

Discover Lernaean:İsınma

Nmap ile açık portları inceledik.

```
(root@kali)-[/home/kali]
# nmap -sS -sV -O -T4 -Pn 172.20.3.179

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 05:13 EDT
Nmap scan report for 172.20.3.179
Host is up (0.085s 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)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
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=10/18%OT=22%CT=1%CU=39234%PV=Y%DS=2%DC=I%G=Y%TM=671
OS:226C7%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A
OS:)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=D)OPS(O1=M509ST11NW7%O2=M509
OS:ST11NW7%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=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=
OS:S+%F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF
OS:=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.26 seconds
```

Ssh ve http servislerinin çalıştığını gördük.

http servisi açık olduğu için siteye girip bakıyoruz.

172.20.3.179

Kali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec



Apache2 Debian Default Page

debian

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the

3) Dizin tarama aracını kullanarak bulduğunuz izin nedir?

```
(root@kali)-[/home/kali]
# dirb http://172.20.3.179 /usr/share/wordlists/dirb/common.txt

DIRB v2.22
By The Dark Raver

START_TIME: Fri Oct 18 05:19:02 2024
URL_BASE: http://172.20.3.179/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
GENERATED WORDS: 4612

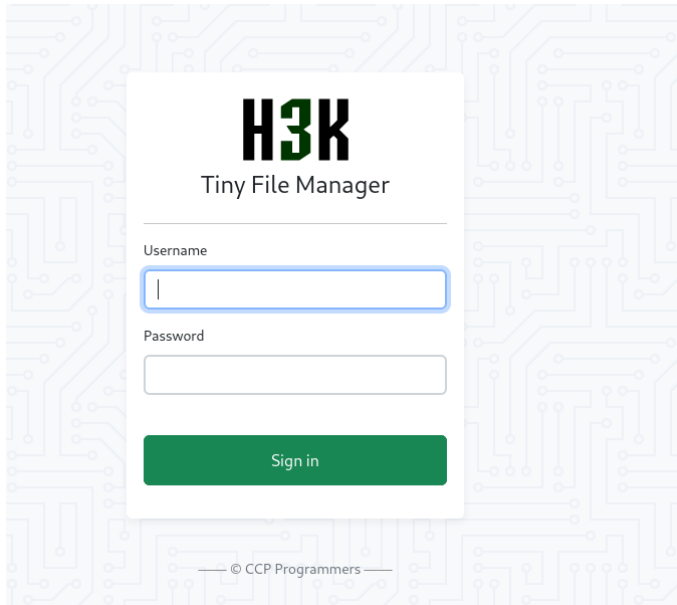
— Scanning URL: http://172.20.3.179/ —
⇒ DIRECTORY: http://172.20.3.179/filemanager/
+ http://172.20.3.179/index.html (CODE:200|SIZE:10701)
+ http://172.20.3.179/server-status (CODE:403|SIZE:277)

— Entering directory: http://172.20.3.179/filemanager/ —
⇒ DIRECTORY: http://172.20.3.179/filemanager/assets/
+ http://172.20.3.179/filemanager/index.php (CODE:200|SIZE:11558)

— Entering directory: http://172.20.3.179/filemanager/assets/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Fri Oct 18 05:46:08 2024
DOWNLOADED: 9224 - FOUND: 3
```

“<http://172.20.3.179/filemanager/>” dizinine bakıyoruz.



Login ekranı görüyoruz. Tiny file manager sayfasını internetten bakıyoruz. Github da sayfayı incelediğimiz de

How to use

Download ZIP with latest version from master branch.

