**CYBER SECURITY & DIGITAL FORENSICS**

Practical-2

Vulnerability scanning using Nikto in Kali Linux

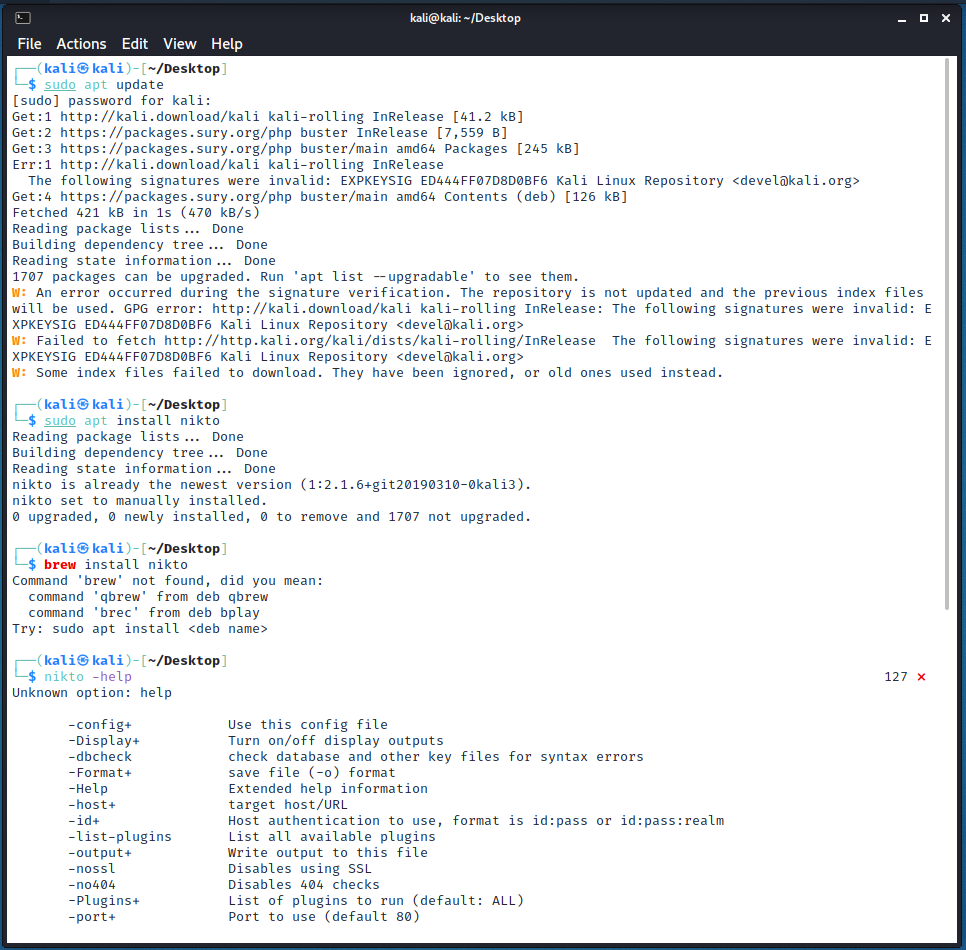
* **Required Software**
  + Kali linux
  + VMware
  + Nikto
* **Vulnerability scanning using Nikto in Kali Linux**

**Step 1-Setting up Nikto**

Check the vulnerability analysis category within Kali Linux to see if it is there; otherwise, you can get Nikto from its GitHub since it is open source or use the apt install command in Kali Linux:

*$*sudo apt update

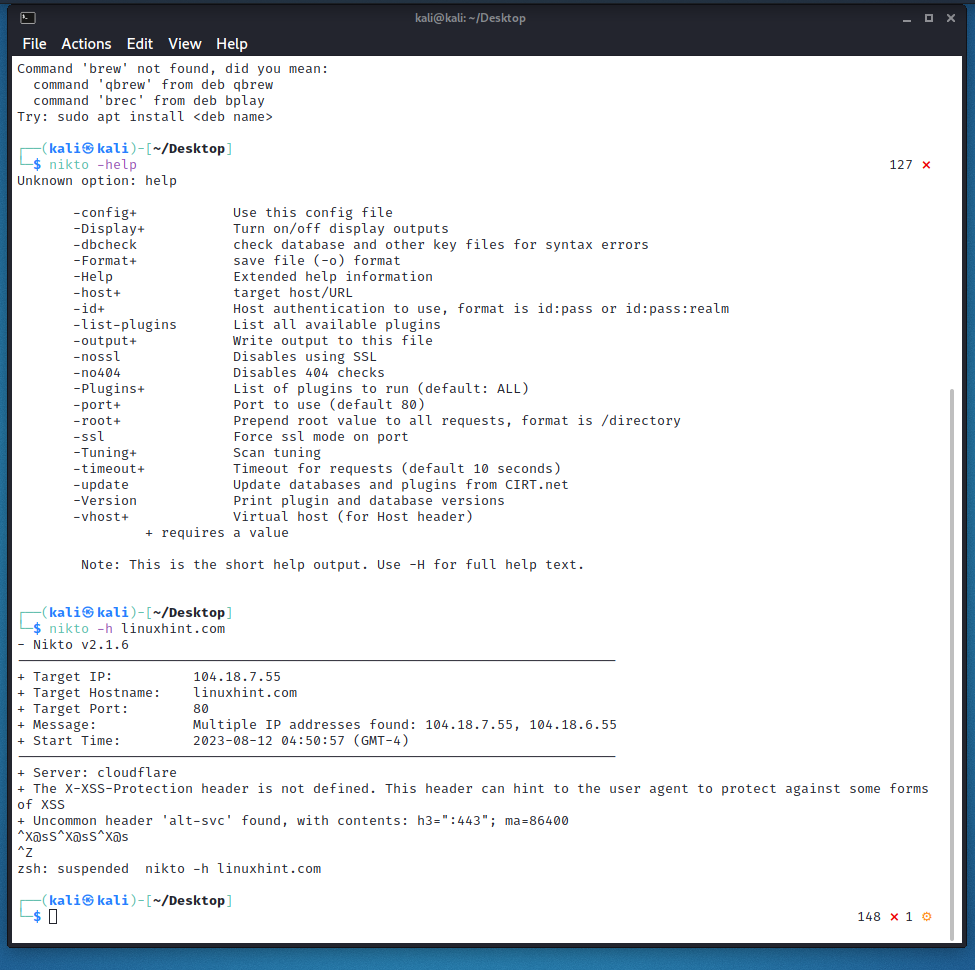
*$*sudo apt install nikto



**Step 2-Getting started**

Use the –Help to see a detailed guide on all the inputs Nikto can take and what each input does. Recommended for those who’re new to this.

