Lab - This is SPARTA!

Overview –

In the lab, students will become familiar with Sparta. Sparta is a network infrastructure scanning and enumeration tool. It performs scans against a target host using Nmap, Nikto, and several other tools managed under a single interface.

Learning Opportunity!

Enumeration is activity in which usernames and info on groups, shares, and services of networked computers are retrieved. Not be confused with network mapping, which only retrieves information about which devices are connected to the network and what operating system runs on them.

Sparta is designed to help pen-testers and hackers during the scanning and enumeration phases of a pentest. When you give it a host to scan, it runs several other tools, such as Nmap, Nikto, and CutyCapt, displaying the results in separate tabs for each tool. Sparta was built to be customizable by the user, meaning other tools can be added to the interface.

Hardware and Software Requirements

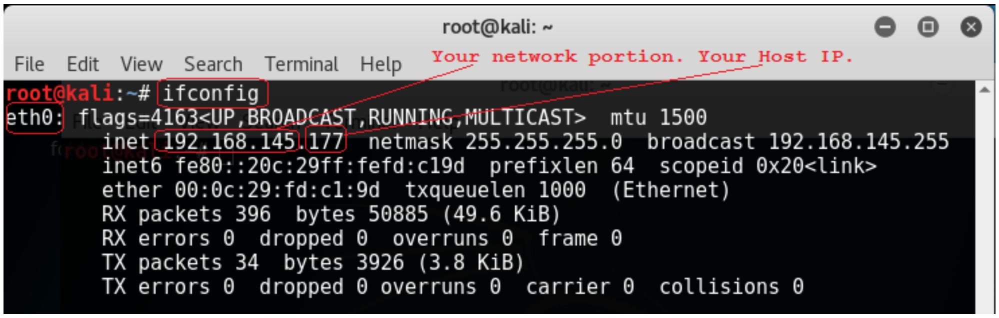
1. An installed hypervisor. This lab is using VMware.
2. One virtual install of Kali
3. One virtual install of Metasploitable2
4. Your network IP

For this lab, you can have Windows XP and Metasploitable2 running. The more victims, the more results.

First Things First

Open a terminal in Kali and type the command to display your TCP/IP setting for your eth0 adapter. Write it down or remember the network portion. You can use either of the following commands:

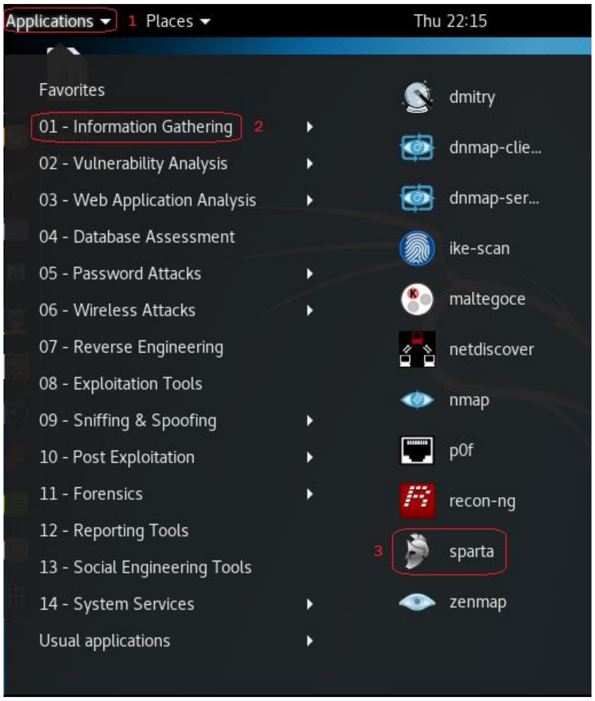
- ifconfig
- ip addr


root@kali: ~
File Edit View Search Terminal Help
Your network portion. Your Host IP.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.145.177  netmask 255.255.255.0  broadcast 192.168.145.255
        inet6 fe80::20c:29ff:fefd:c19d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:fd:c1:9d  txqueuelen 1000  (Ethernet)
        RX packets 396  bytes 50885 (49.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 3926 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

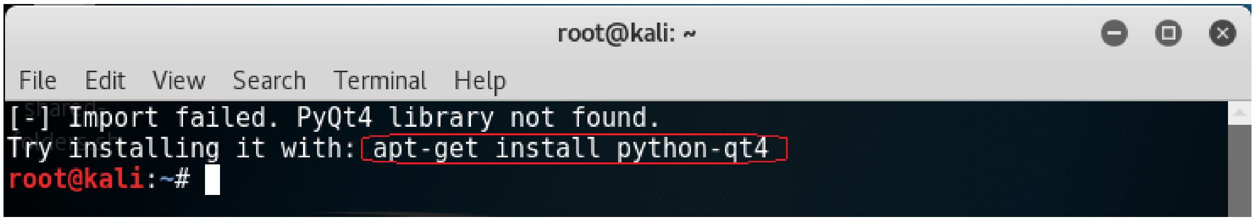
This is my network IP range, not yours! Yours will differ.

In Kali, Sparta is located under “Applications –> Information Gathering.”



When you click on Sparta, the UI will launch, as well as a terminal window that is basically a running log of Sparta’s actions. Leave the terminal running, and if you want to see what is going on, you can observe the terminal window for more information.

