**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

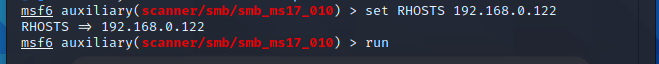
Description automatically generated**

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. I followed the instructions for setting up DVWA so I could access ‘127.0.0.1/dvwa/’.

The first example of how a web application is hacked using DVWA is a **brute force attack.**

The security level I used for this was low:

Graphical user interface, text

Description automatically generated

If we try login, we can see that we are able to log in, but for this we are going to assume that we don’t know the password.

For brute force attacking we want to use hydra which is already installed in Kali Linux.

First command we want to run is to specify the Ip address we want to target, which is 127.0.0.1 in our case.

Once the user types in their username and password the answers are being sent by post request.

The command we run is specifying the argument of the path to the page the user is logging in at.

The command is separated using a colon.

To get the arguments we need for the username and password we go to the page source in get the actions.

Graphical user interface, text, application

Description automatically generated

Now we have the arguments for our command:

Text

Description automatically generated

Now if we login with incorrect password and username we can see that we have this string outputted:

Graphical user interface, text

Description automatically generated

We use this string in our command and specify the files we want to use:

Text

Description automatically generated

These holds the usernames and passwords we are going to try:

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Now we can run our command:

Text

Description automatically generated

As you can see it worked and found the username and passwords:

Text

Description automatically generated

The second example we will look at is **Command Injection:**

If we try to put in our local Ip address, we get this:

Graphical user interface, text

Description automatically generated

Next, we open Wireshark and then try to submit the Ip address again and now we can see the ping request and reply:

Graphical user interface, text, application, email

Description automatically generated

Now we must find the vulnerability.

We can insert something so we can use injection.

For example, we can use this:

Graphical user interface, text

Description automatically generated with medium confidence

Once we submitted the command, we end up with this:

A close-up of a document

Description automatically generated with medium confidence

Now we have all the details of the user’s network, and the parent directory. This is how we do command injection.

We can also see all the files in the directory.

Showing all the files:

Text

Description automatically generated with low confidence

1. **This section is a report that discusses the impact of laws on the use of security tools. It discusses whether it is ethical or not to carry out the experiments I have been doing.**

**Are there any benefits in terms of organisation systems security improvements when we use security tools?**

First, the impact of laws or legislation on the use of security tools will be discussed. In recent years there has been a spike in new legislation against cybersecurity. The goal of this is to protect against cybercrime. All over the world, countries have introduced new laws to combat cybercrime and the growth in technology. In the European union, the NIS Directive has been used to promote legislation to be ready for cyber-attacks.

There are many challenges and impacts of laws on the use of security tools. It can impact stakeholders such as tech companies and normal users. lots of challenges are being created because of this. They are as follows:

One of the impacts is that some laws, whilst helping reduce attacks also outlaw certain security tools in the process which can be used to protect against cyber-attacks. Lots of laws are being passed to combat this are being delayed. So, the enactment of laws is being delayed.

Another big impact that laws have on security tools is that a lot of them are falling behind in context or falling behind in time. Technology is progressing at an extremely fast pace. This means that some laws that were created ion the past are not valid anymore. The standards of the laws and cybersecurity has changed. The laws need to be updated when responding to issues of legislation and cybersecurity.

Lots of countries have different laws in relation to security tool. This means that legal issues are hard to respond to. Some tools may be banned or impacted in a certain country and then in another it has implications. This impacts security tools on an international level.

Normally, laws have a good impact on security tools and cybersecurity. However, some of these laws undermine the use of security tools. The internet is seen free, and you can do whatever you like. Some laws have the opposite effect on security tools.

Finally, limitations are put on certain security tool applications. The enactment or even the absence of laws can undermine the use of security tools. This means users face challenges when investigating or using security tools to learn or act on cyber threats.

Next, I will discuss whether it is ethical to carry out the experiments I have been doing. The word hacking means that you are using a device in an alternate way than it was meant to be used. These experiments that I have been doing are ethical but, sometimes you must be careful even if the techniques you are using are ethical. The techniques like using tools such as Evil-ssdp or brute force attacking etc. are ethical to use if they are intended for educational or security purposes. They should not be used to do harm or to gain something for yourself.

Its also ethical to use these tools if you are not breaching public or private networks of other people. It can be tempting to do this but is wrong.

Sometimes it can also be tempting to use pirated software, this can jeopardise people and their security. If you don’t do this the experiments are ethical.

In the experiments I conducted I never once used someone else data. using someone else’s data for personal gain is not ethical and shouldn’t be practised.

Next, I will discuss the benefits in terms of organisation systems security improvements when we use security tools. There are lots of benefits, the first one is it makes sure all the information is secure. It protects digital data on devices and cloud.

Another benefit is that it improves resilience to attacks. Using security tools increases protection.

Security tools protects confidentiality, availability and integrity of people’s data or company data and information.

Security tools help an enormous amount to responding to security threats. It helps companies to adapt to changes in the environment and reduces risks.

Tools also help organisations reduce the cost of protecting against threats. It allows them to lower the amount of security layers they have whilst keeping the same level of protection.

Finally, security tools provide a good framework for managing information and keeping it protected in organisation systems security.

