2023

Introduction To Information Security And Forensics

Applied Project

Sana Shaheen

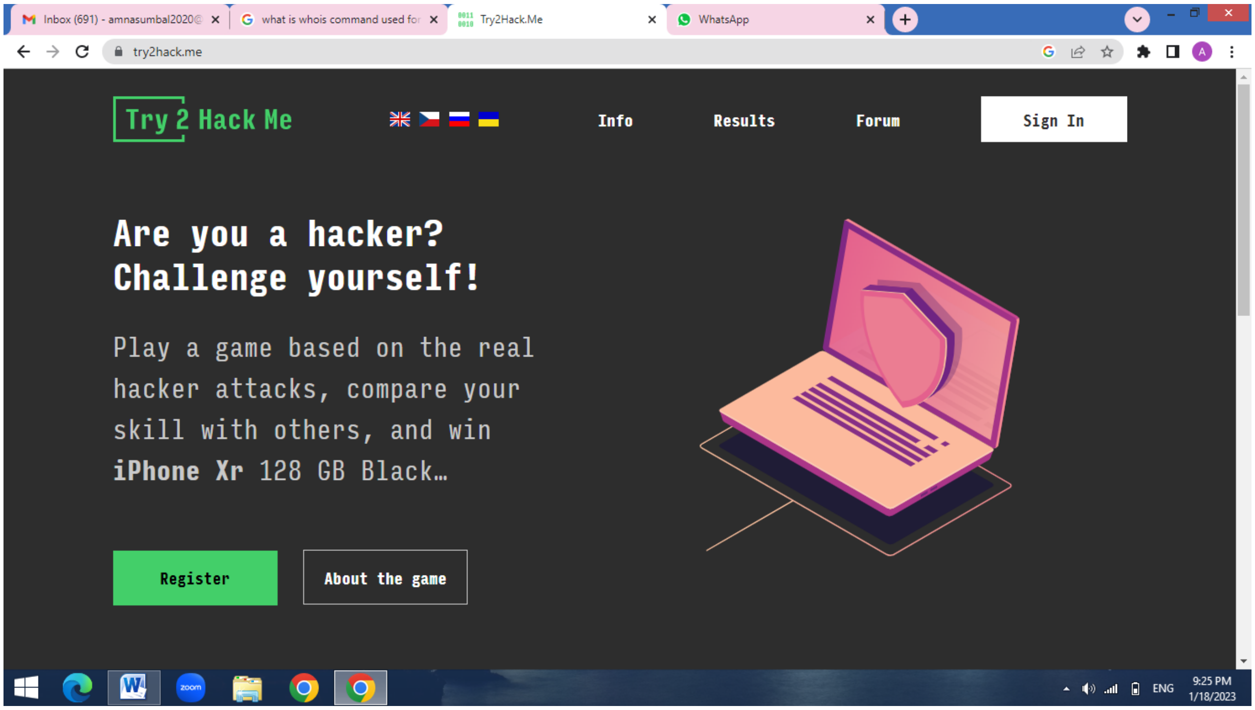
Iqra Ahmad

Amna Sumbal

Submitted to: Ms. Snoober

INTRODUTION:

Website Interface



Are you a hacker?
Challenge yourself!

Play a game based on the real hacker attacks, compare your skill with others, and win **iPhone Xr** 128 GB Black…

https://try2hack.me/

About the Website:

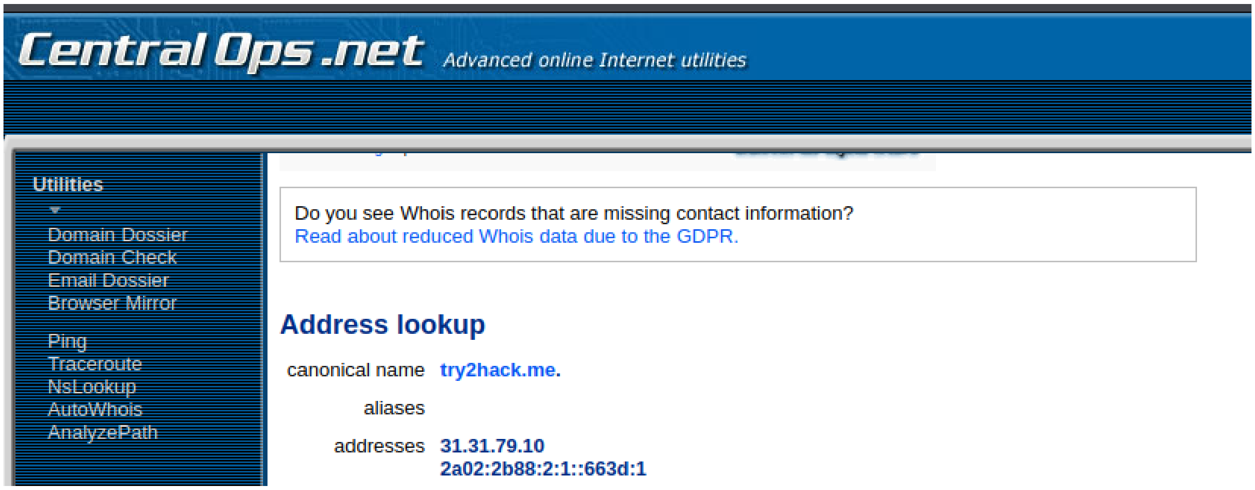
Try2Hack is a website where you can practice your hacking skills. It is considered one of the oldest challenge sites still around. Try2Hack offers multiple security challenges. The game features diverse levels which are sorted by difficulty, all created to practice hacking for one’s entertainment. There is an IRC channel for beginners where they can join the community and ask for help, in addition to a full walkthrough based on GitHub.

Reconnaissance phase

1. Information Gathering (Passive)

We gathered the following information about the website we chose:

- IP Address
- Domain Name
- Open Port
- Network Range
- Access Point



Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

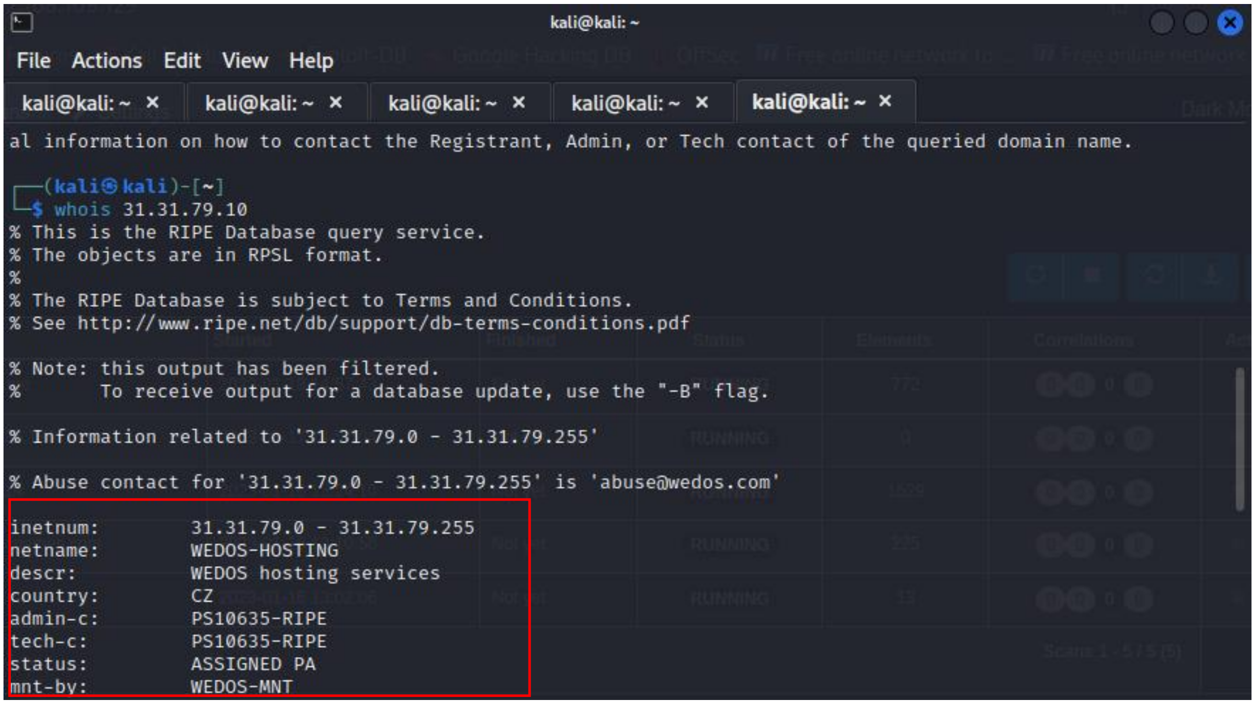
canonical name try2hack.me.

aliases

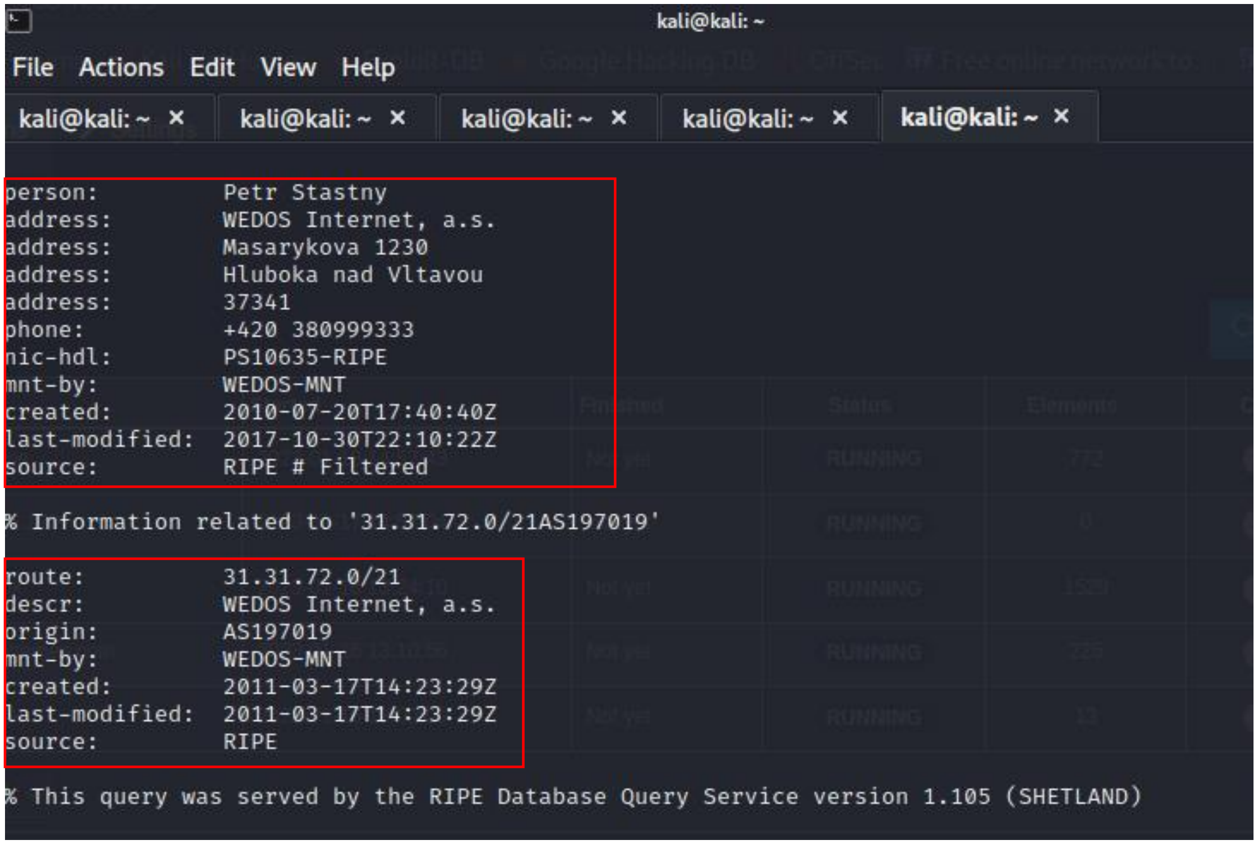
addresses 31.31.79.10
2a02:2b88:2:1::663d:1

Whois

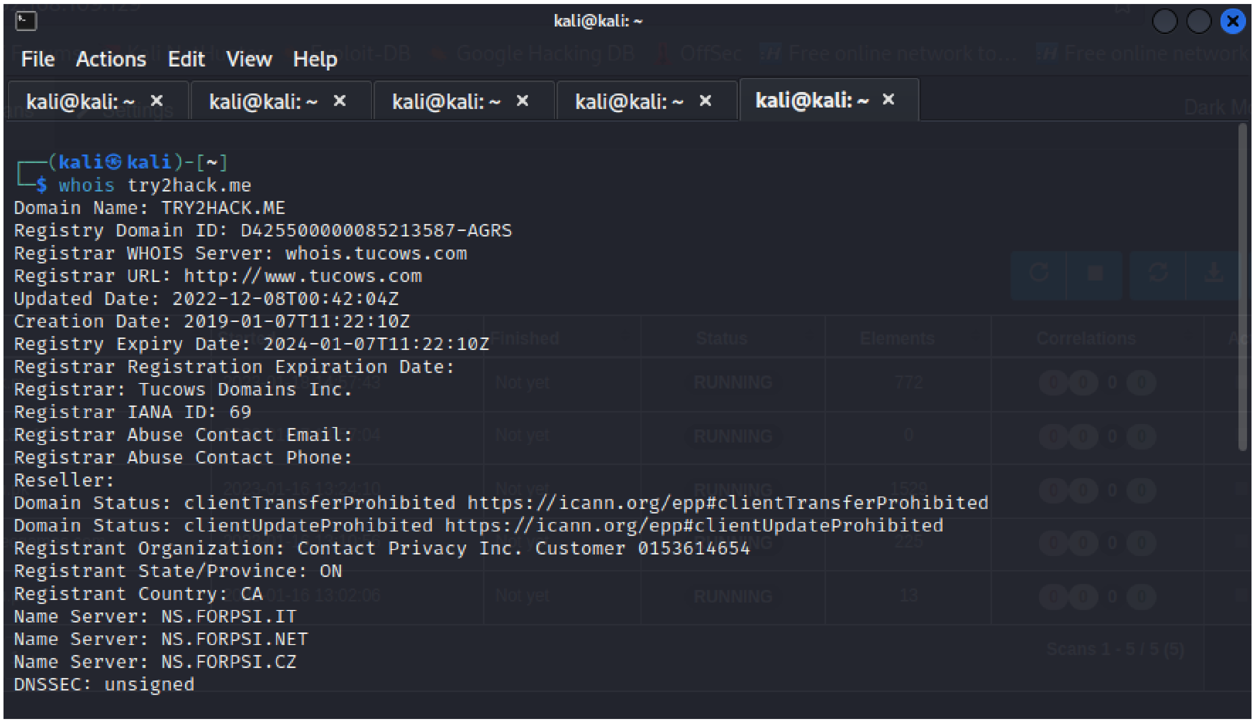
The Whois database contains details such as the registration date of the domain name, when it expires, ownership and contact information, nameserver information of the domain, the registrar via which the domain was purchased.



```
al information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

┌──(kali㉿kali)-[~]
└─$ whois 31.31.79.10
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '31.31.79.0 - 31.31.79.255'

% Abuse contact for '31.31.79.0 - 31.31.79.255' is 'abuse@wedos.com'

inetnum:        31.31.79.0 - 31.31.79.255
netname:        WEDOS-HOSTING
descr:          WEDOS hosting services
country:        CZ
admin-c:        PS10635-RIPE
tech-c:         PS10635-RIPE
status:         ASSIGNED PA
mnt-by:         WEDOS-MNT
```



```
person:         Petr Stastny
address:        WEDOS Internet, a.s.
address:        Masarykova 1230
address:        Hluboka nad Vltavou
address:        37341
phone:          +420 380999333
nic-hdl:        PS10635-RIPE
mnt-by:         WEDOS-MNT
created:        2010-07-20T17:40:40Z
last-modified:  2017-10-30T22:10:22Z
source:         RIPE # Filtered

% Information related to '31.31.72.0/21AS197019'

route:          31.31.72.0/21
descr:          WEDOS Internet, a.s.
origin:         AS197019
mnt-by:         WEDOS-MNT
created:        2011-03-17T14:23:29Z
last-modified:  2011-03-17T14:23:29Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.105 (SHETLAND)
```



