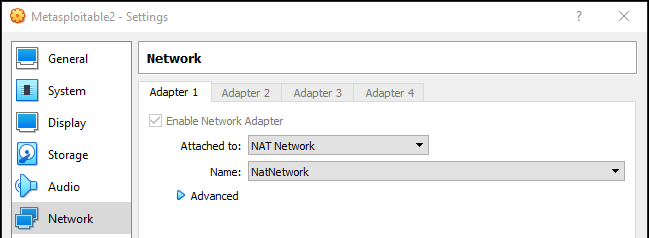
# Lab – Automated Recon/Enumeration Using nmapAutomator

# Overview

In the lab, you will learn how to install and use an automated script that will perform many of the reconnaissance processes and enumeration we usually run against a new target. This excellent tool was developed and created by 21y4d whose Github profile can be seen [here](https://github.com/21y4d).

**Lab Requirements**

* One virtual install of Kali Linux
* One virtual install of Metasploitable2.
* Internet connection
* Ensure both virtual machines have their VirtualBox network setting set to NAT Network.



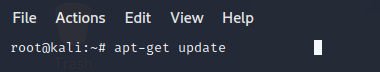
**Required:**

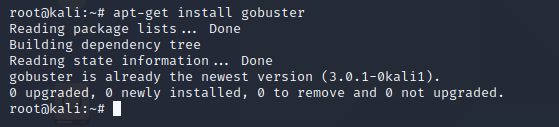
Gobuster v3.0 or higher

You can update gobuster on kali using:

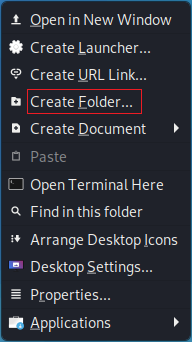
apt-get update

apt-get install gobuster

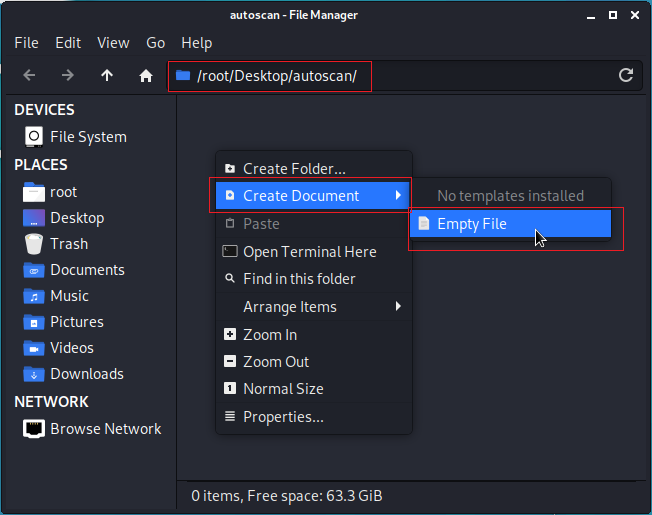
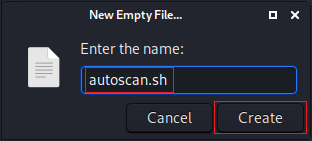




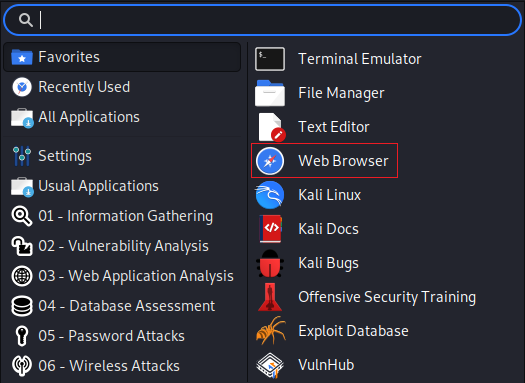
From your Kali desktop, create a new folder called **nmapAutomater,** all lowercase.



Inside the new folder, create a new document. Name the new document, **nmapAutomater.sh**.



In Kali, from the application quick launch bar, open a web browser.



Type or copy and paste the following URL into the address bar.

<https://github.com/21y4d/nmapAutomator/blob/master/nmapAutomator.sh>



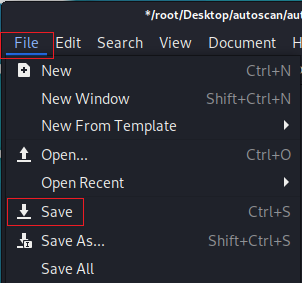
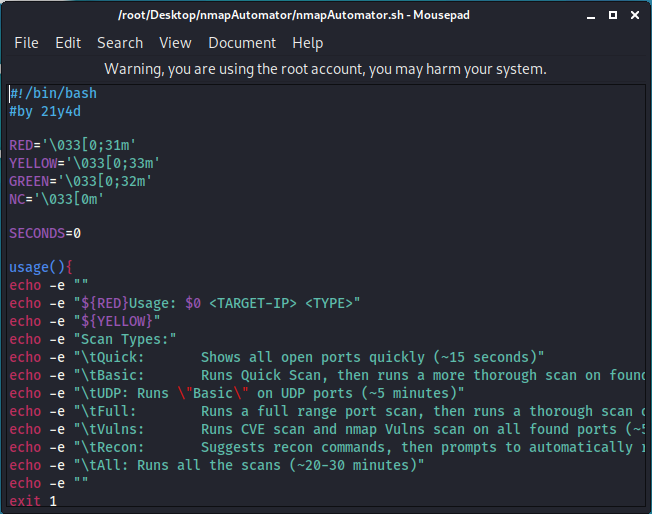


When the page loads, click on the Raw button to view the script.

On the next page, place your mouse anywhere in the right white box. Hold down the Ctrl key and the letter A to select all the text. All the text should now be highlighted in blue. Hold down the Ctrl and press the letter C. This will copy all the highlighted text. Minimize the browser.

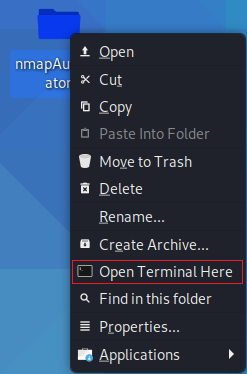
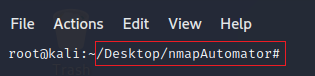
From your Kali desktop, open your nmapAutomater folder. Open the nmapAutomator.sh file. Place your mouse anywhere inside the blank document, right-click, and select Paste from the context menu. You should see something like the following.

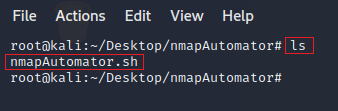
From your document’s taskbar, click File, and from the context menu, click Save.

Close the file. Close the folder. From your Kali desktop, right-click on your nmapAutomater folder, and from the context menu, select Open Terminal Here.

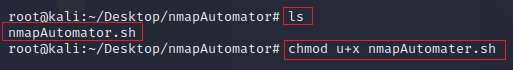
At the terminal prompt, type, **ls**. You should see the contents of the nmapAutomater folder.





We next need to make the file an executable. At the prompt, type

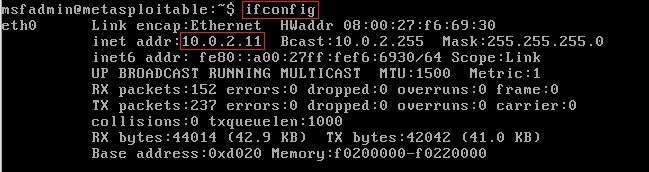
**chmod u+x nmapAutomater.sh**



Press enter. The terminal returns the prompt, letting you know the command completed successfully.

Launch your virtual install of Metasploitable2. Once the machine has started, log in using the username and password of **msfadmin**.

At the prompt, type ifconfig. Find and note the IP address of your eth0 interface. This is my IP address; yours will differ.



The options for running nmapNmapAutomater are as follows. To run the program, we right-click on the nmapAutomator folder and from the context menu, Select Open Terminal Here.

At the prompt, use the option that uses the All option.

