Hack The Box
PEN-TESTING LABS

Shrek

19th October 2017 / Document No D17.100.28

Prepared By: Alexander Reid (Arrexel)

Machine Author: SirenCeol & Cowonaboat

Difficulty: Hard

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Shrek, while not the most realistic machine, touches on many different subjects and is definitely one of the more challenging machines on Hack The Box. This machine features several fairly uncommon topics and requires a fair bit of research to complete.

Skills Required

- Intermediate/advanced knowledge of Linux
- Intermediate understanding of cryptography

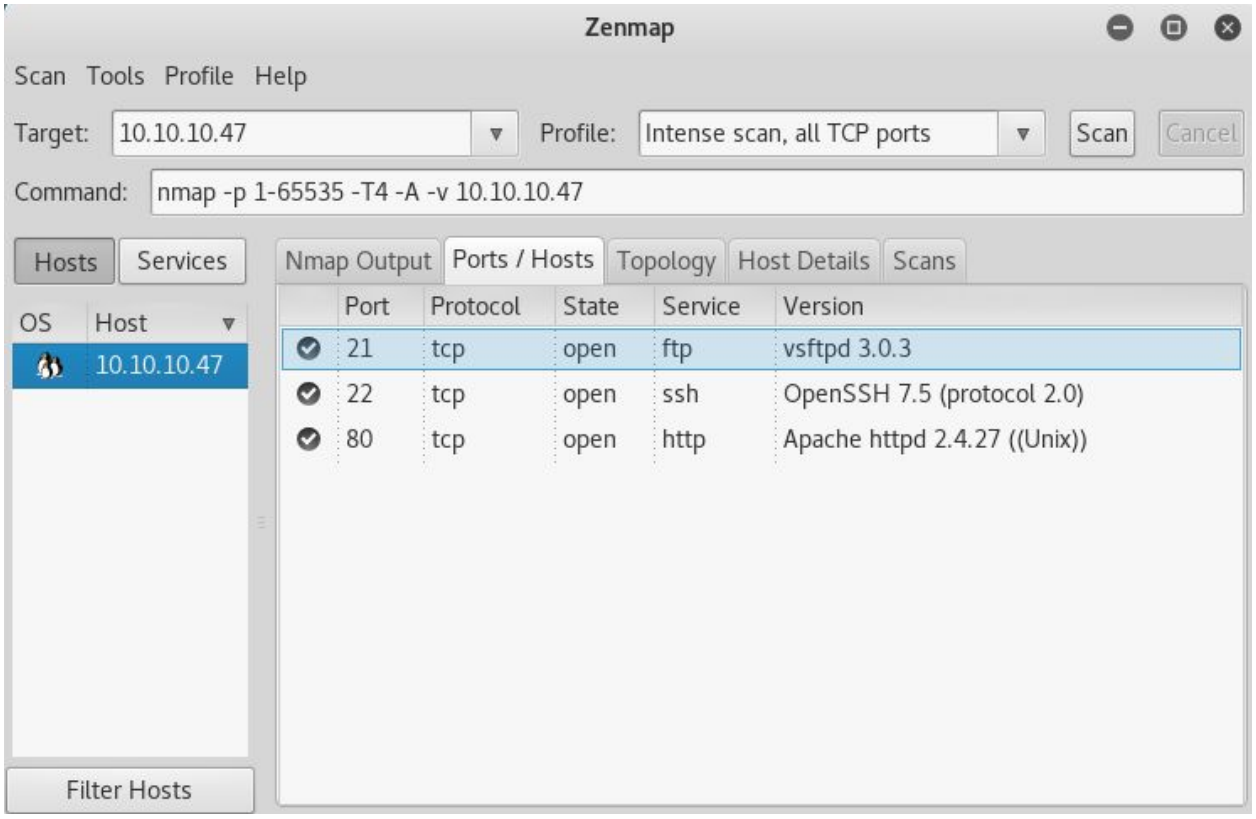
Skills Learned

- Spectrogram analysis
- Recognizing and decrypting elliptic curve cryptography
- Enumerating hidden tasks
- Exploiting chown wildcards

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

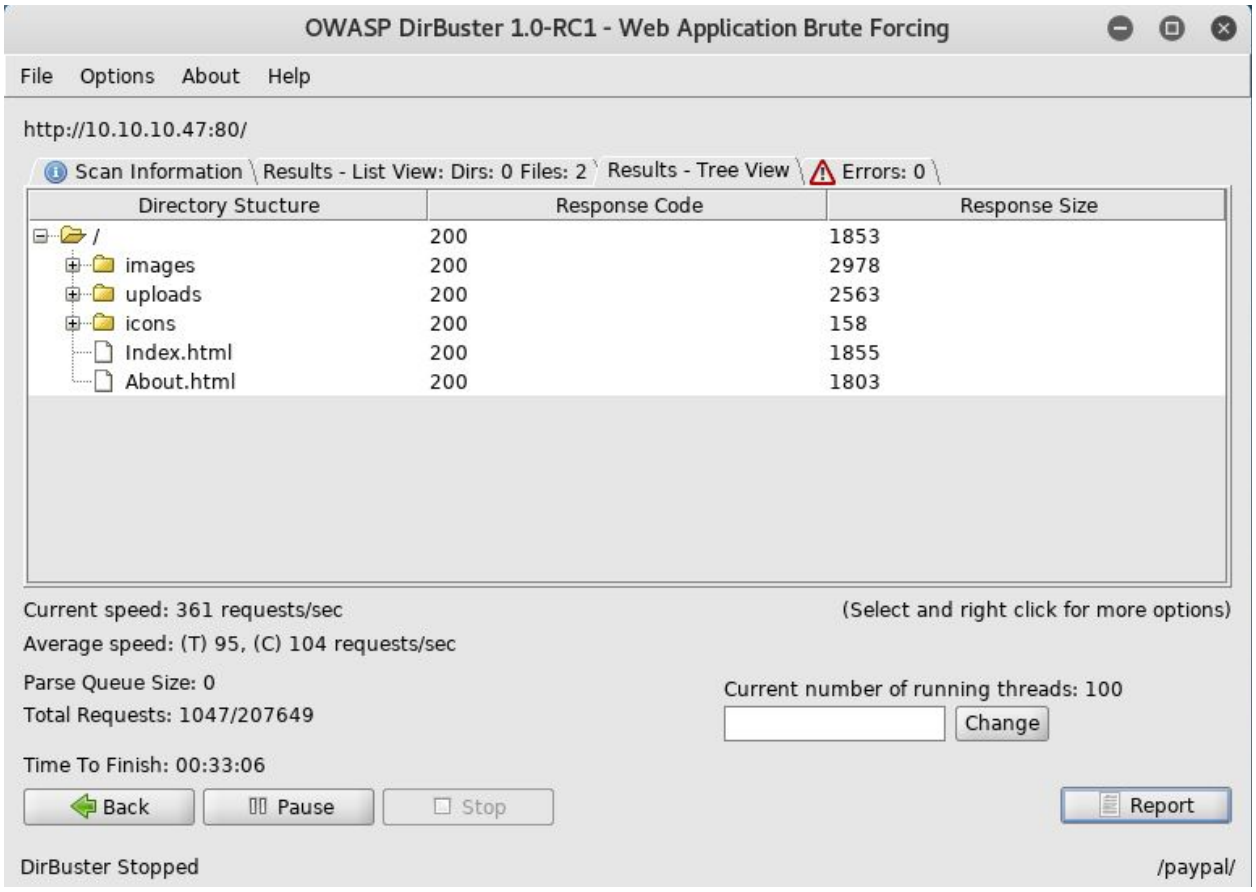
Enumeration

Nmap



Nmap reveals a vsftp server, OpenSSH and Apache.

