Exploring The SimSpace Cyber Range

Maximiliano Villarreal

Simspace is an online tool that allows professionals to train in cybersecurity. Simspace provides a simulation of many different and controlled virtual environments, allowing the user to practice without fear of real data loss or theft. This is achieved by using virtual machines equipped with the same operating systems and tools that are used in the field by experts; by virtualizing and using controlled created situations, the user has total control over their digital infrastructure. It has taken over a decade of investments by the U.S. Military to provide these virtual environments for the Department of Defense testing and training communities.

The portion of Simspace used today is the range. The range allows users to practice their cybersecurity skills in virtual machines with a variety of different operating systems. The range allows the user to utilize more than one operating system on their host computer. The range also allows users to upload files into the cyber range for personal practice. Virtual machines are safer to use while engaging in this practice because when you create a virtual machine on your computer it creates a virtual disc. This virtual disc operates separately from your host disc.

All logging on to Simspace is done through their portal at, https://portal.simspace.com. Once you find access to the range through the Events selection on their website, you can select the desired operating system. I used hunt01 for my lab. You are initially met with a windows server 2008, “Press Ctrl, Alt, + Del”. The login credentials for the virtual machine are located in the simspace portal where you launch the virtual machine. To press control alt delete, you select the commands button on the black ribbon above the VM, and click Control-Alt-Delete on the drop down menu. Upon login you are met with a warning message that you are entering a workspace and misuse is prohibited. After dismissing the warning message, we open a powershell window. By using the nmap command you begin, “network sniffing,” or packet analysis. Nmap command alone will show you the switches the device is connected to. There is a lot of information displayed. Using the nmap command followed by -v 172.16.4.0/24 you scan for open ports at 172.16.4.