If you receive the following error message when launching SPARTA:

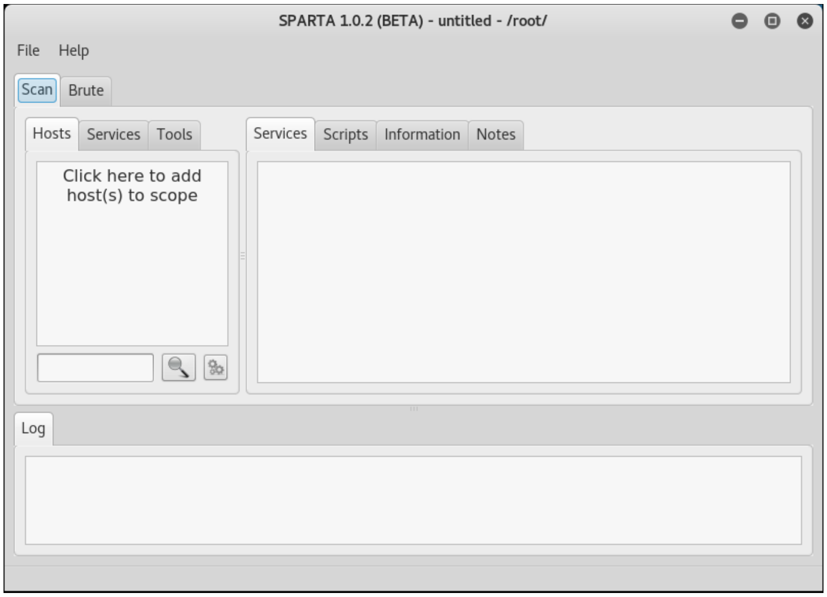


```
[-] Import failed. PyQt4 library not found.
Try installing it with: apt-get install python-qt4
root@kali:~#
```

Copy and paste `apt-get install sparta` at the terminal and update the SPARTA program. Welcome to Linux!

Introduction to SPARTA

This is the user interface for SPARTA. Click on the tabs as you go through the overview.


SPARTA 1.0.2 (BETA) - untitled - /root/
File
Help
Scan
Brute
Hosts
Services
Tools
Services
Scripts
Information
Notes
Click here to add host(s) to scope
Log

File Menu

The options under the File menu:

- New – Start a new project
- Open – Open a saved project
- Save/Save As – Save current project data
- Add Hosts to Scope – Add your target host or IP range
- Import Nmap – Import saved Nmap XML results files

The "Help" function doesn't work but there's plenty of help online, and the program is intuitive enough to figure out.

Scan Tab

The Scan tab has three tabs.

- Hosts – Add host or IP range to scope
- Services – Shows the discovered services for your target(s)
- Tools – Shows output for each of the tools as the scan runs

In addition, there are also sub-tabs on the right which will contain the information discovered during a scan. As different tools run, additional tabs will be added.

Brute Tab

The Brute tab allows you to perform brute force password attacks against the different services you have discovered. Give it the host IP, port to use, the service to attack, and configure the other options.

There are also different configurations you can use for the usernames and passwords. You can manually give it a username and password that you already know, give it a username and password list to use, or let it use any accounts it knows about from running the tools. You can also do a combination, so for example, if you know a username, you can specify it, then let it use a password list to attack that one account. It uses Hydra for this functionality, and you can look at the Sparta config file to see how it's set up.

Starting a New Scan

Before we run a scan, we will make one quick change to the config file for Sparta.

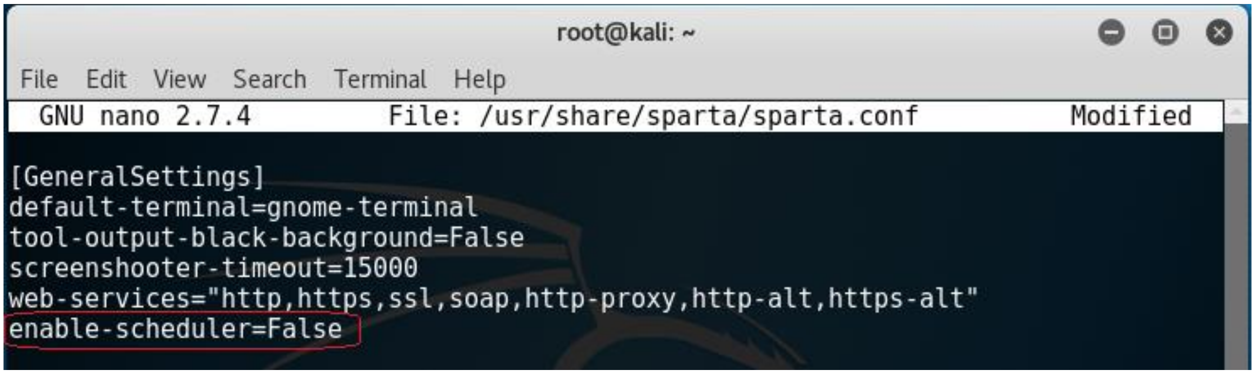
By default, the scans will automatically start running when you add your host. This opens up quite a few tabs we do not need.

To disable automatic scanning, open the sparta.conf file:

1. Close Sparta
2. Open the config file:

(copy and paste to a terminal in Kali. Nano is a text editor. We are telling nano to open the text file so we can edit it)

look under the "General Settings" section, and change the "enable-scheduler" option to "False".

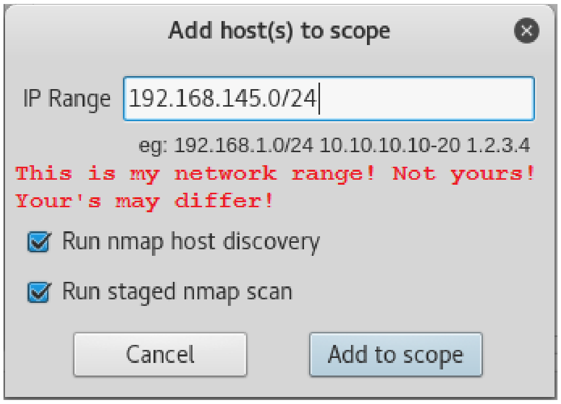


```
 GNU nano 2.7.4        File: /usr/share/sparta/sparta.conf        Modified

[GeneralSettings]
default-terminal=gnome-terminal
tool-output-black-background=False
screenshooter-timeout=15000
web-services="http,https,ssl,soap,http-proxy,http-alt,https-alt"
enable-scheduler=False
```

Save the config file ((ctrl+x to exit, hit ‘Y’ to save using the same file name. Hit enter one more time to close.)

