CS-4331-Special Topics in Security

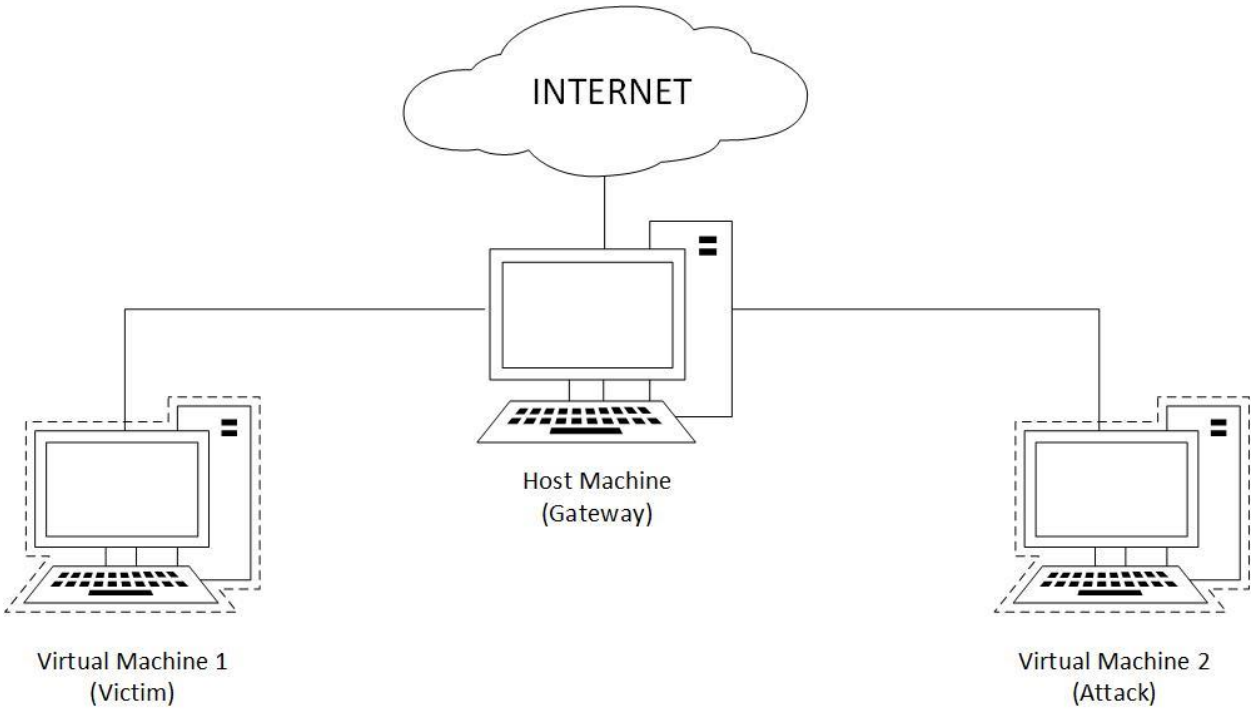
Fall 2016

Lab #5: SSL Strip Attack

In this lab, you will launch a man-in-middle attack on tls/ssl. You will use SSLSTRIP --- a tool that transparently intercepts HTTP traffic from a victim machine on a network, watches for HTTPS links and redirects, and then maps those links back into look-alike HTTP links.