*. Lines upon lines of information are shown in speed. You can “pipe” this information to a text file by using the command, nmap -v 172.16.4.0/24 > filenamescan1.txt. The ls command can be used to ensure your text file was created by displaying all files and directories in the current disc or folder. Files that are created like the filenamescan1.txt will not be available after you have exited the virtual machine. If you have files that are created that are of importance, they need to be moved to a cloud service or the host machine. Created files no longer exist after each virtual machine session.

After locating your filenamescan1.txt file in the information displayed by the ls command, you can display the file using the cat filenamescan1.txt command. The creation and verification of my nmap command text file, MVillarrealscan1.txt can be shown in Appendix 1, it shows the host as down as 0 addresses scanned with 255 hosts found.

Next we execute the nmap command again, but with another slight differentiation. The nmap -v -sU 200.200.200.10 > MVillarrealmachine10scan.txt. Command performs the nmap and the -sU does port scans. The information is ported to the MVillarrealmachine10scan.txt file, as it was in the previous example. The difference between the -sU command and the -sn command in the nmap usage is that the -sU does port scans and the -sn command enables host discovery.

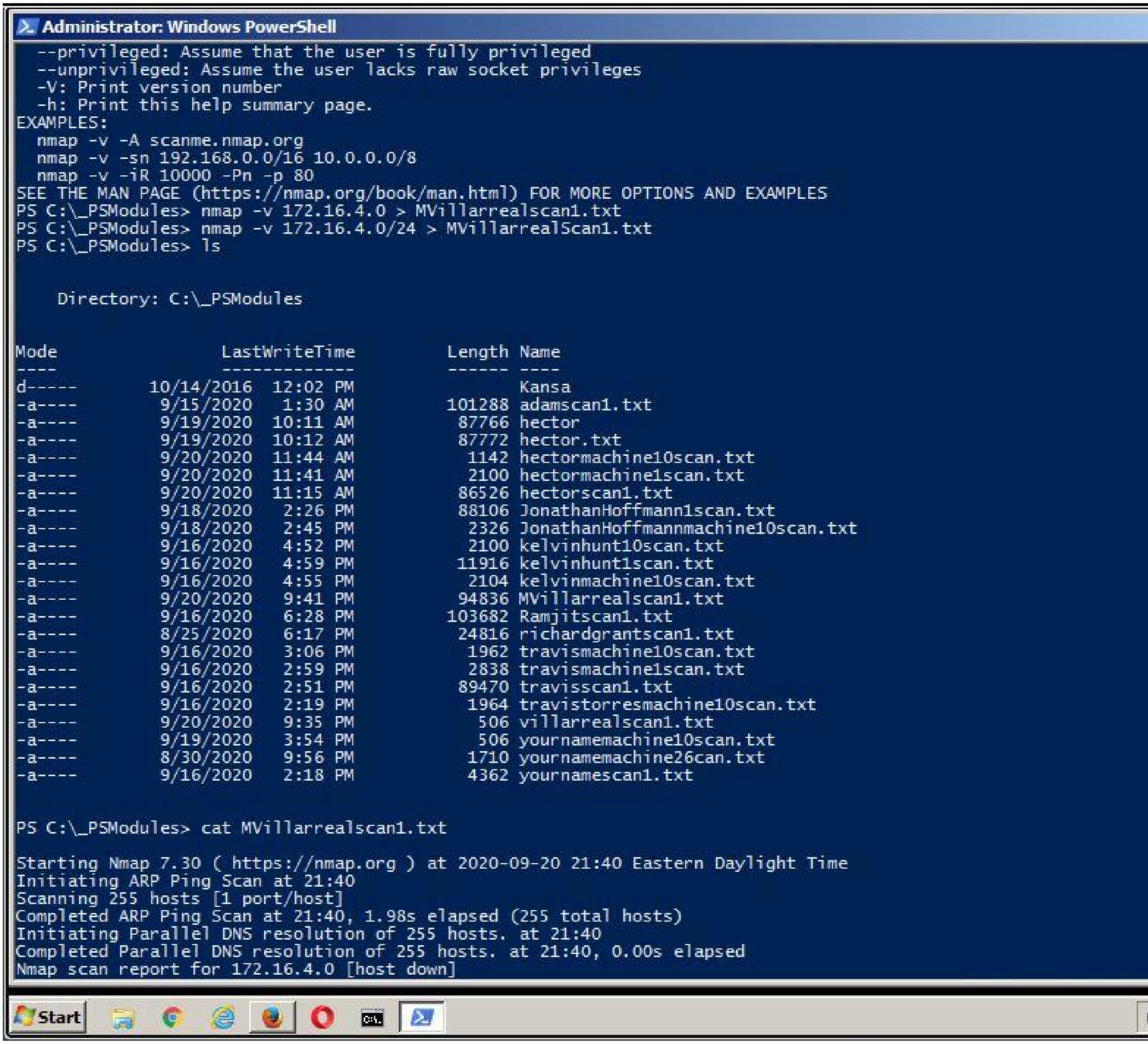
In Appendix 2 you will see me use the Remove command to delete the MVillarrealscan1.txt file. It is also followed by the ls command to verify the file's deletion. Appendix 3 is a continuation of me using the Remove command to rid the virtual machine of duplicate files that were created by me exploring the functions on the virtual machine. The filenames for the deleted files are MVillarrealmachine10scan.txt and Villarrealscan1.txt.

