

Cybersecurity For Beginners

Day 2 – Assignment

~PRATIK PAKHARE(CEHv11)

1) Google Dorking

Site:

The screenshot shows a Microsoft Edge browser window with the search bar containing 'site:microsoft.com'. The results page displays approximately 3,18,00,000 results found in 0.32 seconds. The first result is a link to 'https://devblogs.microsoft.com' under the heading 'Microsoft Developer Blogs: DevBlogs'. Below it is another link to 'https://support.microsoft.com' under the heading 'Microsoft Support'. Further down are links for 'Careers at Microsoft | Microsoft jobs' and 'NET | Free. Cross-platform. Open Source'. The browser's taskbar at the bottom shows other open tabs and system status.

Inurl:

The screenshot shows a Microsoft Edge browser window with the search bar containing 'inurl:login site:simplilearn.com'. The results page displays about 127 results found in 0.36 seconds. The first result is a link to 'https://community.simplilearn.com/threads/account-' under the heading 'Account login | Simplilearn - Discussions on Certifications'. Below it is a link to 'https://courses.skillsnet.simplilearn.com/login' under the heading 'Sign in or Register | Simplilearn'. The browser's taskbar at the bottom shows other open tabs and system status.

InText:

A screenshot of a Google search results page. The search query is "intext:password". The results include links to "Google Password Manager" and "Strong Random Password Generator". Below the results, there is a "People also ask" section with questions like "Can I see my password?", "What is a good 8 character password?", "How do I log into a saved password?", and "What is a nice password?". The browser interface shows tabs for "Get Kali | Kali Linux" and "intext:password - Google Search". The taskbar at the bottom shows various pinned icons.

Filetype:

A screenshot of a Google search results page for "google dorks filetype:pdf". The results include a link to "OFFENSIVE GOGLING" from owasp.org. Below the results, there is a "People also ask" section with questions like "Is Google Dorking illegal?", "What is the use of Google dorks?", "Where can I find Google dorks?", and "What is meant by Google Dorking?". The browser interface shows tabs for "Get Kali | Kali Linux" and "google dorks filetype:pdf - Google Search". The taskbar at the bottom shows various pinned icons.

Google Hacking Database

The screenshot shows a web browser window with three tabs: "Get Kali | Kali Linux", "Google Hacking Database (GHD)", and "New Tab". The main content area displays the "EXPLOIT DATABASE" interface. On the left is a sidebar with various icons. The main search results page has a header "Google Hacking Database" and a search bar with "Quick Search". It includes filters and a "Reset All" button. The results table has columns for "Date Added", "Dork", "Category", and "Author". The results listed are:

Date Added	Dork	Category	Author
2021-08-20	intitle:"geovision inc." inurl:login.htm	Pages Containing Login Portals	s Thakur
2021-08-20	intitle:"7100 login" "lancom"	Various Online Devices	s Thakur
2021-08-20	intitle:"vigor login page"	Pages Containing Login Portals	s Thakur
2021-08-20	intitle:"ADB Broadband" login intext:"ADB Broadband S.p.A" -com	Pages Containing Login Portals	s Thakur
2021-08-20	intitle:"Login - Hitron technologies"	Pages Containing Login Portals	s Thakur
2021-08-20	intitle:"DGS-3100 Login"	Pages Containing Login Portals	s Thakur
2021-08-20	intitle:"lg smart ip device" -com	Various Online Devices	s Thakur
2021-08-20	intitle:"3G wireless gateway" "login" intext:"huawei technologies"	Pages Containing Login Portals	s Thakur
2021-08-20	intitle:"ADMINISTRATOR LOGIN" inurl:adminlogin	Pages Containing Login Portals	Sanem Sudheendra
2021-08-20	intitle:"KNX-IP-Gateway Login"	Pages Containing Login Portals	s Thakur

The bottom of the screen shows a Windows taskbar with icons for File Explorer, Google Chrome, Microsoft Word, and others, along with system status indicators like battery level, signal strength, and date/time.

Webcams

The screenshot shows a web browser window with three tabs: "Get Kali | Kali Linux", "Google Hacking Database (GHD)", and "Not secure | 109.233.191.130:8080/multi.html". The main content area displays the "WEBCAMXP 5" software interface. The top navigation bar includes "Home", "Multi view", "Smartphone", "Gallery", "Administration", and "Not logged in". Below the navigation is a dropdown menu set to "320x240". Four camera feeds are displayed in a grid:

- Top-left: An aerial view of a town square with buildings and trees.
- Top-right: A street-level view of a road with cars and a building in the background.
- Bottom-left: An aerial view of a street with parked cars and trees.
- Bottom-right: An aerial view of a park or plaza with people walking and a yellow car.

The bottom of the screen shows a Windows taskbar with icons for File Explorer, Google Chrome, Microsoft Word, and others, along with system status indicators like battery level, signal strength, and date/time.

Devices in my Network

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:/home/kali
root@kali:/home/kali
(kali㉿kali)-[~]
$ sudo su
We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
root@kali:~/home/kali
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:0e:34:8d, IPv4: 10.0.2.15
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.2      52:54:00:12:35:02      QEMU
10.0.2.3      52:54:00:12:35:03      QEMU
10.0.2.4      52:54:00:12:35:04      QEMU

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.166 seconds (118.19 hosts/sec). 3 responded

