chapter 12

Evading IDS, Firewall, Honeypots

Concepts

IDS

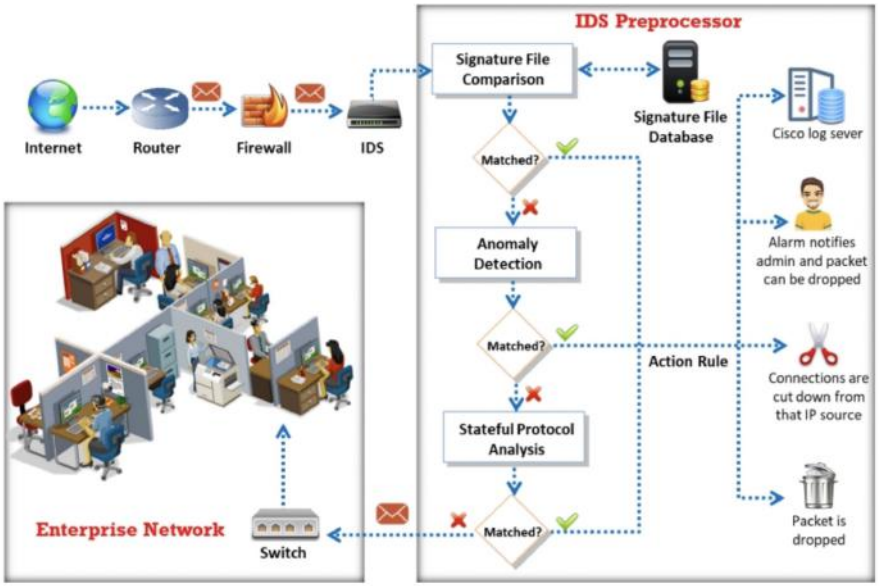
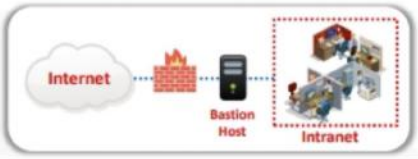


Figure 12.2: Working of IDS

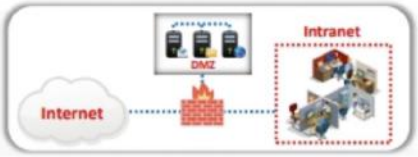
Bastion Host

- A bastion host is a computer system designed and configured to protect **network resources** from attacks
- Traffic entering or leaving the network passes through the firewall. It has two interfaces:
  - a **public interface** directly connected to the Internet
  - a **private interface** connected to the Intranet



Screened Subnet

- The screened subnet or Demilitarized Zone (DMZ) contains **hosts** that offer public services
- The DMZ **responds to public requests**, and has no hosts accessed by the private network
- This private zone can not be accessed by **Internet users**



Multi-homed Firewall

- In this case, a firewall with two or more interfaces is present that allows further subdivision of the network based on the **specific security objectives** of the organization

Firewall Services

- Packet Filtering
- Circuit Level Gateways
- Application Level Firewall
- Stateful Multilayer Inspection
- Application Proxies.
- VPN.
- NAT

OSI Layer	Firewall Technology
Application	▪ Virtual Private Network (VPN) ▪ Application Proxies
Presentation	▪ Virtual Private Network (VPN)
Session	▪ Virtual Private Network (VPN) ▪ Circuit-Level Gateways
Transport	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Network	▪ Virtual Private Network (VPN) ▪ Network Address Translation (NAT) ▪ Packet Filtering ▪ Stateful Multilayer Inspection
Data Link	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Physical	▪ Not Applicable

Packet Filtering Firewall

- Packet compared with rules, criteria.
- can drop packet, forward, send message to originator.
- Rules: source, dest IP, Port, Protocol.

Circuit level Gateway Firewall

- works @ session layer.
- Monitor requests to create sessions & determine if those sessions allowed.
- Passed to a remote system through circuit gateway.

Application Level Firewall

- works & filters @ application layer.

- Incoming / outgoing allowed → Proxy.
  other requests → denied.
- examine traffic, filter app specific commands

Stateful Multilayer Inspection Firewall

- Combination of (Packet, Circuit, Application) firewalls.
- filter packets at network layer
- evaluate content of packets.

Application Proxy

- Proxy Server & filters connections for specific services, protocols.

