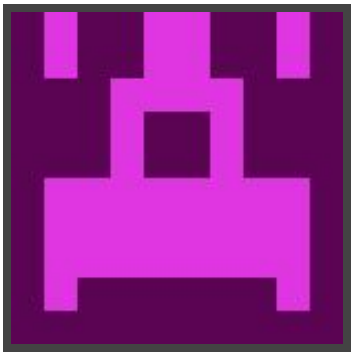
Hack The Box
PEN-TESTING LABS



Lazy

5th October 2017 / Document No D17.100.06

Prepared By: Alexander Reid (Arrexel)

Machine Author: trickster0

Difficulty: Medium

Classification: Official

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

SYNOPSIS

Lazy mainly focuses on the use of padding oracle attacks, however there are several unintended workarounds that are relatively easier, and many users miss the intended attack vector. Lazy also touches on basic exploitation of SUID binaries and using environment variables to aid in privilege escalation.

Skills Required

- Basic understanding of cryptography
- Basic/intermediate knowledge of Linux

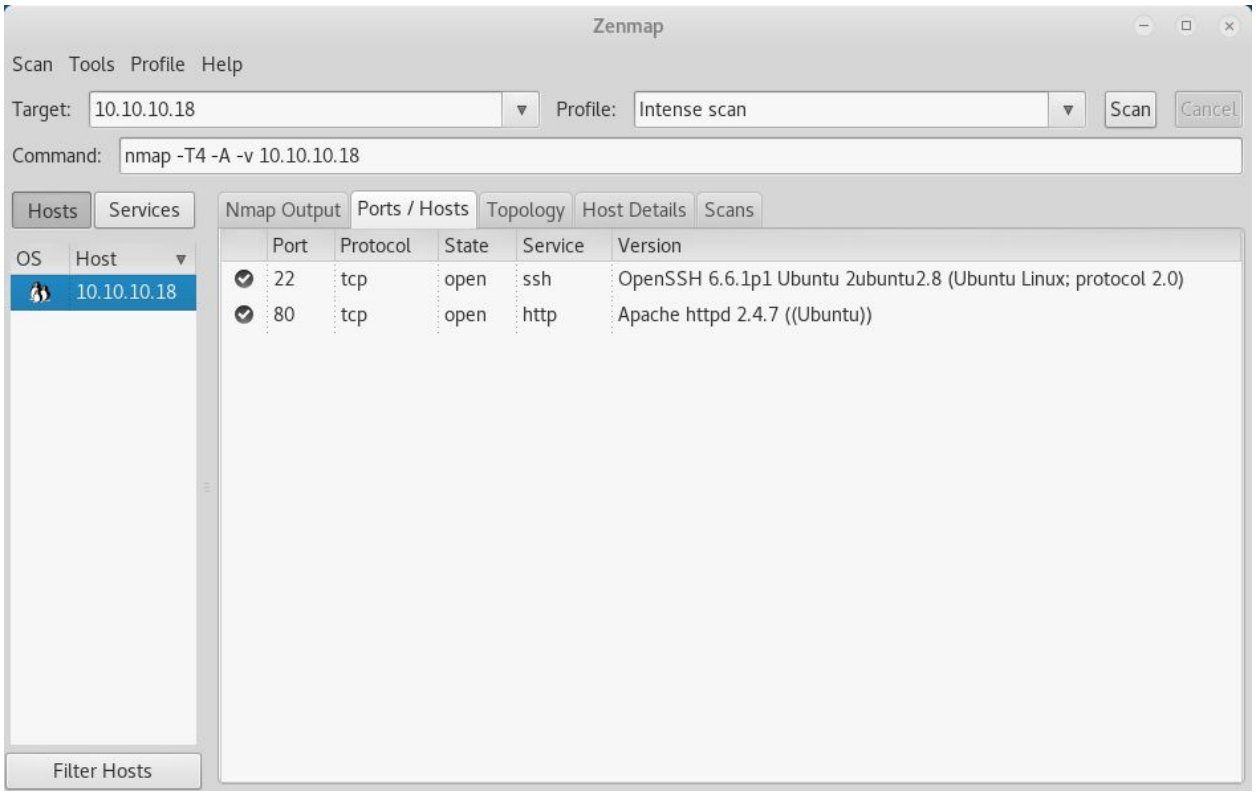
Skills Learned

- Padding Oracle Attack
- Exploiting SUID binaries
- Using the PATH environment variable to aid in exploitation

