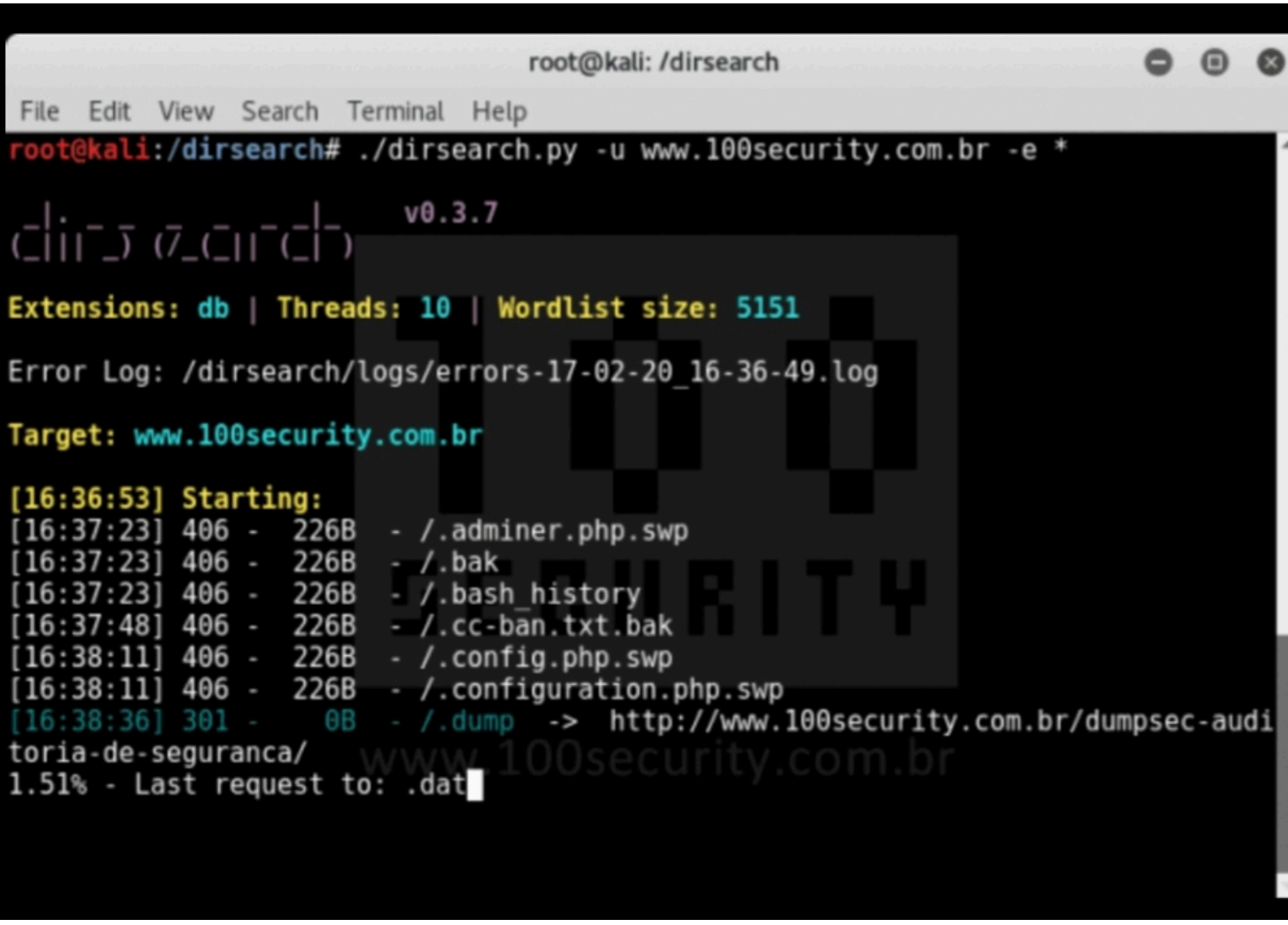
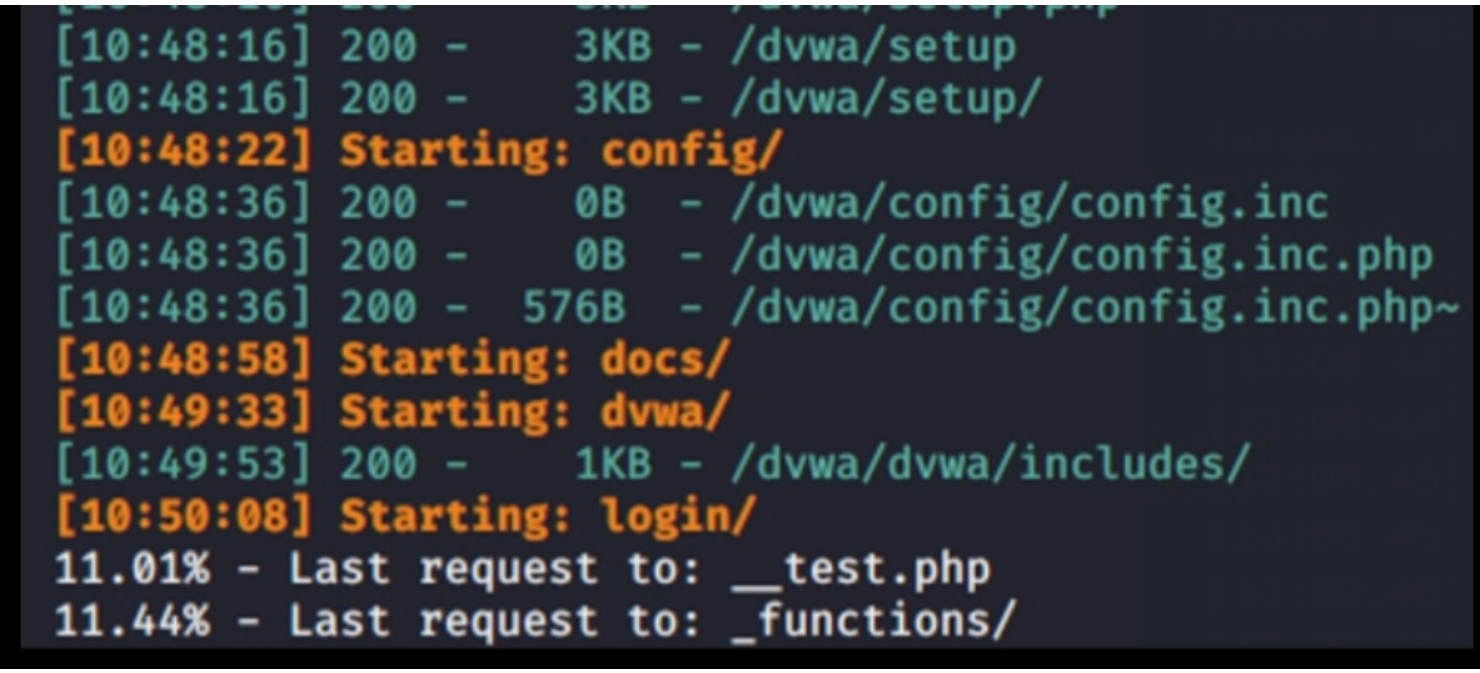
```
root@kali:~/dirsearch# ls -la
total 60
drwxr-xr-x  8 root root 4096 Jan 24 08:02 .
drwxr-xr-x 23 root root 4096 Jan 24 08:01 ..
-rw-r--r--  1 root root 1592 Jan 24 08:02 CHANGELOG.md
drwxr-xr-x  2 root root 4096 Jan 24 08:02 db
-rw-r--r--  1 root root  433 Jan 24 08:02 default.conf
-rwxr-xr-x  1 root root 1352 Jan 24 08:02 dirsearch.py
-rw-r--r--  1 root root  218 Jan 24 08:02 Dockerfile
drwxr-xr-x  8 root root 4096 Jan 24 08:02 .git
-rw-r--r--  1 root root  124 Jan 24 08:02 .gitignore
drwxr-xr-x  9 root root 4096 Jan 24 10:25 lib
drwxr-xr-x  2 root root 4096 Jan 24 08:02 logs
-rw-r--r--  1 root root 5147 Jan 24 08:02 README.md
drwxr-xr-x  2 root root 4096 Jan 24 08:02 reports
drwxr-xr-x  8 root root 4096 Jan 24 10:25 thirdparty
root@kali:~/dirsearch#
```

```
r00t@r00t-PC:/media/r00t/HDD 1TB1/Kitploit/dirsearch$ python3 dirsearch.py -h
Usage: dirsearch.py [-u|--url] target [-e|--extensions] extensions [options]

Options:
  -h, --help            show this help message and exit

  Mandatory:
    -u URL, --url=URL   URL target
    -L URLLIST, --url-list=URLLIST
                        URL list target
    -e EXTENSIONS, --extensions=EXTENSIONS