The first software tool I opened in the Kali hunt linux virtual machine is Wireshark. I have used this software in another Information Security class and found it to be very useful, as well as easy to operate. Wireshark is the most commonly used network protocol analyzer in the world. It is useful because it allows you to capture packets live or do analysis offline. Wireshark's GUI features a standard three-pane packet browser (shown in appendix 5), making it very easy to navigate. Wireshark can run on many platforms and more importantly can read and write in many different capture file formats. Live data can be read and captured from ethernet, IEEE 802.11, bluetooth, USB, and others depending on your platform. Wireshark also allows your work to be exported to plain text or other file formats for compatibility and ease of access. It is important to have a tool that can analyze a network like wireshark. This software is used by professionals to troubleshoot networks and inspect for things like packet loss and intentional data theft. Compared to some cybersecurity tools wireshark has a more developed front end and graphical interface, this allows the user to inspect data using the GUI or by command-line version TShark. Wireshark has many features that make it easier to use, for example wireshark can color code packets by sorting and matching by rules. This can help the user analyze large packets of data at a glance.

The second software I explored on the Kali hunt virtual machine is Mimikatz password tool. This tool is used by penetration testers and other cybersecurity professionals. Mimikatz came together after the notPetya attacks and was very successful due to it being a combination of NSA exploits like eternalblue and a research project done to gain a better grasp of windows security. Mimikatz was far more threatening before Windows 10. Windows used to use a single sign-on (SSO), mimikatz would exploit this and use WDigest to take the encrypted passwords, but also load the secret key to decrypt them. Prevention of a mimikatz exploit is fairly simple if you have already upgraded to Windows 10. A user would need administrator privileges to run WDigest so by limiting control you are effectively preventing a mimikatz attack. The mimikatz open window is shown in appendix 6.

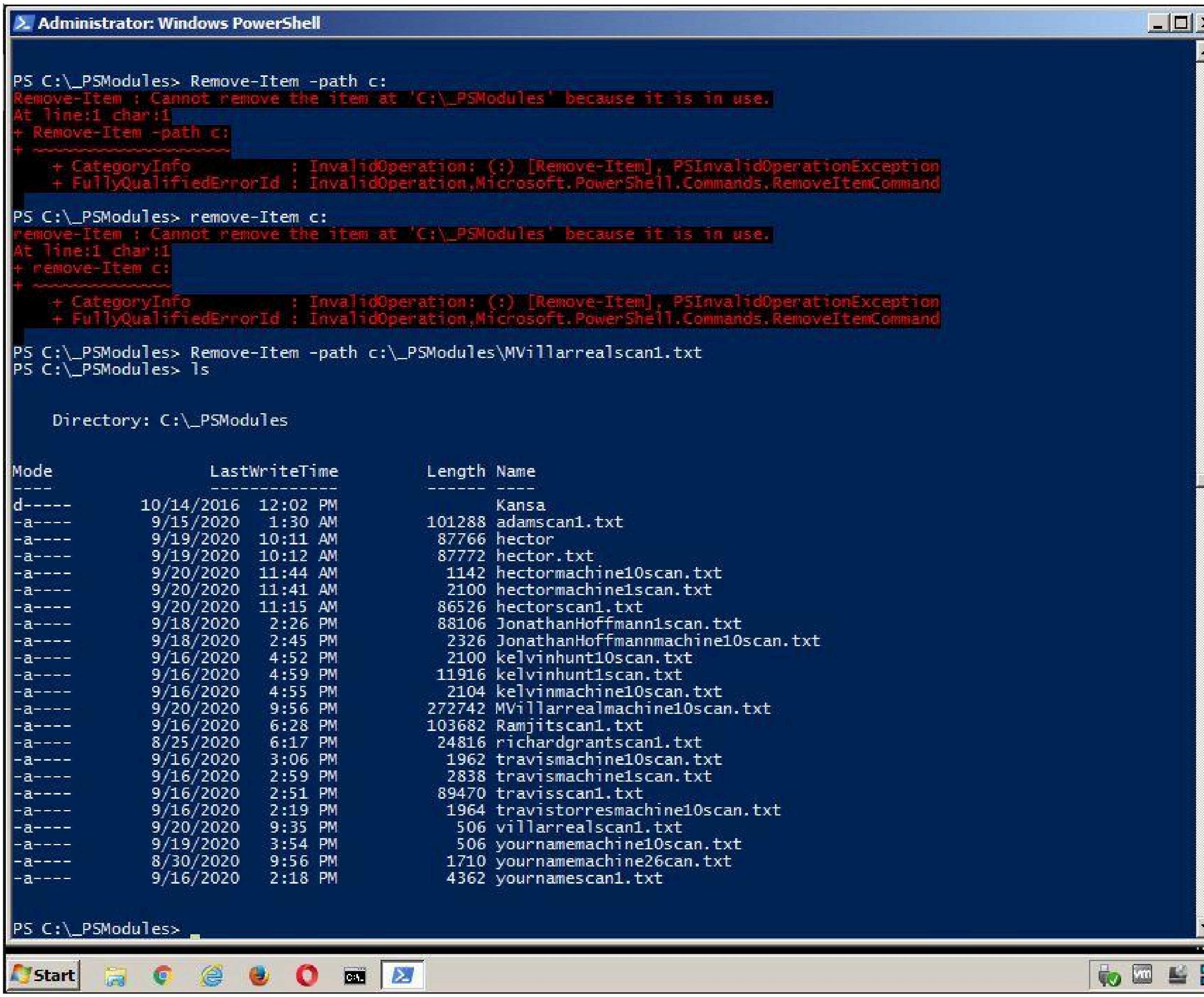
The final tool I opened in the kali hunt linux virtual machine was Sparta. Sparta is a python GUI application which can aid penetration testers by having point-and-click access to their toolkit and making the display. The ideology behind sparta is if less time is spent setting up commands and tools, there is more time to be spent analyzing results. When open and in use sparta displays the host IP and OS type in the ribbon on the left side, under the hosts tab. The user has access to their tools in services in the tabs next to the hosts tab on the left ribbon. The tabs default open on the main window are Services, Scripts, Information, and Notes. The user can navigate Sparta fairly easily and this is by far a more user friendly interface than if you were using a more barebones program. Sparta can be used to run nmap or import nmap XML data. Sparta allows the user to run any script or tool on any host with just the click of a mouse. Sparta is also capable of detecting password reuse on the tested infrastructure. If any usernames/passwords are found, they are stored in internal wordlists that can be used on targets within the network. Sparta also lets you mark hosts that you have worked on for easy identification.

Appendix 1/ Screenshot of powershell after creation of text file



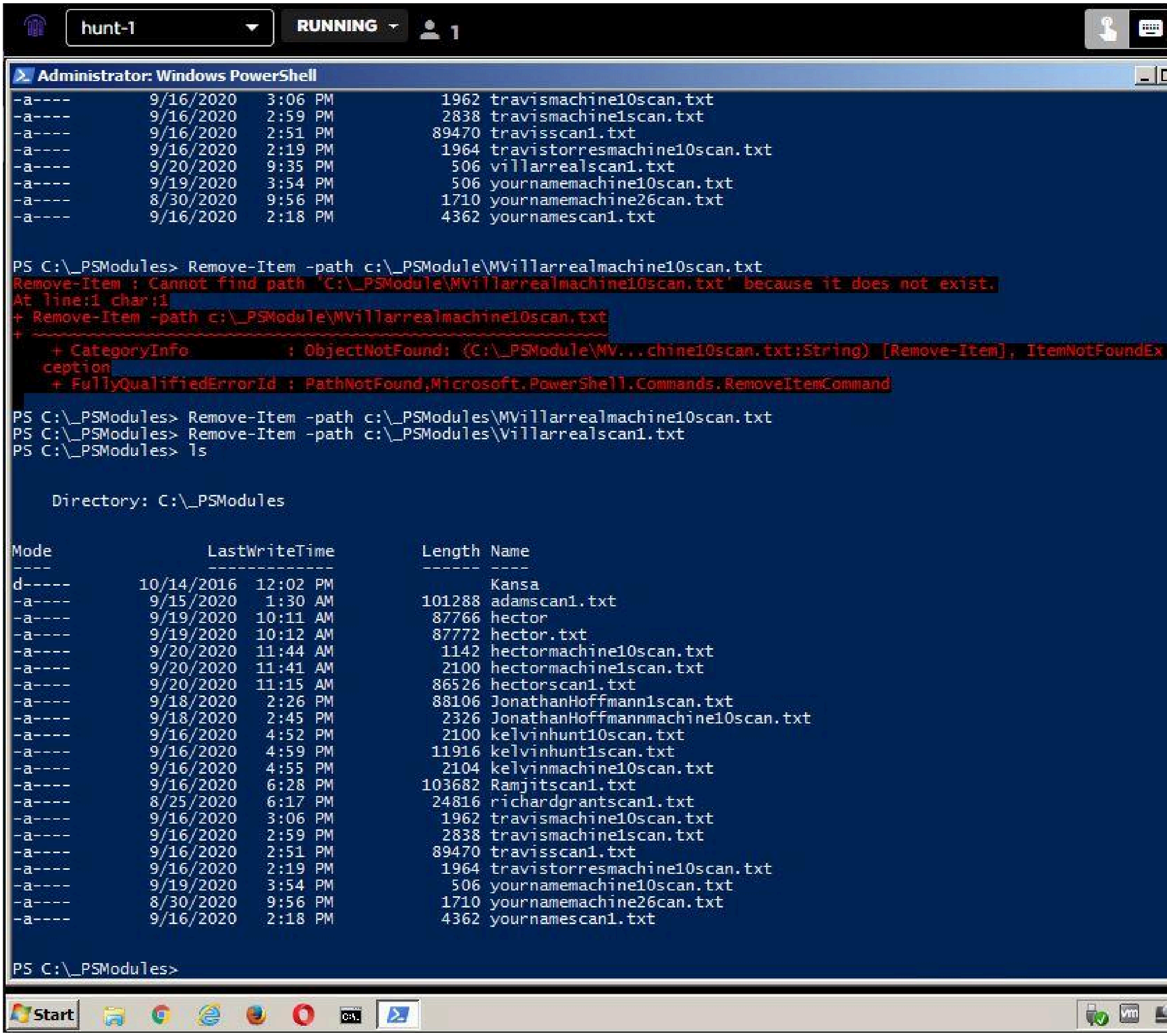
```
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
PS C:\_PSModules> nmap -v 172.16.4.0 > MVillarrealscan1.txt
PS C:\_PSModules> nmap -v 172.16.4.0/24 > MVillarrealScan1.txt
PS C:\_PSModules> ls


    Directory: C:\_PSModules


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/14/2016  12:02 PM                Kansa
-a----        9/15/2020   1:30 AM         101288 adamscan1.txt
-a----        9/19/2020  10:11 AM          87766 hector
-a----        9/19/2020  10:12 AM          87772 hector.txt
-a----        9/20/2020  11:44 AM           1142 hectormachine10scan.txt
-a----        9/20/2020  11:41 AM           2100 hectormachine1scan.txt
-a----        9/20/2020  11:15 AM          86526 hectorscan1.txt
-a----        9/18/2020   2:26 PM          88106 JonathanHoffmann1scan.txt
-a----        9/18/2020   2:45 PM           2326 JonathanHoffmannmachine10scan.txt
-a----        9/16/2020   4:52 PM           2100 kelvinhunt10scan.txt
-a----        9/16/2020   4:59 PM          11916 kelvinhunt1scan.txt
-a----        9/16/2020   4:55 PM           2104 kelvinmachine10scan.txt
-a----        9/20/2020   9:41 PM          94836 MVillarrealscan1.txt
-a----        9/16/2020   6:28 PM         103682 Ramjitscan1.txt
-a----        8/25/2020   6:17 PM          24816 richardgrantscan1.txt
-a----        9/16/2020   3:06 PM           1962 travismachine10scan.txt
-a----        9/16/2020   2:59 PM           2838 travismachine1scan.txt
-a----        9/16/2020   2:51 PM          89470 travisscan1.txt
-a----        9/16/2020   2:19 PM           1964 travistorresmachine10scan.txt
-a----        9/20/2020   9:35 PM            506 villarrealscan1.txt
-a----        9/19/2020   3:54 PM            506 yournamemachine10scan.txt
-a----        8/30/2020   9:56 PM           1710 yournamemachine26can.txt
-a----        9/16/2020   2:18 PM           4362 yournamescan1.txt


PS C:\_PSModules> cat MVillarrealscan1.txt

Starting Nmap 7.30 ( https://nmap.org ) at 2020-09-20 21:40 Eastern Daylight Time
Initiating ARP Ping Scan at 21:40
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 21:40, 1.98s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 21:40
Completed Parallel DNS resolution of 255 hosts. at 21:40, 0.00s elapsed
Nmap scan report for 172.16.4.0 [host down]
```

