Hackviser File Hunter Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki File Hunter isimli Isınmayı çözeceğiz

Başlangıçta bize FTP hakkında bilgi vermiş

FTP (File Transfer Protocol), dosya aktarımlarını internet üzerinden yapmak için kullanılan bir protokoldür. Bu protokol, bir bilgisayarın dosyalarını diğer bir bilgisayara yüklemek veya indirmek için kullanılır.

Bizden toplamda 7 sorunun cevabını istiyor sırasıyla:

- Hangi port(lar) açık?
- FTP'nin açılımı nedir?
- FTP'ye hangi kullanıcı adı ile bağlandınız?
- Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?
- FTP sunucusundaki dosyanın adı nedir?
- *Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?*
- *Dosyada hangi kullanıcıların bilgileri vardır?,*

Öncelikle tarama ile başlayalım

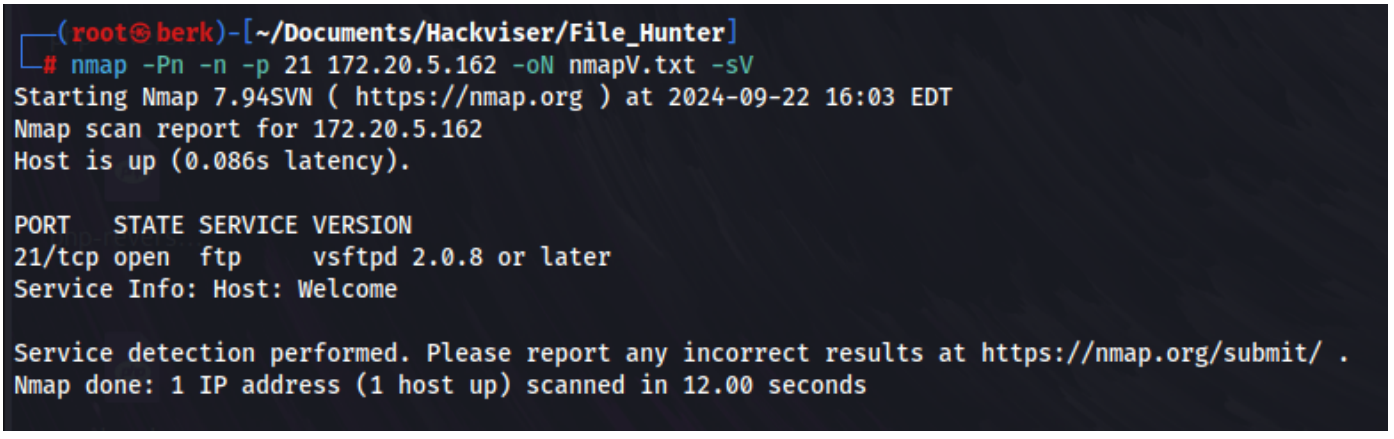
rustscan -a `<ip adresi>`

Sadece **21** portunun açık olduğunu görüyoruz. Bu da ilk sorumuzun cevabı oluyor.

Daha detaylı bilgi için nmap çalıştıralım

nmap -Pn -n -O -sV -p 21 <ip adresi> -oN nmapV.txt

- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.
- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır



21 portunda ftp çalıştığını görüyoruz. Ftp'nin açılımı ise bize en başta verilen açıklamada da dediği gibi **File Transfer Protocol** bu da 2. sorumuzun cevabı oluyor.

Şimdi zafiyet taraması için nmap ile scriptleri çalıştıralım

nmap -Pn -n -O -p 21 <ip adresi> -oN nmapC.txt -sC

Burada farklı olarak sadece -sC var **varsayılan script taraması** anlamına gelir ve Nmap'in yerleşik NSE (Nmap Scripting Engine) betiklerini çalıştırarak ek bilgi toplar.

```
┌──(root㉿berk)-[~/Documents/Hackviser/File_Hunter]
└─# nmap -Pn -n -p 21 172.20.5.162 -oN nmapC.txt -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-22 16:03 EDT
Nmap scan report for 172.20.5.162
Host is up (0.088s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp            25 Sep 08  2023 userlist
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.8.63
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status

Nmap done: 1 IP address (1 host up) scanned in 1.96 seconds
```

Burada ftp için anonymous girişin aktif olduğunu görüyoruz. Yani kullanıcı adı ve şifreye anonymous yazarak giriş yapabiliriz. Hemen altında ftpdeki dosylar gözüküyor tek bi dosya var userlist adında (bu da 5. sorumuzun cevabı). Ftp'ye giriş yapıp bu dosyayı okuyalım. Bu şekilde 3. sorununda cevabını vermiş oluyoruz kullanıcı adı ve şifremiz **anonymous**

Şimdi ftpye bağlandık hangi komutları çalıştırabileceğimiz görmek için help komutunu çalıştıralım.(bu da 4. sorumuzun cevabı)

```
┌──(root㉿berk)-[~/Documents/Hackviser/File_Hunter]
└─# ftp 172.20.5.162
Connected to 172.20.5.162.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.5.162:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!               case            dir             fget            idle            mdelete         modtime         ntrans          progress        rcvbuf          rmdir           sndbuf          type
$               cd              disconnect      form            image           mdir            more            open            prompt          recv            rstatus         status          umask
account         cdup            edit            ftp             lcd             mget            mput            page            proxy           reget           runique         struct          unset
append          chmod           epsv            gate            less            mkdir           mreget          passive         put             remopts         send            sunique         usage
ascii           close           epsv4           get             lpage           mls             msend           pdir            pwd             rename          sendport        system          user
bell            cr              epsv6           glob            lpwd            mlsd            newer           pls             quit            reset           set             tenex           verbose
binary          debug           exit            hash            ls              mlst            nlist           pmlsd           quote           restart         site            throttle        xferbuf
bye             delete          features        help            macdef          mode            nmap            preserve        rate            rhelp           size            trace           ?
ftp>
```

ls komutu ile dosyları listeleyelim ve less komutuylada dosyamızı okuyalım

```
ftp> ls
229 Entering Extended Passive Mode (|||29481|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            25 Sep 08  2023 userlist
l226 Directory send OK.
ftp> less userlist
jack:hackviser
root:root
ftp>
```

dosyamızın içeriğinde root kullanıcısının bilgileri bulunmakta bu da 7. ve son sorumuzun cevabı

6. soruda dosyayı nasıl indireceğimizi sormuş fakat biz less komutuyla direk okumuştuk eğer indirmek isteseydik **get userlist** yazmamız yeterli olacaktı yani 6. sorumuzun cevabıda **get**

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş