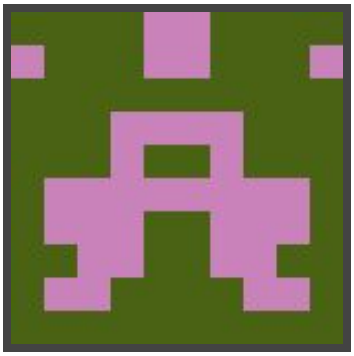
Hack The Box
PEN-TESTING LABS



Nineveh

8th October 2017 / Document No D17.100.11

Prepared By: Alexander Reid (Arrexel)
Machine Author: Yas3r
Difficulty: Medium
Classification: Official

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

SYNOPSIS

Nineveh is not overly challenging, however several exploits must be chained to gain initial access. Several uncommon services are running on the machine, and some research is required to enumerate them.

Skills Required

- Intermediate knowledge of Linux
- Enumerating ports and services

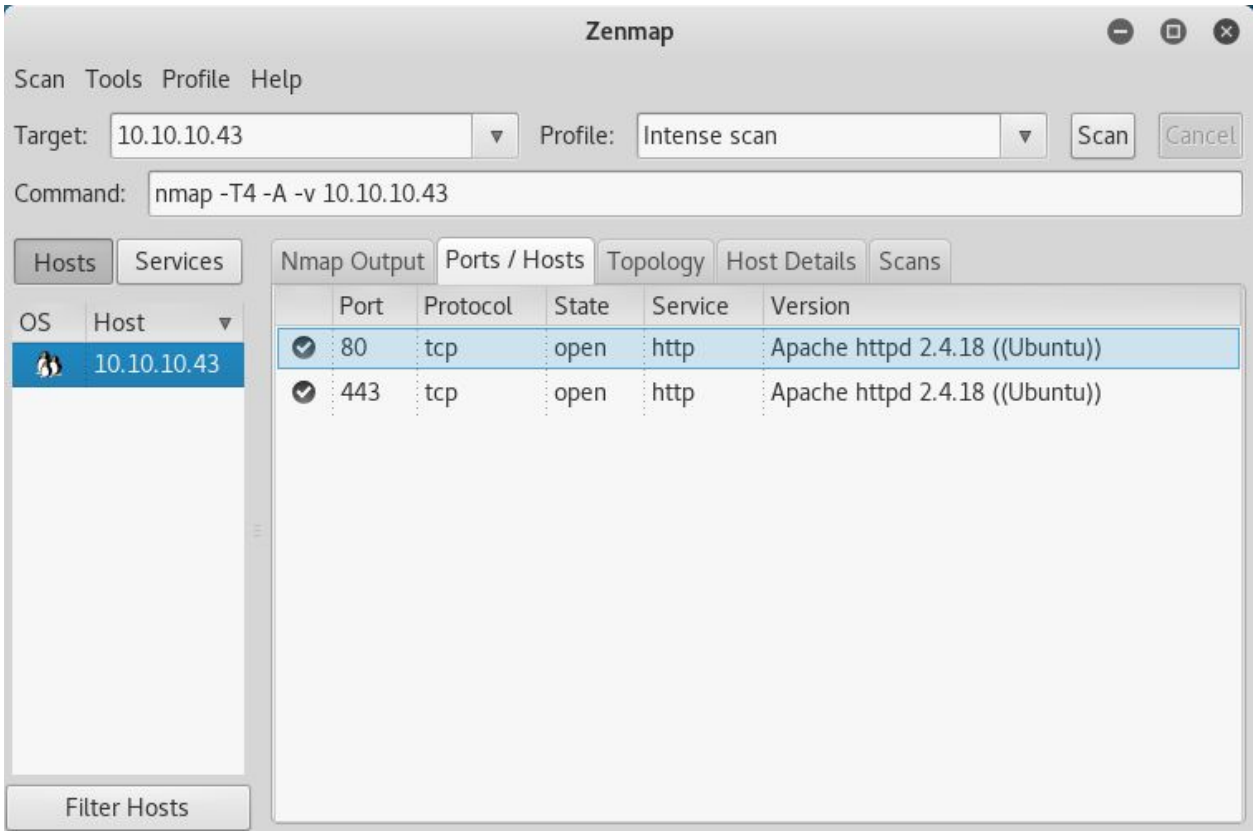
Skills Learned

- HTTP-based brute forcing
- Chaining exploits
- Local file inclusion
- Port knocking

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

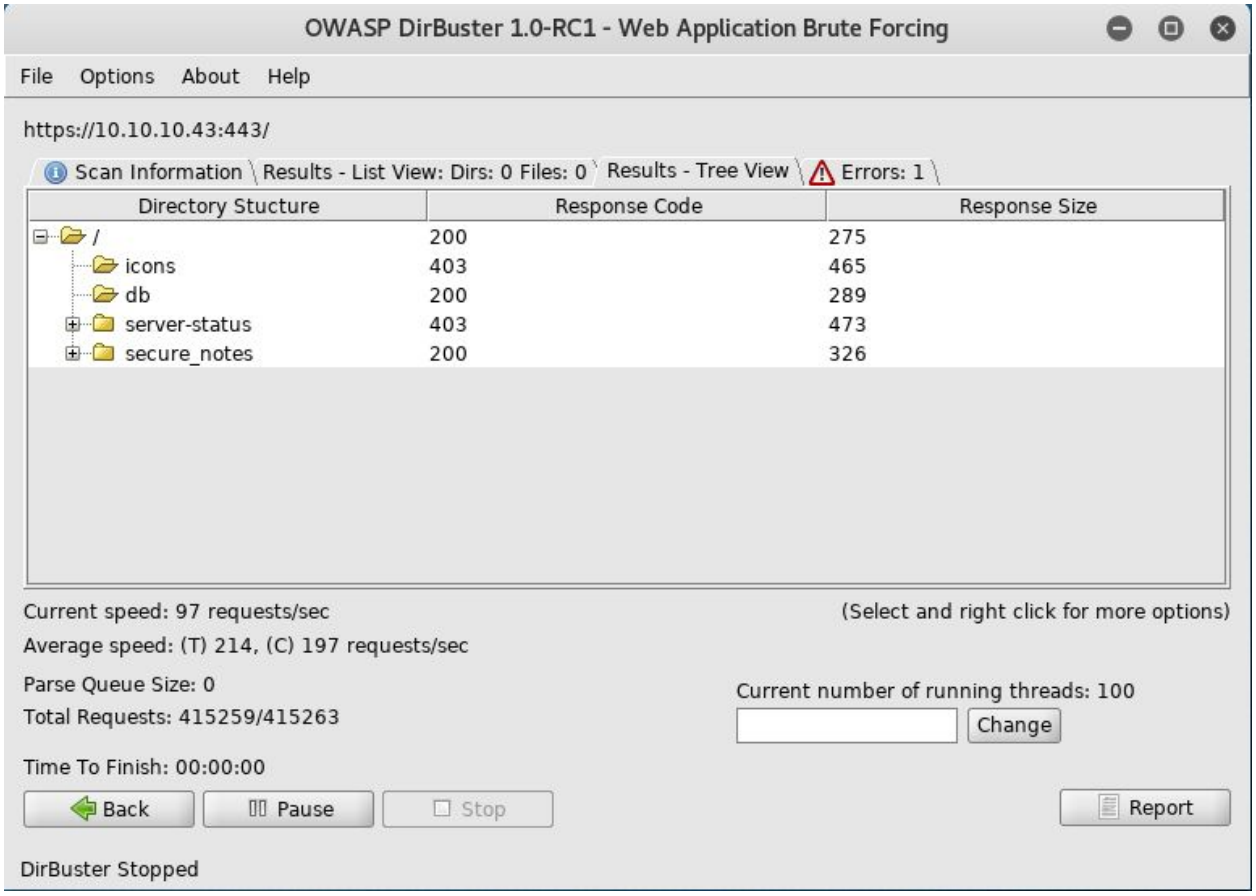
Enumeration

Nmap



Nmap only reveals an Apache server running on ports 80 and 443.

