SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit III- Network Threats

Topic : IP Spoofing - ARP spoofing - Session Hijacking

What is IP Spoofing?

- IP spoofing, also known as "IP address spoofing", **is the process of sending Internet Protocol (IP) packets with a fake source IP address** in order to mimic another computer system.
- Cybercriminals can use **IP spoofing to carry out harmful** acts without being detected.
- It's possible that someone will **steal your data**, infect your device with malware, or crash your server.

What is the Process of IP Spoofing?

- Packets are the **smallest units of data**, transferred over the internet. IP headers in packets include routing information about the packet.
- This information includes addresses. **both the source and destination IP**
- Consider the packet as a parcel in the mail, with the source IP address serving as the return address.
- In IP address spoofing, the **attacker alters the source address** in the outgoing packet header.
- As a result, the destination computer recognizes the packet as coming from a reliable source, such as a computer on a corporate network, and accepts it.

Attackers will require the following to do IP spoofing

- The receiving device would allow a trustworthy IP address to enter the network.
- Device IPs may be found in a variety of methods.
- The ability to intercept a packet and replace the **legitimate IP header** with a fake one.
- To intercept packets on a network and obtain IP addresses to spoof, utilize a network sniffing tool or an **Address Resolution Protocol (ARP)** scan.

How to Prevent IP Spoofing?

To prevent bogus packets from entering their networks, organizations can take the following steps &mins;

- Unusual actions are being observed on networks.
- It's a good idea to use **packet filtering technologies** that can detect anomalies, such as outgoing packets with source IP addresses that don't match those on the company's network.
- Use **severe verification methods** for any remote access, including systems on the workplace intranet, to prevent accepting forged packets from an attacker who has already infiltrated another system on the company network.
- The IP addresses of **inbound IP packets** are verified.
- It's a good idea to use a **network attack blocker.**

ARP Spoofing

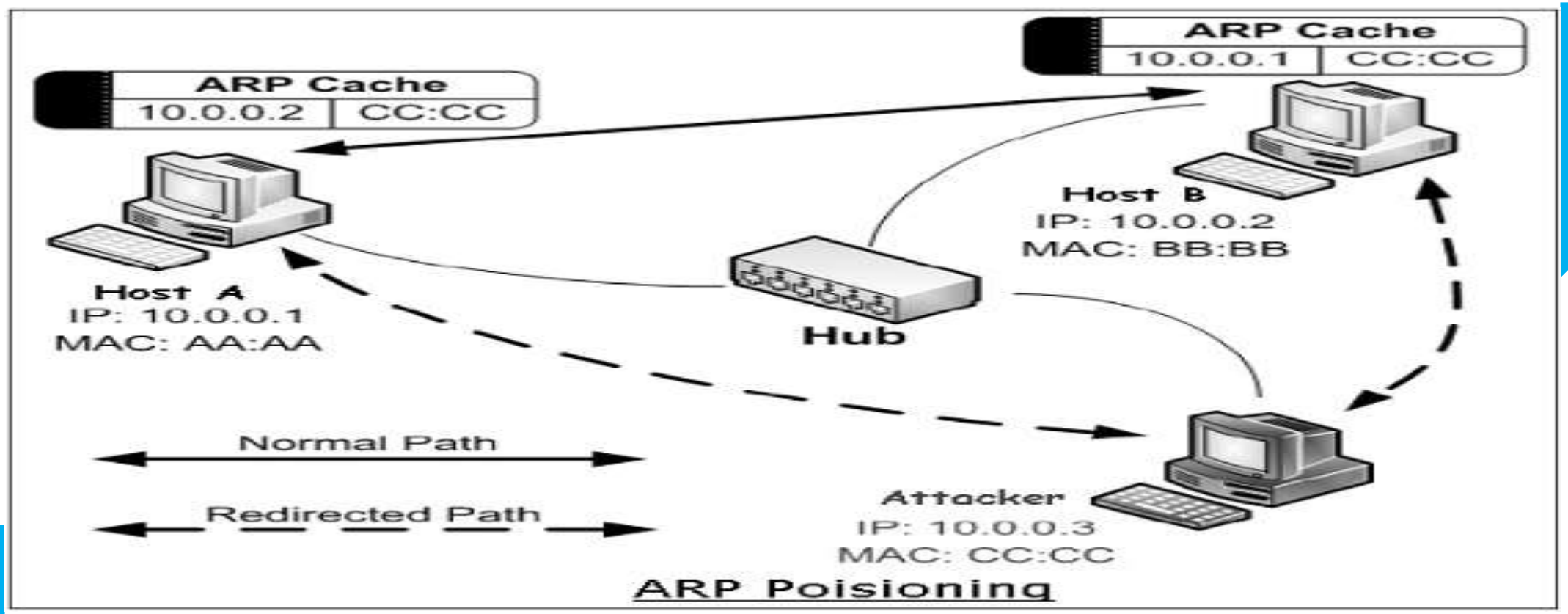
Address Resolution Protocol (ARP) is a protocol **used to map an IP address to a physical machine address** recognizable in the **local Ethernet.**

When a **host machine** needs to find a physical **Media Access Control (MAC)** address for an IP address, it broadcasts an ARP request.

The other host that owns the IP address sends an ARP reply message with its physical address.

Each host machine on network maintains a table, called 'ARP cache'.

The table holds the **IP address and associated MAC** addresses of other host on the network.


