Chapter 2

- Vulnerabilities and Attacks on TCP/IP stack

Cyber Security Datasets for Deep Learning

- **Knowledge Discovery and Dissemination (KDD) 1999 dataset.**
- **NSL-KDD dataset.**
- **CTU-13 dataset.**
- **Malware Datasets:**

- ❑ Top apps in Google Play Store(source of benignware)
- ❑ Contagio
- ❑ DREBIN
- ❑ VirusTotal
- ❑ Genome Project
- ❑ Comodo
- ❑ Microsoft

- Many research experiments or analysis were performed on NSL-KDD data set.
- The primary objective of the investigation and examination of data set is to build better IDS model.
- Using different machine learning tools experiments over NSL-KDD data set were performed by waikato environment for knowledge analysis (WEKA).
- The NSL-KDD data set, which are used, relates to different types of attack. Generally or experimentally they are classified in to four types of attacks:
- **DoS attack**
- **User-to-root attack (U2R)**
- **Remote-to-local attack (R2L)**
- **Probing attack (Probe)**

1. DOS Attack:

- The denial of service (DoS) attack mainly floods the server, system, or network by bombardment of superfluous packets.
- Due to that, the system's buffer becomes full and unable to respond and it is unable to return to the valid request.
- The primary objective of this attack is to consume memory or other resources of the target.

2. User to root attack (u2r)

- the attacker get access to the target system using valid user authentication.
- An attacker can exploit the current system vulnerabilities. Attacks belong to the user to root are as follows.

a. buffer overflow attack
b. load-module
c. Rootkit and
d. Perl

3. Remote to local attack r2l

- Attacker uses existing vulnerabilities to access target account.
- An attacker does not own target system but access it locally. Examples of R2L attacks are as follows.

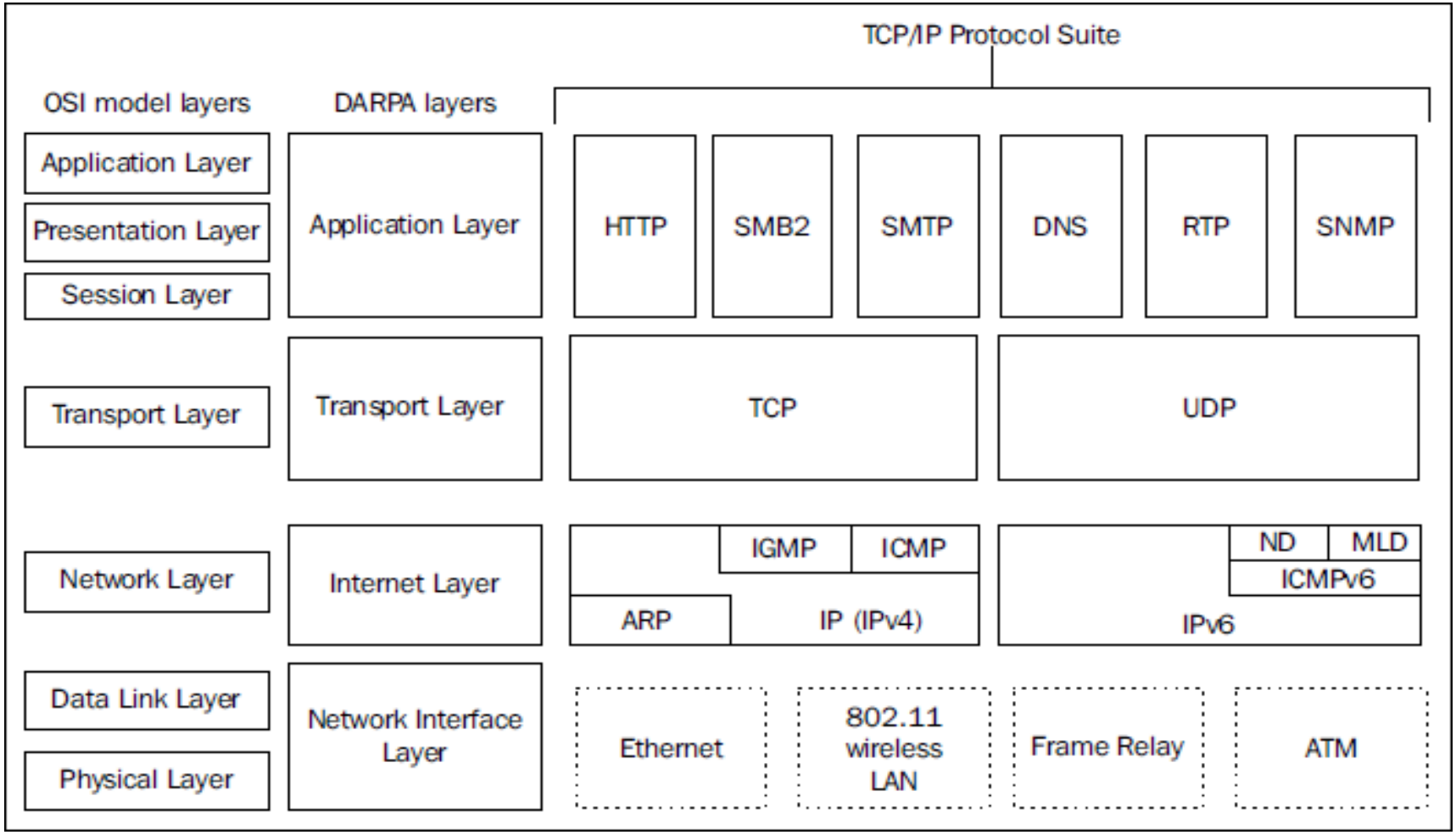
a. multi-hope
b. guess password
c. FTP write.
d. IMAP and

4. Probing Attack

- The security frame is dodged by the attacker and obtain relevant data from the target system. Some of the probe attacks are follows.

a. NMAP b. IPSWEEP c. SATAN d. PORTSWEEP.

TCP/IP Stack


TCP/IP Protocol Suite
OSI model layers
DARPA layers
Application Layer
Presentation Layer
Session Layer
Application Layer
HTTP
SMB2
SMTP
DNS
RTP
SNMP
Transport Layer
Transport Layer
TCP
UDP
Network Layer
Internet Layer
IGMP
ICMP
ARP
IP (IPv4)
ND
MLD
ICMPv6
IPv6
Data Link Layer
Physical Layer
Network Interface Layer
Ethernet
802.11 wireless LAN
Frame Relay
ATM

Protocols in Application layer

Application LayerProtocols:

- FileTransfer Protocol(FTP)
- Telnet
- Secure Shell(SSH)
- Simple MailTransfer Protocol (SMTP)
- Domain Name System(DNS)
- Dynamic Host Configuration Protocol(DHCP)
- HypertextTransfer Protocol

Since the application layer is the closest layer to the end user, it provides hackers with the largest threat surface. Poor app layer security can lead to performance and stability issues, data theft, and in some cases the network being taken down.

Possible Attacks due to vulnerabilties in the Transport Layer protocol

- SYN Flooding Attack
- TCP Session Hijacking
- TCP Reassembly and Sequencing
- UDP Flood Attack
- Secure protocol for Defence-SSL/TLS

Possible Attacks due to vulnerabilties in the Network Layer protocol

1. IP Fragmentation Attack
2. IP Spoofing Attack
3. Ping Flood Attack (ICMP protocol)
4. Smurf Attack
5. Ping of Death Attack
6. IGMP Flood Attack
7. ARP Spoofing /Poisoning Attack

Possible Attacks due to vulnerabilties in the Data Link Layer protocol

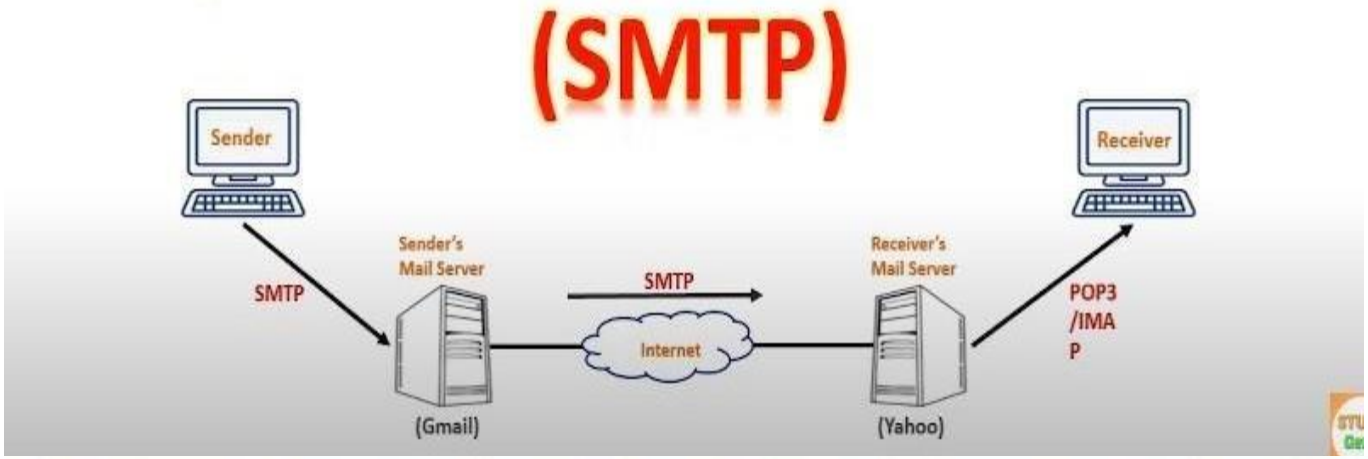
- Port Stealing
- MAC Flooding attack
- DHCP –Starvation and Spoofing

Possible Attacks due to vulnerabilties in the Application Layer protocol

- Account Enuemeration / Email Spoofing(SMTP)
- HTTP Flood Attack-DDoS attack(HTTP)
- DNS Spoofing attack or DNS Cache poisoning
- Anonymous Authentication, Directory Travesal Attack, Driden based Malware Attack(FTP)

Possible attacks at tcp/ip layers

Application Layer SMTP



- SMTP is a set of communication guidelines that allow to transmit an e-mail over the internet.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- The main purpose of SMTP is used to set up communication rules between servers.

- It is an application layer protocol.
- SMTP uses TCP at the transport layer.
- SMTP uses TCP port number 25 and Port 465.
  - **Port 25** - this is the default SMTP non-encrypted port
  - **Port 465** - this is the port used if you want to send messages using SMTP securely
- SMTP is a connection oriented protocol.
- SMTP is a push protocol.

- **SMTP is a pure text based protocol.**
  - SMTP can only handle the messages containing 7 bit ASCII text.
  - SMTP cannot transfer other types of data like images, video, audio etc.
  - SMTP cannot transfer executable files and binary objects.
  - SMTP cannot transfer the text data of other languages like French, Japanese, and Chinese etc. (Since they are represented in 8 bit codes)

- **MIME extends the limited capabilities of email.**
  - Multipurpose Internet Email Extension (MIME) is an extension to the internet email protocol.
  - It extends the limited capabilities of email by enabling the users to send and receive graphics, audio files, video files, etc in the message.
  - MIME was specially designed for SMTP.

SMTP Commands

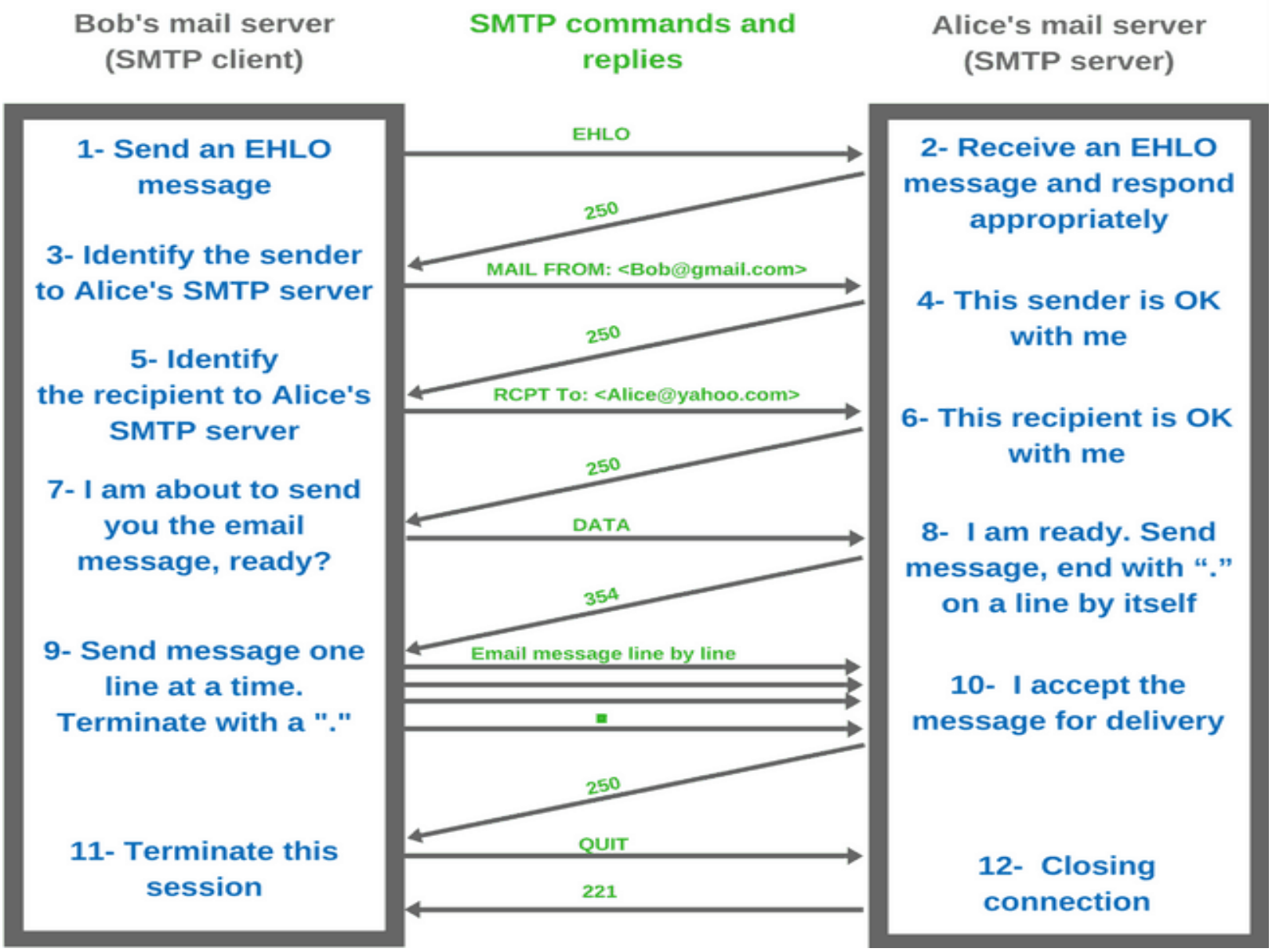
Sender's Mail Server
(SMTP Client)

HELO	:It's the first SMTP command: is starts the conversation identifying the sender server and is generally followed by its domain name.
EHLO	An alternative command to start the conversation, underlying that the server is using the Extended SMTP protocol.
MAIL FROM	This indicates the sender's address.
RCPT TO	It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
SIZE	This SMTP command informs the remote server about the estimated size (in terms of bytes) of the attached email. It can also be used to report the maximum size of a message to be accepted by the server.
DATA	The DATA command signifies that a stream of data will follow.
QUIT	This commands is used to terminate the SMTP connection.
VRFY	The server is asked to verify whether a particular email address or username actually exists. NOOP The NOOP command is used only to check whether the

SMTP response codes

Receiver's Mail Server
(SMTP Server)

Code	Meanings
101	Server connection error (wrong server name or connection port)
211	System status (response to HELP)
214	Help message (response to HELP)
220	The server is ready (response to the client's attempt to establish a TCP connection)
221	The server closes the transmission channel
235	Authentication successful (response to AUTH)
250	The requested command is completed. As a rule, the code is followed by OK
354	The server confirms mail content transfer (response to DATA). After that, the client starts sending the mail. Terminated with a period (".")
500	Syntax error. The server cannot recognize the command

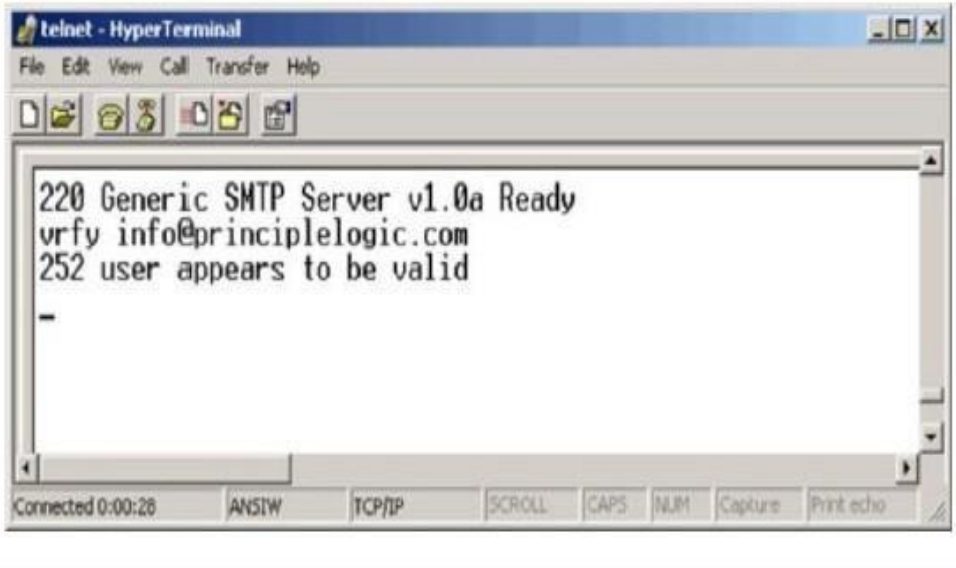

Bob's mail server
(SMTP client)
SMTP commands and
replies
Alice's mail server
(SMTP server)
1- Send an EHLO message
EHLO
2- Receive an EHLO message and respond appropriately
250
3- Identify the sender to Alice's SMTP server
MAIL FROM: <Bob@gmail.com>
4- This sender is OK with me
250
5- Identify the recipient to Alice's SMTP server
RCPT To: <Alice@yahoo.com>
6- This recipient is OK with me
250
7- I am about to send you the email message, ready?
DATA
8- I am ready. Send message, end with "." on a line by itself
354
9- Send message one line at a time. Terminate with a "."
Email message line by line
10- I accept the message for delivery
250
11- Terminate this session
QUIT
12- Closing connection
221

- The basic assumption in this model is that SMTP servers would all be "well-behaved", and not abuse the system by flooding intermediate servers with lots of mail to be delivered, or sending bogus messages to cause problems.

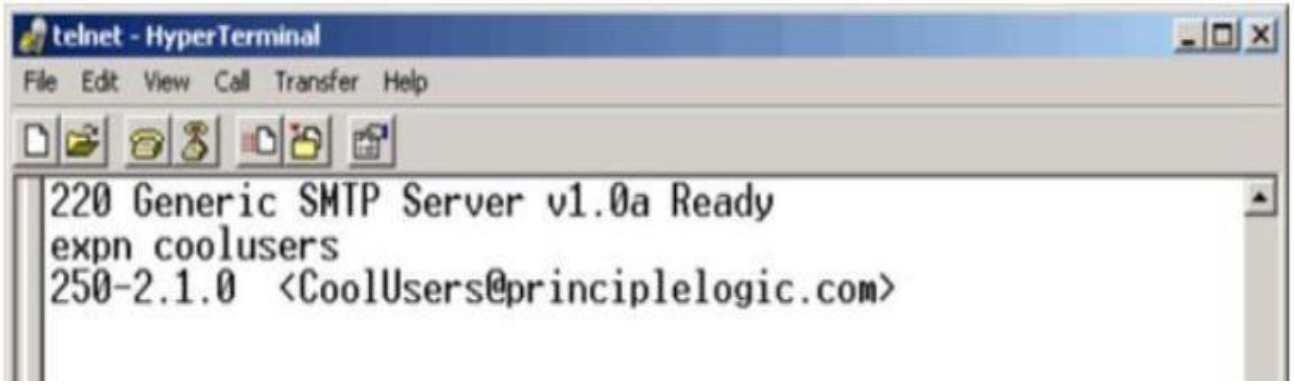
- This e-mail communication protocol was designed for functionality, not security. So, ensuring that you have some level of security will help protect your information.

Account enumeration

- A clever way that attackers can verify whether email accounts exist on a server is simply to telnet to the server on port 25 and run the VRFY command. The VRFY command makes a server check whether a specific user ID exists. Spammers often automate this method to perform a *directory harvest attack*, which is a way of gleaning valid email addresses from a server or domain for hackers to use.

- 

- The SMTP command EXPN might allow attackers to verify what mailing lists exist on a server. You can simply telnet to your e-mail server on port 25 and try EXPN on your system.
-



E-mail header disclosures

If your e-mail client and server are configured with typical defaults, a hacker might find critical pieces of information:

Internal IP address of your e-mail client machine

Software versions of your client and e-mail server along with their vulnerabilities

Hostnames that can divulge your network naming conventions

Countermeasures against header disclosures

The best countermeasure to prevent information disclosures in e-mail headers is to configure your e-mail server or e-mail firewall to rewrite your headers, by either changing the information shown or removing it. Check your e-mail server or firewall documentation to see whether this is an option.

If header rewriting is not available, you still might prevent the sending of some critical information, such as server software version numbers and internal IP addresses.

Malware

E-mail systems are regularly attacked by such malware as viruses and worms. Verify that your antivirus software is actually working.

EICAR offers a safe option for checking the effectiveness of your antivirus software.

EICAR is a European-based malware think tank that has worked in conjunction with anti-malware vendors to provide this basic system test. The EICAR test string transmits in the body of an e-mail or as a file attachment so that you can see how your server and workstations respond. You basically access this file on your computer to see whether your antivirus software detects it:

Defense Mechanisms

- Disable VRFY and EXPN unless you need your remote systems to gather user and mailing list information from your server.
- If you need VRFY and EXPN functionality, check your e-mail server or e-mail firewall documentation for the ability to limit these commands to specific hosts on your network or the Internet.
- **SMTP proxies** are specialized mail transfer agents (MTAs) that, similar to other types of proxy servers, pass SMTP sessions through to other MTAs without using the store-and-forward approach of a typical MTA. When an SMTP proxy receives a connection, it initiates another SMTP session to a destination MTA. Any errors or status information from the destination MTA will be passed back to the sending MTA through the proxy.
- Because SMTP proxies do not store messages like a mail transfer agent (MTA) does, they can reject SMTP connections or message content in real-time, doing away with the need for out-of-band non delivery reports (NDRs), which are the cause of backscatter email, a serious problem in the Internet email system.

https://www.dummies.com/programming/networking/smtp-hacks-and-how-to-guard-against-them/

Relay SMTP relay lets users send e-mails through external servers. Open e-mail relays aren't the problem they used to be, but you still need to check for them. Spammers and hackers can use an e-mail server to send spam or malware through e-mail under the guise of the unsuspecting open-relay owner.

Automatic testing

Here are a couple of easy ways to test your server for SMTP relay:

Free online tools: *www.abuse.net/relay.html*

Windows-based tools: *NetScanTools Pro*

In NetScanTools Pro, you simply enter values for the SMTP mail server name, Your Sending Domain Name. Inside Test Message Settings, enter the Recipient Email Address and Sender's Email Address.

When the test is complete, simply click View Relay Test Results.

Manual testing

You can manually test your server for SMTP relay by telnetting to the e-mail server on port 25. Follow these steps:

1. Telnet to your server on port 25.

You can do this in two ways:

Use your favorite graphical telnet application, such as HyperTerminal or SecureCRT.

Enter the following command at a Windows or UNIX command prompt:

telnet mailserver_address 25

You should see the SMTP welcome banner when the connection is made.

2. Enter a command to tell the server, "Hi, I'm connecting from this domain."
3. Enter a command to tell the server your e-mail address.
4. Enter a command to tell the server who to send the e-mail to.
5. Enter a command to tell the server that the message body is to follow.
6. Enter the following text as the body of the message:
7. End the command with a period on a line by itself.

The final period marks the end of the message. After you enter this final period, your message will be sent if relaying is allowed.

8. Check for relaying on your server:

Look for a message similar to Relay not allowed coming back from the server.

Countermeasures against SMTP relay attacks

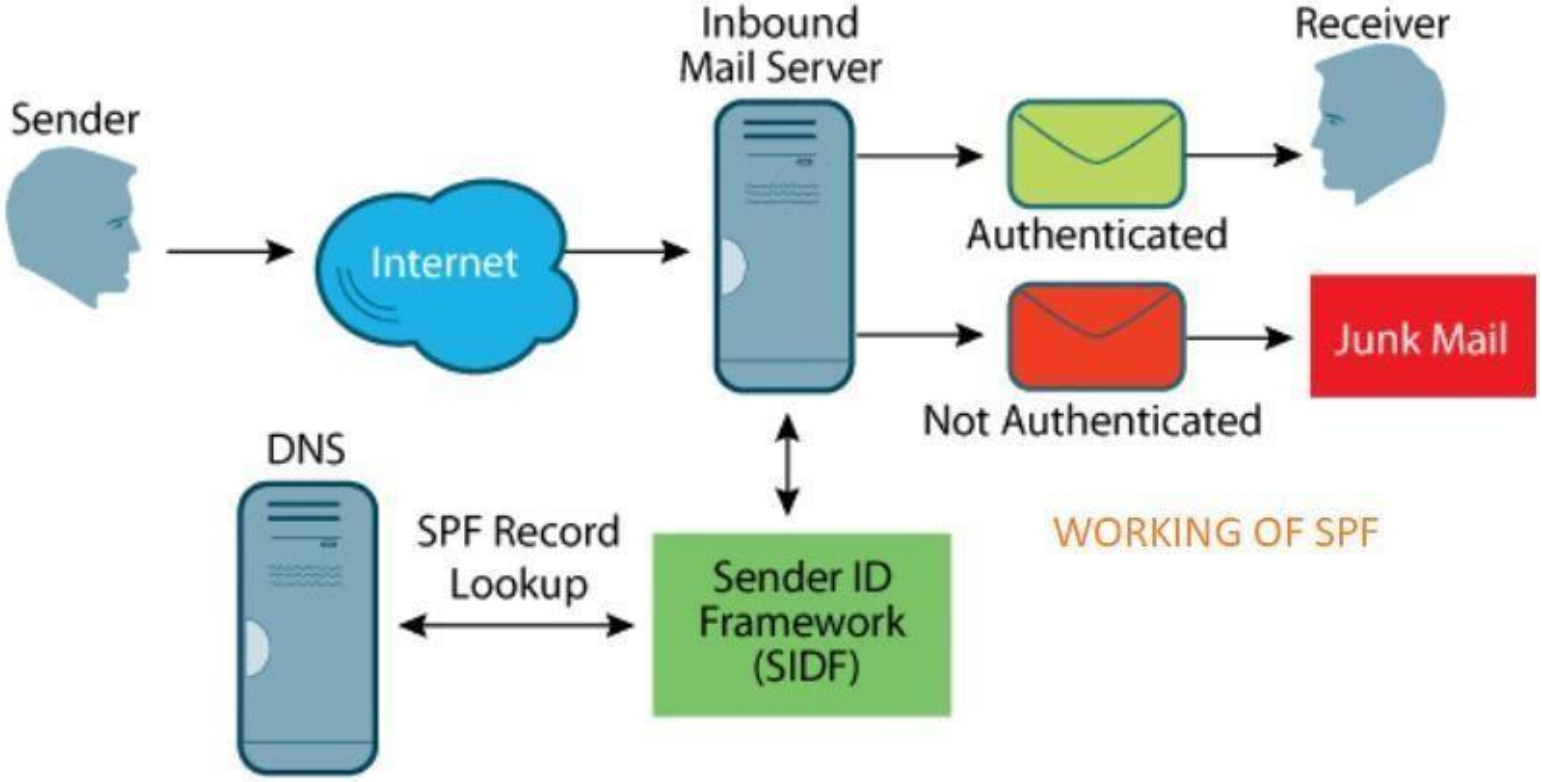
You can implement the following countermeasures on your e-mail server to disable or at least control SMTP relaying:

Disable SMTP relay on your e-mail server. If you don't know whether you need SMTP relay, you probably don't. You can enable SMTP relay for specific hosts on the server or within your firewall configuration.

Enforce authentication if your e-mail server allows it. You might be able to require password authentication on an e-mail address that matches the e-mail server's domain. Check your e-mail server and client documentation for details on setting this up.

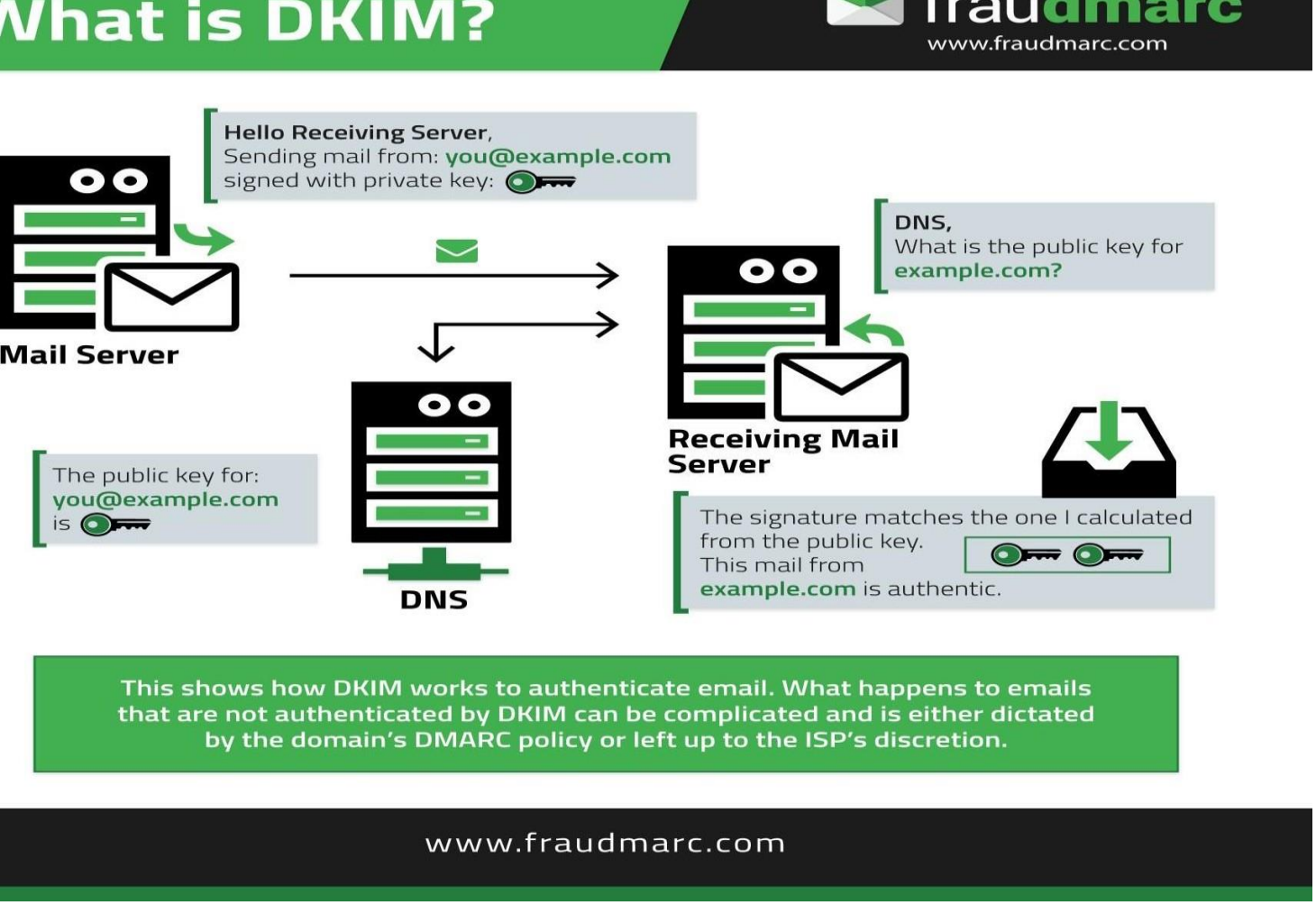
Sender policy framwork

Sender Policy Framework(SPF)



What is SPF? https://dmarcian.com/what-is-spf/

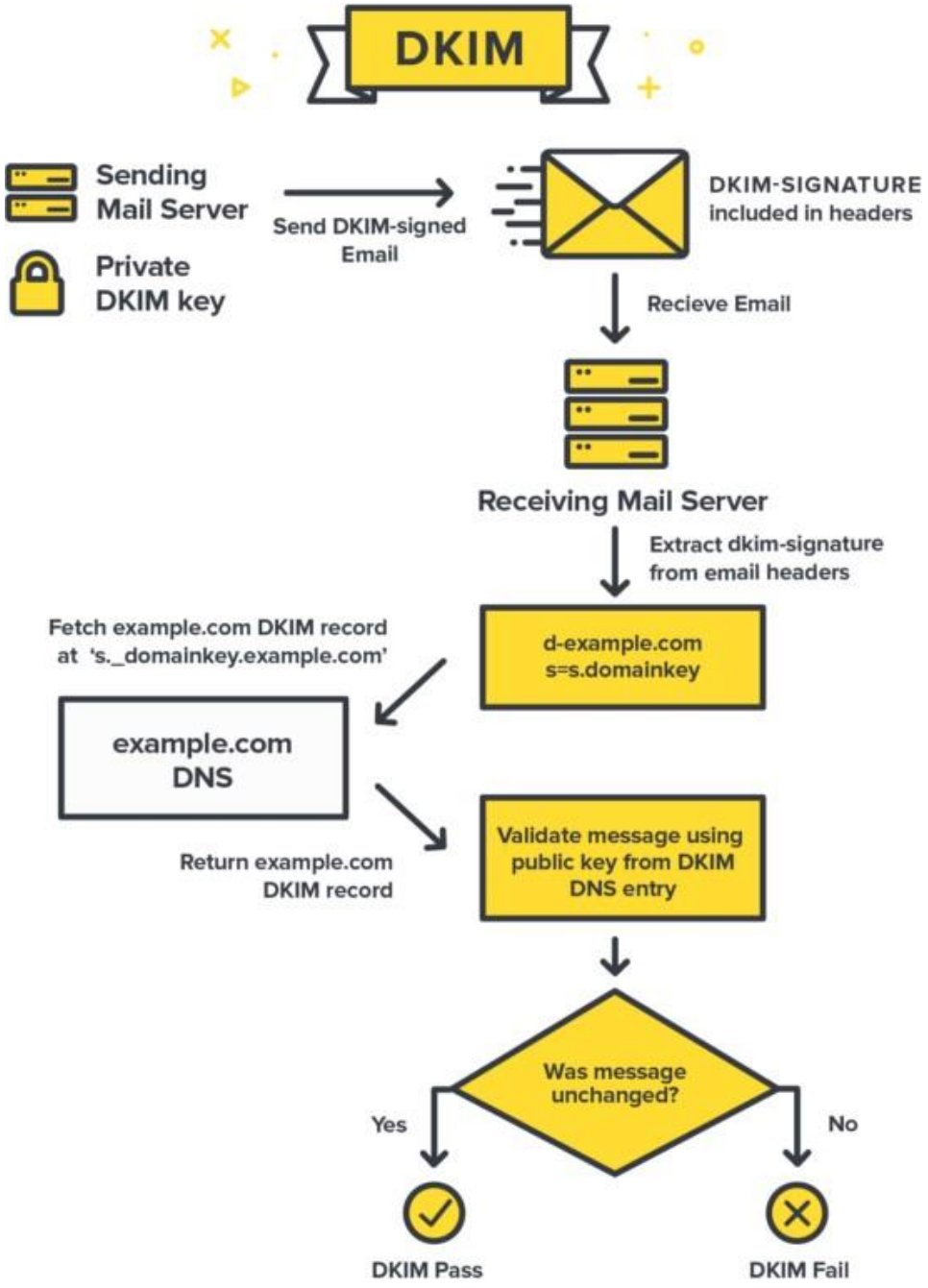
Sender **P**olicy **F**ramework (SPF) is used to authenticate the sender of an email. With an SPF record in place, Internet Service Providers can verify that a mail server is authorized to send email for a specific domain. An SPF record is a DNS TXT record containing a list of the IP addresses that are allowed to send email on behalf of your domain



DKIM (Domain Keys Identified Mail) is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain. This is done by giving the email a digital signature. This DKIM signature is a header that is added to the message and is secured with encryption.

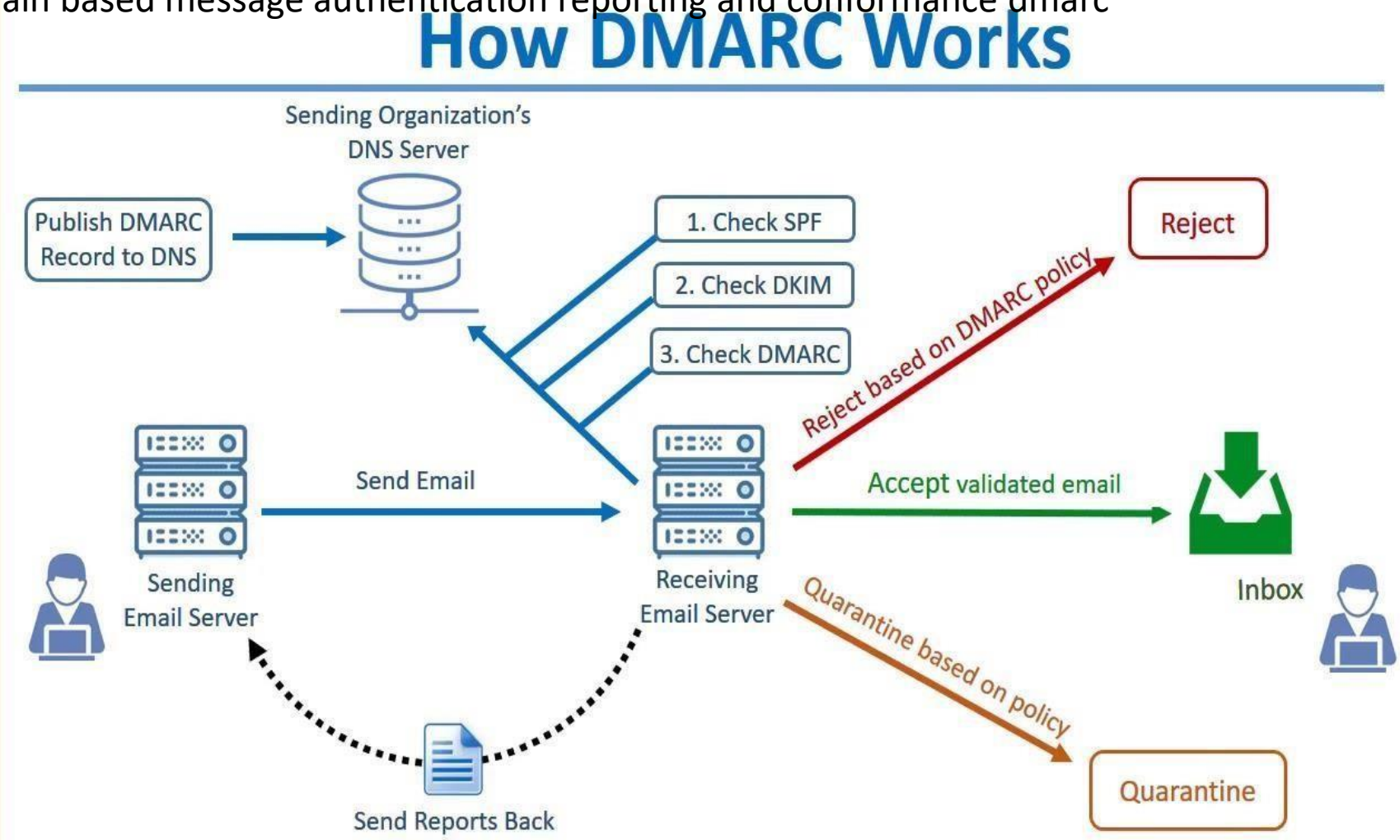
Once receiver (or receiving system) determines that an email is signed with a valid DKIM signature, it's certain that parts of the email among which the message body and attachments haven't been modified. Usually, DKIM signatures are not visible to end-users, the validation is done on a server level.

https://postmarkapp.com/guides/dkim#why-is-a-dkim-record-important



Domain-based Message Authentication, Reporting and Conformance(DMARC)

Domain based message authentication reporting and conformance dmarc



How DMARC prevents spoofing

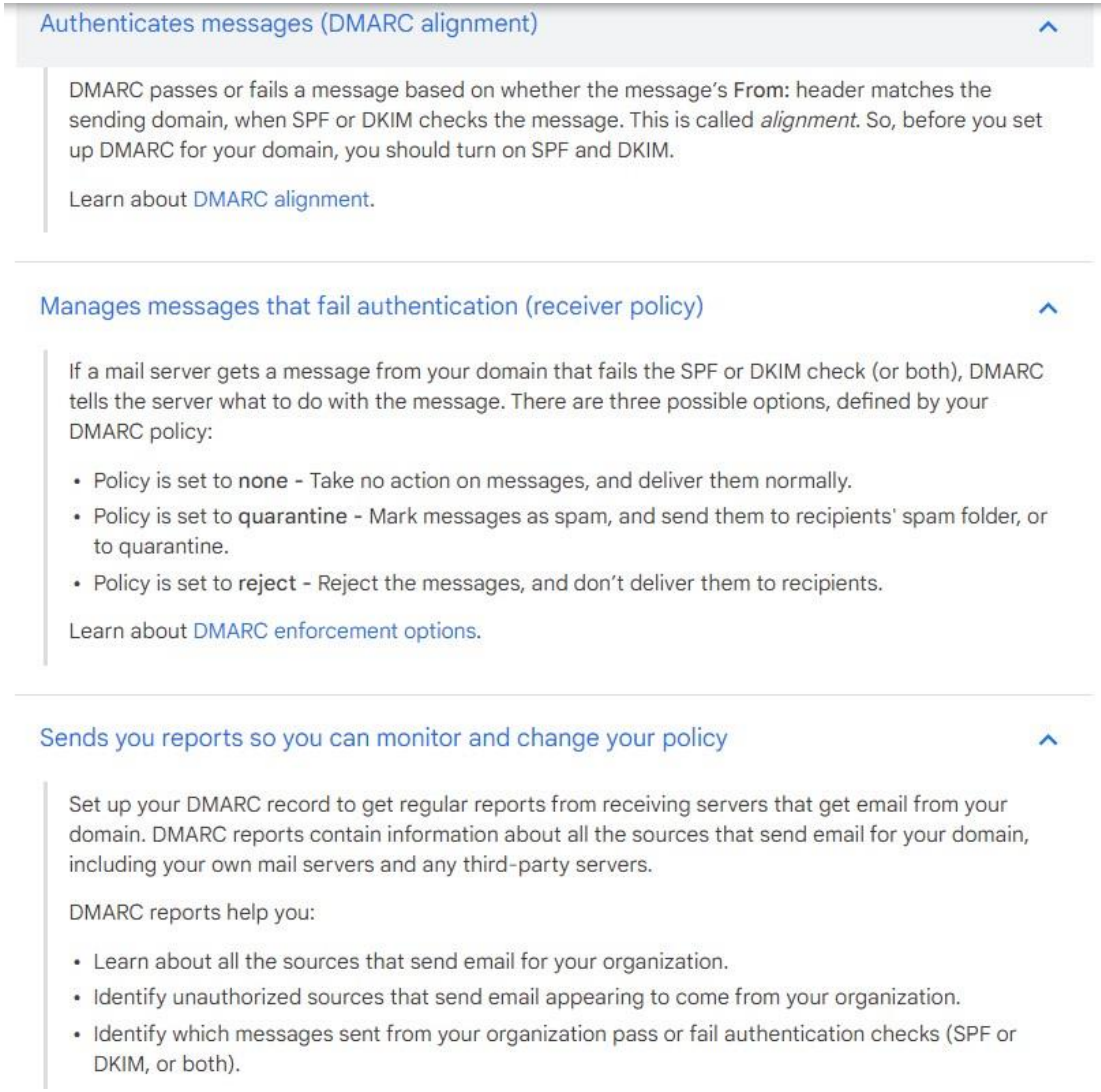
DMARC tells receiving mail servers what to do when they get a message that appears to be from your organization, but doesn't pass authentication checks, or doesn’t meet the authentication requirements in your DMARC policy record.

Messages that aren't authenticated might be impersonating your organization, or might be sent from unauthorized servers.

DMARC is always used with these two email authentication methods or checks:

•Sender Policy Framework (SPF) lets the domain owner authorize IP addresses that are allowed to send email for the domain. Receiving servers can verify that messages appearing to come from a specific domain are sent from servers allowed by the domain owner.

•Domain Keys Identified Mail (DKIM) adds a digital signature to every sent message. Receiving servers use the signature to verify messages are authentic, and weren't forged or changed during transit.



Authenticates messages (DMARC alignment)

DMARC passes or fails a message based on whether the message’s **From:** header matches the sending domain, when SPF or DKIM checks the message. This is called *alignment*. So, before you set up DMARC for your domain, you should turn on SPF and DKIM.

Learn about DMARC alignment.

Manages messages that fail authentication (receiver policy)

If a mail server gets a message from your domain that fails the SPF or DKIM check (or both), DMARC tells the server what to do with the message. There are three possible options, defined by your DMARC policy:

- Policy is set to **none** - Take no action on messages, and deliver them normally.
- Policy is set to **quarantine** - Mark messages as spam, and send them to recipients' spam folder, or to quarantine.
- Policy is set to **reject** - Reject the messages, and don’t deliver them to recipients.

Learn about DMARC enforcement options.

Sends you reports so you can monitor and change your policy

Set up your DMARC record to get regular reports from receiving servers that get email from your domain. DMARC reports contain information about all the sources that send email for your domain, including your own mail servers and any third-party servers.

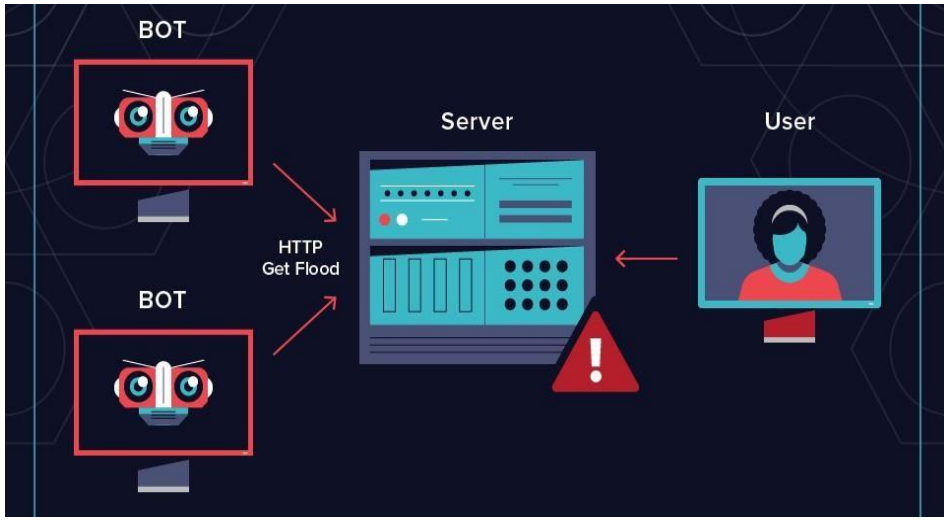
DMARC reports help you:

- Learn about all the sources that send email for your organization.
- Identify unauthorized sources that send email appearing to come from your organization.
- Identify which messages sent from your organization pass or fail authentication checks (SPF or DKIM, or both).

https://support.google.com/a/answer/2466580?hl=en#zippy=%2Cmanages-messages-that-fail-authentication-receiver-policy%2Csends-you-reports-so-you-can-monitor-and-change-your-policy%2Cauthenticates-messages-dmarc-alignment

What is an HTTP flood DDoS Attack?