Dirbuster



Dirbuster, with the dirbuster lowercase medium wordlist, reveals two folders of importance; **db** and **secure_notes**. The **db** directory hosts a copy of phpLiteAdmin v1.9 and **secure_notes** only contains a single image. Running Dirbuster against port 80 reveals another directory, **department**, which contains a login page.

Directory Stucture	Response Code	Response Size
/	200	432
info.php	200	179
icons	403	464
department	200	217

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

Exploitation

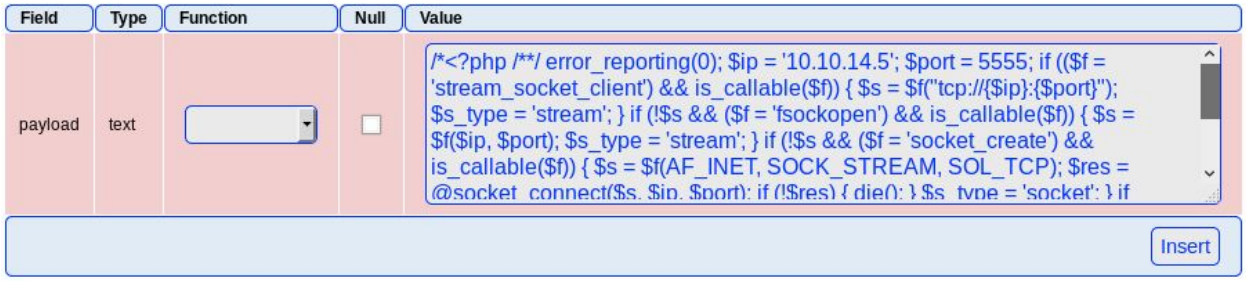
phpLiteAdmin

Exploit: https://www.exploit-db.com/exploits/24044/

A bit of searching turns up a remote code execution vulnerability in phpLiteAdmin, however it requires authentication. Running Hydra against the login with the rockyou.txt wordlist is successful.

Command: hydra -l none -P rockyou.txt 10.10.10.43 https-post-form "/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password" -t 64 -V

Using the exploit described in **exploit-db 24044** is trivial. Simply creating a database named **ninevehNotes.txt.writeup.php** (view next section for more information), adding a table, then inserting a table entry with the PHP payload is all that is required.



It is a bit more challenging to execute the created file as it is not saved in the main website directory. Viewing the **Rename Database** page reveals the full path, which is **/var/tmp/**

