Firewall, IDS and Honeypot Evasion

TERMINOLOGIES

- Intrusion Detection System (IDS)
  - A system that inspects network activity and detects malicious packets in a network
- Firewall
  - A program or device that secures network resources from being accessed form outside the network
- Honeypot
  - A system that is intentionally made vulnerable to observe hacker behavior

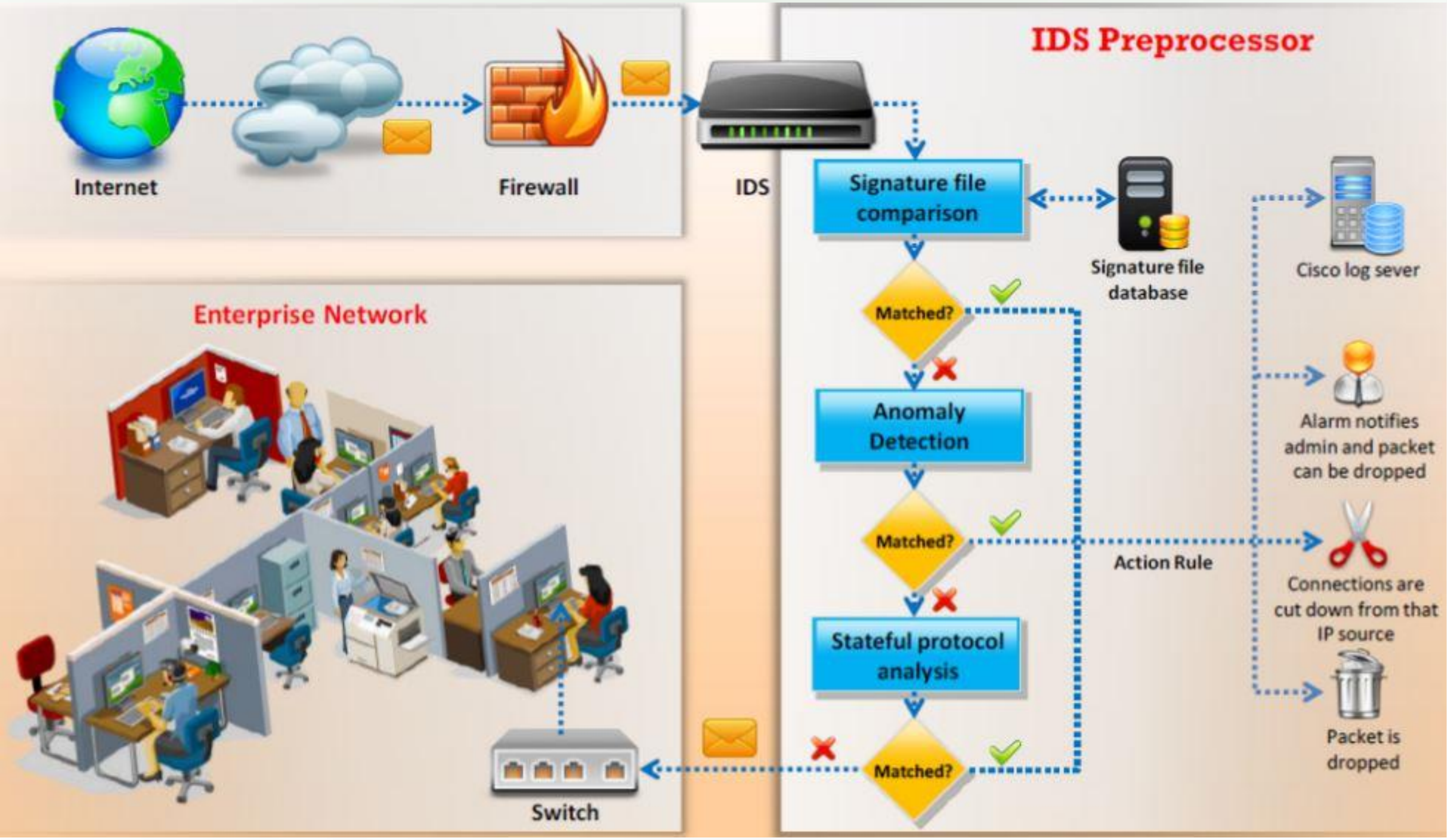
INTRUSION DETECTION SYSTEMS (IDS)