Types of HoneyPot

Low Interaction (limited services, apps)

Medium Interaction (simulate real OS, apps)

High Interaction (simulate all services)

Pure (emulate real production network)

Production, Research } deployment

Malware
Spam
Spider
Database
Email
Honeynets

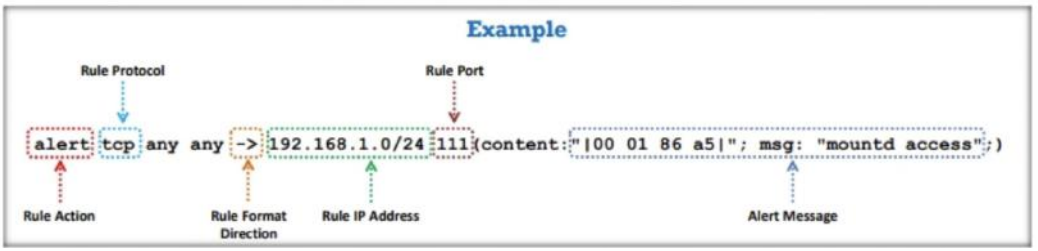
} Technology

Solutions

Tool → Snort

- open source IDS
- detect traffic, analyse packet, log IPs
- Protocol analysis, content match.
- flexible rules language. (single line)
- custom rules can be set based on need.

Two Parts : Rule Header, Rule options.



Rule Header → Complete set of rules.

Actions : Alert, log, Pass

Protocols : TCP, UDP, ICMP

direction operator : → (single direction)

<> (bidirection)

Port number : "any", static, range, negation

Other Tools :

- Suricata (IDS, NSM, offline PCAP)
- AlienVault OSSIM

Mobile Tools :

- zIPS
- WiFi Inspector
- WiFi Intruder Detect

IPS Tools:

- Alienvault USM

Firewall Tools

- Zone Alarm Free Firewall
- ManageEngine Firewall Analyser

Mobile Tools

- NoRoot Firewall
- Mobile Privacy Shield
- NetPatch Firewall

Honeypot Tools

- KFSensor (host based IDS, honeypot)
- SPECTER (IDS, honeypot)

Evade IDS

Insertion Attack:

- confuse IDS to read invalid packets.
- occurs when NIDS is less strict
- data (IDS) > data (internal network)

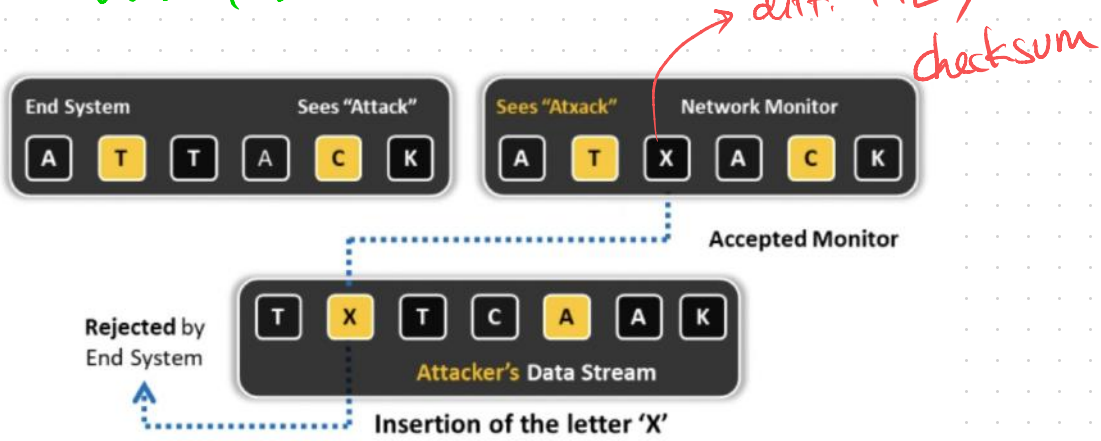


Figure 12.34: Evading IDS using Insertion attack

Evasion

- system accepts packet that IDS rejects
- one byte rejected by IDS.