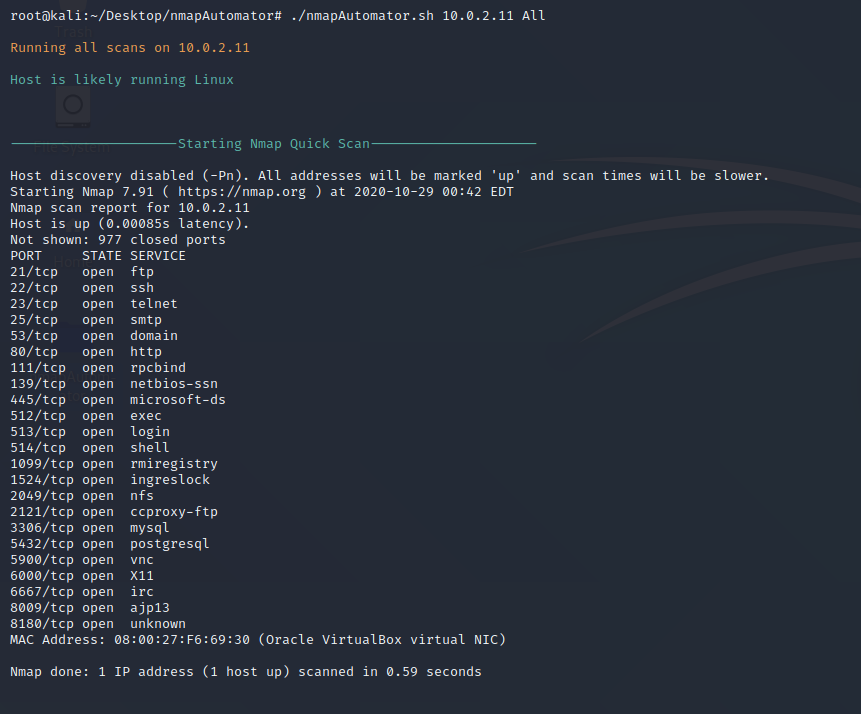
./nmapAutomator.sh <TARGET-IP> <TYPE>

**./nmapAutomator.sh 10.0.2.11 All**

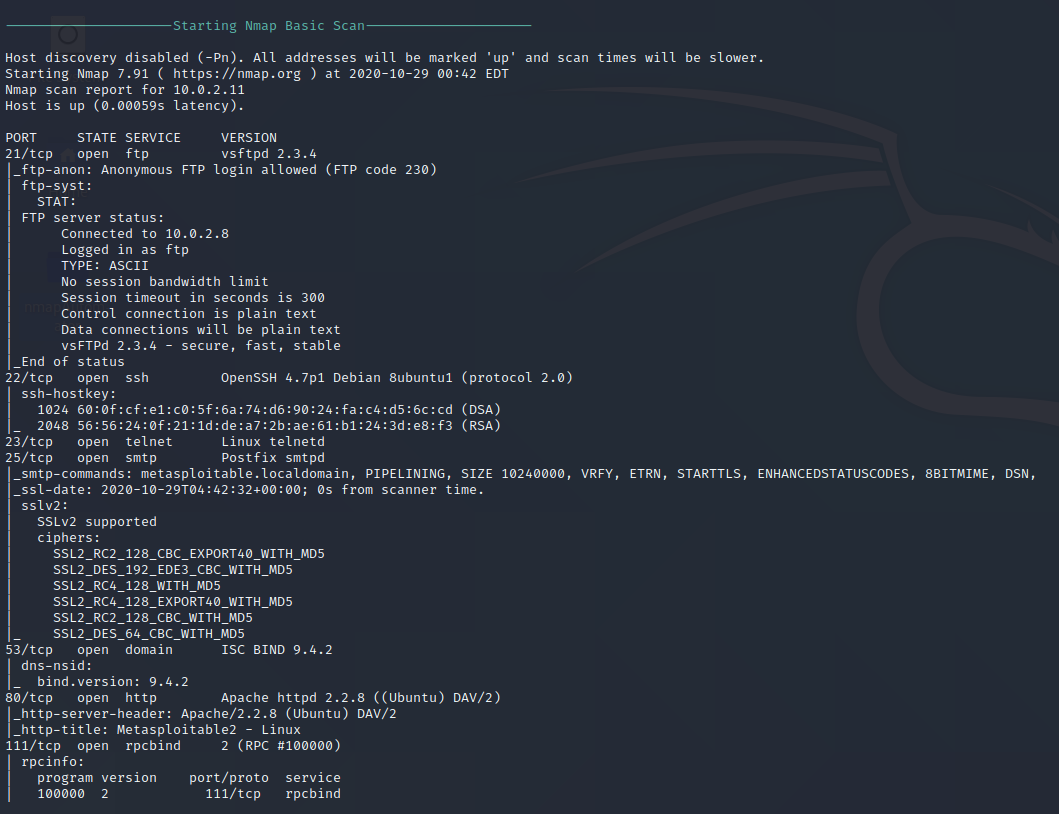
./nmapAutomator.sh 10.0.2.11 Basic

./nmapAutomator.sh 10.0.2.11 Recon

