Authentication Based Attacks

Tools in Kali Linux

Module #29

Man in the Middle Attack

A man-in-the-middle attack is a form of active eavesdropping in which the attacker makes a connection with victims and relays messages between victims, making them believe they are talking directly to each other.

There are many forms of this attack, such as using a Hak5 Pineapple wireless router that pretends to be a trusted wireless access point while really acting as a man-in-the-middle between a victim and wireless network.

Another example is using Kali to forward traffic between a victim and default router while sniffing for useful information, such as login credentials.

dsniff and arpspoof

dsniff is a set of password sniffing and network traffic analysis tools designed to parse different application protocols and extract relevant information.

arpspoof is used when an attacker sends fake address resolution protocol (ARP) messages into a local area network.

The goal of this process is to associate the attacker's MAC address with the IP address of another host, causing any traffic meant for the IP address to be sent to the attacker instead.

dsniff and arpspoof (Contd)

One of the methods to perform a man-in-the-middle is using arpspoof and dsniff to sit between systems.

The first step is identifying the IP address of your victim and default gateway of the network using techniques from Reconnaissance.

Assume the router having an IP of 192.168.1.1. Our victim will have an IP of 192.168.1.9.

We will need to open two terminal windows now, as we need to tell the victim that it should send its packets to us instead of the gateway, and we need to tell the gateway to send packets to us, instead of the victim.

dsniff and arpspoof (Contd)

```
arpspoof -t 192.168.1.9 192.168.1.1
```

```
arpspoof -t 192.168.1.1 192.168.1.9
```

Now run Wireshark or tcpdump to start capturing packets.

It will continuously send arp reply and thus update the arp cache table on both the victim and the router side.

Also its important to enable ip forwarding for the packet to reach from victim to router and vice versa.

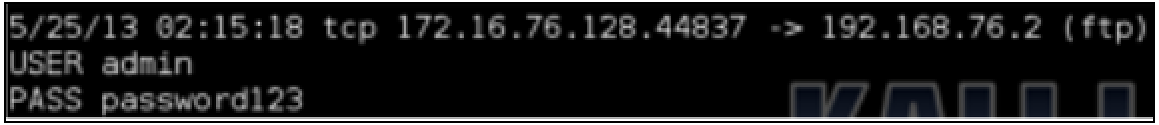
dsniff and arpspoof (Contd)

launch dsniff to watch the traffic. dsniff can be found under Sniffing/Spoofing | Network Sniffers, and selecting dsniff.

To start dsniff, type dsniff and select the interface to sniff using -i and the interface. In this example, dsniff used to sniff all traffic on eth0:

```
root@kali:~# dsniff -i eth0
```

dsniff will catch any login information. If a victim logs into a system via FTP for example, you will see the login attempt and credentials once the session is closed, because dsniff needs to see the entire session.



```
5/25/13 02:15:18 tcp 172.16.76.128.44837 -> 192.168.76.2 (ftp)
USER admin
PASS password123
```

Thank You