Appendix 2/ Continuation of Remove command.



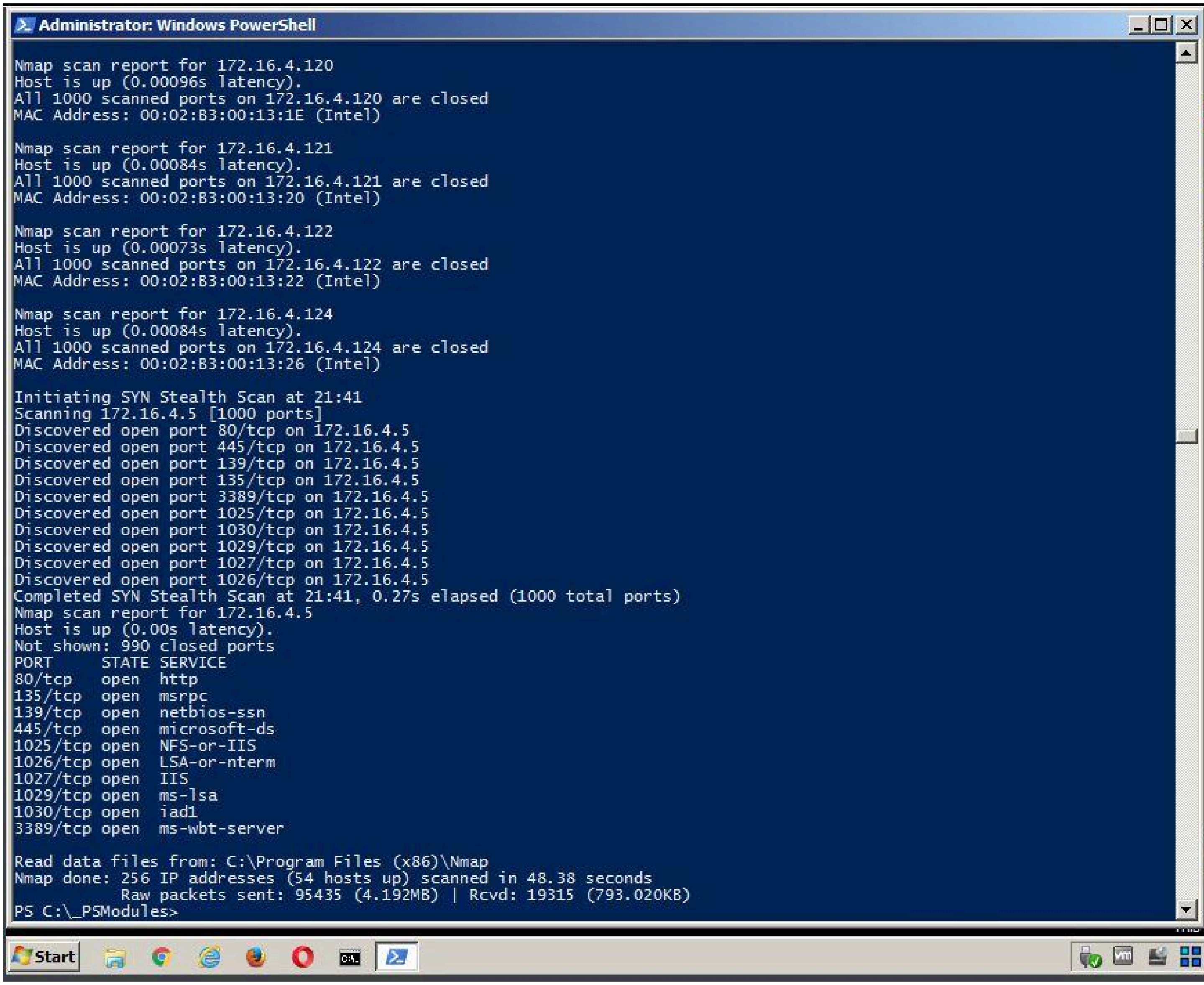
```
PS C:\_PSModules> Remove-Item -path c:
Remove-Item : Cannot remove the item at 'C:\_PSModules' because it is in use.
At line:1 char:1
+ Remove-Item -path c:
+ ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [Remove-Item], PSInvalidOperationException
    + FullyQualifiedErrorId : InvalidOperation,Microsoft.PowerShell.Commands.RemoveItemCommand

PS C:\_PSModules> remove-Item c:
remove-Item : Cannot remove the item at 'C:\_PSModules' because it is in use.
At line:1 char:1
+ remove-Item c:
+ ~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [Remove-Item], PSInvalidOperationException
    + FullyQualifiedErrorId : InvalidOperation,Microsoft.PowerShell.Commands.RemoveItemCommand

PS C:\_PSModules> Remove-Item -path c:\_PSModules\MVillarrealscan1.txt
PS C:\_PSModules> ls


    Directory: C:\_PSModules


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/14/2016  12:02 PM                Kansa
-a----        9/15/2020   1:30 AM         101288 adamscan1.txt
-a----        9/19/2020  10:11 AM          87766 hector
-a----        9/19/2020  10:12 AM          87772 hector.txt
-a----        9/20/2020  11:44 AM           1142 hectormachine10scan.txt
-a----        9/20/2020  11:41 AM           2100 hectormachine1scan.txt
-a----        9/20/2020  11:15 AM          86526 hectorscan1.txt
-a----        9/18/2020   2:26 PM          88106 JonathanHoffmann1scan.txt
-a----        9/18/2020   2:45 PM           2326 JonathanHoffmannmachine10scan.txt
-a----        9/16/2020   4:52 PM           2100 kelvinhunt10scan.txt
-a----        9/16/2020   4:59 PM          11916 kelvinhunt1scan.txt
-a----        9/16/2020   4:55 PM           2104 kelvinmachine10scan.txt
-a----        9/20/2020   9:56 PM         272742 MVillarrealmachine10scan.txt
-a----        9/16/2020   6:28 PM         103682 Ramjitscan1.txt
-a----        8/25/2020   6:17 PM          24816 richardgrantscan1.txt
-a----        9/16/2020   3:06 PM           1962 travismachine10scan.txt
-a----        9/16/2020   2:59 PM           2838 travismachine1scan.txt
-a----        9/16/2020   2:51 PM          89470 travisscan1.txt
-a----        9/16/2020   2:19 PM           1964 travistorresmachine10scan.txt
-a----        9/20/2020   9:35 PM            506 villarrealscan1.txt
-a----        9/19/2020   3:54 PM            506 yournamemachine10scan.txt
-a----        8/30/2020   9:56 PM           1710 yournamemachine26can.txt
-a----        9/16/2020   2:18 PM           4362 yournamescan1.txt


PS C:\_PSModules> _
```

