**Advanced Security 2 Assignment 2 – Security Tools**

**Jake Bolger C18395341**

1. **Using Kali Linux, I have demonstrated two security tools it provides**

The two tools I will be demonstrating are called “0trace” and “tcpick”. The first tool I will be demonstrating is **0trace.**

**0trace:**

0trace is a package that is used as a traceroute tool. This is run within an open TCP connection. This means that it can bypass various stateful packet filters easily.

The first thing I did was install 0trace. Using “sudo apt install 0trace”.

Screenshot:

Text

Description automatically generated

Then I installed “tcpdump” and “libc6” as they are the dependencies for 0trace.

I will be demonstrating the 0trace.sh shell script which is a firewall bypassing tool that enables traceroute within a TCP connection.

As you can see when I type this command in it gives me the format of the command I must use:

Graphical user interface, logo, website

Description automatically generated

1st I needed to get the IP address for a random website:

Text

Description automatically generated

Next, I will use the command that I was shown earlier using my interface name and the Ip address for the site:

Text

Description automatically generated

Next, I needed to establish a connection so 0trace can do its job. So, I opened another terminal and typed in ‘telnet 192.64.119.3’.(make sure telnet is installed):

Text

Description automatically generated

After this connection is established, I typed in “GET / HTTP/1.1”.

Text

Description automatically generated

Then 0trace traces the Ip address back to the source.

You should then get a result saying target reached or probe rejected by target:

A screenshot of a computer

Description automatically generated with medium confidence

**Tcpick:**

“Tcpick” is a tool used to reorder, track, and reassemble TCP streams. It can also be used to save captured flows in files to display them in the terminal.

First step was to install tcpick and its dependencies (libc6 + libpcap0.8)

A screenshot of a computer

Description automatically generated with medium confidence

First I tried out one of the base options to listen on the docker0 interface using the command “tcpick -i –interface docker0”

Text

Description automatically generated