                        Extension list separated by comma (Example: php,asp)

  Dictionary Settings:
    -w WORDLIST, --wordlist=WORDLIST
    -l, --lowercase
    -f, --force-extensions
                        Force extensions for every wordlist entry (like in
                        DirBuster)

  General Settings:
    -r, --recursive     Bruteforce recursively
    --scan-subdir=SCANSUBDIRS, --scan-subdirs=SCANSUBDIRS
                        Scan subdirectories of the given -u|--url (separated
```

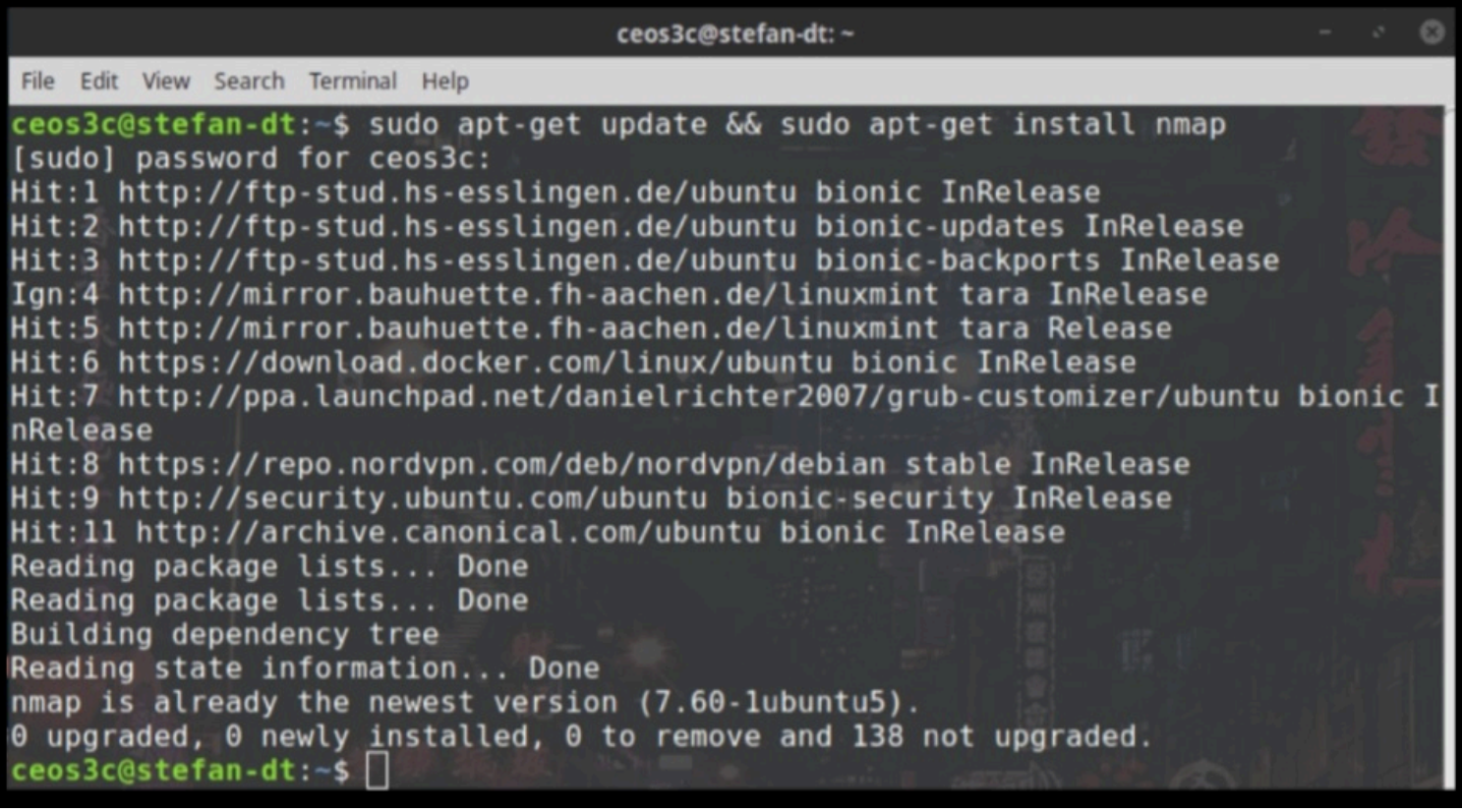
```
[10:37:24] 200 -    5KB - /dvwa/CHANGELOG
[10:37:24] 200 -    5KB - /dvwa/CHANGELOG.txt
[10:37:25] 301 -  325B  - /dvwa/config  →  http://192.168.0.102/dvwa/config/
[10:37:25] 200 -  910B  - /dvwa/config/
[10:37:26] 200 -   32KB - /dvwa/COPYING
[10:37:27] 301 -  323B  - /dvwa/docs  →  http://192.168.0.102/dvwa/docs/
[10:37:27] 200 -  921B  - /dvwa/docs/
[10:37:27] 200 -    1KB - /dvwa/dvwa/
[10:37:28] 200 -    1KB - /dvwa/favicon.ico
[10:37:30] 302 -    0B  - /dvwa/ids_log.php  →  login.php
[10:37:30] 302 -    0B  - /dvwa/index  →  login.php
[10:37:30] 302 -    0B  - /dvwa/index.php  →  login.php
[10:37:30] 302 -    0B  - /dvwa/index.php/login/  →  login.php
[10:37:32] 200 -    1KB - /dvwa/login
[10:37:32] 200 -    1KB - /dvwa/login.php
