Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 1

Aim: To study IP spoofing and ARP spoofing over a local area network.

Theory:

What is Spoofing
A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, ARP spoofing attacksand DNS server spoofing attacks.

What is IP Spoofing

IP address spoofing is one of the most frequently used spoofing attack methods. In an IP address spoofing attack, an attacker sends IP packets from a false or ispoofed" source address in order to disguise itself. Denial-of- service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses.
There are two ways that IP spoofing attacks can be used to overload targets with traffic. One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle. The other method is to spoof the source IP address of known host which exist over same LAN and send request to server using this IP address. And server will response back to the spoofed IP address. This is the scenario weare going to study and implement in this experiment.

Simulation of IP Spoofing attack using netkit

Step1 : Using netkit create a LAN network having three workstations PC1,PC2 and PC3.All these three workstations should have same interface eth0 over same LAN A by using command
vstart pc1 –eth0=A

Step 2: Assign IP addresses to PC1,PC2 and PC3 as 192.168.1.11, 192.168.1.12 and 192.168.1.13 respectivley.
ifconfig eth0 192.168.1.11

Step 3: Ping without address spoofing ping form PC1 to PC3 and check that response is given back PC1.
Step 4: PC1 will spoof IP address of PC2 by making changes in iptables of PC1.
Following command is used to spoof the IP address of PC2 to create false identity by PC1.

iptables -t nat -A POSTROUTING -p icmp -j SNAT --to-source 192.168.1.12

Step 5: Packets are caputred using tcpdump. As response will be sent from PC3 to PC2, tcpdump command is executed on PC2 so that it can capture the reply.

Step 6: As tcpdump is in listening state on PC2 , we can ping PC3 from PC1 to check to outocmes of IP spoofing attack.

Step 7: Due to IP sppofing attack done by PC1, for PC3 the ping request is from PC2 so reply which is given back is for PC2.

What is ARP Spoofing

ARP is short form of Address Resolution Protocol.This is a protocol that is used to resolve IP addresses to MAC (Media Access Control) addresses for transmitting data. In an ARP spoofing attack, a malicious party sends spoofed ARP messages across a local area network in order to link the attacker's MAC address with the IP address of a legitimate member of the network. This type of spoofing attack results in data that is intended for the host's IP address getting sent to the attacker instead. Malicious parties commonly use ARP spoofing to steal information, modify data in-transit or stop traffic on a LAN. ARP spoofing attacks can also be used to facilitate other types of attacks, including denial-of-service, session hijacking and man-in-the-middle attacks. ARP spoofing only works on local area networks that use the Address Resolution Protocol.

Simulation ARP spoofing attack

Step 1: Install arpwatch

Step 2: Check the status of arpwatch to confirm that arpwatch is in running state.

Step 3:arpwatch maintains a log file to store information about IP addresses and MAC addresses.So any change in IP or MAC address can be noticed by the log entries of /var/log/syslog. Check the contents of /var/log/syslog using command tail -f /var/log/syslog.

Step 4: Ping to any node on the same LAN. Here we ping to machine having IP address 192.168.36.101 Now 192.168.36.101 node has the IP adress and MAC address of your machine.

Step 5: Now change the MAC address of your system using ifconfig command. Again ping again to 192.168.36.101 with this changed MAC address.

Step 6: Changes done in MAC address are notified in log entries of /var/log/syslog .

Thus we have simulated ARP spoofing attack and noticed the log entries contaning the changed MAC address alert.

Conclusion: Thus we have studied IP spoofing and ARP spoofing over a local area network. Arpwatch is a great is an open source computer software tool for monitoring Ethernet traffic activity (like Changing IP and MAC Addresses) on your network and maintains a database of ethernet/ip address pairings. It produces a log of noticed pairing of IP and MAC addresses information along with a timestamps, so you can carefully watch when the pairing activity appearedon the network.