SSL MITM Attack

1.0 Objective

The Secure Sockets Layer, SSL 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 based around a man-in-the-middle attack, where the system for redirecting people from the insecure to the secure version of a web page is abused. 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 SSL 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 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 LAB.

1.1 SSLStrip Background Information

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

Please see the course website for the up to date URL of the video.

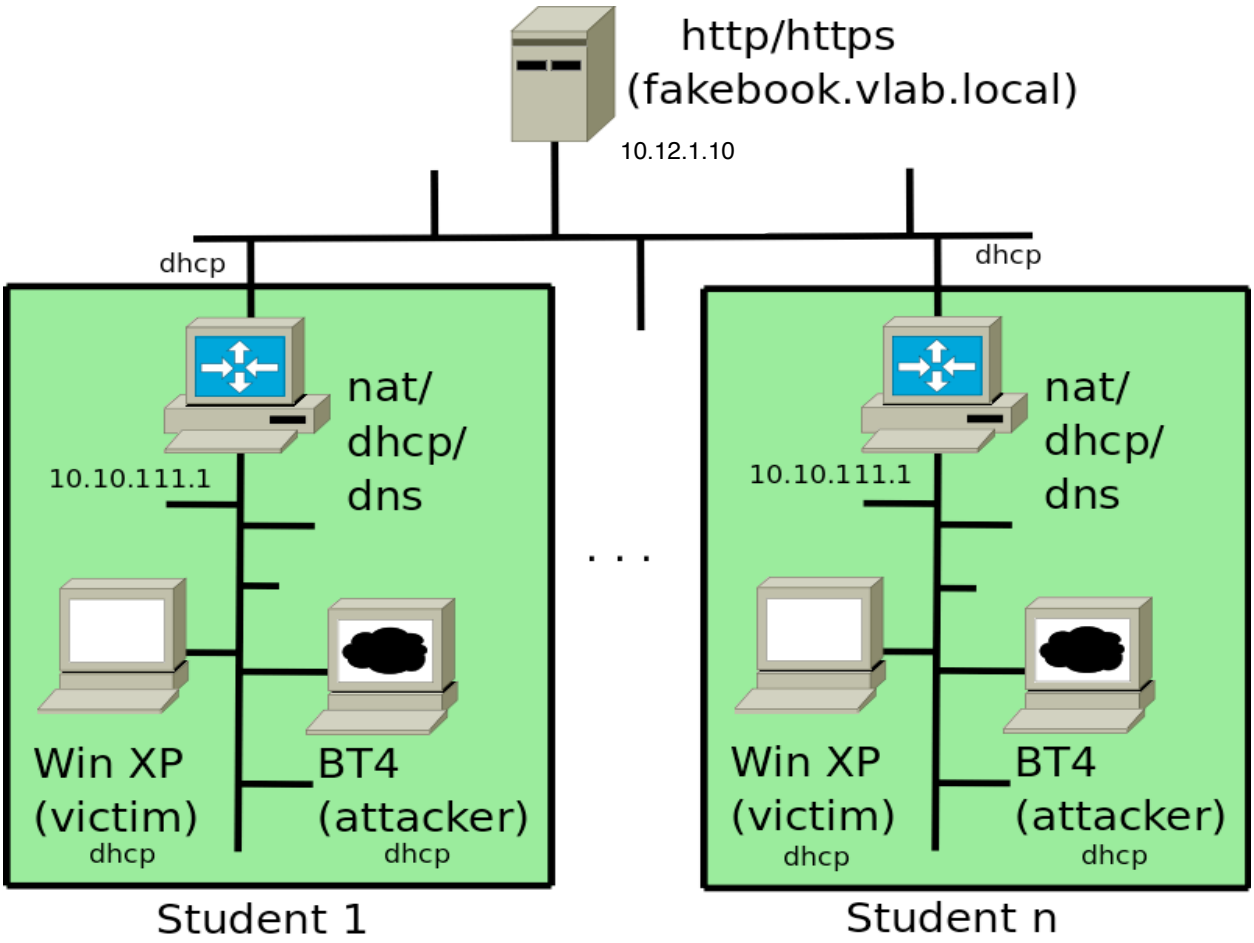
The website for SSLStrip can also be found at:

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

2.0 Perform Man in the Middle Attack

The VLAB is setup so that you have two machines on a common VLAN with a target (client machine) running WindowsXP. The second machine is running Backtrack4.

Additionally there is a gateway (router) which connects these machines to a second VLAN in which resides a webserver which will be used in the attack. A depiction of the setup is below:



Make sure to start the nat/dhcp/dns/default gateway box from within VLAB before proceeding.

The login for the Backtrack 4 machine is:

username: root
password: toor

To enter the GUI in Backtrack type “startx” Then start networking by going to services->networking->start

Since SSLStrip works on domain names you will have to modify your external router machine so that it can serve as a DNS server and properly resolve the name. To do this:

```
In file /etc/bind/db.vlab.local
```

Replace

```
fakebook IN A xxx.xxx.xxx.xxx
```

With

```
fakebook IN A 10.12.1.10
```

```
In file /etc/resolv.conf
```

Append Line

```
nameserver  10.10.111.1
```

Now browse to the webserver from the client and click “view page source” Be sure to use Firefox for this exercise.

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) a single page has both secure and insecure items. That is the vulnerability we will exploit.

Make sure that the Backtrack4 machine has an ip address and that the default gateway is pointed at the .1 address of the router.

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 Backtrack4 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
```

Finally we need to perform a ARP spoofing attack on client machine. Use the command arpspoof to perform this function. ***Research the arpspoof command on the Internet and fully explain its function and how arp spoofing works in detail. In order to use arpspoof you will need the ip address in the client. This can be easily obtained using NMAP from the Backtrack4 machine.***

2.1 SSLstrip Attack

Run SSLstrip on the Backtrack4 machine. To do this use the command:

```
sslstrip.py -a -l 8080
```

This starts sslstrip with it listening on port 8080 of the Backtrack4 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 Backtrack4 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:

- Screenshots of the steps employed during your attack. Perform screen captures of both the Backtrack4 machine and the client machine recording each step of the lab.
- Also submit the information requested in the previous section which are denoted in ***bold itallics***
- Fully explain in a paragraph or two how sslstrip works.