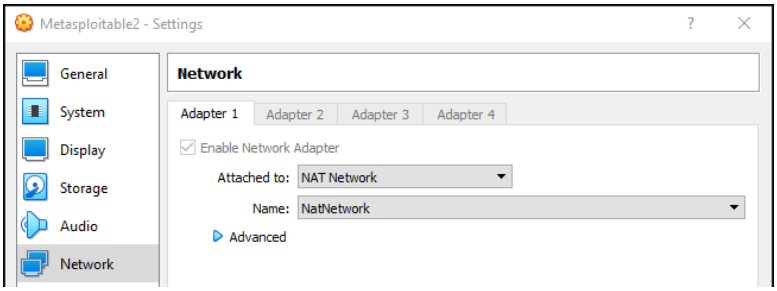
# Lab – Automated Recon/Enumeration Using nmapAutomator

## 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.

## 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.

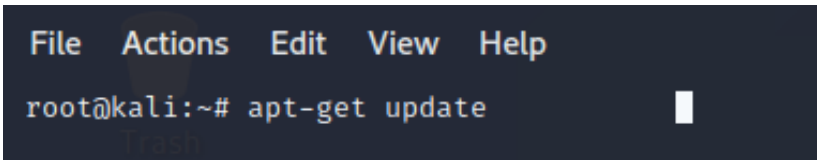


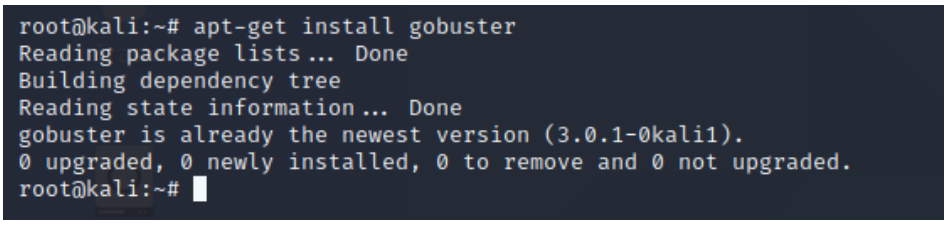

## Required:

Gobuster v3.0 or higher

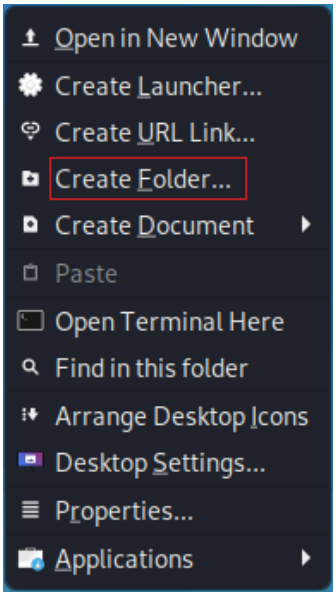
You can update gobuster on kali using:

```
apt-get update
apt-get install gobuster
```

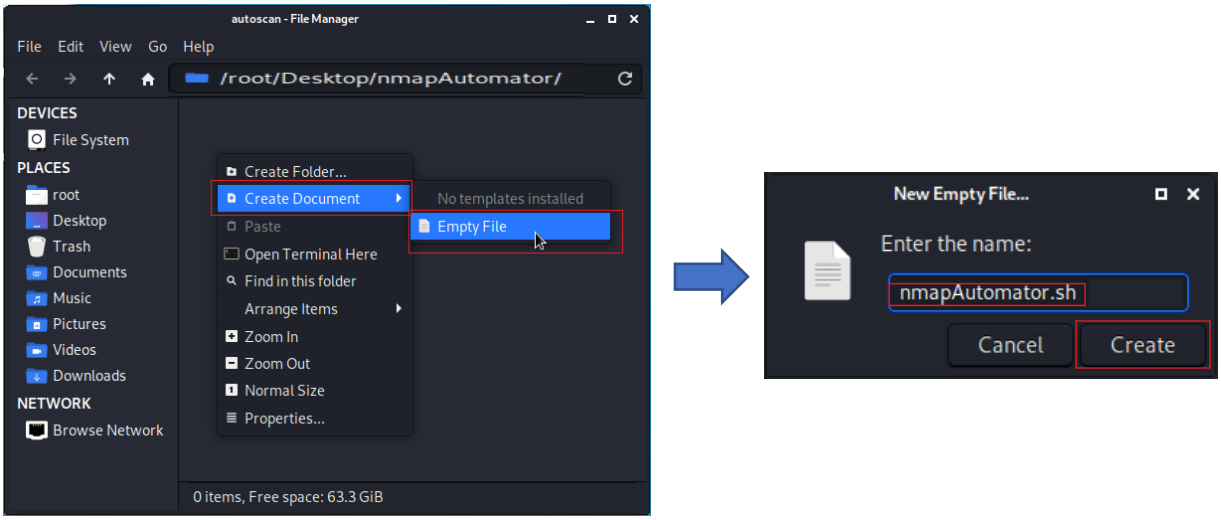


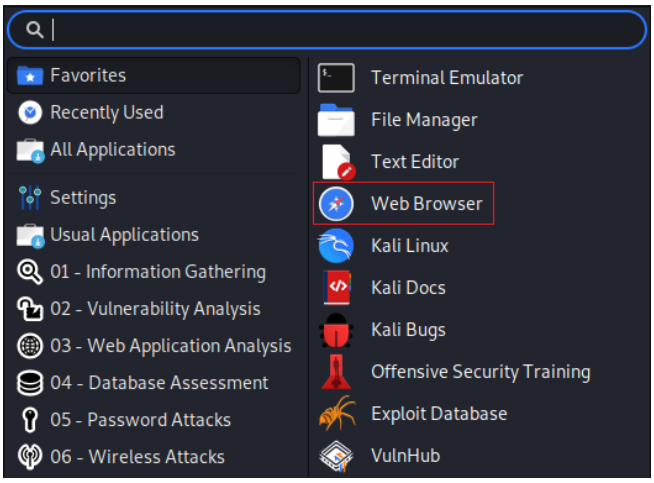
From your Kali desktop, create a new folder called **`nmapAutomater,`** all lowercase.




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

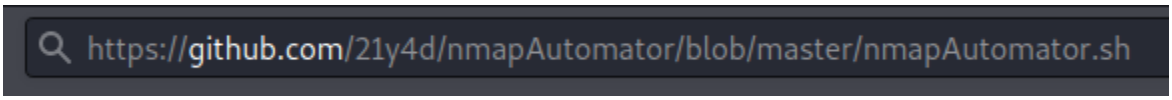



In Kali, from the application quick launch bar, open a web browser.

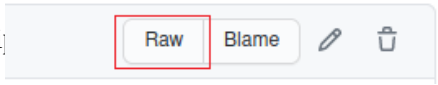



Type or copy and paste the following URL into the address bar.

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



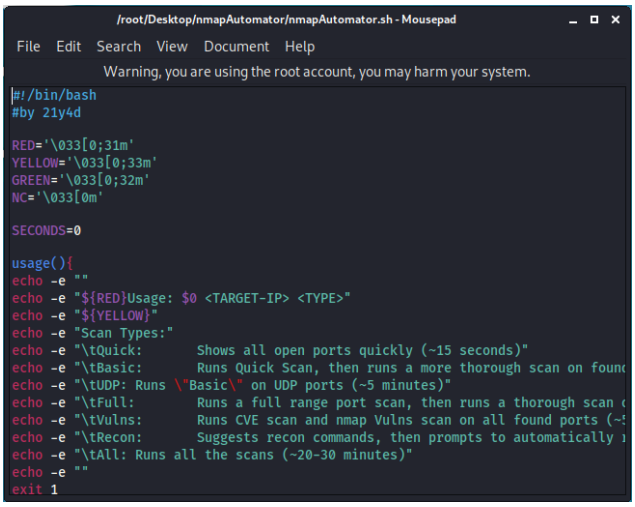

When the page loads, click on the Raw button to view the scri

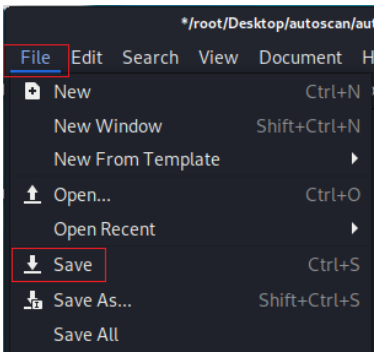



On the next page, place your mouse anywhere in the right white box. Hold down the Ctrl key and the letter A to select all the text. All the text should now be highlighted in blue. Hold down the Ctrl and press the letter C. This will copy all the highlighted text. Minimize the browser.

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.

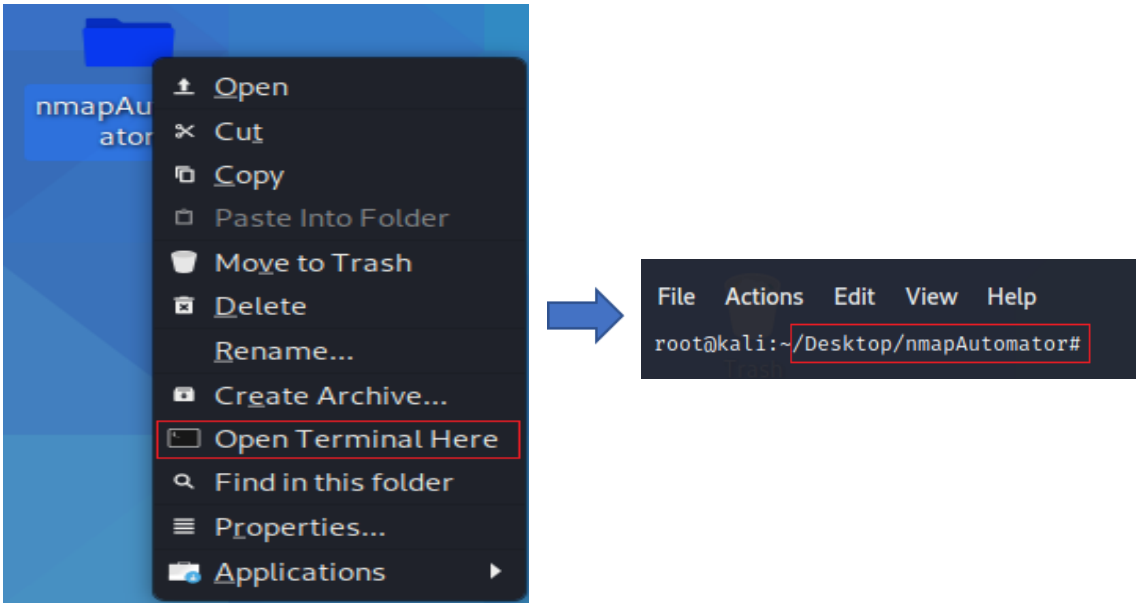
From your document's taskbar, click File, and from the context menu, click Save.

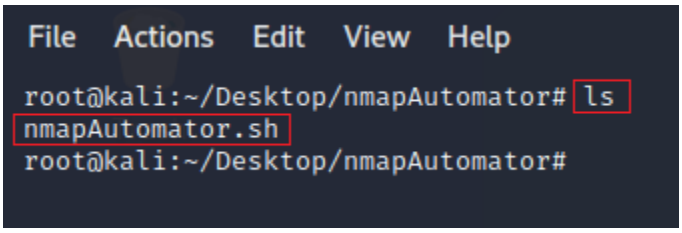


Close the file. Close the folder. From your Kali desktop, right-click on your nmapAutomater folder, and from the context menu, select Open Terminal Here.