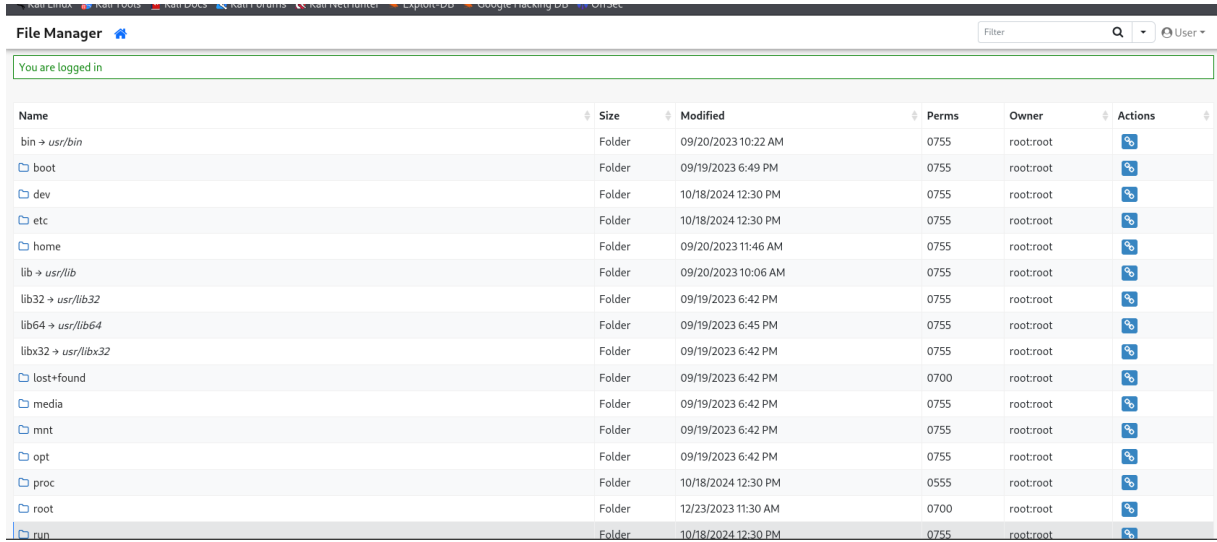
Just copy the tinyfilemanager.php to your webspace - thats all :) You can also change the file name from "tinyfilemanager.php" to something else, you know what i meant for.

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

Username/password bilgilerine ulaşıyoruz.

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

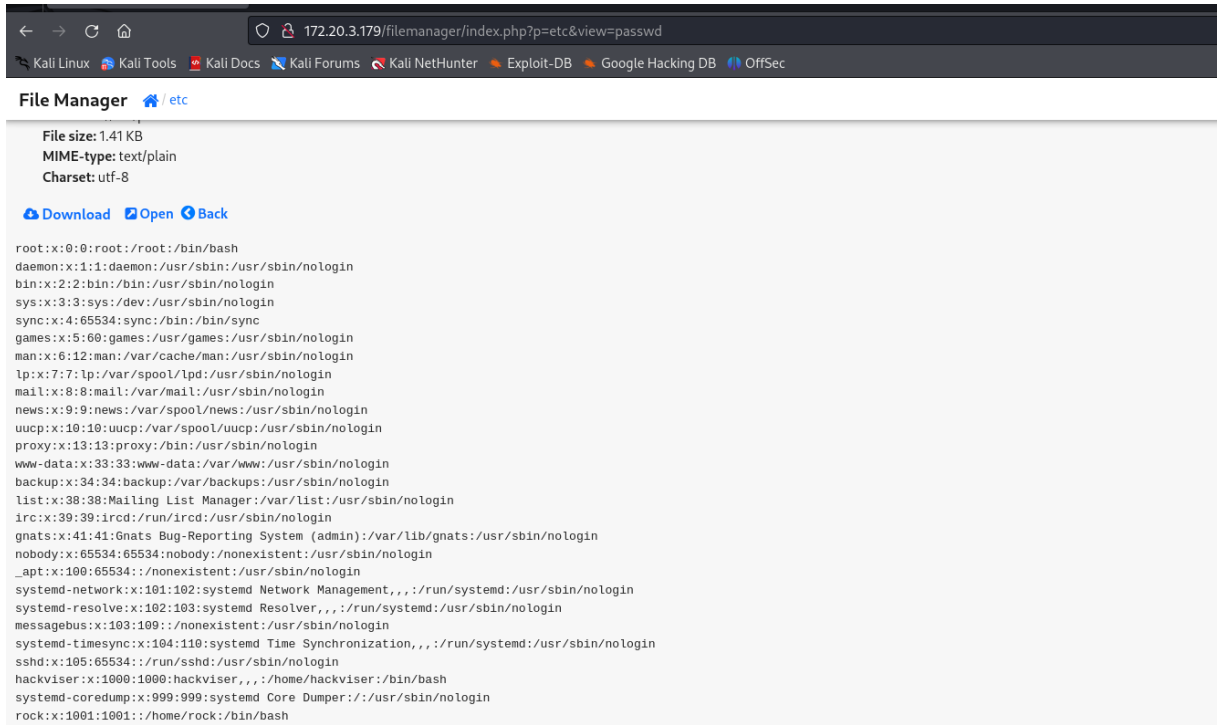
Login ekranına user/12345 girerek giriş yapabiliyoruz.