- An HTTP flood attack is a type of volumetric distributed denial-of-service(DDoS) attack designed to **overwhelm a targeted server with HTTPrequests.**
- Once the target has been **saturated with requests** and is unable to respond to normal traffic, denial-of-service will occur for additional requests from actual users.
- An HTTP flood attack utilizes what appear to be **legitimate HTTP GET or POST requests** to attack a web server or application. These flooding attacks often rely on a **botnet**, which is a group of Internet-connected computers that have been maliciously appropriated through the use

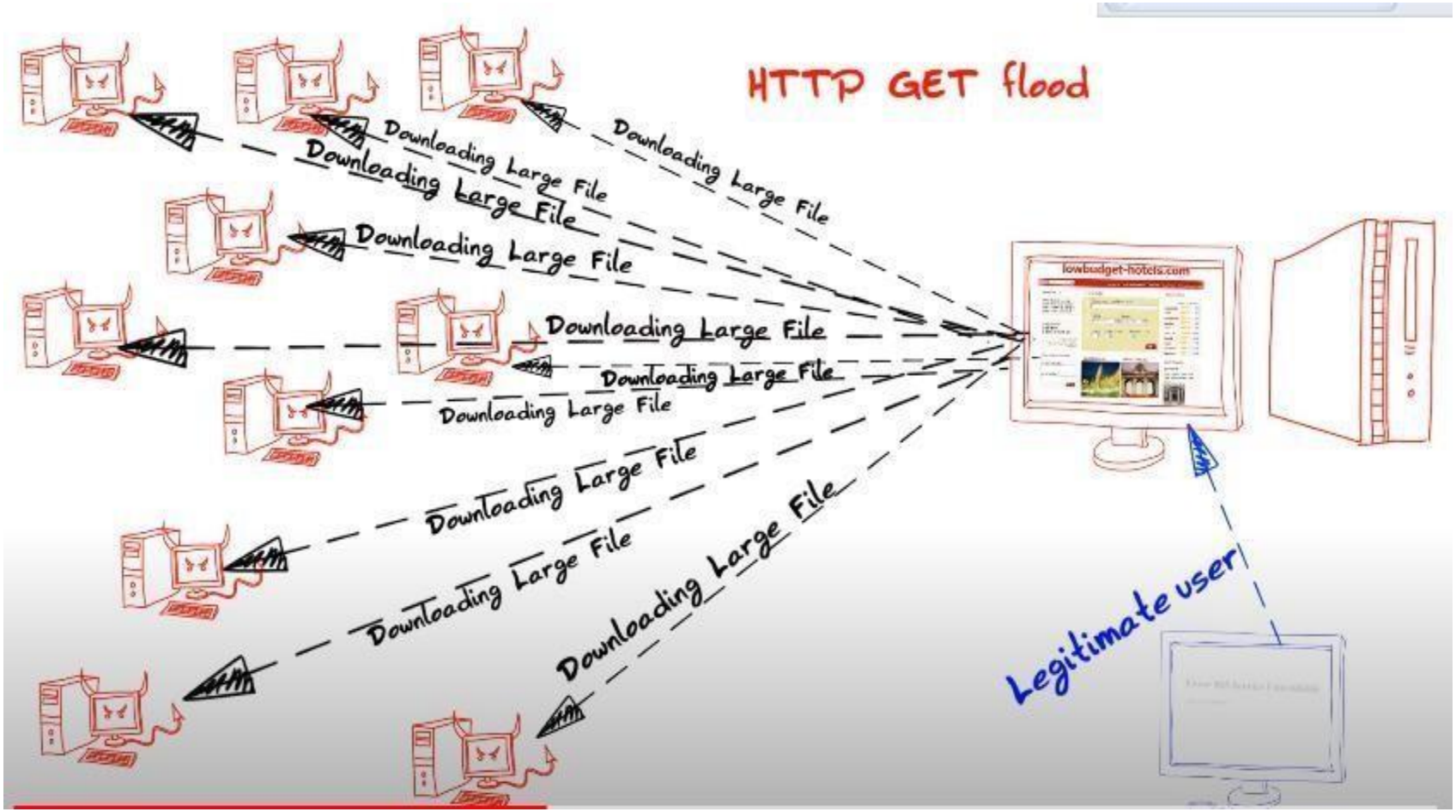


How does an HTTP flood attack work?

- HTTP is the basis of browser-based internet requests, and is commonly used to load webpages or to send form contents over the Internet. Mitigating application layer attacks is particularly complex, as the malicious traffic is difficult to distinguish from normal traffic.
- In order to achieve maximum efficiency, malicious actors will commonly employ or create botnets in order to maximize the impact of their attack

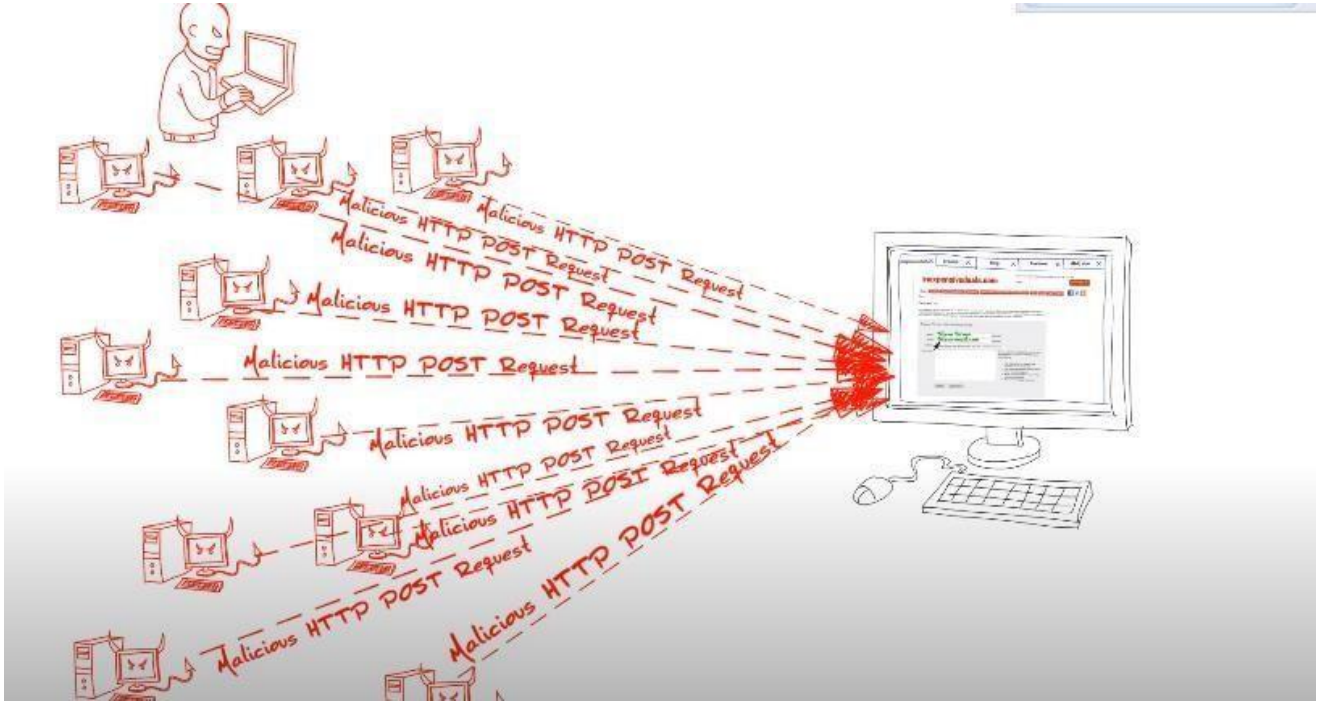
HTTP Get Attack

- In HTTP GET Attack, multiple computers or other devices are coordinated to send multiple requests for images, files, or some other asset from a targeted server. When the target is inundated with incoming requests and responses, denial-of-service will occur to additional requests from legitimate traffic sources.

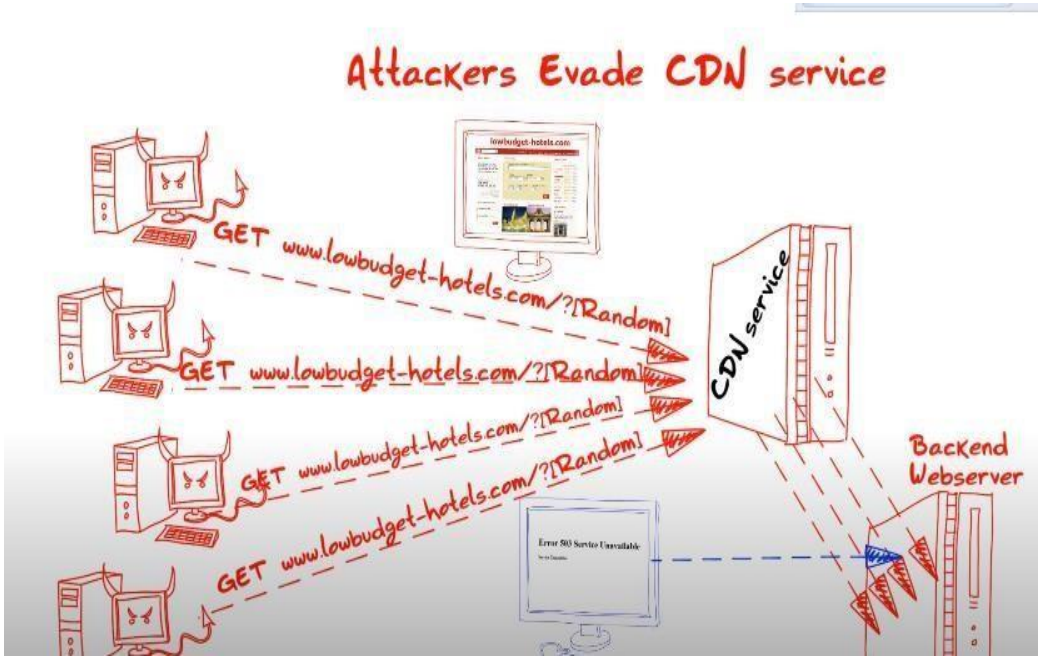


HTTP POST Attack

- Typically when a form is submitted on a website, the server must handle the incoming request and push the data into a persistence layer, most often a database.
- The process of handling the form data and running the necessary database commands is relatively intensive compared to the amount of processing power and bandwidth required to send the POST request.
- This attack utilizes the disparity in relative resource consumption, by sending many post requests directly to a targeted server until it's capacity is saturated and denial-of-service occurs.



HTTP POST Attack



Defence Mechanism for HTTP flood attack

- **implement a challenge** to the requesting machine in order to test whether or not it is a bot, much like a captcha test commonly found when creating an account online. By giving a requirement such as a JavaScript computational challenge, many attacks can be mitigated.
- use of a **web application firewall (WAF),** managing an IP reputation database in order to track and selectively block malicious traffic, and on-the-fly analysis by engineers. Having an advantage of scale with over 20million Internet properties allows Cloud flare the ability to analyze traffic from a variety of sources.
- Since traffic volume in HTTP flooding attacks is generally below detection thresholds, standard rate-based detection is ineffective at detecting these attacks.
- A better approach is a combination of **traffic profiling techniques**, including establishing an IP reputation database so as to **track and block abnormal activity**, and deploying progressive security challenges

Hulk DDoS Tool

- HULK is a Denial of Service (DoS) tool used to attack web servers by generating unique and obfuscated traffic volumes.
- HULK’s generated traffic also bypasses caching engines and hits the server’s direct resource pool.
- This tool is used to test network devices like a firewall.

DNS Spoofing and Cache poisoning

What is DNS cache poisoning?

- 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 cache poisoning is also known as 'DNS spoofing.' IP addresses are the 'room numbers' of the Internet, enabling web traffic to arrive in the right places.
- DNS resolver caches are the 'campus directory,' and when they store faulty information, traffic goes to the wrong places until the cached information is corrected.

  (Note that this does not actually disconnect the real websites from their real IP addresses.)

What do DNS resolvers do?

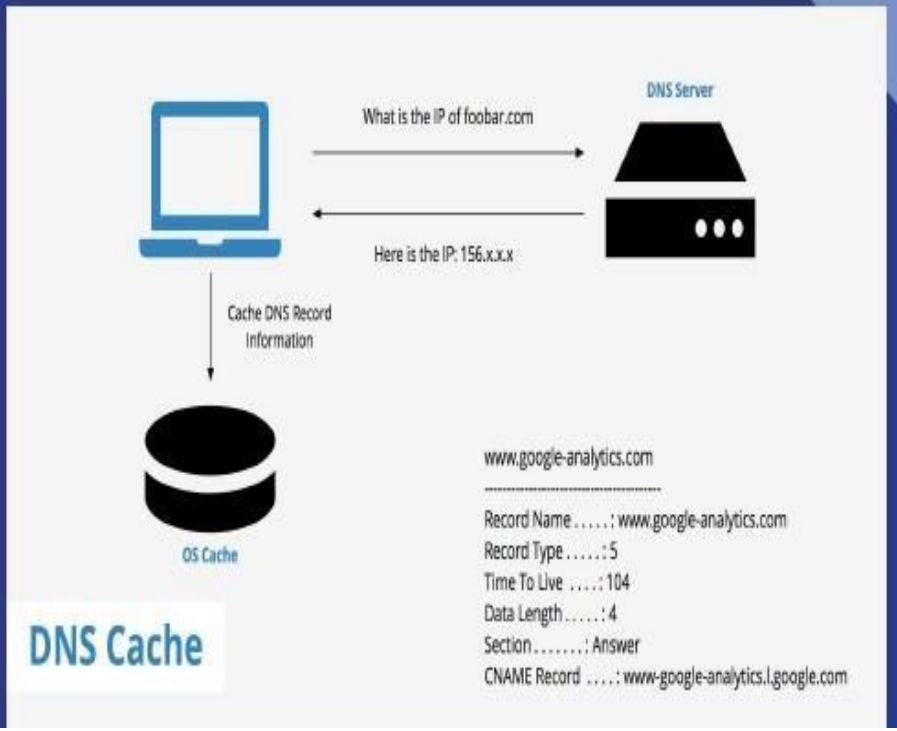
- DNS resolvers provide clients with the IP address that is associated with a domain name. In other words, they take human-readable website addresses like 'vjti.com' and translate them into machine-readable IP addresses.

