Lab - Using Banner Grabbing to Aid in Reconnaissance

Overview

In this lab, you will learn about banner grabbing. Banner grabbing is a technique used to gather information about running services on a computer system. Banners refer to the messages on the host that usually provide a greeting or version information. An attacker can use banner data to their advantage by obtaining specific version numbers of services to aid in reconnaissance and exploitation.

Lab Requirements

- One virtual install of Kali Linux
- One virtual install of Metasploirable2
- Both machines configured with NAT networking

Start the lab!

Make sure you do a network discovery on both your kali and your Metasploital2 to find your host IP addresses. You can use ifconfig on both machines to find their host IP addresses.

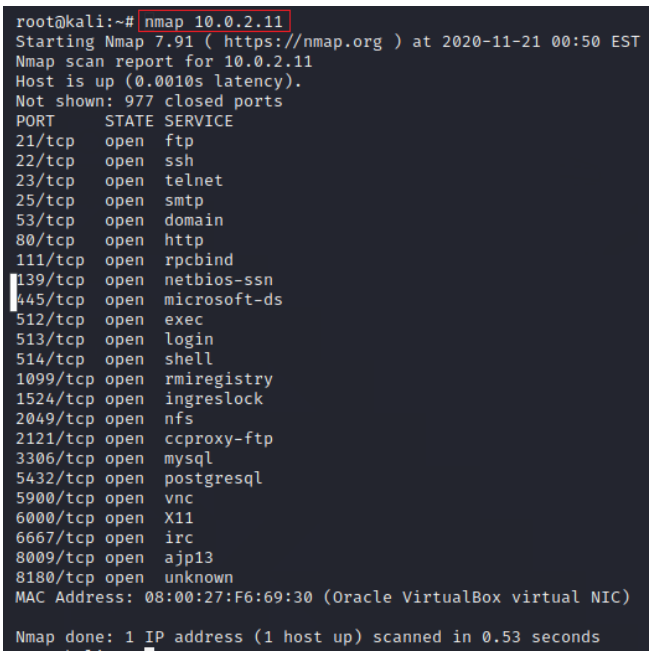
Let us begin by finding what services are currently running on our Metasploitable2 target.

Open a terminal on Kali, and at the prompt type, nmap followed by your target machine's IP address.

```
nmap 10.0.2.11
```

Press enter.

This is my IP address; yours will probably differ!



We now have a listing of all the services and ports available on our installation of Metasploitable2.

Telnet

The first tool we can use for banner grabbing is telnet.

If telnet is not installed by default, you can quickly install the tool using the following command.

`apt-get install telnet`

```
root@kali:~# apt-get install telnet
```

The first service we want to enumerate is the FTP service running on port 21.

At the prompt, I type **`telnet 10.0.2.11 21`**

Press enter.

```
root@kali:~# telnet 10.0.2.11 21
Trying 10.0.2.11 ...
Connected to 10.0.2.11.
Escape character is '^]'.
220 (vsFTPd 2.3.4)

quit
221 Goodbye.
Connection closed by foreign host.
root@kali:~#
```

We have FTP version vsFTPd 2.3.4 running on our remote target.

We can do the same for SSH. Use your up arrow to bring back your previous telnet command. Change port 21 to port 22.

`telnet 10.0.2.11 22`

```
root@kali:~# telnet 10.0.2.11 22
Trying 10.0.2.11 ...
Connected to 10.0.2.11.
Escape character is '^]'.
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
quit
Protocol mismatch.
Connection closed by foreign host.
root@kali:~#
```

And we now have the version number for SSH running on our remote target.

We can use the same procedure to banner grab some information about the HTTP service that is running on our remote target on port 80.

`telnet 10.0.2.11 80`

Once you are connected, type in help and press enter.

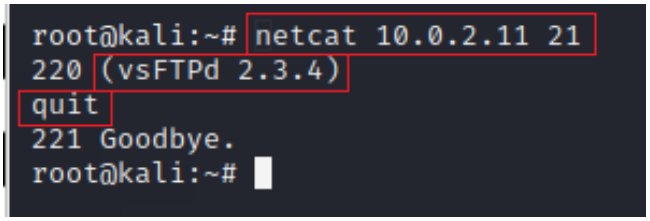
NetCat

We can also use netcat to perform banner grabbing. Netcat is a utility that is commonly found on Linux. We can use netcat to connect to specific ports and gather information.

Just as we did with telnet, we can use netcat to do the same.

At the prompt, type: **`netcat 10.0.2.11 21`**

Press enter.



Type quit to exit.