*$*nikto -help

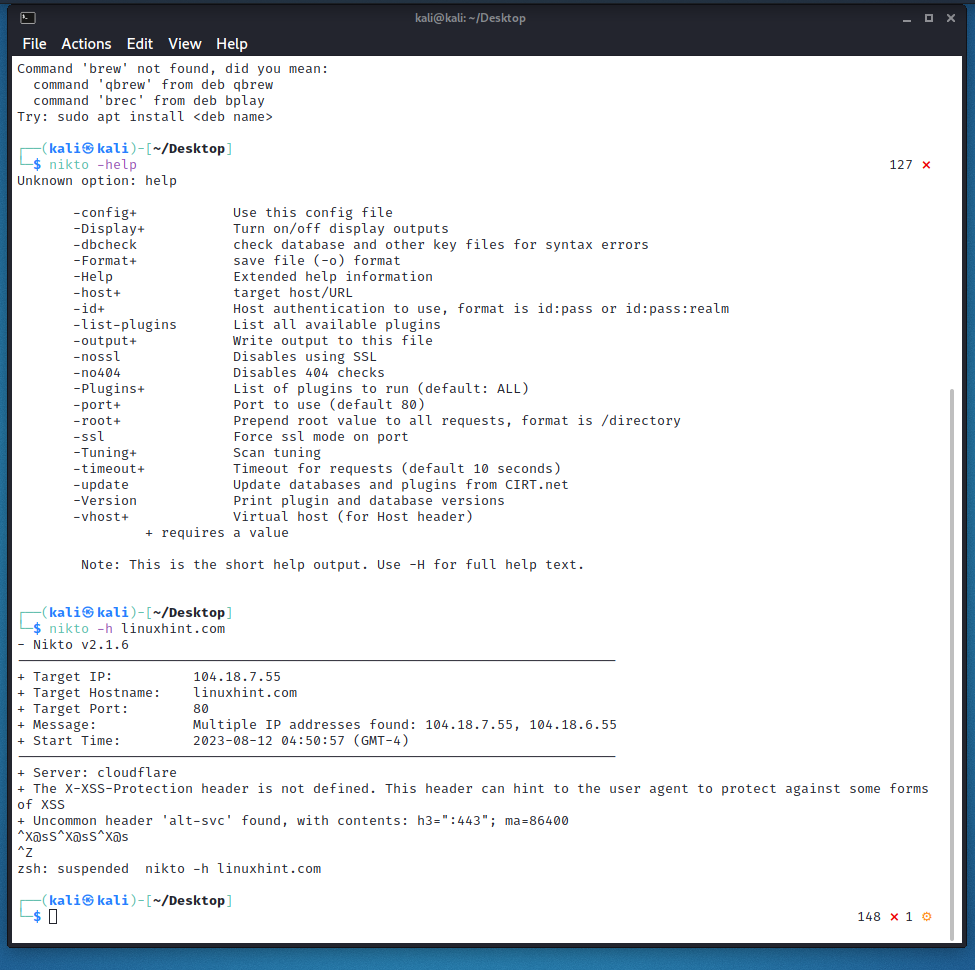


**Step 3-The scanning basics**

Let’s discuss all the basic syntax we can instruct Nikto with.

Substitute the default IP or hostname with a hostname of your choice:

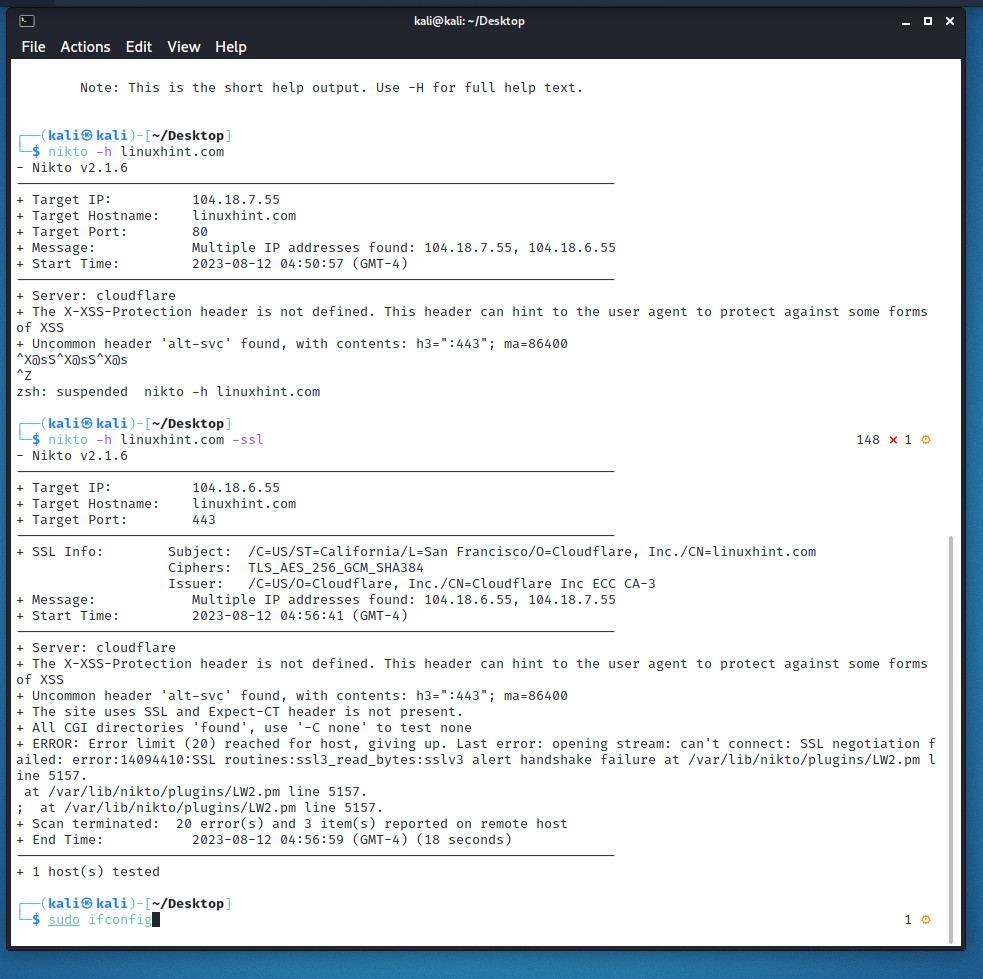
*$*nikto -h linuxhint.com



We can**perform a basic scan** to look for port43 and SSL, which has widespread use in HTTP websites. Although Nikto doesn’t need you to specify the type, specifying helps Nikto save some time with scanning.

To **specify an SSL website**, use the following syntax

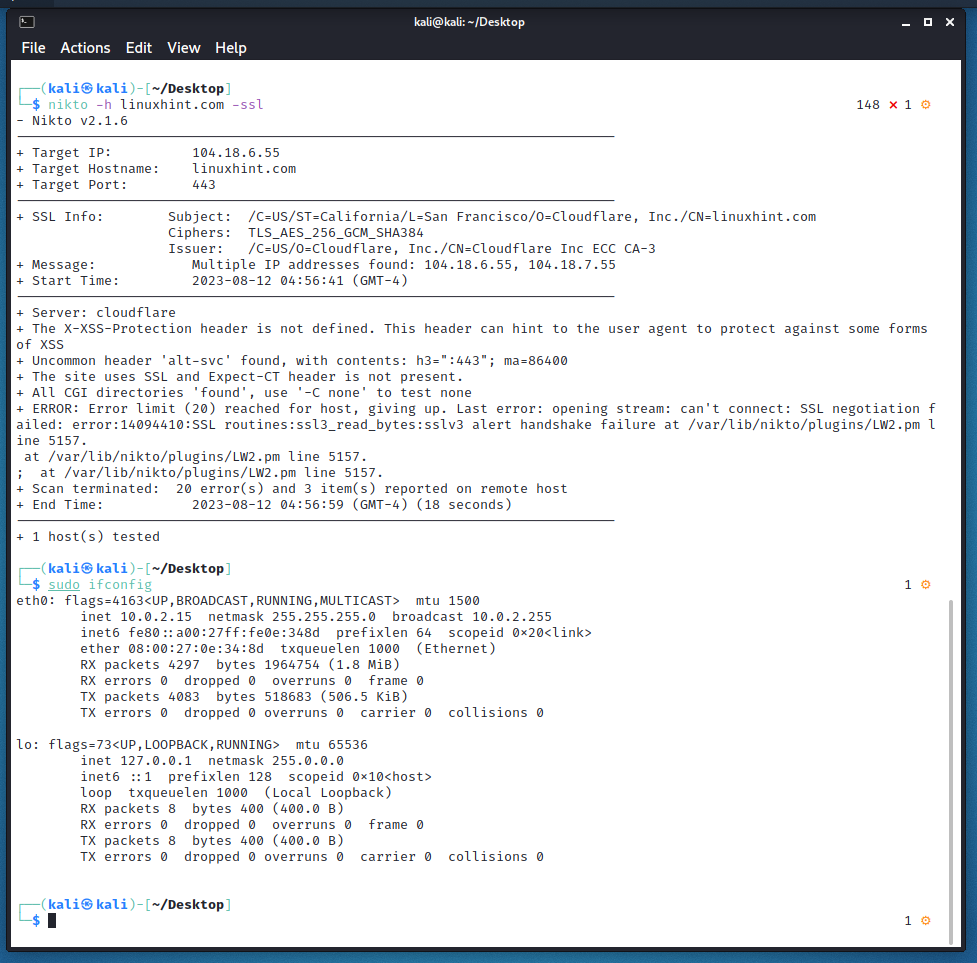
*$*nikto -h linuxhint.com -ssl



### Step 4-Scanning SSL enabled websites with Nikto

Here, we’re scanning pbs.org for demonstration. We shall also learn in this section about the different information Nikto reports once it’s finished with scanning. To initiate scanning, type:

*$*nikto -h pbs.org –ssl



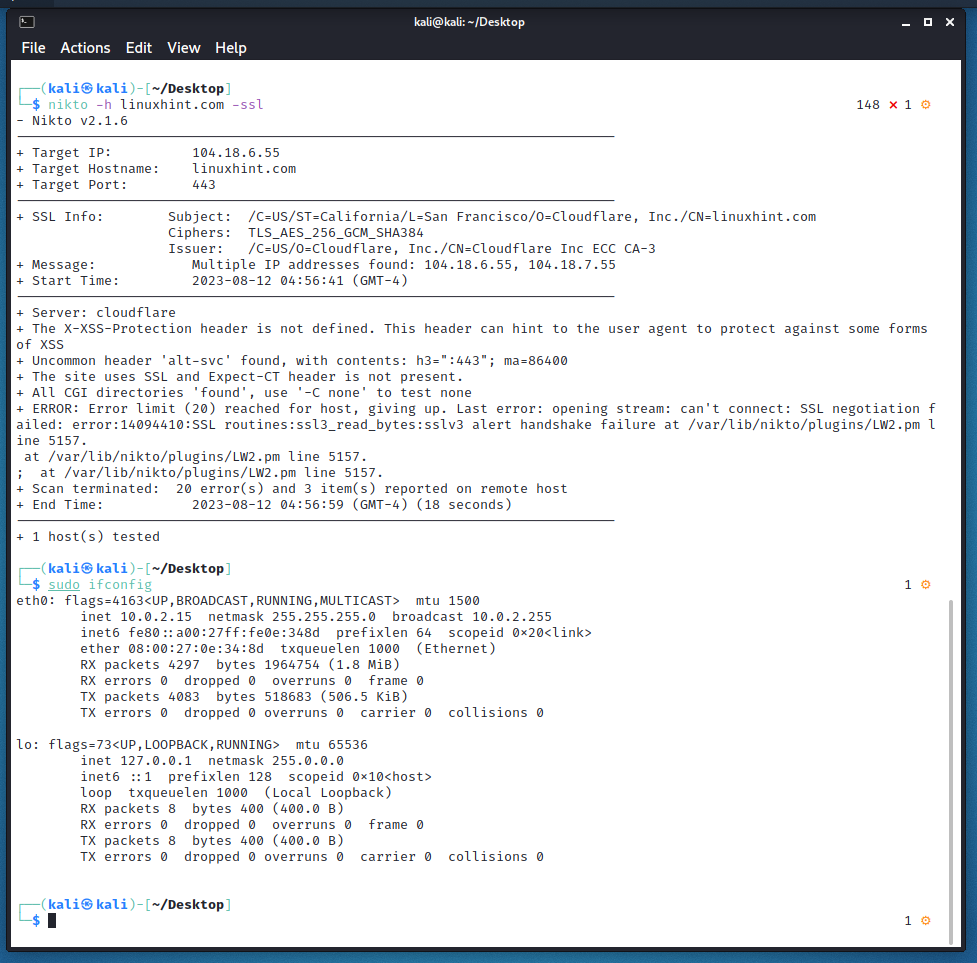
We’ve performed a quick scan of pbs.org

Upon connecting to port 443, it displays some info about the cipher that we can examine. The information here is not very relevant to what we’re trying to do, so we’ll move on to performing more elaborate scans.

**Step 5-Scanning IP addresses**

Nikto can also be used on the local network to search for any embedded servers. To do that, we’ll need to know our IP address. Type the following in command terminal to see the IP address of your local machine’s use.