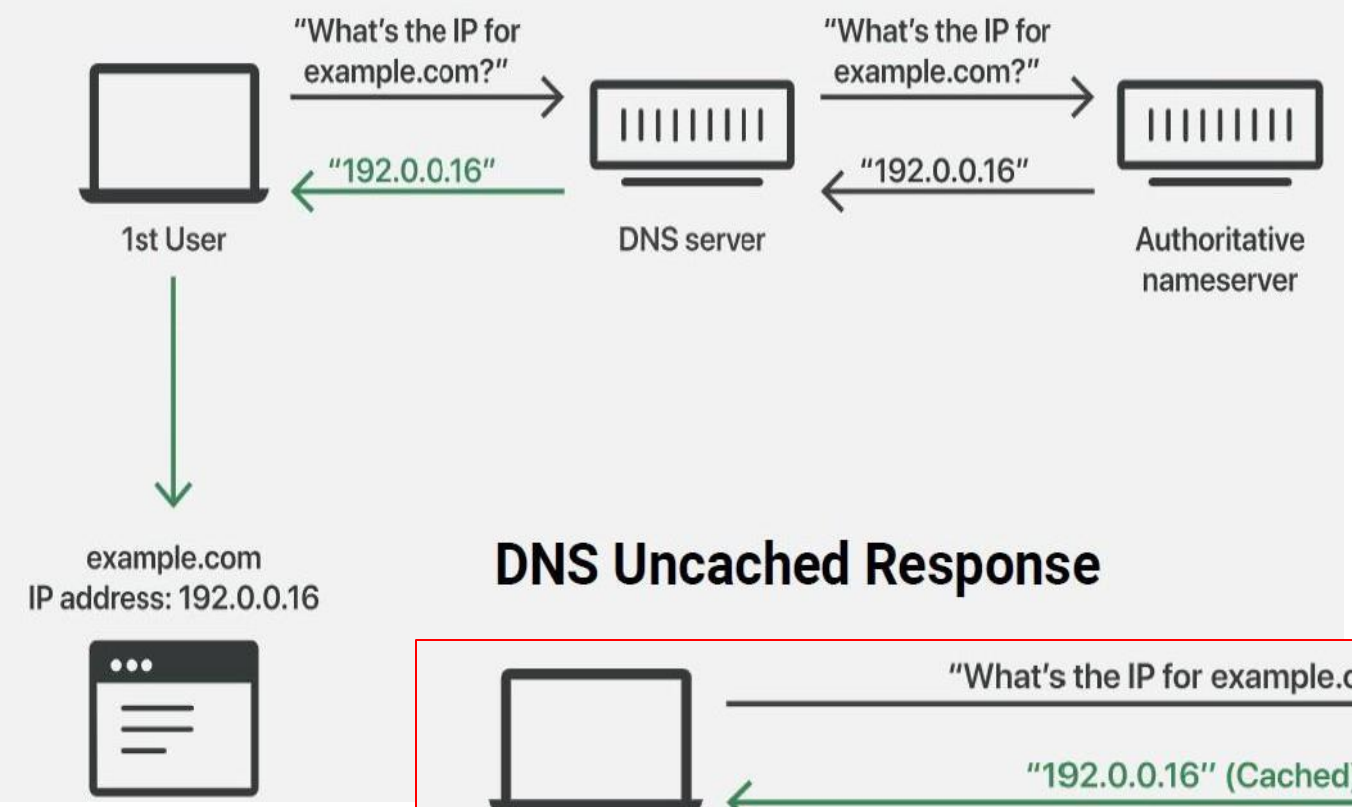
- When a user attempts to navigate to a website, their operating system sends a request to a DNS resolver. The DNS resolver responds with the IP address, and the web browser takes this address and initiates loading the website.

Example
DNS resolution

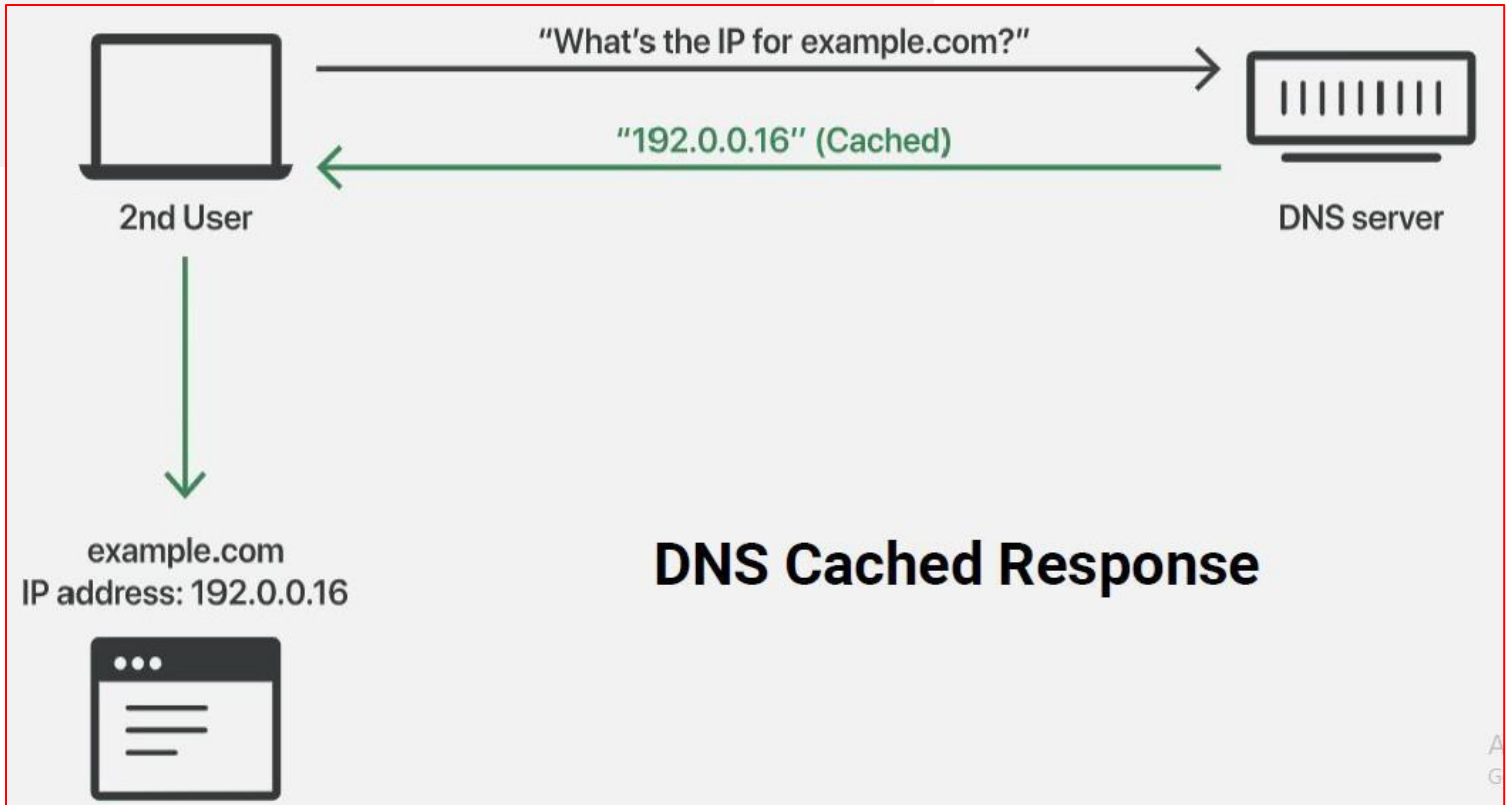
How does DNS caching work?

- A DNS resolver will save responses to IP address queries for a certain amount of time. In this way, the resolver can respond to future queries much more quickly, without needing to communicate with the many servers involved in the typical DNS resolution process.
- DNS resolvers save responses in their cache for as long as the designated time to live (TTL) associated with that IP address allows them to.



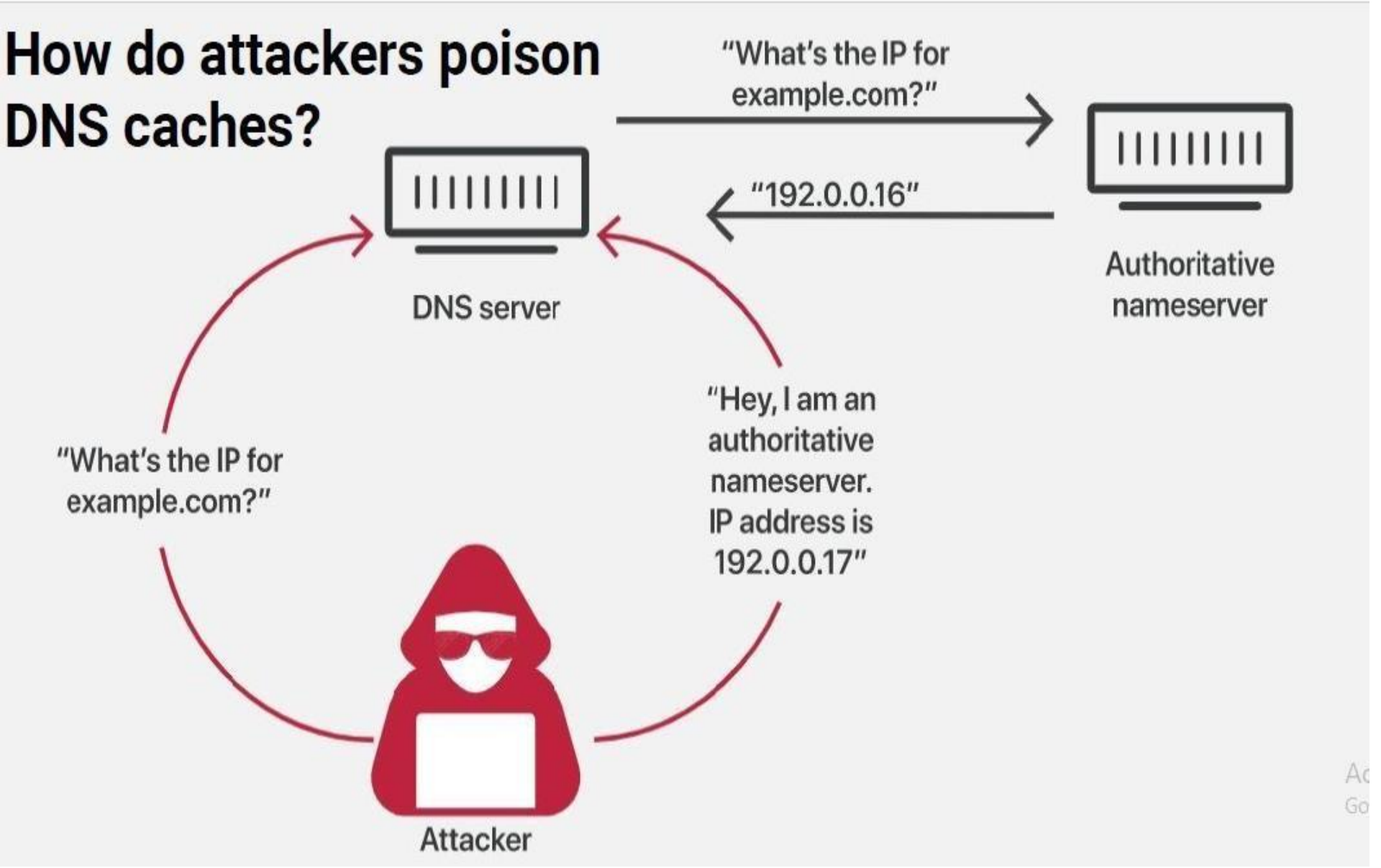


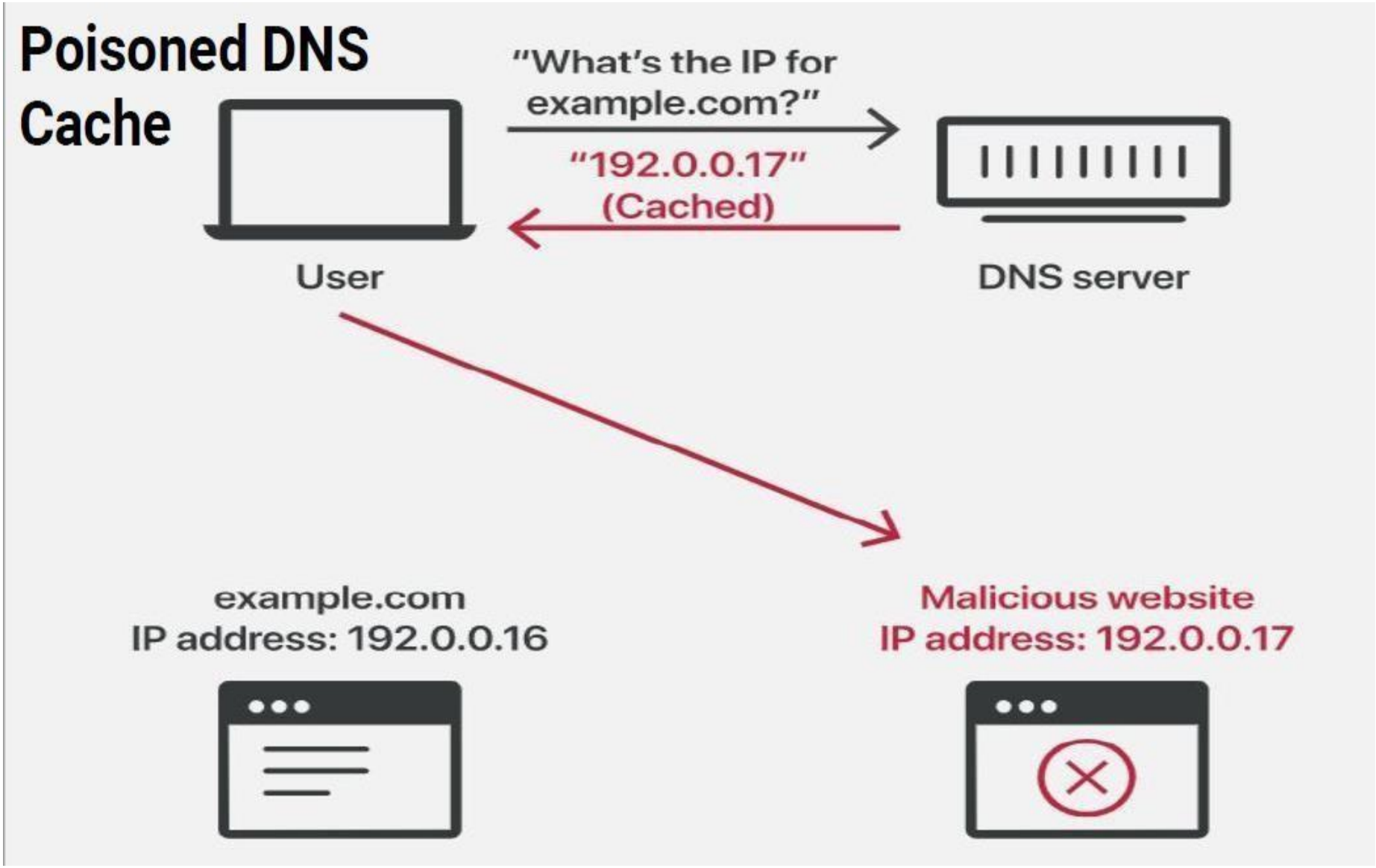
DNS Uncached Response



DNS Cached Response

How do attackers poison DNS caches?




Poisoned DNS Cache
"What's the IP for example.com?"
"192.0.0.17" (Cached)
User
DNS server
example.com
IP address: 192.0.0.16
Malicious website
IP address: 192.0.0.17

Preventing a DNS attack

- **So what can you do to prevent your organization being the victim of a DNS attack?**
- **Keep your resolver private and protected** : If you operate your own resolver, its usage should be restricted to users on your network to help prevent its cache being poisoned by hackers outside your organization. It should not be open to external users. You can check for open resolvers on your network using The Measurement Factory's online tool.
- **Configure it to be as secure as possible against cache poisoning** : Protections built into DNS software to protect against cache poisoning
- include adding **variability to outgoing requests**, to make it harder for a hacker to get a bogus response accepted.
- Manage your DNS servers securely.

DNS Spoofing Demonstration

The demonstration is carried on a LAN network composed of the following three elements:

- Default Gateway (IP address 192.168.224.2)
- Attacker computer (IP address 192.168.224.13)
- Target computer (IP address 192.168.224.211)

The application used to carry out the DNS Spoofing is Ettercap: a free and open source network security tool for man-in-the-middle attacks.

What is File Transfer Protocol (FTP) ?

- File Transfer Protocol(FTP) is an application layer protocol which moves files between local and remote file systems. It runs on the top of TCP, like HTTP.
- For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of control connection. The control connection is initiated on port number 21
- For sending the actual file, FTP makes use of data connection. A data connection is initiated on port number 20.