Launch SPARTA.

1. Go to the Hosts tab, and click inside the window to add a new host or IP range. Alternatively, you can click on the File menu, and select “Add hosts to scope.”



Add host(s) to scope

IP Range 192.168.145.0/24

eg: 192.168.1.0/24 10.10.10.10-20 1.2.3.4

This is my network range! Not yours! Your's may differ!

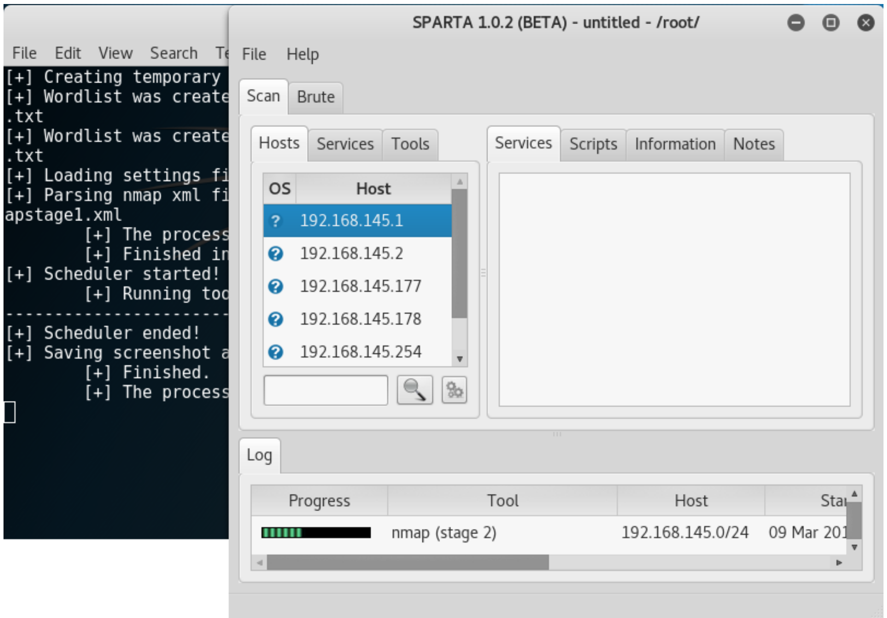
☑ Run nmap host discovery

☑ Run staged nmap scan

2. Type in the network IP range for your virtual network. Specify if you want to use Nmap host discovery, and if you want the nmap scan to be staged (faster results). You can look at the config file to see how each stage of the nmap scans work.

3. Click “Add to Scope.” The scan will start automatically. Monitor progress either in the UI log windows or get more detail in the terminal log window.

Once the scan starts running, you’ll start to see the discovered services in the right window. You can also see the status of each scan in the bottom log window. The Status columns will tell you when everything is finished.



File Edit View Search Te
SPARTA 1.0.2 (BETA) - untitled - /root/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information Notes
Log

```
[+] Creating temporary
[+] Wordlist was create
.txt
[+] Wordlist was create
.txt
[+] Loading settings fi
[+] Parsing nmap xml fi
apstage1.xml
        [+] The process
        [+] Finished in
[+] Scheduler started!
        [+] Running too
------------------------
[+] Scheduler ended!
[+] Saving screenshot a
        [+] Finished.
        [+] The process
```

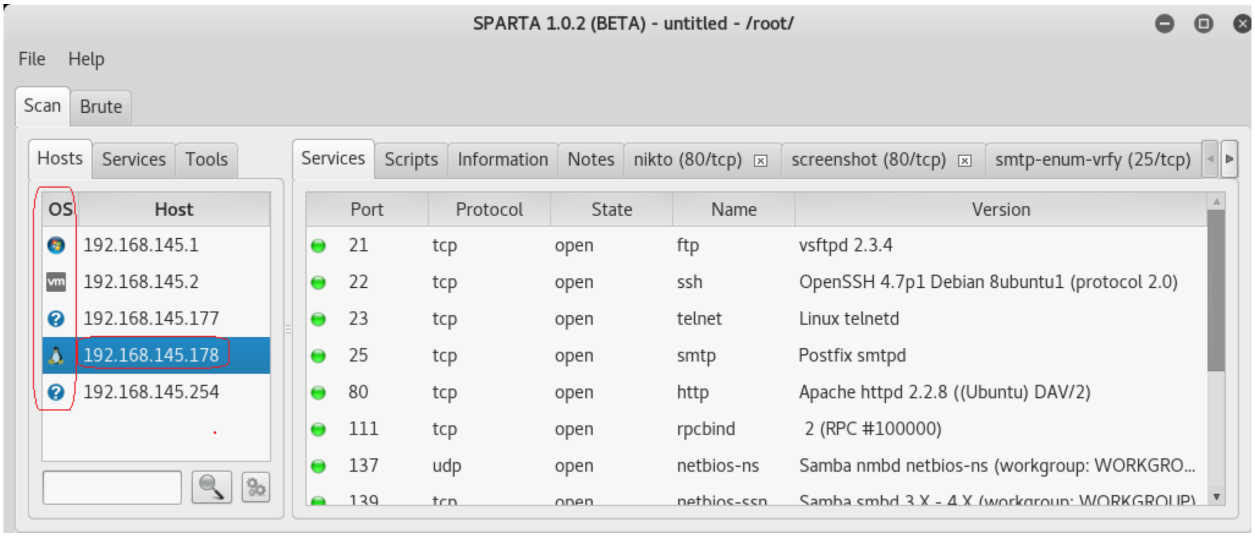
OS	Host
?	192.168.145.1
?	192.168.145.2
?	192.168.145.177
?	192.168.145.178
?	192.168.145.254

Progress	Tool	Host	Sta
▮▮▮▮▮▮	nmap (stage 2)	192.168.145.0/24	09 Mar 201

Wait for the scan to complete!