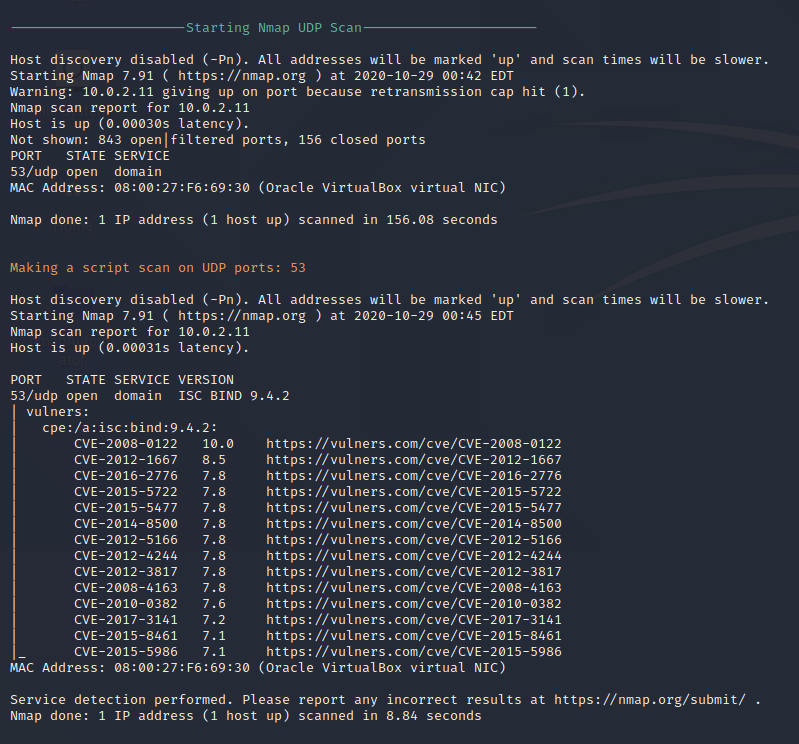
Right away we ae given the **quick scan** results.



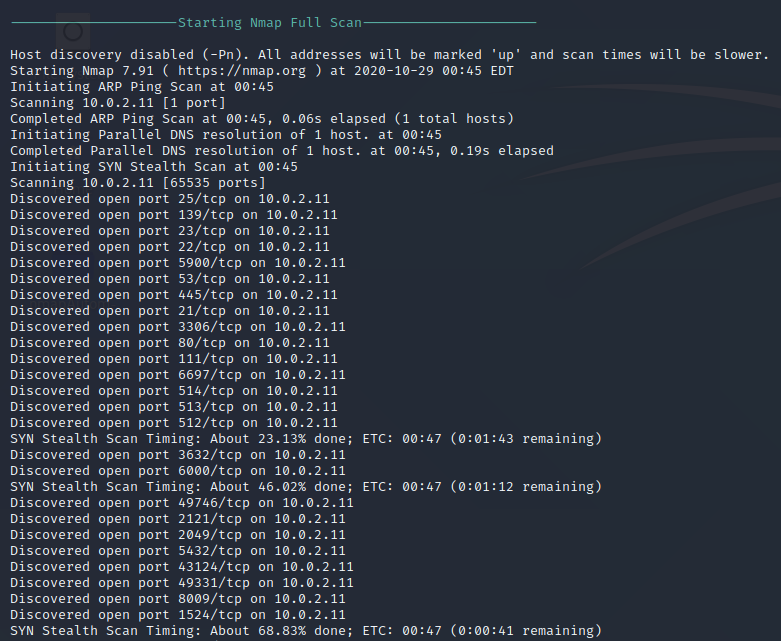
Next, from the results, we are presented with the **basic scan** results.

