MODULE-5: Network Security

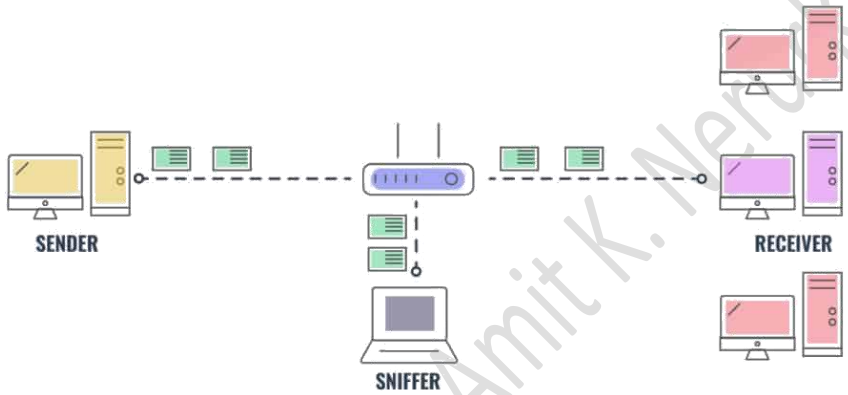
VIT | Vidyalankar Institute of Technology
Accredited A+ by NAAC

Prepared by Prof. Amit K. Nerurkar

Module 5 Network security basics

Packet Sniffing

A packet sniffer — also known as a packet analyzer, protocol analyzer or network analyzer — is a piece of hardware or software used to monitor network traffic. Sniffers work by examining streams of data packets that flow between computers on a network as well as between networked computers and the larger Internet.



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

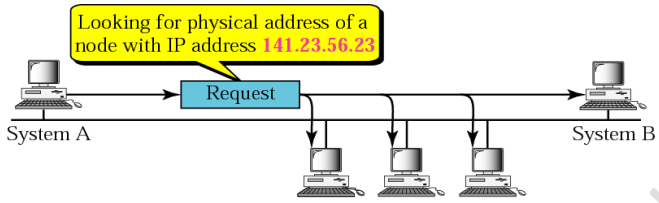
who is receiver of your email
what is content of that email
what you download sites you visit
what you looked on that website
downloads from a site
streaming events like video, audio, etc.

How to prevent packet sniffing –

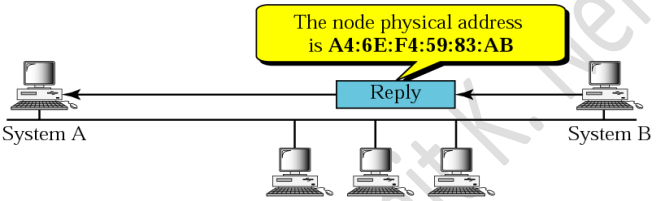
Encrypting data you send or receive.
using trusted Wi-Fi networks.
Scanning your network for dangers or issues.

ARP spoofing

Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address.

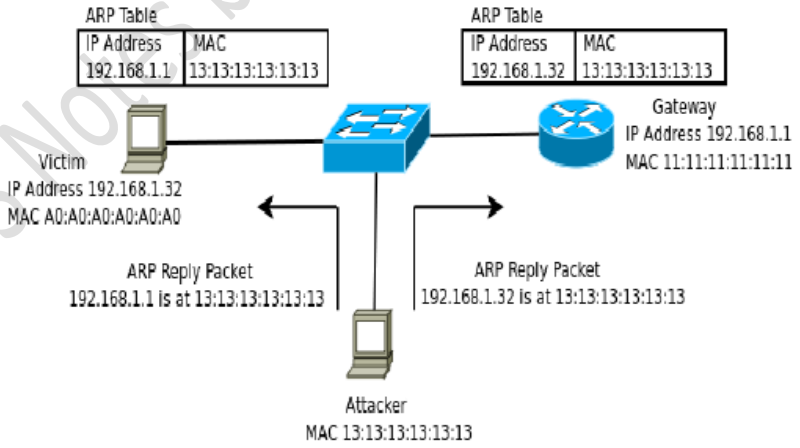


a. ARP request is broadcast



b. ARP reply is unicast

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 to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses.



