CHOO YONG HAN

Assignment-2:Practice all the things that are taught today and note down the findings.

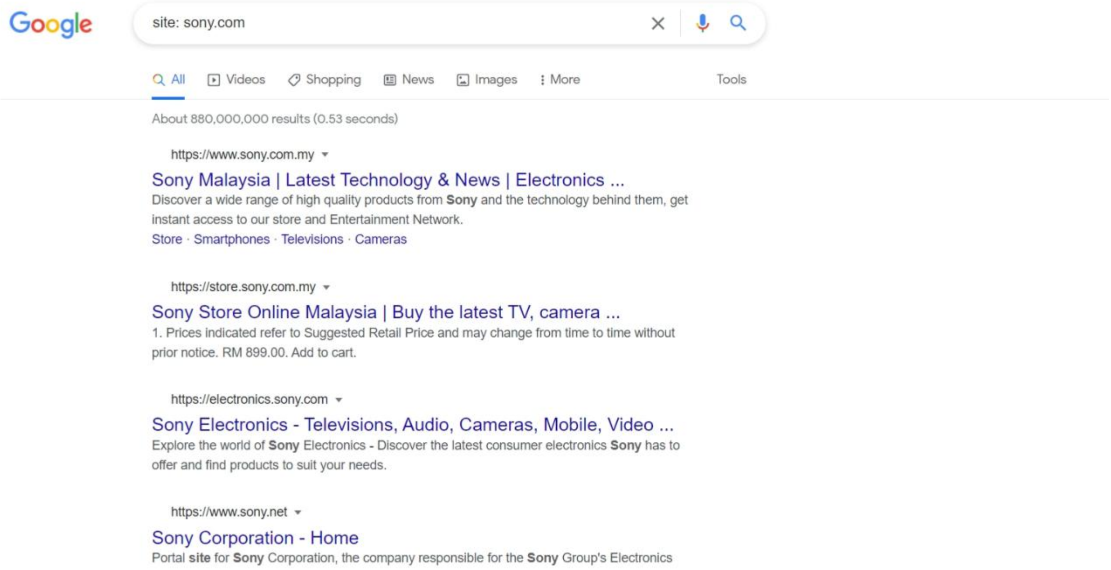
1.INFORMATION GATHERING

Information gathering(also known as recon), there are 2 recons, which are active recon and passive recon

First technique is Google Dorking. It is used to optimize the searching result. There are few ways to perform Google Dorking. Here I will use sony as my example to perform Google Dorking.

(i) Google Dorking

(a) site: sony.com(looking for result that related to domain sony.com only)



site: sony.com

About 880,000,000 results (0.53 seconds)

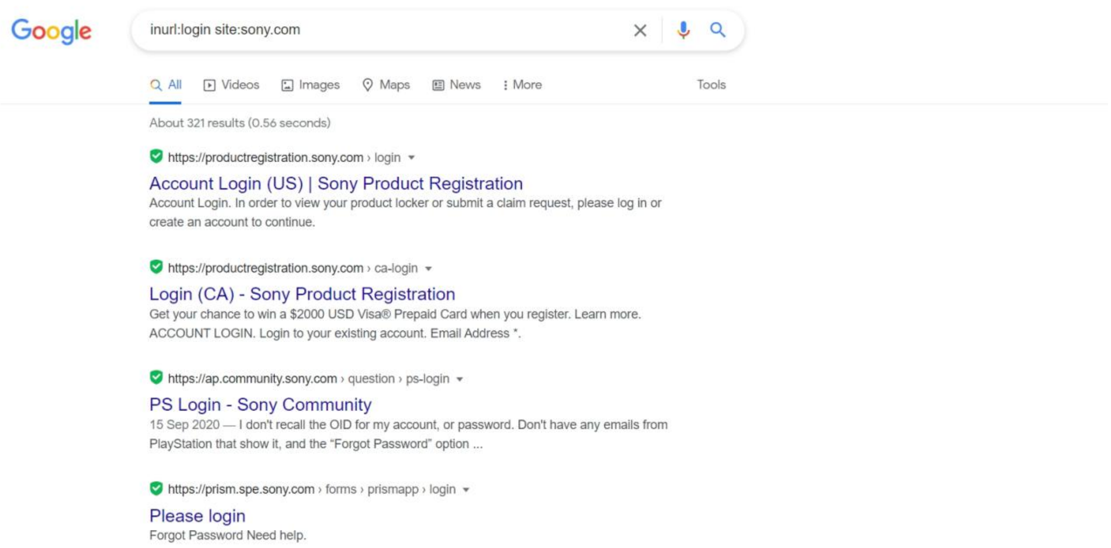
https://www.sony.com.my
Sony Malaysia | Latest Technology & News | Electronics ...
Discover a wide range of high quality products from Sony and the technology behind them, get instant access to our store and Entertainment Network.
Store · Smartphones · Televisions · Cameras

https://store.sony.com.my
Sony Store Online Malaysia | Buy the latest TV, camera ...
1. Prices indicated refer to Suggested Retail Price and may change from time to time without prior notice. RM 899.00. Add to cart.

https://electronics.sony.com
Sony Electronics - Televisions, Audio, Cameras, Mobile, Video ...
Explore the world of Sony Electronics - Discover the latest consumer electronics Sony has to offer and find products to suit your needs.

https://www.sony.net
Sony Corporation - Home
Portal site for Sony Corporation, the company responsible for the Sony Group's Electronics

(b) inurl:login site:sony.com(looking for login result in sony.com)



inurl:login site:sony.com

About 321 results (0.56 seconds)

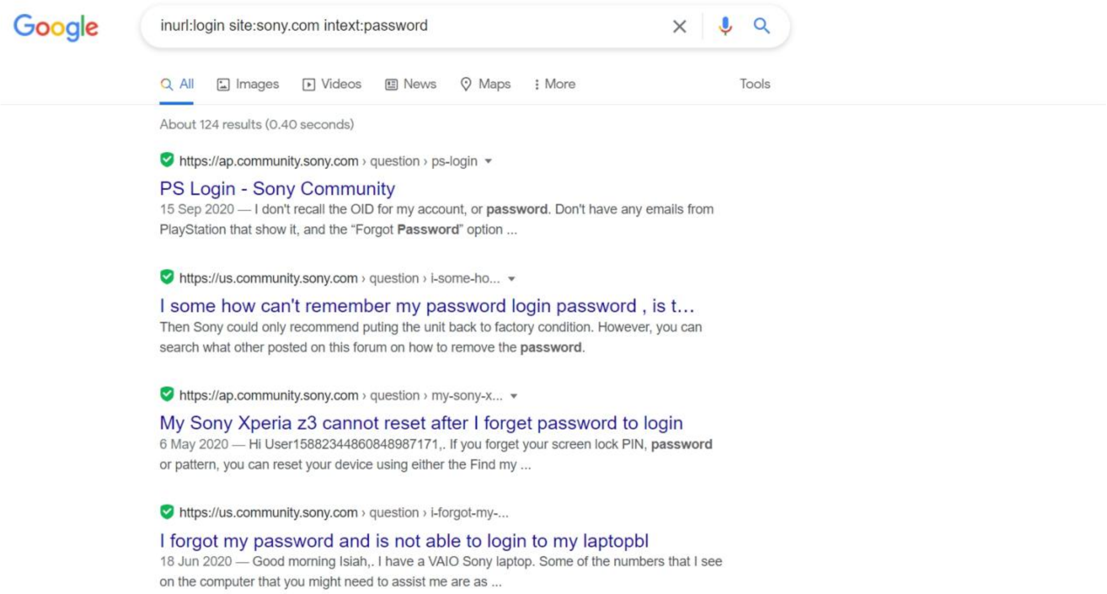
https://productregistration.sony.com › login
Account Login (US) | Sony Product Registration
Account Login. In order to view your product locker or submit a claim request, please log in or create an account to continue.

https://productregistration.sony.com › ca-login
Login (CA) - Sony Product Registration
Get your chance to win a $2000 USD Visa® Prepaid Card when you register. Learn more. ACCOUNT LOGIN. Login to your existing account. Email Address *.

https://ap.community.sony.com › question › ps-login
PS Login - Sony Community
15 Sep 2020 — I don't recall the OID for my account, or password. Don't have any emails from PlayStation that show it, and the "Forgot Password" option ...

https://prism.spe.sony.com › forms › prismapp › login
Please login
Forgot Password Need help.

(c)inurl:login site:sony.com intext:password(find “password” this keyword in login site in sony.com)



inurl:login site:sony.com intext:password

About 124 results (0.40 seconds)

https://ap.community.sony.com › question › ps-login

PS Login - Sony Community

15 Sep 2020 — I don't recall the OID for my account, or **password**. Don't have any emails from PlayStation that show it, and the “Forgot **Password**” option ...

https://us.community.sony.com › question › i-some-ho...

I some how can't remember my password login password , is t...

Then Sony could only recommend puting the unit back to factory condition. However, you can search what other posted on this forum on how to remove the **password**.

https://ap.community.sony.com › question › my-sony-x...

My Sony Xperia z3 cannot reset after I forget password to login

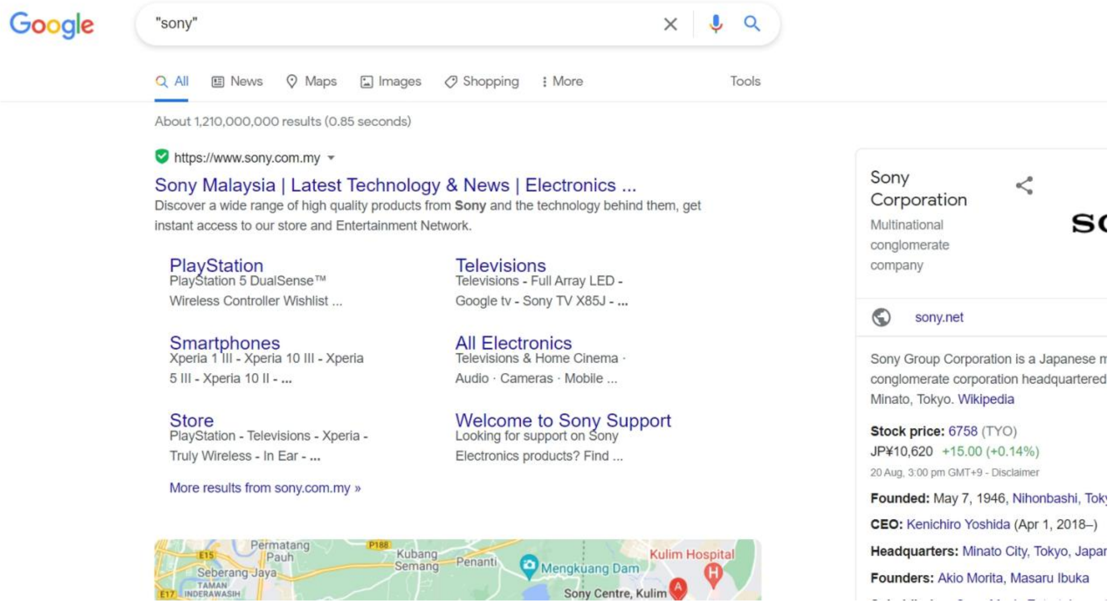
6 May 2020 — Hi User15882344860848987171,. If you forget your screen lock PIN, **password** or pattern, you can reset your device using either the Find my ...

https://us.community.sony.com › question › i-forgot-my-...

I forgot my password and is not able to login to my laptopbl

18 Jun 2020 — Good morning Isiah,. I have a VAIO Sony laptop. Some of the numbers that I see on the computer that you might need to assist me are as ...

(d)"sony"(only focus on sony)



"sony"

About 1,210,000,000 results (0.85 seconds)

https://www.sony.com.my

Sony Malaysia | Latest Technology & News | Electronics ...

Discover a wide range of high quality products from **Sony** and the technology behind them, get instant access to our store and Entertainment Network.

PlayStation
PlayStation 5 DualSense™ Wireless Controller Wishlist ...

Televisions
Televisions - Full Array LED - Google tv - Sony TV X85J - ...

Smartphones
Xperia 1 III - Xperia 10 III - Xperia 5 III - Xperia 10 II - ...

All Electronics
Televisions & Home Cinema · Audio · Cameras · Mobile ...

Store
PlayStation - Televisions - Xperia - Truly Wireless - In Ear - ...

Welcome to Sony Support
Looking for support on Sony Electronics products? Find ...