Moving on….

Notice the icons change to the type of OS. My install of Metasploitable2 is indicated with Linux icon.



SPARTA 1.0.2 (BETA) - untitled - /root/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information Notes nikto (80/tcp) screenshot (80/tcp) smtp-enum-vrfy (25/tcp)

OS	Host
	192.168.145.1
vm	192.168.145.2
?	192.168.145.177
	192.168.145.178
?	192.168.145.254

	Port	Protocol	State	Name	Version
●	21	tcp	open	ftp	vsftpd 2.3.4
●	22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
●	23	tcp	open	telnet	Linux telnetd
●	25	tcp	open	smtp	Postfix smtpd
●	80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
●	111	tcp	open	rpcbind	2 (RPC #100000)
●	137	udp	open	netbios-ns	Samba nmbd netbios-ns (workgroup: WORKGRO...
●	139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Metasploitable is made vulnerable to practicing pentesting or hacking. Everything listed in the results panel probably has some type of exploit. We're enumerating at this stage; we want to find as many vulnerabilities as possible, we need data and lots of it.

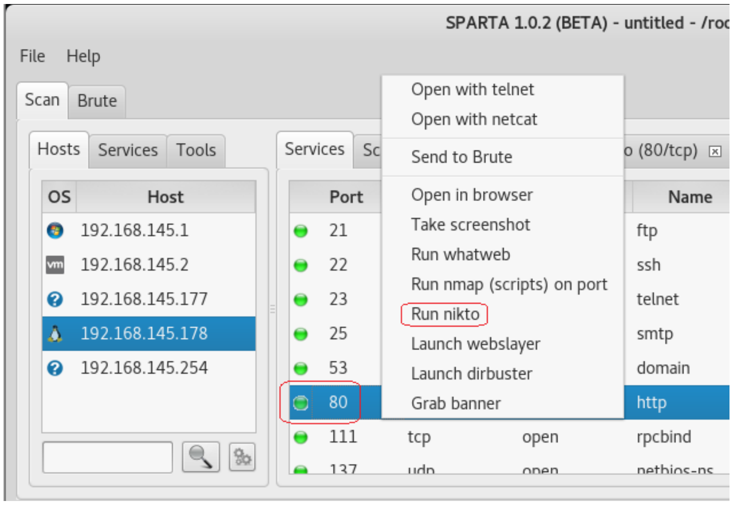
More Discovery

Once the initial Nmap scans have finished and we look at the Services tab on the right, we can see the open ports discovered along with the service names and banners assigned to each port. We can start adding the additional tools to discover more information. By right clicking on any services, a new context menu will appear. This is where we select more scanning options based solely on the service you have selected.

Scan with Nikto

Since TCP port 80 is open, right click on the port and select Nikto from the context menu.

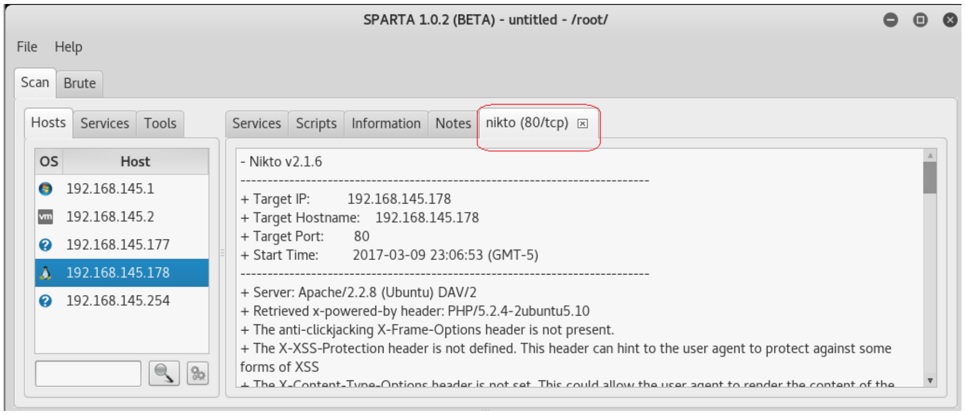
1. Right-click the port 80.
2. Select "Run nikto"



OS	Host
	192.168.145.1
vm	192.168.145.2
	192.168.145.177
	192.168.145.178
	192.168.145.254

Port			Name
21			ftp
22			ssh
23			telnet
25			smtp
53			domain
80			http
111	tcp	open	rpcbind
137	udp	open	netbios-ns

3. Click the "Nikto" tab to see the discovered information



OS	Host
	192.168.145.1
vm	192.168.145.2
	192.168.145.177
	192.168.145.178
	192.168.145.254