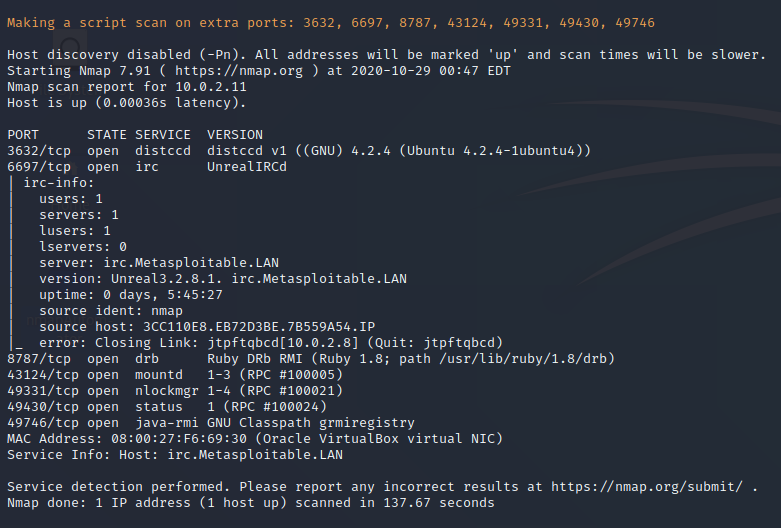


Next, we have the **UDP scan** complete with a script scan showing the vulnerable CVE’s.

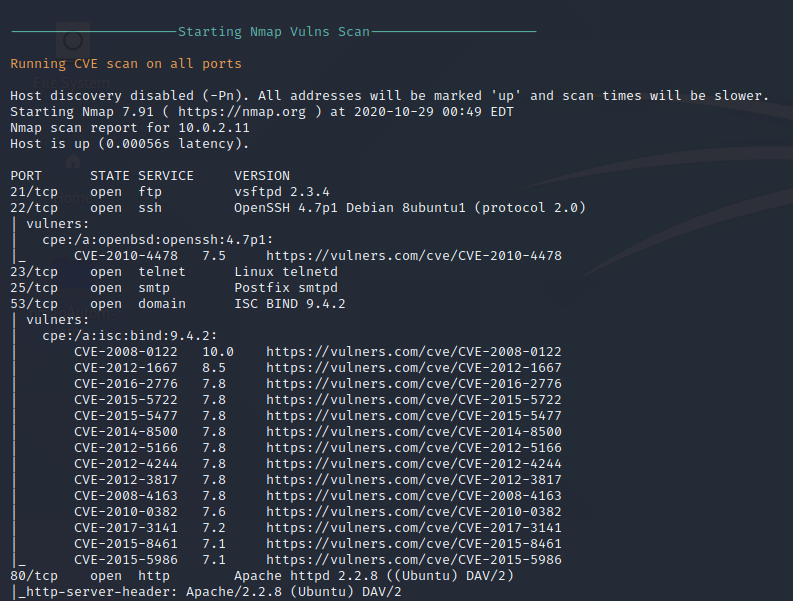


Next, we have the **full scan**.

