Cryptography and System Security (CSS)

Course Code: CSC 604

Subject Incharge

Ankita Karia
Assistant Professor
Room No. 421
email: ankitakaria@sfit.ac.in

Module 5: Network Security and Applications

5.1

- Network Security Basics
- TCP/IP Vulnerabilities
- Packet Sniffing
- ARP Spoofing, DNS Spoofing
- Port Scanning, TCP Syn flood

5.2

- Denial of Service (DOS)
- Classic DOS attcks
- Source Address Spoofing
- ICMP Flood, SYN flood, UDP flood
- Distributed DOS, Defences against DOS Attacks

5.3

- Internet Security Protocols: SSL, IPSEC
- Secure Email: PGP, Firewalls
- IDS and Its types
- Honey pots

Network Security Basics

1. A **network is** defined as two or more computing devices connected together for sharing resources efficiently.
2. Further, connecting two or more networks together is known as internetworking. Thus, the Internet is just an internetwork – a collection of interconnected networks.
3. **Network security** is the process of taking preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure.

For setting up its internal network, an organization has various options. It can use a wired network or a wireless network to connect all workstations. Nowadays, organizations are mostly using a combination of both **wired and wireless networks**.

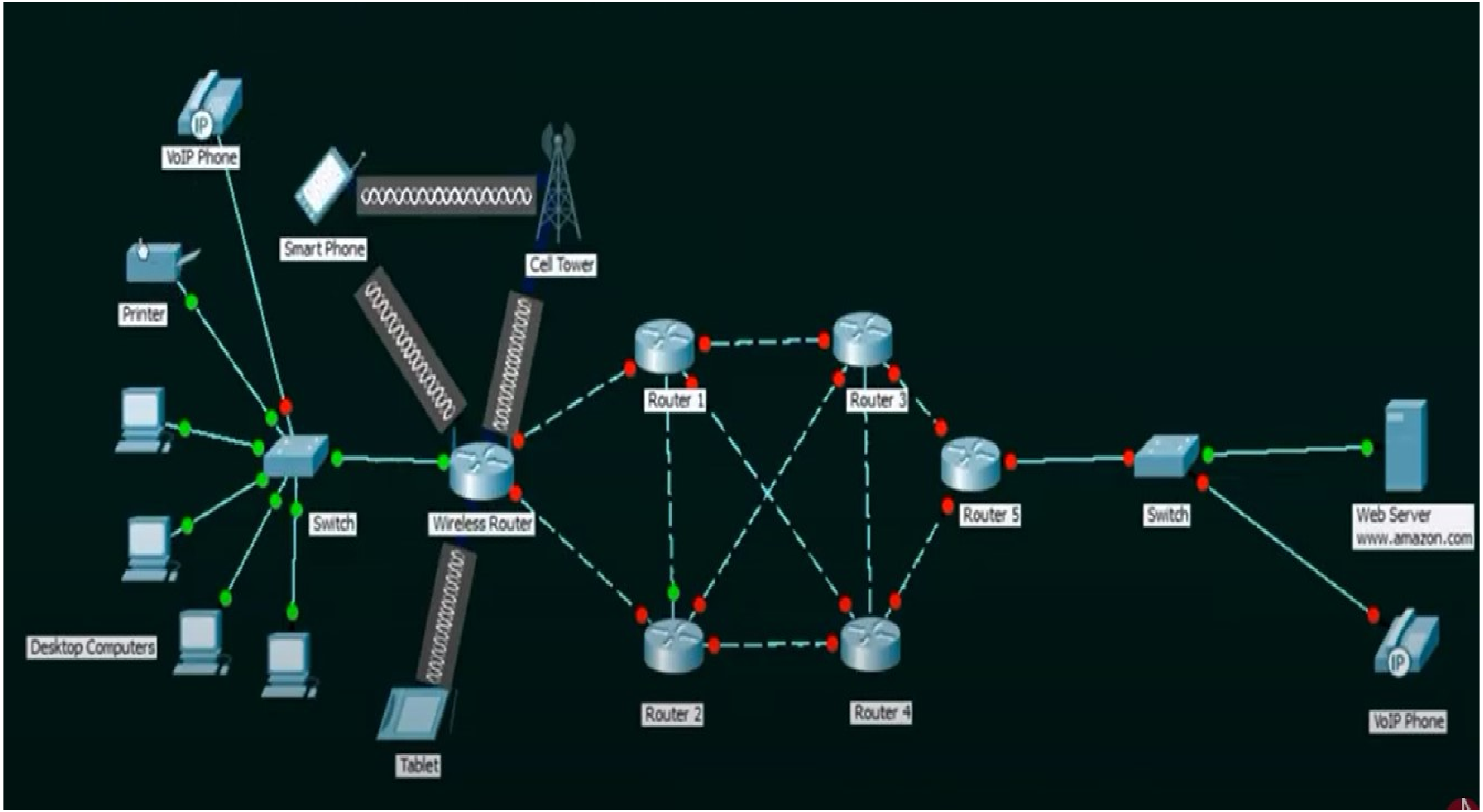
Components of Computer Network

1. **Nodes:** A network node is a connection point that can receive, create, store or send data along distributed network routes
   - **End Nodes:** Starting point or End Point in the communication

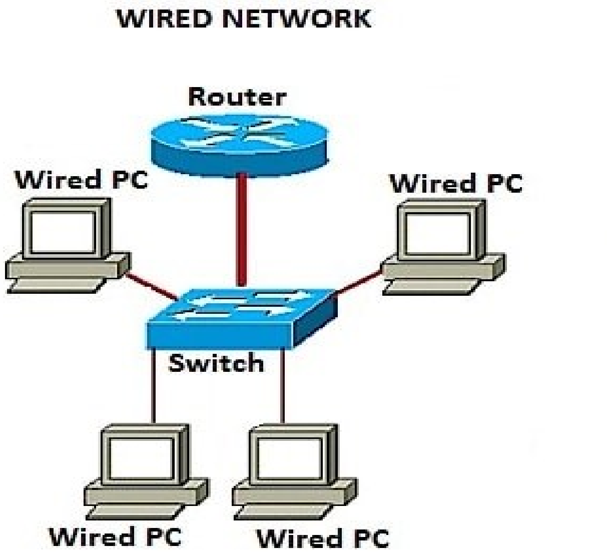
     Example: Computer, Network Printers, VoIP Phones, Security Cameras, Mobile Handheld Devices
   - **Intermediary Nodes:** Forwards data from one node to another. They are in between end nodes. Example: Switches, Router, Bridges, Hubs, Repeater, Cell Tower, Wireless Access Point etc.

2. **Media:** Wired or Wireless Medium
3. **Services:** E-mail, Storage Services, File Sharing, Online Game, Video Conferencing, Instant Messaging

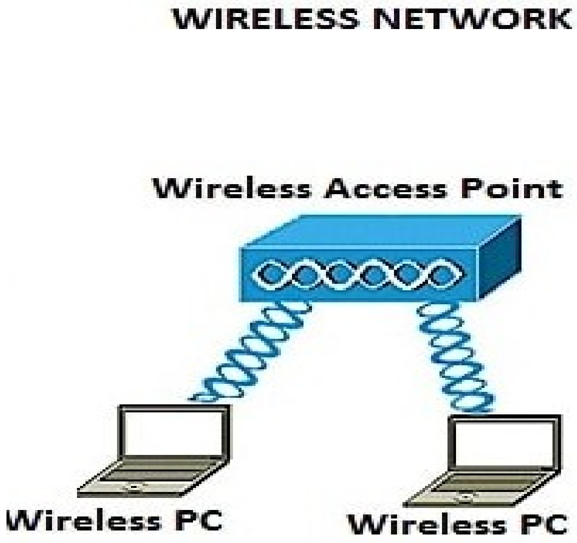
Components of Computer Network



Network Security Basics: Wired and Wireless Network.



- A wired setup uses physical cables to transfer data between different devices and computer systems.
- Wired network is used to carry different forms of electrical signals from one end to the other.
- Most wired networks use Ethernet cables to transfer data between connected PCs.



- Wireless network refers to the use of infrared or radio frequency signals to share information and resources between devices.
- Wireless technologies are designed to reduce the time and different type of obstacles created by the cabales.

Network Security Basics: Vulnerabilities and Attack

- The common vulnerability that exists in both wired and wireless networks is an “unauthorized access” to a network. An attacker can connect his device to a network through unsecure hub/switch port.
- In this regard, **wireless network are considered less secure than wired network**, because wireless network can be easily accessed without any physical connection.

After accessing, an attacker can exploit this vulnerability to launch attacks such as −

1. **Sniffing** the packet data to steal valuable information.
2. **Denial of service** to legitimate users on a network by flooding the network medium with spurious packets.
3. **Spoofing** physical identities (MAC) of legitimate hosts and then stealing data or further launching a ‘man-in-the-middle’ attack.

Network Security Basics: Network Protocol

- Network Protocol is a set of rules that govern communications between devices connected on a network.
- They include mechanisms for making connections, as well as formatting rules for data packaging for messages sent and received.
- Several computer network protocols have been developed each designed for specific purposes.
- The popular and widely used protocols are TCP/IP with associated higher- and lower-level protocols.

PROTOCOL STACK

- A **Protocol Stack** is a prescribed hierarchy of software layers, starting from the application layer at the top (the source of the data being sent) to the data link layer at the bottom (transmitting the bits on the wire).
- The protocols in a stack determine the interconnectivity rules for a layered network model such as in the OSI or TCP/IP models.

TCP/IP

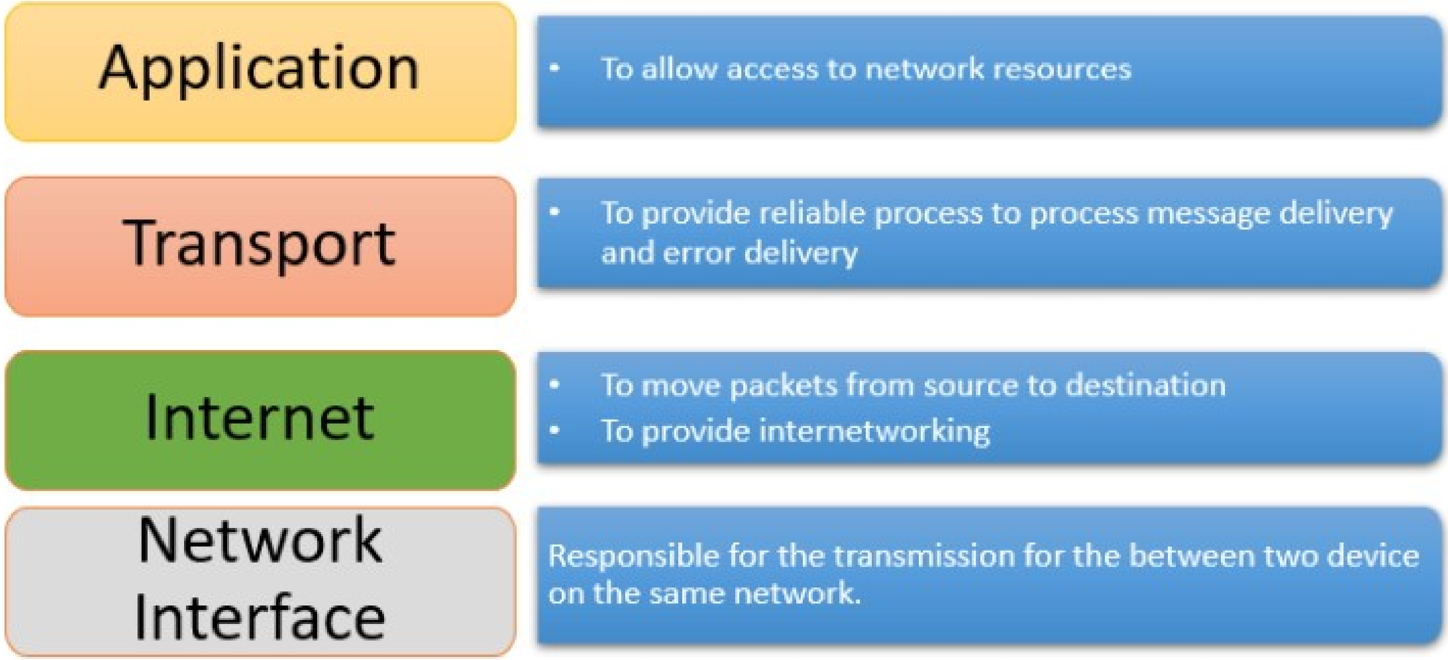
❖ IP stands for the Internet Protocol that deals with routing packets of data from one computer to another or from one router to another.

❖ TCP, which stands for Transmission Control Protocol, has the job of ensuring that the data packets delivered by the IP protocol did arrive at their destination.

TCP protocol sits on top of the IP protocol — in the sense that TCP asks IP to send a packet to its destination and then makes sure that the packet was actually received at the destination

Four Layers of TCP/IP model

1. The functionality of the TCP IP model is divided into four layers, and each includes specific protocols.
2. TCP/IP is a layered server architecture system in which each layer is defined according to a specific function to perform. All these four TCP/IP layers work collaboratively to transmit the data from one layer to another.