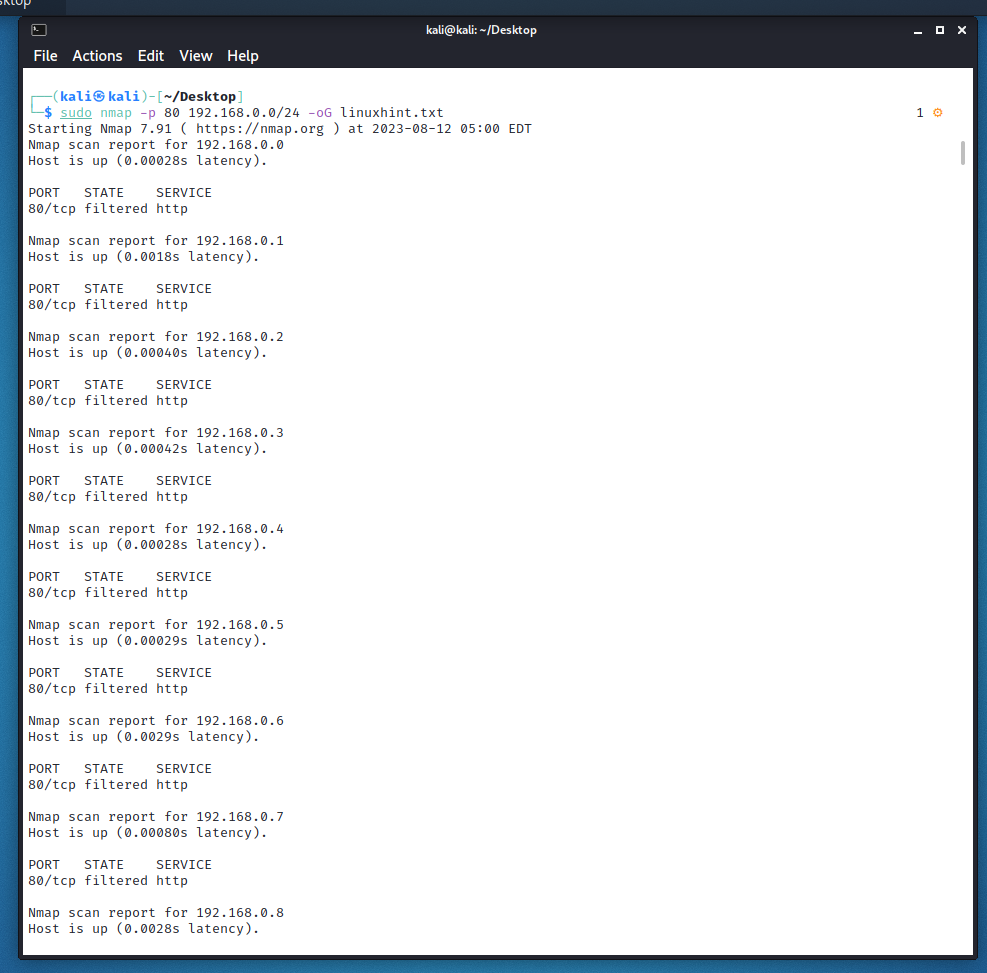
*$*sudo ifconfig

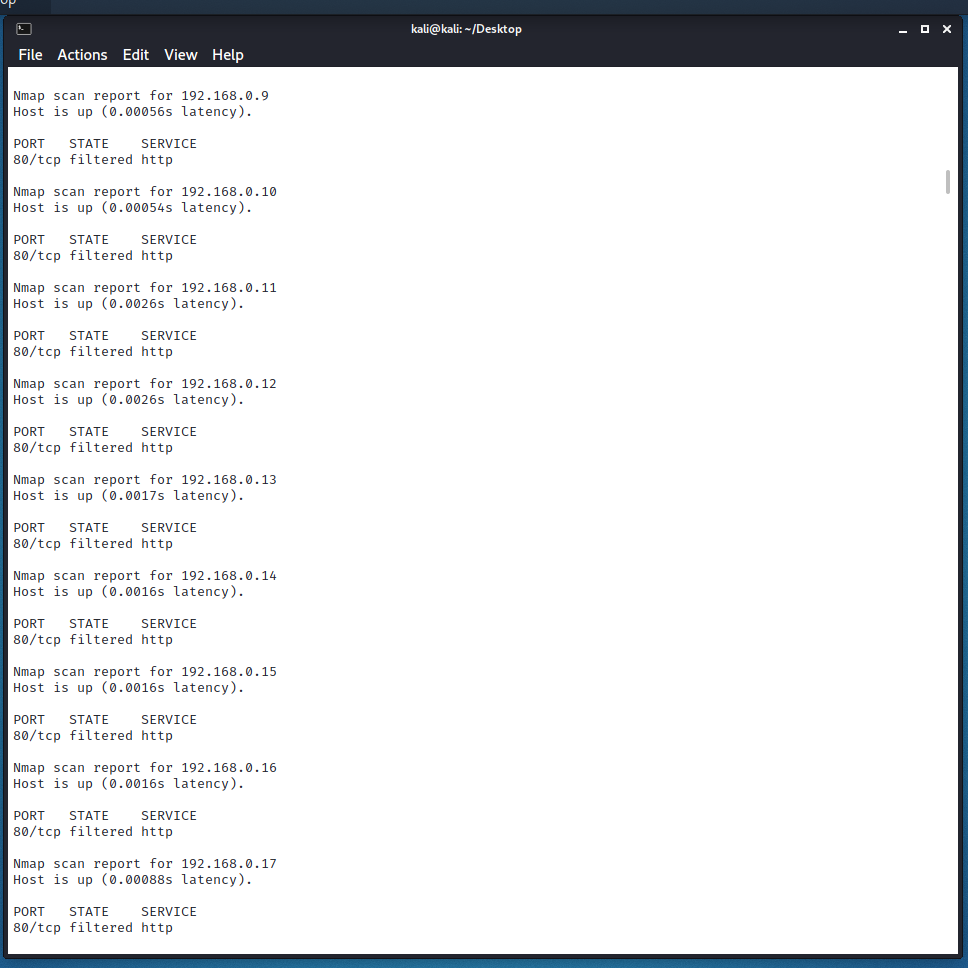


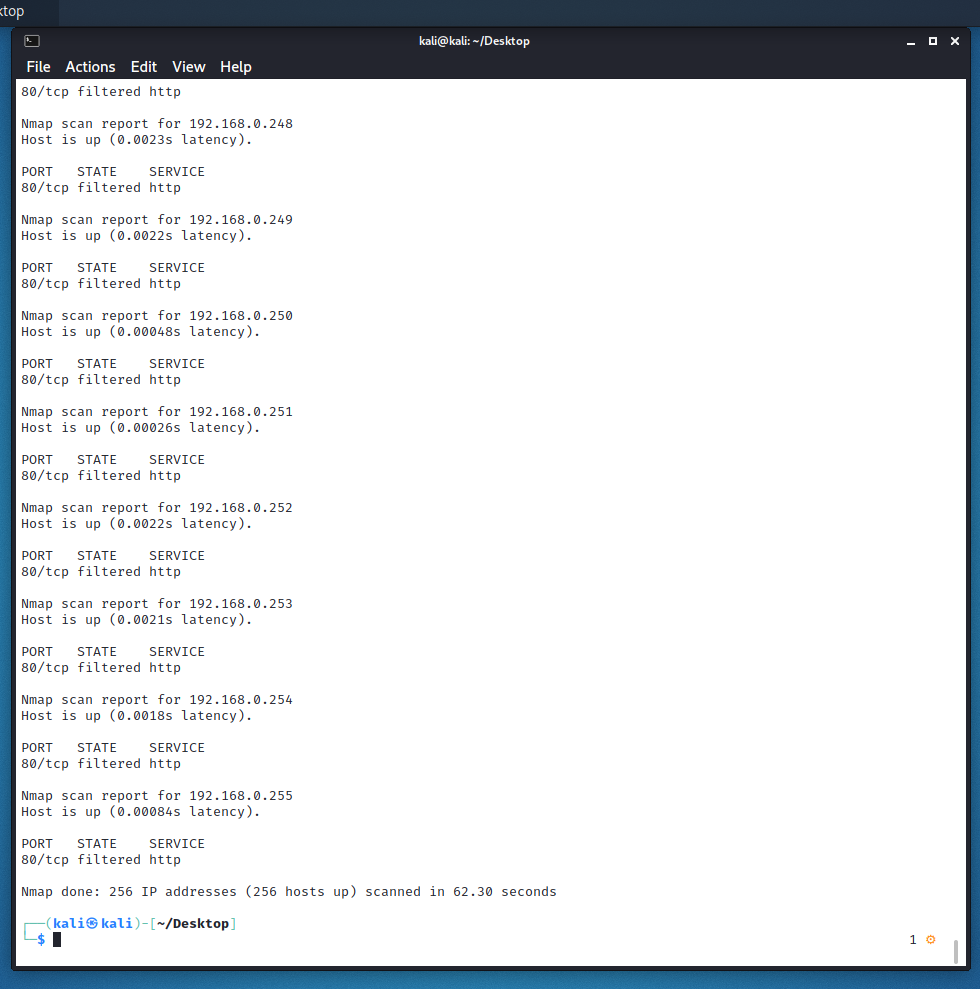
The IP address that we require is the one followed by ‘inet’, so note it down. You can work out your network range by running an ipcalc on it, which you can easily download and install with apt install ipcalc if you don’t have it installed already.