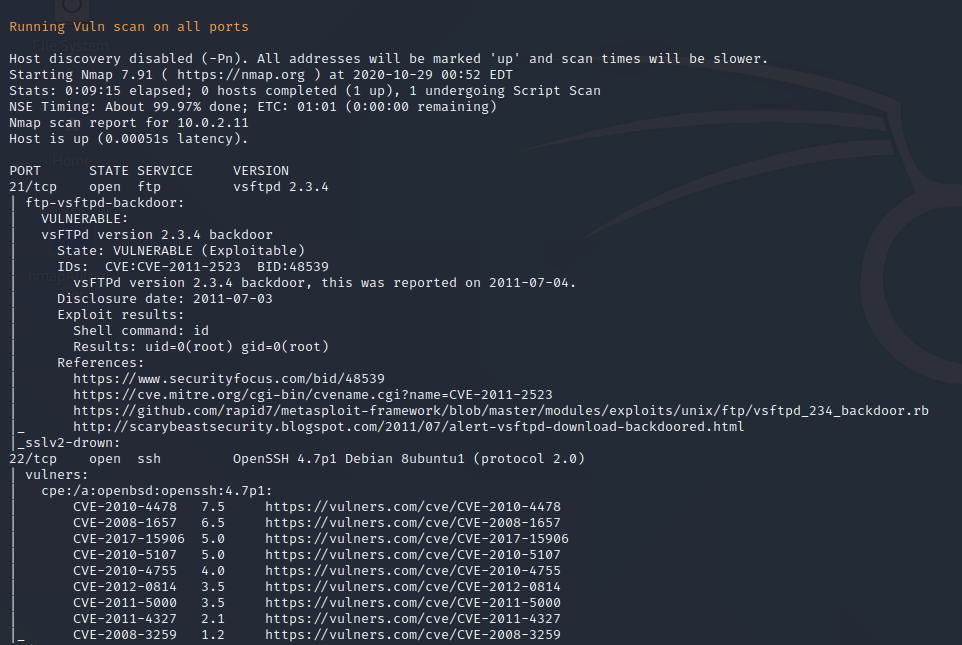




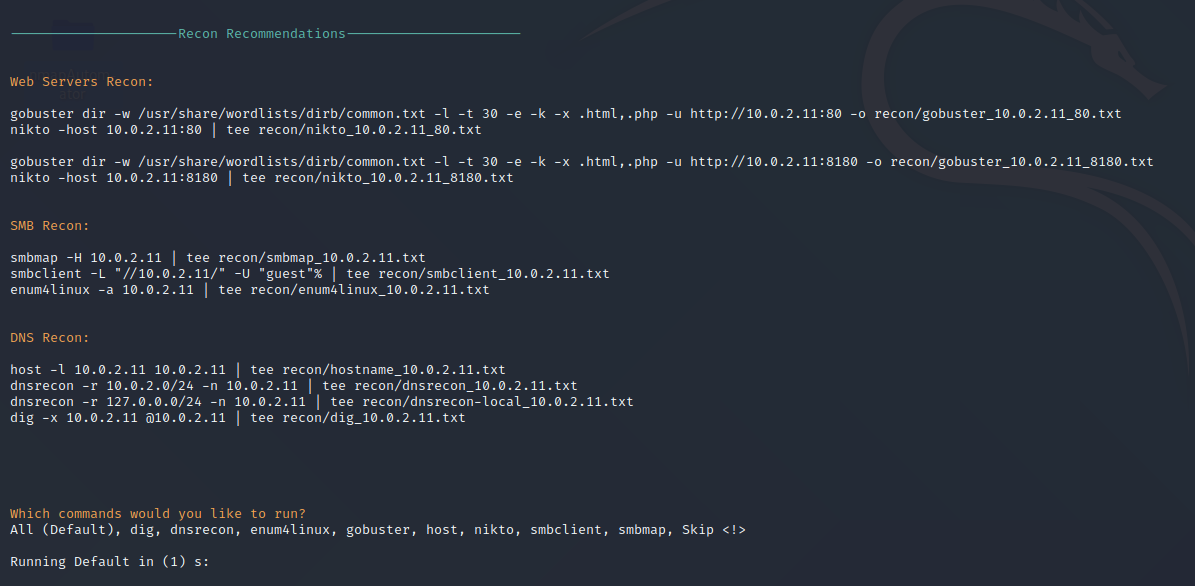
Next, we have the Nmap **Vulns Scan**



The next scan is the Vuln scan being run on all ports. This is a long report.

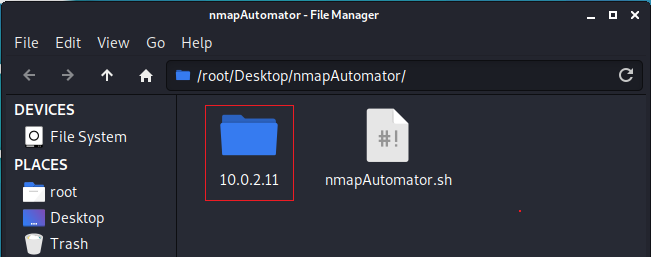


The last scan is the **Recon recommendations**. Here you can run additional scans using some of the additional tools that come with Kali.