Application

- To allow access to network resources

Transport

- To provide reliable process to process message delivery and error delivery

Internet

- To move packets from source to destination
- To provide internetworking

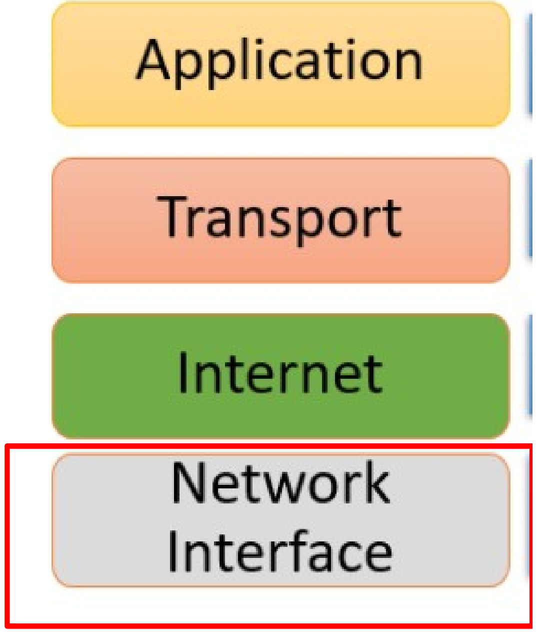
Network Interface

Responsible for the transmission for the between two device on the same network.

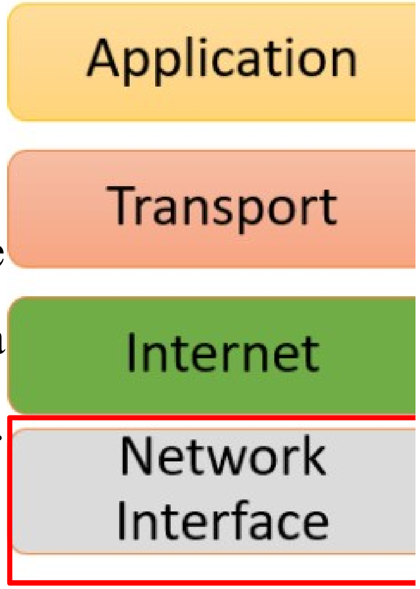
TCPIP Layers and Vulnerabilities

At the Network Interface layer, the packet of information that is placed on the wire is known as a frame. The packet is comprised of three areas: the header, the payload, and the FCS. Because the Network Interface layer is used for communications on a local network, the attacks that occur at this level would be carried out on local networks. Some of the ways the network layer can be exploited to compromise the C-I-A triad include the following:

1. **MAC address spoofing**
2. **Denial of service (DoS)**
3. **ARP cache poisoning**



TCPIP Layers and Vulnerabilities


Application

Transport

Internet

Network Interface

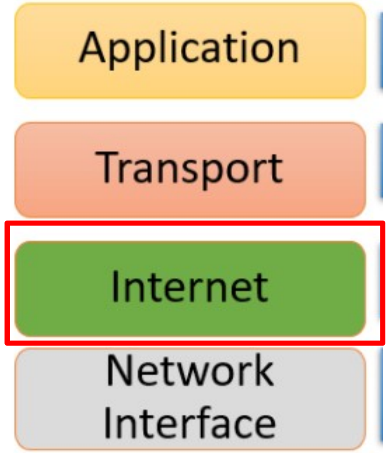
1. **MAC address spoofing:** The header contains the MAC address of the source and destination computers and is required to successfully send a directed message from a source computer to a destination computer. Attackers can easily spoof the MAC address of another computer.
2. **Denial of service (DoS):** A DoS attack overloads a single system so that it cannot provide the service it is configured to provide. An ARP protocol attack could be launched against a computer to overwhelm it, which would make it unavailable to support the C-I-A triad.
3. **ARP cache poisoning:** The ARP cache stores MAC addresses of computers on the local network that have been contacted within a certain amount of time in memory. If incorrect, or spoofed, entries were added to the ARP cache, then the computer is not able to send information to the correct destination.

TCPIP Layers and Vulnerabilities

At the **Internet layer**, IP datagrams are formed. The packet is comprised of two areas: the header and the payload. Some of the ways the Internet layer can be exploited to compromise the C-I-A triad include the following:

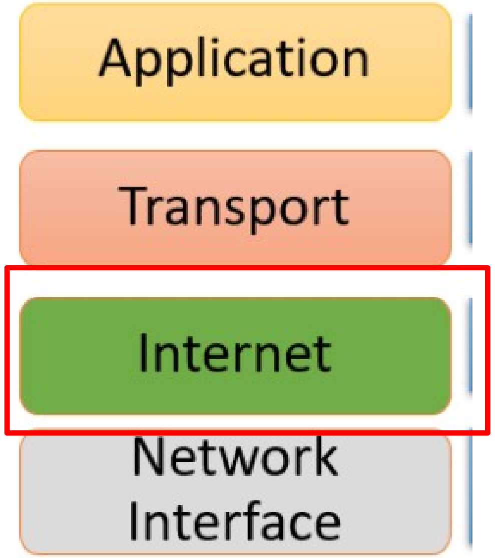
IP address spoofing: If the IP header fields and lengths are known, the IP address in the IP datagram can be easily discovered and spoofed.

Man-in-the-middle attacks: This attack occurs when a hacker places himself or herself between the source and destination computer in such a way that neither notices his or her existence. Meanwhile, the attacker can modify packets or simply view their contents.

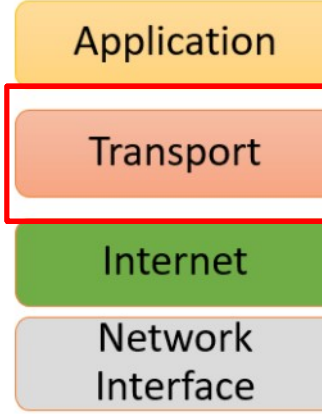


TCPIP Layers and Vulnerabilities

Corrupting packets: Because IP datagrams can pass through several computers between the source and destination, the information in the IP header fields is read and sometimes modified, such as when the information reaches a router. If the packet is intercepted, the information in the header can be modified, corrupting the IP datagram. This could cause the datagram to never reach the destination computer, or it could change the protocols and payload information in the datagram.



TCPIP Layers and Vulnerabilities

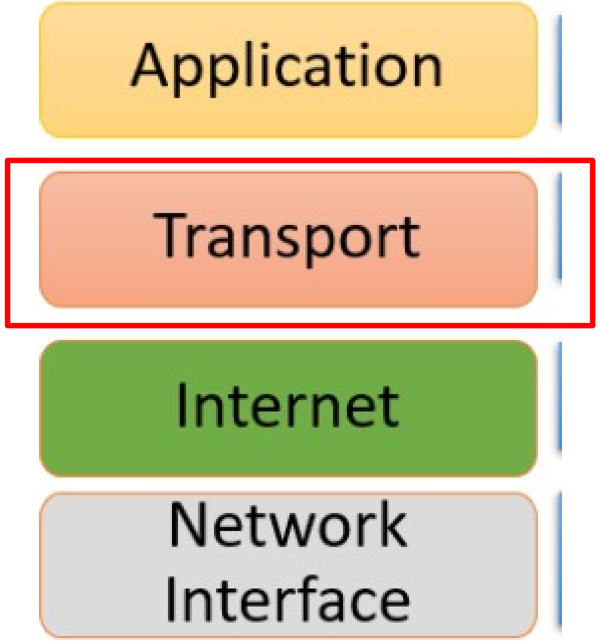


At the Transport layer, either a UDP header is added to the message or a TCP header is added. The application that is requesting the service determines what protocol will be used. Some of the ways the Transport layer can be exploited to compromise the C-I-A triad include the following:

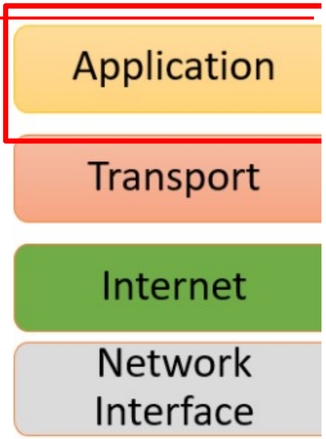
DoS: With a DoS attack at this level, simple IP-level protocols and utilities can be exploited to overload a computer, thus breaking the C-I-A triad. For instance, by knowing the steps involved in a three-way TCP handshake, a hacker or cracker might send the packets in the incorrect order and disrupt the availability of one of your servers. An example of this is a **SYN flood**

TCPIP Layers and Vulnerabilities

Session hijacking: This kind of attack occurs after a source and destination computer have established a communications link. A third computer disables the ability of one the computers to communicate, and then imitates that computer. Because the connection has already been established, the third computer can disrupt your C-I-A triad**.**



TCPIP Layers and Vulnerabilities

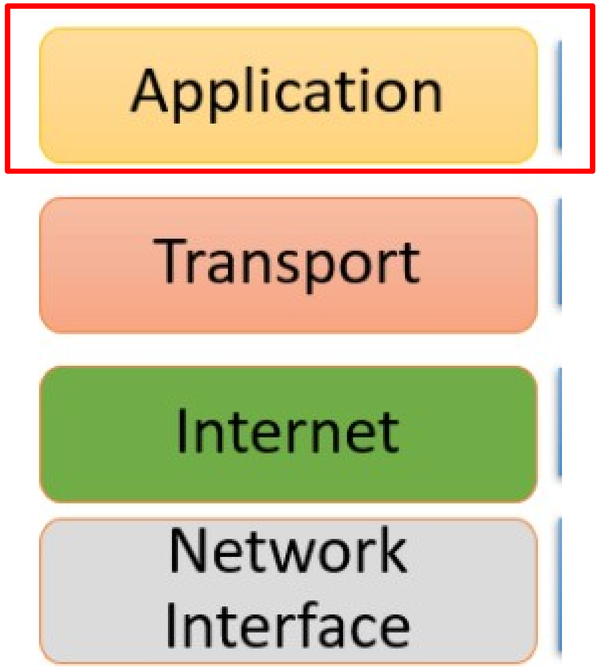


Application layer attacks can be some of the most difficult to protect against because they take advantage of vulnerabilities in applications and lack of end-user knowledge of computer security. Some of the ways the Application layer can be exploited to compromise the C-I-A triad include the following:

E-mail application exploits: Attachments can be added to e-mail messages and delivered to a user's inbox. The user can open the e-mail message and run the application. The attachment might do immediate damage, or might lay dormant and be used later. Similarly, hackers often embed malicious code in Hypertext Markup Language (HTML) formatted messages. Exploits of this nature might take advantage of vulnerability in the client's e-mail application or a lack of user knowledge about e-mail security concerns.

TCPIP Layers and Vulnerabilities

Web browser exploits: When a client computer uses a Web browser to connect to a Web server and download a Web page, the content of the Web page can be active. That is, the content is not just static information, but can be executable code. If the code is malicious, it can be used to disrupt the C-I-A triad.



PACKET SNIFFING

1. When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called **data packets** and reassembled at receiver's node in original format.
2. Data Packets is the smallest unit of communication over a computer network.
3. Data Packet is also called a block, a segment, a datagram or a cell.
4. The act of capturing data packet across the computer network is called **packet sniffing.**
5. It is similar to as wire tapping to a telephone network.

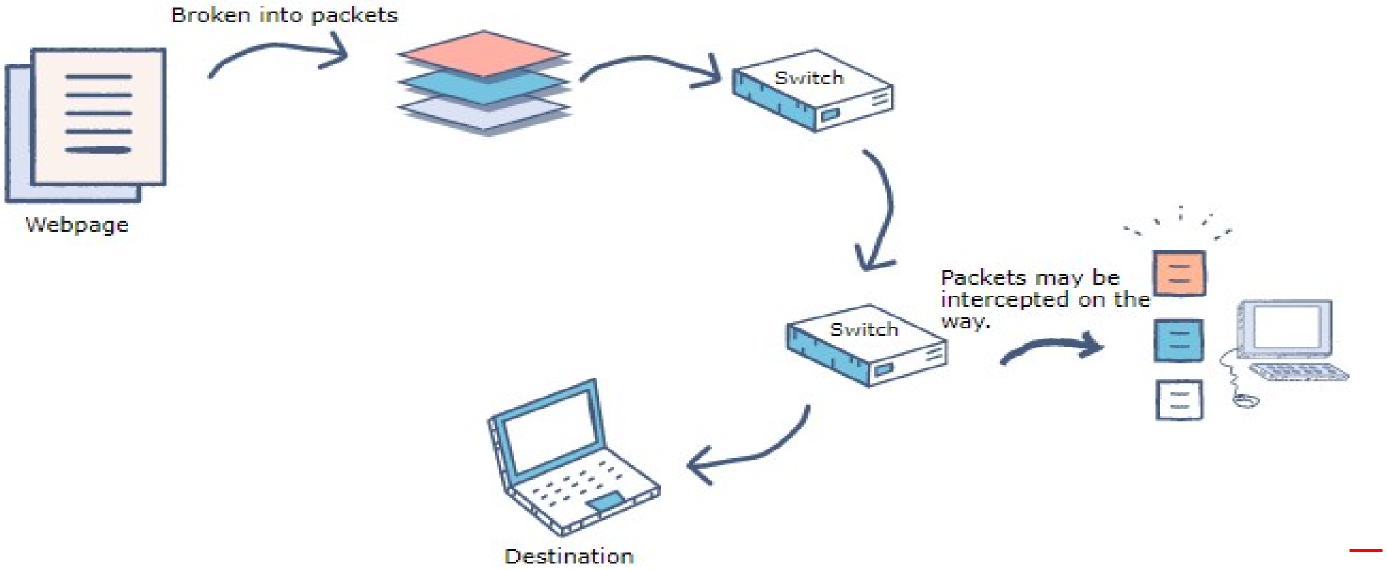
Packet Sniffer

Packet sniffing is done by using tools called *packet sniffer*. It can be either ***filtered or unfiltered*.** Filtered is used when only *specific data packets* have to be captured and Unfiltered is used when *all the packets* have to be captured.