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

Enumeration

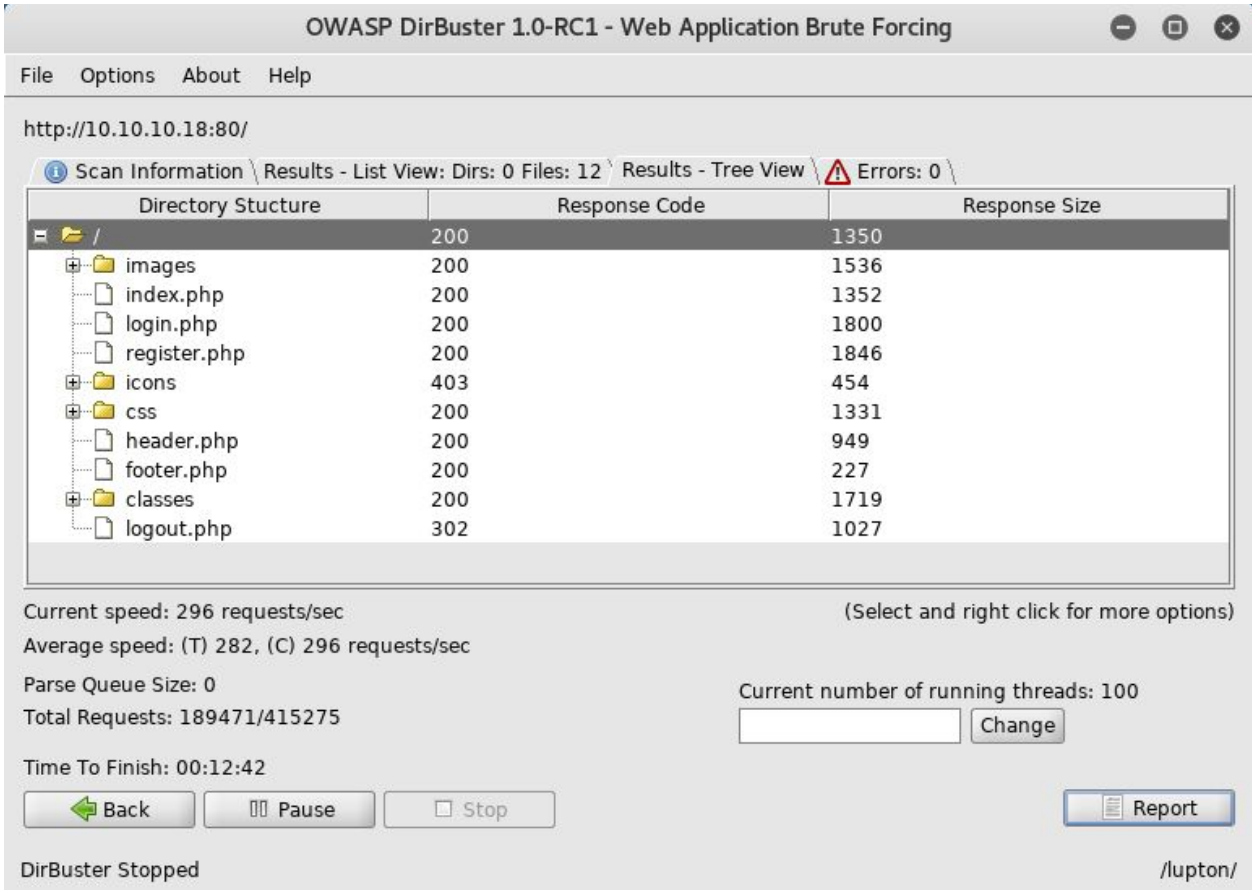
Nmap



Nmap shows only two open services; OpenSSH and an Apache server. Some web fuzzing is required in this case to find an attack surface.

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

Dirbuster



There are a few PHP files, and they all seem to be a part of the same application. The best place to start appears to be the login and register pages, as the other files provide no useful functionality or information when viewed.