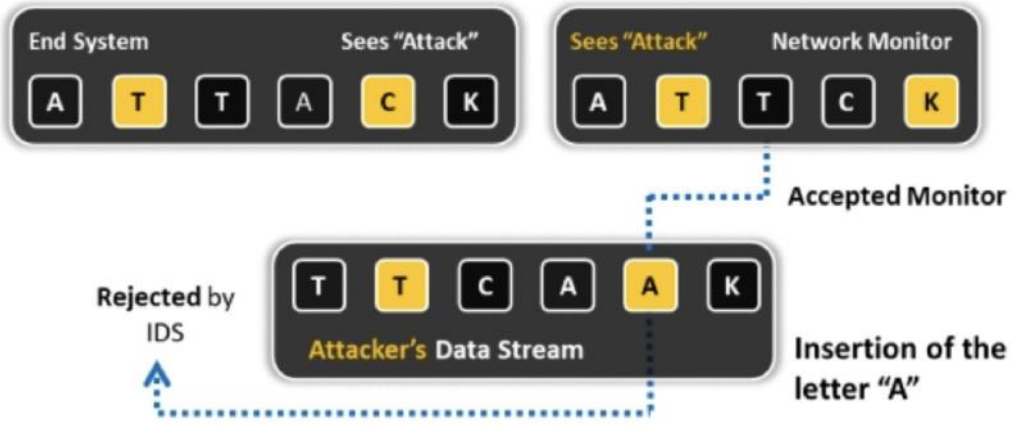


Figure 12.35: Illustration of Evasion technique

- DoS Attack (slow down IDS)
- obfuscating
- False positive Generation
  - confuse attack + False positive requests
- Session splicing (split, delay, stop, reassemble)
- Unicode Evasion technique.
  - convert strings → unicode

- Fragmentation Attack.

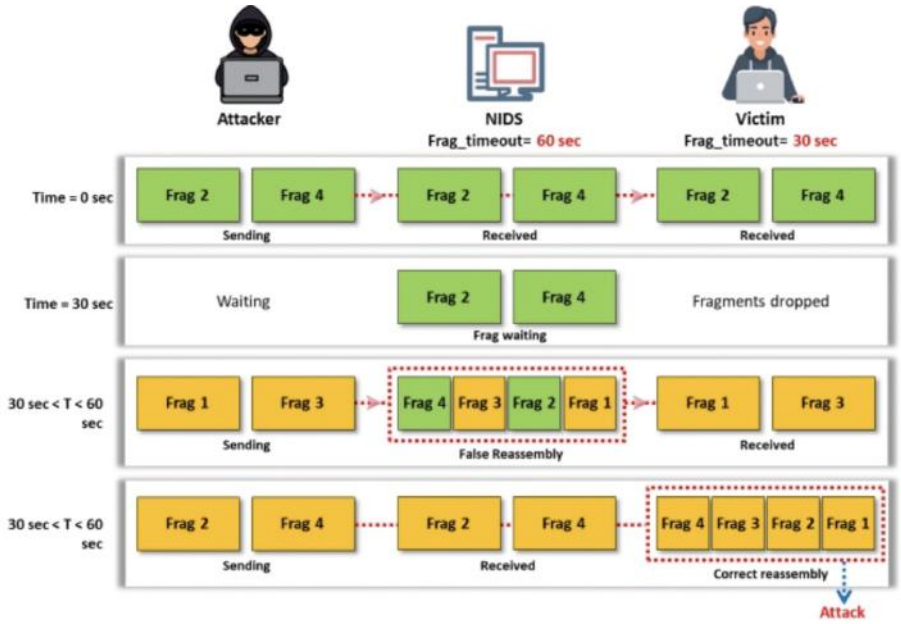


Figure 12.37: Fragmentation attack scenario-2

- Overlapping Fragments (original, received fragments)

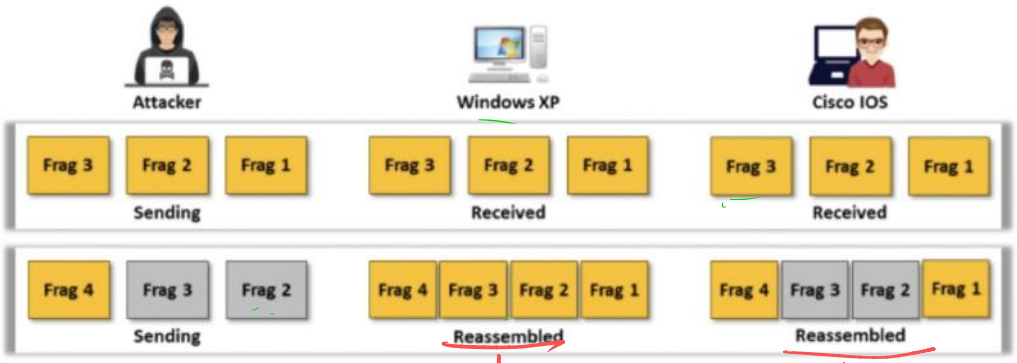


Figure 12.38: Evading IDS using Overlapping Fragments

original

recent

Time to Live attacks

TTL = ?