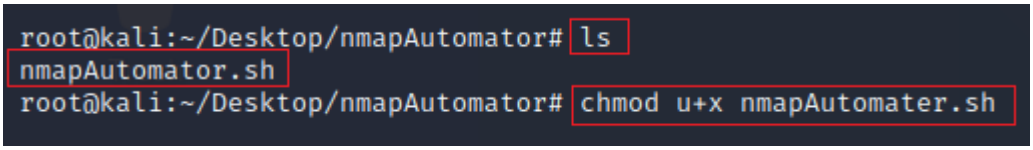
At the terminal prompt, type, **`ls`**. You should see the contents of the nmapAutomater folder.




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.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f6:69:30
          inet addr:10.0.2.11  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef6:6930/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:237 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:44014 (42.9 KB)  TX bytes:42042 (41.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

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**

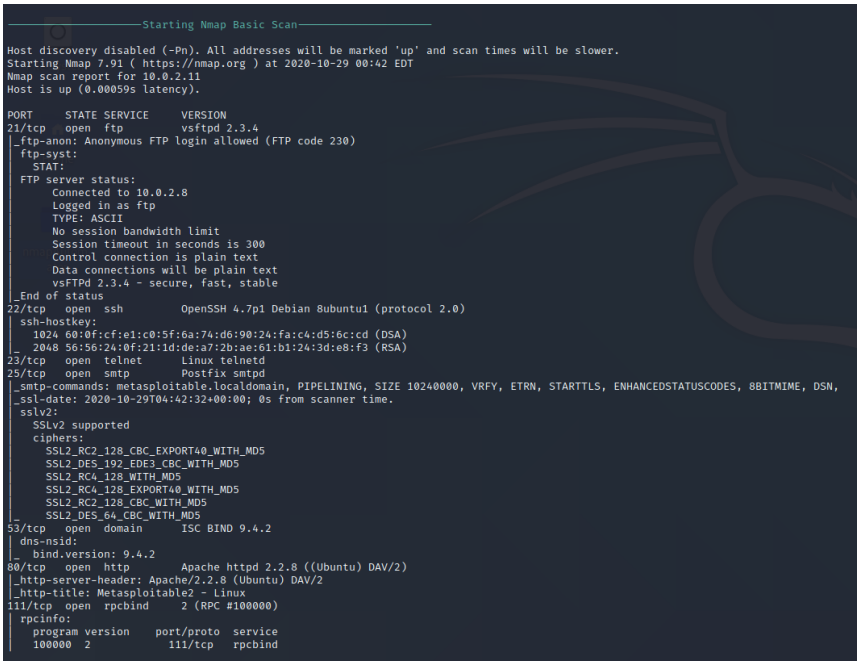
./nmapAutomator.sh 10.0.2.11 Basic

./nmapAutomator.sh 10.0.2.11 Recon

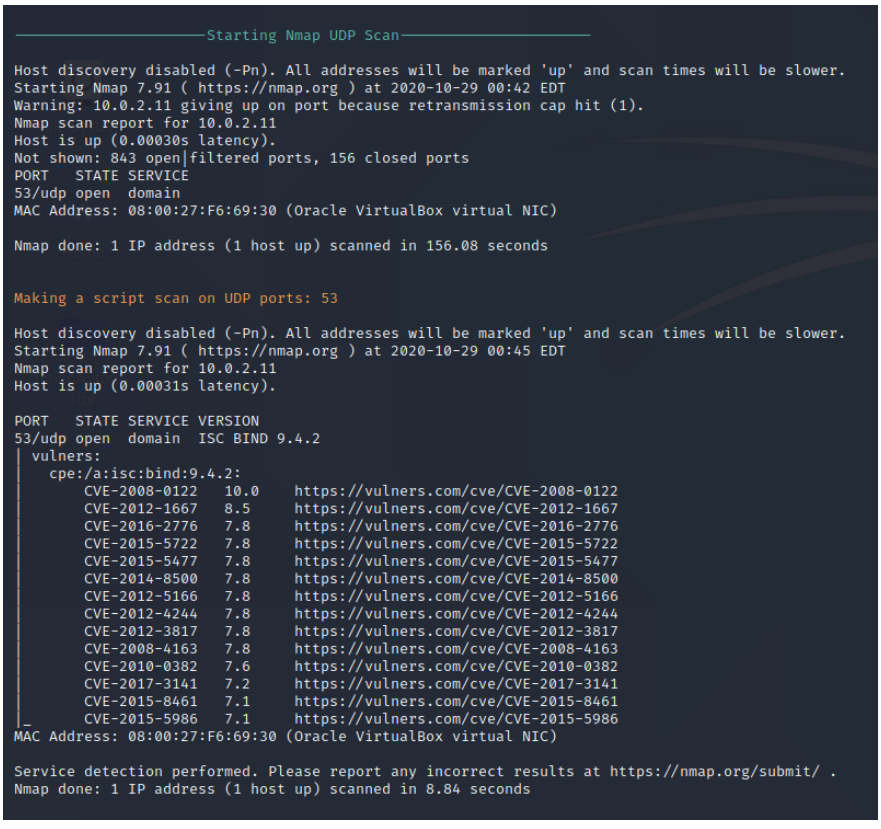
Right away we ae given the **quick scan** results.

```
root@kali:~/Desktop/nmapAutomator# ./nmapAutomator.sh 10.0.2.11 All

Running all scans on 10.0.2.11

Host is likely running Linux


---------------------Starting Nmap Quick Scan---------------------

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-29 00:42 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00085s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:F6:69:30 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

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**.

```
──────────────────Starting Nmap Full Scan──────────────────

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-29 00:45 EDT
Initiating ARP Ping Scan at 00:45
Scanning 10.0.2.11 [1 port]
Completed ARP Ping Scan at 00:45, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:45