(kali㉿kali)-[~/home/kali]
#
```

Type here to search 0 26°C AQI 49 07:46 23-08-2021 Right Ctrl

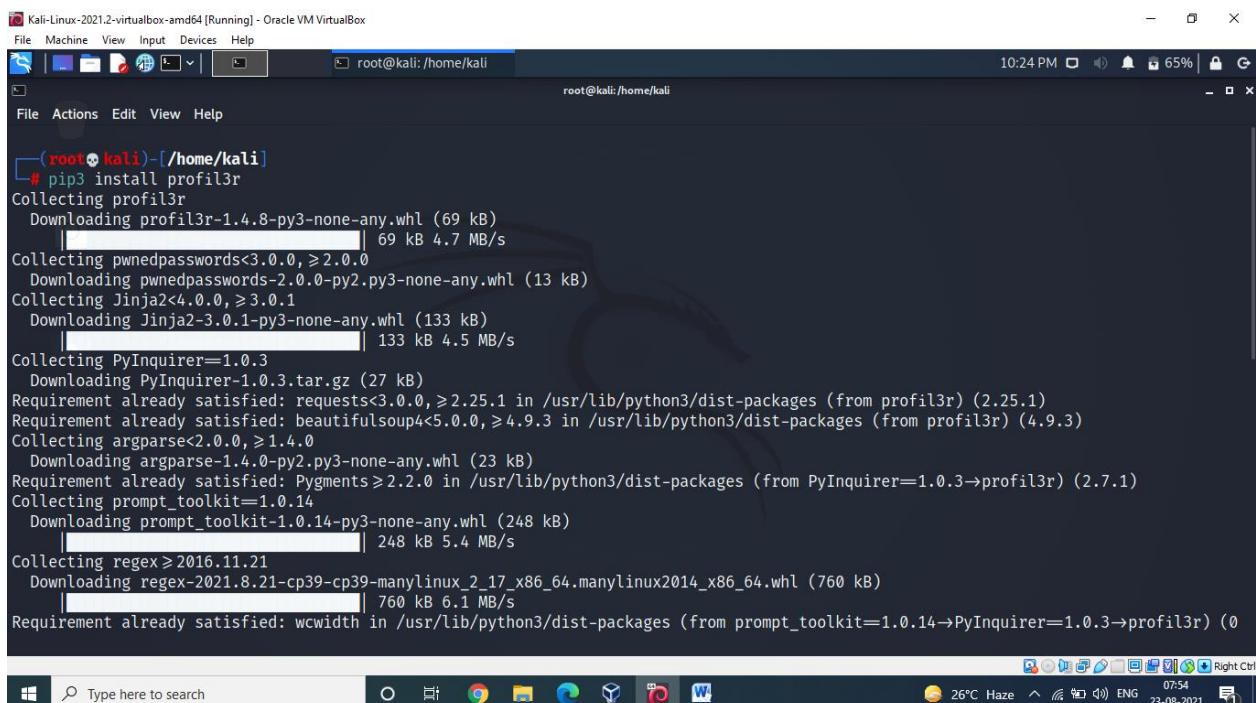
Installing Python3 in Kali Linux

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

```
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:/home/kali
root@kali:/home/kali
(root㉿kali)-[~/home/kali]
# sudo apt install python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python-pip-whl python3-wheel
The following NEW packages will be installed:
  python-pip-whl python3-pip python3-wheel
0 upgraded, 3 newly installed, 0 to remove and 16 not upgraded.
Need to get 2,308 kB of archives.
After this operation, 3,669 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 python-pip-whl all 20.3.4-2 [1,947 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-wheel all 0.34.2-1 [24.0 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 python3-pip all 20.3.4-2 [337 kB]
Fetched 2,308 kB in 3s (841 kB/s)
Selecting previously unselected package python-pip-whl.
(Reading database ... 271628 files and directories currently installed.)
Preparing to unpack .../python-pip-whl_20.3.4-2_all.deb ...
Unpacking python-pip-whl (20.3.4-2) ...
Selecting previously unselected package python3-wheel.
Preparing to unpack .../python3-wheel_0.34.2-1_all.deb ...
Unpacking python3-wheel (0.34.2-1) ...
Selecting previously unselected package python3-pip.
```

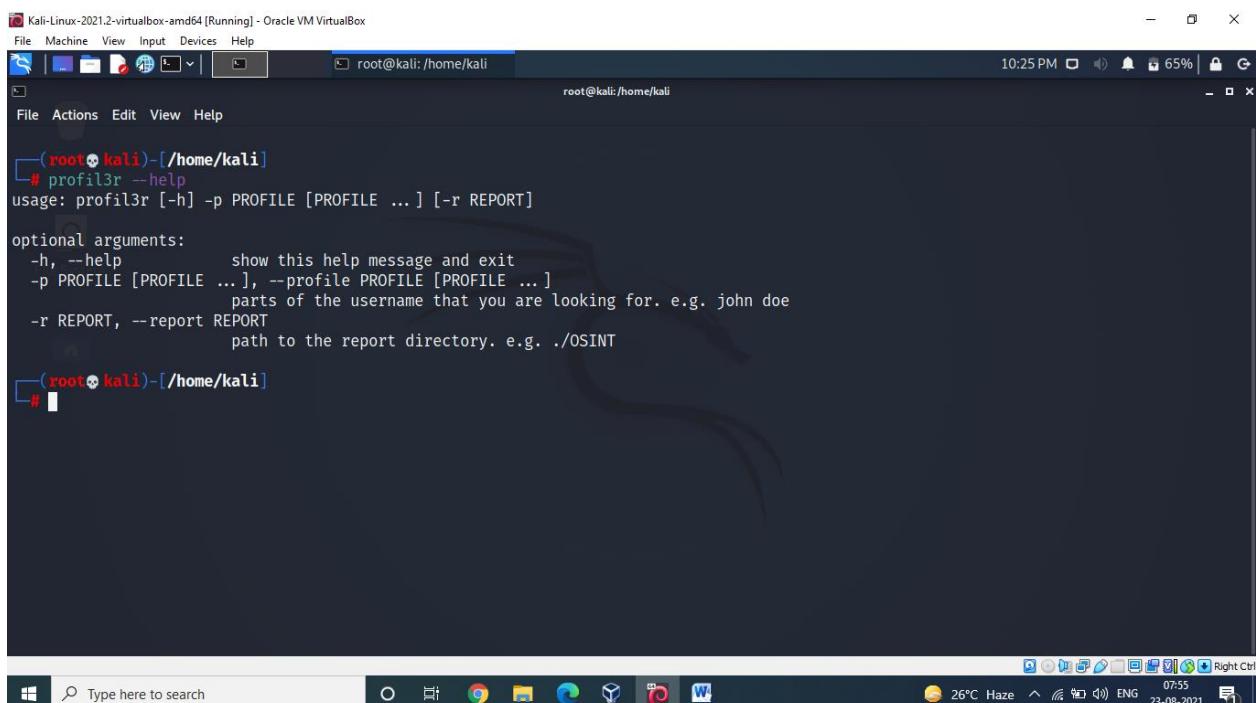
Type here to search 0 26°C Haze 07:52 23-08-2021 Right Ctrl

Installing Profil3r in Kali Linux



```
(root㉿kali)-[~/home/kali]
# pip3 install profil3r
Collecting profil3r
  Downloading profil3r-1.4.8-py3-none-any.whl (69 kB)
    ██████████| 69 kB 4.7 MB/s
Collecting pwncdpasswords<3.0.0,>2.0.0
  Downloading pwncdpasswords-2.0.0-py2.py3-none-any.whl (13 kB)
Collecting Jinja2<4.0.0,>3.0.1
  Downloading Jinja2-3.0.1-py3-none-any.whl (133 kB)
    ██████████| 133 kB 4.5 MB/s
Collecting PyInquirer==1.0.3
  Downloading PyInquirer-1.0.3.tar.gz (27 kB)
Requirement already satisfied: requests<3.0.0,>2.25.1 in /usr/lib/python3/dist-packages (from profil3r) (2.25.1)
Requirement already satisfied: beautifulsoup4<5.0.0,>4.9.3 in /usr/lib/python3/dist-packages (from profil3r) (4.9.3)
Collecting argparse<2.0.0,>1.4.0
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: Pygments≥2.2.0 in /usr/lib/python3/dist-packages (from PyInquirer==1.0.3→profil3r) (2.7.1)
Collecting prompt_toolkit==1.0.14
  Downloading prompt_toolkit-1.0.14-py3-none-any.whl (248 kB)
    ██████████| 248 kB 5.4 MB/s
Collecting regex≥2016.11.21
  Downloading regex-2021.8.21-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (760 kB)
    ██████████| 760 kB 6.1 MB/s
Requirement already satisfied: wcwidth in /usr/lib/python3/dist-packages (from prompt_toolkit==1.0.14→PyInquirer==1.0.3→profil3r) (0
```

To know how the tool Works



```
(root㉿kali)-[~/home/kali]
# profil3r --help
usage: profil3r [-h] -p PROFILE [PROFILE ...] [-r REPORT]

optional arguments:
-h, --help            show this help message and exit
-p PROFILE [PROFILE ...], --profile PROFILE [PROFILE ...]
                     parts of the username that you are looking for. e.g. john doe
-r REPORT, --report REPORT
                     path to the report directory. e.g. ./OSINT
```

Profil3r

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~/home/kali]
# profil3r -p pratik pakhare

Version 1.4.8 - Developed by Rog3rSmith
You can buy me a coffee at : https://www.buymeacoffee.com/givocefo

Select separators []
Select services done (5 selections)
[+] 6 permutations to test for each service, you can reduce this number by selecting less options if it takes too long

Profil3r will search :
[+] twitter
[+] instagram
[+] facebook
[+] steam
[+] github

root@kali:/home/kali
08:00 26°C Haze ENG 23-08-2021 Right Ctrl
```

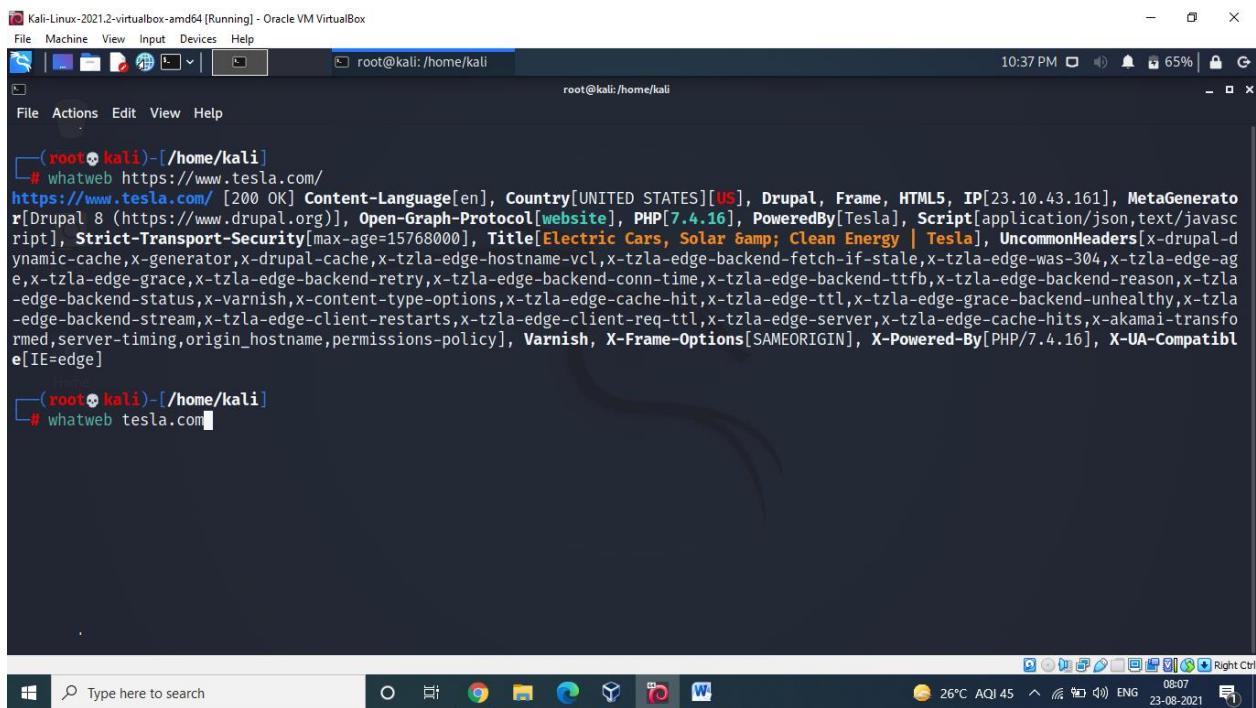
```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Trash
TWITTER ✓
└─ https://twitter.com/pratik
    └─ Full Name : Pratik Prasad
        └─ Username : @pratik
            └─ Tweets : 294
                └─ Following : 1376
                    └─ Followers : 441
                        └─ Likes : 2392
└─ https://twitter.com/pakhare
    └─ Full Name : nitin m pakhare
        └─ Username : @pakhare
            └─ Bio : God is good all the time
                └─ Tweets : 8
                    └─ Following : 8
                        └─ Followers : 5
                            └─ Likes : 5
└─ https://twitter.com/pratikpakhare
    └─ Full Name : Pratik pakhare
        └─ Username : @PratikPakhare
            └─ Tweets : 2
                └─ Following : 4
                    └─ Followers : 1
                        └─ Likes : 4
root@kali:/home/kali
08:01 26°C Haze ENG 23-08-2021 Right Ctrl
```

```
FACEBOOK ✓
└─ https://facebook.com/pratik
└─ https://facebook.com/pakhare
└─ https://facebook.com/pratikpakhare
└─ https://facebook.com/pratik_pakhare
└─ https://facebook.com/pakhare_pratik

STEAM ✓
└─ https://steamcommunity.com/id/pratik

GITHUB ✓
└─ https://github.com/pratik
    └─ Full Name : Pratik Sethia
        └─ Followers : 4
            └─ Following : 0
                └─ stars : 73
                    └─ Website : http://www.pratiksethia.com
                        └─ Location : India
                └─ https://github.com/pakhare
```