TTL

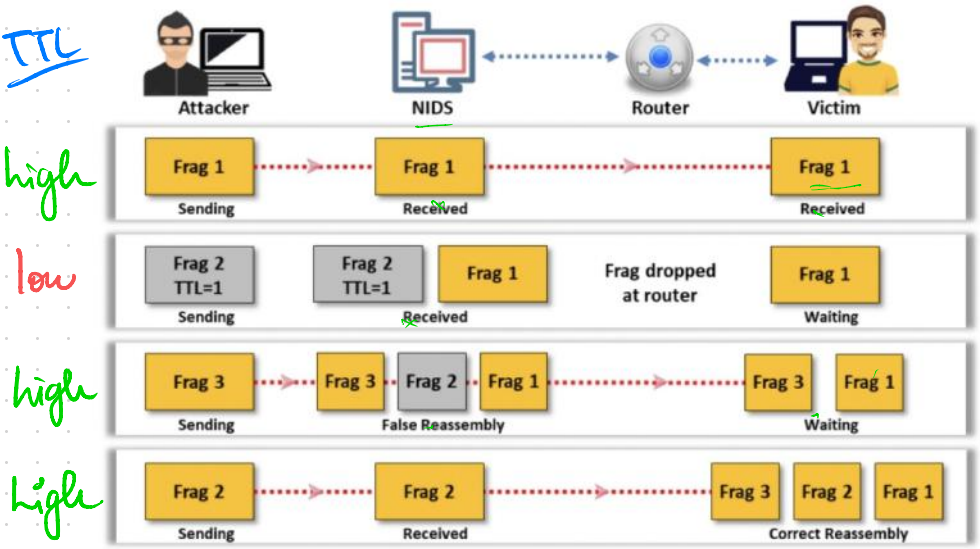


Figure 12.39: Evading IDS using Time-To-Live attack

Invalid RST Packets

- TCP uses 16 bit checksum
- attack sends invalid RST Packet, checksum
- IDS thinks session ended, stops processing

Urgency Flag

- Many IDS do not consider URG

Polymorphic shellcode

- identifies commonly used strings → IDS
- Polymorphic → difficult to detect signature.
- encodes a payload, decoder → decode it

ASCII shellcode

- bypass IDS signature with ASCII standard.
- but limited to certain assembly instructions.

Application layer attack

- media files (audio, video, image)
- IDS → cannot verify signature.
- various integer value (integer overflow)

Desynchronisation

Pre Connection SYN

- invalid TCP checksum (before conn.)
- Sends Fake SYN with invalid seq.
- Stops IDS from Monitoring traffic

Post-Connection SYN

- desynchronise IDS from actual seq. no.
- resynchronise IDS with Post Conn. SYN with new SYN
- ignores legitimate stream.
- attacker send RST → new sequence.

Encryption, Flooding.

Evading Firewalls

Firewalking

- uses TTL values to determine ACL filters
- maps networks by analysing IP responses.
- Firewall → One hop greater

- Banner Grabbing
- IP Spoofing
- Source routing.

Tiny Fragments

- succeeds, if filtering only first segment
- avoids user defined filtering rules.
- when firewall checks only for TCP header

- Bypass blocked sites using IP address.
- Bypass blocked sites using anonymisers.

- Bypass using Proxy Server.

- ICMP tunneling
  - tunnelling backdoor shell.
  - payload not examined by firewall
  - Loki ICMP tunneling.

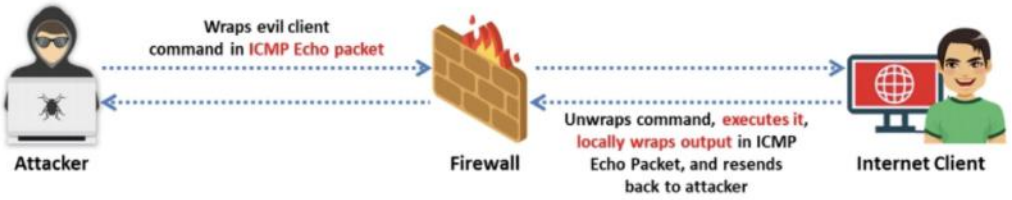
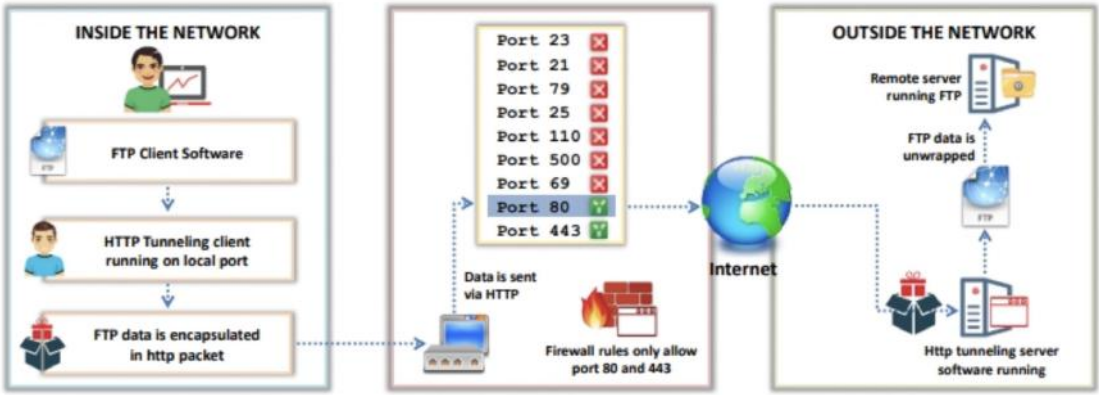