Again, using netcat to enumerate SSH.

```
root@kali:~# netcat 10.0.2.11 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
quit
Protocol mismatch.
root@kali:~#
```

And again, with HTTP. As we did with telnet, to get any information about HTPP, we need to type in help at the prompt.

```
root@kali:~# netcat 10.0.2.11 80
help
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>

root@kali:~#
```

We can also utilize Netcat to communicate with the webserver. For example, we can use the **HEAD** method to get the header information about the server:

At the prompt, type **`HEAD / HTTP/1.1`**

```
root@kali:~# netcat 10.0.2.11 80

HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Thu, 29 Oct 2020 16:24:11 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Connection: close
Content-Type: text/html; charset=iso-8859-1

root@kali:~#
```

Even though it was a bad request, we still got the exact version number of Apache.

We next send a GET request, which will return the contents of the webpage:

`GET / HTTP/1.1`

```
root@kali:~# netcat 10.0.2.11 80

GET / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Thu, 29 Oct 2020 16:27:48 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Length: 323
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.localdomain Port 80</address>
</body></html>
root@kali:~#
```

Whatweb

“WhatWeb” recognizes websites, which helps us to grab the web-applications banner by disclosing the server information with its version, the IP address, the webpage Title, and running operating system.

Type the following command at your terminal prompt.

`whatweb http://10.0.2.11`

```
root@kali:~# whatweb http://10.0.2.11
http://10.0.2.11 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[U
buntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[10.0.2.11], PHP[5.2.4-2ubuntu5
.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubu
ntu5.10]
root@kali:~#
```

cURL

The cURL command includes the functionality for retrieving the banner details from HTTP servers.

`curl 10.0.2.11`

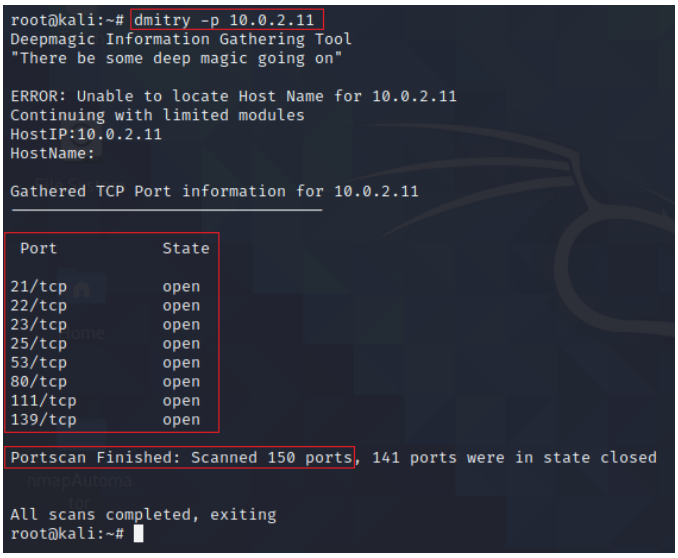
```
root@kali:~# curl 10.0.2.11
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>

root@kali:~#
```

Dmitry

Dmitry is a streamlined yet straightforward tool that can be used to connect to network services running on remote ports.

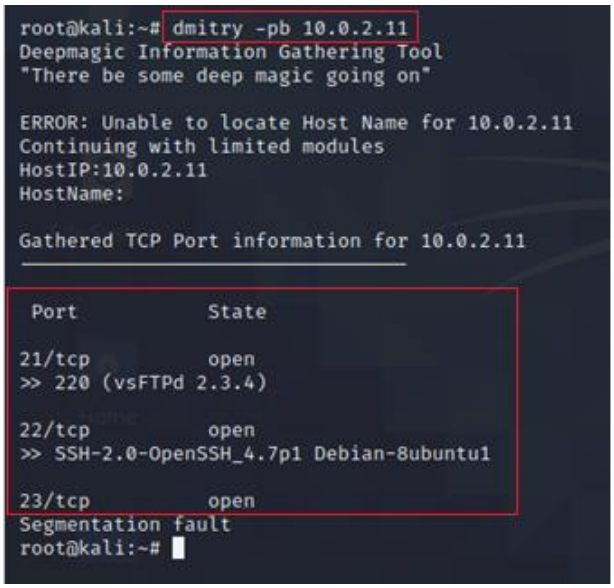
Dmitry can be used to run a quick TCP port scan on 150 of the most used services. This can be done using the -p option:

`dmitry -p 10.0.2.11`



By adding the b switch, we can enumerate some of the services running on our metasploitable2 target and see what version of the program is running on the server.

`dmitry -pb 10.0.2.11`



Summary –

Banner grabbing is one of the easiest and most common recon techniques. There are many tools and scripts that allow you to get this information. We covered the essential Linux/UNIX utilities like the wget, nc, and telnet. However, there are also specialized infosec utilities like Dmitry and ASR. Telnet is by far the easiest to use and almost always readily available.