Let’s scan for services running on our local network by scanning port 80 within our range using Nmap. This will extract only the hosts that are currently up and running, as these are the ones with their port 80 open. Here, we’re exporting this data into a file we’ll name nullbye.txt:

*$*sudo nmap -p 80 192.168.0.0/24 -oG linuxhint.txt

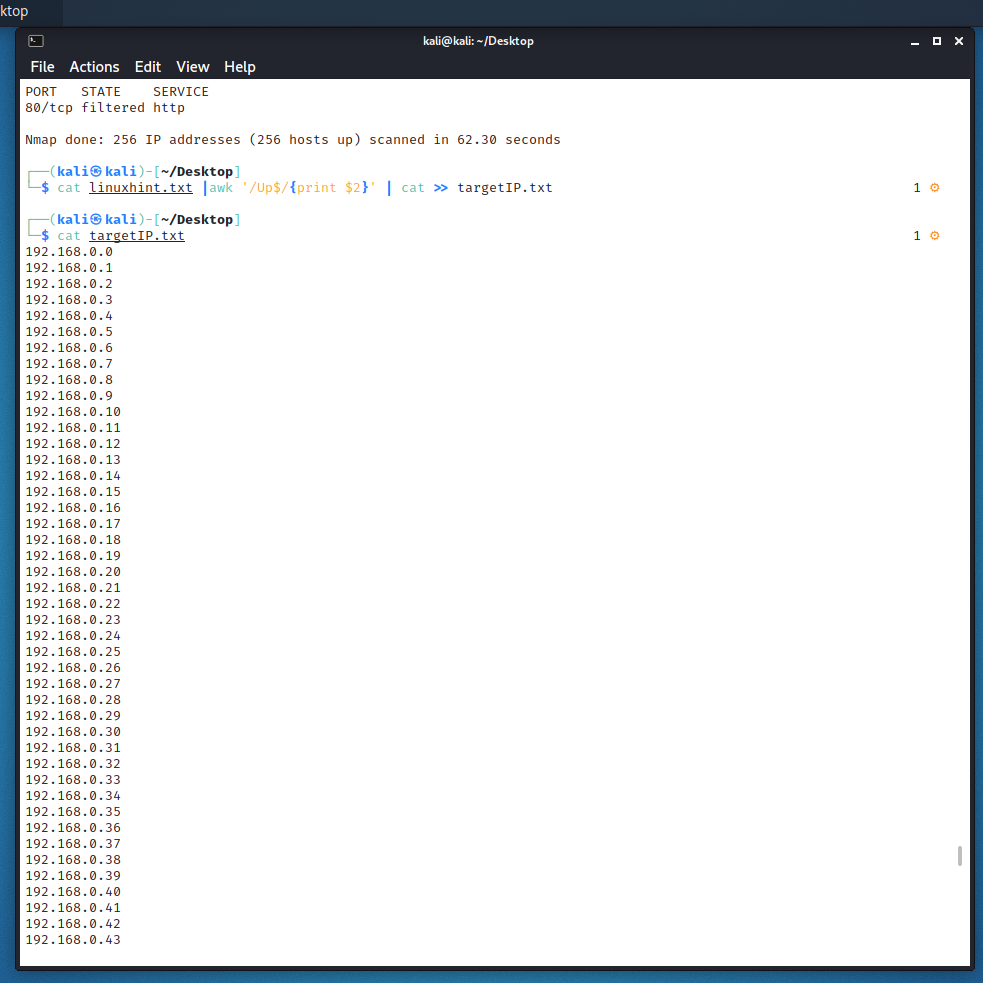






To forward the list of all the current hosts extracted by Nmap to Nikto, we can use the cat to read the file we exported the info to. Here’s the code to run to do so:

*$*cat linuxhint.txt | awk '/Up$/{print $2}' | cat >> targetIP.txt



Let’s talk about each element in the previously stated line of code.

**awk**– searches for the pattern within the targeted file that follows ‘cat’ in the syntax

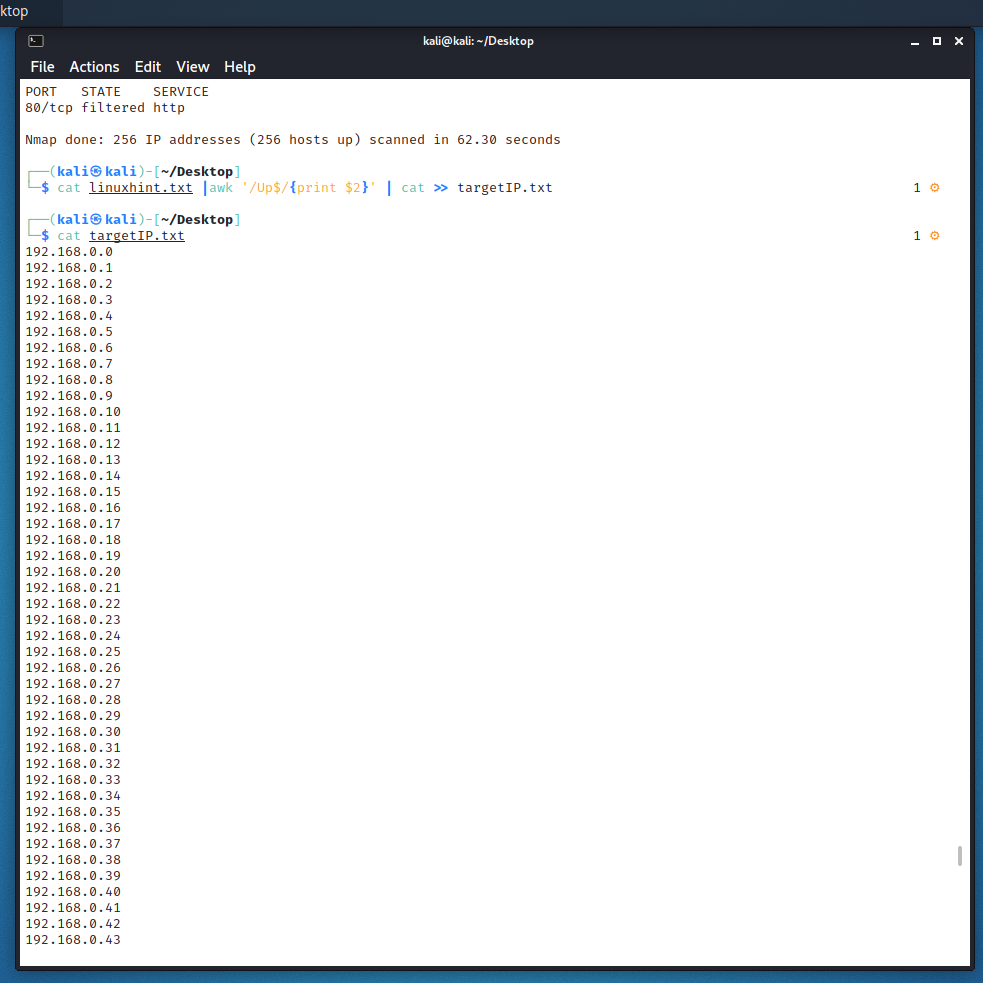
**Up**– about the fact that the host is up

