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.

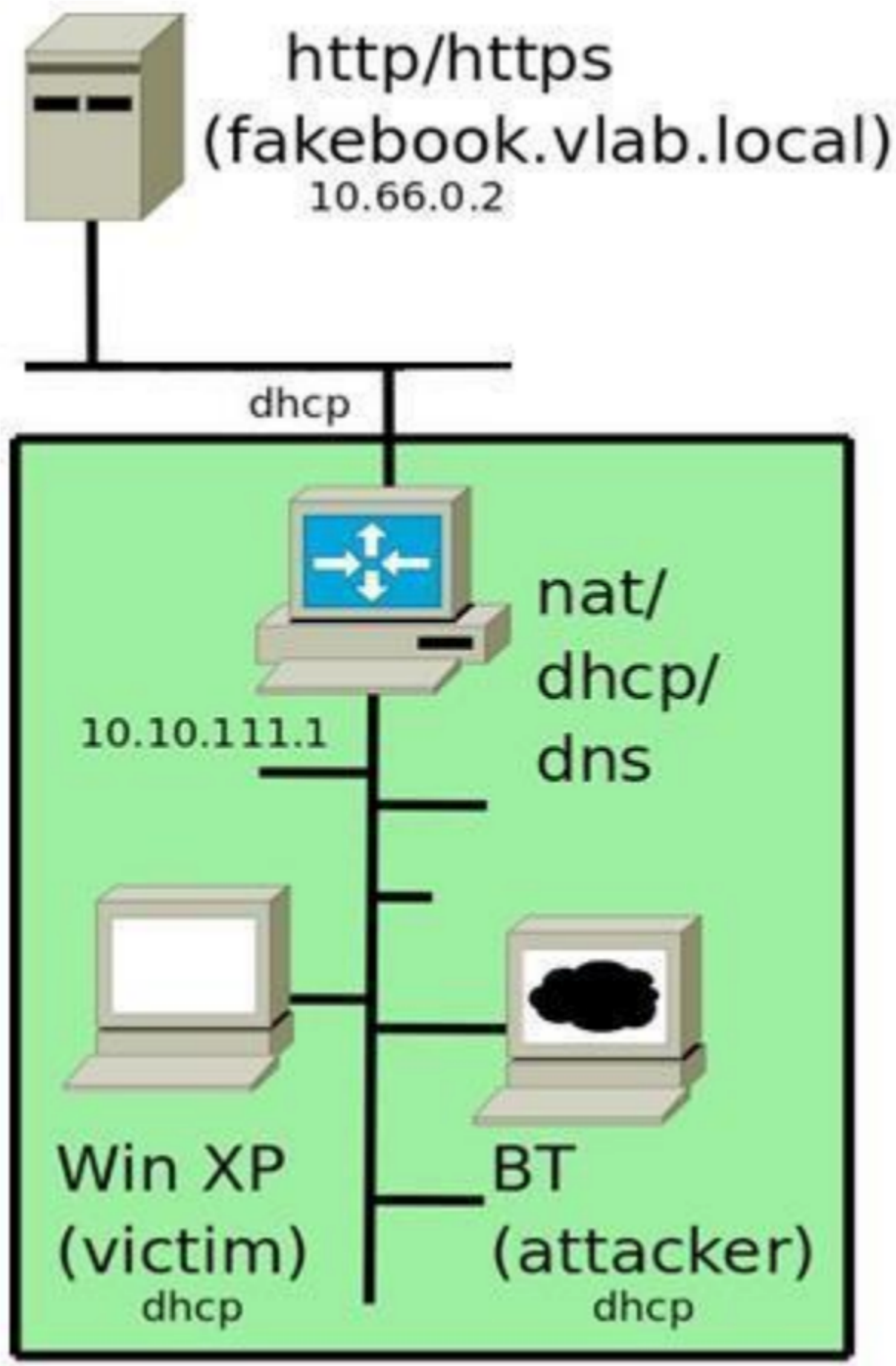
2.0 SSLStrip Background Information

The following presentation from Moxie Marlinspike provides background for this lab:
http://www.youtube.com/watch?v=MFol6IMbZ7Y

The website for SSLStrip can also be found at:
http://www.thoughtcrime.org/software/sslstrip/

3.0 Lab Setup and Background

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


http/https
(fakebook.vlab.local)
10.66.0.2
dhcp
nat/
dhcp/
dns
10.10.111.1
Win XP
(victim)
dhcp
BT
(attacker)
dhcp

There is a gateway (router) that connects the green colored VLAN to a second VLAN in which resides the fakebook webserver that will be used in the attack.

The VMs were started in the following 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 could be accessed at <http://fakebook.vlab.local>. Firefox was opened on the BT5 VM to ensure that fakebook website could be accessed.

4.0 Perform Man- in- the-Middle Attack

Browsed the fakebook webserver from the BT5 machine using Firefox, and clicked "view page source".

The FORM statement 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.

Made 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 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 modified IPTables. IPTables is a firewalling application available in Linux distributions.

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.

A SCAPY program is written(grat.py) 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).

5.0 SSLstrip Attack

Ran SSLstrip on the Backtrack5 machine. To do the following command was used:

```
python grat.py -l 8080
```

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

Now when we browse the webserver from the victim machine we can check the FORM method.

Now when we go back to the Backtrack5 machine. We should see a lot of messages scrolling by. We can now open a new terminal window and find the sslstrip log file “sslstrip.log”.