Appendix 3



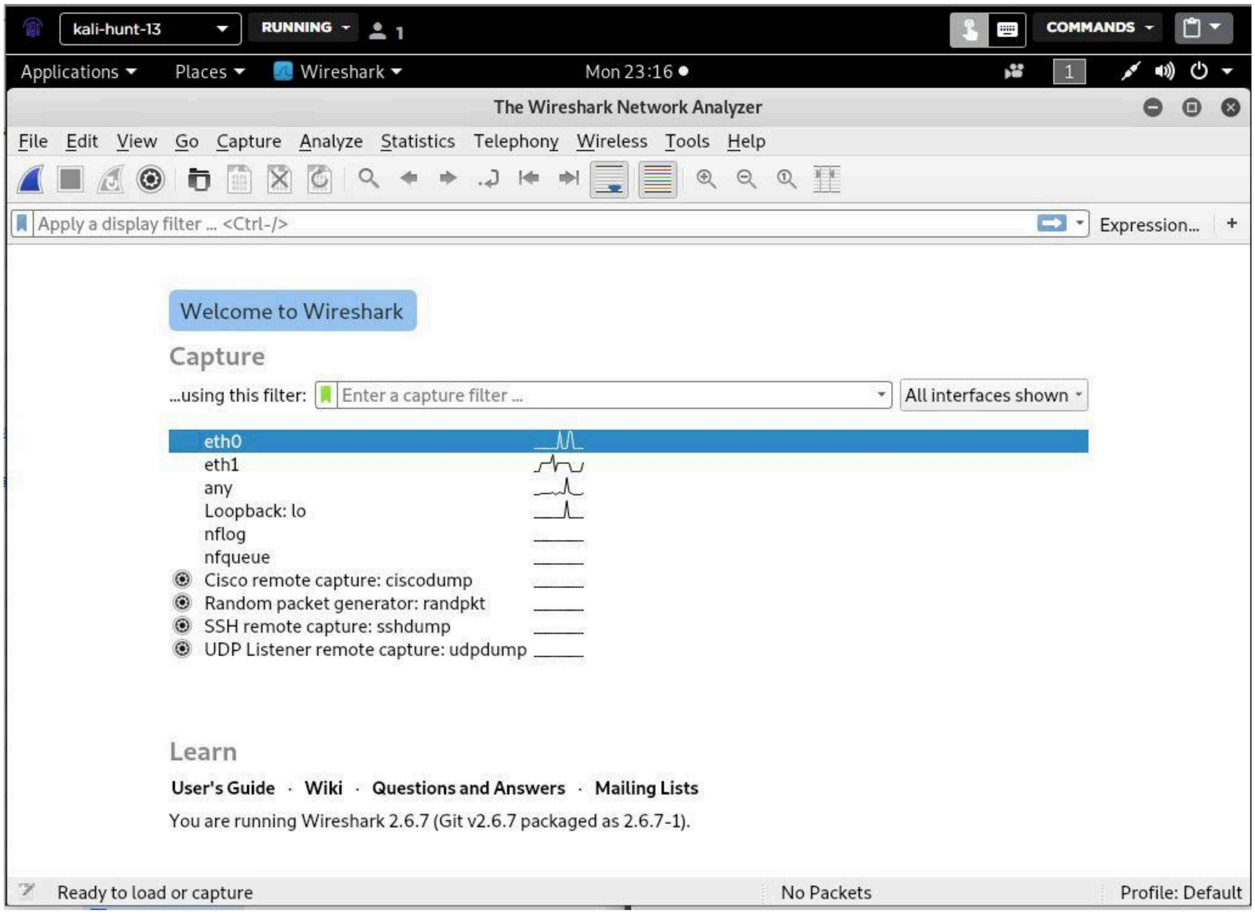
```
-a----         9/16/2020   3:06 PM           1962 travismachine10scan.txt
-a----         9/16/2020   2:59 PM           2838 travismachine1scan.txt
-a----         9/16/2020   2:51 PM          89470 travisscan1.txt
-a----         9/16/2020   2:19 PM           1964 travistorresmachine10scan.txt
-a----         9/20/2020   9:35 PM            506 villarrealscan1.txt
-a----         9/19/2020   3:54 PM            506 yournamemachine10scan.txt
-a----         8/30/2020   9:56 PM           1710 yournamemachine26can.txt
-a----         9/16/2020   2:18 PM           4362 yournamescan1.txt


PS C:\_PSModules> Remove-Item -path c:\_PSModule\MVillarrealmachine10scan.txt
Remove-Item : Cannot find path 'C:\_PSModule\MVillarrealmachine10scan.txt' because it does not exist.
At line:1 char:1
+ Remove-Item -path c:\_PSModule\MVillarrealmachine10scan.txt
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\_PSModule\MV...chine10scan.txt:String) [Remove-Item], ItemNotFoundEx
   ception
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.RemoveItemCommand

PS C:\_PSModules> Remove-Item -path c:\_PSModules\MVillarrealmachine10scan.txt
PS C:\_PSModules> Remove-Item -path c:\_PSModules\Villarrealscan1.txt
PS C:\_PSModules> ls


    Directory: C:\_PSModules


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/14/2016  12:02 PM                Kansa
-a----        9/15/2020   1:30 AM         101288 adamscan1.txt
-a----        9/19/2020  10:11 AM          87766 hector
-a----        9/19/2020  10:12 AM          87772 hector.txt
-a----        9/20/2020  11:44 AM           1142 hectormachine10scan.txt
-a----        9/20/2020  11:41 AM           2100 hectormachine1scan.txt
-a----        9/20/2020  11:15 AM          86526 hectorscan1.txt
-a----        9/18/2020   2:26 PM          88106 JonathanHoffmann1scan.txt
-a----        9/18/2020   2:45 PM           2326 JonathanHoffmannmachine10scan.txt
-a----        9/16/2020   4:52 PM           2100 kelvinhunt10scan.txt
-a----        9/16/2020   4:59 PM          11916 kelvinhunt1scan.txt
-a----        9/16/2020   4:55 PM           2104 kelvinmachine10scan.txt
-a----        9/16/2020   6:28 PM         103682 Ramjitscan1.txt
-a----        8/25/2020   6:17 PM          24816 richardgrantscan1.txt
-a----        9/16/2020   3:06 PM           1962 travismachine10scan.txt
-a----        9/16/2020   2:59 PM           2838 travismachine1scan.txt
-a----        9/16/2020   2:51 PM          89470 travisscan1.txt
-a----        9/16/2020   2:19 PM           1964 travistorresmachine10scan.txt
-a----        9/19/2020   3:54 PM            506 yournamemachine10scan.txt
-a----        8/30/2020   9:56 PM           1710 yournamemachine26can.txt
-a----        9/16/2020   2:18 PM           4362 yournamescan1.txt


PS C:\_PSModules>
```