[10:37:32] 200 -    1KB - /dvwa/login/
[10:37:32] 200 -    1KB - /dvwa/login/admin/admin.asp
[10:37:32] 200 -    1KB - /dvwa/login/administrator/
[10:37:32] 200 -    1KB - /dvwa/login/cpanel/
[10:37:32] 200 -    1KB - /dvwa/login/index
[10:37:32] 200 -    1KB - /dvwa/login/oauth/
[10:37:32] 200 -    1KB - /dvwa/login/super
[10:37:32] 200 -    1KB - /dvwa/login/admin/
[10:37:32] 200 -    1KB - /dvwa/login/cpanel.php
[10:37:32] 200 -    1KB - /dvwa/login/login
[10:37:32] 302 -    0B  - /dvwa/logout  →  login.php
[10:37:32] 302 -    0B  - /dvwa/logout/  →  login.php
[10:37:35] 200 -  148B  - /dvwa/php.ini
[10:37:35] 302 -    0B  - /dvwa/phpinfo.php  →  login.php
[10:37:35] 302 -    0B  - /dvwa/phpinfo  →  login.php
[10:37:37] 200 -    5KB - /dvwa/README
[10:37:37] 200 -    5KB - /dvwa/README.txt
[10:37:38] 200 -   26B  - /dvwa/robots.txt
[10:37:38] 302 -    0B  - /dvwa/security  →  login.php
[10:37:38] 302 -    0B  - /dvwa/security/  →  login.php
[10:37:39] 200 -    3KB - /dvwa/setup
[10:37:39] 200 -    3KB - /dvwa/setup/
[10:37:39] 200 -    3KB - /dvwa/setup.php

Task Completed
root@kali:~#
```

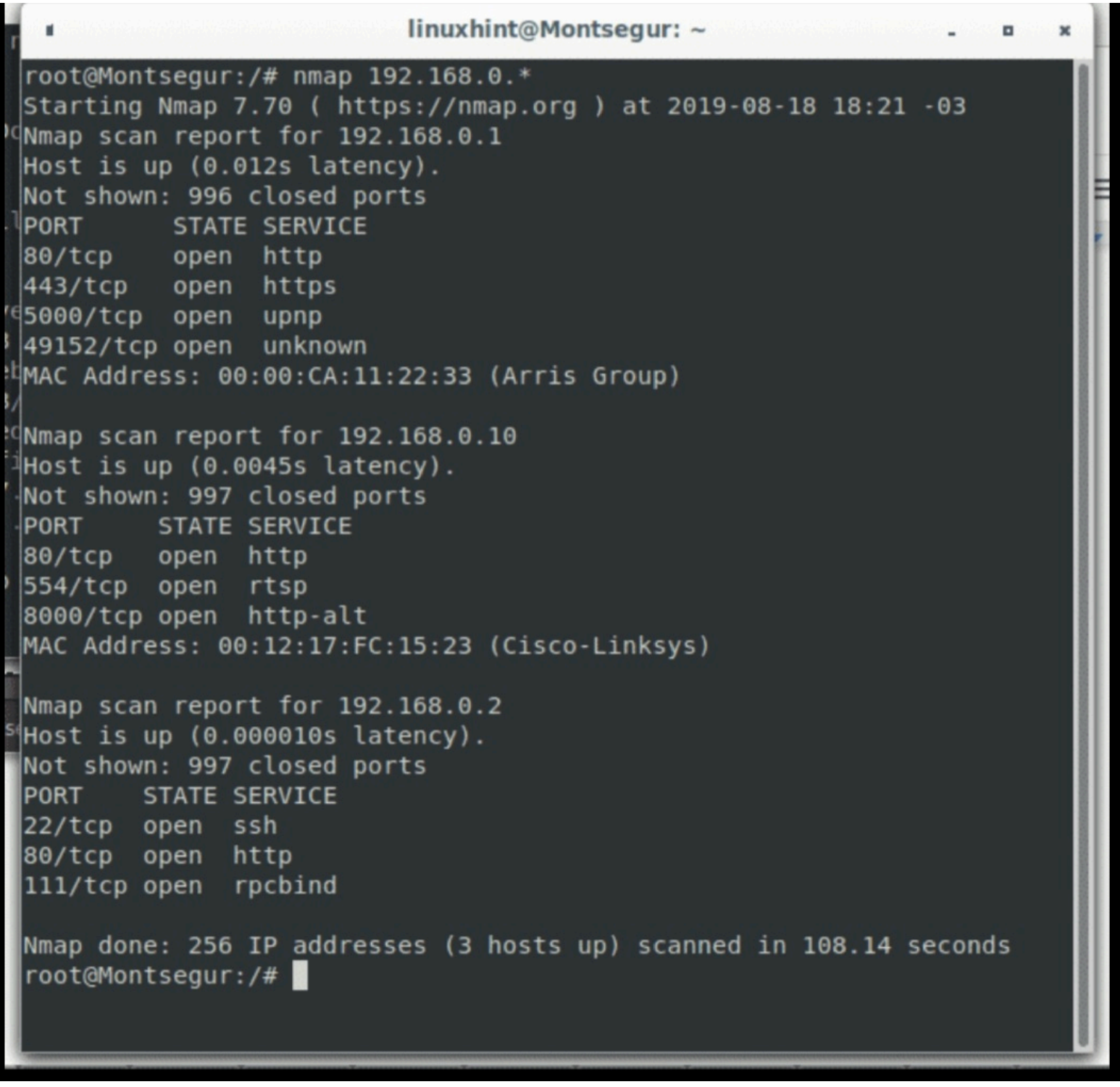

root@kali: /dirsearch
File Edit View Search Terminal Help
root@kali:/dirsearch# ./dirsearch.py -u www.100security.com.br -e *