More results from sony.com.my »

Sony Corporation
Multinational conglomerate company

sony.net

Sony Group Corporation is a Japanese m conglomerate corporation headquartered Minato, Tokyo. Wikipedia

Stock price: 6758 (TYO)
JP¥10,620 +15.00 (+0.14%)
20 Aug, 3:00 pm GMT+9 - Disclaimer

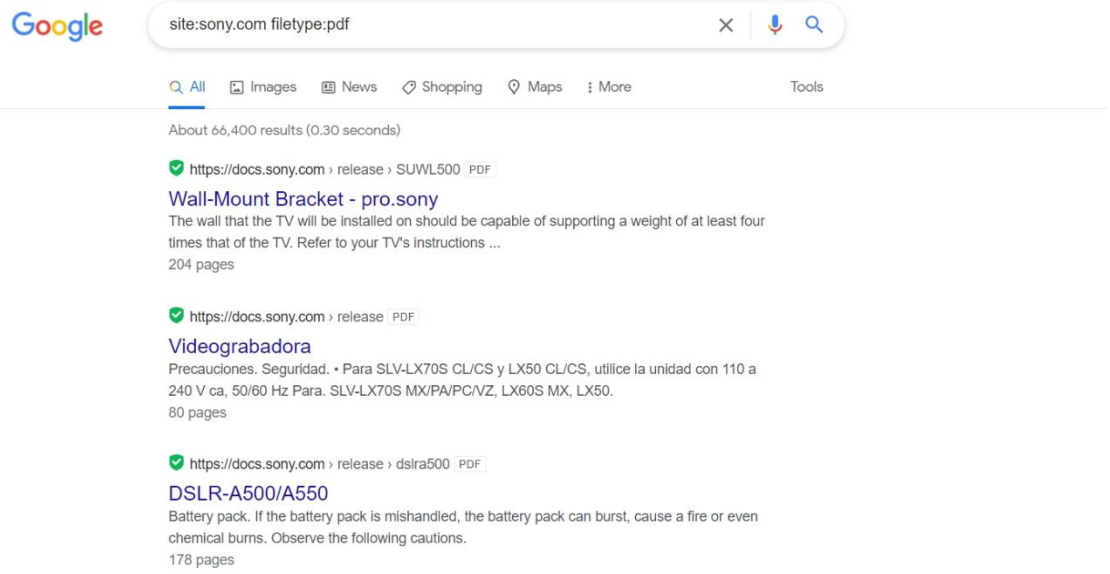
Founded: May 7, 1946, Nihonbashi, Toky

CEO: Kenichiro Yoshida (Apr 1, 2018–)

Headquarters: Minato City, Tokyo, Japar

Founders: Akio Morita, Masaru Ibuka

(e) site:sony.com filetype:pdf(search pdf filetype in domain sony.com)



About 66,400 results (0.30 seconds)

https://docs.sony.com › release › SUWL500 PDF

Wall-Mount Bracket - pro.sony

The wall that the TV will be installed on should be capable of supporting a weight of at least four times that of the TV. Refer to your TV's instructions ...

204 pages

https://docs.sony.com › release PDF

Videograbadora

Precauciones. Seguridad. • Para SLV-LX70S CL/CS y LX50 CL/CS, utilice la unidad con 110 a 240 V ca, 50/60 Hz Para. SLV-LX70S MX/PA/PC/VZ, LX60S MX, LX50.

80 pages

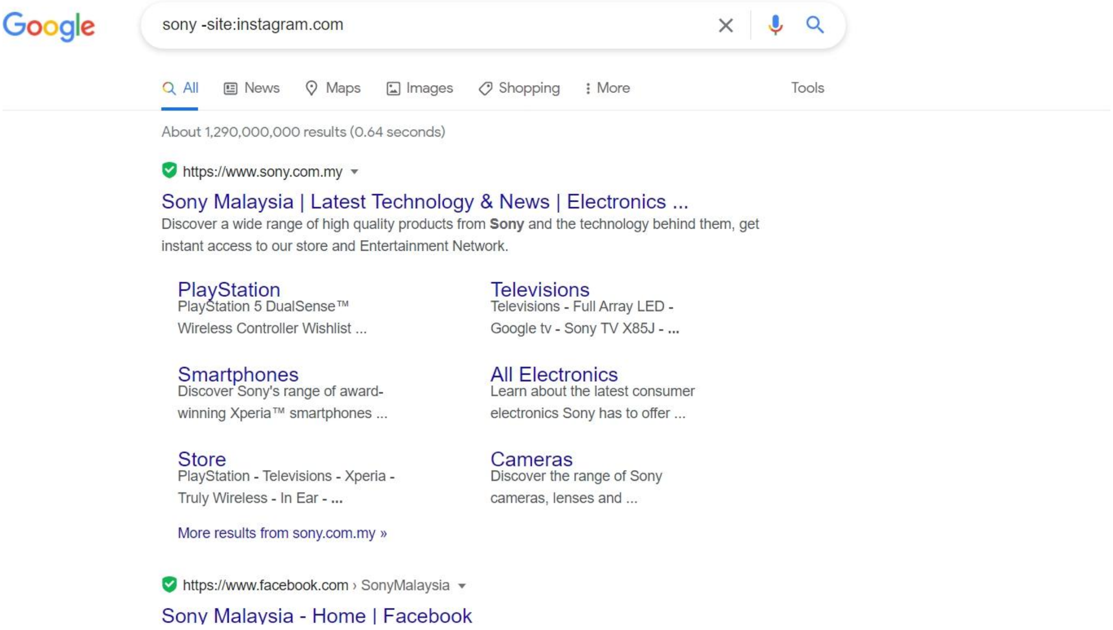
https://docs.sony.com › release › dslra500 PDF

DSLR-A500/A550

Battery pack. If the battery pack is mishandled, the battery pack can burst, cause a fire or even chemical burns. Observe the following cautions.

178 pages

(f)sony -site:instagram.com(exclude sony from instagram result)



About 1,290,000,000 results (0.64 seconds)

https://www.sony.com.my

Sony Malaysia | Latest Technology & News | Electronics ...

Discover a wide range of high quality products from **Sony** and the technology behind them, get instant access to our store and Entertainment Network.

PlayStation
PlayStation 5 DualSense™ Wireless Controller Wishlist ...

Televisions
Televisions - Full Array LED - Google tv - Sony TV X85J - ...

Smartphones
Discover Sony's range of award-winning Xperia™ smartphones ...

All Electronics
Learn about the latest consumer electronics Sony has to offer ...

Store
PlayStation - Televisions - Xperia - Truly Wireless - In Ear - ...

Cameras
Discover the range of Sony cameras, lenses and ...