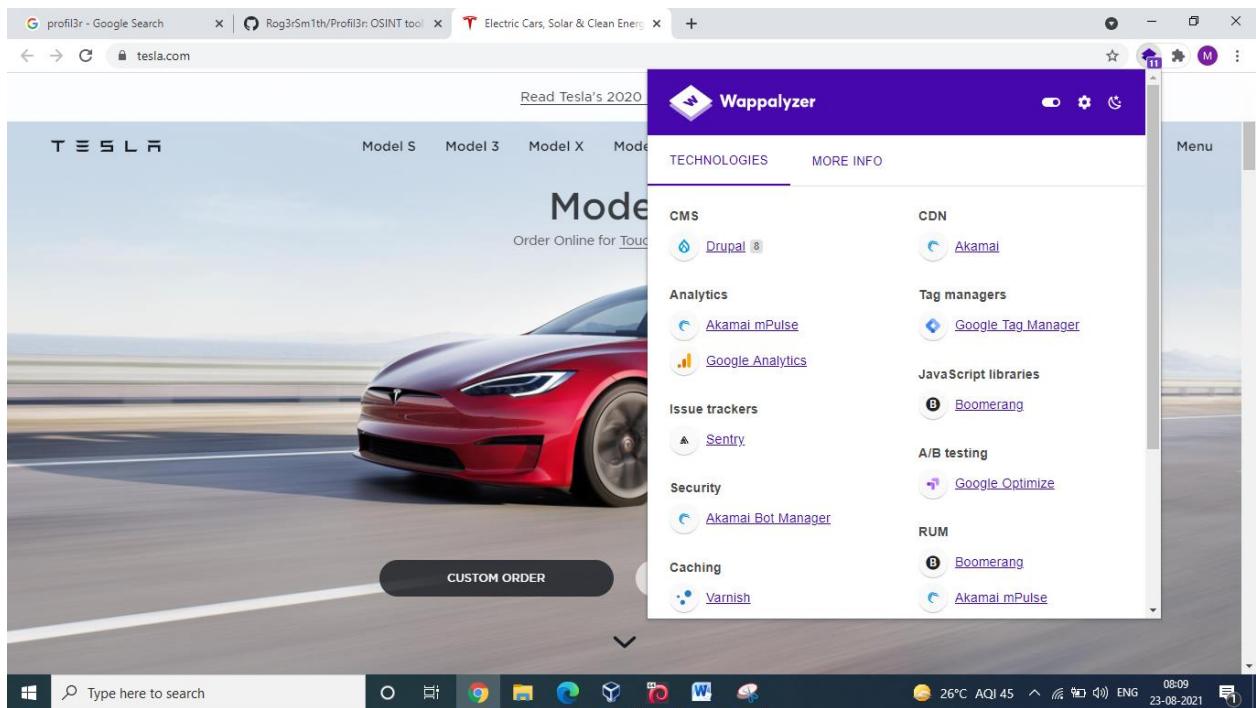
Whatweb



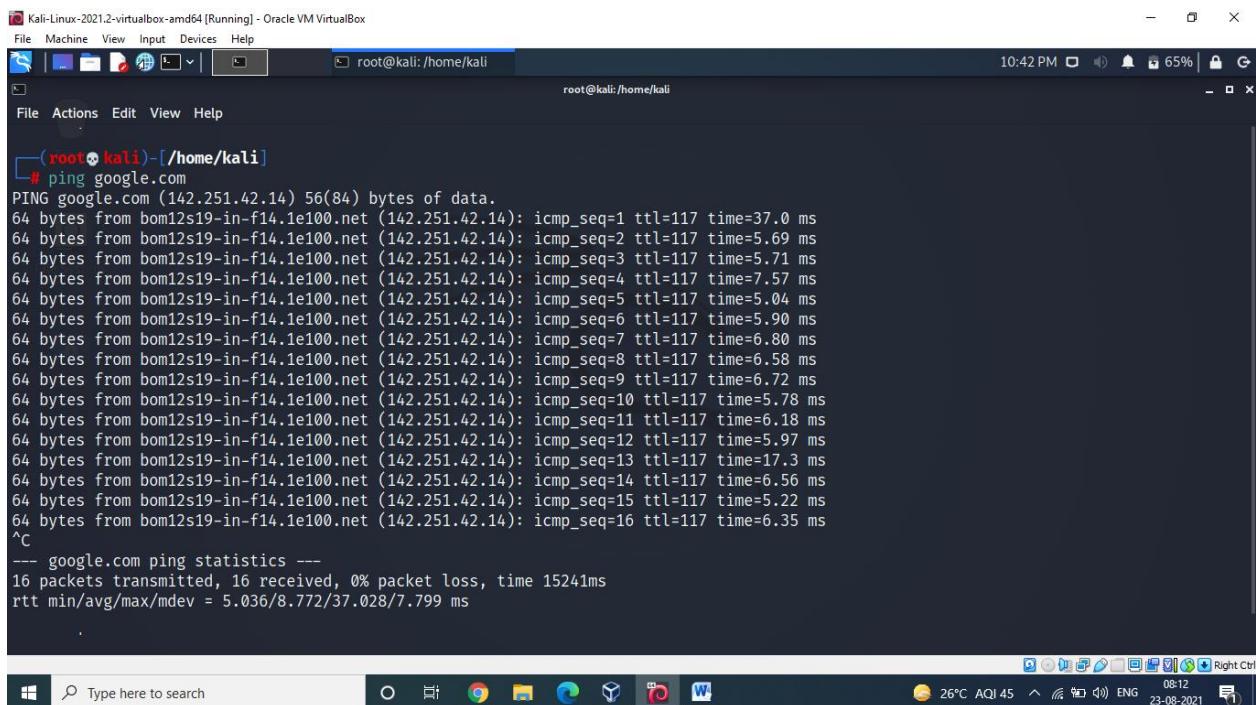
```
(root㉿kali)-[~/home/kali]
# whatweb https://www.tesla.com/
https://www.tesla.com/ [200 OK] Content-Language[en], Country[UNITED STATES][US], Drupal, Frame, HTML5, IP[23.10.43.161], MetaGenerator[Drupal 8 (https://www.drupal.org)], Open-Graph-Protocol[website], PHP[7.4.16], PoweredBy[Tesla], Script[application/json;text/javascript], Strict-Transport-Security[max-age=15768000], Title[Electric Cars, Solar & Clean Energy | Tesla], UncommonHeaders[x-drupal-dynamic-cache,x-generator,x-drupal-cache,x-tzla-edge-hostname-vcl,x-tzla-edge-backend-fetch-if-stale,x-tzla-edge-was-304,x-tzla-edge-ag-e,x-tzla-edge-grace,x-tzla-edge-backend-retry,x-tzla-edge-backend-conn-time,x-tzla-edge-backend-ttfb,x-tzla-edge-backend-reason,x-tzla-edge-backend-status,x-varnish,x-content-type-options,x-tzla-edge-cache-hit,x-tzla-edge-ttl,x-tzla-edge-grace-backend-unhealthy,x-tzla-edge-backend-stream,x-tzla-edge-client-restarts,x-tzla-edge-client-req-ttl,x-tzla-edge-server,x-tzla-edge-cache-hits,x-akamai-transferred,server-timing,origin_hostname,permissions-policy], Varnish, X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/7.4.16], X-UA-Compatible[IE=edge]

(root㉿kali)-[~/home/kali]
# whatweb tesla.com
```