Figure 12.44: Bypassing firewall through ICMP tunneling

- Ack Tunnelling
  - tunnelling backdoor application with tcp packets u Ack bit set.
  - Ackcmd → Implement Ack tunneling
  - Ack bit set not examined by firewall

- HTTP Tunnelling

  - Perform Internet tasks



  - HTTPort, HTTHost, Super Network Tunnel

- SSH Tunneling

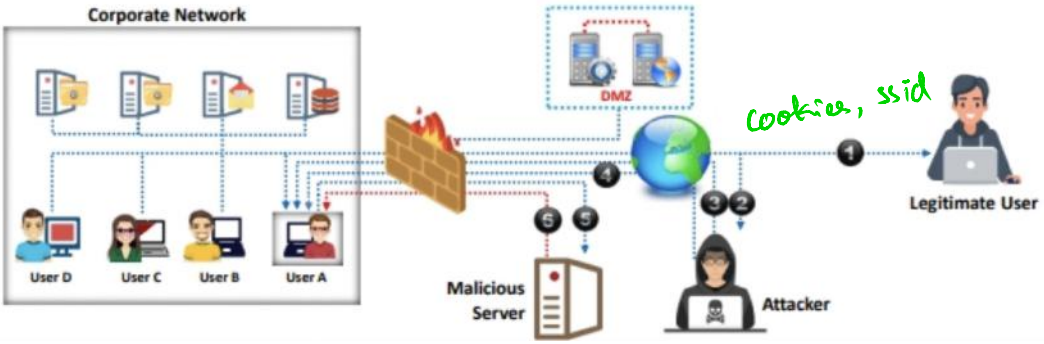
  OpenSSH → encrypt, tunnel all traffic

  Bitvise, Secure Pipes (Tools)

- DNS Tunneling

  - Secretly embed data & exfiltrate using DNS. even DNSSEC can't detect abnormality

- Bypass firewalls - external systems



MITM attacks

Bypass through content

Bypass WAF using XSS

- Malicious HTML Code - bypass WAF

```
<script>alert("XSS")</script>
```

Using ASCII values to bypass the WAF

- After replacing the XSS payload with its equivalent ASCII values

```
<script>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)</script>
```

Using Hex Encoding to bypass the WAF

- After encoding the XSS payload,

```
%3C%73%63%69%72%70%74%3E%61%6C%65%72%74%28%22%58%53%53%22%29%3C%2F%73%63%72%69%70%74%3E
```

Using Obfuscation to bypass the WAF

- After encoding the XSS payload,

```
<sCRiPt>aLeRT("XSS")</sCriPT>
```

IDS / Firewall evading Tools

- Traffic IQ Professional (custom attack traffic)
- Colasoft Packet Builder (custom malicious packets)

Detecting Honey Pots

- Probe services running on system
- craft malicious probe packets (HTTPS, SMTPS, IMAPS)
- Showing service, but deny 3-way handshake.

Tools: Send Safe Honey pot Hunter, kippo-detect

- observe latency of response (Layer 7)
- Analyse TCP window size, when 0 (Layer 4)
- look responses with unique MAC (Layer 3) like a blackhole. 0:0:f:ff:ff:ff

- observe IEEE standards of MAC (VmWare)
- Perform time based TCP fingerprinting (Honeyd)
- analyse files /proc/mounts
  /proc/interrupts (UML honeypot)
  /proc/cmdline
- analyse outgoing packets (Snort_inline)
- AP only send beacon, no traffic
  Monitor network (FAKE AP)
- observe TCP/IP parameters (Bait, Switch)
  [RTT, TTL, TCP timestamp]

Tools:

- Send Safe Honeypot Hunter
  - checks list of HTTPS, SOCKS Proxy.