

Assignment 4

New Attempt

- Due Oct 13, 2024 by 11:59pm
- Points 100
- Submitting a file upload
- File Types pdf

Due: Tuesday, October 13, 2024 (11:59 PM). Please submit your assignment as a PDF on Canvas.

Man-in-the-Middle Attacks

In this assignment, you will learn how to perform a man-in-the-middle (MITM) attack. A Man-in the middle attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. We can perform MITM attack in different ways.

- ARP Spoofing: Involves interfering with ARP packages in order to poison the victim's cache
- Evil Twin: Involves creating an identical WiFi network and tricks the victim into entering that network.

In this assignment, we do ARP spoofing for MITM.

There are various tools to perform ARP spoofing. You can perform a direct MITM attack using a simple tool in Kali called `arpspoof`. The commands to do it are:

```
arpspoof -t <router IP> <target IP>
arpspoof -t <target IP> <router IP>
```

The first command performs an attack to the router and the second command performs an attack to the target machine. In this assignment, you use the tool `BetterCAP` which is a strong tool for performing various types of network attacks.

Setup

For this assignment, we use the following VMs: Router, Kali Linux, and Windows 7. Kali Linux will be the attacker and Windows 7 VM is the target machine.

In Kali, you need to have `BetterCAP` installed. You can type the command `bettercap` and if it does not exist you can download and install `BetterCAP` by using the command:

```
apt-get install bettercap
```

Furthermore, you will need `Wireshark` which is an open-source software for packet analysis.
`Wireshark is preinstalled in Kali.

1 BetterCap

This set of tasks is about learning **BetterCAP**, a Swiss Knife toolkit for network attacks and sniffing. In order to start bettercap type in a console:

```
bettercap
```

Make sure you are using version 2 of **BetterCAP**.

BetterCAP has many modules. One of them is the **ARP module**. The **ARP module** is responsible for performing ARP spoofing.

Task 1: By using the proper command in the target machine (Windows 7) find its ARP table. What command did you use? Report the ARP table you found.

Task 2: Set the proper options for the ARP module to attack the target machine and perform the attack. What commands did you use?

Task 3: What has been changed after the attack on the target machine?

Now, we have successfully performed a man-in-the-middle attack.

Next, open **Wireshark** and start capturing packets by pressing the blue “shark fin” button. In the textbox, you can type a filter to filter out any unwanted packets.

We want to capture all the packets that come from the IP address of the target machine and also have the POST HTTP method.

Navigate to a website without HTTPS (e.g. <http://solanaceaesource.org/> (<http://solanaceaesource.org/>)) and try to login. The login will create a POST HTTP request and Wireshark should capture it.

If you're unable to access the internet from the Windows machine, you may need to add iptables rules in the Kali VM which filter the packets at the Kernel level.

```
iptables -A FORWARD -i eth0 -j ACCEPT  
iptables -A FORWARD -o eth0 -j ACCEPT
```

Task 4: Report the filter you used to capture all packets from the target's IP address containing POST requests. Also, post a screenshot of the POST requests you captured.

Task 5: Try doing the same with an HTTPS request on an HTTPS website (e.g. <https://google.com> (<https://google.com/>)). Did it work? If yes, include a screenshot of the captured packet in your report, if not explain why.

2 SSL Strip

In this set of tasks, we are going to try to bypass HTTPS and try to redirect HTTPS websites to the equivalent HTTP ones. The method and tool you use for this purpose is called **SSL Strip** (in Kali).

In order to run **SSL Strip** we need to have an active MITM attack with **BetterCAP** and the **http.proxy** module set to off (**http.proxy off** from **BetterCAP**). We also need to redirect requests from port 80 to a port of our choice. For the port redirect, we are going to use a tool in Kali Linux called **iptables**.

Setup SSLStrip

```
mkdir ~/Documents/Tools && cd ~/Documents/Tools && git clone https://github.com/moxie0/sslstrip.git && cd sslstrip;
sudo apt update && curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py && python2 get-pip.py;
python2 -m pip install setuptools && sudo apt install python2-dev && python2 -m pip install Twisted==9.0.0 pyOpenSSL;
```

Task 6: What is the command to redirect requests from port 80 to port 10000?

Task 7: After enabling the redirect we can use `sslstrip` by typing

```
python2 ~/Documents/Tools/sslstrip.py -l 10000
```

Verify that `sslstrip` is working by visiting (from the target machine) a website which is using HTTPS and see if it is transformed to HTTP (e.g. bmo.ca). Report a screenshot of the website.

Note: `sslstrip` might not work on Chrome/Firefox and will work on Internet Explorer. If you can get this working on Chrome/Firefox it'll be great!

Task 8: Do research and find out how the `SSL Strip` method works. Report your findings.

Task 9: If you have previously visited a website you will notice that `SSL Strip` might not work on that particular website on your next visit. Explain why it doesn't work. What is the mechanism that prevents it from working?

3 MitmProxy

Before continuing with this task you should stop `sslstrip` and delete all `iptables` rules set using the command:

```
iptables -t nat -F
```

In this set of tasks, we use the tool `mitmproxy` in order to read HTTPS traffic. To do so, we need to deactivate the `http.proxy module` of `BetterCAP` using the command `http.proxy off`. And we need to maintain an active MITM attack. Also installing Chrome browser on the target machine is advised.

`mitmproxy` works only if we redirect all connections to ports 80 and 443 to port 8080. We also need to enable IP forwarding and disable ICMP redirects.

Task 10: What is the command to enable IP forwarding? What is the command to disable ICMP redirects? What are the commands to redirect requests from ports 80 and 443 to port 8080?

Task 11: In the previous task we redirected ports 80 and 443 to 8080. Why is this important? Why these two ports specifically?

After preparing the environment for mitmproxy run the command:

```
mitmproxy --mode transparent --showhost
```

Task 12: What do the flags `--mode transparent` and `--showhost` do?

At the target machine visit the address mitm.it. If you see the following: "If you can see this, traffic is not passing through mitmproxy. This means that `mitmproxy` and man-in-the-middle attack is not working." That means that the MITM is not working.

If you do not see this message visit mitm.it/cert/cer and download the certificate. After installing it visit a Website (e.g. github.com) and confirm that from the attacker machine, you can see the traffic recorded in mitmproxy.

Note: The mitm site offers several certificate options for various operating systems and browsers. If the default Windows certificate isn't installable, you can select an alternative, such as one for a specific browser, or even try using a certificate designed for another OS, like Android, which might still work.

Task 13: According to your opinion how does `mitmproxy` work? What would happen if we did not install the certificate and did not use `--mode transparent` ?

Task 14: How can you confirm from the target machine which certificate is being used for the connection? Report a screenshot if needed.