

Lesson 5. Exploring iptables

GOAL

In this lesson, we explore how we can change the rules in the iptables of the Ubuntu VM (Mallory) to control the network traffic from the Windows machine (Alice).

TASK A.

Explore the effect of typing the following on the Ubuntu VM (Mallory).

- a. `echo "0" > /proc/sys/net/ipv4/ip_forward`
On the Windows machine (Alice), try to navigate to any website on the browser. Try to ping google.com from the command prompt. What do you observe?
You should **not** be able to navigate to or ping any website. The Ubuntu machine is not forwarding any traffic and that has effectively isolated the Windows machine.
- b. `echo "1" > /proc/sys/net/ipv4/ip_forward`
On the Windows machine (Alice), try to navigate to any website on the browser. Try to ping google.com from the command prompt. What do you observe?
You should be able to browse or ping any website. The Ubuntu machine forwards all requests from Alice's machine to the internet.
- c. `iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080`

The flags are interpreted as the following.

-t flag denotes to which table the rule should be added to

-p represents the protocol to which the rule will be applied to

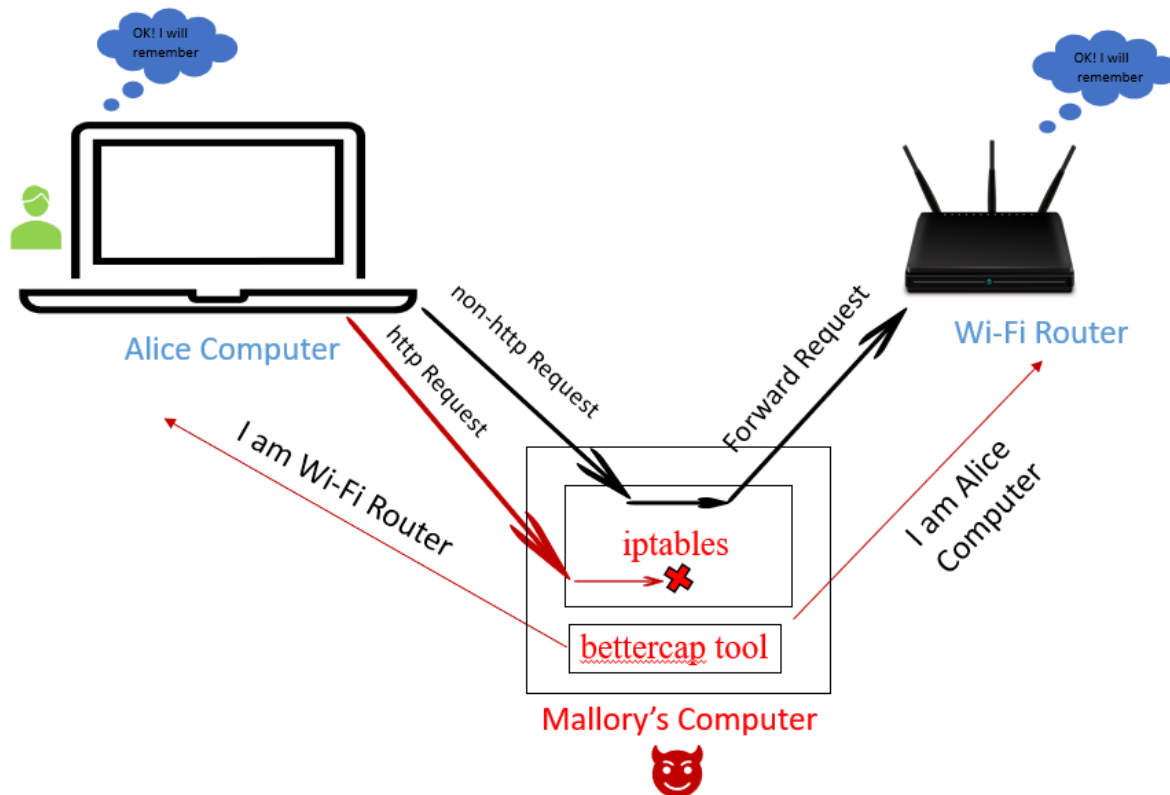
--dport is the destination port where the traffic will be sent to on the server (80 is for HTTP)

--to-port is the port number (of Kali VM) to which the traffic will be redirected to

On the Windows machine, navigate to an HTTP server (web.interhack.com). Try to navigate to an HTTPS server (google.com). What do you observe?

Only HTTP traffic is rerouted to port 8080 (where mitmproxy is not yet running), so HTTP traffic dies down in the Ubuntu VM. Other traffic is forwarded.