v0.3.7
Extensions: db | Threads: 10 | Wordlist size: 5151
Error Log: /dirsearch/logs/errors-17-02-20_16-36-49.log
Target: www.100security.com.br
[16:36:53] Starting:
[16:37:23] 406 - 226B - /.adminer.php.swp
[16:37:23] 406 - 226B - /.bak
[16:37:23] 406 - 226B - /.bash_history
[16:37:48] 406 - 226B - /.cc-ban.txt.bak
[16:38:11] 406 - 226B - /.config.php.swp
[16:38:11] 406 - 226B - /.configuration.php.swp
[16:38:36] 301 - 0B - /.dump -> http://www.100security.com.br/dumpsec-audi
toria-de-seguranca/
1.51% - Last request to: .dat
www.100security.com.br

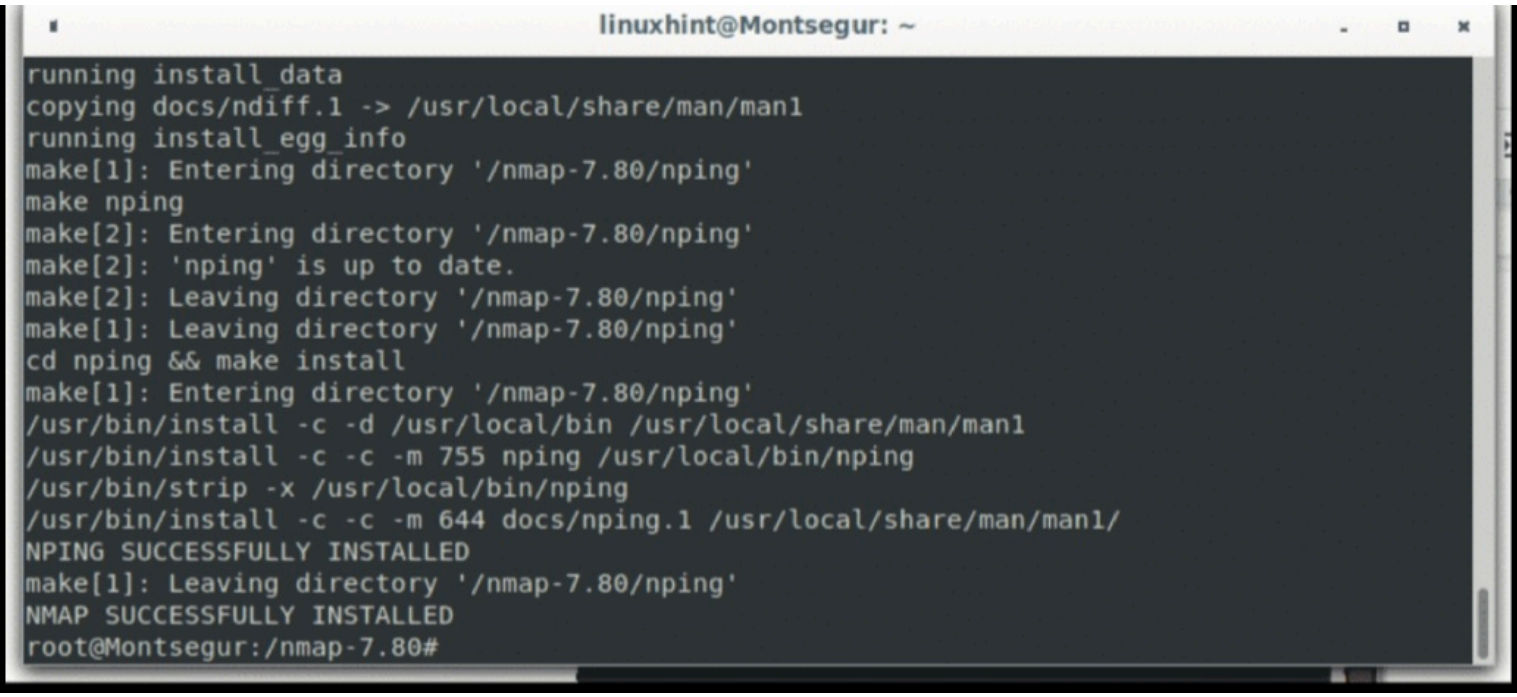
```
root@hackingloops:~/dirsearch# python3 dirsearch.py -u http://testphp.vulnweb.com -X .php

 _|. _ _  _  _  _ _|_    v0.4.0
(_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, html, htm, js | HTTP method: GET | Threads: 20 | Wordlis
t size: 11123

Error Log: /root/dirsearch/logs/errors-20-12-03_23-56-37.log

Target: http://testphp.vulnweb.com/

Output File: /root/dirsearch/reports/testphp.vulnweb.com/_20-12-03_23-56-39.txt

[23:56:40] Starting:
[23:56:51] 301 -  169B  - /.idea  ->  http://testphp.vulnweb.com/.idea/     (Added to que
ue)
[23:56:51] 200 -  951B  - /.idea/
[23:56:52] 200 -    6B  - /.idea/.name
[23:56:52] 200 -  171B  - /.idea/encodings.xml