1. Network Setup

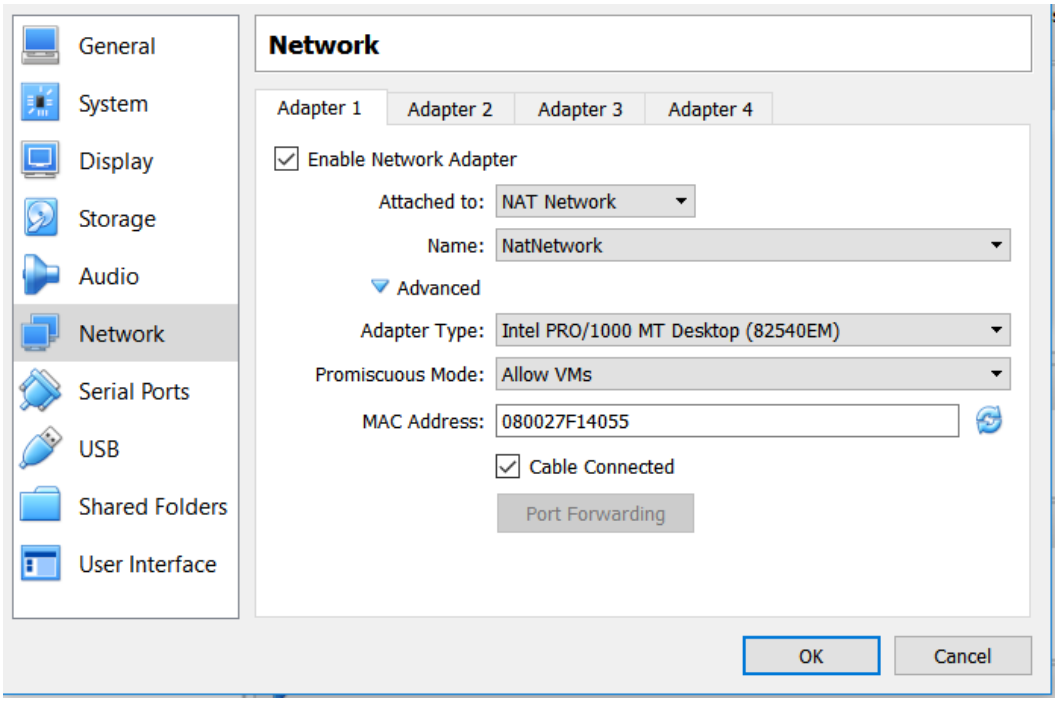
Follow the following steps to set up two virtual machines i.e. victim and attack machine that should form a Local Area Network (LAN) and also have ability to access the internet as shown below:



(a) Create two VMs in your Oracle VM VirtualBox Manager (you may just create a clone of a VM you have already so you have two VMs).
(b) In the Oracle VM VirtualBox Manager, click “File” and then click “Preferences…”
(c) Select “Network” in the VirtualBox – Preferences dialog and click the icon “Adds new NAT network” to add a new NAT network. You have now created a NatNetwork (which allows the VMs connected to it to communicate to each other and also connect to the internet). You will next connect your two VMs to this network.

(d) In the settings option of each VM (this option can be seen by right-clicking on the VM), click “Network” and then select “Nat Network” from the Attached to: options under “Adapter 1” tab. Choose the name of your NAT Network as: NatNetwork (which is the name of the NAT network you created in the previous step).

(e) Click “Advanced” on the “Adapter 1” tab and then click the “Refresh” button/icon besides the MAC address input box. You current screen should look like the one below.



(f) Click the “OK” button to save the changes.

Verify that the victim and attacker can communicate to each other, and that they can each connect to the internet (show the series of commands you use to verify this. HINT: You will have to retrieve the IP addresses of your machines first).

2. (a) Configure Kali on your attack machine to forward incoming packets. Use the following command for this task:

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

   (b) Check to confirm if the command has made the desired edit

3. (a) Find out your network gateway using the command

   netstat –nr

   (b) Identify your gateway address from the returned result

4. (a) Use the arpspoof tool to redirect to the attacker any traffic meant for the gateway
   (b) Use the command arpspoof –i Interface_Name –t victim_IP Gateway_IP

(c) Use ifconfig to determine your active network interface
(d) Use the gateway IP address returned from Step 2 as your Gateway_IP

5. (a) Set up firewall rules on the attack machine to redirect traffic received on port 80 to port 8080

   iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port <listenPort>

6. (a) Run SSLStrip on the attacker machine using:

   sslstrip –l 8080

7. (a) View the log file produced by sslstrip. The log file is sslstrip.log

   A common command for this is “tail” for viewing the last part of a changing file. As the file keeps changing, it records the tail.

   Command: tail –f sslstrip.log

8. (a) The victim attempts to browse to a web page (unaware that an adversary is eavesdropping on the connection). This website/webpage runs over https, however, the victim is not aware of this, and instead types an http address. For this web page use: securityisfun.com/CS4331 or http://securityisfun.com. The web page will present you with a login page requiring a username and password. Enter a user name and password (please don’t use your real username and password).

   Keep watching the log file mentioned in step 7.

   You should at some point see the credentials entered by the victim. Explain in details how/why the attacker is able to see this information.

   The vast majority of websites these days are secure against this attack. Explain the security mechanism they use to prevent this attack.