- Inspects information from within a computer or network to identify possible violations of security policies
  - Unauthorized access
  - Misuse
- Sniffs and analyzes packets in a network
- Signals an alarm when suspicious activity is detected
- e.g. Enterasys Dragon, Snort

INTRUSION PREVENTION SYSTEMS (IPS)

- Similar to IDS, with the added capability of blocking the attacks
- e.g. Tipping Point, DefensePro

HOW AN IDS/IPS WORKS



IDS/IPS TERMINOLOGIES

	True	False
Positive	Attack present Alarm raised	No Attack Alarm raised
Negative	No attack No alarm	Attack present No alarm

DETECTION METHOD

- Signature Recognition
  - detects known attacks based on a certain pattern
  - uses pattern/signature matching e.g. specific values in packet content
  - useless if signature database is not updated
  - sub-methods
    - protocol stack verification
    - application protocol verification

DETECTION METHODS

- Anomaly Detection
  - detects attacks based on a certain baseline
  - uses artificial intelligence
  - prone to false positive
  - Potential of detecting “zero-day attacks”

IDS/IPS TYPES

- Network-based
  - Monitors network activity, and typically implemented as a box that sniffs packets while connected to a network
- Host-based
  - Monitors computer system activity (network and system events) and are usually implemented as software installed on the host
- Log File Monitoring
  - Searches through log files of systems and identifies malicious events

SAMPLE INTRUSION INDICATIONS

- System
  - Unfamiliar processes, configuration changes, incomplete logs, incorrect timestamps, unusual logins
- File System
  - Permission changes, unfamiliar or missing files, unexplainable changes in file size
- Network
  - Connections from unusual locations, repeated service probes, repeated log in attempts

POST-DETECTION PROCEDURE

- configure firewall to filter out the IP address of the intruder
- alert administrator
- log the event
  - Save attack info
  - Save tracefile of raw packets
- terminate the TCP session

EVADING IDS

- changing the attack script such that its signature is changed
- Foils pattern-matching detection methods