WireShark, SmartSniff are examples of packet sniffing tools.

PACKET SNIFFING – How it Works

1. Web pages and emails are not sent through the internet as one document. Instead they are broken down into many little data packets.
2. These packets are then addressed to an IP address at the receiving end, which has to send back an acknowledgment of each packet it receives.
3. These packets are not transferred from the sender to the receiver through a single direct connection. Instead, as each packet traverses the internet en-route to its destination, it passes through a number of traffic control devices such as routers and switches. Each time a packet passes through one of these traffic control devices, it is susceptible to capture and analysis.



PACKET SNIFFING – Who can sniff packets

1. It is mostly used by crackers and hackers to collect information illegally about network.
2. It is also used by ISPs, advertisers and governments.

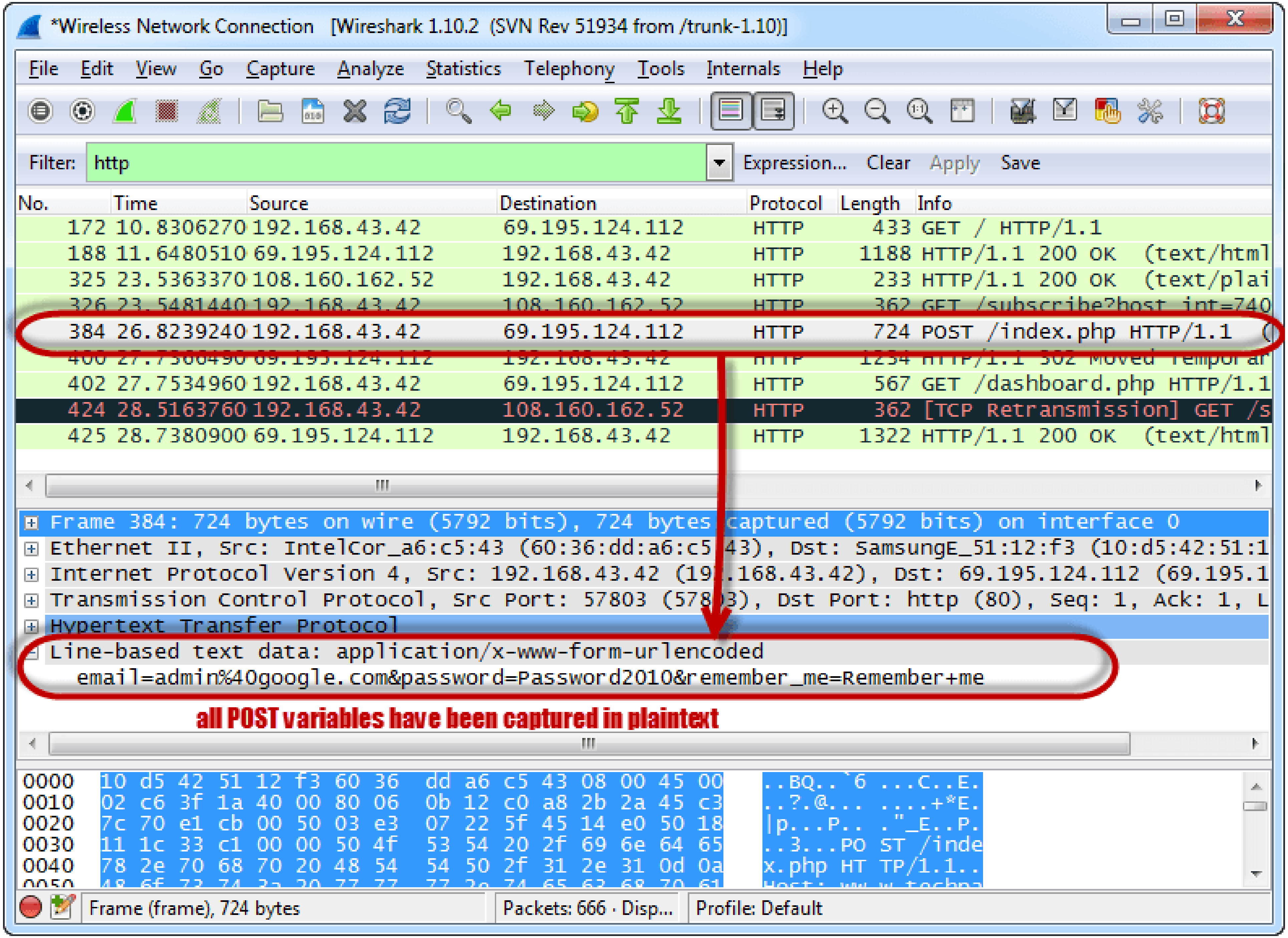
ISPs use packet sniffing to track all your activities such as:

- ✓ who is receiver of your email
- ✓ what is content of that email
- ✓ what you download
- ✓ sites you visit
- ✓ what you looked on that website
- ✓ downloads from a site
- ✓ streaming events like video, audio, etc.

To achieve this target, these agencies use packet sniffing to *inject advertisements* into the flowing packets. Most of the time these ads *contain malware*.

Advertising agencies or internet advertising agencies are paid according to:

- ✓ number of ads shown by them.
- ✓ number of clicks on their ads also called PPC (pay per click).


*Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save

```
No.    Time       Source          Destination     Protocol Length Info
   172 10.8306270 192.168.43.42   69.195.124.112  HTTP     433 GET / HTTP/1.1
   188 11.6480510 69.195.124.112  192.168.43.42   HTTP    1188 HTTP/1.1 200 OK  (text/html
   325 23.5363370 108.160.162.52  192.168.43.42   HTTP     233 HTTP/1.1 200 OK  (text/plai
   326 23.5481440 192.168.43.42   108.160.162.52  HTTP     362 GET /subscribe?host_int=740
   384 26.8239240 192.168.43.42   69.195.124.112  HTTP     724 POST /index.php HTTP/1.1  (
   400 27.7366490 69.195.124.112  192.168.43.42   HTTP    1234 HTTP/1.1 302 Moved Temporar
   402 27.7534960 192.168.43.42   69.195.124.112  HTTP     567 GET /dashboard.php HTTP/1.1
   424 28.5163760 192.168.43.42   108.160.162.52  HTTP     362 [TCP Retransmission] GET /s
   425 28.7380900 69.195.124.112  192.168.43.42   HTTP    1322 HTTP/1.1 200 OK  (text/html
```

```
⊞ Frame 384: 724 bytes on wire (5792 bits), 724 bytes captured (5792 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_a6:c5:43 (60:36:dd:a6:c5:43), Dst: SamsungE_51:12:f3 (10:d5:42:51:1
⊞ Internet Protocol Version 4, Src: 192.168.43.42 (192.168.43.42), Dst: 69.195.124.112 (69.195.1
⊞ Transmission Control Protocol, Src Port: 57803 (57803), Dst Port: http (80), Seq: 1, Ack: 1, L
⊞ Hypertext Transfer Protocol
⊟ Line-based text data: application/x-www-form-urlencoded
    email=admin%40google.com&password=Password2010&remember_me=Remember+me
```

all POST variables have been captured in plaintext

```
0000  10 d5 42 51 12 f3 60 36  dd a6 c5 43 08 00 45 00   ..BQ..`6 ...C..E.
0010  02 c6 3f 1a 40 00 80 06  0b 12 c0 a8 2b 2a 45 c3   ..?.@... ....+*E.
0020  7c 70 e1 cb 00 50 03 e3  07 22 5f 45 14 e0 50 18   |p...P.. ."_E..P.
0030  11 1c 33 c1 00 00 50 4f  53 54 20 2f 69 6e 64 65   ..3...PO ST /inde
0040  78 2e 70 68 70 20 48 54  54 50 2f 31 2e 31 0d 0a   x.php HT TP/1.1..
0050  48 6f 73 74 3a 20 77 77  77 2e 74 65 63 68 70 61   Host: ww w.techpa
```

SPOOFING

- Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity.
- It's one of many tools hackers use to gain access to computers to mine them for sensitive data, turn them into zombies (computers taken over for malicious use), or launch Denial-of-Service (DoS) attacks.

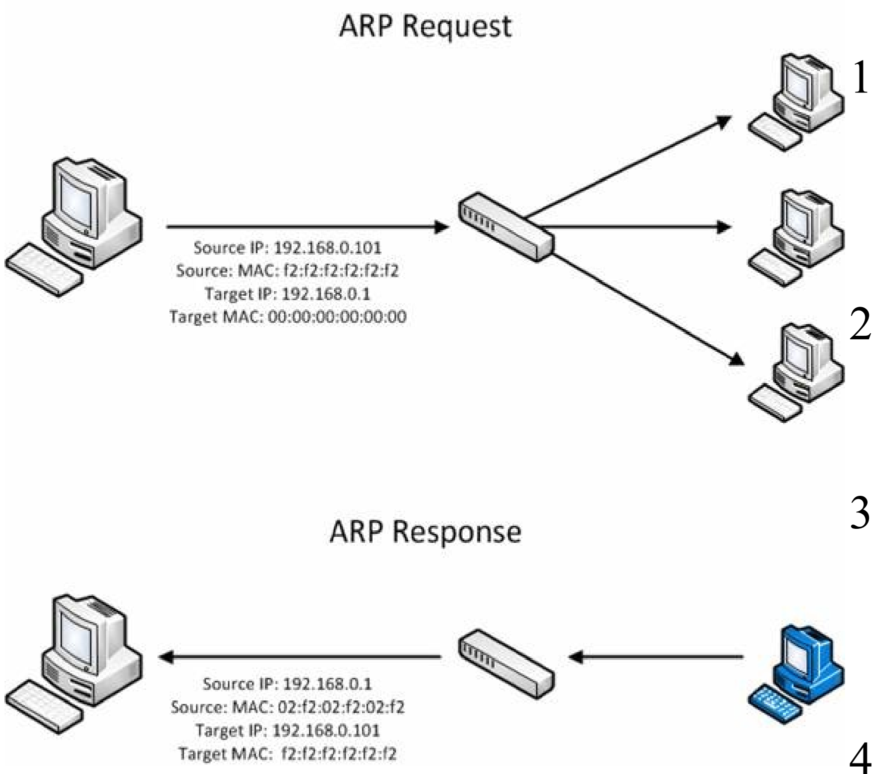
Three types of spoofing attacks exist:

DNS Server Spoofing: Alters a DNS server to point a domain name to a different IP address, usually with the intent of spreading a virus.

ARP Spoofing: Connects hackers to an IP address through a spoofed address resolution protocol (ARP) message, usually to enable denial of service (DoS) and man-in-the-middle attacks.

IP Spoofing: Disguises one IP address to gain access as a trusted system, usually to enable a DDoS attack or redirect communications.

