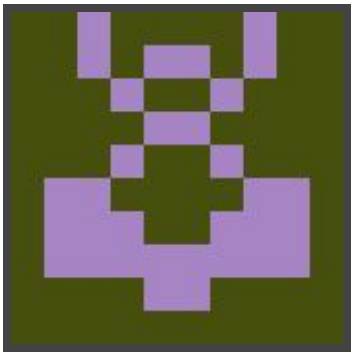
Hack The Box
PEN-TESTING LABS



Brainfuck

17th October 2017 / Document No D17.100.24

Prepared By: Alexander Reid (Arrexel)
Machine Author: ch4p
Difficulty: Hard
Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

SYNOPSIS

Brainfuck, while not having any one step that is too difficult, requires many different steps and exploits to complete. A wide range of services, vulnerabilities and techniques are touched on, making this machine a great learning experience for many.

Skills Required

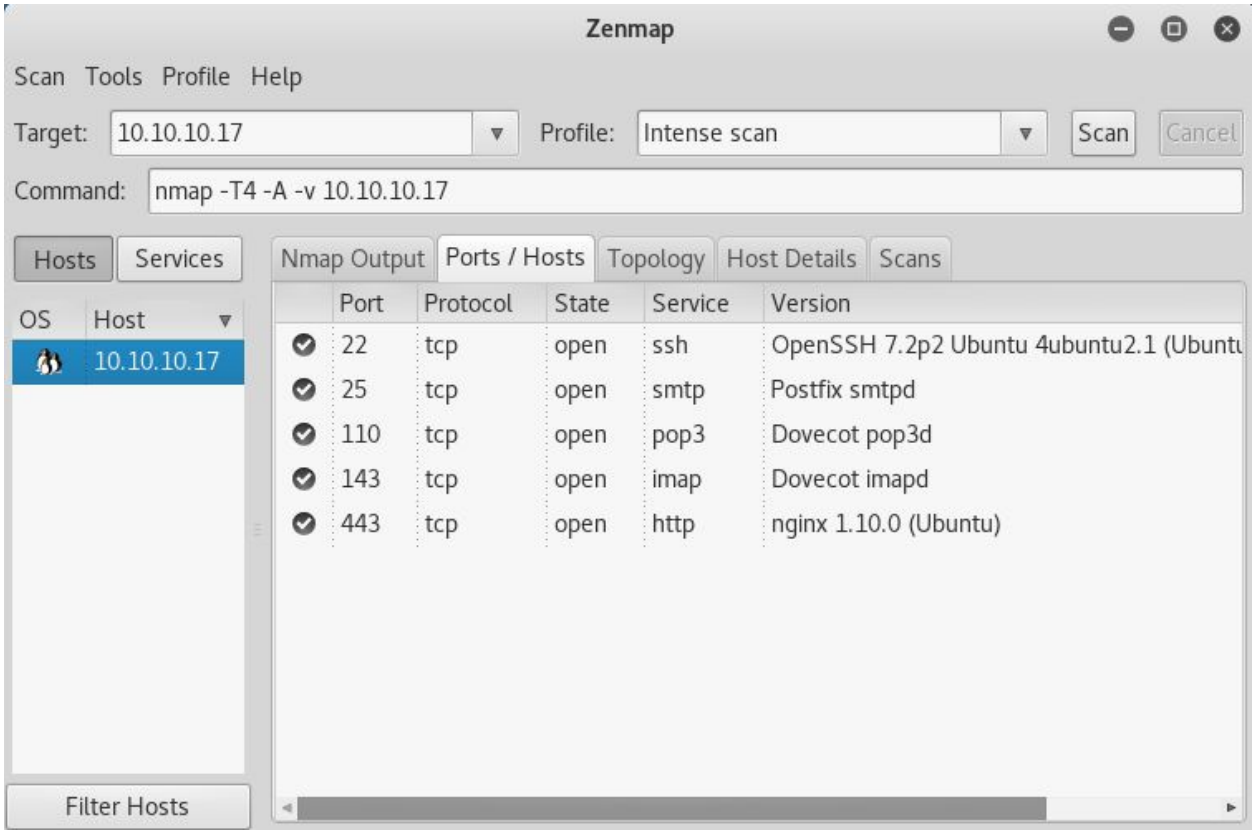
- Intermediate knowledge of Linux
- Basic understanding of RSA cryptography

Skills Learned

- Enumerating SSL certificates
- Exploiting Wordpress
- Exploit modification
- Enumerating mail servers
- Decoding Vigenere ciphers
- SSH key brute forcing
- RSA decryption techniques