More results from sony.com.my »

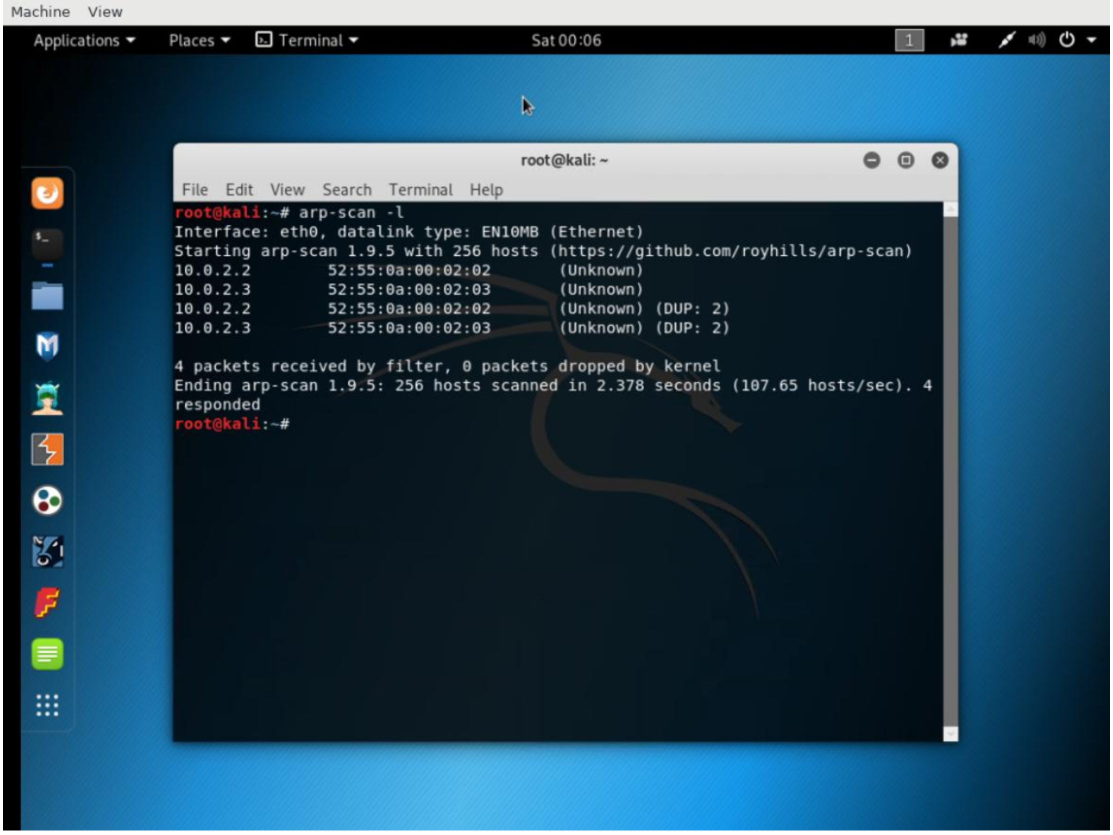
https://www.facebook.com › SonyMalaysia

Sony Malaysia - Home | Facebook

Also, Google Hacking Database also can be used to find the exploit database as shown in lecture video such as screen shown by webcam

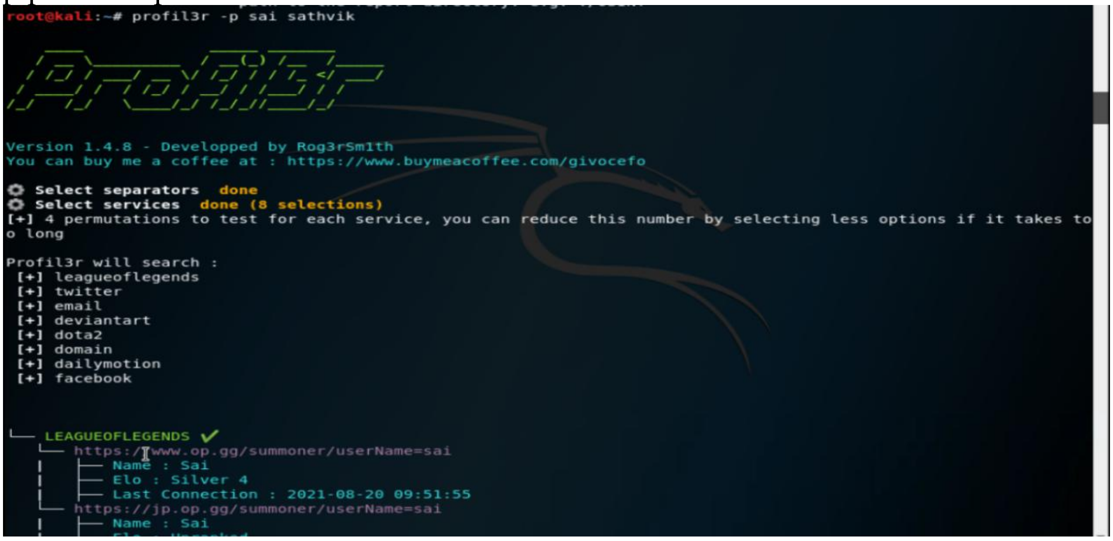
OSINT(Using Command to Perform OSINT)

(i)arp-scan -l (to scan surrounding IP address)



```
root@kali:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.2        52:55:0a:00:02:02       (Unknown)
10.0.2.3        52:55:0a:00:02:03       (Unknown)
10.0.2.2        52:55:0a:00:02:02       (Unknown) (DUP: 2)
10.0.2.3        52:55:0a:00:02:03       (Unknown) (DUP: 2)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.5: 256 hosts scanned in 2.378 seconds (107.65 hosts/sec). 4
responded
root@kali:~#
```

(ii) profil3r -p sai sathvik(find information about target eg: Mr Sai Sathvik)
*to perform this, profil3r need to be installed. The command of installing profil3r is pip3 install profil3r