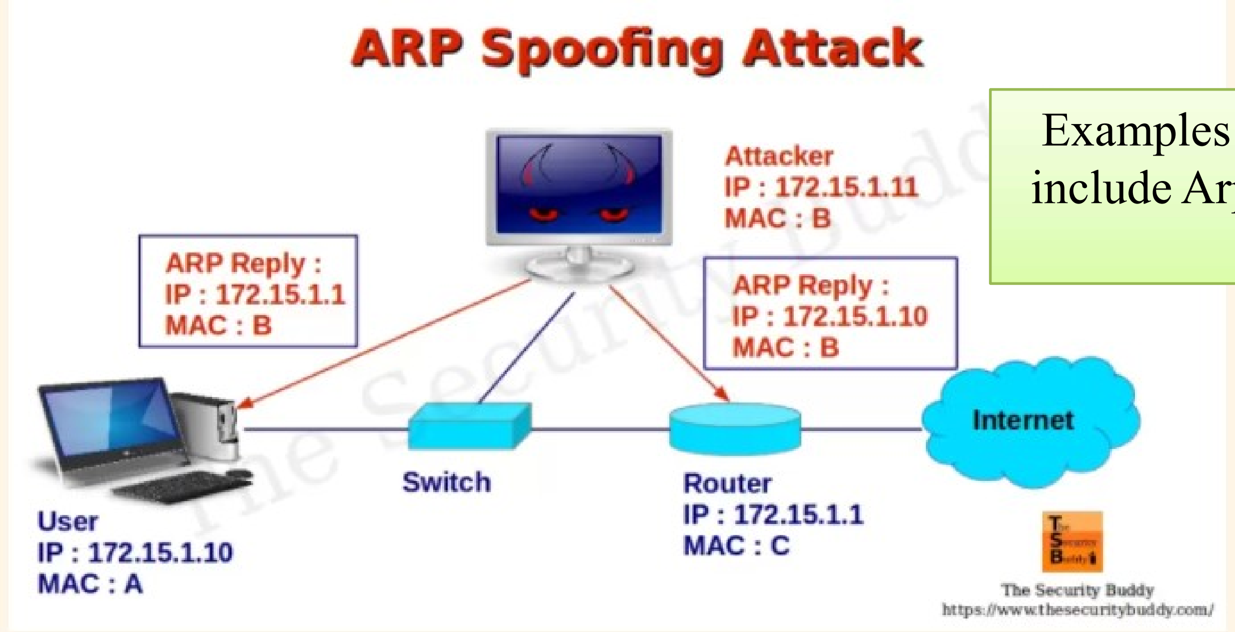
ARP SPOOFING


ARP Request
Source IP: 192.168.0.101
Source: MAC: f2:f2:f2:f2:f2:f2
Target IP: 192.168.0.1
Target MAC: 00:00:00:00:00:00
ARP Response
Source IP: 192.168.0.1
Source: MAC: 02:f2:02:f2:02:f2
Target IP: 192.168.0.101
Target MAC: f2:f2:f2:f2:f2:f2

1. ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network.
2. This results in the linking of an attacker’s MAC address with the IP address of a legitimate computer or server on the network.
3. Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.
4. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

ARP SPOOFING

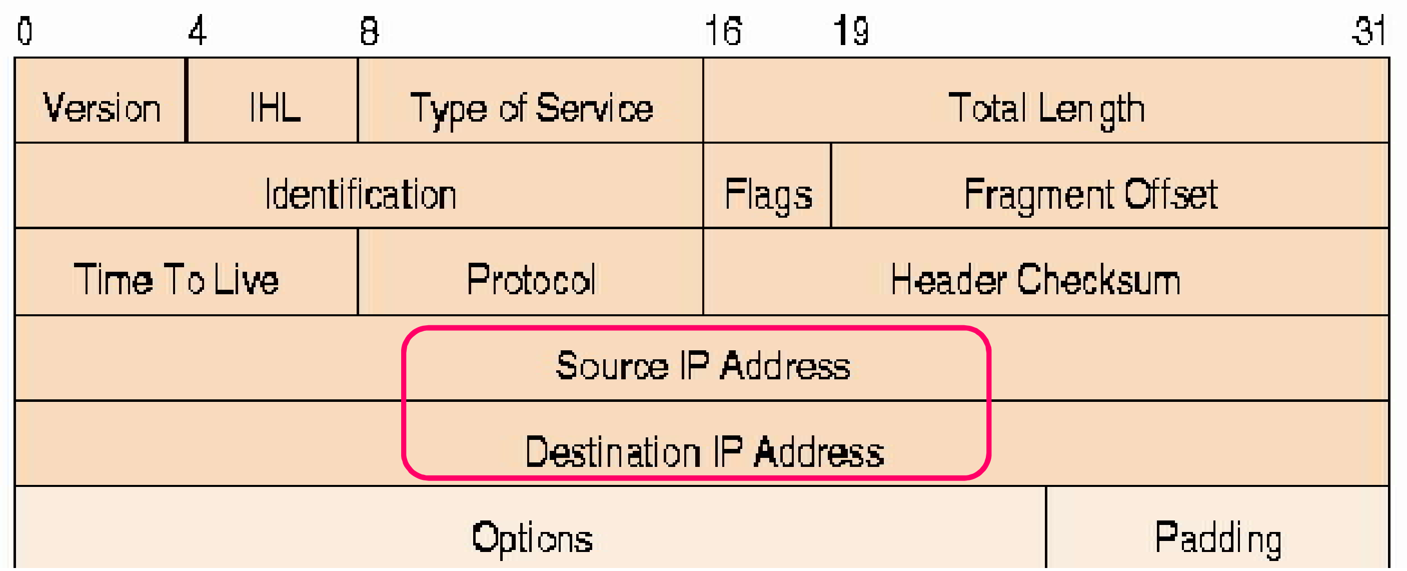
1. An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.
2. It is an attack in which an attacker can send falsified ARP MESSAGES over a local area network and link the victim's IP address with the MAC address of the attacker's device .
3. As a result, all the traffic that is meant for the victim will reach the attacker first.
4. The attacker can afterward steal sensitive information or prepare for more attacks



Examples of popular ARP spoofing software include Arpspoof, Cain & Abel, Arpoison and Ettercap.

IP SPOOFING

1. The data transmitted over the internet is first broken into multiple packets, and those packets are transmitted independently and reassembled at the end.
2. Each packet has an IP (Internet Protocol) header that contains information about the packet, including the source IP address and the destination IP address.



Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it.

IP SPOOFING

1. IP spoofing enables an attacker to replace a packet header's source IP address with a fake, or spoofed IP address.
2. The attacker does this by intercepting an IP packet and modifying it, before sending it on to its destination. This means that the IP address looks like it's from a trusted source – the original IP address – while masking its true source: an unknown third-party.
3. Once a hacker has successfully spoofed an IP address, they can access controlled systems and intercept communications intended for someone else (i.e., the person or device whose IP address they are impersonating).

IP spoofing commonly enables three different types of attacks:

1. DDoS Attacks
2. Botnet Attacks
3. Man in the Middle Attacks

DNS SPOOFING

1. DNS Spoofing is a type of computer attack wherein a user is forced to navigate to a fake website disguised to look like a real one, with the intention of diverting traffic or stealing credentials of the users.
2. DNS spoofing and by extension, DNS cache poisoning are among the more deceptive cyberthreats

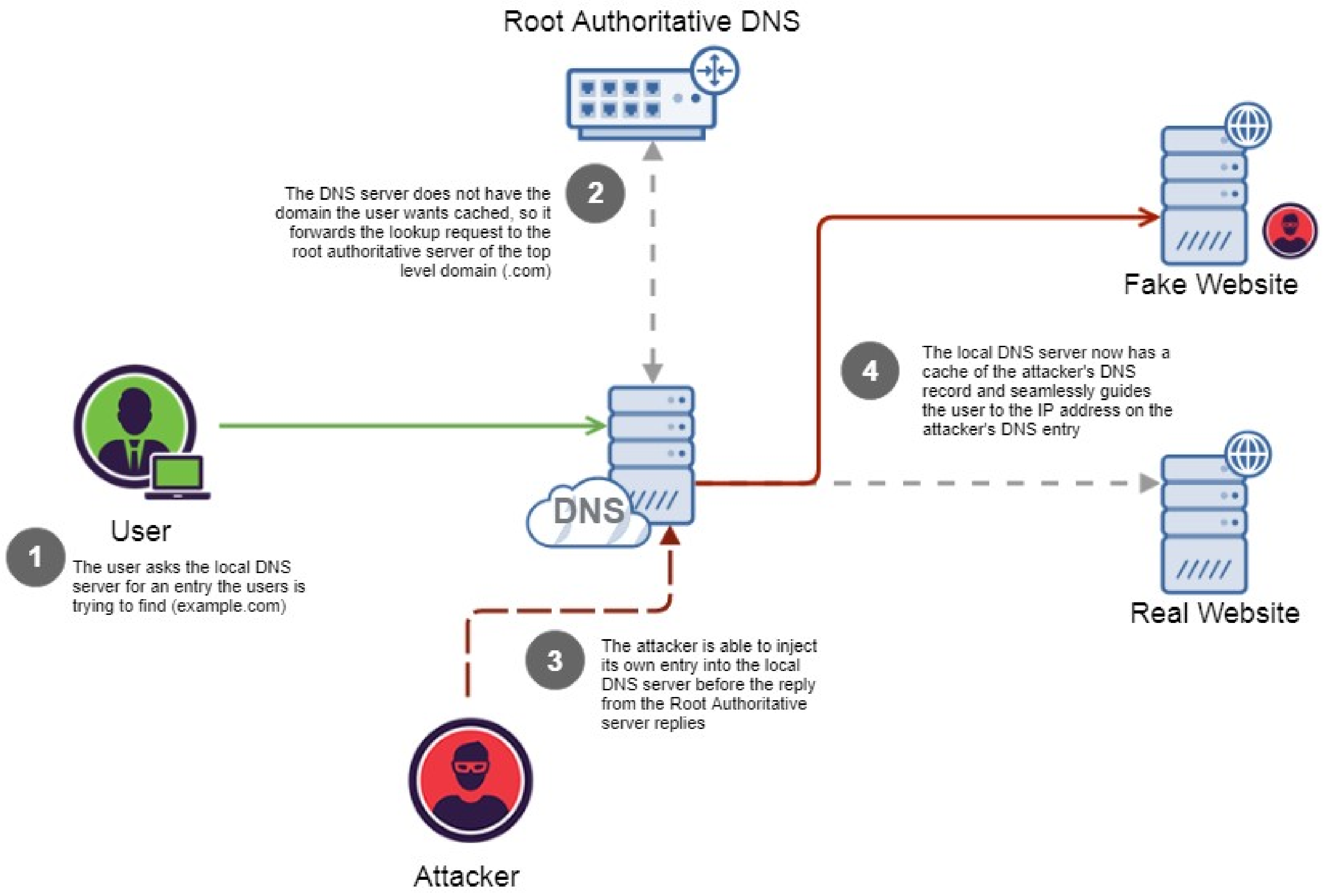
DNS Concept

1. DNS stands for “Domain Name System.”
2. The Domain Name System (DNS) is the phonebook of the Internet.
3. Humans access information online through domain names, like economictimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses.
4. DNS translates domain names to IP addresses so browsers can load Internet resources.

DNS Resolver

A DNS resolver, also called a **recursive resolver**, is a server designed to receive DNS queries from web browsers and other applications. The resolver receives a hostname - for example, www.example.com - and is responsible for tracking down the IP address for that hostname.

DNS SPOOFING



The DNS server does not have the domain the user wants cached, so it forwards the lookup request to the root authoritative server of the top level domain (.com)

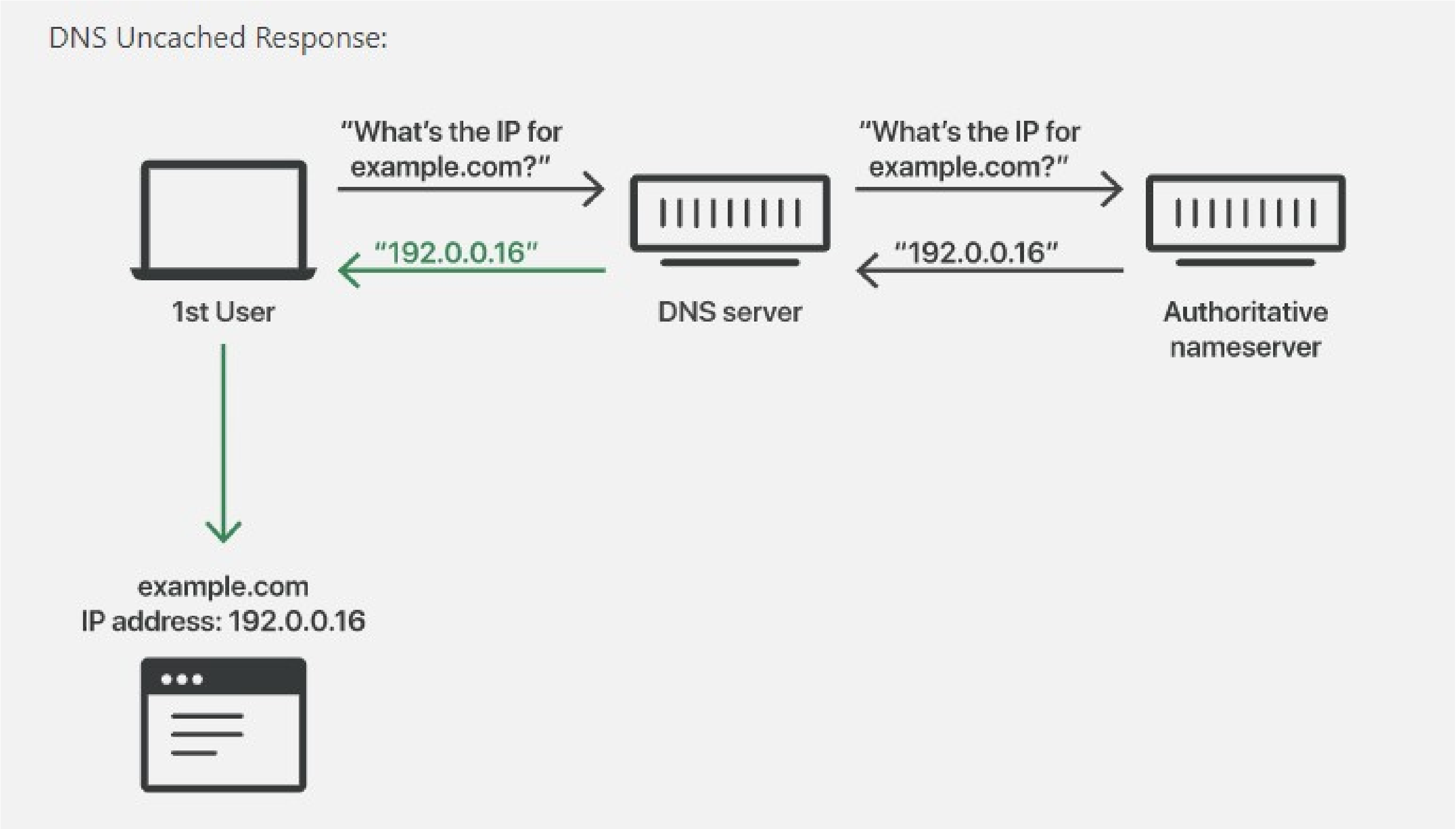
The local DNS server now has a cache of the attacker's DNS record and seamlessly guides the user to the IP address on the attacker's DNS entry

