TLS MITM Attack

1.0 Objective

Transport Layer Security, TLS, is one of the world's most important forms of commercial encryption. It is the public key system generally employed by e-commerce websites like Amazon in order to prevent payment details from being intercepted by third parties.

The tool called "SSL strip" is an attack on TLS based around a man-in-the-middle vulnerability where the system redirects people from the secure version of a webpage to an unsecured one. By acting as a man-in-the-middle, the attacker can compromise any information sent between the user and the supposedly secure webpage.

This kind of vulnerability has always existed with TLS because it is difficult to be certain about where the endpoints of communication lie. Rather than having a secure end-to-end connection between Amazon and you, there might be a (un)secure connection between you and an attacker (who can read everything you do in the clear), and then a second secure connection between the attacker and Amazon.

DO NOT TARGET ANYTHING OUTSIDE OF VLAB. THIS EXERCISE MUST BE PERFORMED WITHIN THE CONFINES OF VLAB.

1.1 SSLStrip Background Information

Before beginning this lab watch the following presentation from Moxie Marlinspike the author of SSLStrip.

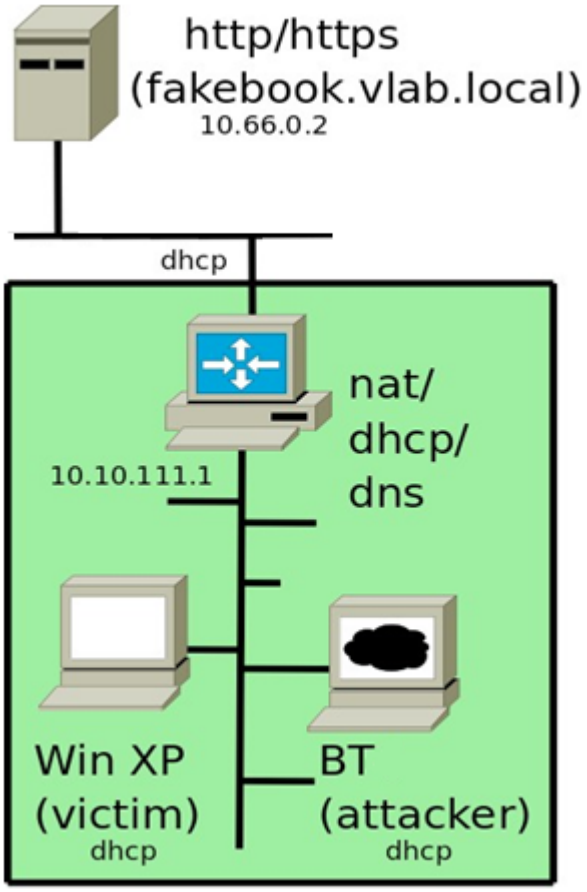
http://www.youtube.com/watch?v=MFol6IMbZ7Y

The website for SSLStrip can also be found at:

http://www.thoughtcrime.org/software/sslstrip/

1.2 Lab Setup and Background

The VLAB architecture for this attack is depicted in the diagram below:



The green box represents the VLAB environment that each student has an individual instance of. There is a gateway (router) that connects the student VLAN to a second VLAN in which resides the fakebook webserver that will be used in the attack.

Start up the following VMs in order: rtr (external router), bt5 (the attacking machine), and XP (the Windows XP victim).

The website to be attacked is inside the VLAB environment, and can be accessed at <http://fakebook.vlab.local>. Startup Firefox on the BT5 VM and ensure that you can successful get to the fakebook website.

2.0 Perform Man- in- the-Middle Attack

Browse the fakebook webserver from the BT5 machine using Firefox, and click “view page source”.

Find and record the FORM statement for the login. This shows that although the page is not secure, the actual login method uses a URL starting with https. Many websites use this system (Facebook, Back of America, etc) in which a single page has both secure and insecure items. That is the vulnerability we will exploit.

Make sure that the Backtrack5 machine has an IP address and that the default gateway is pointed at the .1 address of the router (rtr).

Now on the Backtrack machine, we first have to setup up the machine to accept packets inbound and forward them outbound and vice versa. This functionality can be modified in Linux by performing the following:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Next we need to modify IPTables. IPTables is a firewalling application available in Linux distributions. We will be covering IPTables in more detail later in the course. For now, understand that IPtables is taking traffic coming inbound to the Backtrack5 machine which is destined to port 80 (HTTP Web) and redirecting only that traffic to the SSLStrip application which in turn is listening on port 8080.

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

Note: These changes are lost after a reboot.

Finally we need to perform an ARP spoofing attack on client machine. Write a SCAPY program that sends gratuitous ARP messages from BT5 to both the XP machine (XP) and the router (rtr). The gratuitous ARPs sent to the Windows XP changes the entry for the MAC address for rtr to that of BT5s MAC address (making the Windows XP machine think that BT5 is actually the router), while the gratuitous ARPs sent to the router changes the entry for the MAC address of the Windows XP address that of BT5 MAC address (making the rtr think that the BT5 is actually the Windows XP machine). Use the ARP command on each to show that the IP-MAC association has been changed on each.

2.1 SSLstrip Attack

Run SSLstrip on the Backtrack5 machine. To do this use the command:

```
python sslstrip.py -l 8080
```

This starts sslstrip with it listening on port 8080 of the Backtrack5 machine.

Go back to the victim machine and browse back to the webserver (use Firefox). Again go to "view source" in the web browser. Look for the FORM method. ***Record the new FORM post method and explain what is different.***

From the victim machine, login to the webserver using the credentials

username: memon
password: evilproffy

Now go back to the Backtrack5 machine. You should see a lot of messages scrolling by. Open a new terminal window and find the sslstrip log file "sslstrip.log"

Open this log file in your favorite text editor and find and record the captured login and passwords.

What to submit:
Write a report documenting the steps employed during the attack. The report should include screen captures of both the Backtrack5 machine and the client Windows XP machine, recording each step of the attach process. Include a clear description of each step that was taken.

a. [30 pts] Write a SCAPY program on BT5 that sends gratuitous ARPs to XP and rtr so that BT5 is in the middle of the communication between rtr and XP.
b. [10 pts] Show the results of successful ARP spoofing by taking screenshots showing the output of the arp command.
c. [20 pts] Perform sslstrip attack on the client accessing Fakebook.
d. [20 pts] Record the new FORM post method and explain what is different.
e. [10 pts] Open this log file in your favorite text editor and find and record the captured login and passwords.
f. [10 pts] Fully explain in a paragraph or two how sslstrip works.