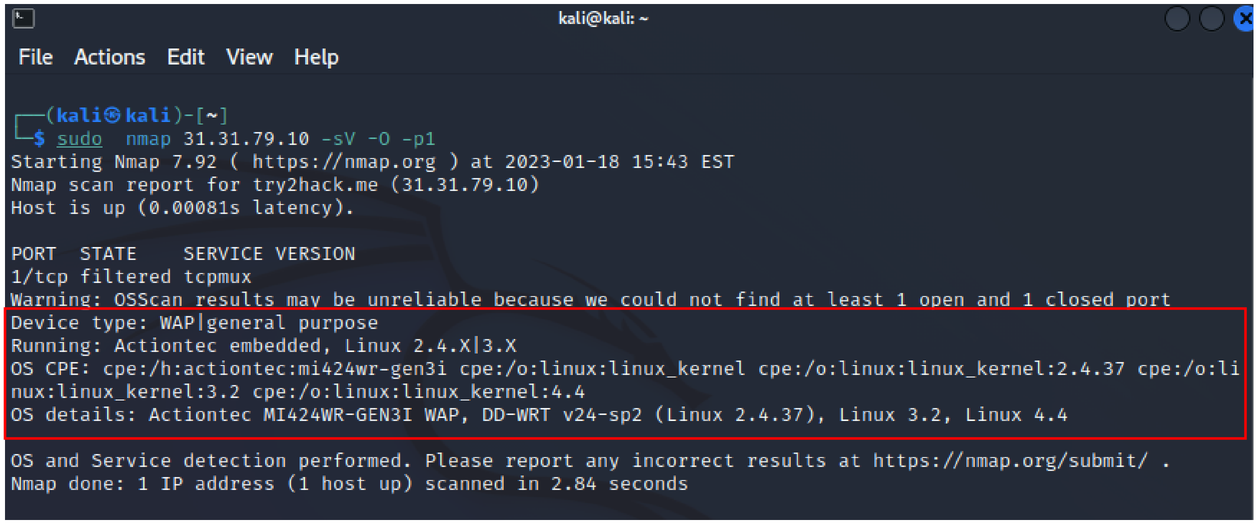
```
┌──(kali㉿kali)-[~]
└─$ whois try2hack.me
Domain Name: TRY2HACK.ME
Registry Domain ID: D425500000085213587-AGRS
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://www.tucows.com
Updated Date: 2022-12-08T00:42:04Z
Creation Date: 2019-01-07T11:22:10Z
Registry Expiry Date: 2024-01-07T11:22:10Z
Registrar Registration Expiration Date:
Registrar: Tucows Domains Inc.
Registrar IANA ID: 69
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: Contact Privacy Inc. Customer 0153614654
Registrant State/Province: ON
Registrant Country: CA
Name Server: NS.FORPSI.IT
Name Server: NS.FORPSI.NET
Name Server: NS.FORPSI.CZ
DNSSEC: unsigned
```

As highlighted in the above image we gained a lot of information from the command Whois like the NetRange, NetName, Organization, ServerName Registration Date and when was the website last updated.

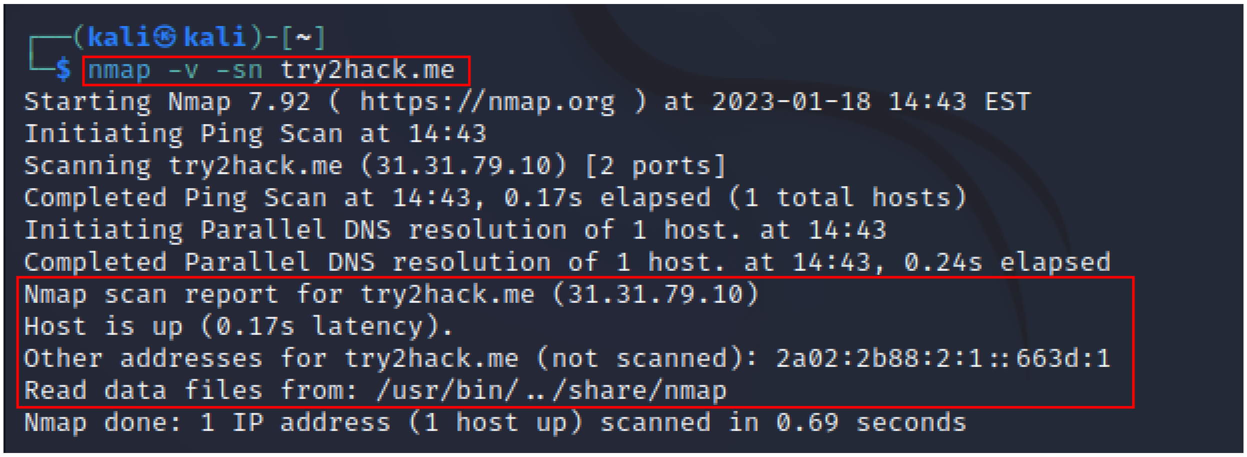
Moreover, the command also provided with the phone no, email, fax no, postal code, street, city, country and province where the website's organization might be located.

Nmap

Nmap, the acronym for **Network Mapper**, is an open-source security auditing and network scanning tool. It can also be used to gain access to uncontrolled ports on a system. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features.