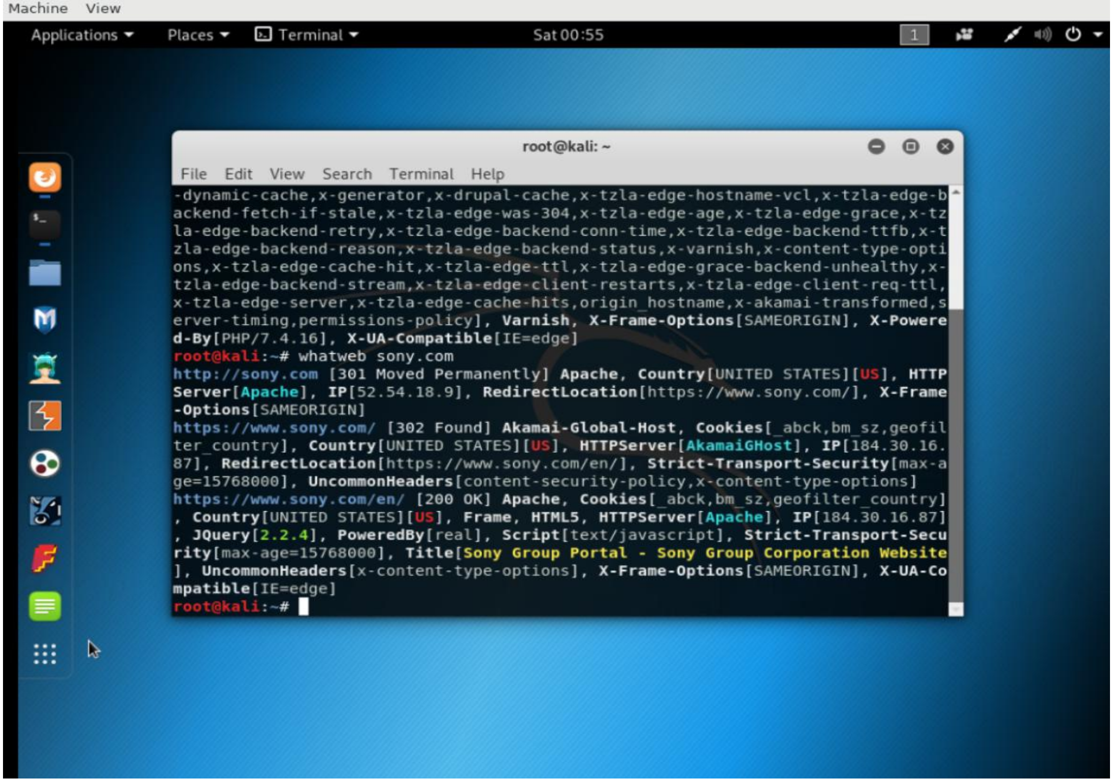
```
root@kali:~# profil3r -p sai sathvik

Version 1.4.8 - Developped by Rog3rSm1th
You can buy me a coffee at : https://www.buymeacoffee.com/givocefo

 Select separators  done
 Select services  done (8 selections)
[+] 4 permutations to test for each service, you can reduce this number by selecting less options if it takes to
o long

Profil3r will search :
 [+] leagueoflegends
 [+] twitter
 [+] email
 [+] deviantart
 [+] dota2
 [+] domain
 [+] dailymotion
 [+] facebook


└── LEAGUEOFLEGENDS ✓
    └── https://www.op.gg/summoner/userName=sai
    |    ├── Name : Sai
    |    ├── Elo : Silver 4
    |    ├── Last Connection : 2021-08-20 09:51:55
    └── https://jp.op.gg/summoner/userName=sai
    |    ├── Name : Sai
```

The result will be shown after choosing selected criteria.

Also, python3 is necessary to be installed to make sure it is able to perform more operations well that require python. The command to install python3 is sudo apt install python3.pip in terminal Kali Linux.

WEBSITE INFORMATION

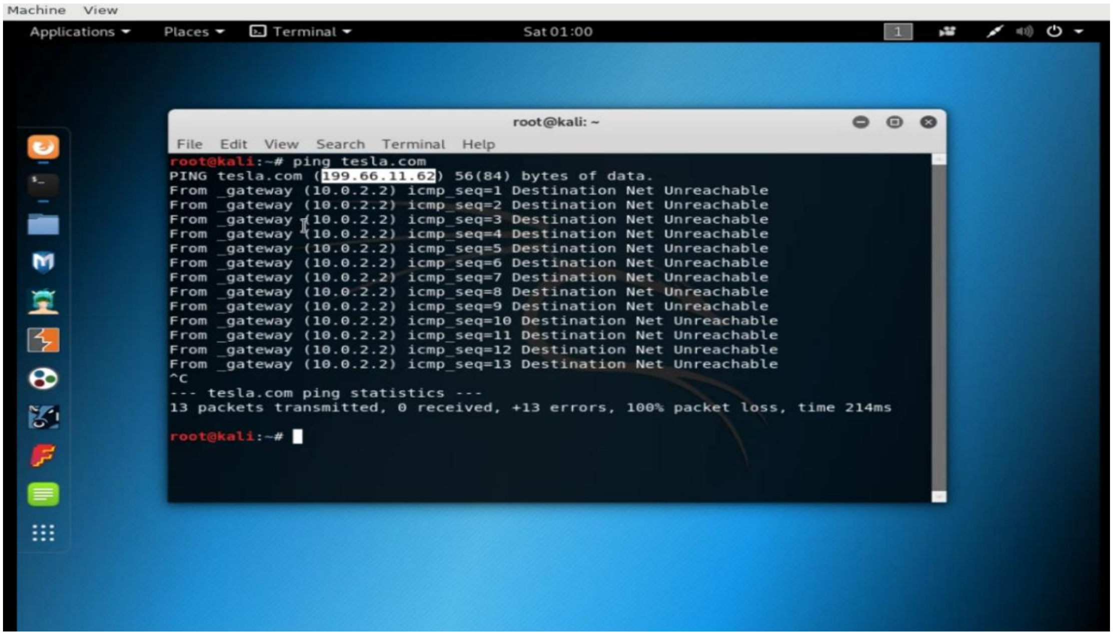
(i)whatweb sony.com (by using this, we could find the related information of this website)



```
-dynamic-cache,x-generator,x-drupal-cache,x-tzla-edge-hostname-vcl,x-tzla-edge-b
ackend-fetch-if-stale,x-tzla-edge-was-304,x-tzla-edge-age,x-tzla-edge-grace,x-tz
la-edge-backend-retry,x-tzla-edge-backend-conn-time,x-tzla-edge-backend-ttfb,x-t
zla-edge-backend-reason,x-tzla-edge-backend-status,x-varnish,x-content-type-opti
ons,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,origin_hostname,x-akamai-transformed,s
erver-timing,permissions-policy], Varnish, X-Frame-Options[SAMEORIGIN], X-Powere
d-By[PHP/7.4.16], X-UA-Compatible[IE=edge]
root@kali:~# whatweb sony.com
http://sony.com [301 Moved Permanently] Apache, Country[UNITED STATES][US], HTTP
Server[Apache], IP[52.54.18.9], RedirectLocation[https://www.sony.com/], X-Frame
-Options[SAMEORIGIN]
https://www.sony.com/ [302 Found] Akamai-Global-Host, Cookies[_abck,bm_sz,geofil
ter_country], Country[UNITED STATES][US], HTTPServer[AkamaiGHost], IP[184.30.16.
87], RedirectLocation[https://www.sony.com/en/], Strict-Transport-Security[max-a
ge=15768000], UncommonHeaders[content-security-policy,x-content-type-options]
https://www.sony.com/en/ [200 OK] Apache, Cookies[_abck,bm_sz,geofilter_country]
, Country[UNITED STATES][US], Frame, HTML5, HTTPServer[Apache], IP[184.30.16.87]
, JQuery[2.2.4], PoweredBy[real], Script[text/javascript], Strict-Transport-Secu
rity[max-age=15768000], Title[Sony Group Portal - Sony Group Corporation Website
], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN], X-UA-Co
mpatible[IE=edge]
root@kali:~#
```

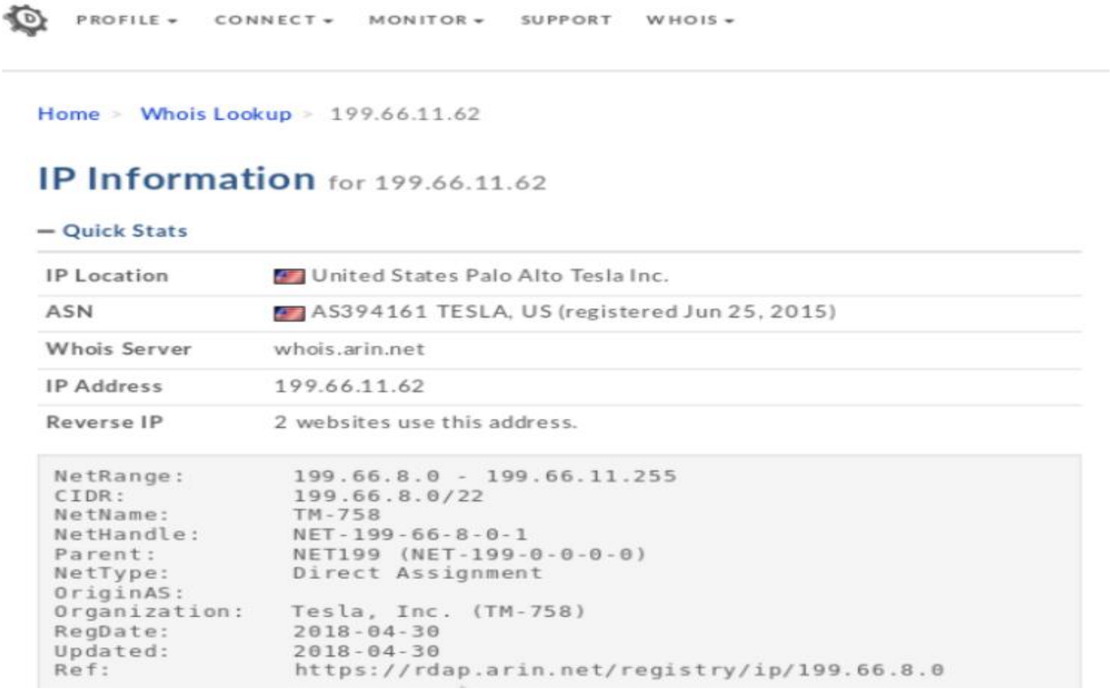
Besides using this command, there are browser extension such as wappalzyer also can perform this same action by just download and install in browser to check the information of website.

(iii) ping tesla.com(after finding its IP address, we could use its IP address, to find its related information)



```
root@kali:~# ping tesla.com
PING tesla.com (199.66.11.62) 56(84) bytes of data.
From _gateway (10.0.2.2) icmp_seq=1 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=2 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=3 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=4 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=5 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=6 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=7 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=8 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=9 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=10 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=11 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=12 Destination Net Unreachable
From _gateway (10.0.2.2) icmp_seq=13 Destination Net Unreachable
^C
--- tesla.com ping statistics ---
13 packets transmitted, 0 received, +13 errors, 100% packet loss, time 214ms

root@kali:~# 
```

After checking the targeted IP Address, can use this IP address in Whois Look up website to explore more information about the IP Address eg: owner of the server, location and so on.



