## **Hackviser Arrow Write Up**

# Öncelikle herkese merhaba bugün Hackviser platformundaki Arrow isimli Isınmayı çözeceğiz

Isınmanın başlangıcında bize telnet hakkında bilgi vermiş

Telnet (Telecommunication Network), internet üzerinden uzak bilgisayarlara erişmek için kullanılan bir protokoldür. Kullanıcıların başka bir makineyle iletişim kurması ve kontrol etmesi için metin tabanlı bir arayüz sağlar, ancak şifreleme bulunmadığından güvenli bir protokol değildir.

### Bizden yanıtlamamızı istediği sorular şu şekilde

- Hangi port(lar) açık?
- Çalışan servisin adı nedir?
- · Hostname nedir?
- Telnet'e bağlanmak için kullandığınız username:password nedir?
- Telnet'e bağlandığınızda çalışma dizini konumunuz nedir?

Şimdi sırasıyla bu soruları cevaplandıralım

### İlk olarak tarama ile başlayalım

rustscan -a <ip adresi>

```
root@berk: ~/Documents/Hackviser/Arrow
  —(root@berk)-[~/Documents/Hackviser/Arrow]
—# rustscan -a 172.20.2.139
 : http://discord.skerritt.blog
: https://github.com/RustScan/RustScan
TCP handshake? More like a friendly high-five!
[~] 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
   Starting Script(s)
     Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-22 09:29 EDT
Initiating Ping Scan at 09:29
Scanning 172.20.2.139 [4 ports]
Completed Ping Scan at 09:29, 2.58s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:29
Completed Parallel DNS resolution of 1 host. at 09:29, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 09:29
Scanning 172.20.2.139 [1 port]
Discovered open port 23/tcp on 172.20.2.139
Completed SYN Stealth Scan at 09:29, 0.11s elapsed (1 total ports)
Nmap scan report for 172.20.2.139
Host is up, received echo-reply ttl 63 (0.44s latency).
Scanned at 2024-09-22 09:29:33 EDT for 0s
PORT STATE SERVICE REASON
23/tcp open telnet syn-ack ttl 63
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.11 seconds
Raw packets sent: 5 (196B) | Rcvd: 627 (25.072KB)
```

- 23 Portunun açık olduğunu görüyoruz bu da ilk sorumuzun cevabı oluyor
- 23 Portundan daha fazla detaylı bilgi almak için nmap çalıştıralım

### nmap -Pn -n -p 23 172.20.2.139 -oN nmapV.txt -sV

- Pn : hedefin çevrimdişi 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/Arrow]
# nmap -Pn -n -p 23 172.20.2.139 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-22 09:33 EDT
Nmap scan report for 172.20.2.139
Host is up (0.090s latency).

PORT STATE SERVICE VERSION
23/tcp open telnet Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

23 Portunda telnet çalıştığını görüyoruz bu da 2. sorumuzun cevabı oluyor

Şimdi telnete giriş yapmayı deneyelim

telnet <ip adresi>

```
t®berk)-[~/Documents/Hackviser/Arrow]
 # telnet 172.20.2.139
Trying 172.20.2.139...
Connected to 172.20.2.139.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root
it's just beginning *_*
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@arrow:~#
```

giriş yapmaya çalışırken karşımızda çıkan ilk bilgilendirme yazısında kullanıcı adı ve şifrenin **root:root** olduğunu öğreniyor ve sisteme giriş yapıyoruz. Bu da 4. sorunun cevabı oluyor.

Giriş yaptıktan sonra hostname in **arrow** olduğunu görüyoruz. Bu da 3. sorumuzun cevabı oluyor.

Son olarak bizden telnete giriş yaptığımızdaki konumumuzun ne olduğunu soruyor pwd komutunu kullanarak hangi dizinde olduğumuzu bulabiliriz

```
root@arrow:~# pwd
/root
root@arrow:~#
```

Ve bu da 5. ve son sorumuzun cevabı oluyor /root

# Başka bir yazıda görüşmek üzere ! Linkedin Github İnstagram Medium Ayberk İlbaş