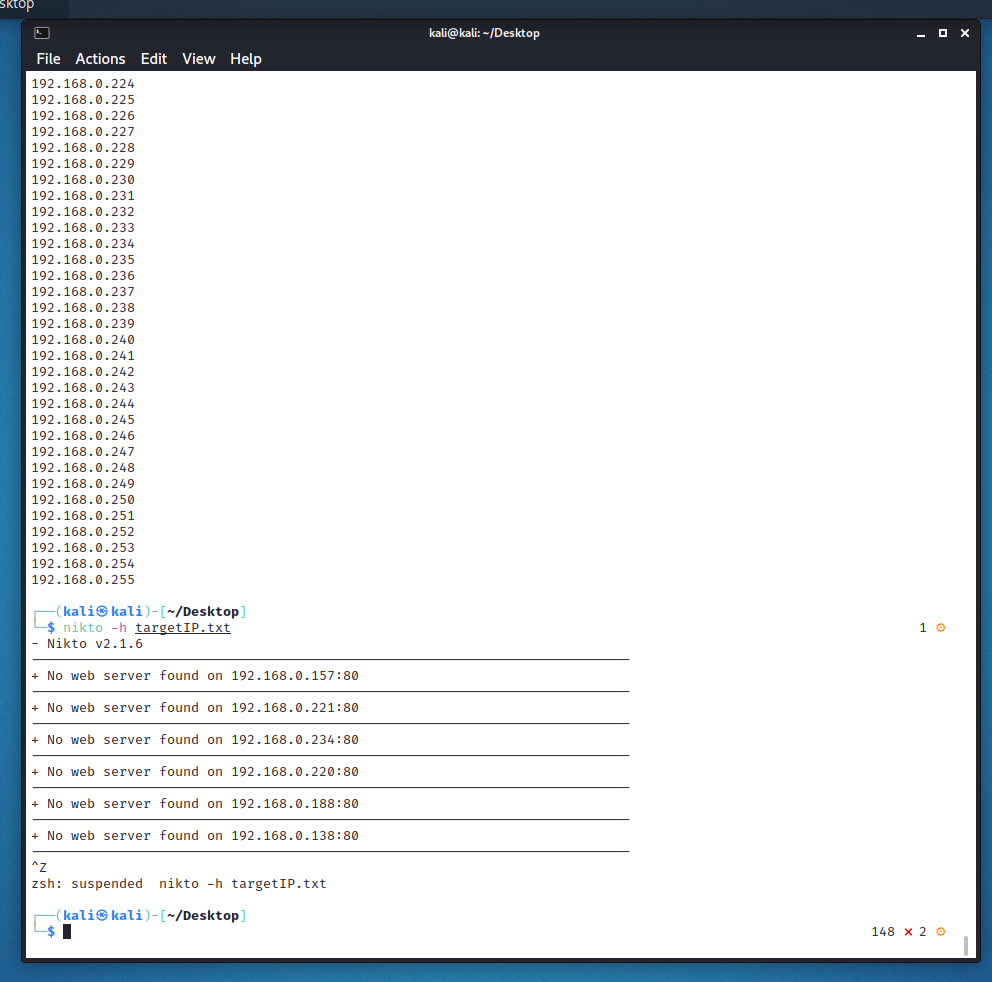
**Print $2**– means you’re instructing to print out the second word in each line of the .txt file

targetIP.txt is just a file we’re sending our data to, which in your case you can name it whatever you want.

Now we can access our new file, which is targetIP in our case, to see what IP addresses have port 80 open.