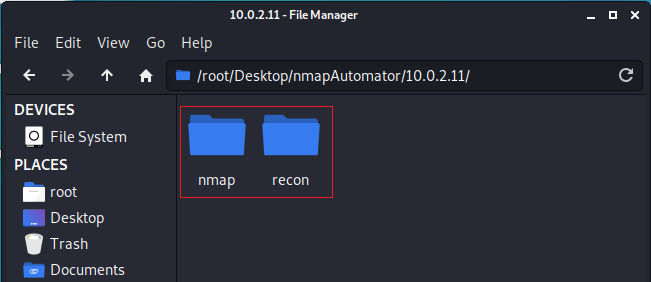


Not all the tools may be installed, but most can be installed using the **apt get install** command.

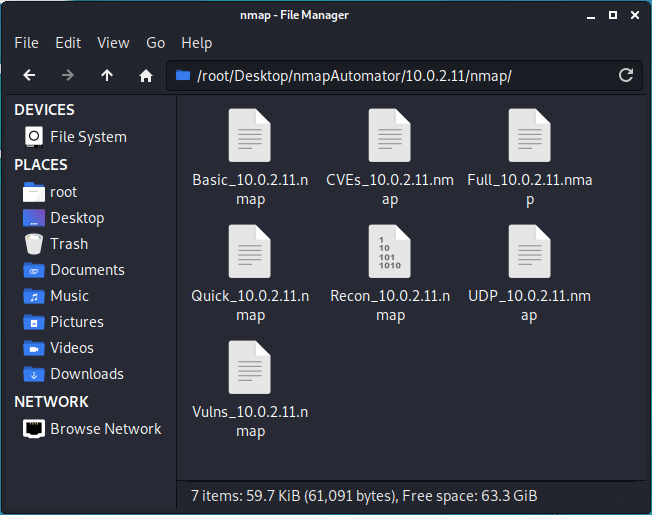
Minimize your terminal showing the scan results. From your terminal, open your nmapAutomator folder. Here you will find text files containing all the different scan results.



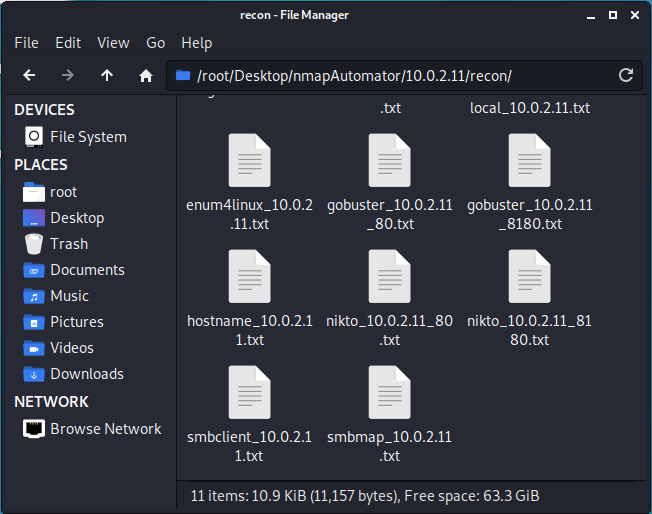
When you open the scan results, you will be presented with two subfolders.



Inside each subfolder, you will find a text file showing the results for each scan. Here we see the scan results of the nmap scan.



In the recon folder, you have the scan results from the following additional tools.



Other Recon tools used within the script include:

* nmap Vulners
* sslscan
* nikto
* joomscan
* wpscan
* droopescan
* smbmap
* enum4linux
* dnsrecon
* odat

**Summary –**

The tool developer, 21y4d, wrote this script to help get him through the OSCP exam. The benefits of using this tool as a pentester, hacker, or trying to complete a CTF. This should be a part of everyone’s roottoolbox.