**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 “evil-Ssdp”. 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

**Evil-Ssdp:**

SSDP multicast discovery requests are responded to with this tool, posing as a generic UPNP device on the local network. You'll be able to see the spoofed device in Microsoft Windows Explorer on machines in your local network. A configurable webpage is presented to users who are tempted to open the device.

First, I installed **evil-ssdp.**

**Text

Description automatically generated**

Also installed dependencies which was ‘python3’.

Then I ran the program using python3:

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

Next, we are going to use the spoofing scanner SSDP. This allows us to spoof a scanner as a reliable UPnP device. We must configure the template to start:

Text

Description automatically generated

The next step is to manipulate the user to click on the application. A fake scanner will appear on the network. When the user clicks it, they are directed to the default web browser. They think they are connected to a genuine scanner.

They enter their credentials in the template at this link:



Graphical user interface, text, website

Description automatically generated

Once the user has entered the credentials, I checked the terminal and found the credentials that were entered by the user. This gives me access to their network username and password. Admin and ‘mynameisjake’

Text

Description automatically generated

1. **Using Metasploit to show how vulnerabilities can be exploited.**

First, we will need to do an investigation on the ports for the IP address that we’re trying to find vulnerabilities on.

Use Nmap:

Text

Description automatically generated

Now, we need to start up Metasploit to give us access.

Start-up Metasploit:

Graphical user interface, diagram

Description automatically generated

Now we can check if the computer system is vulnerable to certain type of attacks.

Search SMB to see all the results that see scanner. We can check if the system is vulnerable to SMB attacks.

**Text

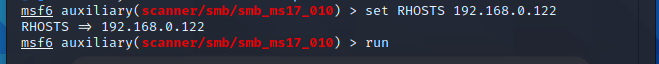
Description automatically generated**

Now we enter this command to show all the options to whether this computer is vulnerable to an attack.

**A screenshot of a computer

Description automatically generated with medium confidence**

Setting the IP address and running it:

****

**Text

Description automatically generated with low confidence**

Next step is to search for exploits:

**Text

Description automatically generated**

This shows the exploits we can use and utilise.

We need to find an exploit.

Now we will enter to use the exploit.

A picture containing graphical user interface

Description automatically generated

Now we want to set the RHOSTS again.

Graphical user interface

Description automatically generated with low confidence

Now we can set the payload.

A picture containing graphical user interface

Description automatically generated

Now we can enter exploit.

Text

Description automatically generated

Now we are in the computers system. we have hacked into the computer system.

If you enter something like ‘sysinfo’ you will be able to see all the system information.

Now, you will be able to migrate the shell we have receive and take a screen capture of the entire computer system.

We do this using ‘migrate’ followed by the number of the drive.

Once this is done, we can enter ‘screenshot’

Now an entire copy of the desktop screen is saved to whatever you want.

After you’ve saved this, you will have full access to another computer system.

1. **Using DVWA to demonstrate how web applications can be hacked with two examples.**

The two examples I will be demonstrating are Brute force attacks and Command injections. First step was to Download and set up DVWA.

This was done by downloading the GitHub repo and setting it up from there.