NIPUN SHRIVASTAVA
2011CS50288
SIL 765
ASSIGNMENT 1

In order to perform a PITM attack using SSLSTRIP for the given assignment, I used the following commands:

- *ifconfig*

This command was used to find the ipaddress of the attacking machine so that it can be later used to define the new routing path for the packets emerging from the victim's machine.

- *echo "1" > /proc/sys/net/ipv4/ip_forward*

This command enables the IP packet forwarding in the attacking machine.

- *iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080*

This command sets up iptables to redirect HTTP traffic to sslstrip. What this command essentially does is it redirects all the requests from Port 80 to Port 8080 in order to enable the attacking system to proper route the incoming packets on port 80.

- *sslstrip -l 8080*

This command runs SSLSTRIP in KALI. What it does is it enables listening to the specified port in 8080.

- *tail sslstrip.log*

This command was used again and again to see the latest entries to the log file which was being continuously populated by the SSLSTRIP utility.

For this assignment we redirected the network traffic of victim's machine by enlisting the attacking machine's ipaddress as the proxy server for the targeted machine. This was done physically. Obviously for attacking a system this is not a feasible way. There are other ways possible but we didn't use them because of the risks they carry. Never the less, I am mentioning them below for the sake of completeness.

- *sudo route del default gw (Gatway IP), sudo route add default gw (Attacker's IP)*

This commands when run on the victim's PC, deletes the IP address of the default gateway and replaces it with its own address. This will have a similar effect on the targeted machines as of setting the attacker's machine as its proxy server.

If gaining control of the targeted machine even for an instant is not possible, we can use the following command:

- *arpspoof -i interface -t Target IP -r Gateway IP*

This command convinces the target machine to route their HTTP packets through you.

Web sites subverted for this assignment:

www.gmail.com
www.google.com
www.facebook.com
www.yahoo.com
http://webmail.iitd.ernet.in/roundcube/
http://www.cc.iitd.ernet.in

I was able to successfully run SSLSTRIP on the above listed sites while the passwords from the top 5 sites were successfully harvested. The last one didn't had any information to be harvested.

Below is the information about the web browser on which the attack happened. The browser was being run on 64 bit Windows 8 PRO operating system.

As stated above, username and passwords were harvested from the famous sites. These sites have https by default which makes it impossible to cipher out the encrypted information transferred over the network. But the SSLSTRIP utility changes all these https site links to http when accessed through a link from another webpage – say from a Google search page. Although Facebook login page still appeared as https when googled. Anyhow, when I directly wrote the address of the above mentioned sites with http on the targeted machine, all the information sent over like passwords which were supposed to be encrypted was completely exposed as they were not sent on https any more but http and our utility easily captured all that in an SSLSTRIP.log file. Later we were able to extract the same from the log file.

For security reasons we have replaced the critical passwords or passwords of accounts still in use with *. Also netstat –nr was used to find the ipaddress of the gateway.