The user asks the local DNS server for an entry the users is trying to find (example.com)

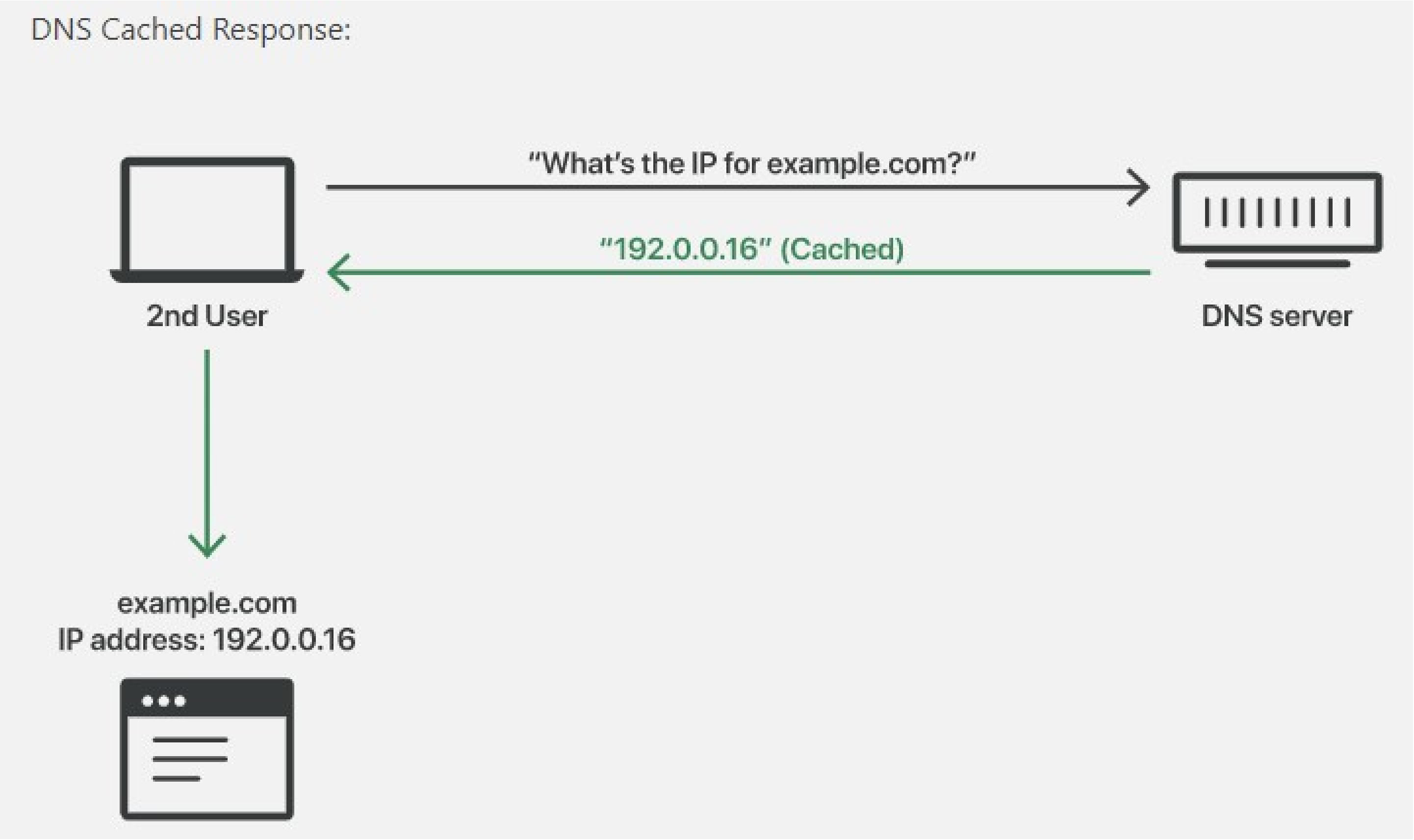
The attacker is able to inject its own entry into the local DNS server before the reply from the Root Authoritative server replies

DNS SPOOFING

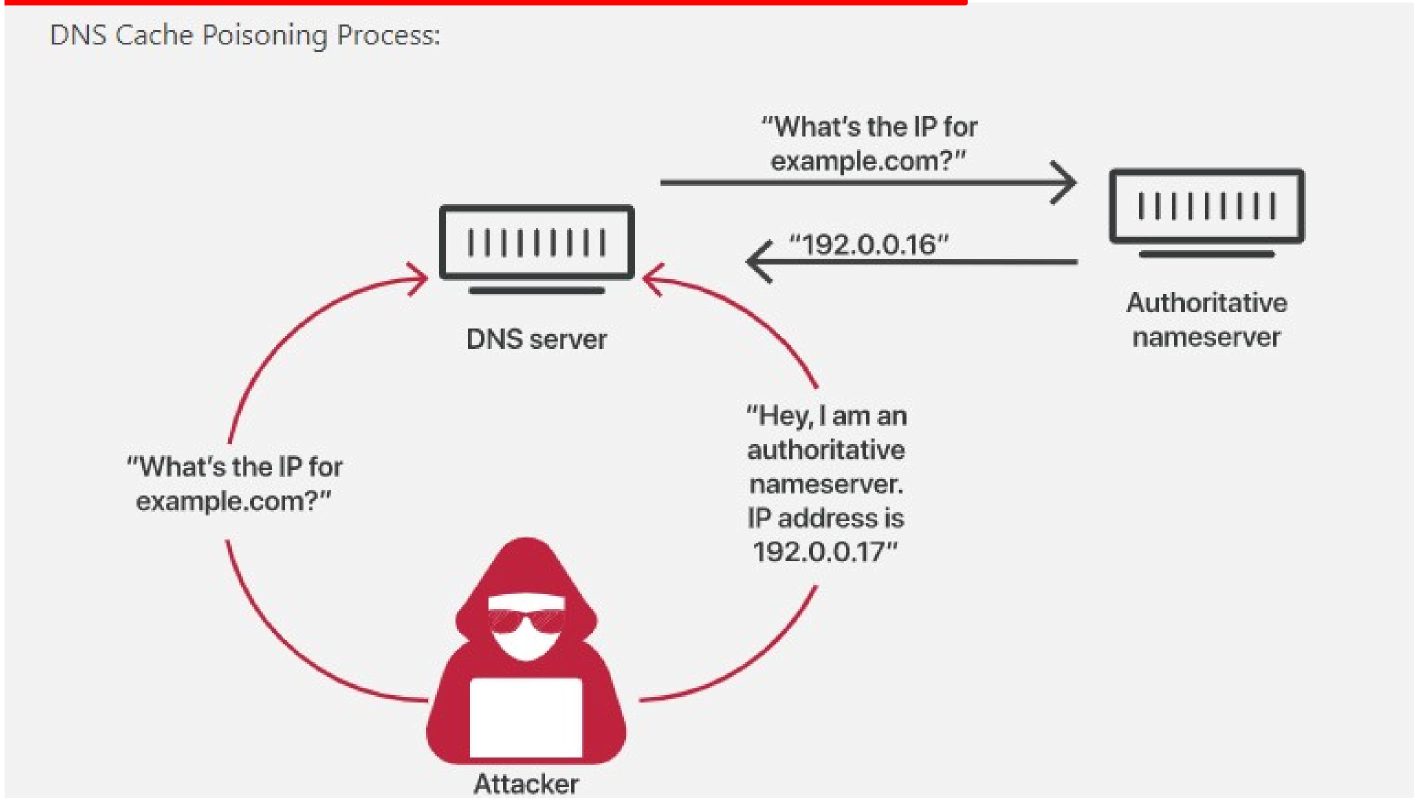
1. DNS Spoofing is also known as DNS cache poisoning
2. DNS cache poisoning is the act of entering false information into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong websites



DNS SPOOFING



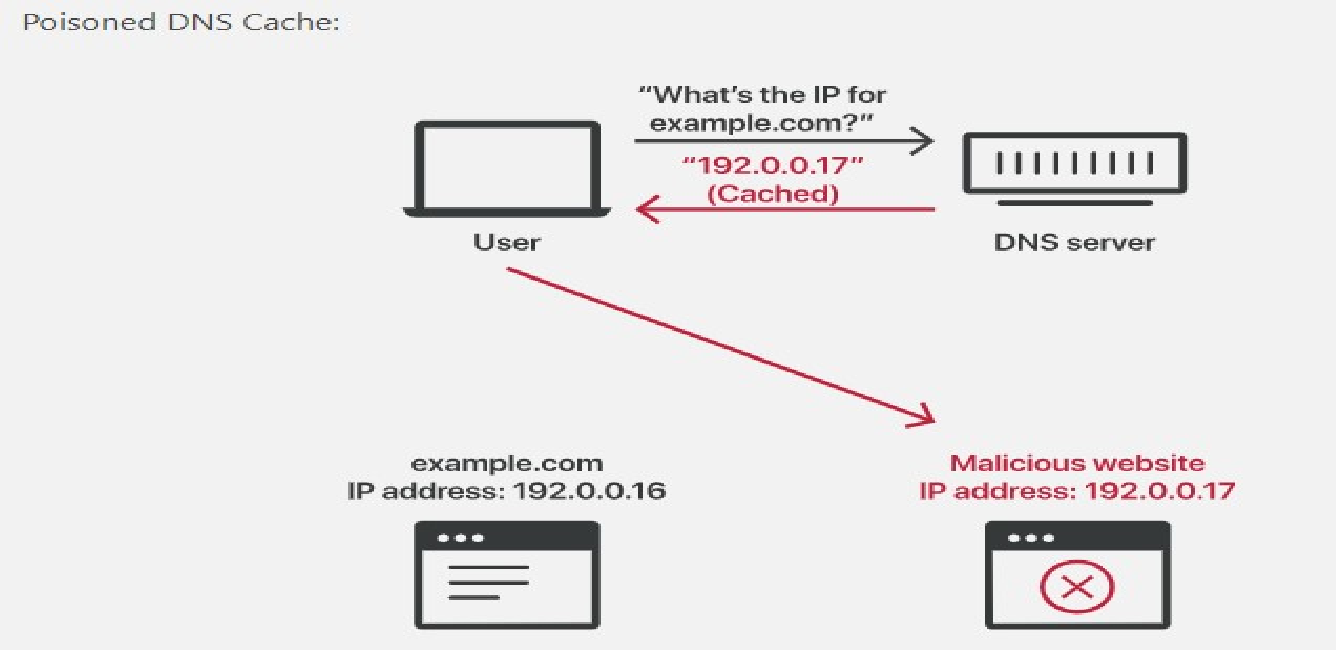
DNS SPOOFING



DNS Cache Poisoning Process:
"What's the IP for example.com?"
"192.0.0.16"
DNS server
Authoritative nameserver
"What's the IP for example.com?"
"Hey, I am an authoritative nameserver. IP address is 192.0.0.17"
Attacker

Attackers can poison DNS caches by impersonating DNS nameservers, making a request to a DNS resolver, and then forging the reply when the DNS resolver queries a nameserver. This is possible because DNS servers use UDP instead of TCP, and because currently there is no verification for DNS information.

DNS SPOOFING



Instead of using TCP, which requires both communicating parties to perform a 'handshake' to initiate communication and verify the identity of the devices, DNS requests and responses use UDP, or the User Datagram Protocol. With UDP, there is no guarantee that a connection is open, that the recipient is ready to receive, or that the sender is who they say they are. UDP is vulnerable to forging for this reason – an attacker can send a message via UDP and pretend it's a response from a legitimate server by forging the header data.