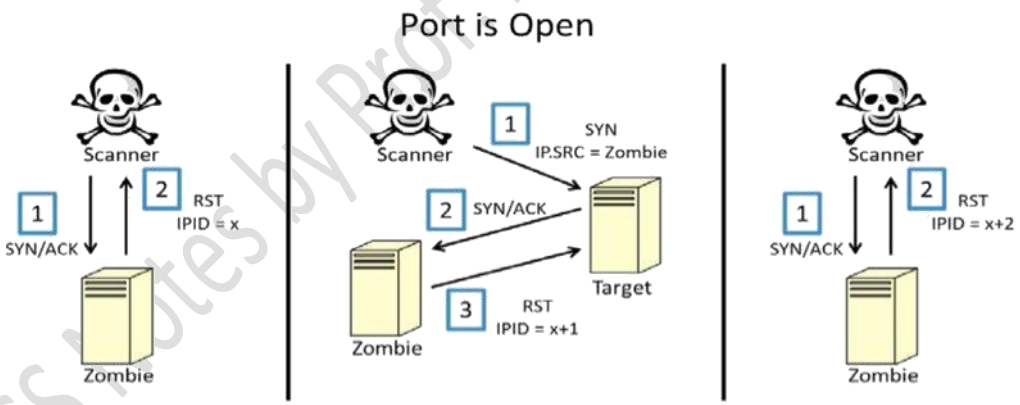
Port scanning

A port scan attack, therefore, occurs when an attacker sends packets to your machine, which can vary the destination port. The attacker can use this to find out what services you are running and to get a pretty good idea of the operating system you have.

A Serious Threat

Any time there are open ports on one's personal computer, there is potential for the loss of data, the occurrence of a virus, and at times, even complete system compromise. It is essential for one to protect his or her virtual files, as new security risks concerning personal computers are discovered every day. Computer protection should be the number one priority for those who use personal computers. Port scanning is considered a serious threat to one's PC, as it can occur without producing any outward signs to the owner that anything dangerous is taking place.

The following diagram shows the interactions that take place when a zombie host is used to scan an open port:

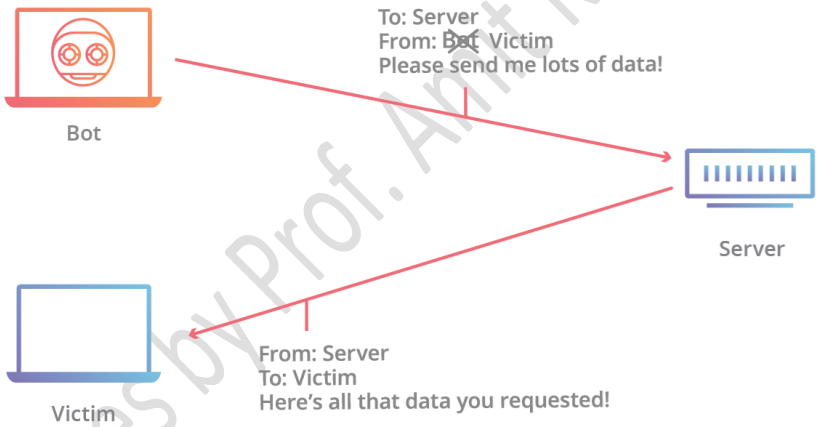


To perform a zombie scan, an initial SYN/ACK request should be sent to the zombie system to determine the current IPID value in the returned RST packet. Then, a spoofed SYN packet is sent to the scan target with a source IP address of the zombie system. If the port is open, the scan target will send a SYN/ACK response back to the zombie. Since the zombie did not actually send the initial SYN request, it will interpret the SYN/ACK response as unsolicited and send an RST packet back to the target, thereby incrementing its IPID by one. Finally, another SYN/ACK packet should be sent to the zombie, which will return an

RST packet and increment the IPID one more time. An IPID that has incremented by two from the initial response is indicative of the fact that all of these events have transpired and that the destination port on the scanned system is open. Alternatively, if the port on the scan target is closed, a different series of events will transpire, which will only cause the final RST response IPID value to increment by one.

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.



Sending and receiving IP packets is a primary way in which networked computers and other devices communicate, and constitutes the basis of the modern internet. All IP packets contain a header which precedes the body of the packet and contains important routing information, including the source address. In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.