Appendix 4/Nmap



```
Nmap scan report for 172.16.4.120
Host is up (0.00096s latency).
All 1000 scanned ports on 172.16.4.120 are closed
MAC Address: 00:02:B3:00:13:1E (Intel)

Nmap scan report for 172.16.4.121
Host is up (0.00084s latency).
All 1000 scanned ports on 172.16.4.121 are closed
MAC Address: 00:02:B3:00:13:20 (Intel)

Nmap scan report for 172.16.4.122
Host is up (0.00073s latency).
All 1000 scanned ports on 172.16.4.122 are closed
MAC Address: 00:02:B3:00:13:22 (Intel)

Nmap scan report for 172.16.4.124
Host is up (0.00084s latency).
All 1000 scanned ports on 172.16.4.124 are closed
MAC Address: 00:02:B3:00:13:26 (Intel)

Initiating SYN Stealth Scan at 21:41
Scanning 172.16.4.5 [1000 ports]
Discovered open port 80/tcp on 172.16.4.5
Discovered open port 445/tcp on 172.16.4.5
Discovered open port 139/tcp on 172.16.4.5
Discovered open port 135/tcp on 172.16.4.5
Discovered open port 3389/tcp on 172.16.4.5
Discovered open port 1025/tcp on 172.16.4.5
Discovered open port 1030/tcp on 172.16.4.5
Discovered open port 1029/tcp on 172.16.4.5
Discovered open port 1027/tcp on 172.16.4.5
Discovered open port 1026/tcp on 172.16.4.5
Completed SYN Stealth Scan at 21:41, 0.27s elapsed (1000 total ports)
Nmap scan report for 172.16.4.5
Host is up (0.00s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1029/tcp open  ms-lsa
1030/tcp open  iad1
3389/tcp open  ms-wbt-server

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 256 IP addresses (54 hosts up) scanned in 48.38 seconds
           Raw packets sent: 95435 (4.192MB) | Rcvd: 19315 (793.020KB)
PS C:\_PSModules>
```

Appendix 5/ The wireshark network analyzer.


kali-hunt-13
RUNNING
1
COMMANDS
Applications
Places
Wireshark
Mon 23:16
1
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

eth0
eth1
any
Loopback: lo
nflog
nfqueue
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

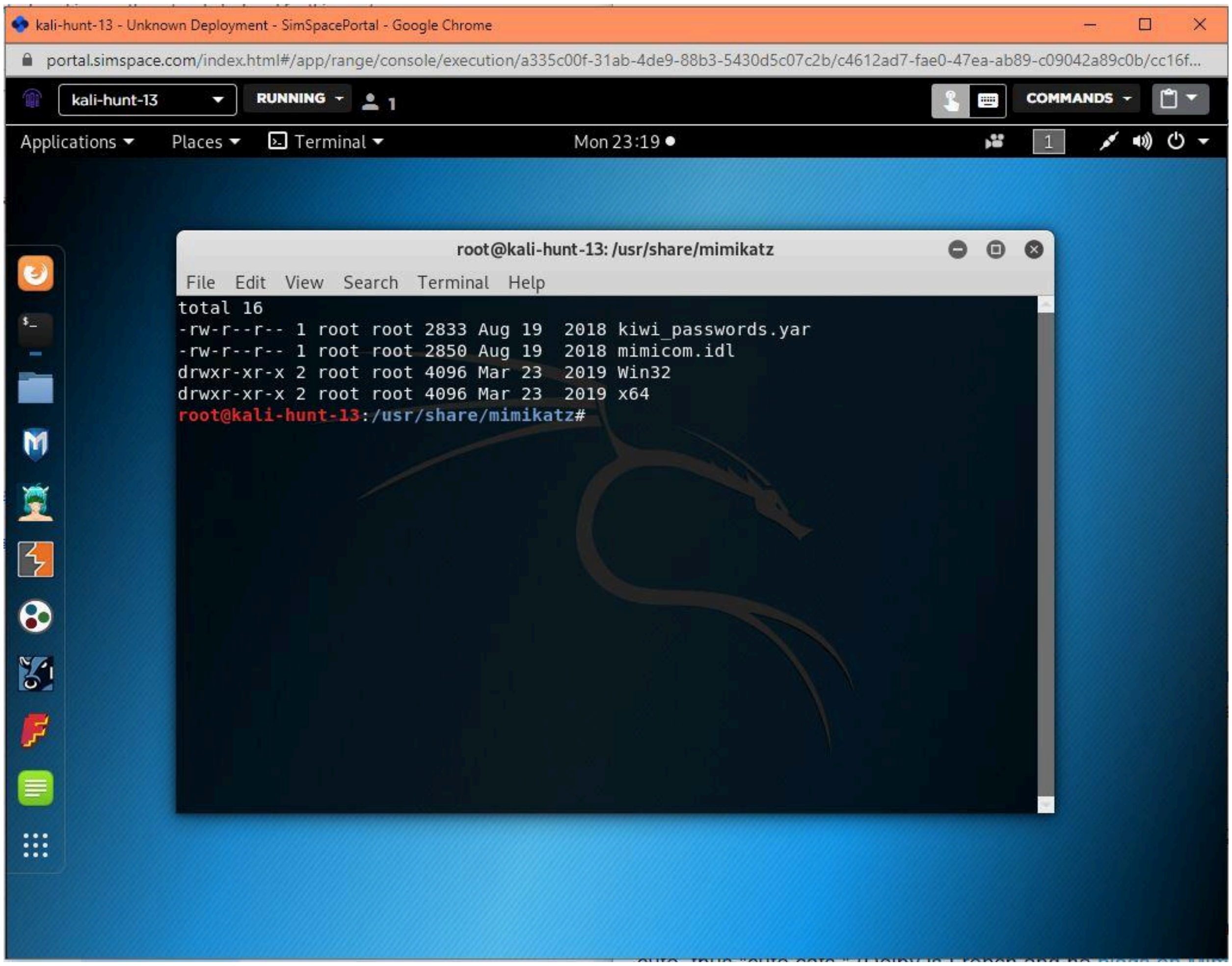
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.6.7 (Git v2.6.7 packaged as 2.6.7-1).