[23:56:52] 200 -  266B  - /.idea/misc.xml
[23:56:52] 200 -  275B  - /.idea/modules.xml
[23:56:52] 200 -  143B  - /.idea/scopes/scope_settings.xml
[23:56:52] 200 -  173B  - /.idea/vcs.xml
[23:56:52] 200 -   12KB - /.idea/workspace.xml
```

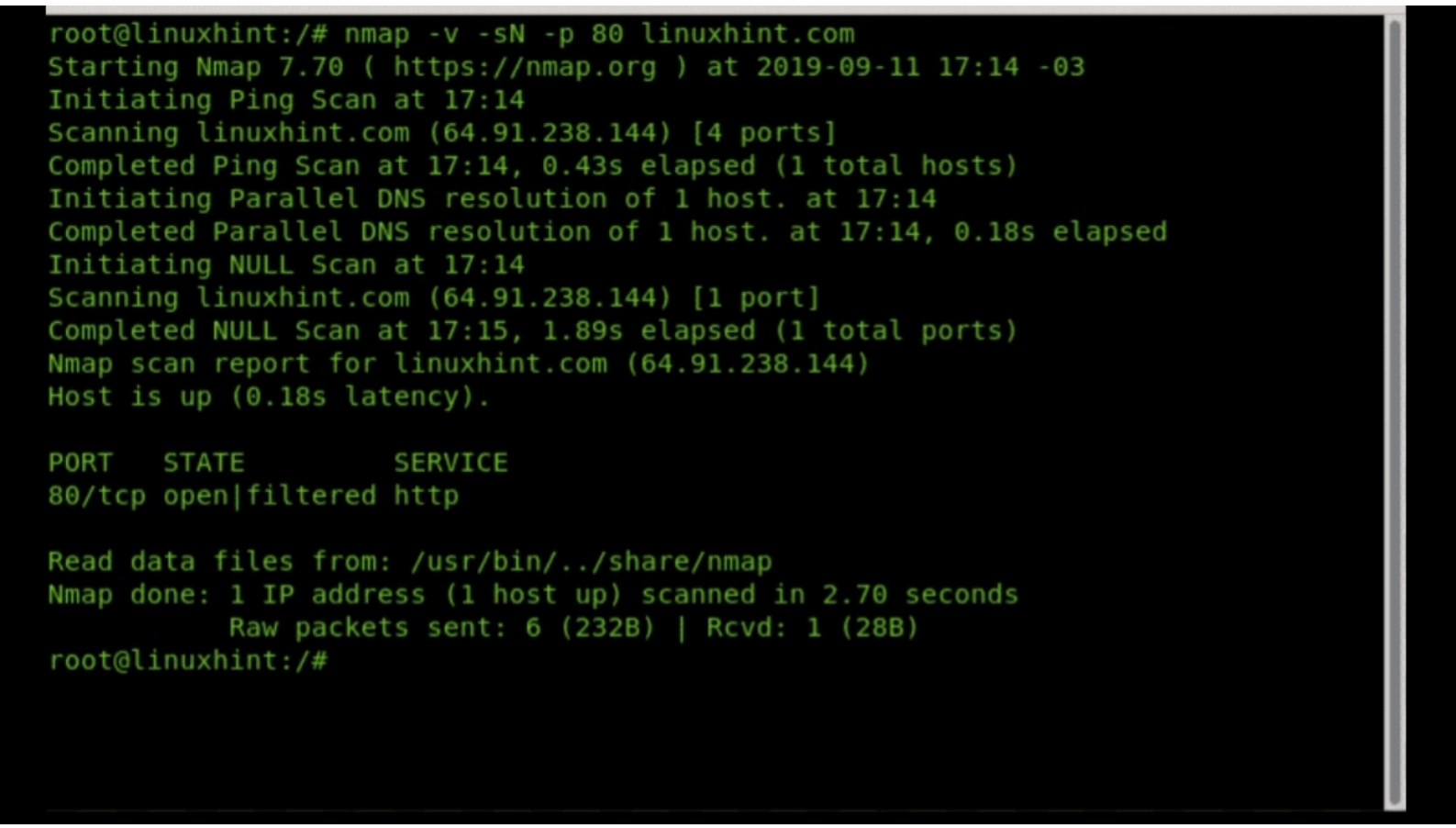

[10:48:16] 200 - 3KB - /dvwa/setup
[10:48:16] 200 - 3KB - /dvwa/setup/
[10:48:22] Starting: config/
[10:48:36] 200 - 0B - /dvwa/config/config.inc
[10:48:36] 200 - 0B - /dvwa/config/config.inc.php
[10:48:36] 200 - 576B - /dvwa/config/config.inc.php~
[10:48:58] Starting: docs/
[10:49:33] Starting: dvwa/
[10:49:53] 200 - 1KB - /dvwa/dvwa/includes/
[10:50:08] Starting: login/
11.01% - Last request to: __test.php
11.44% - Last request to: _functions/

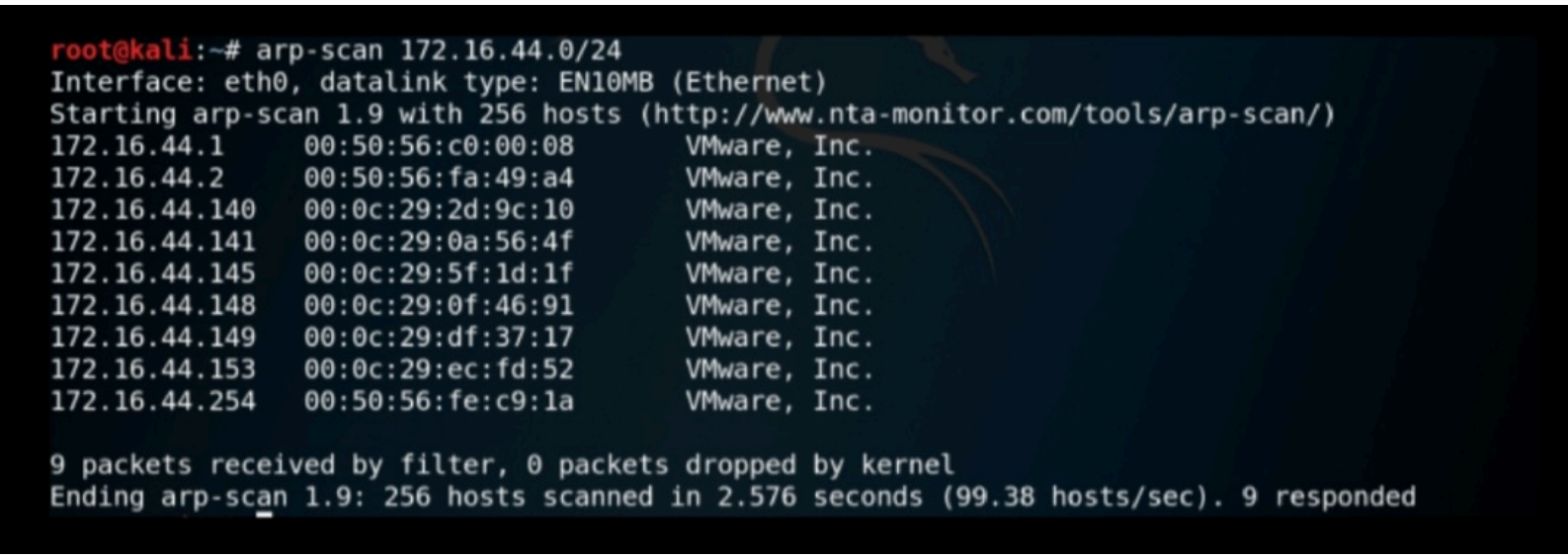
```
[23:47:24] info:    27.4% [10108/36942] - 20B - Denied http://10.10.10.6/cgi-bin/
[23:47:40] info:    37.0% [13651/36942] - 20B - Denied http://10.10.10.6/doc/
[23:47:40] info:    37.0% [13654/36942] - 20B - Denied http://10.10.10.6/doc/en/changes.html
[23:47:40] info:    37.0% [13656/36942] - 20B - Denied http://10.10.10.6/doc/stable.version
[23:47:40] info:    40.7% [15046/36942] - 20B - http://10.10.10.6/equity/
[23:47:40] warning: skip [00000/36942] - Ignored /error.php