Completed Parallel DNS resolution of 1 host. at 00:45, 0.19s elapsed
Initiating SYN Stealth Scan at 00:45
Scanning 10.0.2.11 [65535 ports]
Discovered open port 25/tcp on 10.0.2.11
Discovered open port 139/tcp on 10.0.2.11
Discovered open port 23/tcp on 10.0.2.11
Discovered open port 22/tcp on 10.0.2.11
Discovered open port 5900/tcp on 10.0.2.11
Discovered open port 53/tcp on 10.0.2.11
Discovered open port 445/tcp on 10.0.2.11
Discovered open port 21/tcp on 10.0.2.11
Discovered open port 3306/tcp on 10.0.2.11
Discovered open port 80/tcp on 10.0.2.11
Discovered open port 111/tcp on 10.0.2.11
Discovered open port 6697/tcp on 10.0.2.11
Discovered open port 514/tcp on 10.0.2.11
Discovered open port 513/tcp on 10.0.2.11
Discovered open port 512/tcp on 10.0.2.11
SYN Stealth Scan Timing: About 23.13% done; ETC: 00:47 (0:01:43 remaining)
Discovered open port 3632/tcp on 10.0.2.11
Discovered open port 6000/tcp on 10.0.2.11
SYN Stealth Scan Timing: About 46.02% done; ETC: 00:47 (0:01:12 remaining)
Discovered open port 49746/tcp on 10.0.2.11
Discovered open port 2121/tcp on 10.0.2.11
Discovered open port 2049/tcp on 10.0.2.11
Discovered open port 5432/tcp on 10.0.2.11
Discovered open port 43124/tcp on 10.0.2.11
Discovered open port 49331/tcp on 10.0.2.11
Discovered open port 8009/tcp on 10.0.2.11
Discovered open port 1524/tcp on 10.0.2.11
SYN Stealth Scan Timing: About 68.83% done; ETC: 00:47 (0:00:41 remaining)
```

```
Making a script scan on extra ports: 3632, 6697, 8787, 43124, 49331, 49430, 49746

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-29 00:47 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00036s latency).