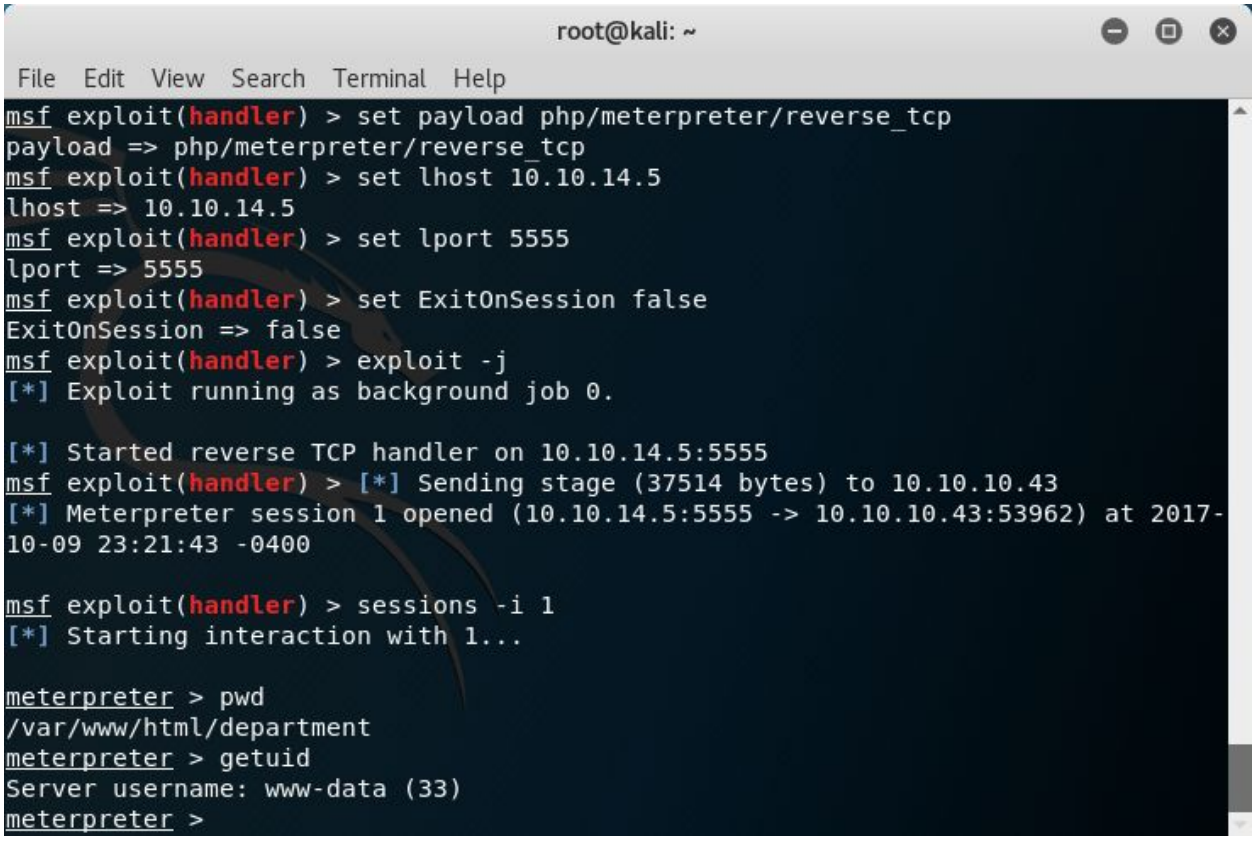
Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Department

Attempting to log in with invalid credentials shows an error message specifying incorrect username. Because of this, it is possible to enumerate a valid user (by fuzzing, or just trying the obvious). In this case the valid username is **admin**. Running Hydra against the login, while targeting the admin user, successfully discovers the password.

Command: hydra -l none -P rockyou.txt 10.10.10.43 http-post-form "/department/login.php:username=admin&password=^PASS^:Invalid Password" -t 64 -V

Browsing to the **Notes** page, it is clear quite quickly that there is a local file inclusion vulnerability. After a bit of trial and error, it appears it will only include a file that contains **ninevehNotes.txt** in the name. By naming the database **ninevehNotes.txt.writeup.php**, it is possible to bypass this restriction. Execute the PHP payload by browsing to **/department/manage.php?notes=/var/tmp/ninevehNotes.txt.writeup.php**