METHODS USED

- Insertion
- DoS
- False Positive Generation
- Obfuscation
- Fragmentation

INSERTION

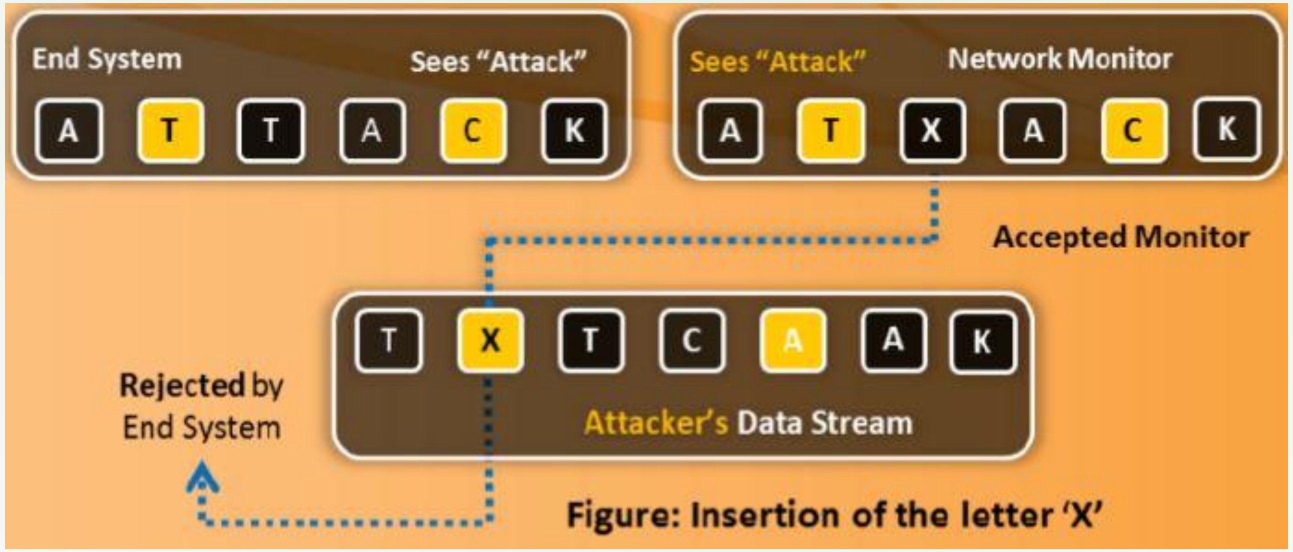


Figure: Insertion of the letter 'X'

- Attacker forces the IDS to read a different data stream by sending packets that will reach the IDS but not the target system
  - TTL that stops at IDS
  - Corrupted checksum for inserted packets

DOS

- Many IDS use a central server for logging
- Attack involves causing a denial of service on the IDS central server
    - Fill up disk space so that events are not logged
    - Cause too many alarms / too much network traffic that IDS cannot keep up
    - Cause the server to lock up

FALSE POSITIVE GENERATION

- Intentionally create a large number of malicious packets to generate multiple alerts

- Used to hide real attack traffic

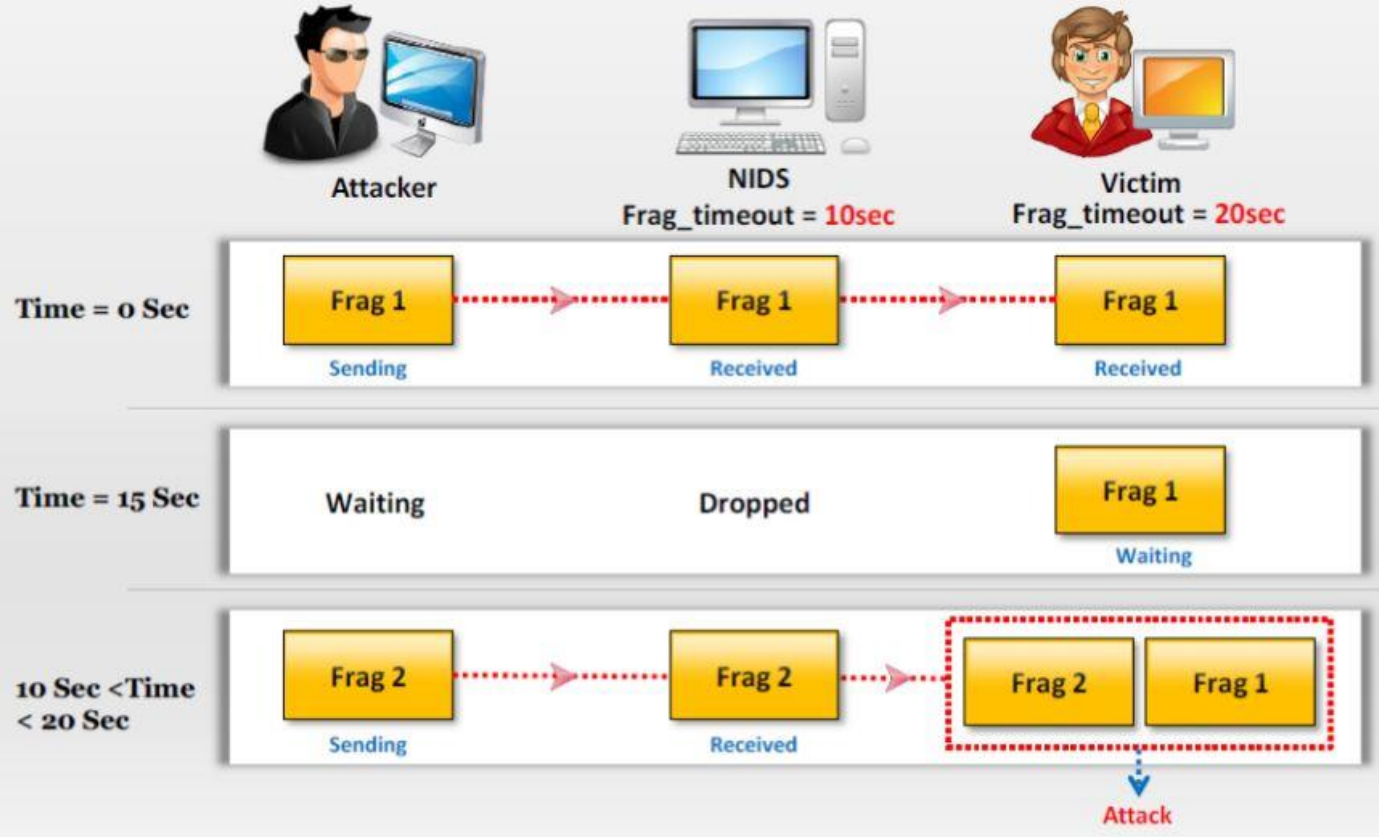
- Attacker can bypass the IDS unnoticed because of difficulty to differentiate the real attack from false positives