FTP commands:

How does FTP put security of data at risk?

- FTP was not built to be secure. It is generally considered to be an insecure protocol because it relies on clear-text usernames and passwords for authentication and does not use encryption. Data sent via FTP is vulnerable to sniffing, spoofing, and brute force attacks, among other basic attack methods.

- FTP lacks many of the crucial security, compliance, or workflow needs of today's modern organization.

FTP Exploits by hacker

- Anonymous Authentication:

  FTP weak password and anonymous logon vulnerabilities generally involve an FTP-ready user enabling the anonymous logon functionality, or using a system password that is too short or not complex enough (only containing numbers or letters), which makes the system vulnerable to hacker attacks, unauthorized file uploading, or more serious intrusions.

- Directory Traversal Attack

  Another FTP vulnerability includes directory traversal attacks in which the successful attack overwrites or creates unauthorized files that are stored outside of the web root folder. In turn, the original FTP owner is then subject to the file or directory permissions and controls of the hacker.

- Dridex-based Malware Attack

  Dridex malware targeted Windows users that would open Word or Excel email attachments, which would then cause macros to download the malware and infect the computer, exposing the user to the banking theft. In the latest version of the Dridex malware, the hackers use FTP sites and credentials to avoid detection by email gateways and network policies that trust FTP.

Trivial File Transport Protocol(TFTP)

- TFTP is a stripped back version of FTP.
- It provides very simple way to transfer the files quickly and efficiently
- It uses UDP port 69.
- Features such as authentication and encryption does not exist on TFTP.
- Hence none would want to use it over internet but can very handy in a local network for very basic transfers.
- Example ,you could use to quickly backup a Cisco ios image or a config file.

Then Thereis

- FTPS (FileTransfer protocol secure) Encryption of file usingTLS/SSL.
- SFTP(SSH FileTransferProtocol)
- Using SSH(SecureShell)

Defense Mechanism

Authentication Level:

- The verification of any identity called authentication which also verify the integrity of data. If an individual request generated fo an operation, without knowledge of that individual it is often difficult to decide that either this operation is allowed or not.
- Traditional authentication methods are not suitable for computer networks having sensitive data.
- 2-Factor Authentication

Kerberos

- In traditional networks a user types a password to verify its identity during login phase, this process is called authentication.
- Password based authentication is not a good solution.Because passwords sent across the network and any intruder can intercept these password.
- A strong authentication based c**ryptography'require**d so that intruder could not gain information that will helpful to impersonate him.
- The most common example of this type of authentication is Kerberos, which is based on conventional encryption. It is a distributed authentication service in which server verifies a user without sending information on network.

Same key is used for encryption and decryption

- There is a trusted authority called the **authentication server (AS**)
  –Keeps the secrets
  - Every user shares its private secret key with AS
  –User X doesn't know the private key of user Y
- **Key Distribution**: When X wants to communicate with Y,they need to use a secret key between them
  –AS is responsible for distributing this session key (conversation key) between X and Y
- Everybody has to trust AS

Vulnerabilities in Transport layer

Transport layer uses TCP and UDP protocol.

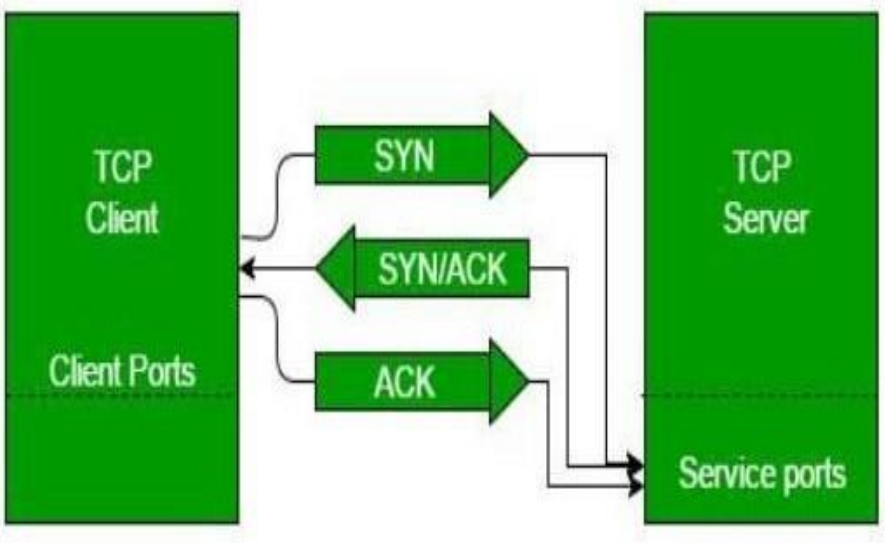
- TCP protocol :It is a connection-oriented protocol ,means the connection established between both the ends of the transmission.
- For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of transmission i.e **3-way handshake protocol.**
- UDP protocol:UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.

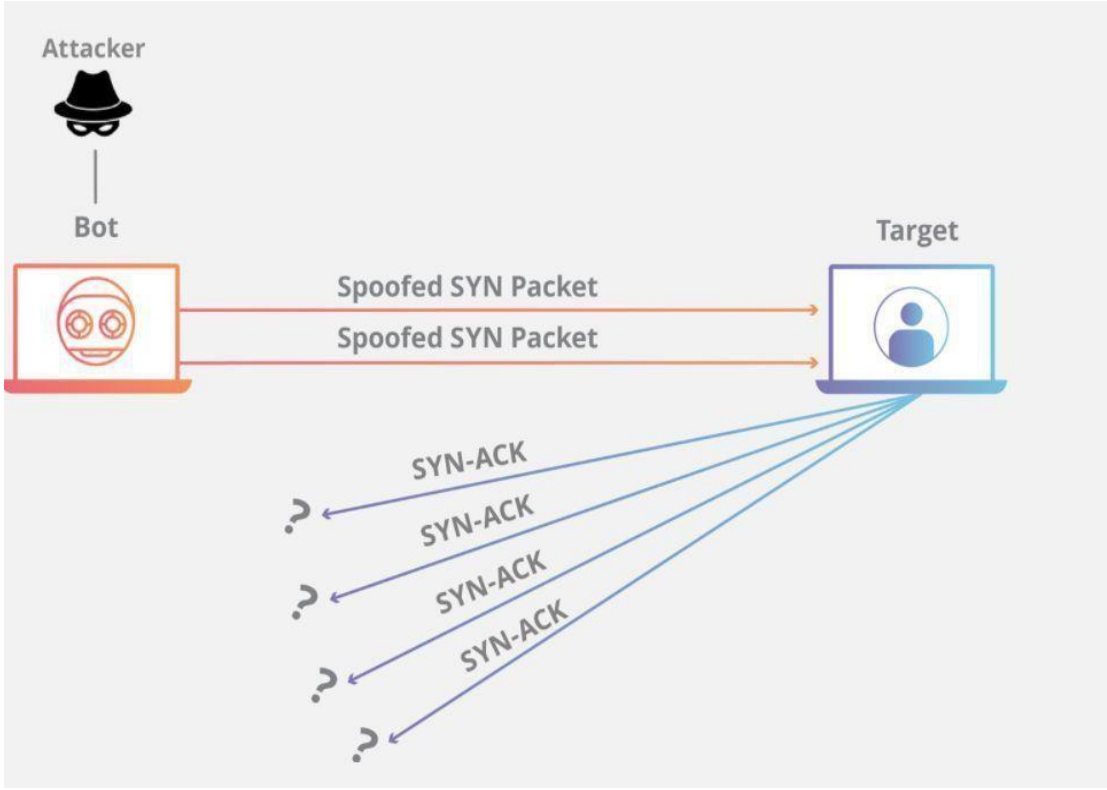
Vulnerabilities and Attacks

- SYN Flooding.
- TCP Session Hijacking.
- TCP Reassembly and Sequencing.
- UDP Flood Attack.

Transport Layer/TCP/3-way Handshake protocol.

- Exploiting the three way handshake protocol in TCP leads to SYN flood attack.





Here's how it works:

- The attacker sends a high volume of SYN packets to the targeted server, often with spoofed IP addresses.
- The server then responds to each one of the connection requests and leaves an open port ready to receive the response.
- 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.
- Receipt of SYN packets creates Transmission Control Block (TCB) data structure.
- TCB's range from 300-1400 bytes depending on OS options etc.
- There is a potential for memory exhaustion DOS
- SYN flood attacks are not intending to use up all of the host's memory, but rather, to exhaust the reserve of open connections connected to a port, from individual and often phony IP addresses.
- SYN floods are often called —half-open attacks because this type of attack intends to send short burst of SYN messages into the ports, leaving insecure connections open and available,often resulting in a complete server crash.

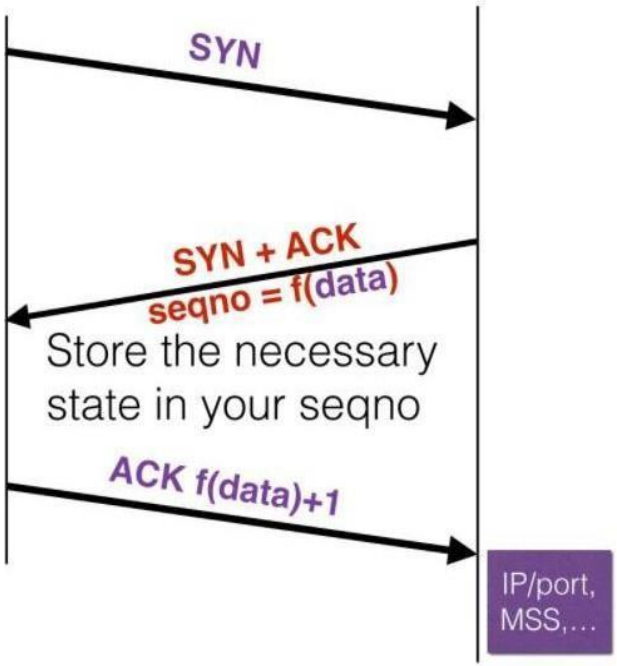
Defense Mechanism for SYN flood

- **Increasing Backlog queue:**

Each operating system on a targeted device has a certain number of half-open connections that it will allow. One response to high volumes of SYN packets is to increase the maximum number of possible half-open connections the operating system will allow.

In order to successfully increase the maximum backlog, the system must reserve additional memory resources to deal with all the new requests. If the system does not have enough memory to be able to handle the increased backlog queue size, system performance will be negatively impacted, but that still may be better than denial-of-service.

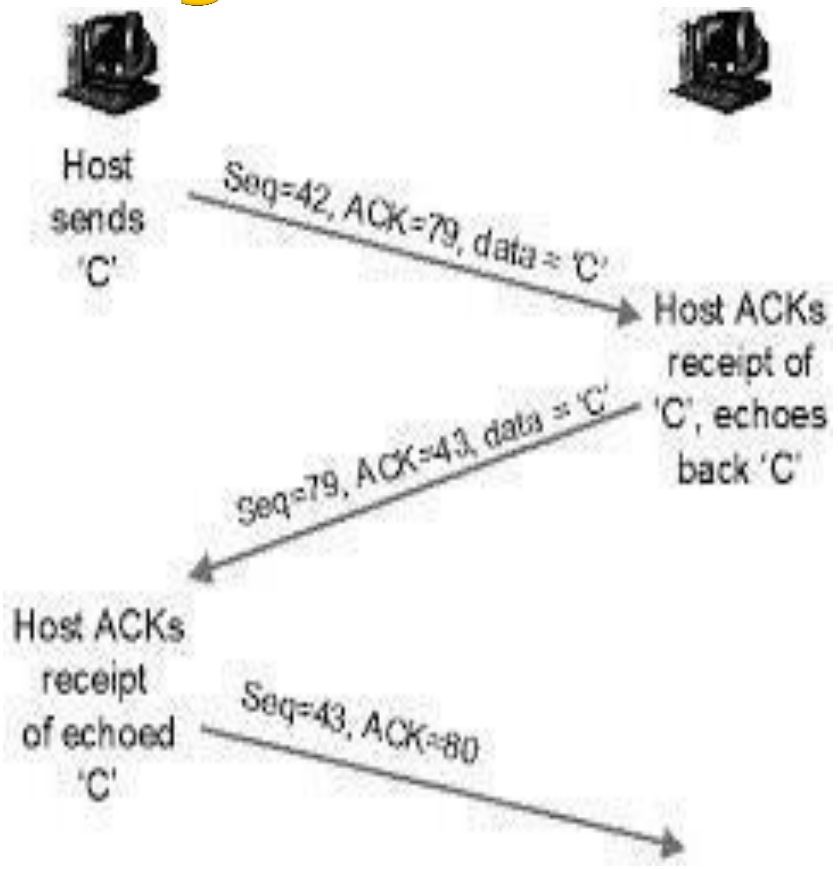
SYN Cookies- Defense



- Rather than store this data, send it to the host who is initiating the connection and have him return it to you
- Check that f(data) is valid for this connection. Only at that point do you allocate state.
- This technique is used to protect the server SYN Queue from filling up under TCP SYN floods.
- The secure hash makes it difficult for the attacker to guess what f() will be, and therefore the attacker cannot guess a correct ACK if he spoofs.

TCP Reassembly and Segmentation

- An attacker can attempt to **guess the sequencing numbers of packets and inject malicious packets into the network destined for the target.**

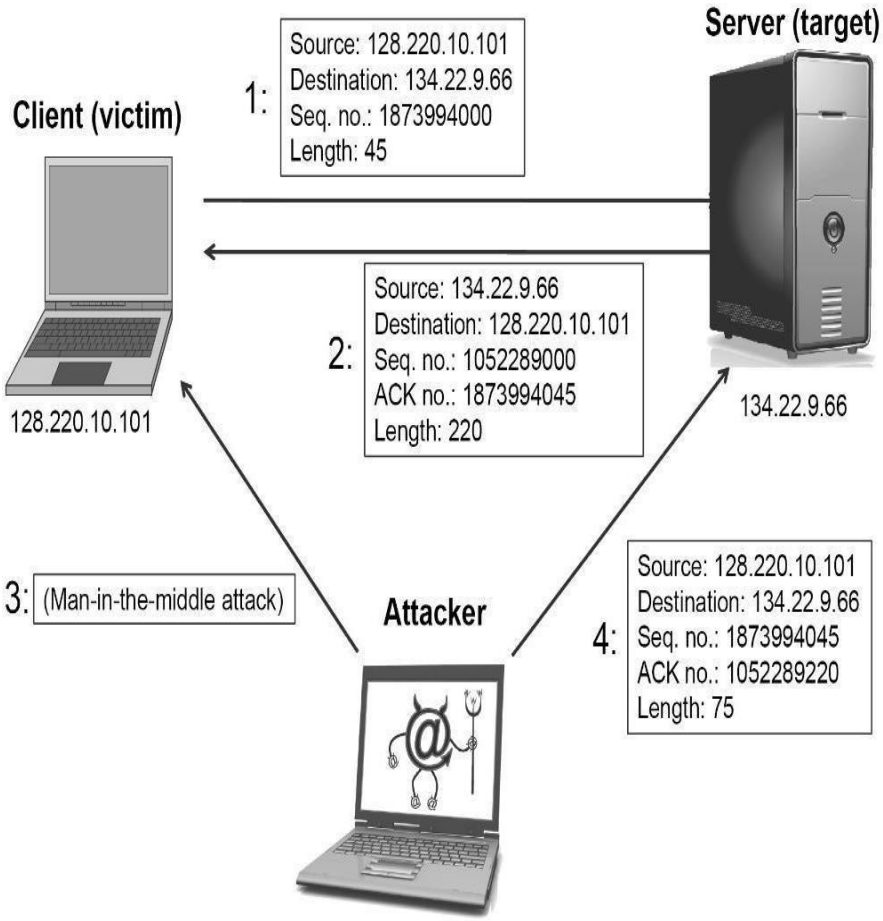


Defense

- Theoretically, **other information such as timing differences or information from lower protocol** layers could allow the receiving host to distinguish authentic TCP packets from the sending host and counterfeit TCP packets with the correct sequence number sent by the attacker.
- Another solution to this type of attack is to **configure any router or firewall to not allow packets to come in from an external source but with an internal IP address.**

TCP Session Hijacking

- Attacker takes over a valid TCP communication session between two computers
- Attacker can sniff all the traffic from the established TCP session.