ARP Cache
10.0.0.2 | CC:CC
ARP Cache
10.0.0.1 | CC:CC
Host A
IP: 10.0.0.1
MAC: AA:AA
Hub
Host B
IP: 10.0.0.2
MAC: BB:BB
Normal Path
Redirected Path
Attacker
IP: 10.0.0.3
MAC: CC:CC
ARP Poisioning

ARP spoofing may allow an attacker to **masquerade as legitimate host and then intercept data frames on a network**, modify or stop them.

Often the attack is used to launch other attacks such as man-in-the-middle, session hijacking, or denial of service.

What is Session Hijacking?

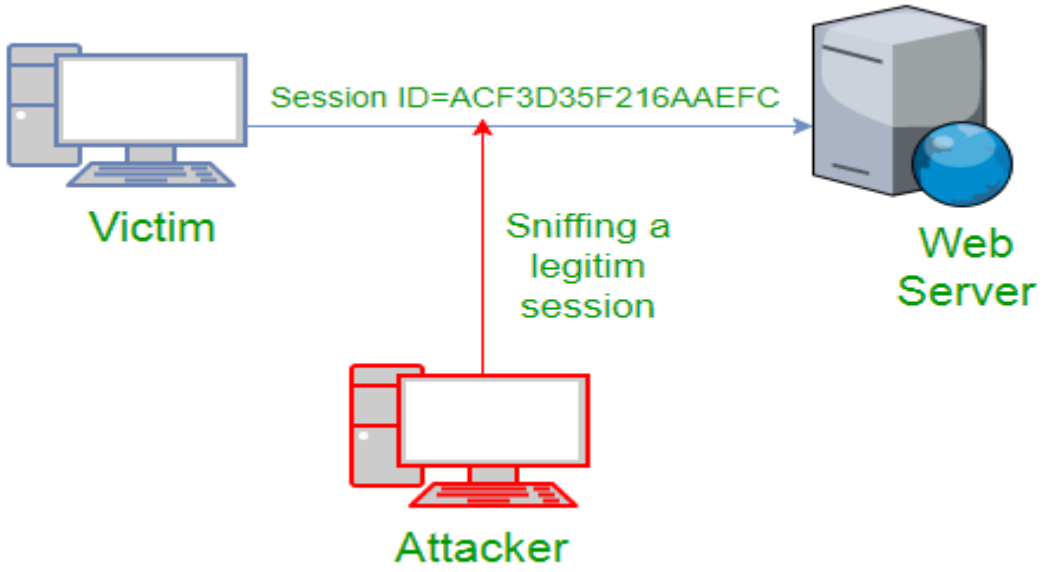
TCP session hijacking is a **security attack on a user session** over a protected network.

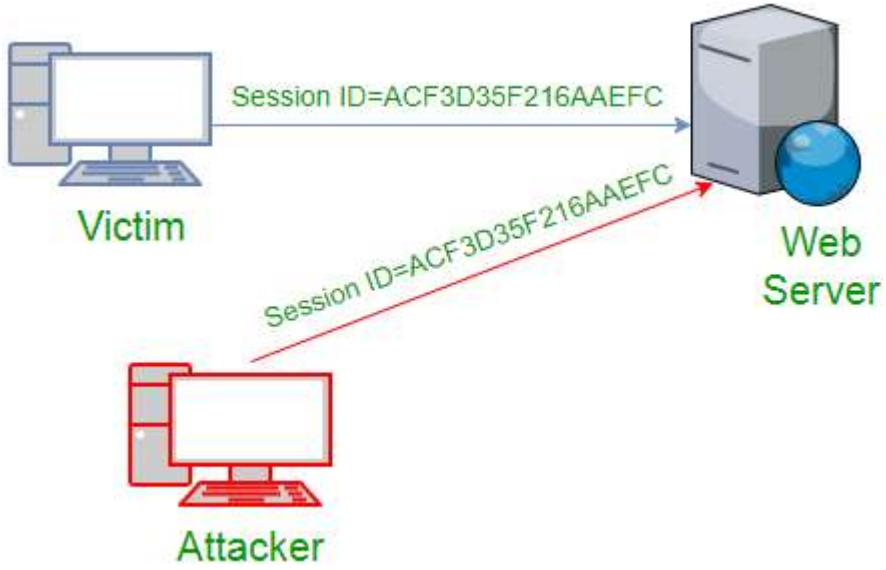
- The most common method of session hijacking is called IP spoofing, when an **attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network** and disguise itself as one of the authenticated users.
- This type of attack is possible because authentication typically is only done at the start of a **TCP session.**
- Another type of session hijacking is known as a **man-in-the-middle attack,** where the attacker, using a **sniffer,** can observe the communication between devices and collect the data that is transmitted.

Different ways of session hijacking :

There are many ways to do Session Hijacking. Some of them are given below –

Using Packet Sniffers




Session ID=ACF3D35F216AAEFC
Victim
Session ID=ACF3D35F216AAEFC
Web
Server
Attacker

Cross Site Scripting(XSS Attack)

Attacker can also capture victim's Session ID using XSS attack by using javascript.

If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

```
<SCRIPT type="text/javascript">
var adr = '../attacker.php?victim_cookie=' + escape(document.cookie);
</SCRIPT>
```

IP Spoofing

Spoofing is pretending to be someone else.

This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host.

In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e. the original host.

Blind Attack

If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

Any Query????

Thank you……