[23:48:02] info:    50.4% [18615/36942] - 0B - http://10.10.10.6/icons2/
[23:48:02] info:    50.4% [18615/36942] - 0B - OK http://10.10.10.6/icons/
[23:48:03] info:    51.7% [19113/36942] - 0B - http://10.10.10.6/includes/fckeditor/editor/filemanager/connectors/asp/upload.asp
[23:48:04] warning: skip [00000/36942] - Ignored /index.php
[23:48:04] info:    51.8% [19154/36942] - 177B - OK http://10.10.10.6/index.html
[23:48:40] info:    77.3% [28553/36942] - 0B - http://10.10.10.6/removed/
[23:48:40] info:    77.3% [28553/36942] - 20B - OK http://10.10.10.6/rename/
[23:49:02] info:    87.1% [32188/36942] - 20B - http://10.10.10.6/support.php
[23:49:02] info:    87.1% [32188/36942] - 20B - Denied http://10.10.10.6/server-status/
[23:49:04] info:    89.1% [32924/36942] - 0B - http://10.10.10.6/test.txt
[23:49:04] info:    89.1% [32924/36942] - 20B - OK http://10.10.10.6/test.php
[23:49:04] info:    89.1% [32924/36942] - 20B - OK http://10.10.10.6/test/
[23:49:05] info:    90.9% [33594/36942] - 0B - OK http://10.10.10.6/torrent/
[23:49:23] info:    100.0% [36939/36942] - 0B - http://10.10.10.6/privat.txt
+-------------------------+----------+
| Statistics (10.10.10.6) |  Summary |
|-------------------------+----------|
| failed                  |    36894 |
| forbidden               |       39 |
| ignored                 |        3 |
| success                 |        6 |
| items                   |    36942 |
| workers                 |       25 |
+-------------------------+----------+
[23:49:23] debug:   Total time running: 0:02:46.300093
```

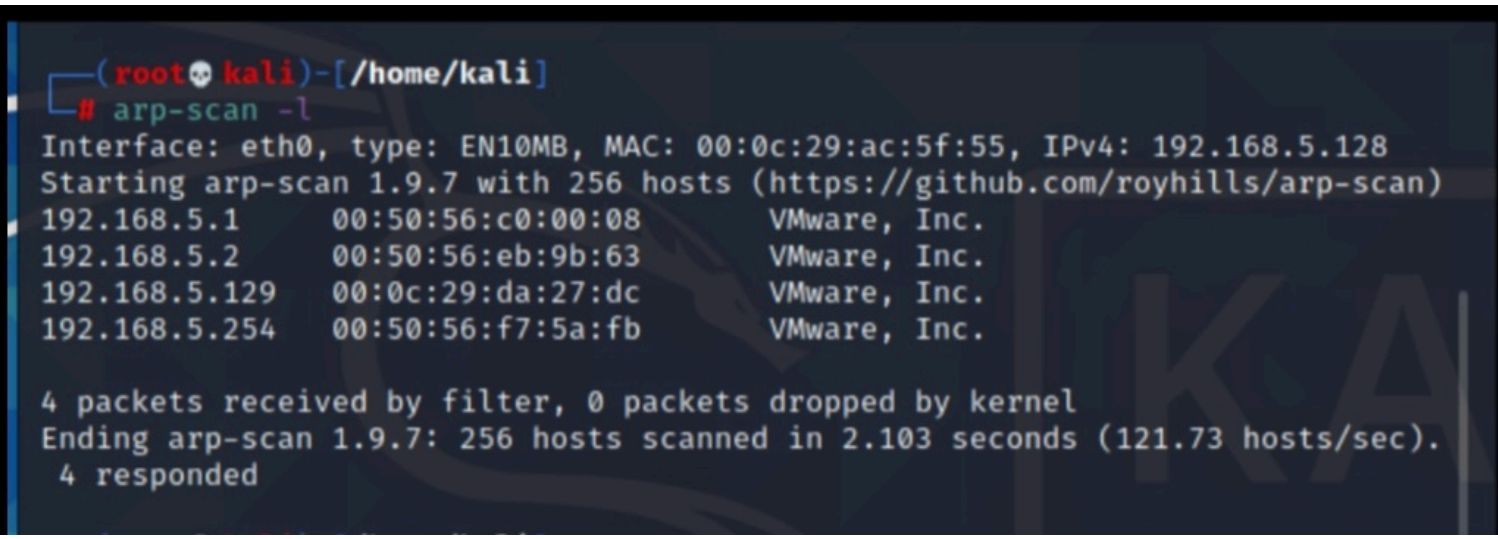

ceos3c@stefan-dt: ~
File Edit View Search Terminal Help
ceos3c@stefan-dt:~$ sudo apt-get update && sudo apt-get install nmap
[sudo] password for ceos3c:
Hit:1 http://ftp-stud.hs-esslingen.de/ubuntu bionic InRelease
Hit:2 http://ftp-stud.hs-esslingen.de/ubuntu bionic-updates InRelease
Hit:3 http://ftp-stud.hs-esslingen.de/ubuntu bionic-backports InRelease
Ign:4 http://mirror.bauhuette.fh-aachen.de/linuxmint tara InRelease
Hit:5 http://mirror.bauhuette.fh-aachen.de/linuxmint tara Release
Hit:6 https://download.docker.com/linux/ubuntu bionic InRelease
Hit:7 http://ppa.launchpad.net/danielrichter2007/grub-customizer/ubuntu bionic I
nRelease
Hit:8 https://repo.nordvpn.com/deb/nordvpn/debian stable InRelease
Hit:9 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:11 http://archive.canonical.com/ubuntu bionic InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
nmap is already the newest version (7.60-1ubuntu5).