The screenshot shows a web-based file manager interface. At the top, there's a navigation bar with links to various resources like 'Rain Linux', 'Rain Tools', etc. Below the navigation bar, the title 'File Manager' is displayed. A status message 'You are logged in' is shown. The main content area is a table listing system directories. The table has columns for Name, Size, Modified, Perms, Owner, and Actions. The listed folders include bin, boot, dev, etc, home, lib, lib32, lib64, libx32, lost+found, media, mnt, opt, proc, root, and run. Each folder entry shows its permissions (e.g., 0755, 0700, 0555) and owner (root:root).

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	10/18/2024 12:30 PM	0755	root:root	
etc	Folder	10/18/2024 12:30 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	10/18/2024 12:30 PM	0555	root:root	
root	Folder	12/23/2023 11:30 AM	0700	root:root	
run	Folder	10/18/2024 12:30 PM	0755	root:root	

Sisteme giriş yapıyoruz. En son eklenen kullanıcıyı bulmamız gerekiyor. /etc/passwd: dizinine gidiyoruz.



5) Bilgisayara eklenen son kullanıcı adı nedir?

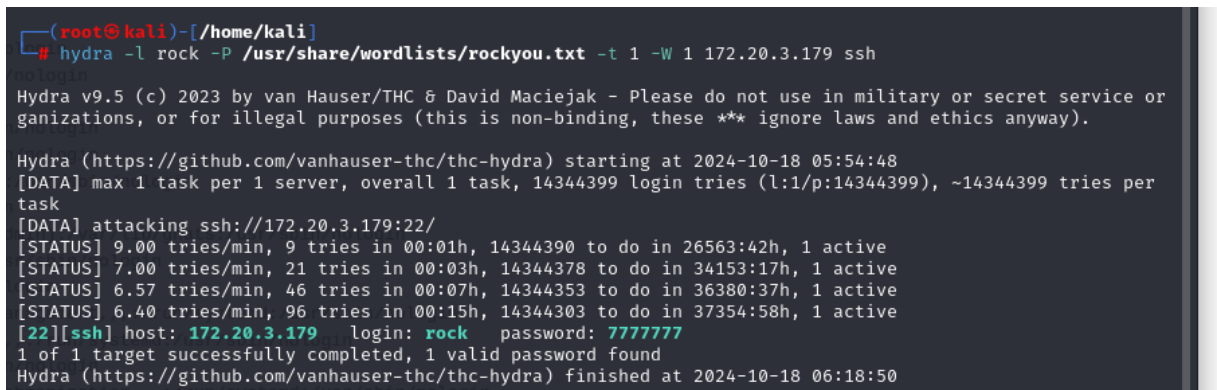
Son kullanıcı rock kullanıcısı olarak gözüküyor.

Ssh servisi açık olduğundan rock kullanıcısı ile bağlanıyoruz.



Rock şifresini brute force yaparak elde etmemiz gerekiyor.

6) rock kullanıcısının parolası nedir?



Rock kullanıcısının şifresini bulmuş oluyoruz.

7) rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

Bunu bulmak ssh ile bağdalandığımız sistemde history sorgusu ile ilk çalıştırdığı komudu buluyoruz.

```
(root@kali)~[/home/kali]
# ssh rock@172.20.3.179

[Discover]

Welcome ^_^
rock@172.20.3.179's password:
Linux discover-lernaean 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-lernaean:~$ history
rock 1 cat .bash_history
      2 cd
      3 ls -la
      4 history
      5 ls
      6 bls -la login
      7 exit
      8 cd
      9 exit
     10 pwd
     11 cd /var/www/html/
     12 ls -la /run/systemd:/usr/sbin/nologin
     13 cd filemanager/
     14 ls -la
     15 cd
     16 ls -la /run/systemd:/usr/sbin/nologin
     17 history
rock@discover-lernaean:~$ client_loop: send disconnect: Broken pipe
```