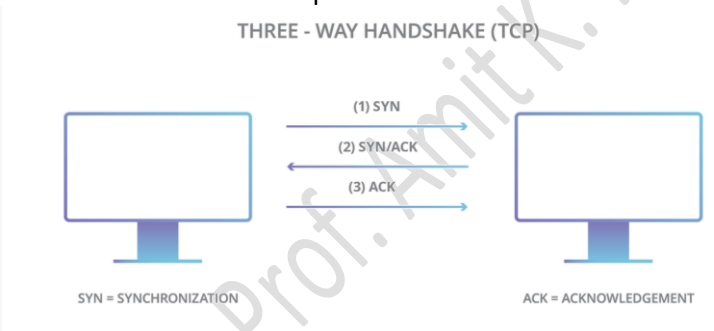
TCP syn flood

SYN flood attacks work by exploiting the handshake process of a TCP connection. 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.

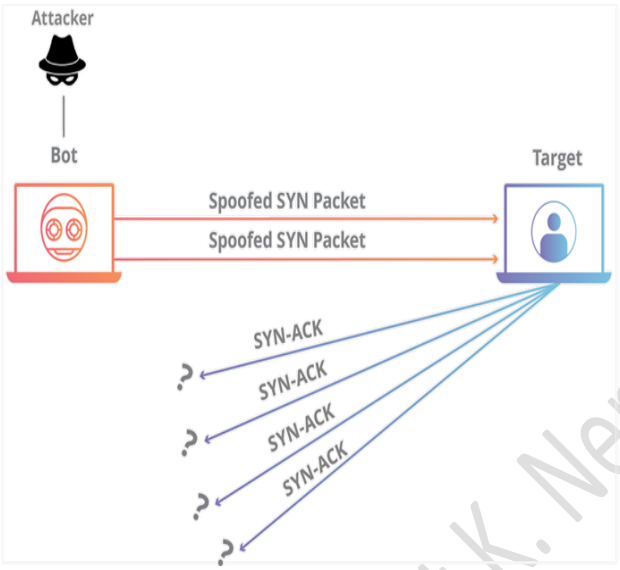
Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.



To create denial-of-service, an attacker exploits the fact that after an initial SYN packet has been received, the server will respond back with one or more SYN/ACK packets and wait for the final step in the handshake. Here's how it works:

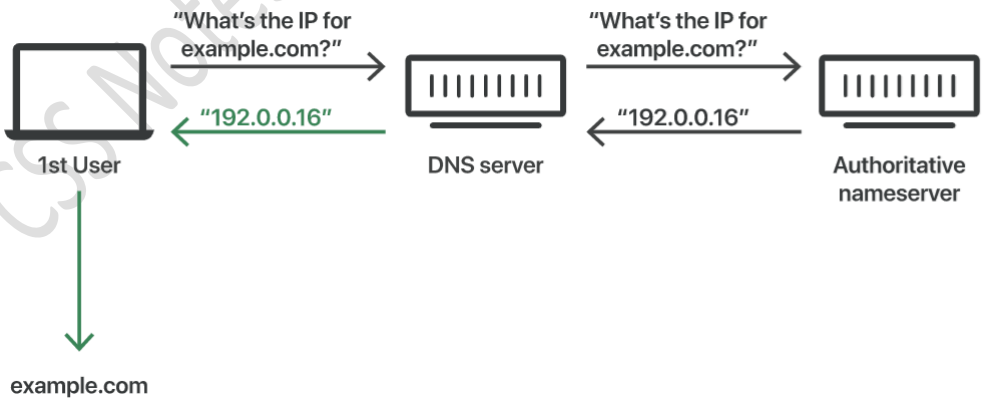
The attacker sends a high volume of SYN packets to the targeted server, often with spoofed IP addresses.
The server then responds to each one of the connection requests and leaves an open port ready to receive the response.

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.