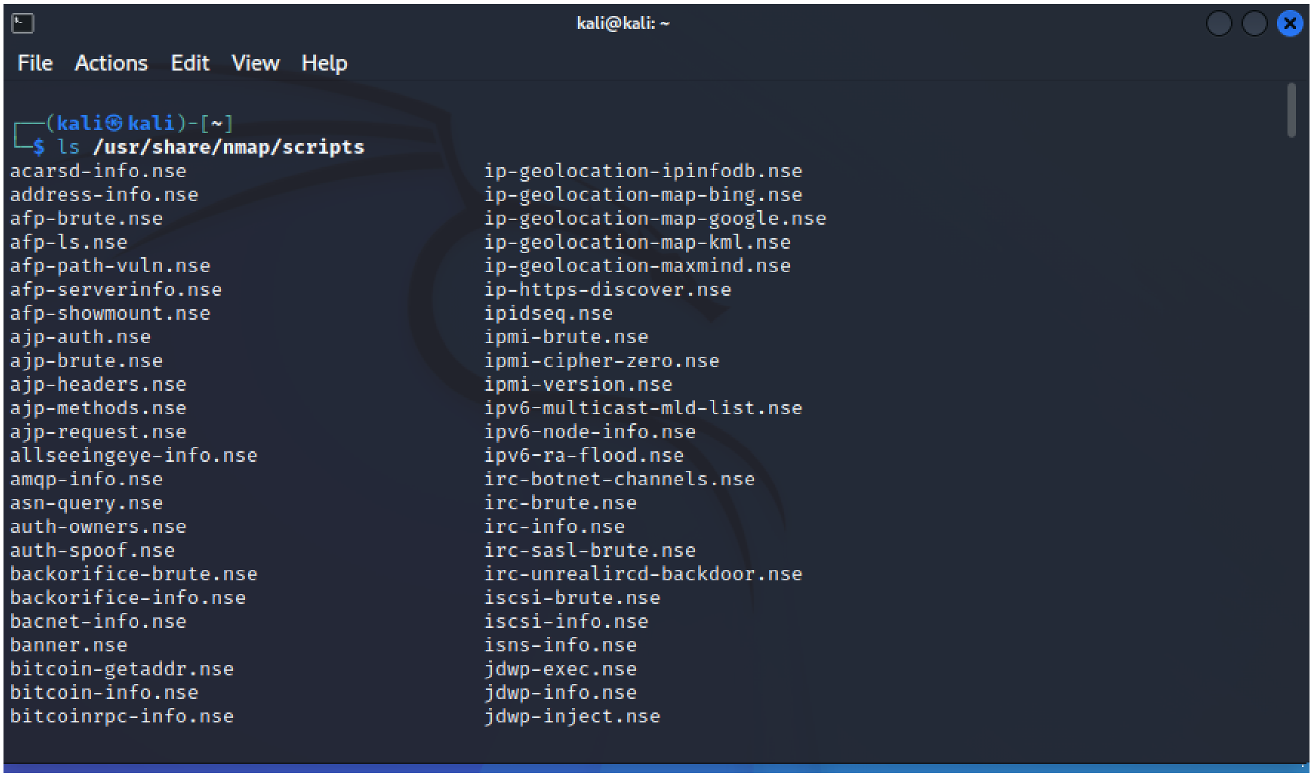


```
┌──(kali㉿kali)-[~]
└─$ sudo  nmap 31.31.79.10 -sV -O -p1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 15:43 EST
Nmap scan report for try2hack.me (31.31.79.10)
Host is up (0.00081s latency).

PORT   STATE    SERVICE VERSION
1/tcp filtered tcpmux
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:li
nux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4

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 2.84 seconds
```