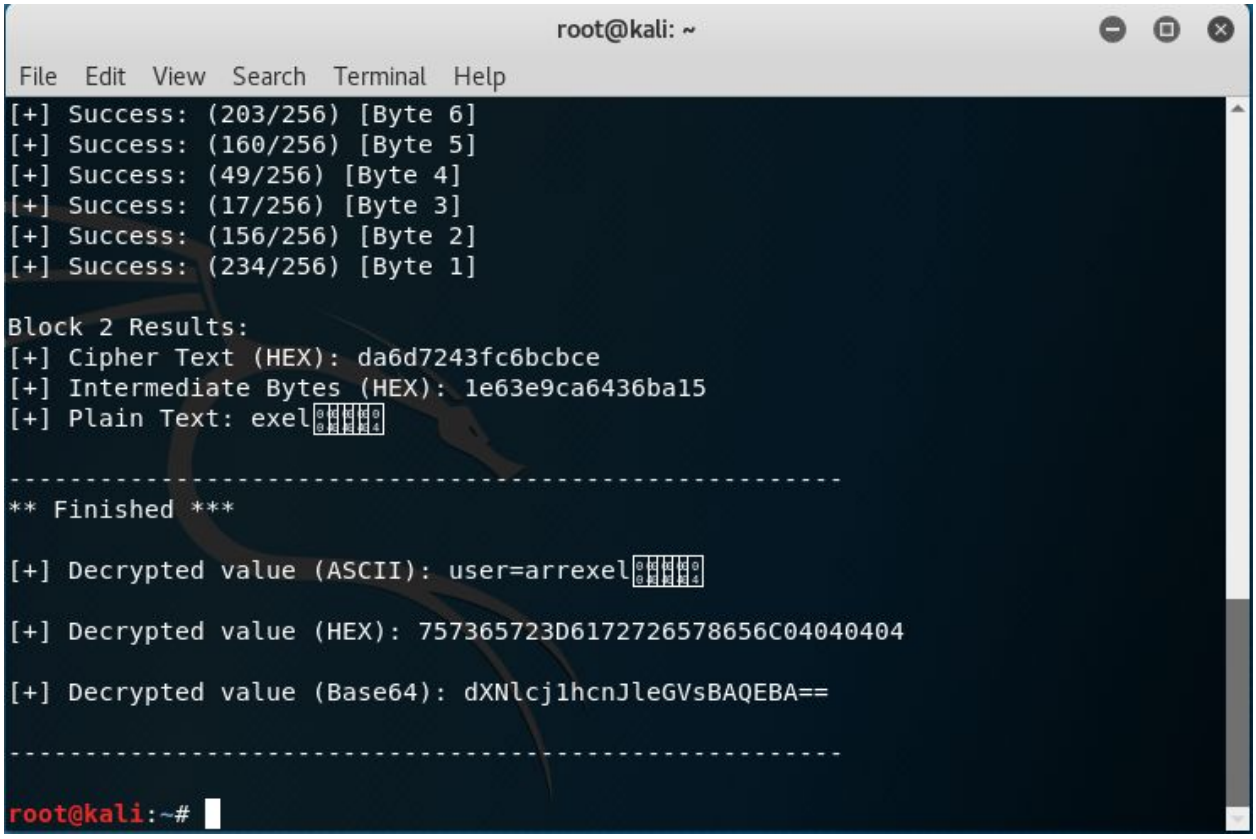
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation

Padding Oracle Attack - Decrypt

Attempting to register as the user **admin** shows that the account already exists. After testing for SQL injection and other typical user-supplied input vulnerabilities, the login form and registration pages do not appear to be vulnerable. However, there is one more attack surface; cookies. The only cookie created by the server is the **auth** cookie, which appears as **auth=2zKLNWhe0Xt7G4ymYDK%2BEdptckP8a8vO**

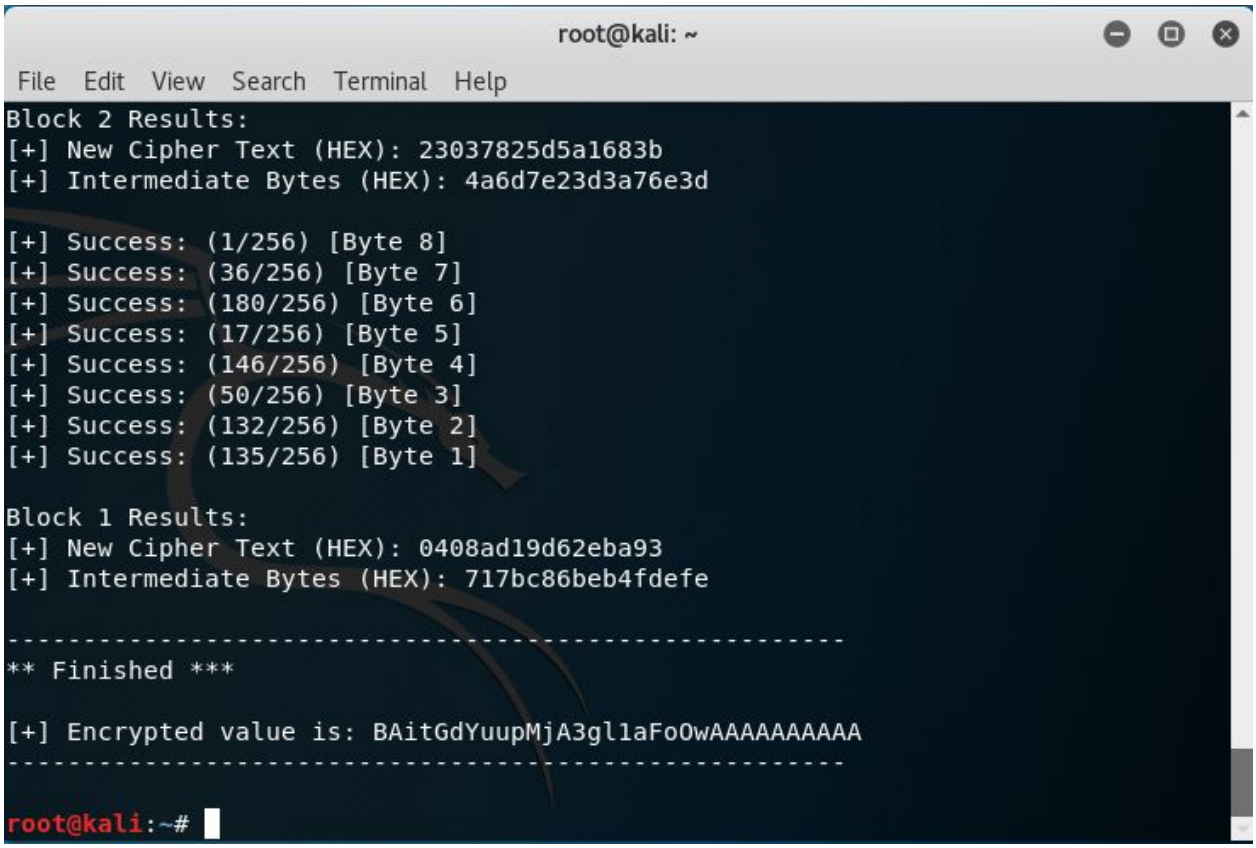
Running a padding oracle attack against the target with padbuster reveals the target is indeed vulnerable. The output reveals the username, which is stored client-side. This can be easily exploited. Command: **padbuster http://10.10.10.18 2zKLNWhe0Xt7G4ymYDK%2BEdptckP8a8vO 8 -cookies auth=2zKLNWhe0Xt7G4ymYDK%2BEdptckP8a8vO -encoding 0**



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

Padding Oracle Attack - Encrypt

Knowing that a padding oracle attack can be used against this target, it is possible to encrypt user supplied data with the same method. In this case, encrypting **user=admin** will produce a valid **auth** cookie. Command: **padbuster http://10.10.10.18 2zKLNWhe0Xt7G4ymYDK%2BEdptckP8a8vO 8 -cookies auth=2zKLNWhe0Xt7G4ymYDK%2BEdptckP8a8vO -encoding 0 -plaintext user=admin**



Upon modifying the cookie with the new data and reloading the page, some additional content is presented. Most notably a link to an SSH key. The filename indicates the user is **mitsos**.

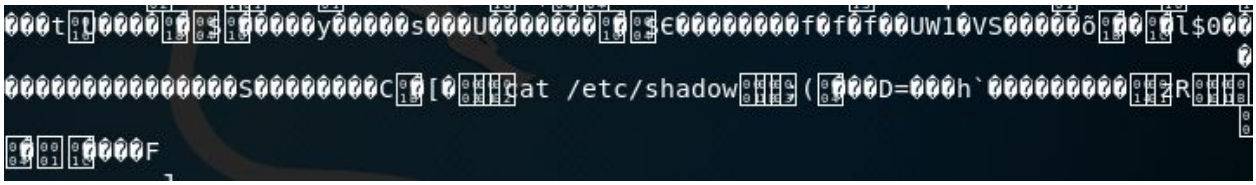
Tasos this is my ssh key, just in case, if you ever want to login and check something out.

My Key

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

Privilege Escalation

After gaining entry to the target via SSH (and grabbing the user flag at **/home/mitsos/user.txt**), the next step is to observe the **backup** binary available in the user's home directory. A quick glimpse shows that it has sticky bits set, which will run it as the root user. Running **strings** against the binary shows that it executes the command **cat /etc/shadow**



Because a full path to the cat binary is not specified, this specific command is vulnerable to hijacking by modifying the **PATH** system variable. This can be achieved by setting the working directory as the first option in PATH, with the command **export PATH=.:$PATH**

After this, creating a file named **cat** in the working directory will cause the file to be executed by the root user. In this case, a bash script will do the trick. Note, do not use the **cat** command in the script as this will cause the script to loop endlessly. Don't forget to **chmod +x ./cat** before running the backup binary. The script below creates a copy of the root flag in the home directory.