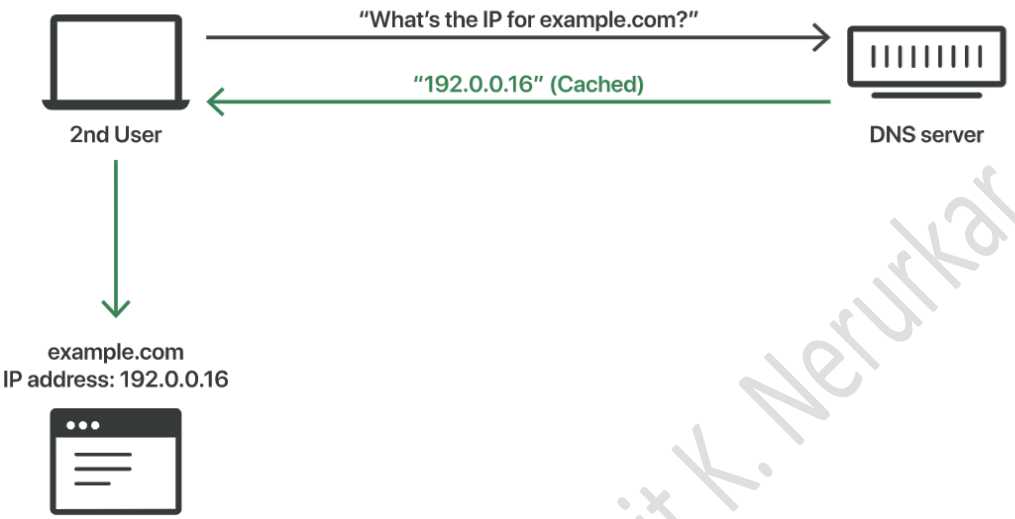


DNS Spoofing.

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.



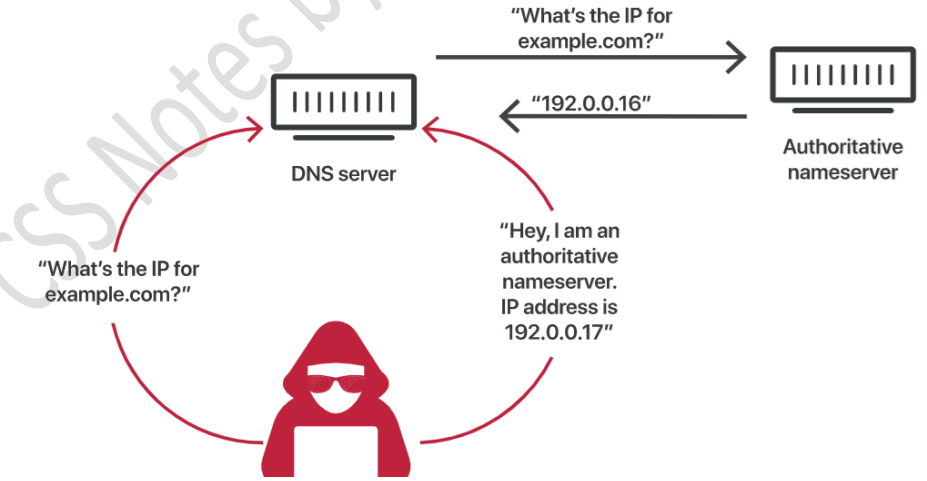
DNS Cached Response:



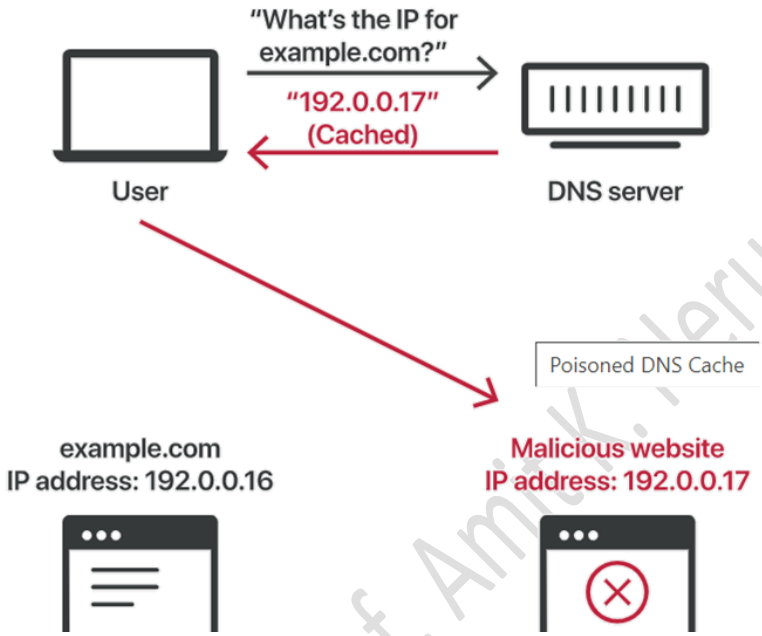
How do attackers poison DNS caches?

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 Cache Poisoning Process:



Poisoned DNS Cache:



References

1. https://www.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer
2. https://www.geeksforgeeks.org/what-is-packet-sniffing/
3. https://www.imperva.com/learn/application-security/arp-spoofing/
4. https://whatismyipaddress.com/port-scan
5. https://www.networkcomputing.com/network-security/port-scanning-techniques-introduction
6. https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/
7. https://www.cloudflare.com/learning/dns/dns-cache-poisoning/