Effect of running bettercap tool and iptables tool:

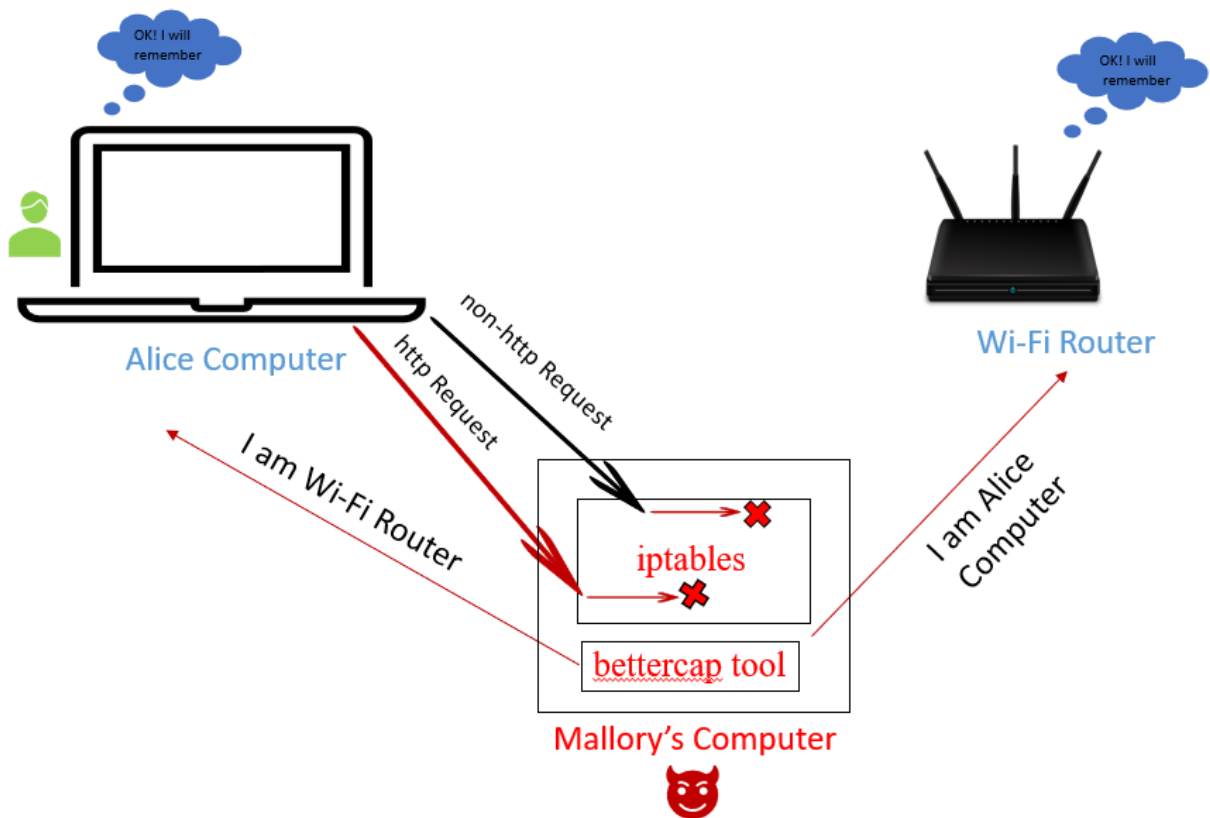


d. `iptables -t nat -A PREROUTING -p tcp --dport 01: -j REDIRECT --to-port 8080`

`--dport 01:` means all destination ports starting from 1.

On the Windows machine, navigate to an HTTP server (web.interhack.com). Try to navigate to an HTTPS server (google.com). What do you observe?

Effect of running bettercap tool and iptables tool:



Executing this rule blocks all TCP traffic because **01:** represents all destination ports. As a result, neither HTTP nor HTTPS web browsing works. But you can still play a video on youtube.com as playing a video uses UDP traffic.

So far in the rule we have only blocked tcp traffic. So, video traffic is still working as it uses udp protocol. Let's block this traffic as well.

e. `iptables -t nat -A PREROUTING -p udp --dport 01: -j REDIRECT --to-port 8080`

This blocks all TCP and UDP traffic. As a result, HTTP or HTTPS web browsing does not work or video playing does not work.

f. At this point, victim can only do this: `ping google.com`

Now, you should have a better understanding of how modifying the rules in the iptables can help us achieve man-in-the-middle attacks.