Dirbuster



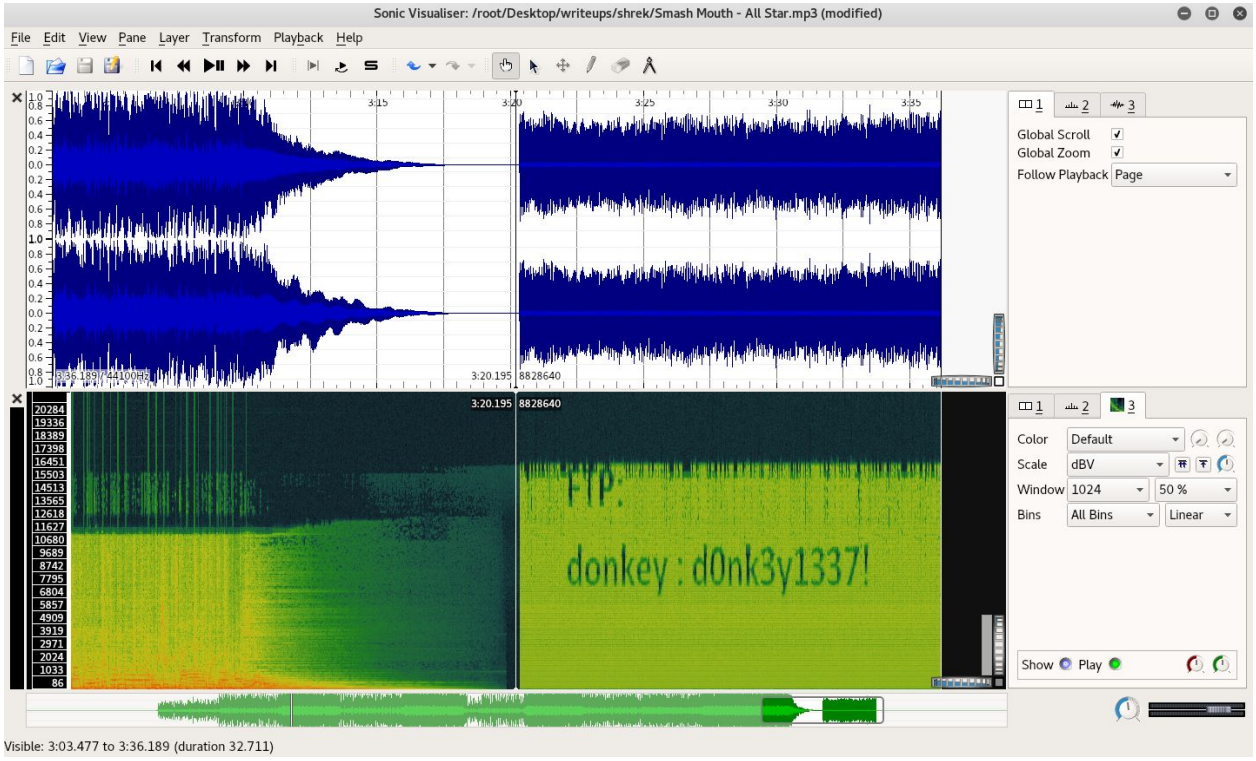
Running Dirbuster reveals an /**uploads/** folder that contains a file named **secret_ultimate.php**. Viewing the file in-browser does not reveal any useful information, but if it is downloaded with **wget**, it reveals another directory named **/secret_area_51/**

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation

Steganography

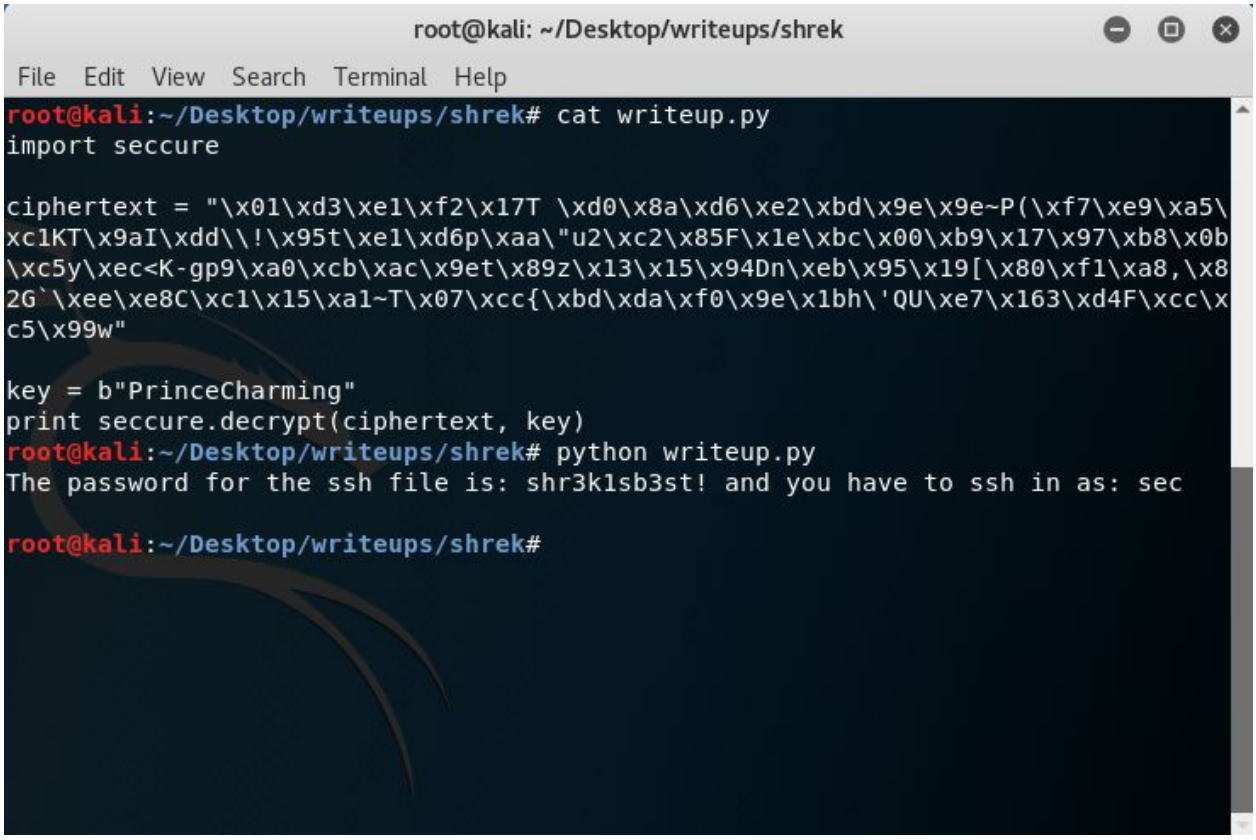
Using **Sonic Visualiser** (apt-get install sonic-visualiser) on the mp3 file and viewing the spectrogram (**Pane > Add Spectrogram**) reveals some FTP credentials.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Elliptic Curve Cryptography

In two of the txt files found on the FTP server, there are Base64 strings. Note that the filenames change every time the machine is reset. Decoding the strings reveals some ciphertext and the string **PrinceCharming**. Using the **seccure** Python library, it is possible to decrypt the ciphertext using **PrinceCharming** as the key.



There is a **key** file that can be found on the FTP server. Using the above credentials, it is possible to SSH in.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

Exploit: https://www.defensecode.com/public/DefenseCode_Unix_WildCards_Gone_Wild.txt

Depending on the escalation enumeration script used, the correct attack vector may be fairly challenging to locate.

The **/usr/src** folder is writeable for the **sec** user and contains a **thoughts.txt** file owned by root. Attempting to create a file will reveal (after a bit of a delay) that there is a scheduled task which runs **chown** * in the directory. Using the above exploit, it is possible to force chown to use a reference file and apply the owner:group of that file to everything in the directory. The command **touch -- --reference=thoughts.txt** will create a file, with the name being passed as an argument to chown when it runs.

After that is configured, it is possible to create a binary and set its SUID bit. After the task runs and chowns the binary, it is possible to execute code as root.

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

int main()
{
    setuid(0);
    system("cat /root/root.txt > /usr/writeup.flag.txt");
    return 0;
}
```

```
[sec@shrek src]$ ls -la
total 24
drwxr-xr-x 2 sec  root  4096 Oct 22 07:01  .
drwxr-xr-x 8 sec  root  4096 Oct 22 06:59  ..
-rw-r--r-- 1 sec  users    0 Oct 22 05:44 '--reference=thoughts.txt'
-rw-r--r-- 1 root root    91 Aug 22 00:51  thoughts.txt
-rwsrwsrwx 1 root root  8504 Oct 22 06:59  writeup
[sec@shrek src]$
```