OBFUSCATION

- Refers to making code harder to read or understand for security purposes
- Methods to evade IDS pattern matching
  - Encrypting attack code
  - Using a different character encoding
  - Using polymorphic code

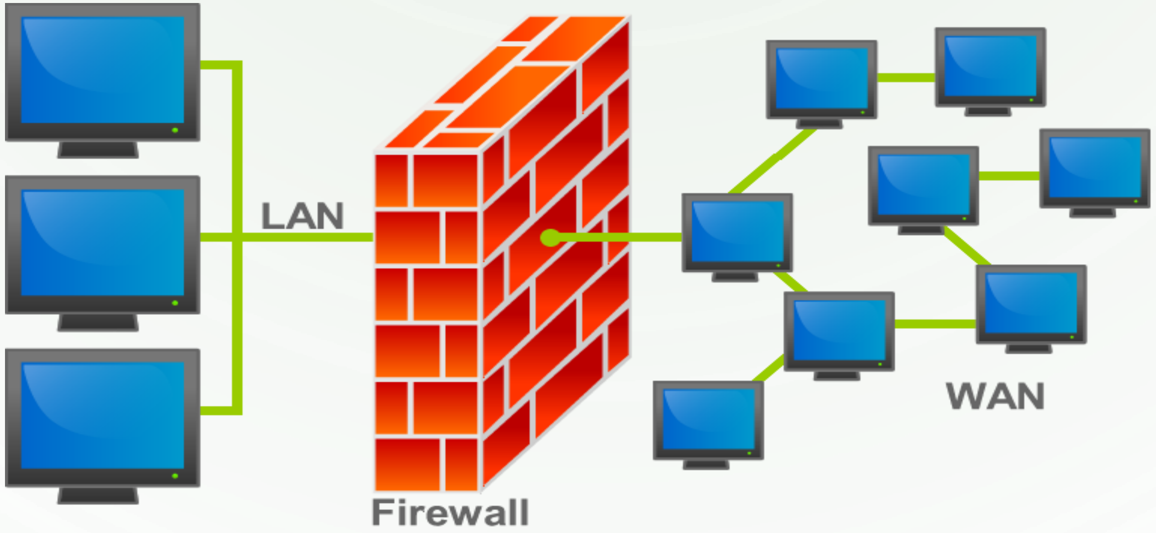
FRAGMENTATION

- Relies on an IDS reassembly timeout that is different from the victim timeout



FIREWALLS

- Protects network resources from access outside the network
- Normally positioned at junctions between 2 networks



