WEB Vulnerability- The Man in the Middle Attack

By: Rajashekar Rao Bandari

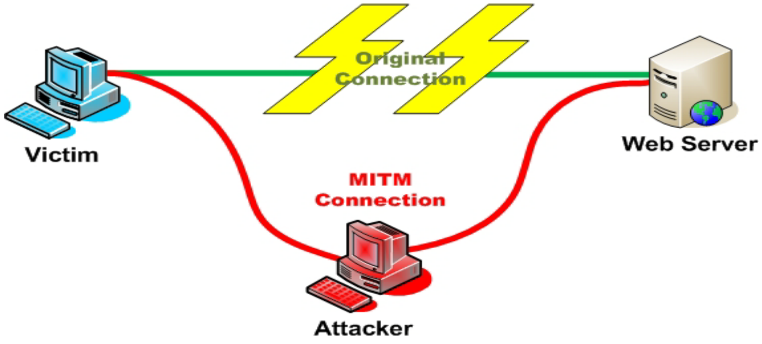
Abstract:

The Man in the middle attack which is also referred by other names like the monkey in the middle attack, bucket-brigade attack and session hijacking. The attack primarily aims at gaining access to a legitimate user (victim) session to tamper it or gain information. This attack is done by sniffing on a network and then manipulating or reroute the intercepted data. The most common MITM attack would be when an attacker intercepts the communication channel between the user(victim) and server(host) and then the attacker makes both the parties feel they are in touch one on one rather than him intruding into their channel. There are mainly three different types or grounds on which we can make MITM attacks.

1. Local Area Network (Arp poisoning, DNS spoofing)
2. Local to remote (ICMP redirecting, IRDP spoofing)
3. Remote (traffic tunneling, route mangling)

Description Of the Attack:

The attack is done by using tools in order to send ARP (address resolution protocol) which is also known as “ARP poisoning”. Here we intend to use this ARP spoof to sniff data frames on LAN and modify the packets in order that we may corrupt the ARP caches of directly connected hosts by which we can take over the IP address of the victim computer. Once this is done we would send a fake SSL certificate created by the attacker using the tools and send it to the victim and as soon as the victim accepts the new SSL we have setup a connection through which we can get all his authentication information and store it as a file using the ETTERCAP software. We can see a picture how exactly a man in the middle attack takes place.



In order to accomplish this we need the following Hardware and software.

Hardware Details: Router/Switch:

- D-Link wireless N router
- switch Board for ports

Victim Computer:

- Desktop
- 1 RAM
- Integrated Network Card
- Windows XP Professional

Attacker Computer:

- HP Pavilion dx6650us (Laptop)
- 2GB RAM
- Intel Centrino Duo
- Windows Vista Enterprise

Software:

Attackers Computer:

Operating System: Ubuntu (Linux).

Ettercap: This software is a suite which has features for sniffing; content filtering, OS fingerprinting, password collections, and remote traffic and is one of the best suitable if the man in the middle attacks. This software comprises of different tools through which we can do many things like Arp poisoning, DNS spoofing etc.

Winpcap: This is a port of libpcap in windows which is used for the packet capture in a UNIX like systems. This is an API which is used along with monitoring software in our case Ettercap in order to capture packets on a network.

Victims Computer:

Operating System: Windows XP professional

Software: Internet Explorer.

Summary:

In this document we have been given a brief description about the man in the middle attack, the requirements in terms of the tools and software. Also the way these tools are useful. This would be explained in much more detail along with the executed experiment and its output.

References:

1. Man in the Middle attack from http://www.owasp.org/index.php/Man-in-the-middle_attack

2. About Secure socket layer from Wikipedia (http://en.wikipedia.org/wiki/SSL)

3. Ettercap information from http://ettercap.sourceforge.net/

4. Winpcap information can be read at http://en.wikipedia.org/wiki/WinPcap#WinPcap

5. **MITM** attack document wiki by http://it.toolbox.com/wiki/index.php/Man-in-the-Middle_Attack

6. Attack on SSL using MITM document http://www.docstoc.com/docs/11837353/A-Real-Life-Man-in-the-Middle-Attack-on-SSL