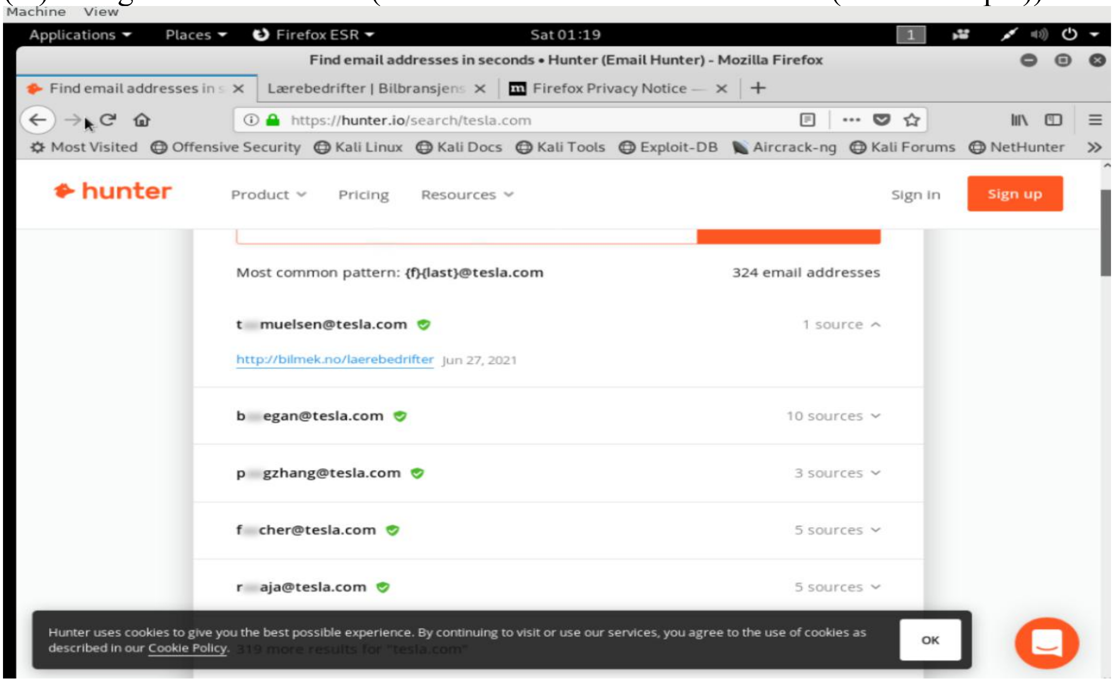
IP Information for 199.66.11.62

— Quick Stats

IP Location	United States Palo Alto Tesla Inc.
ASN	AS394161 TESLA, US (registered Jun 25, 2015)
Whois Server	whois.arin.net
IP Address	199.66.11.62
Reverse IP	2 websites use this address.

```
NetRange:       199.66.8.0 - 199.66.11.255
CIDR:           199.66.8.0/22
NetName:        TM-758
NetHandle:      NET-199-66-8-0-1
Parent:         NET199 (NET-199-0-0-0-0)
NetType:        Direct Assignment
OriginAS:
Organization:   Tesla, Inc. (TM-758)
RegDate:        2018-04-30
Updated:        2018-04-30
Ref:            https://rdap.arin.net/registry/ip/199.66.8.0
```

(iv) Using hunter.io website (find email to associate to tesla.com(as an example))



Most common pattern: {f}{last}@tesla.com 324 email addresses

t[redacted]muelsen@tesla.com 1 source

http://bilmek.no/laerebedrifter Jun 27, 2021

b[redacted]egan@tesla.com 10 sources

p[redacted]gzhang@tesla.com 3 sources

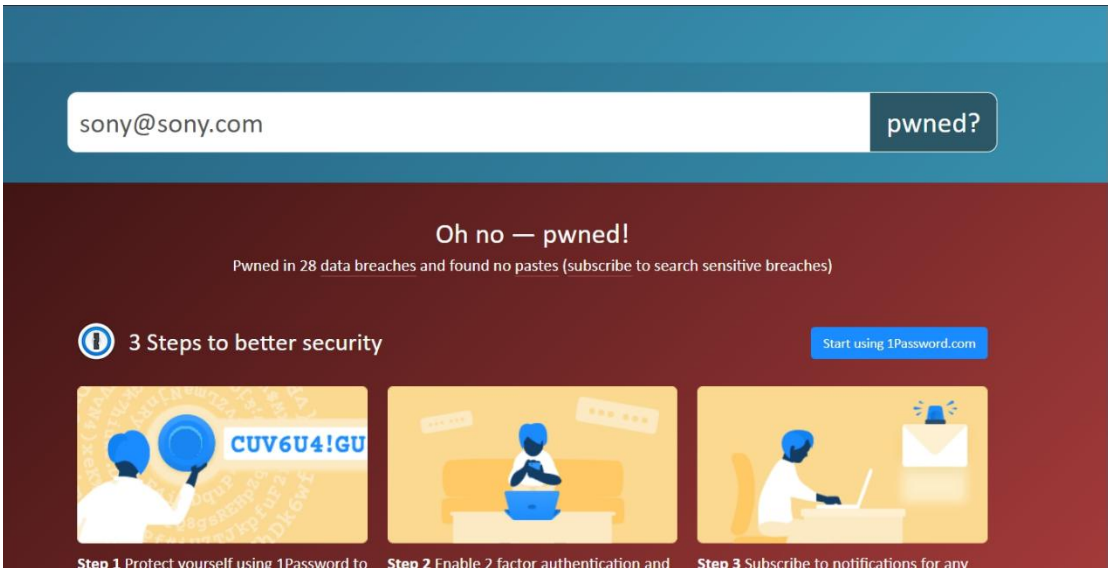
f[redacted]cher@tesla.com 5 sources

r[redacted]aja@tesla.com 5 sources

Hunter uses cookies to give you the best possible experience. By continuing to visit or use our services, you agree to the use of cookies as described in our Cookie Policy. 319 more results for "tesla.com"

OK

(v) Using haveibeenpwned.com to check whether the email has been pwned or vice versa. If shows a below, it shows that it’s dangerous because the information has been leaked and pwned. Password should be changed to avoid cyberattack such as bruteforce attack



Oh no — pwned!

Pwned in 28 data breaches and found no pastes (subscribe to search sensitive breaches)

Step 1 Protect yourself using 1Password to

Step 2 Enable 2 factor authentication and

Step 3 Subscribe to notifications for any

(vi) By using sublist3r -d [targeted website], eg: sublist3r-d tesla.com, we can check the subdomain of tesla.com

(vii) theHarverster -d tesla.com is used to find emails of tesla.com, same as iv. However, sometimes it is not working.

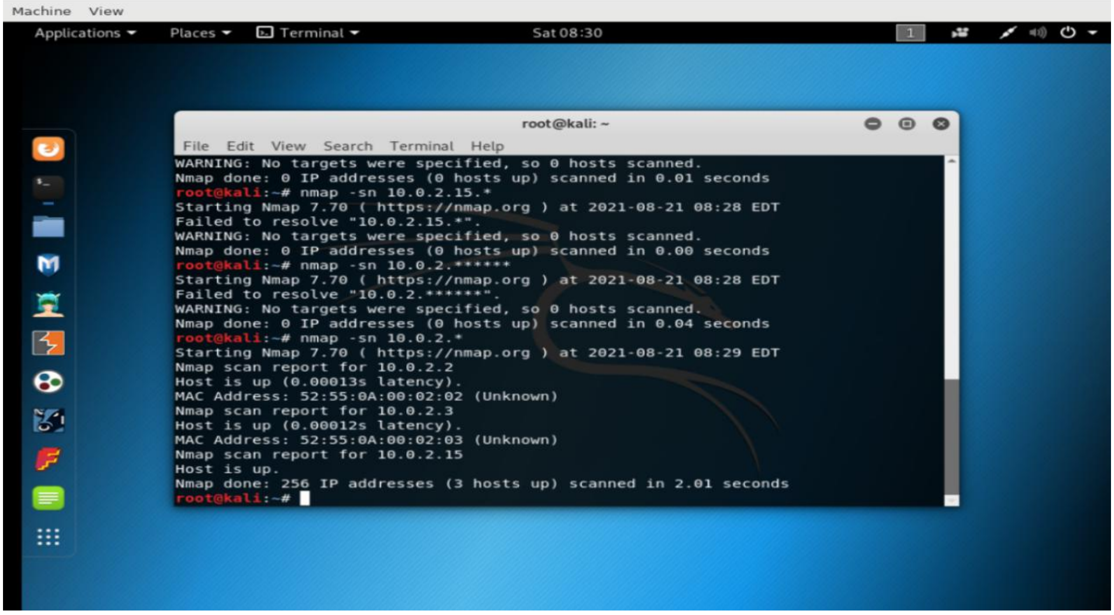
2. SCANNING(TO FIND VULNERABILITIES)