0 upgraded, 0 newly installed, 0 to remove and 138 not upgraded.
ceos3c@stefan-dt:~$


linuxhint@Montsegur: ~
root@Montsegur:/# nmap 192.168.0.*
Starting Nmap 7.70 (https://nmap.org) at 2019-08-18 18:21 -03
Nmap scan report for 192.168.0.1
Host is up (0.012s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
5000/tcp open upnp
49152/tcp open unknown
MAC Address: 00:00:CA:11:22:33 (Arris Group)
Nmap scan report for 192.168.0.10
Host is up (0.0045s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
554/tcp open rtsp
8000/tcp open http-alt
MAC Address: 00:12:17:FC:15:23 (Cisco-Linksys)
Nmap scan report for 192.168.0.2
Host is up (0.000010s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
Nmap done: 256 IP addresses (3 hosts up) scanned in 108.14 seconds
root@Montsegur:/#


linuxhint@Montsegur: ~
running install_data
copying docs/ndiff.1 -> /usr/local/share/man/man1
running install_egg_info
make[1]: Entering directory '/nmap-7.80/nping'
make nping
make[2]: Entering directory '/nmap-7.80/nping'
make[2]: 'nping' is up to date.
make[2]: Leaving directory '/nmap-7.80/nping'
make[1]: Leaving directory '/nmap-7.80/nping'
cd nping && make install
make[1]: Entering directory '/nmap-7.80/nping'
/usr/bin/install -c -d /usr/local/bin /usr/local/share/man/man1
/usr/bin/install -c -c -m 755 nping /usr/local/bin/nping
/usr/bin/strip -x /usr/local/bin/nping
/usr/bin/install -c -c -m 644 docs/nping.1 /usr/local/share/man/man1/
NPING SUCCESSFULLY INSTALLED
make[1]: Leaving directory '/nmap-7.80/nping'
NMAP SUCCESSFULLY INSTALLED
root@Montsegur:/nmap-7.80#


root@linuxhint:/# nmap -v -sN -p 80 linuxhint.com
Starting Nmap 7.70 (https://nmap.org) at 2019-09-11 17:14 -03
Initiating Ping Scan at 17:14
Scanning linuxhint.com (64.91.238.144) [4 ports]
Completed Ping Scan at 17:14, 0.43s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:14
Completed Parallel DNS resolution of 1 host. at 17:14, 0.18s elapsed
Initiating NULL Scan at 17:14
Scanning linuxhint.com (64.91.238.144) [1 port]
Completed NULL Scan at 17:15, 1.89s elapsed (1 total ports)
Nmap scan report for linuxhint.com (64.91.238.144)
Host is up (0.18s latency).
PORT STATE SERVICE
80/tcp open|filtered http
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.70 seconds
Raw packets sent: 6 (232B) | Rcvd: 1 (28B)
root@linuxhint:/#


root@kali:~# arp-scan 172.16.44.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
172.16.44.1 00:50:56:c0:00:08 VMware, Inc.
172.16.44.2 00:50:56:fa:49:a4 VMware, Inc.
172.16.44.140 00:0c:29:2d:9c:10 VMware, Inc.
172.16.44.141 00:0c:29:0a:56:4f VMware, Inc.
172.16.44.145 00:0c:29:5f:1d:1f VMware, Inc.
172.16.44.148 00:0c:29:0f:46:91 VMware, Inc.
172.16.44.149 00:0c:29:df:37:17 VMware, Inc.
172.16.44.153 00:0c:29:ec:fd:52 VMware, Inc.
172.16.44.254 00:50:56:fe:c9:1a VMware, Inc.
9 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.576 seconds (99.38 hosts/sec). 9 responded


┌──(root💀kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:ac:5f:55, IPv4: 192.168.5.128
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.5.1 00:50:56:c0:00:08 VMware, Inc.
192.168.5.2 00:50:56:eb:9b:63 VMware, Inc.
192.168.5.129 00:0c:29:da:27:dc VMware, Inc.
192.168.5.254 00:50:56:f7:5a:fb VMware, Inc.
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.103 seconds (121.73 hosts/sec).
4 responded