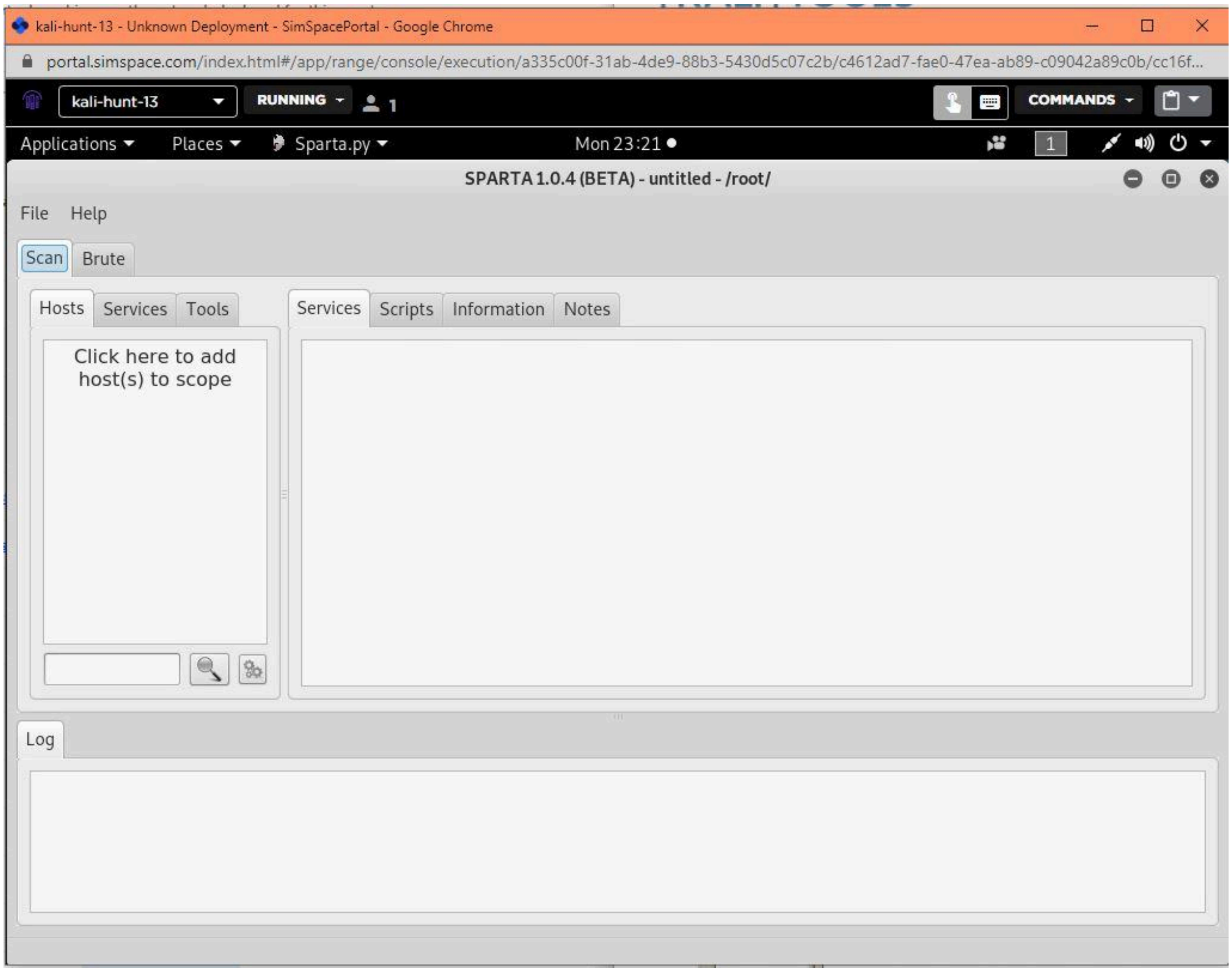
Ready to load or capture | No Packets | Profile: Default

Appendix 6/ Mimikatz password tool


kali-hunt-13 - Unknown Deployment - SimSpacePortal - Google Chrome
portal.simspace.com/index.html#/app/range/console/execution/a335c00f-31ab-4de9-88b3-5430d5c07c2b/c4612ad7-fae0-47ea-ab89-c09042a89c0b/cc16f...
kali-hunt-13
RUNNING
1
COMMANDS
Applications
Places
Terminal
Mon 23:19
1
root@kali-hunt-13: /usr/share/mimikatz
File
Edit
View
Search
Terminal
Help

```
total 16
-rw-r--r-- 1 root root 2833 Aug 19  2018 kiwi_passwords.yar
-rw-r--r-- 1 root root 2850 Aug 19  2018 mimicom.idl
drwxr-xr-x 2 root root 4096 Mar 23  2019 Win32
drwxr-xr-x 2 root root 4096 Mar 23  2019 x64
root@kali-hunt-13:/usr/share/mimikatz#
```

Appendix 7/Sparta penetration tool.



kali-hunt-13 - Unknown Deployment - SimSpacePortal - Google Chrome
portal.simspace.com/index.html#/app/range/console/execution/a335c00f-31ab-4de9-88b3-5430d5c07c2b/c4612ad7-fae0-47ea-ab89-c09042a89c0b/cc16f...
kali-hunt-13
RUNNING
1
COMMANDS
Applications
Places
Sparta.py
Mon 23:21
1
SPARTA 1.0.4 (BETA) - untitled - /root/
File
Help
Scan
Brute
Hosts
Services
Tools
Services
Scripts
Information
Notes
Click here to add host(s) to scope
Log

References

(n.d.). Retrieved from http://sparta.secforce.com/

Corporation, S. (n.d.). Retrieved from https://portal.simspace.com/docs/index.html

Download. (n.d.). Retrieved from https://www.wireshark.org/

Porup, J. (2019, March 05). What is Mimikatz? And how this password-stealing tool works. Retrieved from https://www.csoonline.com/article/3353416/what-is-mimikatz-and-how-to-defend-against-this-password-stealing-tool.html

SPARTA. (n.d.). Retrieved from https://tools.kali.org/information-gathering/sparta

Virtual Machines: Pros & Cons. (2019, December 09). Retrieved from https://www.cynexlink.com/2017/08/18/virtual-machines-pros-cons/

Wireshark Training. (n.d.). Retrieved from http://www.wiresharkbook.com/