**Technologies used to build a website?
Download Wappalyzer Chrome Extension.**

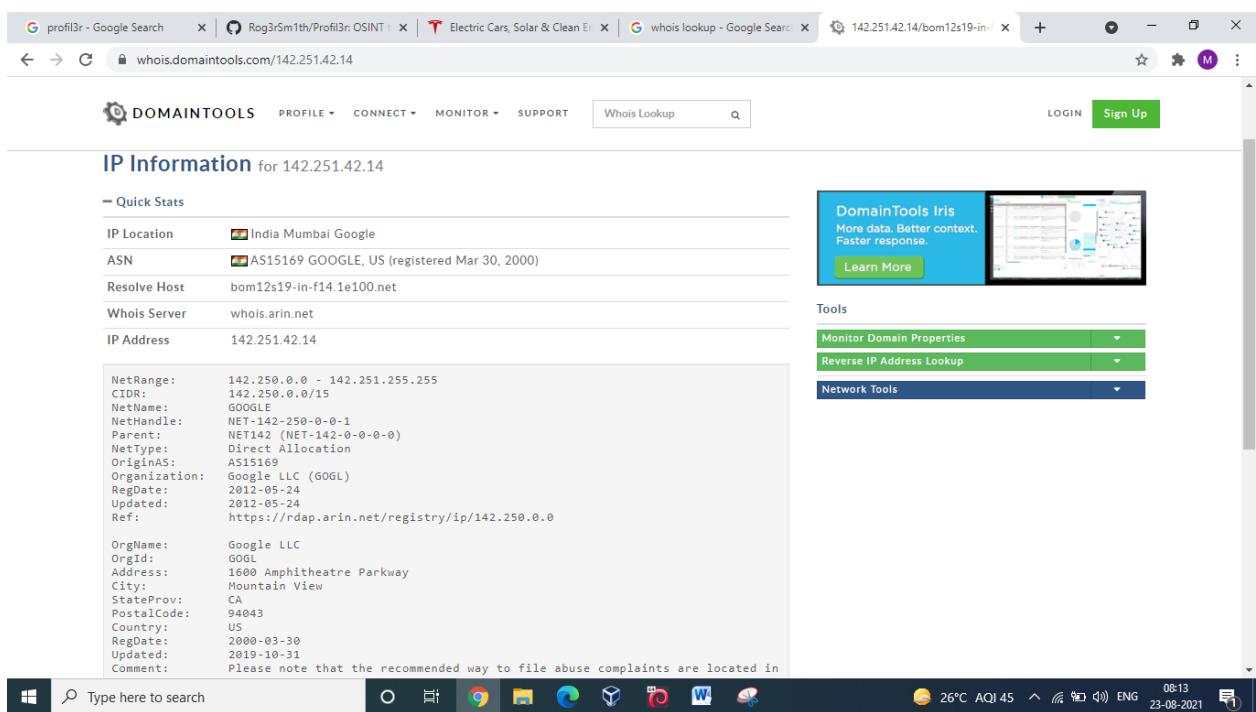


To find IP address of any Website



```
(root㉿kali)-[~/home/kali]
# ping google.com
PING google.com (142.251.42.14) 56(84) bytes of data.
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=1 ttl=117 time=37.0 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=2 ttl=117 time=5.69 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=3 ttl=117 time=5.71 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=4 ttl=117 time=7.57 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=5 ttl=117 time=5.04 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=6 ttl=117 time=5.90 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=7 ttl=117 time=6.80 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=8 ttl=117 time=6.58 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=9 ttl=117 time=6.72 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=10 ttl=117 time=5.78 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=11 ttl=117 time=6.18 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=12 ttl=117 time=5.97 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=13 ttl=117 time=17.3 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=14 ttl=117 time=6.56 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=15 ttl=117 time=5.22 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=16 ttl=117 time=6.35 ms
^C
--- google.com ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15241ms
rtt min/avg/max/mdev = 5.036/8.772/37.028/7.799 ms
```

Whois Lookup



IP Information for 142.251.42.14

Quick Stats	
IP Location	India Mumbai Google
ASN	AS15169 GOOGLE, US (registered Mar 30, 2000)
Resolve Host	bom12s19-in-f14.1e100.net
Whois Server	whois.arin.net
IP Address	142.251.42.14

NetRange: 142.250.0.0 - 142.251.255.255
CIDR: 142.250.0.0/15
NetName: GOOGLE
NetHandle: NET-142-250-0-0-1
Parent: NET142 (NET-142-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS15169
Organization: Google LLC (GOGL)
RegDate: 2012-05-24
Updated: 2012-05-24
Ref: https://rdap.arin.net/registry/ip/142.250.0.0

OrgName: Google LLC
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2019-10-31
Comment: Please note that the recommended way to file abuse complaints are located in

DomainTools Iris
More data. Better context.
Faster response.
[Learn More](#)

Tools

- Monitor Domain Properties
- Reverse IP Address Lookup
- Network Tools

How to find Subdomains of any Domain?

```
(root㉿kali)-[~/home/kali]
# sublist3r -d google.com

# Coded By Ahmed Aboul-Ela - @aboula3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..

1.google.com
alt1.i.google.com
alt.aspmx.1.google.com
client.1.google.com
clients.1.google.com
gmail-smtp-mas.1.google.com
misc-anycast.1.google.com
167.179.108.100.google.com
100-cache-blicnet.google.com
101-cache-blicnet.google.com
102-cache-blicnet.google.com
34.14.230.103.google.com
96.60.68.103.google.com
5.61.68.103.google.com
```

```
virtual.google.com
vm_0.google.com
vpls-gw.google.com
vpn.google.com
vps-122302.google.com
vps87406.google.com
vuua.google.com
wa.google.com
weblocal.google.com
welh.google.com
who.google.com
wifi.google.com
```

```
google-proxy-66-249-81-13.google.com
google-proxy-66-249-81-130.google.com
google-proxy-66-249-81-131.google.com
google-proxy-66-249-81-132.google.com
google-proxy-66-249-81-133.google.com
google-proxy-66-249-81-134.google.com
google-proxy-66-249-81-135.google.com
google-proxy-66-249-81-136.google.com
google-proxy-66-249-81-137.google.com
google-proxy-66-249-81-138.google.com
google-proxy-66-249-81-139.google.com
google-proxy-66-249-81-14.google.com
google-proxy-66-249-81-140.google.com
google-proxy-66-249-81-141.google.com
google-proxy-66-249-81-142.google.com
google-proxy-66-249-81-143.google.com
google-proxy-66-249-81-144.google.com
google-proxy-66-249-81-145.google.com
google-proxy-66-249-81-146.google.com
google-proxy-66-249-81-147.google.com
google-proxy-66-249-81-148.google.com
google-proxy-66-249-81-149.google.com
google-proxy-66-249-81-15.google.com
google-proxy-66-249-81-150.google.com
google-proxy-66-249-81-151.google.com
```

To find Emails (hunter.io)

hunter

Product ▾ Pricing Resources ▾

Sign in Sign up

tesla.com Find email addresses

Most common pattern: {first}{last}@tesla.com 323 email addresses

t_muelsen@tesla.com 1 source ▾

b_eghan@tesla.com 10 sources ▾

p_gzhang@tesla.com 3 sources ▾

f_cher@tesla.com 5 sources ▾

r_aaja@tesla.com 5 sources ▾

318 more results for "tesla.com"

Type here to search

27°C Haze 08:25 23-08-2021

To check your Email has been compromised or not?

