The Hacker's Toolkit

Module 5 | Activity 2

Introduction

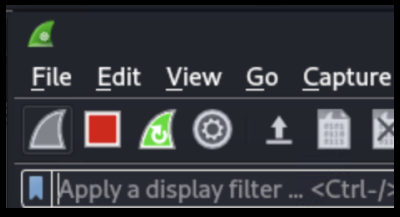
Every profession has its arsenal of tools used to get the job done. Within the field of cyber security, there is an ever growing plethora of programs and applications that can help us test services or find out if our network has been compromised. In this activity, we will run through some basic tools commonly used to get information from our systems.

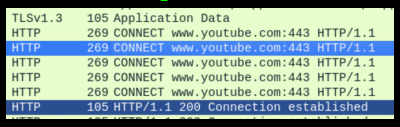
Note

It is likely that you will have to install a lot of these tools before using them, but fear not. The process is relatively generic. Follow the steps below the chart to install the tool if you get a "command not found" error.

Program/ Tool	Purpose	For You To Do!
ping	A tool that is used to test whether or not you are connected to a server or router within your network. Could be thought of as "poking" your friend that's driving to ensure that they are in fact awake or "up".	Try pinging your DNS server using **ping 199.100.16.100** Then ping your default gateway, but this time use the **man** pages to figure out how to send only 10 packets. *__ctrl + C__ to exit*
dig	Helps us talk to and obtain information from DNS nameservers. Think of it as a domain name-to-IP address converter.	Use this command to find the address of these nameservers - iastate.edu - apple.com - microsoft.com You will see that using dig on its own outputs a lot of data we might not know how to use yet. So append these two flags **+noall +answer** to the end of your queries, like so. **dig iastate.edu +noall +answer**
whois	Tells us information about the domain and the domain owner. Information includes:	Using ICANN discover the information about the following domain names… - apple.com - cnn.com

	-who the owner is -who the domain was registered by -registration dates *Essentially answers "who is the…"	- iastate.edu - Coolmathgames.com Notice the difference between websites that have more security than others. Feel free to compare some more domains.
traceroute	This tool helps trace the path the network packet takes.	Install this command using **sudo apt install traceroute**. As you know, ISEAGE blocks all external traffic. Discover what happens when you type the following commands… **traceroute 199.100.16.100**
netstat	Helps us figure out what ports and services are open and running on a machine.	Install using **sudo apt install net-tools**, all on one line. Since we don't have any services or open ports right now, running netstat will look pretty boring. However, we will use it in the future. **netstat -tl**
Wireshark	An application that helps us "sniff" network traffic packets. When network traffic is being transmitted in an unencrypted	Go to your desktop and click on the blue kali dragon icon in the top left corner of the screen. Start typing "Wireshark" into the

	format, otherwise known as "plaintext". Wireshark will let us see anything from passwords being sent over to the contents of emails.	search bar and click on it once it shows up. It should look like a blue shark's fin. Once you click on it, you might be asked to type in your password. Click on the eth0 interface which should be the first option to begin capturing traffic. Now that Wireshark is running, open up a firefox tab and go to youtube.com. A few seconds after you land on the youtube page, go back to wireshark and press the red STOP button on the top left corner of the wireshark interface.  Now, right below the STOP button there is a "filter bar" to filter the hundreds of packets that wireshark picks up. In that filter type in "http" and press Enter. Scroll down a few entries and keep your eye on the "Info" column. You should run into the

		following:  This shows the very website we accessed just seconds ago! It's not very exciting to spy on yourself, but this exact idea is what can be applied to spy on other machines on your network.
hashcat	Hashcat is another password cracking tool installed on Linux.	Head to the link to learn how this tool is used. https://hashcat.net/hashcat/

Installation Guide

If you're here then it's probably because the dig tool gave you an error. I will base these instructions off of the dig tool installation and then you could adjust them accordingly for the other commands.

- The dig tool exists under the package dnsutils which makes sense since it is a utility that helps us collect information from nameservers.
- So we need to install this package using the command **sudo apt install dnsutils**
- You will be prompted to enter your password. Type it in and press Enter.
- The download will begin and shortly thereafter you will be asked if you will allow the new package to take up "x" amount of disk space to which you simply type in **Y** for "yes" and then press Enter.
- You should now be able to use the dig tool.


```
┌──(wall-e㉿Hailey)-[~]
└─$ sudo apt install dnsutils
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
  bind9-dnsutils bind9-libs
The following NEW packages will be installed:
  bind9-dnsutils dnsutils
The following packages will be upgraded:
  bind9-libs
1 upgraded, 2 newly installed, 0 to remove and 1333 not upgraded.
Need to get 2,050 kB of archives.
After this operation, 1,125 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 bind9-libs amd64 1:9.16.15-1 [1,404 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 bind9-dnsutils amd64 1:9.16.15-1 [391 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 dnsutils all 1:9.16.15-1 [255 kB]
Fetched 2,050 kB in 15s (134 kB/s)
(Reading database ... 261864 files and directories currently installed.)
Preparing to unpack .../bind9-libs_1%3a9.16.15-1_amd64.deb ...
Unpacking bind9-libs:amd64 (1:9.16.15-1) over (1:9.16.6-3) ...
Selecting previously unselected package bind9-dnsutils.
Preparing to unpack .../bind9-dnsutils_1%3a9.16.15-1_amd64.deb ...
Unpacking bind9-dnsutils (1:9.16.15-1) ...
Selecting previously unselected package dnsutils.
Preparing to unpack .../dnsutils_1%3a9.16.15-1_all.deb ...
Unpacking dnsutils (1:9.16.15-1) ...
Setting up bind9-libs:amd64 (1:9.16.15-1) ...
Setting up bind9-dnsutils (1:9.16.15-1) ...
Setting up dnsutils (1:9.16.15-1) ...
Processing triggers for kali-menu (2020.4.0) ...
Processing triggers for libc-bin (2.31-4) ...
Processing triggers for man-db (2.9.3-2) ...
```