PORT SCANNING

1. A port scan is a process which identifies “open doors” to a computer.
2. Ports are points at which information comes and goes from a computer, so by scanning for open ports, attackers can find weakened pathways with which to enter your computer.
3. Port scanning is one of the most popular techniques attackers use to discover services they can exploit to break into your computer system
4. Port scanning provides the following information to attackers:
    - What services are running
    - Which users own the services
    - If anonymous logins are allowed
    - What network services require authentication
5. During a port scan, hackers send a message to each port, one at a time. The response they receive from each port determines whether it’s being used and reveals potential weaknesses.

PORT SCANNING – How does it work

1. Port scans send requests to every port, asking to connect to a network. The scan then makes note of the ports that respond and which seem vulnerable.
2. Once the attacker has determined vulnerable ports in a network, the scan will classify ports into three categories:
   - **Open:** The host responds, announcing it is listening and open to requests. An open port means it's a path to attack the network.
   - **Closed:** The host responds, but notes there is no application listening. Often, hackers will come back to scan again in case it opens up.
   - **Filtered:** The host does not respond to a request. This could mean the packet was dropped due to congestion or a firewall.

Module 5: Network Security and Applications

5.1

- Network Security Basics
- TCP/IP Vulnerabilities
- Packet Sniffing
- ARP Spoofing, DNS Spoofing
- Port Scanning, TCP Syn flood

5.2

- Denial of Service (DOS)
- Classic DOS attacks
- Source Address Spoofing
- ICMP Flood, SYN flood, UDP flood
- Distributed DOS, Defences against DOS Attacks

5.3

- Internet Security Protocols: SSL, IPSEC
- Secure Email: PGP, Firewalls
- IDS and Its types
- Honey pots

DENIAL OF SERVICE (DoS)

1. A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.
2. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
3. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

DENIAL OF SERVICE (DoS)

1. Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations.
2. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.
3. There are two general methods of DoS attacks: **flooding services or crashing services.**
4. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop.
5. Popular flood attacks include: **ICMP Flood, SYN Flood.**

Internet Control Message Protocol (ICMP) Flood

1. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.
2. Commonly, the ICMP protocol is used on network devices, such as routers.
3. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.
4. Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim’s computer by overwhelming it with ICMP echo requests, also known as pings.
5. The ICMP echo-request and echo-reply messages are commonly used for the purpose of performing a ping.

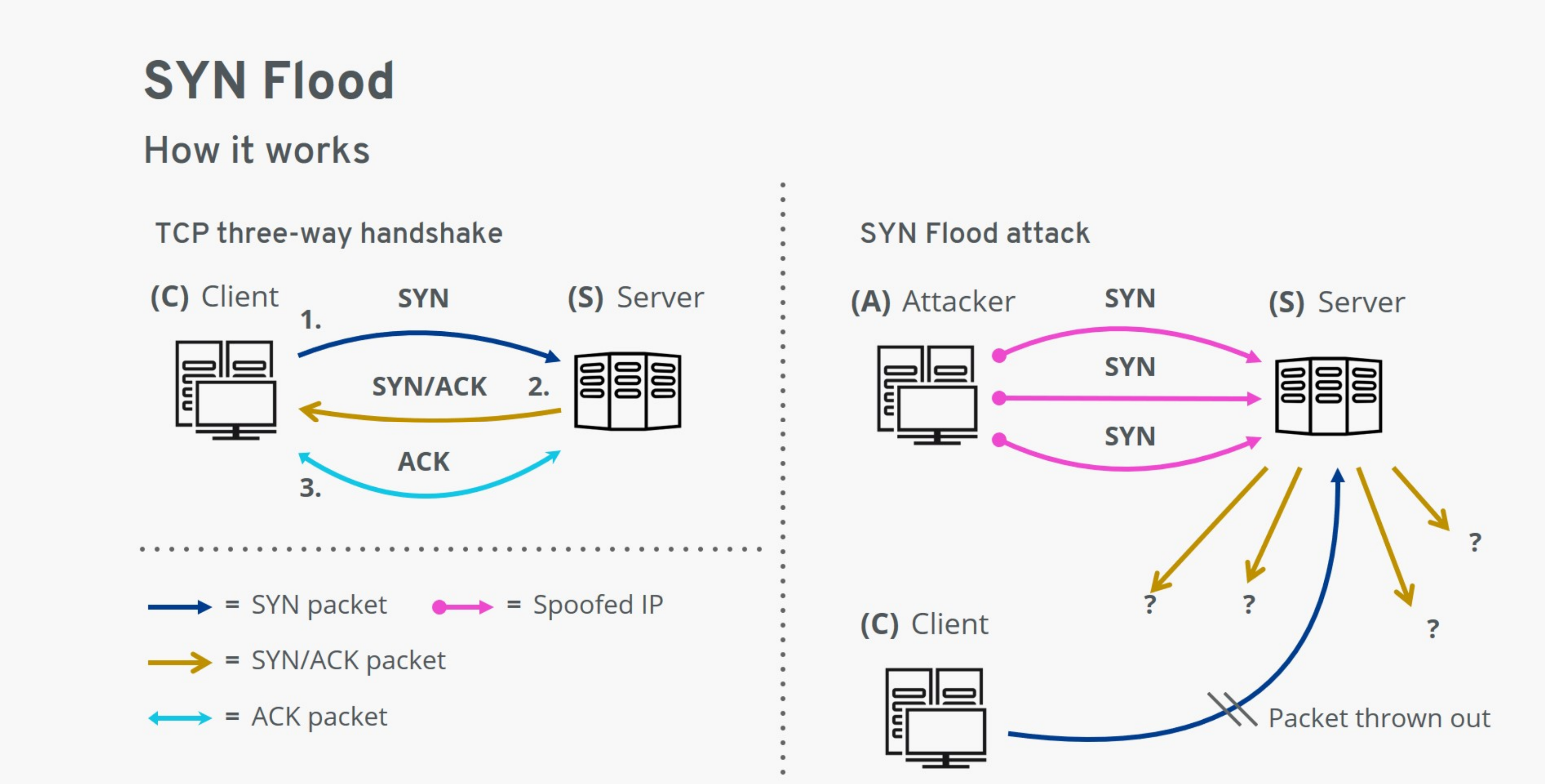
Ping Flood Attack (ICMP Attack)

1. Ping Flood is a Denial of Service Attack. In this attack, the attacker sends a large number of ICMP Echo request or ping packets to the targeted victim’s IP address.
2. As a result, victim’s machine starts responding to each ICMP packet by sending an ICMP Echo Reply Packet
3. Now, the victim’s machine takes twice the bandwidth of the attacker- Once for receiving the packets and once for sending replies.
4. Thus, if the attacker has a much higher bandwidth than the victim, the victim’s machine will get flooded with network Traffic
5. The victim’s machine will consume a large number of CPU Cycles and notices a significant slow down
6. This attack is called Ping Flood

SYN Flood

1. TCP SYN flood (a.k.a. SYN flood) is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.
2. Under normal conditions, TCP connection exhibits three distinct processes in order to make a connection.
   - ✓ First, the client sends a SYN packet to the server in order to initiate the connection.
   - ✓ The server then responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication.
   - ✓ Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.

SYN Flood


SYN Flood
How it works
TCP three-way handshake
(C) Client
SYN
(S) Server
1.
SYN/ACK
2.
ACK
3.
= SYN packet
= Spoofed IP
= SYN/ACK packet
= ACK packet
SYN Flood attack
(A) Attacker
SYN
(S) Server
SYN
SYN
?
?
?
?
(C) Client
Packet thrown out

SYN Flood

1. The attacker sends a high volume of SYN packets to the targeted server, often with spoofed IP addresses.
2. The server then responds to each one of the connection requests and leaves an open port ready to receive the response.
3. While the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the server to temporarily maintain a new open port connection for a certain length of time, and once all the available ports have been utilized the server is unable to function normally.

Distributed Denial of Service Attack

1. A distributed denial-of-service (DDoS) attack is one of the most powerful weapons on the internet.
2. When we hear about a website being “brought down by hackers,” it generally means it has become a victim of a DDoS attack.
3. In short, this means that hackers have attempted to make a website or computer unavailable by flooding or crashing the website with too much traffic.
4. In a DoS attack, it’s one system that is sending the malicious data or requests; a DDoS attack comes from multiple systems.

Distributed Denial of Service Attack

1. DDoS attacks are carried out with networks of Internet-connected machines.
2. These networks consist of computers and other devices (such as IoT devices)which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.
3. Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.
4. When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.
5. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

Distributed Denial of Service Attack

1. A DDoS is a cyberattack on a server, service, website, or network floods it with Internet traffic. If the traffic overwhelms the target, its server, service, website, or network is rendered inoperable.
2. Network connections on the Internet consist of different layers of the Open Systems Interconnection (OS) model. Different types of DDoS attacks focus on particular layers. A few examples:
   - Layer 3, the Network layer. Attacks are known as Smurf Attacks, ICMP Floods, and IP/ICMP Fragmentation.
   - Layer 4, the Transport layer. Attacks include SYN Floods, UDP Floods, and TCP Connection Exhaustion.
   - Layer 7, the Application layer. Mainly, HTTP-encrypted attacks.

Module 5: Network Security and Applications

5.1

- Network Security Basics
- TCP/IP Vulnerabilities
- Packet Sniffing
- ARP Spoofing, DNS Spoofing
- Port Scanning, TCP Syn flood

5.2

- Denial of Service (DOS)
- Classic DOS attacks
- Source Address Spoofing
- ICMP Flood, SYN flood, UDP flood
- Distributed DOS, Defences against DOS Attacks

5.3

- Internet Security Protocols: SSL, IPSEC
- Secure Email: PGP, Firewalls
- IDS and Its types
- Honey pots

Internet Security

1. Internet security refers to securing communication over the internet. It includes specific security protocols such as:
   - ✓ Internet Security Protocol (IPSec)
   - ✓ Secure Socket Layer (SSL)

Secure Socket Layer (SSL)

It is a security protocol developed by Netscape Communications Corporation.). It provides security at transport layer. It addresses the following security issues:

1. Privacy
2. Integrity
3. Authentication

Internet Security Protocol (IPSec)

It consists of a set of protocols designed by Internet Engineering Task Force (IETF). It provides security at network level and helps to create authenticated and confidential packets for IP layer.

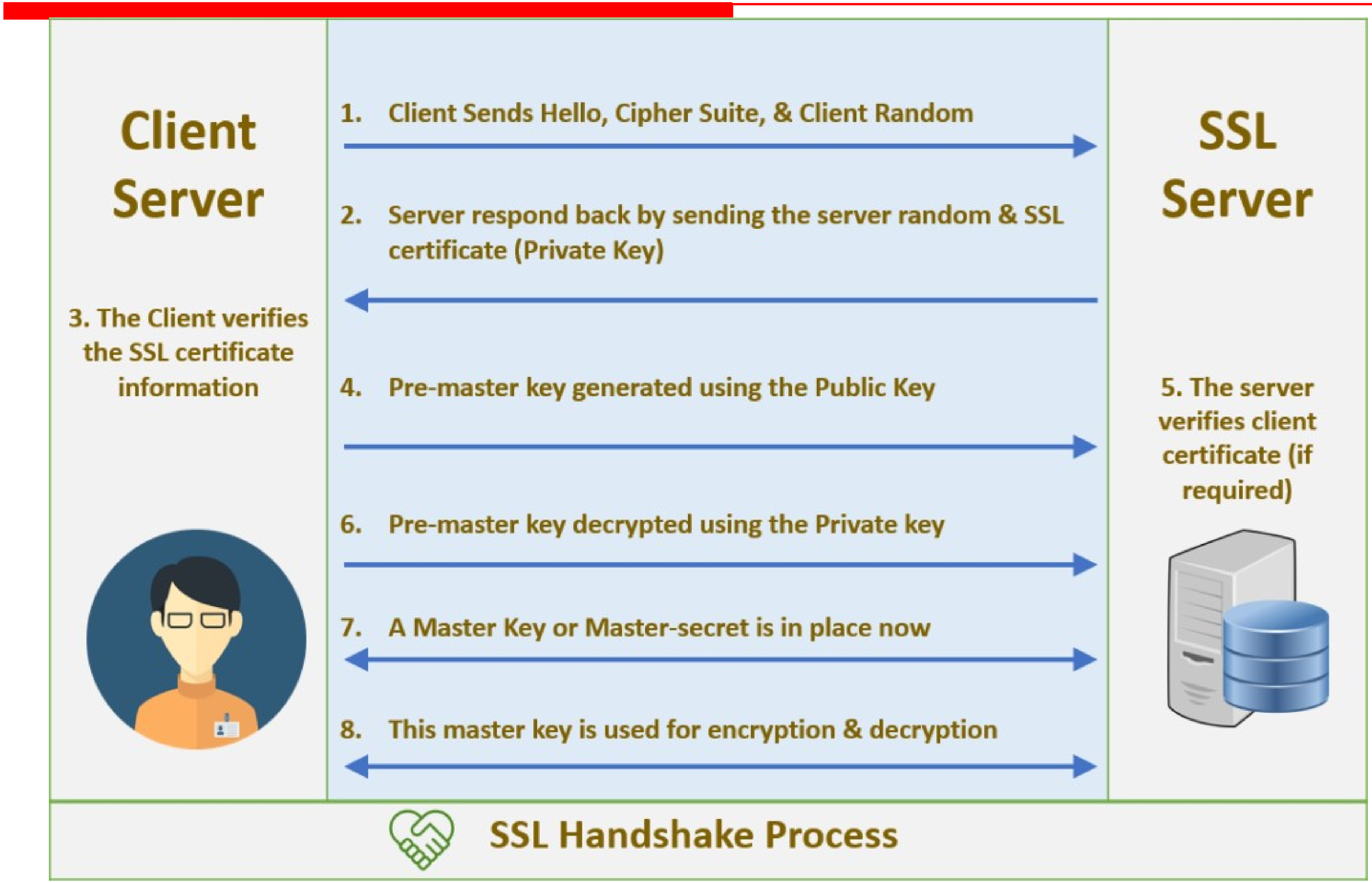
SSL (Secure Socket Layer) – How it works

1. In order to provide a high degree of privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
2. SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
3. SSL also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.

