

Hackviser File Hunter Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki File Hunter isimli ısınmayı 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>

```
(root@berk)~[~/Documents/Hackviser/File_Hunter]
# rustscan -a 172.20.5.162

[... ASCII art ...]

The Modern Day Port Scanner.

-----
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
-----

RustScan: Where '404 Not Found' meets '200 OK'.

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.20.5.162:21
^[[18-~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-22 16:00 EDT
Initiating Ping Scan at 16:00
Scanning 172.20.5.162 [4 ports]
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 16:00 (0:00:00 remaining)
Completed Ping Scan at 16:00, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:00
Completed Parallel DNS resolution of 1 host. at 16:00, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 16:00
Scanning 172.20.5.162 [1 port]
Discovered open port 21/tcp on 172.20.5.162
Completed SYN Stealth Scan at 16:00, 0.14s elapsed (1 total ports)
Nmap scan report for 172.20.5.162
Host is up, received echo-reply ttl 63 (0.25s latency).
Scanned at 2024-09-22 16:00:47 EDT for 0s

PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
Raw packets sent: 5 (196B) | Rcvd: 2 (72B)
```

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

```
(root@berk)-[~/Documents/Hackviser/File_Hunter]
# nmap -Pn -n -p 21 172.20.5.162 -oN nmapV.txt -sV
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 (0.086s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
```

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 dosyalar gözüküyor tek bi dosya var userlist adında (bu da 5. sorumuzun cevabı). Ftp'ye giriş yapıp bu dosyayı okuyalım. Bu şekilde 3. sorusunda 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 dosyaları listeleyelim ve less komutuyla 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](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaş