Ethical Hacking

License

Contents

General notes about the labs

Often the lab instructions are intentionally open ended, and you will have to figure some things out for yourselves. This module is designed to be challenging, as well as fun!

However, we aim to provide a well planned and fluent experience. If you notice any mistakes in the lab instructions or you feel some important information is missing, please feel free to add a comment to the document by highlighting the text and click the comment icon (▤), and we will try to address any issues. Note that your comments are public.

You should maintain a lab logbook / document, which should include your answers to the questions posed throughout the labs (in this colour).

Preparation

Start by loading the latest version of the LinuxZ template from the IMS system. If you have access to this lab sheet, you can read ahead while you wait for the image to load.

> To load the image: press F12 during startup (on the boot screen) to access the IMS system, then login to IMS using your university password. Load the template image: LinuxZ (load the latest version).

Once your LinuxZ image has loaded, log in using the username and password allocated to you by your tutor.

Using the VM download script (as described in a previous lab), download and **start** these VMs:

- Kali Linux - **with Armitage and MSF Pro (username: root, password: toor)**
- Win2k - vulnerable web server

Note: the download may take some time, so please read ahead while you wait.

Introduction

This lab covers the fundamentals of attacking computer systems. These techniques are used by malicious attackers and security professionals alike. In this lab you will attack a computer system, following the typical steps in an attack: reconnaissance, scanning, gaining access, maintaining access, and covering tracks[1].

Please note: complete these lab exercises within the Leeds Met lab environment. Conducting these attacks against other machines without explicit permission could be considered illegal.

Scenario

The Windows virtual machine (VM) may be vulnerable to attack, it is your job to identify the machine, and see if you can gain access to it. We will use the Kali Linux VM as our attack machine.

Step 1: Reconnaissance and Footprinting

[1] This lab gives an overview of the very large topic of security assessment and ethical hacking. For more detailed ethical hacking, you can look forward to later security modules.

The first phase of an attack typically involves identifying the IP address(es) used by an organisation, so that we can target attacks against it, and gather information using non-invasive techniques. In this scenario, we only need to identify which host on our network is the Windows machine and determine its IP address.

Kali Linux is a Linux distribution especially designed for penetration testing, and forensics. These distros have become the industry standard for ethical hacking.

If you have not already done so (it should already be running), start the Kali VM.

On the Kali Linux VM:

Assuming you downloaded the Live disk VM, select the Live boot option, by pressing enter. Tip: to get your mouse back to your host OS, press “Ctrl-Alt”.

Before long you are greeted by the Kali Linux desktop.

Start by browsing through the tools that are available.

Click the “Applications” menu → “Kali Linux”

There are an amazing amount of security/hacking tools included with Kali. Take a few minutes to familiarise yourself with the layout of this menu.

Most of these programs are command line tools. Open a terminal, by clicking the console icon (>_).

This is where the magic happens!

To further emphasise the sheer amount of ~~awesomeness~~ tools, run:

```
ls /usr/bin
```

Have a quick scroll through the vast “arsenal” of tools. Do you already recognise any of these programs?

First, since the server is on our network, we need to know what IP addresses are used.

Open a terminal, by clicking the console icon (>_).

Run the command:

```
ifconfig
```

Note the IP address starting with 172 (this is your IP address for the host-only network, which your target is also on).

Question: IP = __

Nmap can be used to scan IP address ranges for active hosts.

Run the command (where *XXX.XXX* is from the above):

```
nmap 172.XXX.XXX.0-255 -sn
```

Question: Explain what the "-sn" above does: (Hint: Run the command: "nmap --help" or "man nmap")

In this case we know the machine we are looking for is running a web server. Web servers typically listen on a particular port, and send information on that port when web browsers connect and request pages.

Question: what port does HTTP (Web) traffic normally use?

Port = __

We can use this information to discover which IP addresses on our network are running web servers.

Run the command (where PP is the port above, and *XXX.XXX* is as above):

```
nmap -p PP 172.XXX.XXX.1-255
```

Send the results to a text file, for easier searching, by adding "> results.txt" to the end of the previous command.

View the results:

```
less results.txt
```

(Press "q" when you are ready to quit).

Question: What is the significance of ports being in the following states? How does this relate to security? (Hint: you could Google "nmap man page")

Open:

Filtered:

Closed:

Question: List all of the IP addresses running web servers (with the port open):

Question: Which host do you think your web server is?

Target = __

Step 2: Scanning

Now that you have identified a possible IP addresses of the target, you can determine all of the services running on each host.

The most popular tool for scanning for open ports is, without a doubt, Nmap.

Read the man page:

```
man nmap
```

From the man page:

> "Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime."
>
> (by Insecure.Com LLC, licensed under the Creative Commons Attribution License version 3.0)

When you are ready, press “q” to quit.

Run this nmap command to list the accessible ports on a target (where target is as above):

```
nmap Target-IP-Address
```

Question: List all of the ports in an “open” state in your log book:

Question: What command can you use to probe open ports to determine the services that are running, and to attempt to identify the OS the target is running?

> Hint: view the man page, or try using “-A” at the end of the previous command to discover the versions of software that is running on the remote host.

Question: Record the services and version information obtained using nmap:

At this point, check that you are indeed dealing with the intended target. You should have determined that it is running Windows with IIS 5.0. If not, and if there were multiple IP addresses, repeat these steps again with another host identified during footprinting.

Visit the security focus vulnerabilities website.

Look up vulnerabilities that exist in Microsoft IIS 5 and Microsoft Windows 2000.