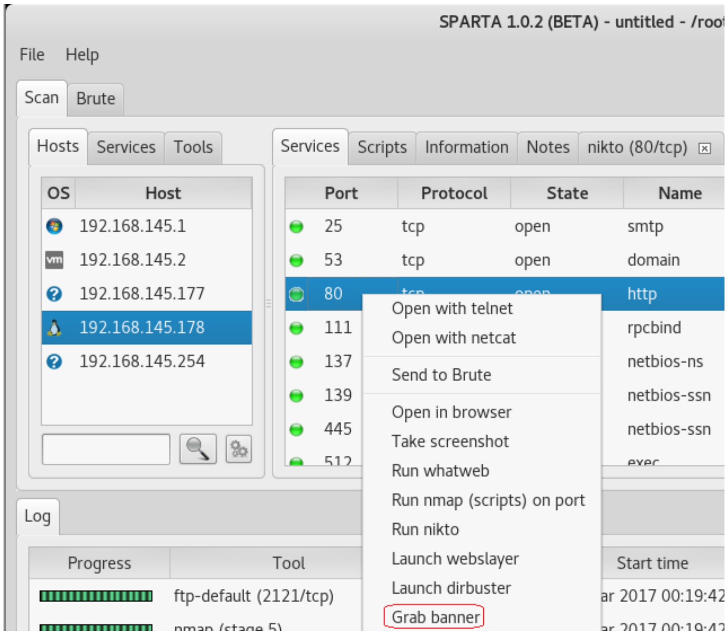
```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.145.178
+ Target Hostname:    192.168.145.178
+ Target Port:        80
+ Start Time:         2017-03-09 23:06:53 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some
forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
```

Additional Options – Port 80

In addition to being able to run Nikto, there are other tools you can run from the context menu.

Grab Banner

1. Right-click port 80, and select "Grab Banner." Don't be too upset is does not find anything. Not everything is going to work as advertises. New updates, new versions, things break.



OS	Host
	192.168.145.1
vm	192.168.145.2
	192.168.145.177
	192.168.145.178
	192.168.145.254

	Port	Protocol	State	Name
●	25	tcp	open	smtp
●	53	tcp	open	domain
●	80	tcp	open	http
●	111			rpcbind
●	137			netbios-ns
●	139			netbios-ssn
●	445			netbios-ssn
●	512			exec

Progress	Tool	Start time
	ftp-default (2121/tcp)	ar 2017 00:19:42
	nmap (stage 5)	ar 2017 00:19:42

Other Options

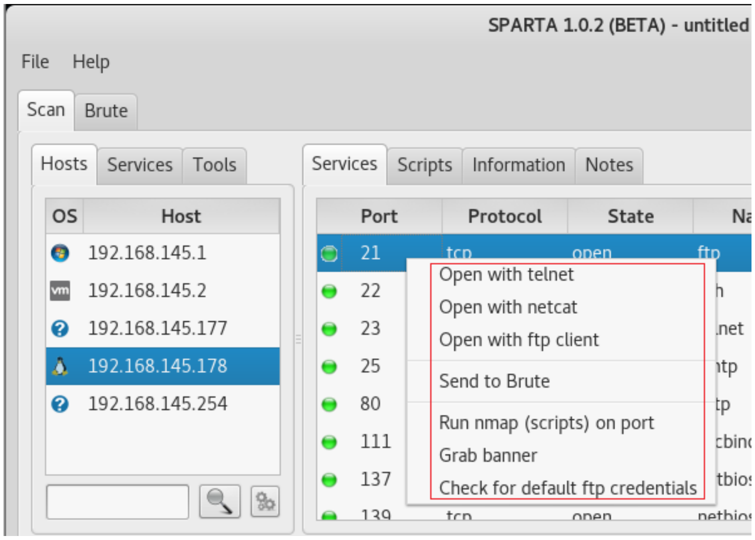
There are other options you can select, such as DirBuster, opening with telnet, and others.

Caveat!

There is an option on the context menu to launch webslayer. This software isn't installed in Kali 2.0, so you won't be able to run it with Sparta. If you try to run webslayer from within Sparta, that process will crash.

Other Services and Options

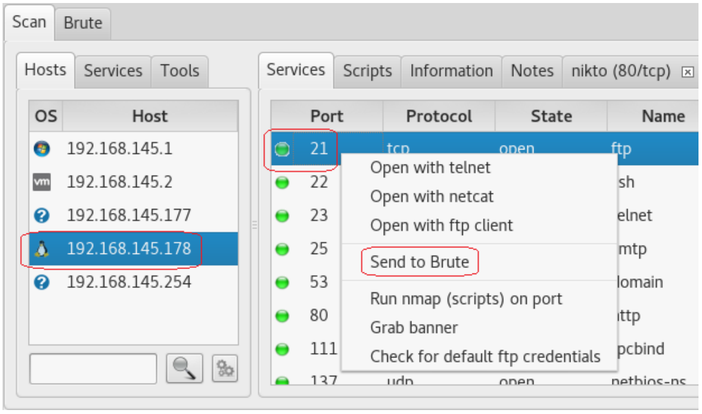
Let's go back to the Services tab, and select one of the other services. You can right-click each one to see the tools that are available to use with that service. The options will be different depending on the port/service you select. For example, if we select the FTP service on port 21, we see a different set of option under the context menu then we did for port 80.



OS	Host
	192.168.145.1
vm	192.168.145.2
?	192.168.145.177
	192.168.145.178
?	192.168.145.254

There are a couple of different options available. We can connect to using an FTP client, or send it to the brute force tab and look for any account information. Select the brute force option, to see how this works.

