between then that the IDS stops reassembling them merely passes them through, they can conceal that payload and circumvented the control of the IDS.

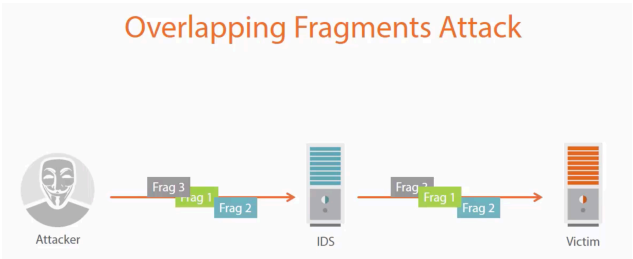
 # Fragmentation Attacks :



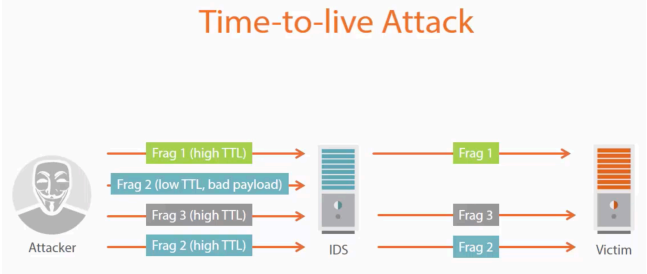
 # TCP Sequence Numbers



 # Overlapping Fragment Attacks :



 # Time-to-Live Attacks :



 # DOS and Resources Exhaustion Attacks :
- Flood the IDS with traffic that triggers alerts (Flooding Attack)
  "stick" and "snot" tools
- Make identifying legitimate attacks More difficult amongst all the noide
- Often referred to as "False Positive Generation"
- Can overwhelm the ability of the IDS to inspect traffic
- May lead to Exhaustion of resources such as disk Capacity
  Which may leads to events not being logged

 # Other TCP Level Attacks :

- Invalid RST Packets
- URG Flag
- Desynchronization

 # Honeypots :

 # Honey Trapping :

Honey Trapping is the private investigative practice of evaluating the fidelity of partners in martial and non martial romantic relationship.

 # Honeypot : A Security Resource whose values lies in being probed, attacked , or compromised

Honeypots Tools :

1. Canary
2. Honeyd
3. Canary tokens : They are also known as honey tokens,

 # Observing Honeypot Behaviour :

- Internally Observable :
  Machine looks like it was just set up yet has “enticing” files
  Abnormal Behaviour of drives and devices
  Driver names not consistent with norms

- Externally Obsevable :
  There’s lack of “normal’ outbound traffic
  it’s a sole machine in a DMZ or other subnet
  Honeypot or not : https://honeyscore.shodan.io
  conpot.org