Defense

- Encryption
- Secure Protocol

UDP Flood Attack

- A UDP flood is a type of denial-of-service attack in which a large number of User Datagram Protocol (UDP) packets are sent to a targeted server with the aim of overwhelming that device's ability to process and respond.

Defense

- Most operating systems **limit the response rate of ICMP** packets in part to disrupt DDoS attacks that require ICMP response.
- One drawback of this type of mitigation is that during an attack legitimate packets may also be filtered in the process.
- If the UDP flood has a volume high enough to saturate the state table of the targeted server's firewall, any mitigation that occurs at the server level will be insufficient as the bottleneck will occur upstream from the targeted device.

Defense Mechanism in Transport layer

Secure Sockets Layer (SSL)

- Developed by Netscape in 1995.
- An encryption-based Internet security protocol.

Transport Layer Security (TLS)

- This protocol designed to facilitate privacy and data security for communications over the Internet. TLS is an improved version of SSL

Vulnerabilities and Attacks in Network Layer

Internet Protocol(IP):

- The **Internet Protocol**(**IP**) is the principal communications protocol in the Internet protocol suite for relaying datagramns across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

- IP has the task of delivering packets from the source host to thedestination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

- The first major version of IP, Internet Protocol Version 4(IPv4), is the dominant protocol of the Internet. Its successor is Internet ProtocolVersion 6(IPv6), which has been in increasing deployment on the public Internet since c. 2006.

IP fragmentation attack

- IP fragmentation attacks are a common form of denial of service attack, in which the **perpetrator overbears a network by exploiting datagram fragmentation mechanisms.**

- Fragmentation is necessary for data transmission, as every network has a unique limit for the size of datagrams that it can process known as the maximum transmission unit (MTU). If a datagram is being sent that is larger than the receiving server's MTU, it has to be fragmented in order to be transmitted completely.

- These attacks involve the transmission of fraudulent packets that are larger than the network's MTU, (usually ~1500 bytes). As these packets are fake, and are unable to be reassembled, the target server's resources are quickly consumed, resulting in server unavailability.

IP fragmentation Mitigation

- IP fragmentation attacks are mitigated in several different ways, depending on the type and severity of the attack.
- Most mitigation methods ensure that malicious data packets never reach their target destinations. The most common one involves inspecting incoming packets for violations of fragmentation rules (e.g., using a router or a secured proxy).

IP Spoofing

- IP spoofing is the creation of Internet Protocol (IP) packets which have a **modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both.**
- It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.
- IP Spoofing is analogous to an attacker sending a package to someone with the **wrong return address listed**. If the person receiving the package wants to stop the sender from sending packages, blocking all packages from the bogus address will do little good, as the return address is easily changed
- Relatedly, if the receiver wants to respond to the return address, **their response package will go somewhere other than to the real sender**. The ability to spoof the addresses of packets is a core vulnerability exploited by many DDoS attacks.
- Spoofing can also be done with the aim of masquerading as another device in order to sidestep authentication and gain access to or —hijack a user's session.

IP Spoofing Mitigation

- While IP spoofing can't be prevented, measures can be taken to stop spoofed packets from infiltrating a network.
- A very common defense against spoofing is **ingress filtering**. Ingress filtering is a form of packet filtering usually implemented on a network edge device which examines incoming IP packets and looks at their source headers.
- If the source headers on those packets don't match their origin or they otherwise look fishy, the packets are rejected.
- Some networks will also implement **egress filtering**, which looks at IP packets exiting the network, ensuring that those packets have legitimate source headers to prevent someone within the network from launching an outbound malicious attack using IP spoofing.

Internet Control Message Protocol(ICMP)

- The **Internet Control Message Protocol(ICMP)** is a supporting protocolin the Internet protocol suite.
- It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address
- For example, an error is indicated when a requested service is not available or that a host or router could not be reached.

Ping Flood Attack

- A ping flood is a denial-of-service attack in which the attacker attempts to **overwhelm a targeted device with ICMP echo-request packets**, causing the target to become inaccessible to normal traffic.
- ICMP echo-request and echo-reply messages are used to ping a network device for the purpose of diagnosing the health and connectivity of the device and the connection between the sender and the device.
- This attack can be broken down in 2 repeating steps:
  - The attacker sends many **ICMP echo request** packets to the targeted server using multiple devices.
  - The targeted server then **sends an ICMP echo reply** packet to each requesting device's IP address as a response.
  - The damaging effect of a Ping Flood is directly proportional to the number of requests made to the targeted server.

Ping Flood Attack Mitigation

- Disabling a ping flood is most easily accomplished by disabling the ICMP functionality of the targeted router, computer or other device.
- A network administrator can access the administrative interface of the device and disable its ability to send and receive any requests using the ICMP, effectively eliminating both the processing of the request and the Echo Reply.
- The consequence of this is that all network activities that involve ICMP are disabled, making the device unresponsive to ping requests, trace route requests, and other network activities.

Smurf Attack

- A Smurf attack is a distributed denial-of-service (DDoS) attack in which an attacker **attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets.**

  By making requests with the spoofed IP address of the targeted device to one or more computer networks, the computer networks then respond to the targeted server, amplifying the initial attack traffic and potentially overwhelming the target, rendering it inaccessible.

- This type of DDoS attack can be thought of metaphorically as a prankster calling an office manager and pretending to be the company's CEO. The prankster asks the manager to tell each employee to call the executive back on his private number and give him an update on how they're doing. The prankster gives the callback number of a targeted victim, who then receives as many unwanted phone calls as there are people in the office.

Smurf Attack Mitigation

- Several mitigation strategies for this attack vector have been developed and implemented over the years, and the exploit is largely considered solved. On a limited number of legacy systems, mitigation techniques may still need to be applied.
- A simple solution is to **disable IP broadcastingaddresses at each network router and firewall.** Older routers are likely to enable broadcasting by default, while newer routers will likely already have it disabled.

Ping of Death

- A Ping of Death attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by **sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash**.
- When a maliciously large packet is transmitted from the attacker to the target, the packet becomes **fragmented into segments, each of which is below the maximum size limit.**
- When the target machine attempts to put the pieces back together, the total **exceeds the size limit and a buffer overflow can occur**, causing the target machine to freeze, crash or reboot.
- **While ICMP echo can be used for this attack, anything that sends an IP datagram can be used for this exploit. That includes TCP, UDP and IPX transmissions**.

MITIGATION

- One solution to stop an attack is to add checks to the reassembly process to make sure the maximum packet size constraint will not be exceeded after packet recombination.
- Another solution is to create a memory buffer with enough space to handle packets which exceed the guideline maximum.

Internet Group Management Protocol (IGMP)

- The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.
- IGMP is an integral part of IP multicast and allows the network to direct multicast transmissions only to hosts that have requested them.
- IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

IGMP Flood Attack

- An IGMP flood is non-vulnerability based, as IGMPis designed to allow multicast.
- Such floods involve a **large number of IGMP message reports being sent to a network or router, significantly slowing and eventually preventing legitimate traffic from being transmitted across the target network.**

Address Resolution Protocol (ARP)

- The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.
- This mapping is a critical function in the Internet protocol suite.
- The Address Resolution Protocol is a request-response protocol whose messages are encapsulated by a link layer protocol. It is communicated within the boundaries of a single network, never routed across internetworking nodes.

ARP Poisoning (ARP Spoofing) Attack

- ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves **sending malicious ARP packets to a default gateway on a LAN in order tochange the pairings in its IP to MAC address table**. ARP Protocol translates IP addresses into MAC addresses.
- The attack itself consists of an attacker sending a false ARP replymessage to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address (and vice-versa, so his or her target's MAC is now associated with the attacker's IP address).
- Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to itsreal destination.

ARP Cache Poisoning Mitigation

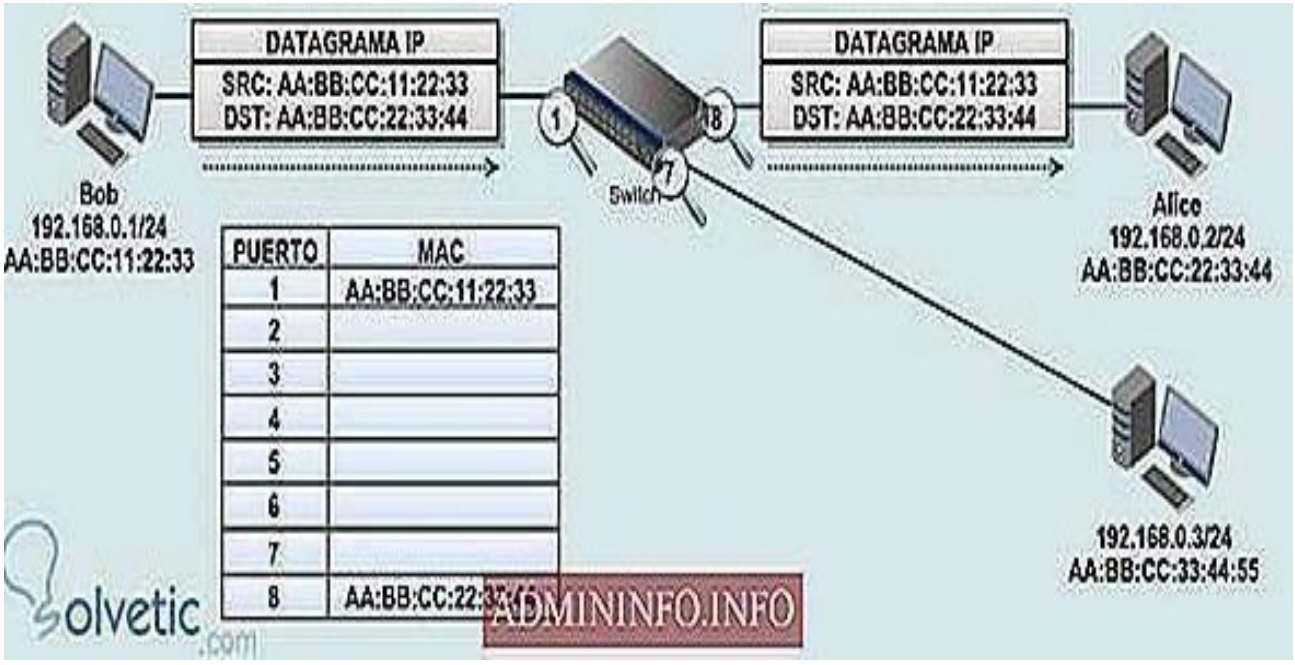
- **Use a Virtual Private Network** (VPN)—a VPN allows devices to connect to the Internet through an encrypted tunnel. This makes all communication encrypted, and worthless for an ARP spoofing attacker.
- ***Use static ARP***—the ARP protocol lets you define a static ARP entry for an IP address, and prevent devices from listening on ARP responses for that address. For example, if a workstation always connects to the same router, you can define a static ARP entry for that router, preventing an attack.
- ***Use packet filtering***—packet filtering solutions can identify poisoned ARP packets by seeing that they contain **conflicting source information**, and stop them before they reach devices on your network.
- ***Run a spoofing attack***—check if your existing defenses are working by mounting a spoofing attack, in coordination with IT and security teams. If the attack succeeds, identify weak points in your defensive measures and remediate them.

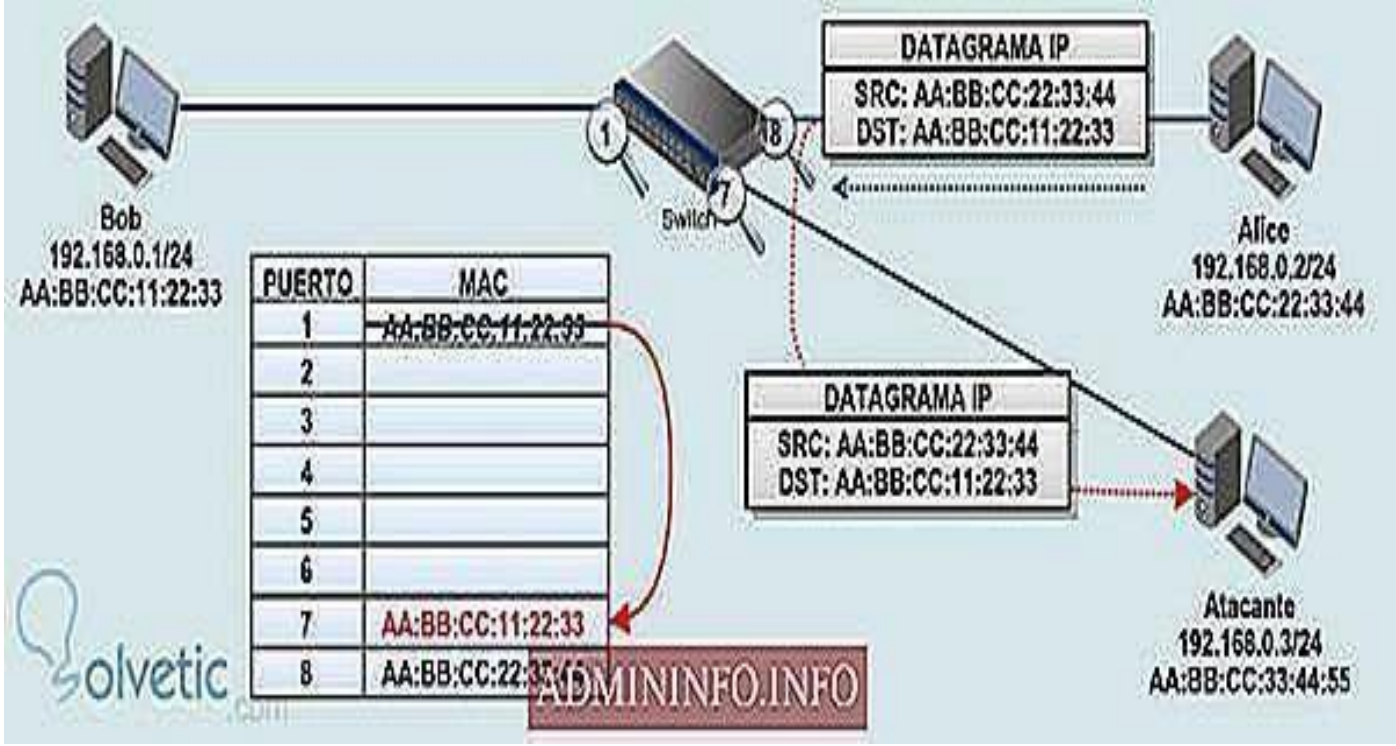
Vulnerabilities and attacks -Data Link layer

- The data link layer is the protocol layer that handles the moving of **data in and out of the physical link layer** of the network.
- **Data bits are encoded, decoded** and organized before they are transported as frames between two nodes on the network.
- The data link layer ensures an **initial connection** has been set up, divides output data into data frames and handles the acknowledgements from a receiver that the data arrived successfully.
- It also ensures **incoming data has been received successfully** by **analyzing bit patterns at special places in the** frames.
- **Frame sequencing capabilities** within the data link layer permit the receiving device to reorder frames that might have been transmitted out of sequence.
- The data link layer also has the **ability to detect congestion**.
- Nearby devices then **transmit congestion information**, so traffic can be rerouted accordingly.
- The data link layer has two sublayers: the logical link control (LLC) sublayer and the media access control (MAC)sublayer