(i) **Use gitclone dirsearch on terminal Kali Linux** to find available files or folder on the targeted site. (using dirbuster and dirb)

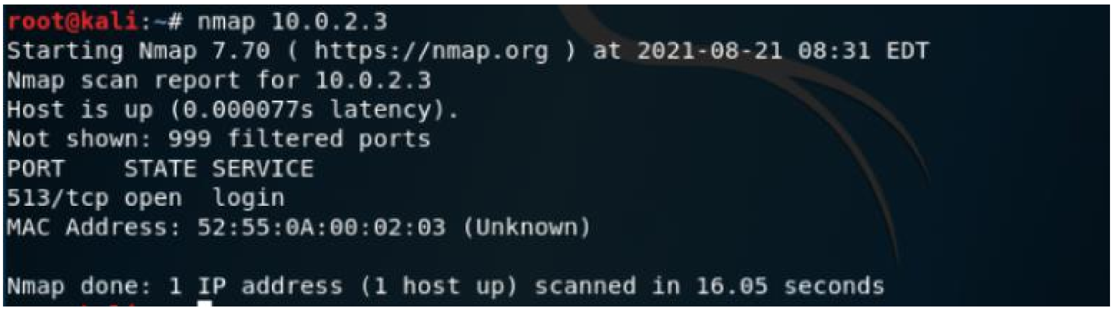
(ii)Using Nmap(Network Mapper)(to scan)

Nmap is available by default. Also, nmap also can just check first 10000 ports.

Firstly, we can use command ip a, to find out our IP Address. After that, use command nmap -sn [IP Address. *]

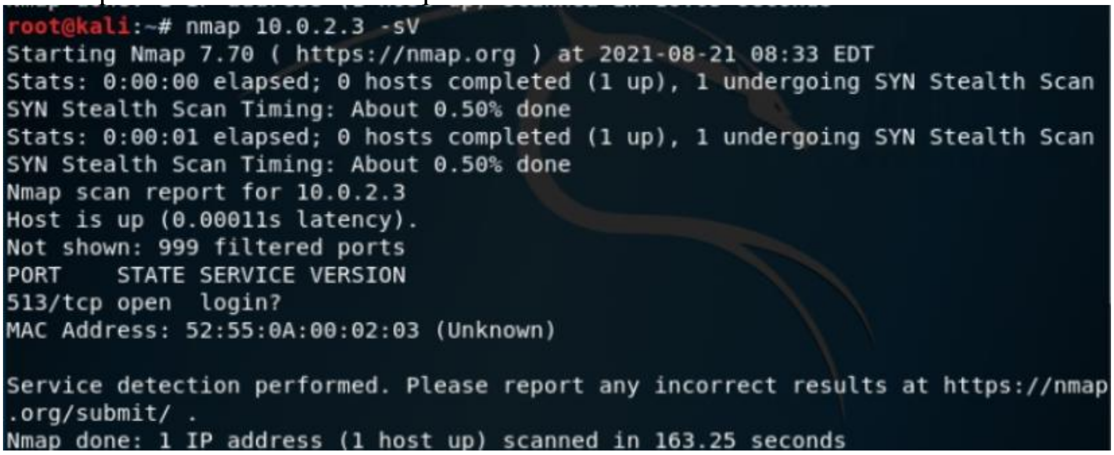


```
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.01 seconds
root@kali:~# nmap -sn 10.0.2.15.*
Starting Nmap 7.70 ( https://nmap.org ) at 2021-08-21 08:28 EDT
Failed to resolve "10.0.2.15.*".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.00 seconds
root@kali:~# nmap -sn 10.0.2.******
Starting Nmap 7.70 ( https://nmap.org ) at 2021-08-21 08:28 EDT
Failed to resolve "10.0.2.******".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@kali:~# nmap -sn 10.0.2.*
Starting Nmap 7.70 ( https://nmap.org ) at 2021-08-21 08:29 EDT
Nmap scan report for 10.0.2.2
Host is up (0.00013s latency).
MAC Address: 52:55:0A:00:02:02 (Unknown)
Nmap scan report for 10.0.2.3
Host is up (0.00012s latency).
MAC Address: 52:55:0A:00:02:03 (Unknown)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.01 seconds
root@kali:~#
```



```
root@kali:~# nmap 10.0.2.3
Starting Nmap 7.70 ( https://nmap.org ) at 2021-08-21 08:31 EDT
Nmap scan report for 10.0.2.3
Host is up (0.000077s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
513/tcp open  login
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 16.05 seconds
```

It is help to check the version of particular services to run



```
root@kali:~# nmap 10.0.2.3 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2021-08-21 08:33 EDT
Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Nmap scan report for 10.0.2.3
Host is up (0.00011s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE VERSION
513/tcp open  login?
MAC Address: 52:55:0A:00:02:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.25 seconds
```

Command nmap -p [range of port] [IP Address], eg: nmap -p 1-1024 192.168.128.132 is performed to check the IP Address at range of 1 to 1024

Command nmap -p [IP Address], eg: nmap -p 192.168.128.132 is performed to check the IP Address at all range[maximum 10000]

Command nmap -O [IP Address], eg: nmap -O 192.168.128.132 is performed to check the operating system used in system.

Command nmap -A [IP Address], eg: nmap -A 192.168.128.132 is performed to check traceroute and so on.

Command nmap -O [IP Address] -T[number], eg: nmap -O 192.168.128.132 -T4 is performed to check the operating system used in system in the selected speed. As the number is decreased, the speed will be increased.

Command nmap [IP Address] -oN nmap-scan.txt, eg: nmap 192.168.128.132 -oN nmap-scan.txt is performed to check the reporting.

(ii) Using Nikto(is used to vulnerabilites of website)

Nikto -h [website] eg: nikto -h http:192.168.128.132/

(iii) Acunetix

This is a scanner software to check the vulnerabilities, rather than using command line in Terminal Kali Linux