PORT      STATE SERVICE  VERSION
3632/tcp  open  distccd  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
6697/tcp  open  irc      UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 5:45:27
|   source ident: nmap
|   source host: 3CC110E8.EB72D3BE.7B559A54.IP
|_  error: Closing Link: jtpftqbcd[10.0.2.8] (Quit: jtpftqbcd)
8787/tcp  open  drb      Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
43124/tcp open  mountd   1-3 (RPC #100005)
49331/tcp open  nlockmgr 1-4 (RPC #100021)
49430/tcp open  status   1 (RPC #100024)
49746/tcp open  java-rmi GNU Classpath grmiregistry
MAC Address: 08:00:27:F6:69:30 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 137.67 seconds
```

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

```
──────────────────Starting Nmap Vulns Scan──────────────────

Running CVE scan on all ports

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-29 00:49 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00056s latency).

PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|_      CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|       CVE-2008-0122   10.0    https://vulners.com/cve/CVE-2008-0122
|       CVE-2012-1667   8.5     https://vulners.com/cve/CVE-2012-1667
|       CVE-2016-2776   7.8     https://vulners.com/cve/CVE-2016-2776
|       CVE-2015-5722   7.8     https://vulners.com/cve/CVE-2015-5722
|       CVE-2015-5477   7.8     https://vulners.com/cve/CVE-2015-5477
|       CVE-2014-8500   7.8     https://vulners.com/cve/CVE-2014-8500
|       CVE-2012-5166   7.8     https://vulners.com/cve/CVE-2012-5166
|       CVE-2012-4244   7.8     https://vulners.com/cve/CVE-2012-4244
|       CVE-2012-3817   7.8     https://vulners.com/cve/CVE-2012-3817
|       CVE-2008-4163   7.8     https://vulners.com/cve/CVE-2008-4163
|       CVE-2010-0382   7.6     https://vulners.com/cve/CVE-2010-0382
|       CVE-2017-3141   7.2     https://vulners.com/cve/CVE-2017-3141
|       CVE-2015-8461   7.1     https://vulners.com/cve/CVE-2015-8461
|_      CVE-2015-5986   7.1     https://vulners.com/cve/CVE-2015-5986
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

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

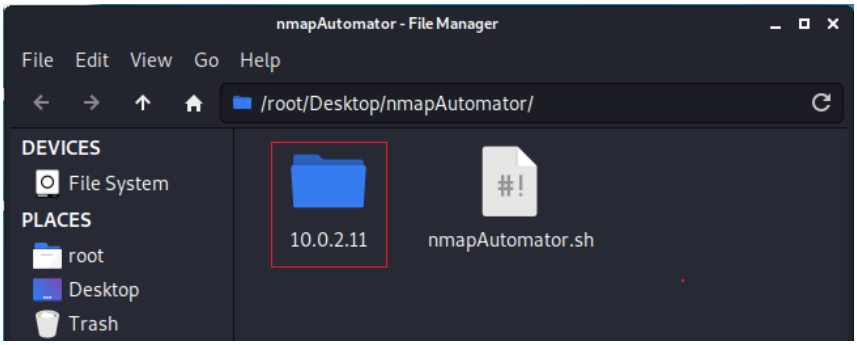
```
Running Vuln scan on all ports

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-29 00:52 EDT
Stats: 0:09:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 01:01 (0:00:00 remaining)
Nmap scan report for 10.0.2.11
Host is up (0.00051s latency).

PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_sslv2-drown:
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-1657
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
|       CVE-2010-4755   4.0     https://vulners.com/cve/CVE-2010-4755
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
|       CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
|_      CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2008-3259
```

