**Advanced Security 2 CA2**

**Part 1 Two Security Tools:**

Nmap:

This a built-in tool in kali Linux. Nmap is a powerful assessment tool which I used to scan a network. Nmap allows you to see running ports and running services along with there associated version numbers. Once it find theses, the software then sends information to hose hosts and services to see its response. From the that response then it can make a map of the network.

The first command I ran was nmap -h to get help using the tool:

Text

Description automatically generated

Text

Description automatically generated

I then ran nmap -v 192.168.0.0 to print the version number:

Text

Description automatically generated

After that then I ran this command to show me the open ports on my IP address:

Text

Description automatically generated

After running that command I saw that port 80 was open so I decided to google what port 80 is usually used for. My google search suggested that its commonly used for websites.

Load Balancer Detector (LBD):

This is a kali Linux tool which is useful for determining the presence of load balancing. It used for penetration testing and ethical happening. It offers a few security benefits it offers protection against DOS attacks etc.

The example I am going to use is bing.com and port 80. I am going to check if bing.com uses load balancing:

So firstly I opened the lbd tool in my kali linux environment and typed in this command:

A screenshot of a computer

Description automatically generated with medium confidence

As you can see bing.com does use load balancing and it also gives us bing.com IP address.

**Part 2 Metaspoilt:**

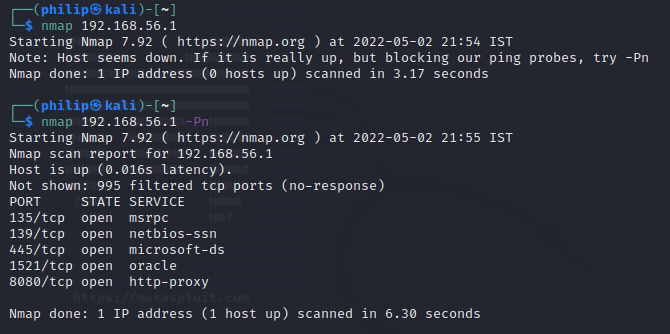
For this part of the assignment I am using metaspoilt on kali linux to demonstrate how vulnerabilities can be exploited.

The first thing I done was ran ipconfig on my windows machine to get the IP address and I will then try and find vulnerabilities on my machine that I can exploit.

Text

Description automatically generated

I then used the nmap function to find out more about my IP address:



This shows me the version of the OS and access that I may be able to gain access to. I can see that ports 139 and 445 are open. These are what known as smb services ( Service message block ). This allows for file sharing. The next thing I want to do then is find out there version so I will use the following command.

A picture containing text

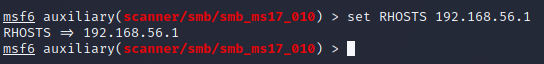
Description automatically generated

After getting this information I can open up Metasploit and try exploit these services.sudo mfs. The first command I then run is search smb this shows the different modules I can run to check the computer system. Now I am going to check if this system is vulnerable to smb attacks:

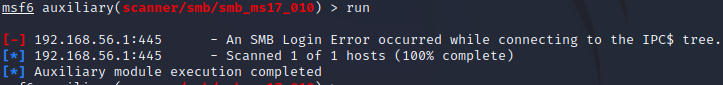
Graphical user interface

Description automatically generated with medium confidence

As you can see I tried using the auxiliary/scanner/smb/smb\_ms17\_010 tool. Next I set rhosts to the windows machine IP address:



I then enter run in the command line to see if my host is vunerable to this attack:



Its not vulnerable to this attack but if it was I would then search grep exploits smb and find a tool to exploit the vulnerability.

**Part 3 DVWA:**

For this section I am going to demonstrate how web applications can be hacked with two examples. DVWA stands for DAMM Vulnerable Web Application. Its what’s known as an open source web application designed to be vulnerable so one can practise ethical hacking.

The first thing I done was download DVWA and change some of the original configuration (Username and password). I then started a mysql service and logged in.

The next thing I done grant permissions to and create the new user:

Text

Description automatically generated

The next thing I had to do was start and configure my apache server:

**Part 4:**

Impact of laws in security tools:

Security tools are software or sometimes hardware-based tools that security teams use to protect there organizations networks, critical infrastructure, and sensitive data form attacks. There are a lot of these tools out there which can be used depending on the specific function the security team are looking to accomplish.

Laws for protecting organizations from cyber attacks are inherently a good thing but makes using certain tools tricky. Ethical hacking tools which are used by security teams to penetration test and check the cyber security of the organization can also be used by hackers with ill intent to hack an organization and tack control of system or get protected data etc. Laws are in place to hinder the use of security tools being used for the wrong reasons. Laws are in place to make it illegal to use these tools against organizations without there approval.

Is it ethical to carry out the experiments I done in the first 3 parts?:

In my opinion the experiments I carried out were ethical as I am currently completing a bachelor’s degree in computer science, and I done these tests for a module called Advanced Security 2. These tools are very commonly used by security teams in the industry so if I decided I wanted to go into security after I finish my degree, I should be able to use the basic tools before I get a job.

I also didn’t hack or use any of these tools against any organizations which didn’t give me permissions. I used them against my own windows machine and against DVWA which is a site I ran on my own machine again and its only purpose is to learn different ethical hacking techniques so I would say it is ethical what I done in the first three parts in this assignment

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

Yes, there is security tools especially ethical hacking tools which can greatly improve the security of an organizations system. Ethical hacking tools can be used to test an organizations system using penetration testing. This can show a security team if there are week points in the system that can be exploited by hackers. When these weak points are found then security teams can start on fixing these weak points and put security systems in place to stop these weak points getting exploited.