Question: Provide details of some vulnerabilities that likely apply to the server:

Question: Identify a remotely exploitable vulnerability from the above list (if you can't find one, see the next question):

Question: Read about the Microsoft Plug and Play Service Overflow Vulnerability, does it apply to this target? How did you come to this conclusion?

Automated tools exist that suggest likely vulnerabilities based on the services running, using databases of known security flaws. If you are interested, you could try scanning the target with Nessus (one such tool); this would involve running a VM with Nessus, or install Nessus on an OS/VM of your choice. Nessus can simplify the process of identifying likely security weaknesses.

Step 3: Gaining Access

An *exploit* is an action or software that takes an action to take advantage of a security vulnerability. At this point you could download an exploit from Security Focus for a particular vulnerability that you have identified, or from another security website. Exploiting vulnerabilities this way typically involves compiling C code, which can be easier if you are using Linux. You may wish to look into this further, and attempt to use such an exploit, when you have time.

Next, we will use Metasploit to gain access to the target machine. Metasploit is free open source software that can simplify exploitation of vulnerabilities.

Start the Metasploit services:

```
service postgresql start

service metasploit start

msfconsole

msf > go_pro
```

Please wait... eventually the web interface should load. If it fails to load you can try:

Start Iceweasel (Firefox), by clicking the icon ().

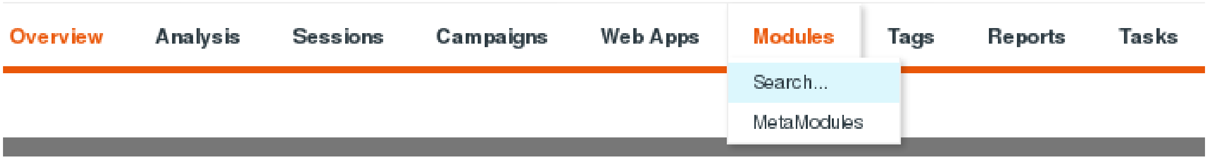
Visit https://localhost:3790

Log in with username: ***xxxxx***, password: ***xxxxx***.[2]

Click on “default”, in the projects list.

Click “Modules->Search”.

[2] Ask your tutor for the key. Note this account must only be used for educational purposes.



Search for the “Microsoft Plug and Play Service Overflow” module (*with the surrounding quotes*).

In the Target Addresses field enter the IP address of the target Windows 2000 computer.

For Payload Type select “**Command shell**”, and set connection as “**Bind**”.

Click “**Run Module**”.

This will run the exploit over the network, which takes advantage of a stack-based buffer overflow: a simple programming error that fails to correctly check variable boundaries, writing over important internal control information.

The feedback should indicate that a “session” has started.

Click the “**Sessions**” tab, then “**Session 1**”.

Open a command prompt, by clicking “**Command Shell**”.

Voila! You have access to run commands on the remote computer! Note that there was no need to trick a user into running anything, this exploit works remotely, against computers that are vulnerable to this attack.

Try these commands...

List the files and directories in C:\

```
dir C:\
```

List all the user accounts on the machine

```
net user
```

Question: Do you think your own lab computer would be vulnerable to this attack?

Attempt to attack your own Kali Linux VM using this vulnerability.

Experiment with Metasploit, and what you can now do to the victim computer.

Question: What kinds of actions can you now take on the victim system?

Step 4: Maintaining Access

Create a user account on the target computer...

In the hacked command prompt, run the command:

```
net user me pass /add
```

Use commands to confirm a new user account now exists.

Question: How else could an attacker ensure they would later have access to the computer? (Hint: consider the types of malware that may apply)

Step 5: Covering Tracks

Sometimes an attacker may wish to hide files, programs, or information on the target computer. For example, they may want to leave security tools for later use. One method of hiding data on Windows is using alternative data streams (ADS). The NTFS filesystem allows a file to have more than one "stream" of data. The default data stream will be used, unless otherwise specified when opening a file. ADS can be used to store files within existing files, and these are very hard to detect using native Windows utilities, although third party tools exist that can detect the use of ADS.

Lets hide some information and a program on the target computer.

At the prompt that you acquired earlier on the Windows 2000 target, run the command:

```
echo "looks like this" > test.txt
```

```
echo "hello, this is a hidden message" >
test.txt:secret
```

We have stored two different contents into the file.

Now display the contents of the file that is normally displayed:

```
more < test.txt
```

And to see the hidden message:

```
more < test.txt:secret
```

Note that the size of the file does not appear to grow when adding alternative streams, even though the amount of free disk space is reduced.

We can even hide executable programs in there!

This can be tricky on Win2000, so download a XP VM, and put a copy of notepad.exe in an ADS of a file:

```
type c:\windows\system32\notepad.exe >
test.txt:notepad.exe
```

Run the hidden copy of notepad:

```
start .\test.txt:notepad.exe
```

Open the test.txt file in another program, and confirm it looks like a plain text file.

This technique can be used to hide security tools within standard system files.

If you are interested, you may wish to test tools that detect ADS, and experiment with other information hiding tools, including steganography techniques that hide information within images.

Question: System logs record important events, such as security sensitive operations. If activity is only logged locally (not over a network), then what is the risk regarding traceability and accountability once an attacker has access to a host?

Conclusion

In this lab we have guided you through one specific case of attacking a vulnerable Windows host. In order to effectively audit security systems and perform attacks in real-life situations, security auditors needs a deep knowledge of security theory, tools, and techniques. Security auditing can be challenging and a lot of fun. It requires the professional to “think like an attacker”, and requires a particular mindset.