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

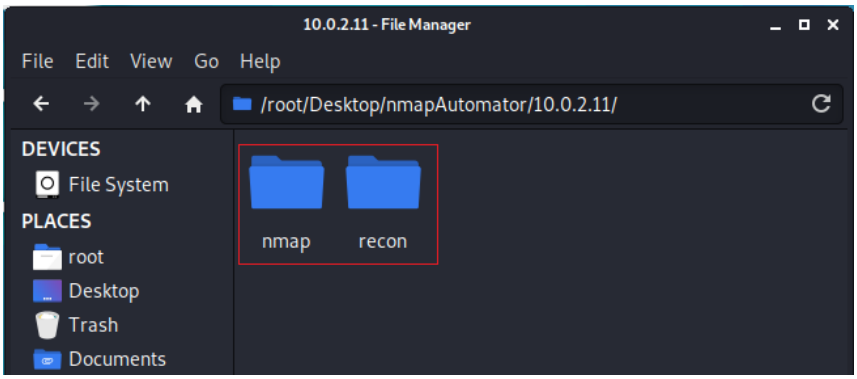
```
──────────────────Recon Recommendations──────────────────

Web Servers Recon:

gobuster dir -w /usr/share/wordlists/dirb/common.txt -l -t 30 -e -k -x .html,.php -u http://10.0.2.11:80 -o recon/gobuster_10.0.2.11_80.txt
nikto -host 10.0.2.11:80 | tee recon/nikto_10.0.2.11_80.txt

gobuster dir -w /usr/share/wordlists/dirb/common.txt -l -t 30 -e -k -x .html,.php -u http://10.0.2.11:8180 -o recon/gobuster_10.0.2.11_8180.txt
nikto -host 10.0.2.11:8180 | tee recon/nikto_10.0.2.11_8180.txt


SMB Recon:

smbmap -H 10.0.2.11 | tee recon/smbmap_10.0.2.11.txt
smbclient -L "//10.0.2.11/" -U "guest"% | tee recon/smbclient_10.0.2.11.txt
enum4linux -a 10.0.2.11 | tee recon/enum4linux_10.0.2.11.txt


DNS Recon:

host -l 10.0.2.11 10.0.2.11 | tee recon/hostname_10.0.2.11.txt
dnsrecon -r 10.0.2.0/24 -n 10.0.2.11 | tee recon/dnsrecon_10.0.2.11.txt
dnsrecon -r 127.0.0.0/24 -n 10.0.2.11 | tee recon/dnsrecon-local_10.0.2.11.txt
dig -x 10.0.2.11 @10.0.2.11 | tee recon/dig_10.0.2.11.txt




Which commands would you like to run?
All (Default), dig, dnsrecon, enum4linux, gobuster, host, nikto, smbclient, smbmap, Skip <!>

Running Default in (1) s:
```

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

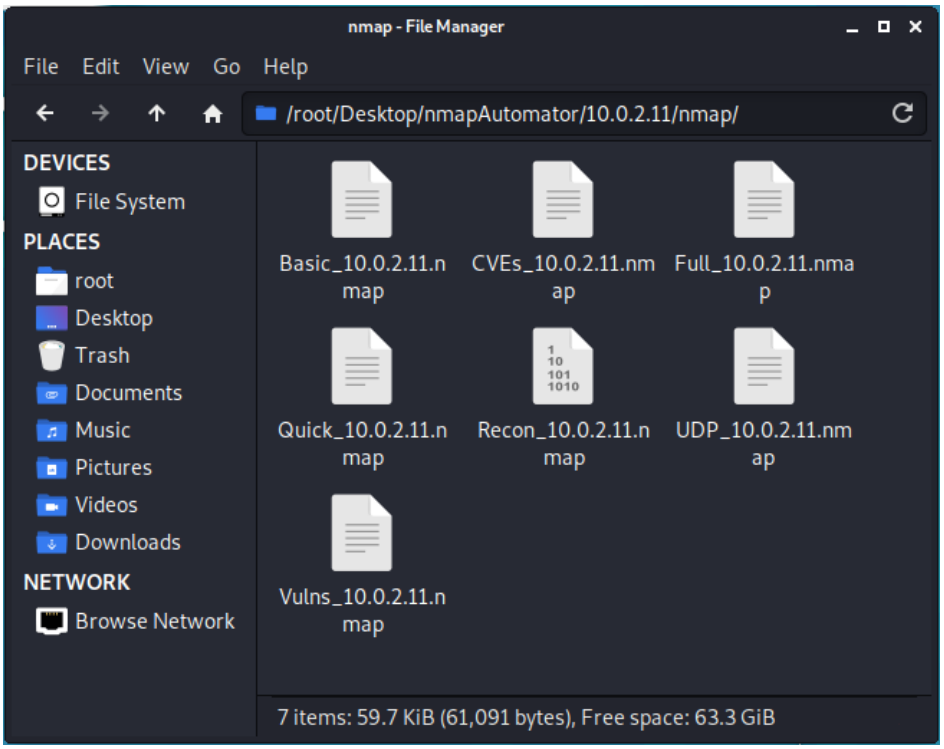
Minimize your terminal showing the scan results. From your terminal, open your nmapAutomator folder. Here you will find text files containing all the different scan results.



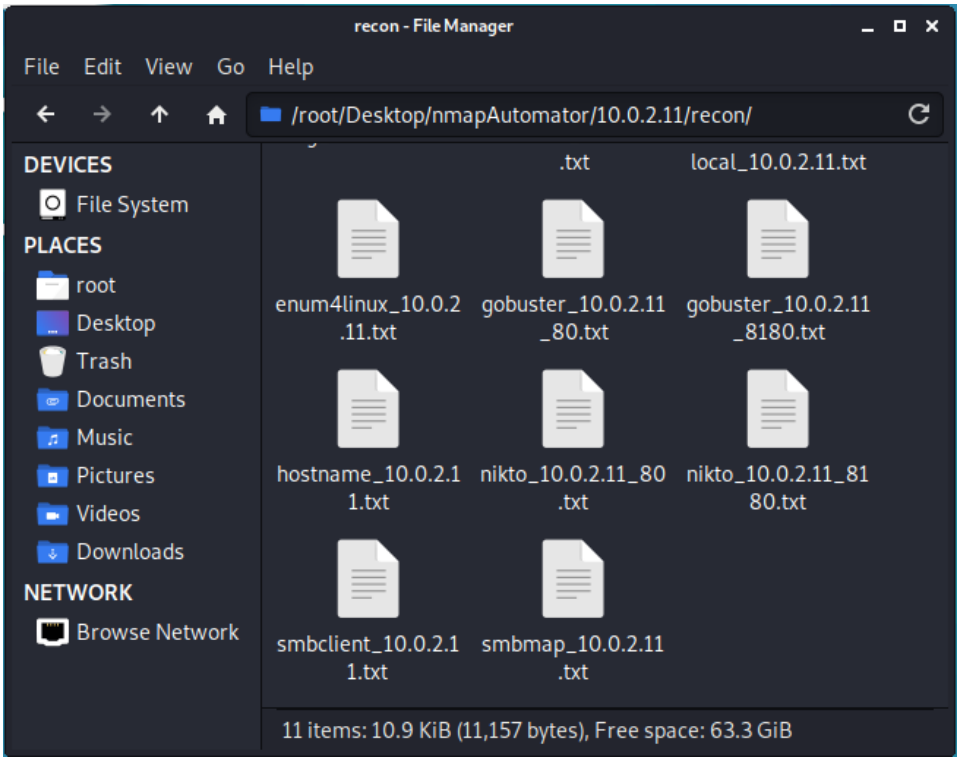

When you open the scan results, you will be presented with two subfolders.




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.