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email or phone is in a data breach

ppratik1307@gmail.com pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security Start using 1Password.com

Type here to search

27°C Haze 08:28 23-08-2021

To find Directories and folders in website..

1)dirsearch

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~/Desktop/dirsearch]
# l
banner.txt CONTRIBUTORS.md default.conf Dockerfile lib/ README.md requirements.txt setup.py* thirdparty/
CHANGELOG.md db/ dirsearch.py* __init__.py* logs/ reports/ setup.cfg static/
(root@kali)-[~/Desktop/dirsearch]
# python3 dirsearch.py -u https://www.udemy.com/
dirsearch v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10916
Output File: /home/kali/Desktop/dirsearch/reports/www.udemy.com/-_21-08-22_23-11-12.txt
Error Log: /home/kali/Desktop/dirsearch/logs/errors-21-08-22_23-11-12.log

Target: https://www.udemy.com/

[23:11:13] Starting:
[23:11:18] 403 - 123B - /html.old
[23:11:18] 403 - 123B - /php.old
[23:11:18] 403 - 123B - /!.htaccess
[23:11:18] 403 - 123B - /html.bak
```

2)dirb

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~/kali]
# dirb https://www.udemy.com/
DIRB v2.22
By The Dark Raver

START_TIME: Sun Aug 22 23:15:49 2021
URL_BASE: https://www.udemy.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

HOME

GENERATED WORDS: 4612
---- Scanning URL: https://www.udemy.com/
+ https://www.udemy.com/.bash_history (CODE:403|SIZE:123)
+ https://www.udemy.com/.bashrc (CODE:403|SIZE:123)
+ https://www.udemy.com/.cvs (CODE:403|SIZE:123)
+ https://www.udemy.com/.htaccess (CODE:403|SIZE:123)
+ https://www.udemy.com/.htpasswd (CODE:403|SIZE:123)
```

To check open IPs in our Network.

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:/home/kali

11:26 PM 65% 65%

File Actions Edit View Help

```
(root@kali)-[~/home/kali]
# nmap -sn 10.2.0.0
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-22 23:23 EDT
Nmap scan report for 10.2.0.0
Host is up (0.0011s latency).
Nmap scan report for 10.2.0.1
Host is up (0.0021s latency).
Nmap scan report for 10.2.0.2
Host is up (0.0020s latency).
Nmap scan report for 10.2.0.3
Host is up (0.00097s latency).
Nmap scan report for 10.2.0.4
Host is up (0.00090s latency).
Nmap scan report for 10.2.0.5
Host is up (0.0022s latency).
Nmap scan report for 10.2.0.6
Host is up (0.0022s latency).
Nmap scan report for 10.2.0.7
Host is up (0.0032s latency).
Nmap scan report for 10.2.0.8
Host is up (0.0032s latency).
Nmap scan report for 10.2.0.9
Host is up (0.0011s latency).
Nmap scan report for 10.2.0.10
```

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    group default qlen 1000
    link/ether 08:00:27:0e:34:8d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 81745sec preferred_lft 81745sec
        inet6 fe80::a0:27ff:fe0e:348d/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

Type here to search 28°C Haze 08:56 ENG 23-08-2021 Right Ctrl

Basic Nmap Scan on My Windows Operating Systems.

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:/home/kali

11:32 PM 65% 65%

File Actions Edit View Help

```
(root@kali)-[~/home/kali]
# nmap 192.168.56.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-22 23:31 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0083s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5800/tcp   open  vnc-http
5900/tcp   open  vnc
12345/tcp  open  netbus

Nmap done: 1 IP address (1 host up) scanned in 5.23 seconds
```

File Actions Edit View Help

```
(root@kali)-[~/home/kali]
#
```

Type here to search 28°C Haze 09:02 ENG 23-08-2021 Right Ctrl

Nmap scans with versions.

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:[/home/kali]
nmap 192.168.56.1 -sV
Starting Nmap 7.91 (https://nmap.org) at 2021-08-22 23:37 EDT
Nmap scan report for 192.168.56.1
Host is up (0.016s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5800/tcp open vnc-http RealVNC E4
5900/tcp open vnc RealVNC Enterprise (protocol 4.1)
12345/tcp open netbus?
Service Info: Host: DESKTOP-61B0L42; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 82.30 seconds