FIREWALL FUNCTIONS

- Monitor traffic routed between the junction
- Routes packets
- Filters inbound and outbound traffic for those that do not meet security criteria
- Manage public access to private resources (e.g. servers)
- Logs attempts to enter the protected network

FIREWALL LIMITATIONS

- Cannot guard against traffic that is not routed through its path
- Does not guard against employee misconduct
- Cannot detect if the protected network /host has already been hacked

FIREWALL TYPES

Packet Filters

Circuit Level Gateways

Application level Gateways

Stateful Multilayer Inspection Firewall

PACKET FILTERS

- Usually part of a router (layer 3 filter)
- Packets are compared against certain criteria before forwarding
- Address Filtering
  - Based on source and destination addresses and ports
- Network Filtering
  - Monitors protocols
  - Packet attributes
- Low overhead

CIRCUIT LEVEL GATEWAY

- Work at the session layer
- Monitor TCP handshakes to determine if a requested session is legitimate
- Do not monitor individual packets once the connection is established
- Inexpensive
- Makes requests appear as if they originate from the gateway

APPLICATION-LEVEL GATEWAY

- Filter packets at the application layer (proxy)
- Inbound/Outbound packets cannot access services that have no proxy
- Are able to recognize application-specific commands contained in the packet payloads (deep packet inspection)
- Effective but higher impact on performance

MULTILAYER INSPECTION FIREWALL

- Combine characteristics of different firewall types
- Filter packets at the network layer to determine if session packets are legitimate, and also inspect the application layer packet data
- Expensive and require administrative competence

BREACHING FIREWALLS

- Most firewalls allow access to selected protocols - usually port 80
- Penetration usually involves disguising traffic to look like a permitted protocol