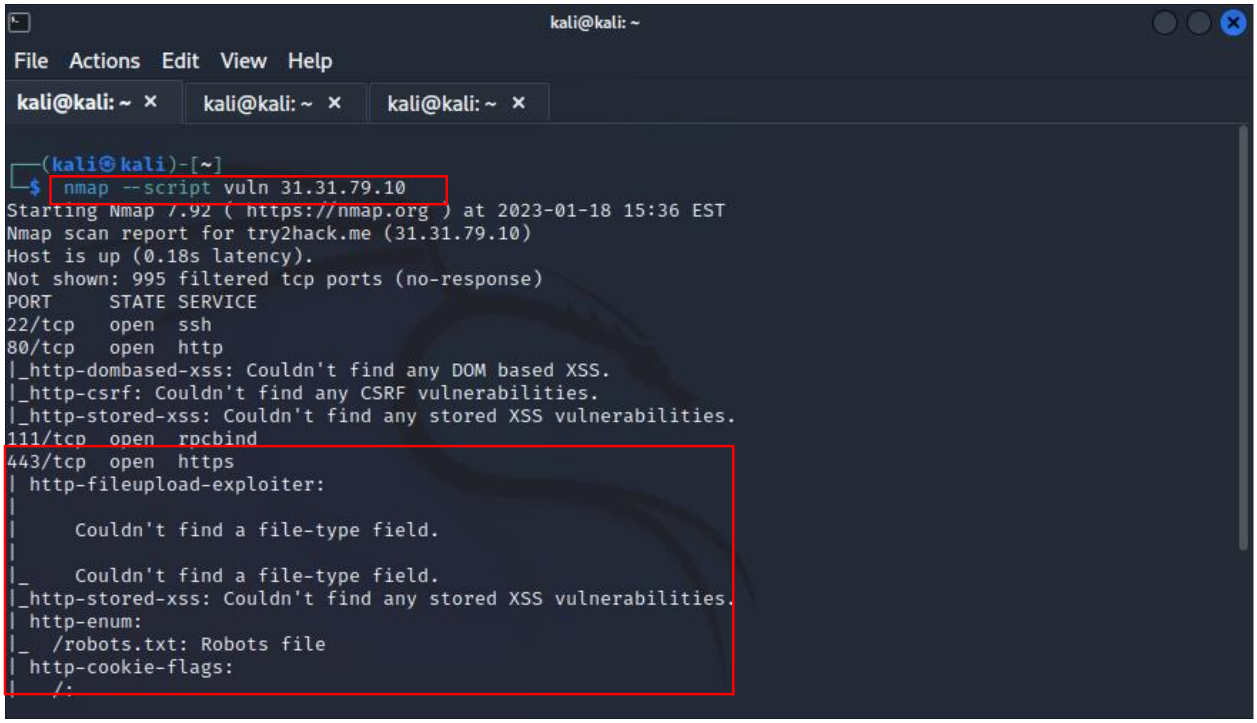


```
┌──(kali㉿kali)-[~]
└─$ nmap -v -sn try2hack.me
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 14:43 EST
Initiating Ping Scan at 14:43
Scanning try2hack.me (31.31.79.10) [2 ports]
Completed Ping Scan at 14:43, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:43
Completed Parallel DNS resolution of 1 host. at 14:43, 0.24s elapsed
Nmap scan report for try2hack.me (31.31.79.10)
Host is up (0.17s latency).
Other addresses for try2hack.me (not scanned): 2a02:2b88:2:1::663d:1
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

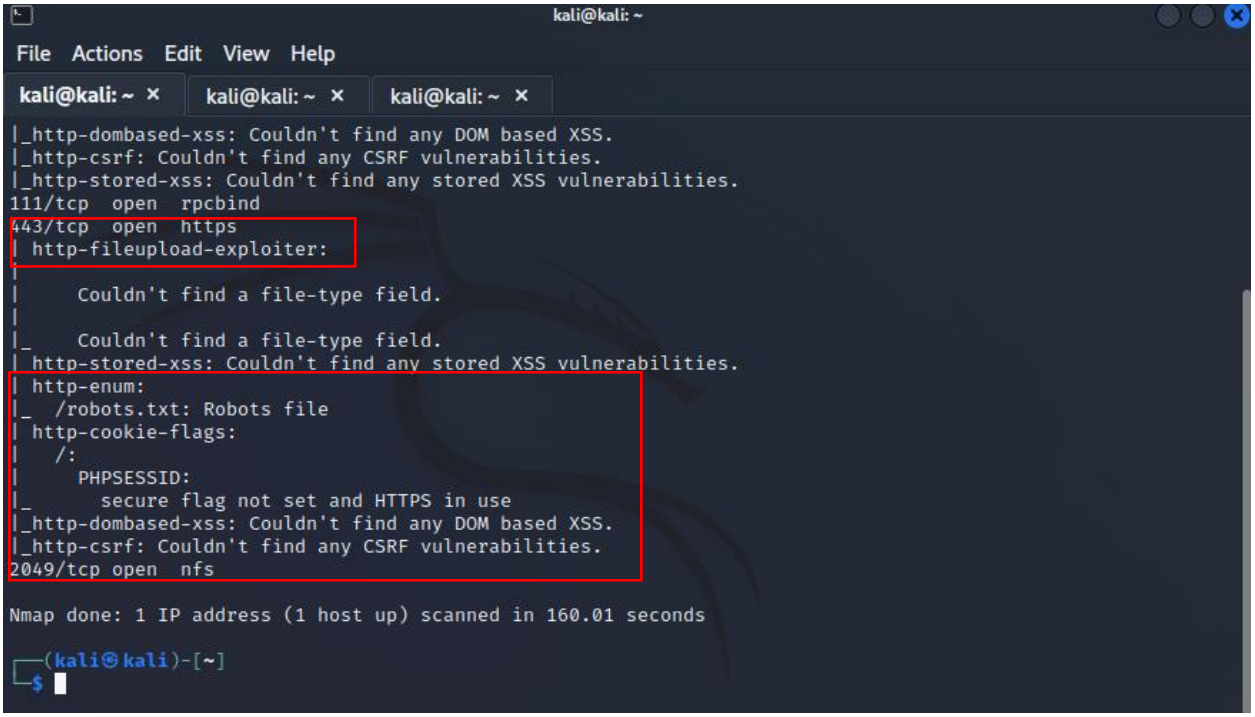
Nmap Scripts



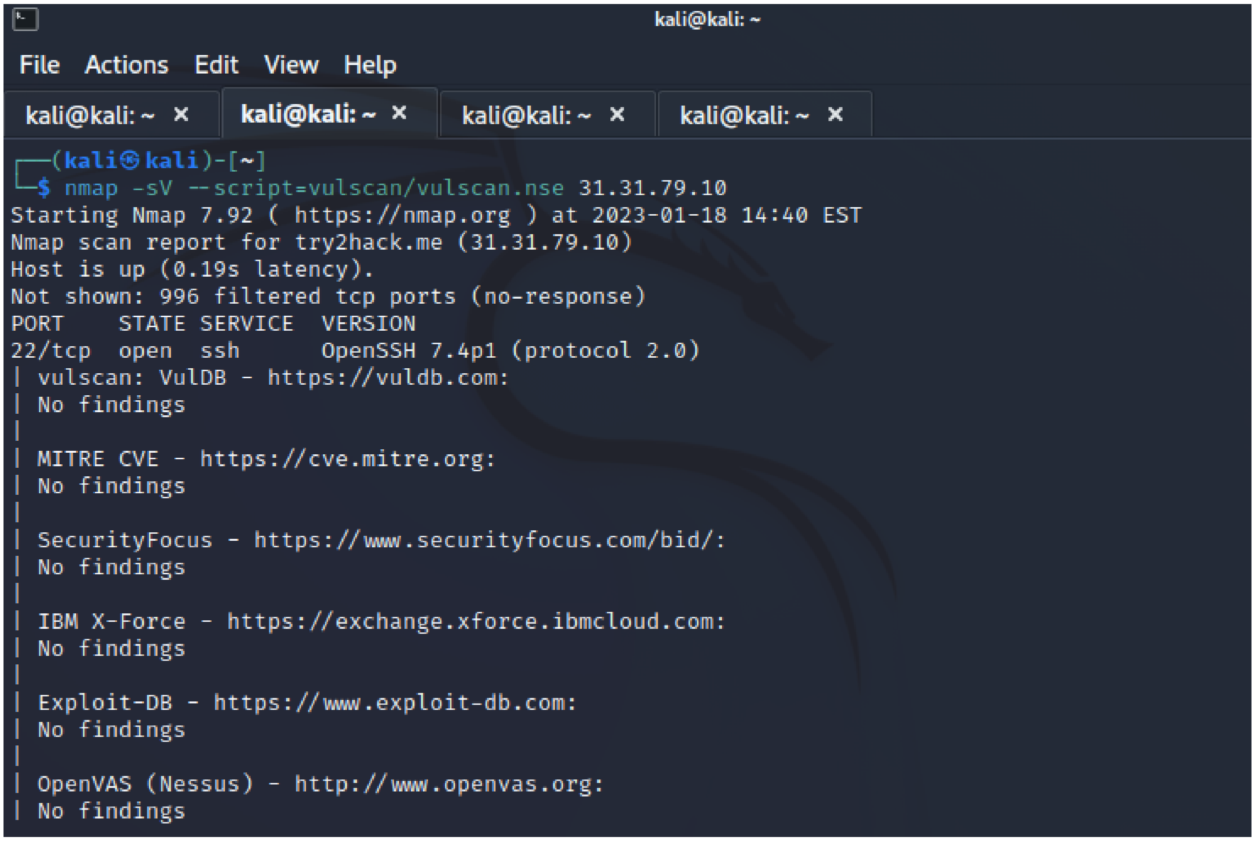
```
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/nmap/scripts
acarsd-info.nse                         ip-geolocation-ipinfodb.nse
address-info.nse                        ip-geolocation-map-bing.nse
afp-brute.nse                           ip-geolocation-map-google.nse
afp-ls.nse                              ip-geolocation-map-kml.nse
afp-path-vuln.nse                       ip-geolocation-maxmind.nse
afp-serverinfo.nse                      ip-https-discover.nse
afp-showmount.nse                       ipidseq.nse
ajp-auth.nse                            ipmi-brute.nse
ajp-brute.nse                           ipmi-cipher-zero.nse
ajp-headers.nse                         ipmi-version.nse