SSL (Secure Socket Layer) – Handshake

1. The SSL/TLS handshake involves a series of steps through which both the parties – client and server, validate each other and start communicating through the secure SSL/TLS tunnel.
2. A TLS handshake takes place whenever a user navigates to a website over HTTPS and the browser first begins to query the website's origin server.
3. During the course of a TLS handshake, the client and server together will do the following:
   - ✓ Specify which version of TLS (TLS 1.0, 1.2, 1.3, etc.) they will use
   - ✓ Decide on which cipher suites (see below) they will use
   - ✓ Authenticate the identity of the server via the server’s public key and the SSL certificate authority’s digital signature
   - ✓ Generate session keys in order to use symmetric encryption after the handshake is complete

SSL (Secure Socket Layer) – Handshake



Client Server

SSL Server

1. Client Sends Hello, Cipher Suite, & Client Random

2. Server respond back by sending the server random & SSL certificate (Private Key)

3. The Client verifies the SSL certificate information

4. Pre-master key generated using the Public Key

5. The server verifies client certificate (if required)

6. Pre-master key decrypted using the Private key

7. A Master Key or Master-secret is in place now

8. This master key is used for encryption & decryption

SSL Handshake Process

IPSec

1. Within the term "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure.“
2. The Internet Protocol is the main routing protocol used on the Internet; it designates where data will go using IP addresses.
3. IPsec is secure because it adds encryption* and authentication to this process.
4. The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality.
5. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

IPSec - USES

1. To encrypt application layer data.
2. To provide security for routers sending routing data across the public internet.
3. To provide authentication without encryption, like to authenticate that the data originates from a known sender.
4. To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

IPSec – Protocols used

The following protocols make up the IPsec suite:

1. **Authentication Header (AH):** The AH protocol ensures that data packets are from a trusted source and that the data has not been tampered with, like a tamper-proof seal on a consumer product. These headers do not provide any encryption; they do not help conceal the data from attackers.
2. **Encapsulating Security Protocol (ESP):** ESP encrypts the IP header and the payload for each packet — unless transport mode is used, in which case it only encrypts the payload. ESP adds its own header and a trailer to each data packet.
3. **Security Association (SA):** SA refers to a number of protocols used for negotiating encryption keys and algorithms. One of the most common SA protocols is Internet Key Exchange (IKE).

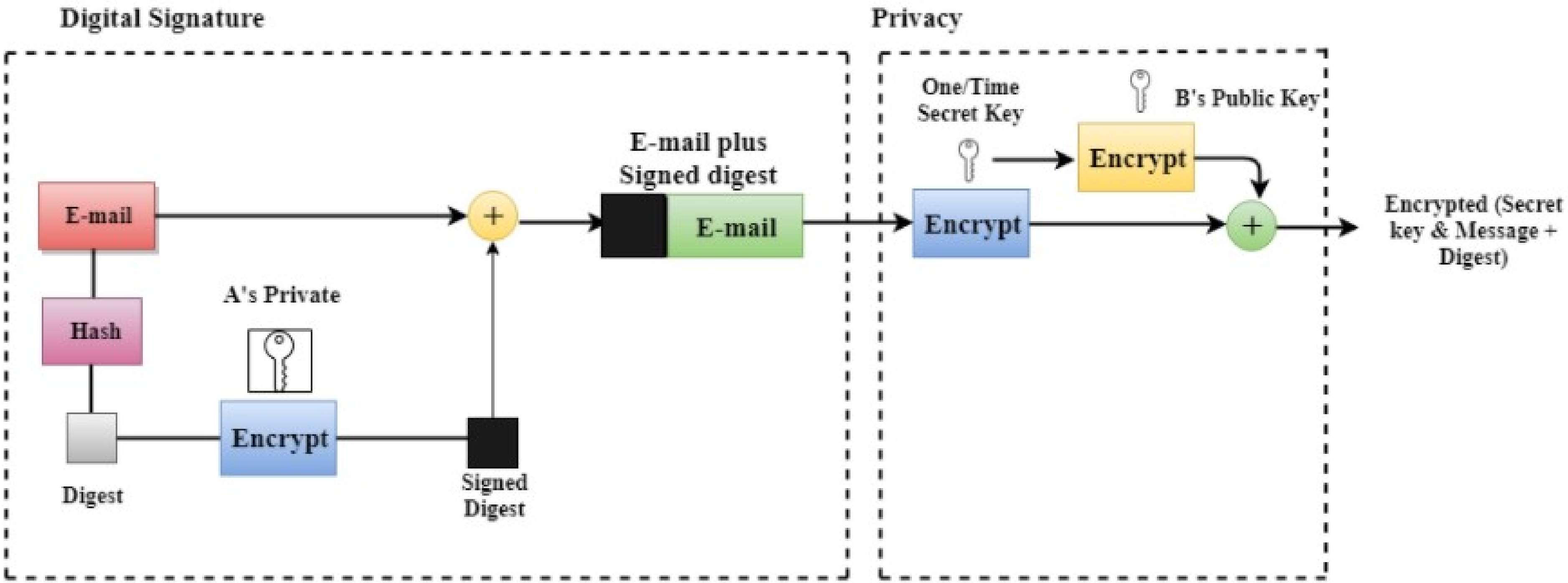
PGP: Pretty Good Privacy

1. Pretty Good Privacy (PGP) is an encryption system used for both sending encrypted emails and encrypting sensitive files.
2. The popularity of PGP is based on two factors.

✓ It is available as freeware, and so spread rapidly among users who wanted an extra level of security for their email messages.

✓ PGP uses both symmetric encryption and public-key encryption, it allows users who have never met to send encrypted messages to each other without exchanging private encryption keys.

Steps taken by PGP to create secure e-mail at the sender

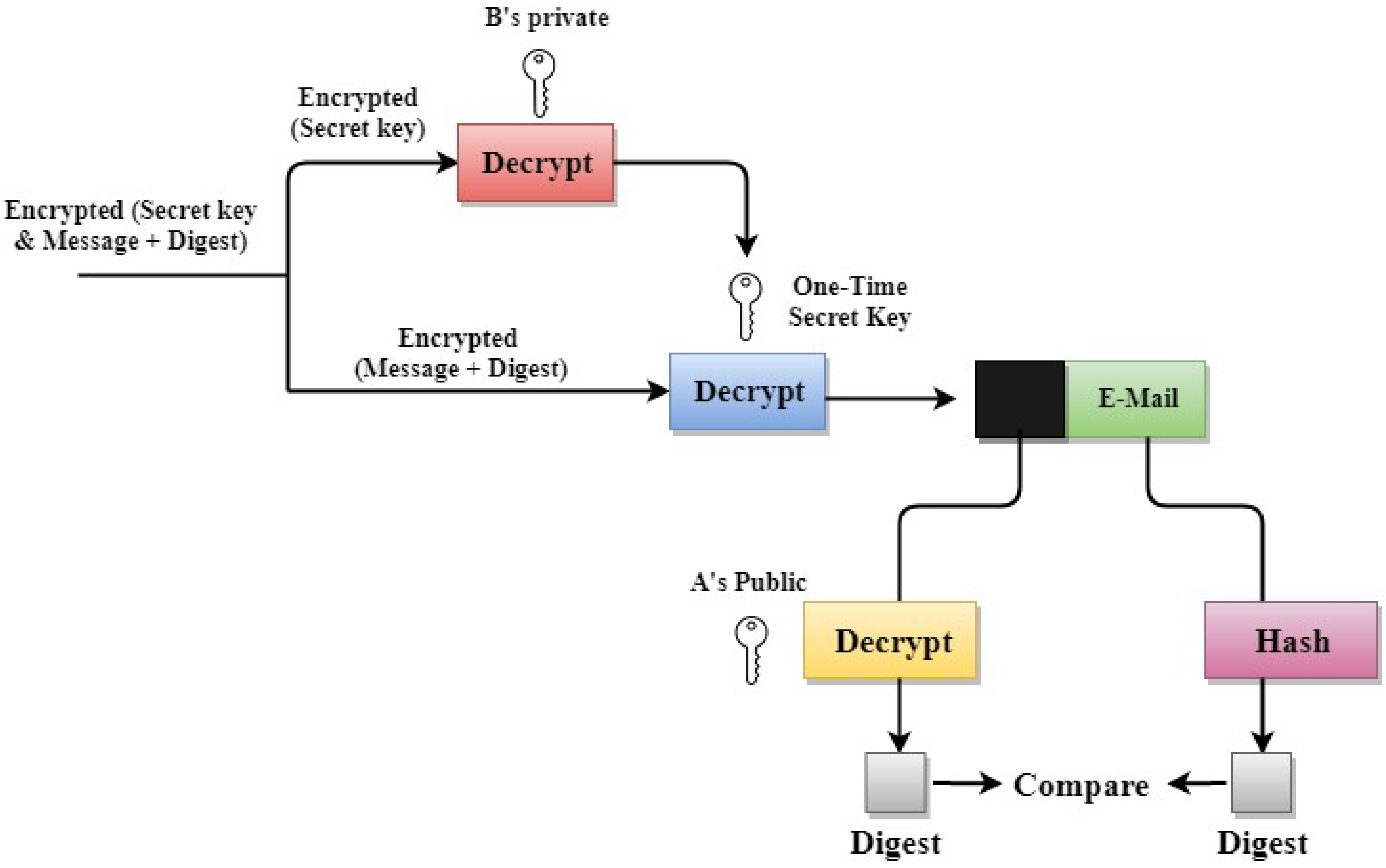


Steps taken by PGP to create secure e-mail at the sender

1. The e-mail message is hashed by using a hashing function to create a digest.
2. The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
3. The original message and signed digest are encrypted by using a one-time secret key created by the sender.
4. The secret key is encrypted by using a receiver's public key.
5. Both the encrypted secret key and the encrypted combination of message and digest are sent together.

Steps taken by PGP to create secure e-mail at the receiver

PGP at the Receiver site (B)



Steps taken by PGP to create secure e-mail at the receiver

1. The receiver receives the combination of encrypted secret key and message digest is received.
2. The encrypted secret key is decrypted by using the sender's private key to get the one-time secret key.
3. The secret key is then used to decrypt the combination of message and digest.
4. The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
5. Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

Disadvantages of PGP Encryption

1. **The Administration is difficult:** The different versions of PGP complicate the administration.
2. **Compatibility issues:** Both the sender and the receiver must have compatible versions of PGP.
3. **Complexity:** PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.
4. **No Recovery:** PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.