Enumeration

Nmap

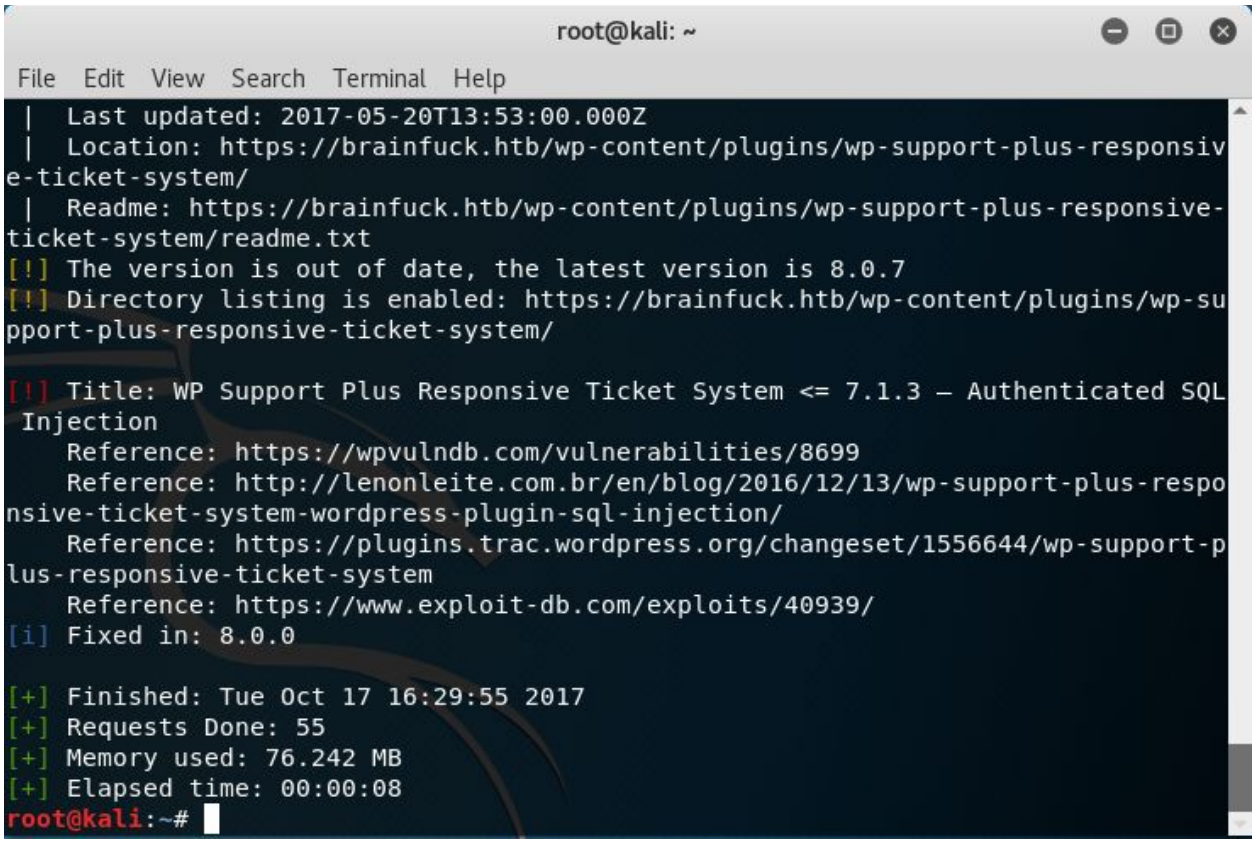



```
| ssl-cert: Subject: commonName=brainfuck.htb/
organizationName=Brainfuck Ltd./stateOrProvinceName=Attica/
countryName=GR
| Subject Alternative Name: DNS:www.brainfuck.htb,
DNS:sup3rs3cr3t.brainfuck.htb
| Issuer: commonName=brainfuck.htb/organizationName=Brainfuck
Ltd./stateOrProvinceName=Attica/countryName=GR
```

Nmap reveals several open services as well as several hostnames that were enumerated through the SSL certificate. Adding the hostnames to **/etc/hosts** is required to view the sites.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

WPScan



WPScan finds an authenticates SQL injection vulnerability, however the results overall do not find anything of much use. Searching Exploit-DB for more exploits related to the ticket system yields https://www.exploit-db.com/exploits/41006/

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Exploitation

Wordpress

Gaining access to the Wordpress admin account is trivial using the above exploit. All that is required is setting the target URL and user. The username, **admin**, can be easily guessed and it is the default username when installing Wordpress. After running the exploit, the admin panel can be accessed at **/wp-admin/**

After gaining access, some credentials can be found on the **Settings > Easy WP SMTP** page. The password can be extracted simply by viewing the page source.

Mail Server

Using the credentials obtained from wordpress, it is trivial to extract the emails from the server. Any IMAP-capable mail client or even Telnet can be used here. The example below will use Telnet.

1. telnet brainfuck.htb 143
2. a1 LOGIN orestis kHGuERB29DNiNE
3. a2 LIST "" "*"
4. a3 EXAMINE INBOX
5. a4 FETCH 1 BODY[]
6. a5 FETCH 2 BODY[]

The second email exposes credentials that can be used to log in at **sup3rs3cr3t.brainfuck.htb**

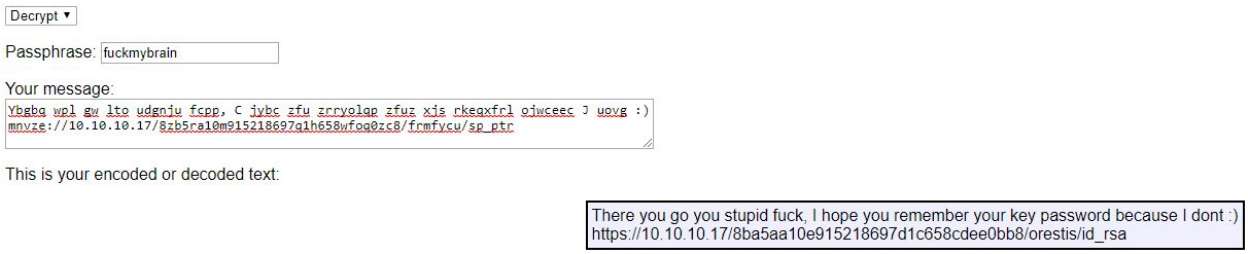
Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Forums

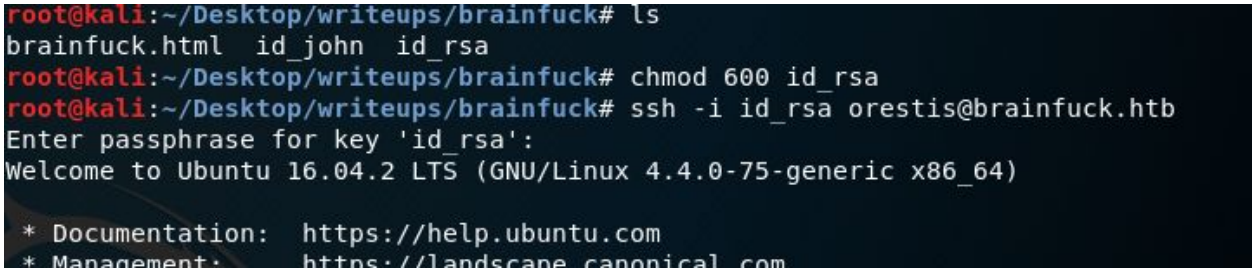
Tool: http://rumkin.com/tools/cipher/vigenere.php

Looking at the **Key** discussion, it appears that the post is encrypted. In this case, the cipher used is basic Vigenere. By comparing the last line of text in each of orestis' posts to the posts in the **SSH Access** discussion, it is possible to extract the key.

After a bit of playing around with the output, the key appears to be **fuckmybrain**. Using that, it is possible to decrypt the posts.



The RSA key has a passphrase that must be cracked. This can be achieved by running **ssh2john id_rsa > id_john** and then **john id_john --wordlist=<PATH TO ROCKYOU.TXT>**



The user flag can be obtained from **/home/orestis/user.txt**

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

RSA Decryption

Script: https://crypto.stackexchange.com/a/19530

Looking at the contents of the files in the **/home/orestis** directory, specifically **encrypt.sage**, it appears that the file **output.txt** contains an encrypted root flag and the file **debug.txt** contains the P, Q and E values used to do the encryption. By using the above Python script, it is possible to decrypt the ciphertext and get the root flag.

```
root@kali:~/Desktop/writeups/brainfuck# python rsa.py
n:  873061943450542420269524339311087529982483791600518349571160587159970422697829509624135727770919760163726737095730026723557679458891077938400356544917133668554739877161801869664740465726670553685912522743622820226974780988443888583759932176299727684945739700654800982460836544662623257092201816561014915197 7
pt: 24604052029401386049980296953784287079059245867880966944246662849341507003750
root@kali:~/Desktop/writeups/brainfuck#
```

To convert the plaintext result from decimal to ASCII, the following command can be used:
python -c "print format(<DECIMAL NUMBER>, 'x').decode('hex')"

The output of the command is the hash value from **root.txt**.

```
root@kali: ~/Desktop/writeups/brainfuck
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop/writeups/brainfuck# python -c "print format(2460405202940138604998029695378428707905924586788096694424666284934150700375 0, 'x').decode('hex')"
6efc1a5dbb8904751ce6566a305bb8ef
root@kali:~/Desktop/writeups/brainfuck#
```