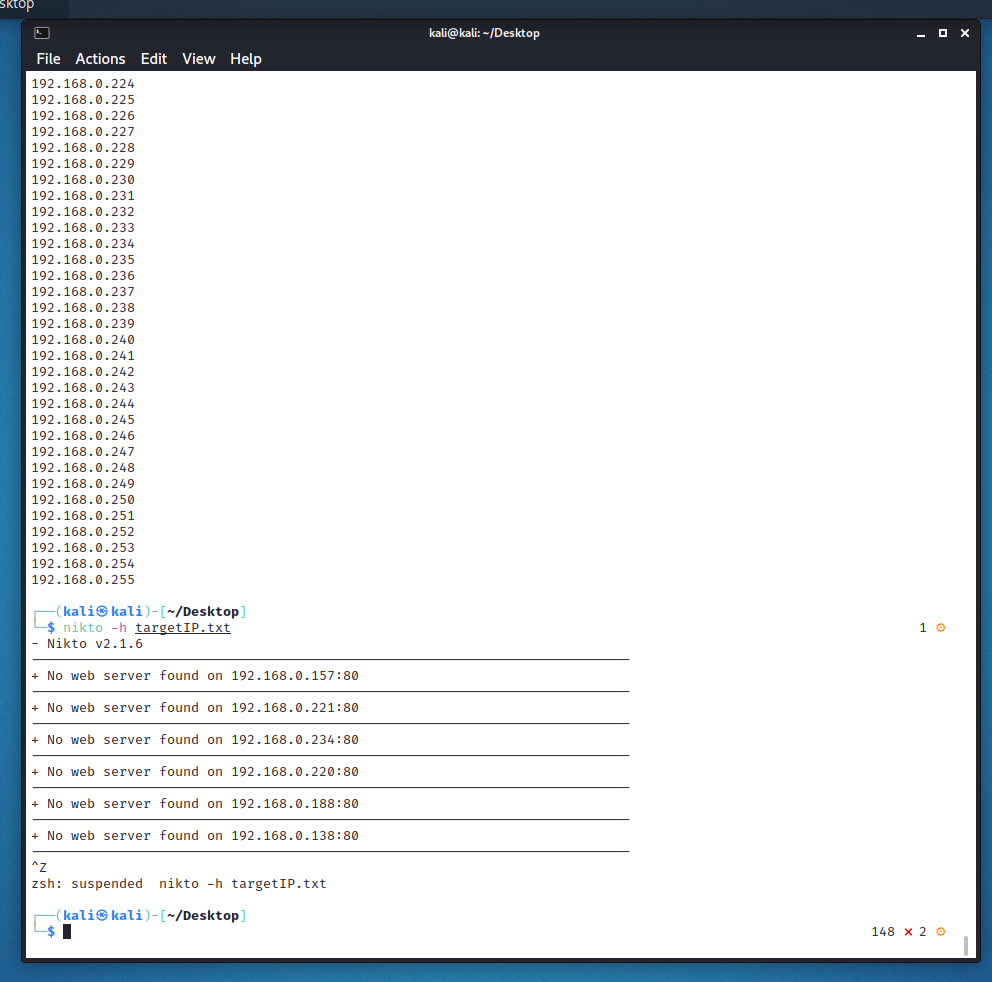
*$*cat targetIP.txt





Send its output over to Nikto with the following command:

*$*nikto -h targetIP.txt

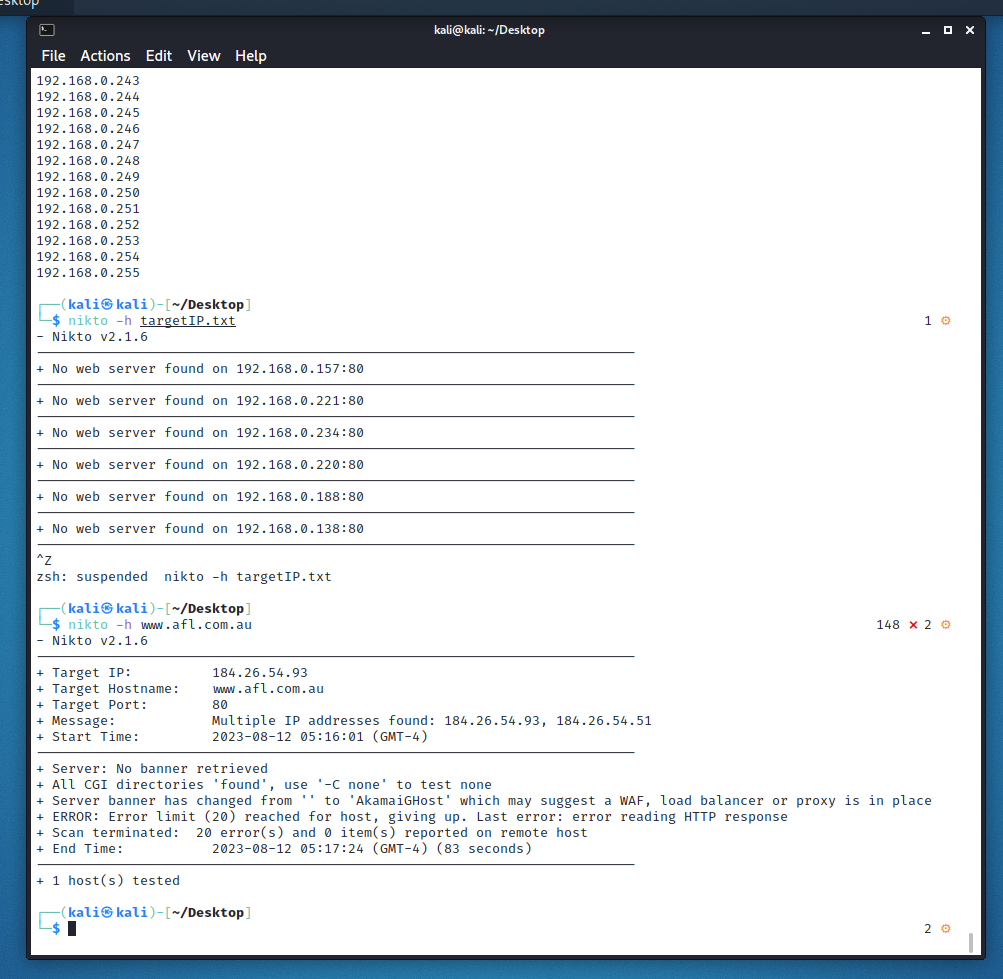


Notice how similar the results here are when compared to those we received in SSL web scanning.

**Step 6-Scanning HTTP websites with Nikto**

Let’s scan afl.com.alu to see how HTTP scanning with Nikto looks like. WE’re once again scanning for web domains that are easy pickings using port 80.

*$*nikto -h www.afl.com.au



The information herewith most relevant to our users is the directories it has located. We can use these to acquire any user credentials, among other things that were either misconfigured or were unintentionally left open to be accessed.

**Coupling Nikto with Metasploit**

Once you’re done with web scanning, you’re eventually going to move on to perform the actual pen testing, preferably with Metasploit. So it’s a good thing that Nikto comes with functionality that lets you export information to other reconning tools.

To export information into a format readable by Metasploit, you may perform the scan as we’ve explained above, but add -Format msf+ after the code, like:

*$*nikto -h linuxhint.com -Format msf+