Port Redirection

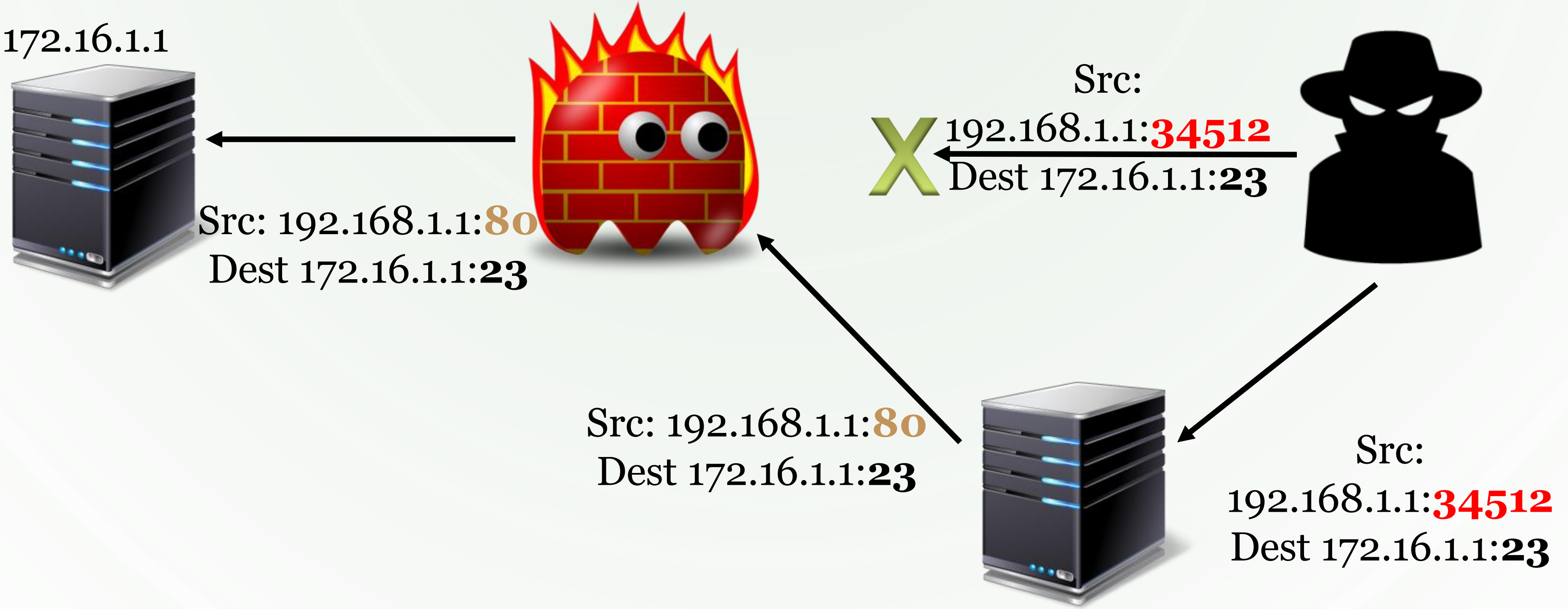
Tunneling

Reverse Shells

PORT REDIRECTION

- Effective against firewalls that do not perform stateful packet inspection.
- Uses a server that accepts connections from a client and replaces the source port in the packets sent by the client with one that a firewall permits.
- The packet is then redirected to the intended recipient behind the firewall.

PORT REDIRECTION



Allows inbound traffic from HTTP servers only

172.16.1.1

Src: 192.168.1.1:80
Dest 172.16.1.1:**23**

Src:
192.168.1.1:**34512**
Dest 172.16.1.1:**23**

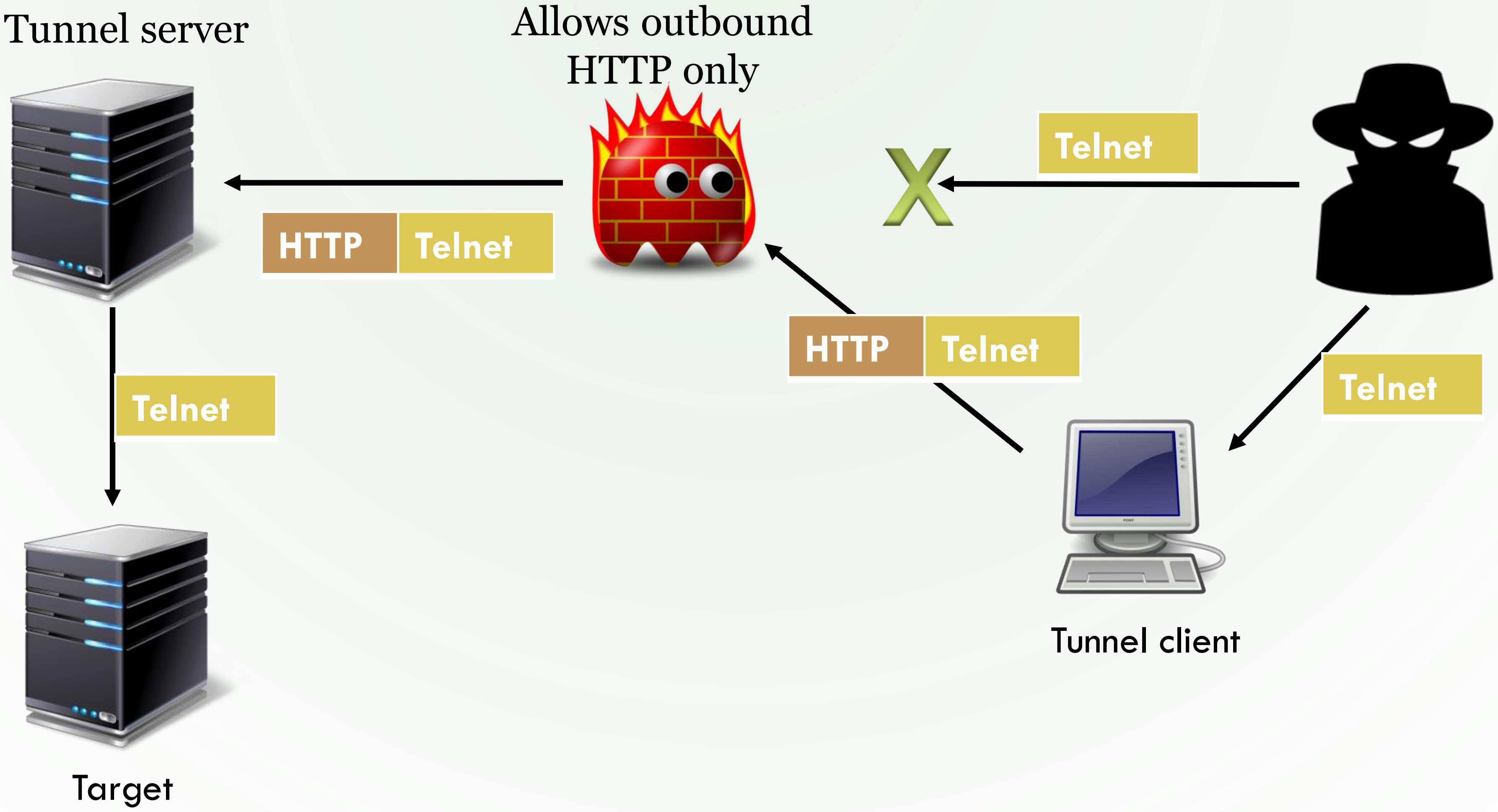
Src: 192.168.1.1:80
Dest 172.16.1.1:**23**