Intrusion Detection System (IDS)

1. An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
2. It is a software application that scans a network or a system for harmful activity or policy breaching.
3. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a Security Information and Event Management (SIEM) system.
4. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Intrusion Detection System (IDS)

1. Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms.
2. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.
3. Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

Intrusion Detection System (IDS) – How do they work

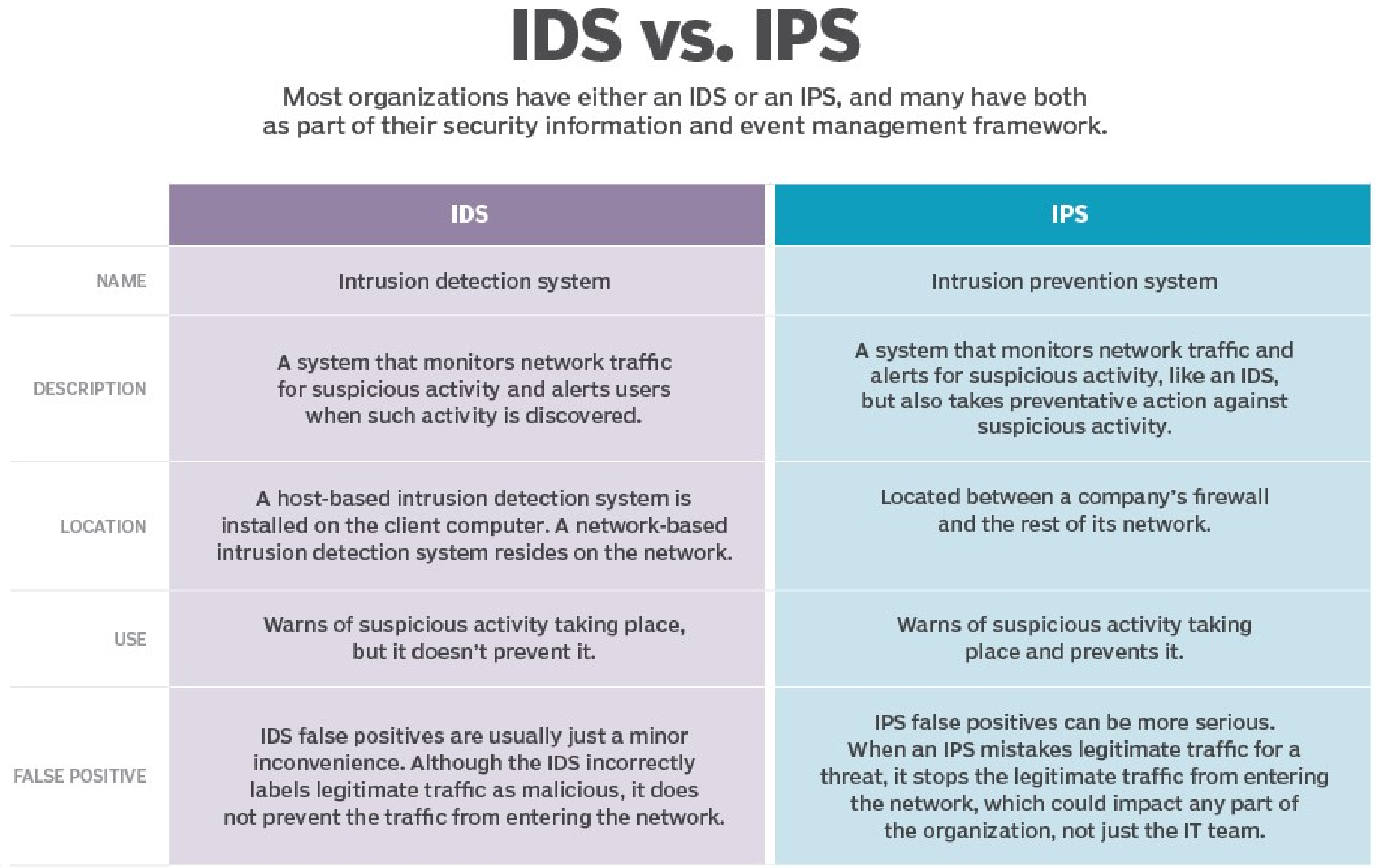
1. Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. They can be either network- or host-based.
2. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network.
3. Intrusion detection systems work by either looking for signatures of known attacks or deviations from normal activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer. They can effectively detect events such as Christmas tree scans and domain name system (DNS) poisonings.
4. An IDS may be implemented as a software application running on customer hardware or as a network security appliance. Cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments.

Is is a unique arrangement of information that can be used to identify an attacker's attempt to exploit a known operating system or application vulnerability.

Intrusion Detection System (IDS) vs. Intrusion Prevention System(IPS)

1. An IDS can be contrasted with an **Intrusion Prevention System** (IPS), which monitors network packets for potentially damaging network traffic, like an IDS, but has the primary goal of preventing threats once detected, as opposed to primarily detecting and recording threats.

Intrusion Detection System (IDS) vs. Intrusion Prevention System(IPS)



IDS vs. IPS

Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.

Types of Intrusion Detection System (IDS)

1. **Network Intrusion Detection System (NIDS)**

   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It can monitor inbound and outbound traffic to and from all the devices on the network.. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

2. **Host Intrusion Detection System (HIDS):** runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network. A HIDS may also be able to identify malicious traffic that originates from the host itself, such as when the host has been infected with malware and is attempting to spread to other systems.

Types of Intrusion Detection System (IDS)

3. **Signature-based Intrusion Detection System (SIDS):** monitors all the packets traversing the network and compares them against a database of attack signatures or attributes of known malicious threats, much like antivirus software.

4. **Anomaly-based Intrusion Detection System (AIDS):** monitors network traffic and compares it against an established baseline to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices.

HONEY POTS

1. A **honeypot** is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems.
2. The principle behind them is simple: **Don’t go looking for attackers.** Prepare something that would attract their interest — the **honeypot — and then wait for the attackers to show up.**
3. Like mice to cheese-baited mousetraps, cybercriminals are attracted to honeypots — not because they’re honeypots.
4. The bad guys think the honeypot is a legitimate target, something worthy of their time. That’s because the bait includes applications and data that simulate a real computer system.

HONEY POTS

1. The function of a honeypot is to represent itself on the internet as a potential target for attackers -- usually, a server or other high-value asset -- and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.
2. The honeypot looks like a real computer system, with applications and data, fooling cybercriminals into thinking it's a legitimate target.
3. For example, a honeypot could mimic a company's customer billing system - a frequent target of attack for criminals who want to find credit card numbers.
4. Once the hackers are in, they can be tracked, and their behavior assessed for clues on how to make the real network more secure.

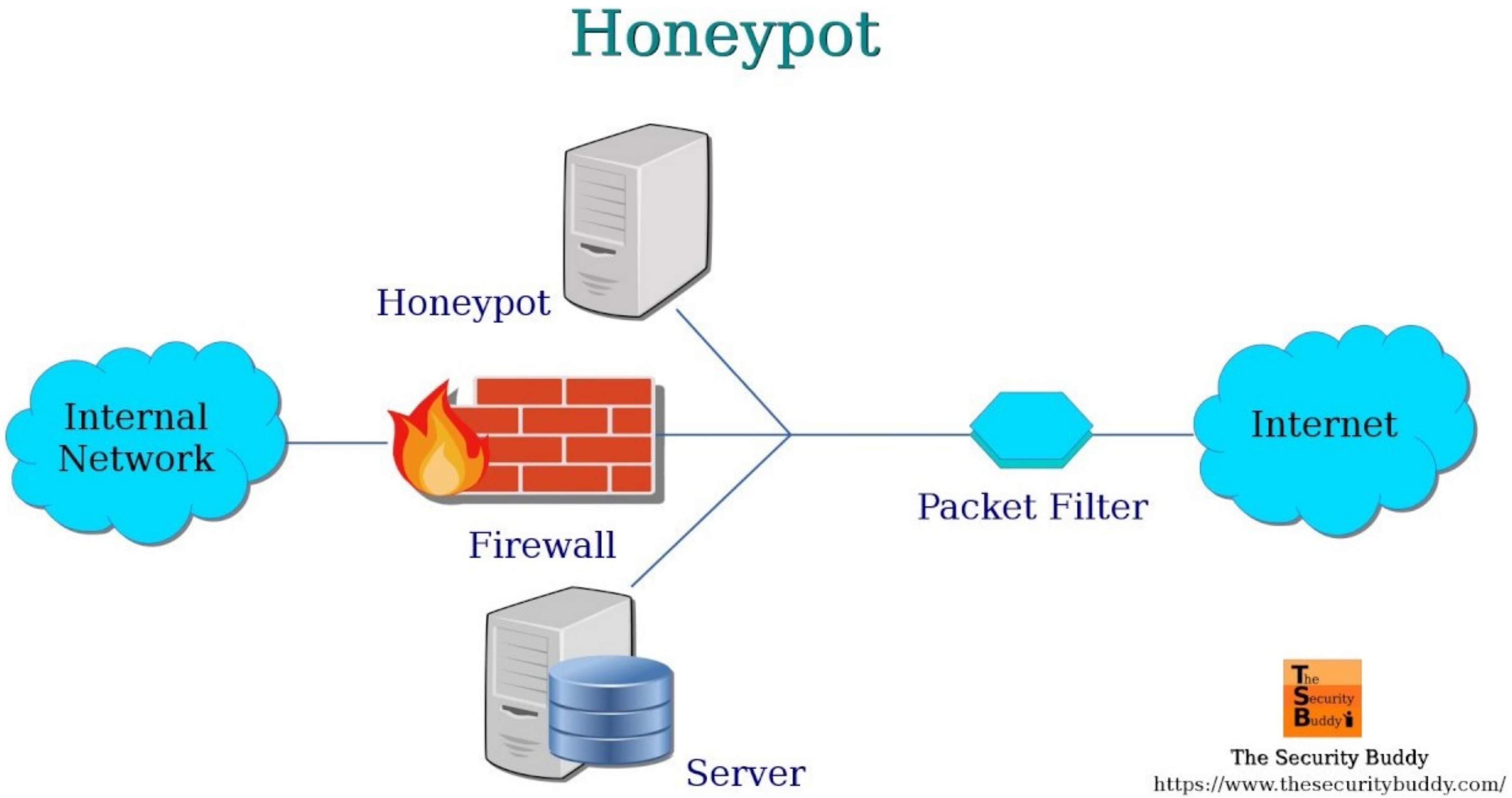
In a nutshell, honeypots help organizations:

a) Assess the latest trends in attacks,

b) Understand where cyber attacks arise, and

c) Better frame security policies to mitigate future risks.

HONEY POTS



The Security Buddy
https://www.thesecuritybuddy.com/

HONEY POTS – How do they work

1. Generally, a honeypot operation consists of a computer, applications and data that simulate the behavior of a real system that would be attractive to attackers, such as a financial system, internet of things (IoT) devices, or a public utility or transportation network. It appears as part of a network but is actually isolated and closely monitored. Because there is no reason for legitimate users to access a honeypot, any attempts to communicate with it are considered hostile.

2. Honeypots are often placed in a demilitarized zone (DMZ) on the network. That approach keeps it isolated from the main production network, while still being a part of it. In the DMZ, a honeypot can be monitored from a distance while attackers access it, minimizing the risk of the main network being breached.

HONEY POTS – TYPES

Honeypots are typically categorized in one of two ways — either based on their interaction levels or the types of threats they’re able to detect.

Types of Honeypots Based on Interaction Level and Complexity

High-Interaction Honeypots

These honeypots imitate real-world systems and applications with actual services, functions, and operating systems involving high levels of interactivity (though less than pure honeypots). Setting up high-interaction honeypots is a complex and resource-intensive process. It gives extensive details about how an attack progresses and how payloads execute in a network. However, since there are actual operating systems and services involved, the chance of infection is higher if the hackers are able to compromise the honeypots and use them gain access to your organization’s real production environment.

HONEY POTS – TYPES

Types of Honeypots Based on Interaction Level and Complexity

Medium-Interaction Honeypots

Come with expanded capabilities compared to low interaction honeypots but reduced implementation complexities than high interaction honeypots. They imitate the application layer but don’t have their own operating system. Organizations typically deploy these types of honeypots to stall attackers to give them time to respond to attacks.

Low-Interaction Honeypots

Low-interaction honeypots allow partial interaction with systems since they run limited emulated services with restricted functionality as would be typically expected from a server. Though these are the easiest to set up and maintain, they run the risk of coming across as inauthentic targets to potential attackers. These types of honeypots serve as an early detection mechanism, and organizations commonly use them in production environments.

HONEY POTS – TYPES

Some Other Types of Honeypots

Malware Honeypots — These types of honeypots detect malware based on known replication techniques and propagation vectors.

Database Honeypots — Since attacks on databases like SQL injections are fairly common, you can use database honeypots to distract an attacker from your legitimate database servers by setting up decoy databases.

Client Honeypots — These honeypots typically act as servers, listening in for incoming connections. Client honeypots actively engage with malicious servers that attack clients. They pose as a client to monitor and record any modifications.

Email Honeypots — Email honeypots are a list of email addresses used by email service providers to detect spammers. Typically, accounts inactive over a long period of time are used for this purpose.

Spider Honeypots — These honeypots are used to trap web-crawlers by creating fake web pages and links only reachable by crawlers. Detecting these crawlers can be useful in blocking bot activity.

HONEY POTS – TYPES

Types of Honeypots Based on Purpose

Research Honeypots

These honeypots are deployed and used by researchers to gain a better understanding of attack techniques, motivations, information about malware strains in the wild, and security vulnerabilities. This is done to specifically use the knowledge gained to make informed decisions about:

- ✓ Defense strategies,
- ✓ Patching prioritizations,
- ✓ Future security investments, and
- ✓ Identifying and developing new security solutions.

Production Honeypots

Production honeypots are placed within your organization's internal network with other production servers. Though the intention is similar in terms of gaining insights about active attacks, it is typically less complex than research honeypots with lesser data. It is primarily deployed to identify active attacks on the internal network and distract or misdirect hackers from attacking your legitimate servers

FIREWALL

1. A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.
2. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.
3. Firewalls have been a first line of defense in network security
4. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
5. A firewall can be hardware, software, or both.
6. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.

FIREWALL – How does they work

1. Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices.
2. For example, “Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

FIREWALL – Types

1. **Proxy Firewall:** An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

2. **Stateful inspection firewall:** Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

FIREWALL – Types

3. **Next Generation Firewall:** Combine traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more. Most notably, it includes deep packet inspection (DPI). While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious data.