root@kali:[/home/kali]
#

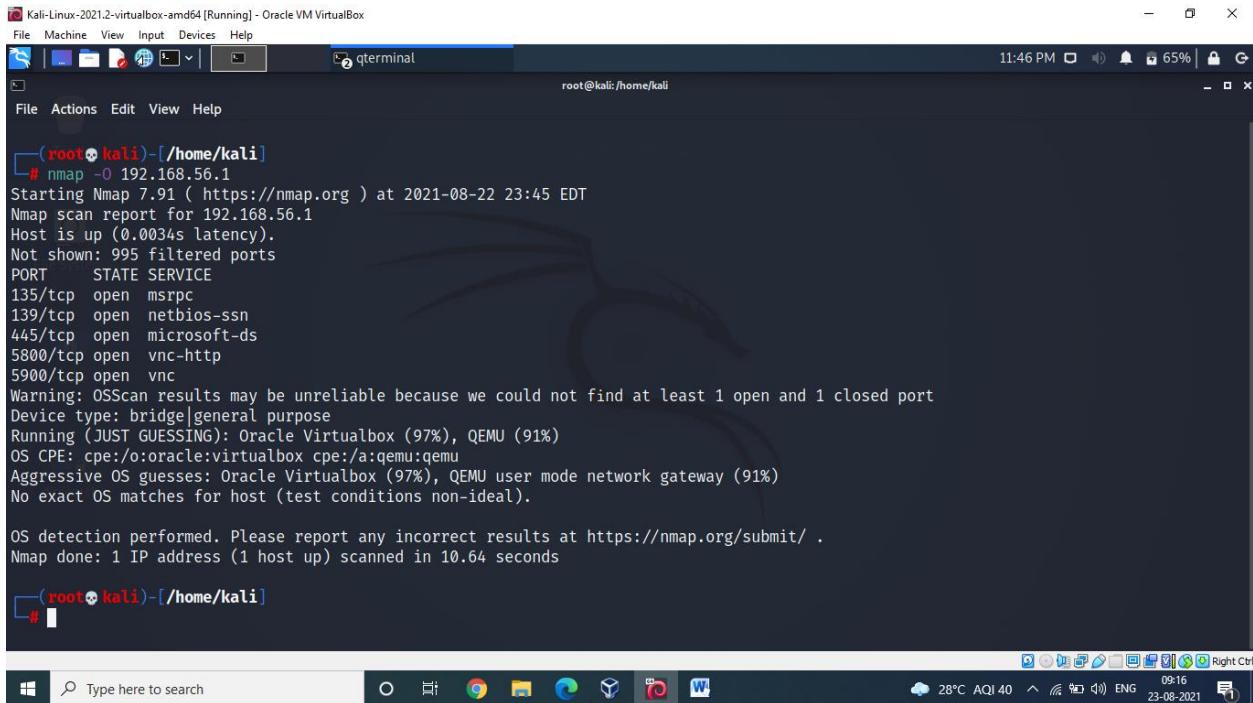
Stealth Scan

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:[/home/kali]
nmap -sS 192.168.56.1
Starting Nmap 7.91 (https://nmap.org) at 2021-08-22 23:42 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0055s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5800/tcp open vnc-http
5900/tcp open vnc

Nmap done: 1 IP address (1 host up) scanned in 6.25 seconds

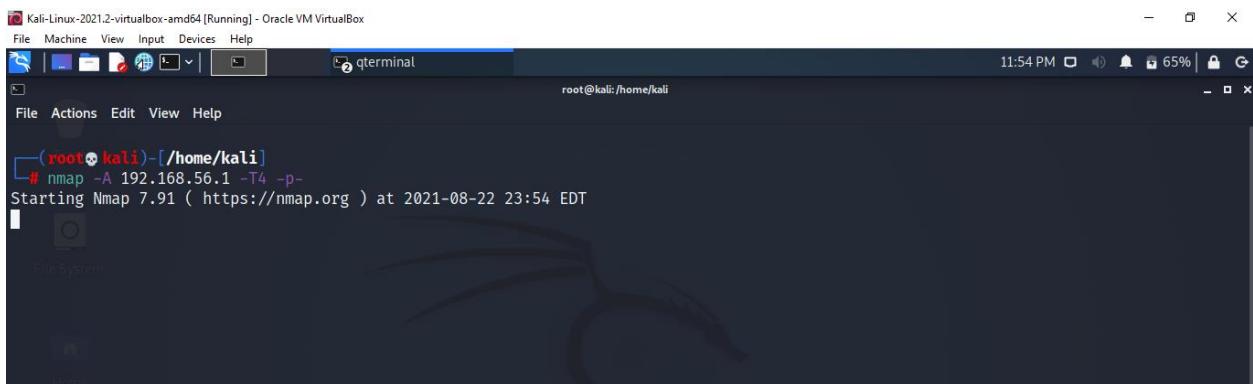
root@kali:[/home/kali]
#

Operating systems Scan



Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:[/home/kali]
nmap -O 192.168.56.1
Starting Nmap 7.91 (https://nmap.org) at 2021-08-22 23:45 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0034s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5800/tcp open vnc-http
5900/tcp open vnc
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (91%)
No exact OS matches for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 10.64 seconds
root@kali:[/home/kali]
#

Complete Scan



Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:[/home/kali]
nmap -A 192.168.56.1 -T4 -p-
Starting Nmap 7.91 (https://nmap.org) at 2021-08-22 23:54 EDT
#

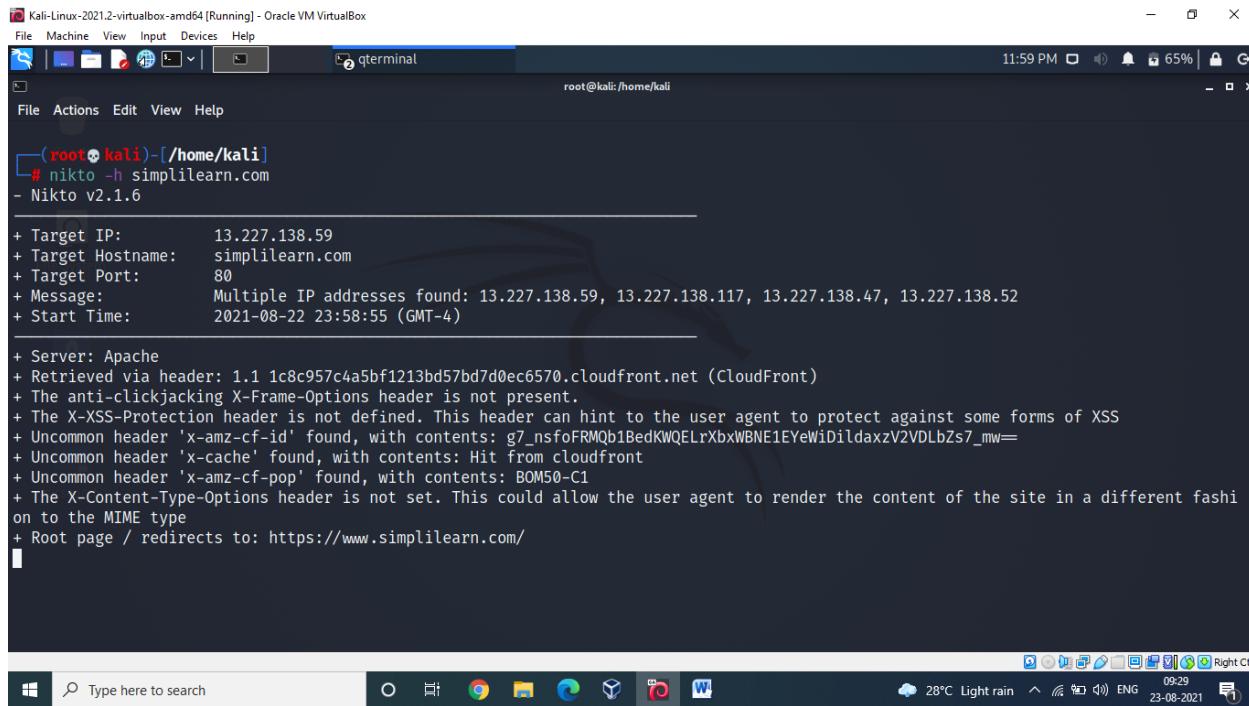
To find everything about that IP address

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~/home/kali]
# nmap -A 192.168.56.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-22 23:47 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00071s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
5800/tcp   open  vnc-http     RealVNC E4
|_http-server-header: RealVNC/E4
|_http-title: VNC Viewer for Java
5900/tcp   open  vnc        RealVNC Enterprise (protocol 4.1)
| vnc-info:
|   Protocol version: 004.001
|   Security types:
|     Unknown security type (13)
|     Unknown security type (133)
|     RA2 (5)
|     Unknown security type (129)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
Type here to search  09:19 28°C Light rain ENG 23-08-2021 Right Ctrl
```