Src:
192.168.1.1:**34512**
Dest 172.16.1.1:**23**

TUNNELING

- Create data paths by encapsulating the data of a blocked protocol within a packet that meets the firewall's allowed criteria
- Composed of a client and a server on opposite sides of a firewall
  - Client – takes care of wrapping the data and sending it through the firewall
  - Server – takes care of unwrapping the data and relaying it to the real destination

TUNNELING


Tunnel server
Allows outbound HTTP only
Telnet
X
HTTP
Telnet
HTTP
Telnet
Telnet
Telnet
Tunnel client
Target

REVERSE SHELLS

- Used against firewalls that do not allow any inbound connections that are not initiated by an inside host
- Hacker tricks victim into downloading malware (usually Trojans)
- Malware runs on victim and initiates the connection from victim to hacker

HONEYPOT

- An information system which is intentionally set up for illicit use
- No production value therefore any attempts to contact it are obviously attacks
- used to observer hacker’s behavior like keystrokes to certain ports.
- Detects or deflects attacks
- Honeynet – two or more honeypots on a network

HONEYPOT TYPES

- Low interaction honeypot
  - Emulate services and OS that cannot be exploited to get complete access to the honeypot.
  - Ex. Honeyd, Specter
- High interaction honeypot
  - Can be compromised completely
  - Use real operating systems and services
  - Tuned to capture hostile activity
  - Ex. honeynets

PHYSICAL AND VIRTUAL HONEYPOTS

- Physical
  - Real machine with its own IP address
  - Often high interaction
- Virtual
  - Simulated by another machine that responds to traffic sent to the virtual honeypot
  - Used for large address spaces

ADVANTAGES AND DISADVANTAGES OF HONEYPOTS

- Advantages
  - small data set of high value
  - catches new attacks
  - cost effective
  - Requires minimal resources
- Disadvantages
  - Limited field of view
  - Risk (high-interaction)