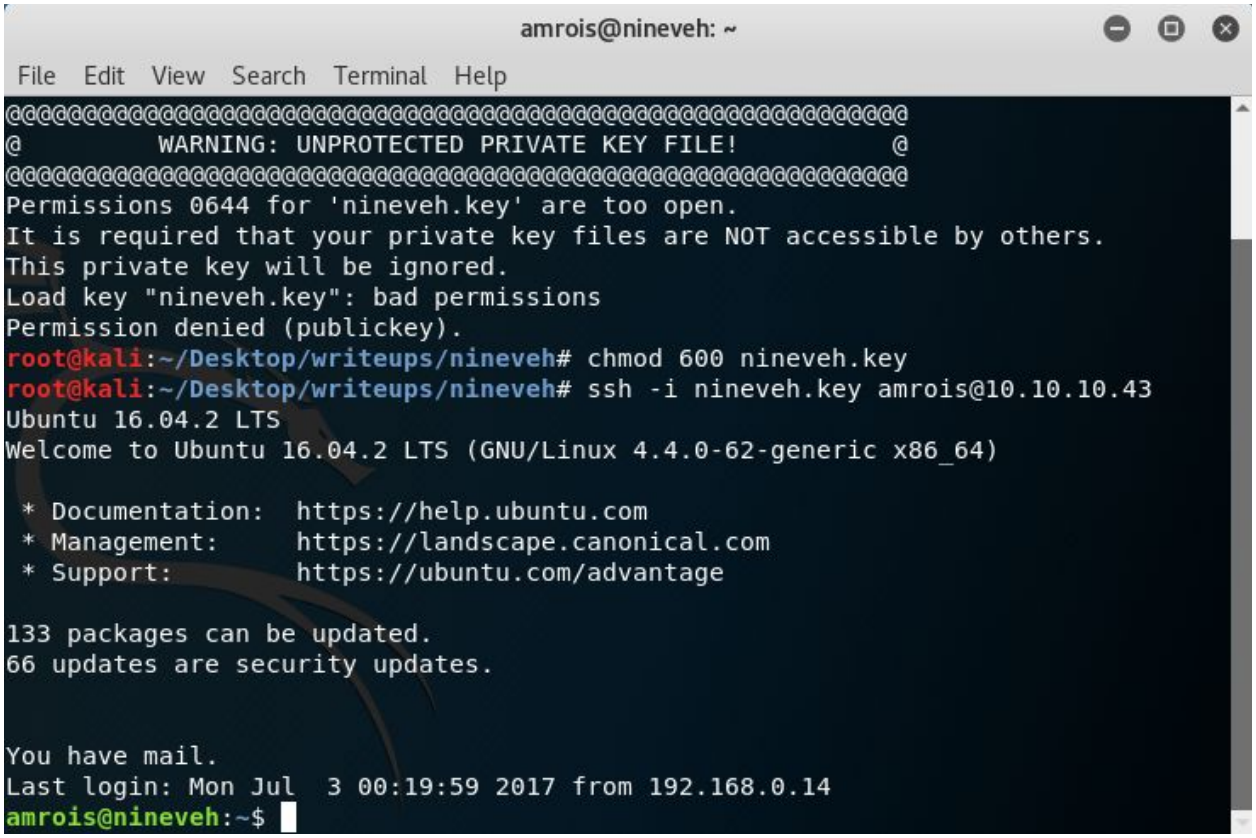


Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

SSH

The **secure_notes** directory found earlier now comes into play. By running **strings** against the image file, both a public and private key are exposed. However, from the port scan, it appears there is no SSH server running.

After a bit of searching around, it appears the machine is running **knockd**, which is a port knock listener. Viewing the configuration file at **/etc/knockd.conf** reveals the correct knock code to open the SSH port. It can be opened by running the command **for x in 571 290 911; do nmap -Pn --host_timeout 201 --max-retries 0 -p $x 10.10.10.43; done** in terminal. Afterwards, SSH into the machine as the **amrois** user and grab the user flag from **/home/amrois/user.txt**



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

Privilege Escalation

LinEnum: https://github.com/rebootuser/LinEnum

Running LinEnum locates a bash script at **/usr/sbin/report-reset.sh**. The script removes files in the **/reports/** directory. Reviewing a report file and searching some of the static strings reveals that it was created by **chkrootkit**. Searching for chkrootkit vulnerabilities finds **exploit-db 33899**. The file **/tmp/update** is executed by ckhrootkit as root. As this file does not currently exist, it is possible to put a bash script in its place and use it to extract the root flag.

Exploit: https://www.exploit-db.com/exploits/33899/