```
Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Host script results:
clock-skew: mean: -1h49m58s, deviation: 3h10m29s, median: 0s
smb-os-discovery:
OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
OS CPE: cpe:/o:microsoft:windows_10::-
Computer name: DESKTOP-61B0L42
NetBIOS computer name: DESKTOP-61B0L42\x00
Workgroup: WORKGROUP\x00
System time: 2021-08-23T09:17:57+05:30
smb-security-mode:
account_used: guest
authentication_level: user
challenge_response: supported
message_signing: disabled (dangerous, but default)
smb2-security-mode:
2.02:
Message signing enabled but not required
smb2-time:
date: 2021-08-23T03:47:58
start_date: N/A
TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.14 ms 10.0.2.2
Type here to search  09:19 28°C Light rain ENG 23-08-2021 Right Ctrl
```

```
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DESKTOP-61B0L42; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nikto Vulnerability Scanner

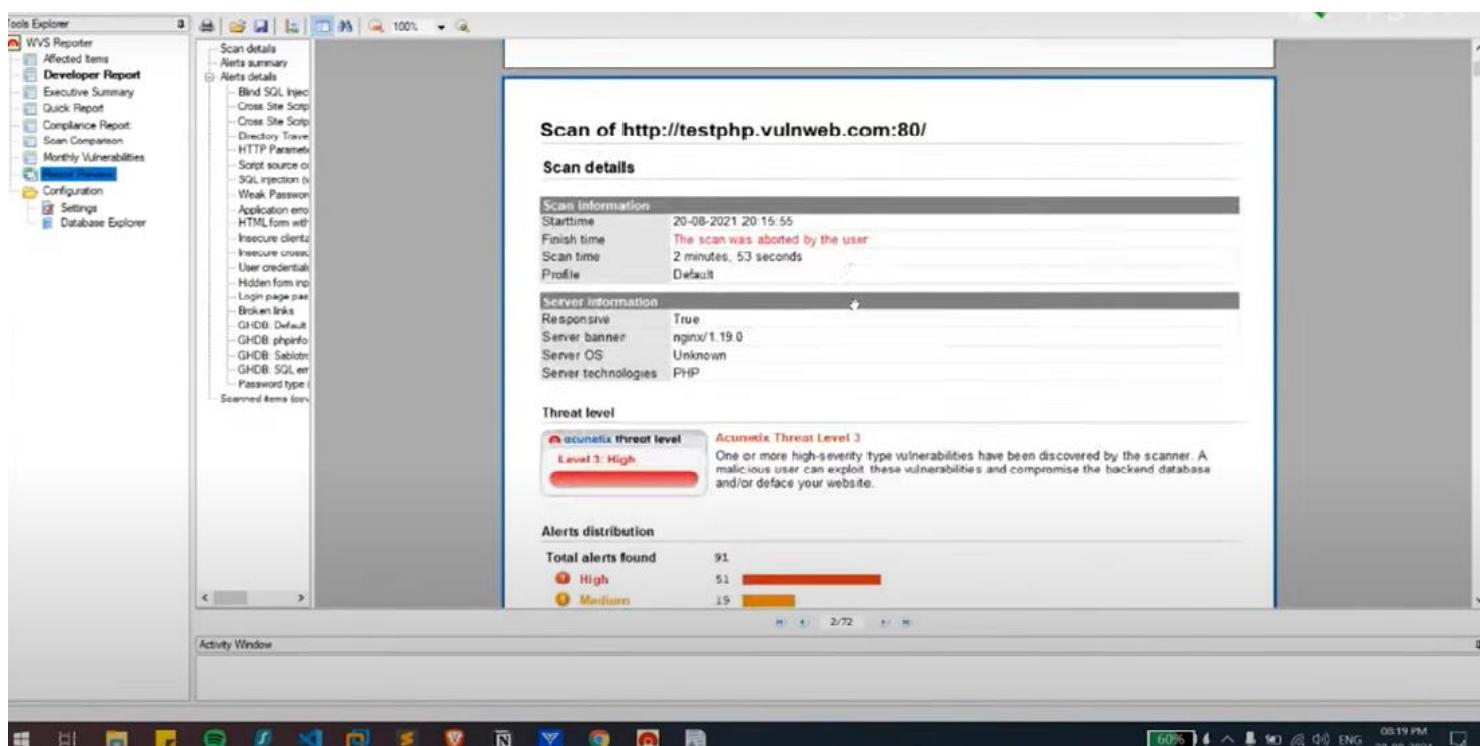


```
(root㉿kali)-[~/home/kali]
# nikto -h simplilearn.com
- Nikto v2.1.6

+ Target IP:          13.227.138.59
+ Target Hostname:    simplilearn.com
+ Target Port:        80
+ Message:           Multiple IP addresses found: 13.227.138.59, 13.227.138.117, 13.227.138.47, 13.227.138.52
+ Start Time:         2021-08-22 23:58:55 (GMT-4)

+ Server: Apache
+ Retrieved via header: 1.1c8c957c4a5bf1213bd57bd7d0ec6570.cloudfront.net (CloudFront)
+ 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
+ Uncommon header 'x-amz-cf-id' found, with contents: g7_nsfoFRMqb1BedKQELrXbxWBNE1EYeWiDildaxzV2VLbZs7_mw==
+ Uncommon header 'x-cache' found, with contents: Hit from cloudfront
+ Uncommon header 'x-amz-cf-pop' found, with contents: BOM50-C1
+ 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 on to the MIME type
+ Root page / redirects to: https://www.simplilearn.com/
```

Acunetix web vulnerability scanner



The screenshot shows the Acunetix Web Vulnerability Scanner interface. On the left, there's a sidebar with navigation links like 'Affected items', 'Developer Report', 'Executive Summary', 'Quick Report', 'Compliance Report', 'Scan Comparison', 'Monthly Vulnerabilities', 'Configuration', 'Settings', and 'Database Explorer'. The main panel displays a scan report for the URL <http://testphp.vulnweb.com:80/>. The 'Scan details' section shows the following information:

Scan information	Value
Start time	20-08-2021 20:15:55
Finish time	The scan was aborted by the user
Scan time	2 minutes, 53 seconds
Profile	Default

The 'Server information' section lists:

Information	Value
Responsive	True
Server banner	nginx/1.19.0
Server OS	Unknown
Server technologies	PHP

The 'Threat level' section indicates a threat level of **Level 3: High** (Acunetix Threat Level 3), with a note: "One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website."

The 'Alerts distribution' section shows the total alerts found: 91, with a breakdown: 51 High and 19 Medium.