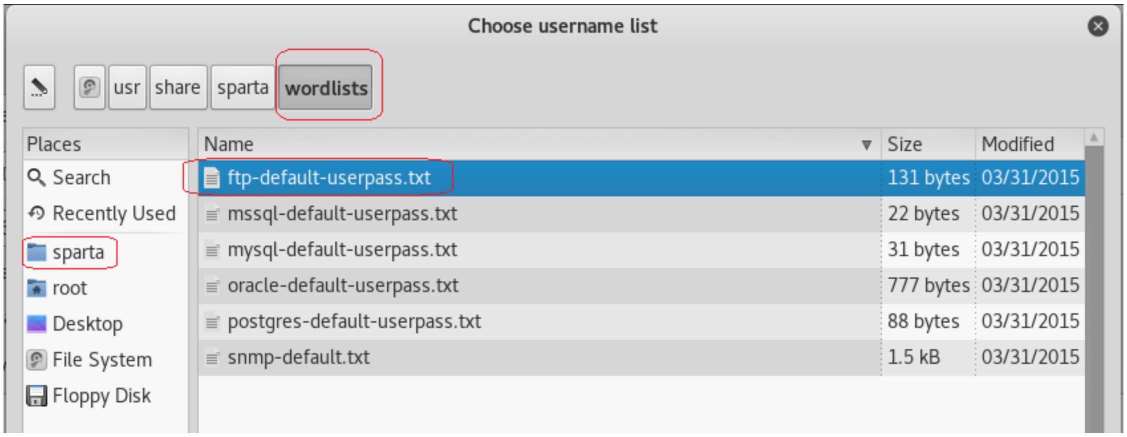
1. Right-click the FTP service, and select “Send to Brute”



OS	Host
	192.168.145.1
vm	192.168.145.2
?	192.168.145.177
	192.168.145.178
?	192.168.145.254

2. Click on the Brute tab

3. Configure options for brute force attack. Here we’re going to specify user/password lists. From places, select Sparta. From name windows select Wordlist, from the text files select a wordlist. I used the username ‘anonymous’ for the username and the password wordlist.

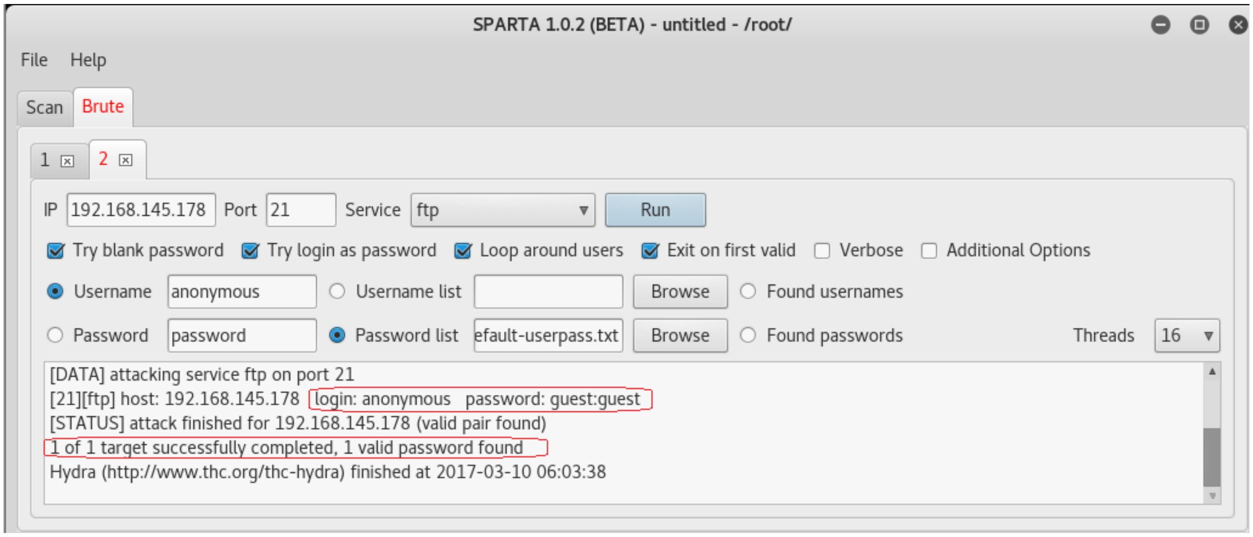


Choose username list

Places: Search, Recently Used, sparta, root, Desktop, File System, Floppy Disk

Name	Size	Modified
ftp-default-userpass.txt	131 bytes	03/31/2015
mssql-default-userpass.txt	22 bytes	03/31/2015
mysql-default-userpass.txt	31 bytes	03/31/2015
oracle-default-userpass.txt	777 bytes	03/31/2015
postgres-default-userpass.txt	88 bytes	03/31/2015
snmp-default.txt	1.5 kB	03/31/2015

4. When everything is set, click on "Run" to begin the attack



SPARTA 1.0.2 (BETA) - untitled - /root/

IP 192.168.145.178 Port 21 Service ftp

☑ Try blank password ☑ Try login as password ☑ Loop around users ☑ Exit on first valid □ Verbose □ Additional Options

● Username anonymous ○ Username list ○ Found usernames

○ Password password ● Password list efault-userpass.txt ○ Found passwords Threads 16

```
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.145.178   login: anonymous   password: guest:guest
[STATUS] attack finished for 192.168.145.178 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-03-10 06:03:38
```

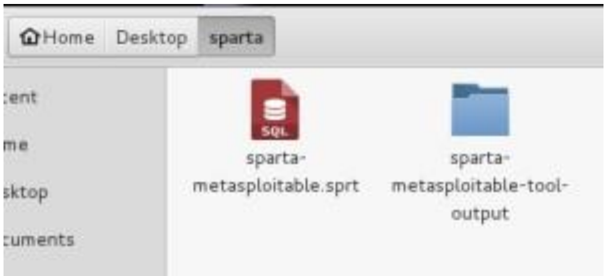
If you go back to the "Scan" tab, then click on the "Tools" sub-tab, then "hydra," you can see the results there as well. If you don't see any results, try anonymous for both the username and the password.

Saving Results

At some point, you'll want to save your results, either because you're finished with Sparta, or you may need to perform another task outside of Sparta, and come back to your session later.

When you save your results, everything will be saved as a Sparta project file. It creates a main .sprt file, then a separate folder that contains the results from each of the tools you've used.

I've created a folder on the Desktop and saved my results there.



Inside this folder, there are several sub-directories for each tool you ran and results files for each. Most are saved in either TXT or XML formats, so you could import those into other tools if needed.

If you need to open the project again, go to the File menu, select Open, and point it to the .sprt file that Sparta created.

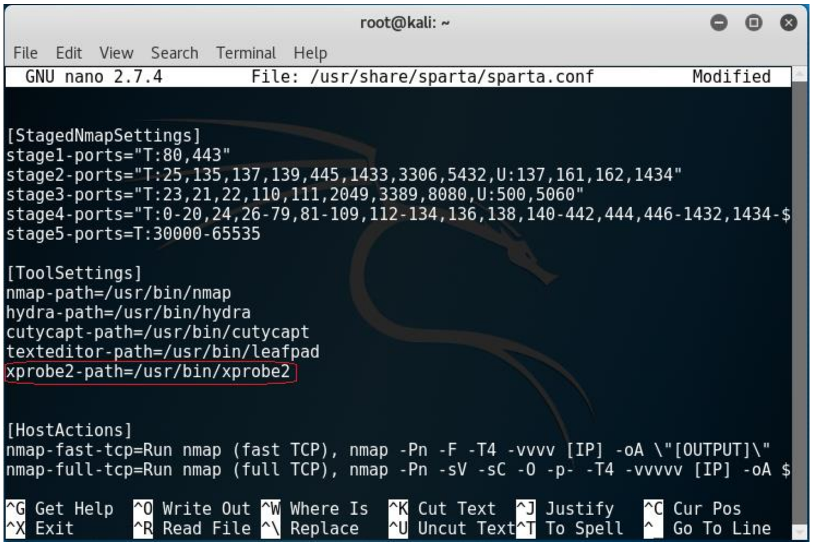
Adding a New Tool to SPARTA

We can modify the SPARTA config file to add tools to the application. The caveat you must remember is if the tool you add is a command line tool, it can't be interactive. You must be able to set the options and let the tool run to completion on its own.

Example:

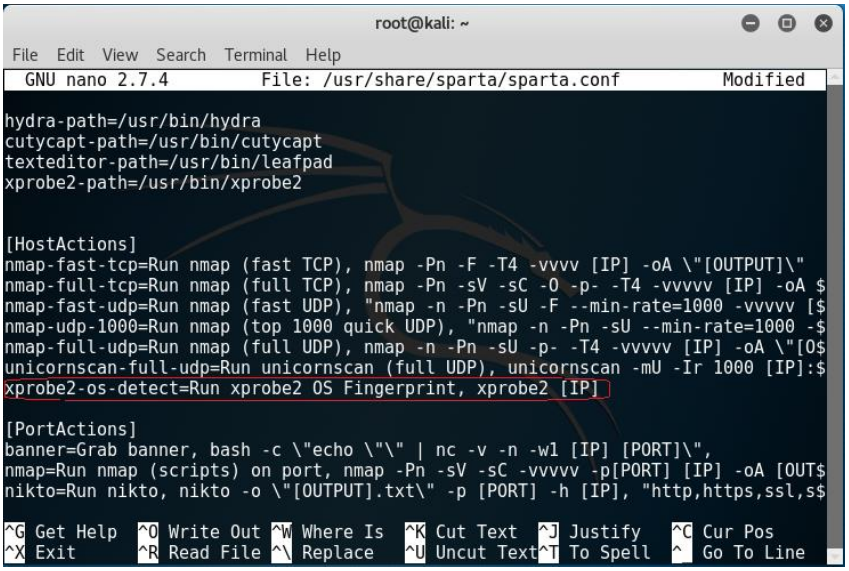
We can add "xprobe2", and set it, so it appears as an option when we right click on a host. Xprobe2 is an OS fingerprinting tool, used to identify the operating system during an assessment.

1. Close Sparta
2. Open the config file: `nano /usr/share/sparta/sparta.conf` (copy and paste to a terminal in Kali. Nano is a text editor. We are telling nano to open the text file for us so we can edit it)
3. Use the down arrow to go to the "Tool Settings" section, and add the path to xprobe2. (You can look at the path for the current tools and see they are all located in the bin folder as is Xprope2. Move your cursor to the end of the last line and hit enter and start typing)



```
  GNU nano 2.7.4          File: /usr/share/sparta/sparta.conf          Modified


[StagedNmapSettings]
stage1-ports="T:80,443"
stage2-ports="T:25,135,137,139,445,1433,3306,5432,U:137,161,162,1434"
stage3-ports="T:23,21,22,110,111,2049,3389,8080,U:500,5060"
stage4-ports="T:0-20,24,26-79,81-109,112-134,136,138,140-442,444,446-1432,1434-$
stage5-ports=T:30000-65535

[ToolSettings]
nmap-path=/usr/bin/nmap
hydra-path=/usr/bin/hydra
cutycapt-path=/usr/bin/cutycapt
texteditor-path=/usr/bin/leafpad
xprobe2-path=/usr/bin/xprobe2


[HostActions]
nmap-fast-tcp=Run nmap (fast TCP), nmap -Pn -F -T4 -vvvv [IP] -oA \"[OUTPUT]\"
nmap-full-tcp=Run nmap (full TCP), nmap -Pn -sV -sC -O -p- -T4 -vvvvv [IP] -oA $

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

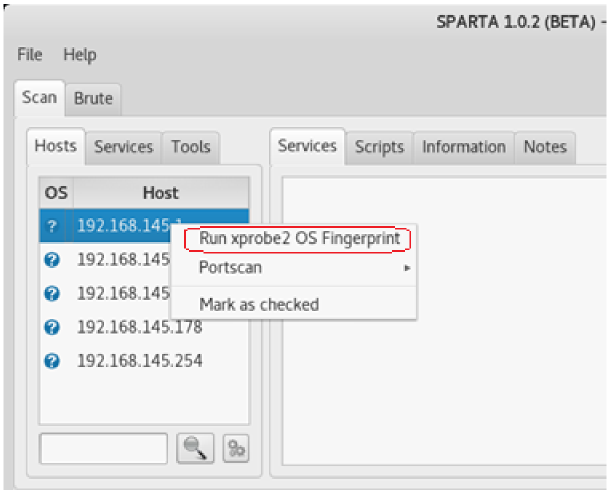
4. Go to “Host Actions,” and add the information to run the tool:



```
  GNU nano 2.7.4          File: /usr/share/sparta/sparta.conf          Modified

hydra-path=/usr/bin/hydra
cutycapt-path=/usr/bin/cutycapt
texteditor-path=/usr/bin/leafpad
xprobe2-path=/usr/bin/xprobe2

[HostActions]
nmap-fast-tcp=Run nmap (fast TCP), nmap -Pn -F -T4 -vvvv [IP] -oA \"[OUTPUT]\"
nmap-full-tcp=Run nmap (full TCP), nmap -Pn -sV -sC -O -p- -T4 -vvvvv [IP] -oA $
nmap-fast-udp=Run nmap (fast UDP), "nmap -n -Pn -sU -F --min-rate=1000 -vvvvv [$
nmap-udp-1000=Run nmap (top 1000 quick UDP), "nmap -n -Pn -sU --min-rate=1000 -$
nmap-full-udp=Run nmap (full UDP), nmap -n -Pn -sU -p- -T4 -vvvvv [IP] -oA \"[O$
unicornscan-full-udp=Run unicornscan (full UDP), unicornscan -mU -Ir 1000 [IP]:$
xprobe2-os-detect=Run xprobe2 OS Fingerprint, xprobe2 [IP]

[PortActions]
banner=Grab banner, bash -c \"echo \"\" | nc -v -n -w1 [IP] [PORT]\",
nmap=Run nmap (scripts) on port, nmap -Pn -sV -sC -vvvvv -p[PORT] [IP] -oA [OUT$
nikto=Run nikto, nikto -o \"[OUTPUT].txt\" -p [PORT] -h [IP], "http,https,ssl,s$

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Be sure to not delete any of the other lines in the config file. Doing so could cause the other tools not to work properly. Remember to restart Sparta any time you make a change to this file.

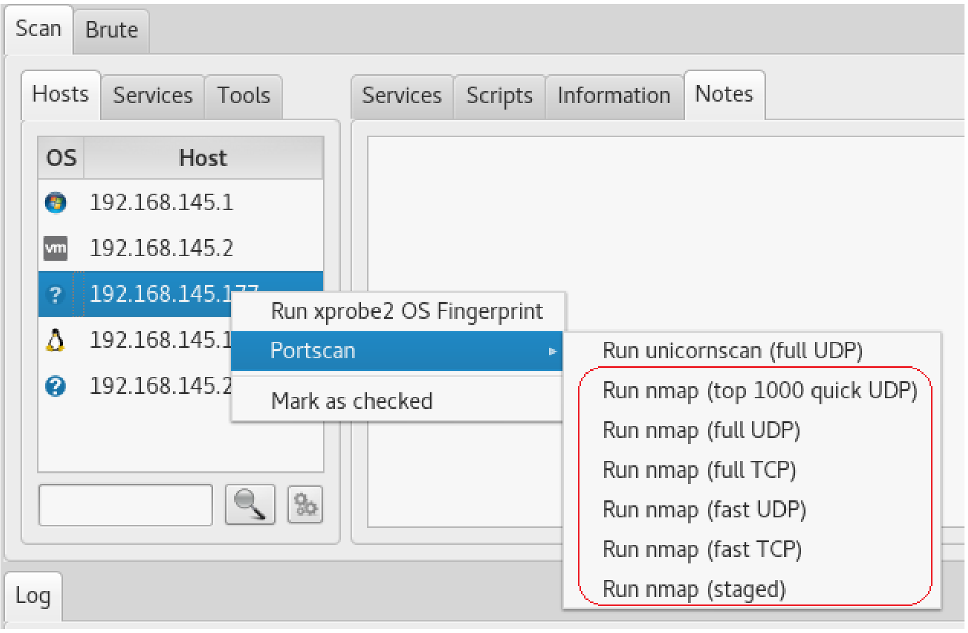
5. Save the config file ((ctrl+x to exit, hit ‘Y’ to save using the same file name. Hit enter one more time to close.)
6. Launch Sparta again
7. Open your saved results from your previous scan, and select any host under the host tab. Right-click to see the new xprobe2 tool showing in the context menu.



Summary

SPARTA is a great tool for the pentesting arsenal. Not every tool works the same for every situation, so we need options. Here we have the most sought-after Nmap scrips automated to run for us. We have Nmap, and other tools are our disposal. All NMap information in the terminal is now given to us using a GUI. Right-click on the different ports and services to see what tools each context menu offers.

We also used Hydra to crack the FTP username and password.



End of the lab!