Port Stealing

- Ethernet switches have the ability to learn and bind MAC addresses to ports. When a switch receives traffic from a port with a MAC source address, it binds the port number and that MAC address.
- The port stealing attack exploits this ability of the switches. The attacker floods the switch with forged ARP frames with the target host's MAC address as the source address.
- Switch is fooled to believe that the target host is on port, on which actually an attacker is connected.
- Now all data frames intended for the targeted host are sent to the attacker's switch port and not to the target host.
- Thus, the attacker now receives all the frames which were actually destined only for the target host





- *Systems involved*

Bob AA: BB: CC: 11: 22: 33 (192.168.0.1/24) Alice AA: BB: CC: 22: 33: 44 (192.168.0.2/24) ,Attacker AA: BB: CC: 33: 44: 55 (192.168.0.3/24)

- To apply the *Port Stealing* technique using **arping**, run as root:

 # arping -s MAC_VICTIM IP_DESTINATION -S IP_ORIGIN -i INTERFACE_LAN

Where

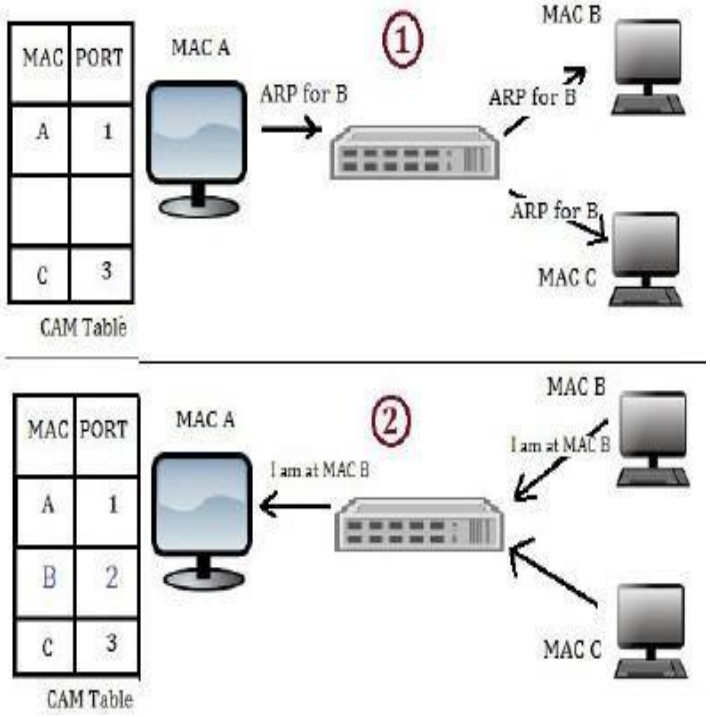
- **MAC_VICTIM: MAC addr of the system that is intended to "steal the port".**
- **IP_DESTINATION: since it is an ARP request message, a destination IP address must be indicated.**
- **IP_ORIGIN: source or sender IP address of the ARP message.**
- **INTERFACE_LAN: name of the network interface to use.**

MAC Flooding Attack

- MAC flooding is one of the most common network attacks.
- It is an attacking method intended to compromise the security of the network switches.

What is CAM Table ?

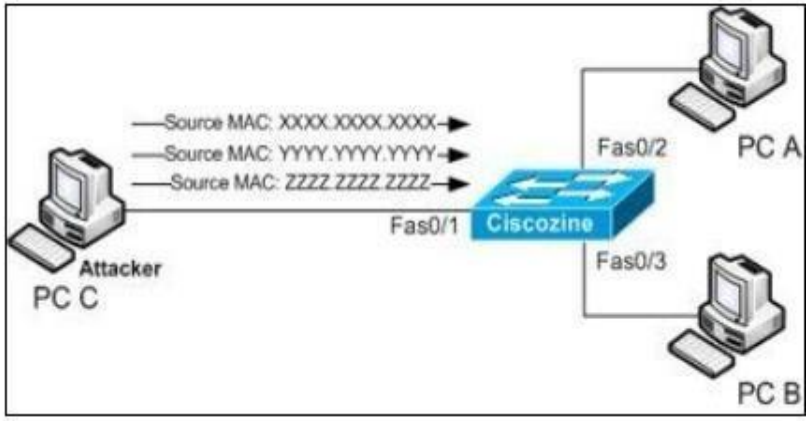
- The CAM Table is stored inside switches and it consists of MAC addresses of the host computers on the network which are connected to ports of the switch.
- This table allows the switches to direct the data out of the ports where the recipient is located.



How does MAC flooding attack works

How does the MAC Flooding Attack Work ?

- The aim of the MAC Flooding is to takedown the MAC Table.
- The attacker sends Ethernet Frames in a huge number with different MAC addresses.
- The intention is to consume the limited memory set aside in the switch. The MAC addresses of legit users will be pushed out of the CAM Table.
- The desired effect by the attacker is to cause significant amount of incoming frames to be flooded out on all ports.
- Now, as the attacker is part of the network, the attacker will also get the data packets intended for the victim machine.



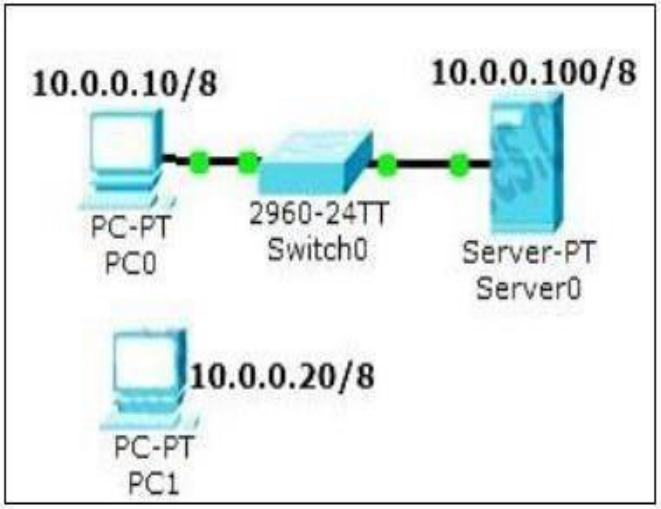
Defense Mechanism

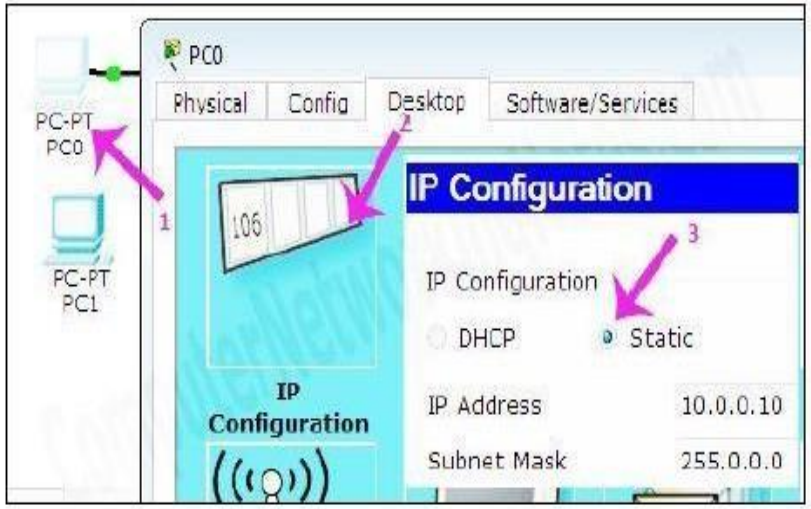
Port Security

User can secure a port in two steps:

- Limiting the number of MAC addresses
- If an unauthorized access is observed, the traffic should be discarded

Create a simple network shown:





DHCP

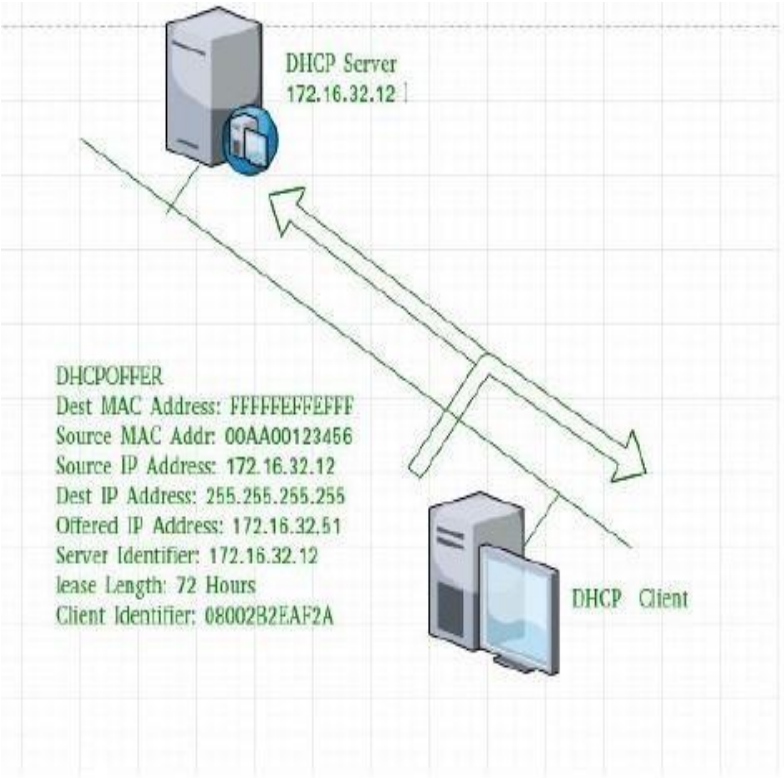
- DHCP states for Dynamic Host Configuration Protocol is a protocol that maintains DHCP Server which Dynamically assigns the IPAddr.
- DHCP Protocol Requires 2 Devices : Server (Router has a built in DHCP Server) Client
- It also provides configuration information such as the subnet mask and default gateway within a network.

DHCP Process

- DHCP port number for server is 67 and for the client is 68.
- It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses.
- In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection,

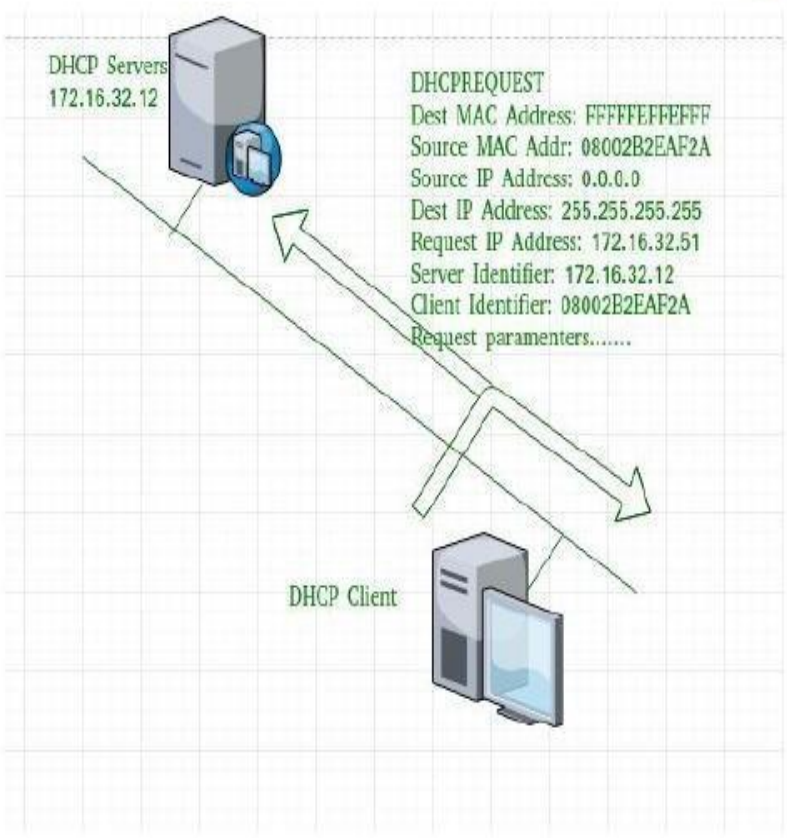
1. DHCP Discover message This message is **generated by Client host in order to discover if there is any DHCP server/servers** are present in a network or not. This message is **broadcasted** to all devices present in a network to find the DHCP server.
   - This message is 342 or 576 bytes long

DHCP Offer Message



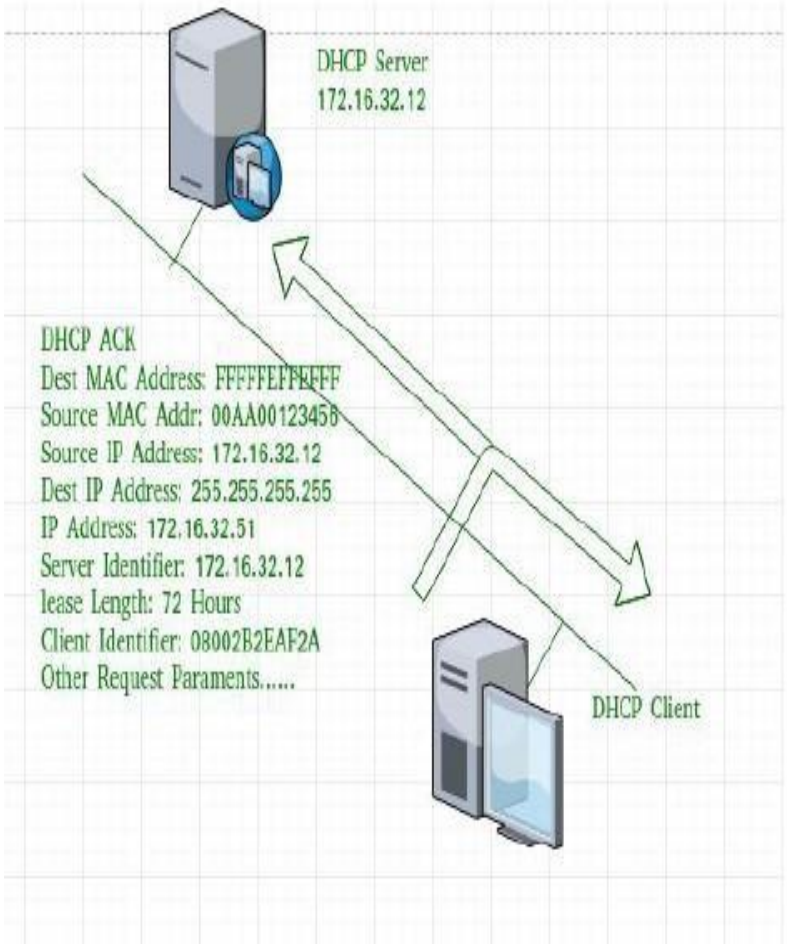
- The server will respond to host in this message specifying the IP address . This message is broadcasted by server.
- Size of message is 342 bytes
- If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives

DHCP Request Message



- When a client receives a offer message, it responds by broadcasting a DHCP request message.
- The client will produce ARP in order to find if there is any other host present in the network with same IP address.
- With this message the host expresses its intention to accept the given ip address.

DHCP Acknowledgement message



- In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time.

- Now, the client will have the IP address provided by server.

DHCP Attacks

- There are 2 Types of DHCP Attacks :
- ***Starvation:*** It is an Attack in which an **Attacker Broadcasts large Number of DHCP Requests Packets with some spoofed MAC Address.**
- The entire range of available IP addresses are allotted to a single device.
- This makes it almost impossible for new devices to connect to a network and obtain IP address.

Solution: Switch can limit number of MAC addresses per port (Port security)
– Important to check the DHCP payload also

- ***Spoofing***
- The client may get an offer from the real DHCP server, but in addition it may also get an offer from a rogue DHCP server and it may accept that offer.
- When a client requests an IP address from a DHCP server, the client has no reassurance that the server is legitimate. In addition, the server has no way of knowing that the client requesting the address is a legitimate client on the network.
- It can cause serious problems as they may be used in **a Man in the Middle attack**.
- The attacker configures the rogue server with bogus DNS server and default gateway IP addresses to misdirect traffic to other rogue devices.

Solution: Switch configured with trusted ports (DHCP snooping)
– trusted ports can source all DHCP messages
– untrusted ports only requests (DHCP discover/request)