ajp-methods.nse                         ipv6-multicast-mld-list.nse
ajp-request.nse                         ipv6-node-info.nse
allseeingeye-info.nse                   ipv6-ra-flood.nse
amqp-info.nse                           irc-botnet-channels.nse
asn-query.nse                           irc-brute.nse
auth-owners.nse                         irc-info.nse
auth-spoof.nse                          irc-sasl-brute.nse
backorifice-brute.nse                   irc-unrealircd-backdoor.nse
backorifice-info.nse                    iscsi-brute.nse
bacnet-info.nse                         iscsi-info.nse
banner.nse                              isns-info.nse
bitcoin-getaddr.nse                     jdwp-exec.nse
bitcoin-info.nse                        jdwp-info.nse
bitcoinrpc-info.nse                     jdwp-inject.nse
```



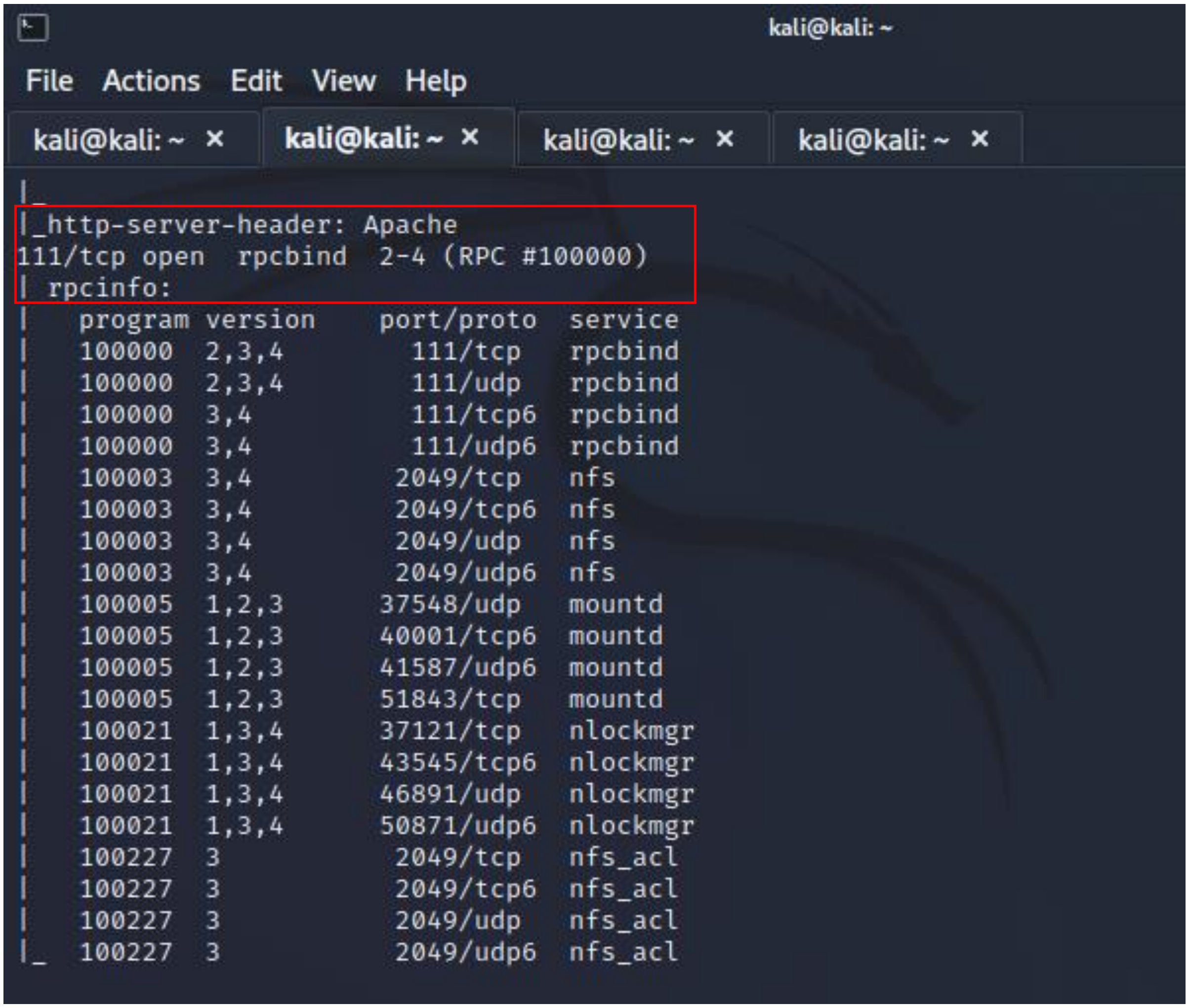
```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 31.31.79.10
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 15:36 EST
Nmap scan report for try2hack.me (31.31.79.10)
Host is up (0.18s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp  open  rpcbind
443/tcp  open  https
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /robots.txt: Robots file
| http-cookie-flags:
|   /:
```



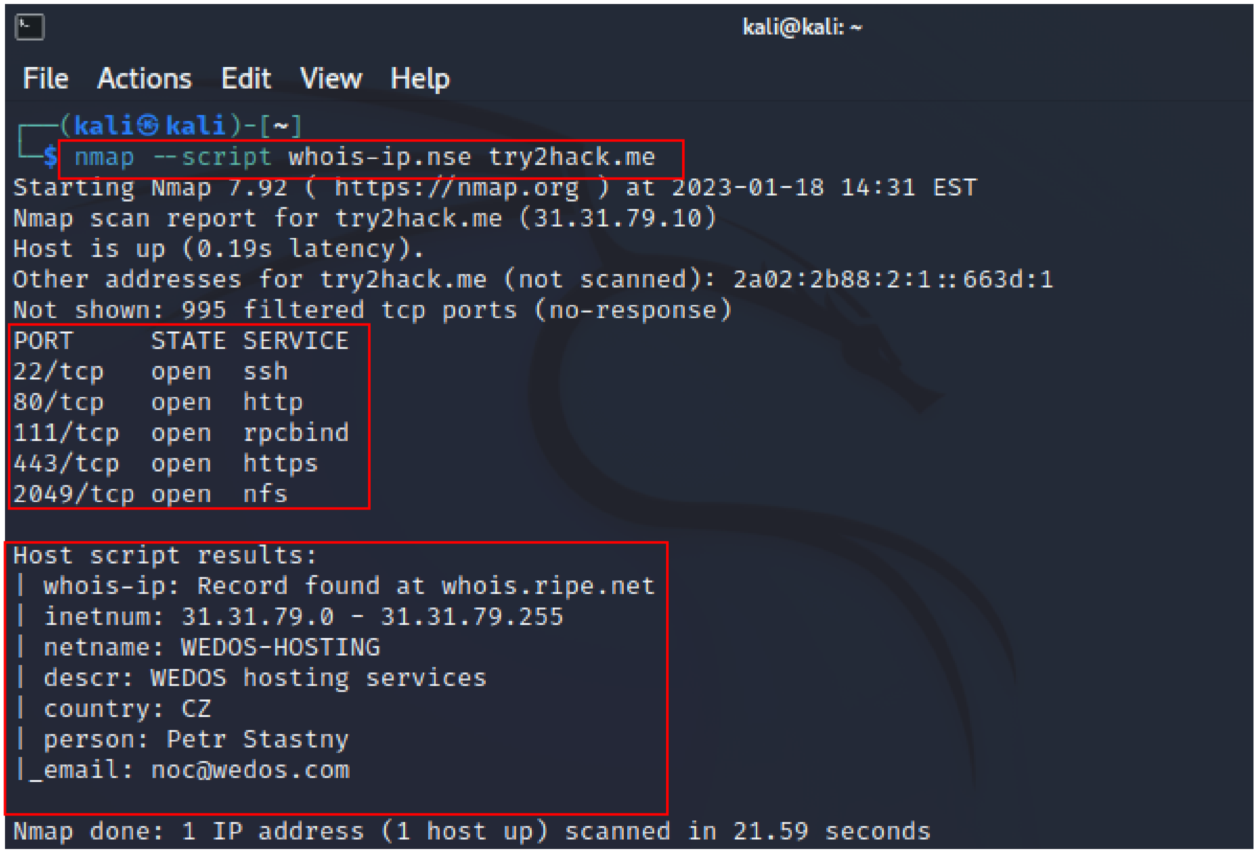
```
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp  open  rpcbind
443/tcp  open  https
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /robots.txt: Robots file
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      secure flag not set and HTTPS in use
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 160.01 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=vulscan/vulscan.nse 31.31.79.10
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 14:40 EST
Nmap scan report for try2hack.me (31.31.79.10)
Host is up (0.19s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4p1 (protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| No findings
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| No findings
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| No findings
|
| Exploit-DB - https://www.exploit-db.com:
| No findings
|
| OpenVAS (Nessus) - http://www.openvas.org:
| No findings
```



```
|_
|_http-server-header: Apache
111/tcp open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100003  3,4         2049/udp   nfs
|   100003  3,4         2049/udp6  nfs
|   100005  1,2,3      37548/udp   mountd
|   100005  1,2,3      40001/tcp6  mountd
|   100005  1,2,3      41587/udp6  mountd
|   100005  1,2,3      51843/tcp   mountd
|   100021  1,3,4      37121/tcp   nlockmgr
|   100021  1,3,4      43545/tcp6  nlockmgr
|   100021  1,3,4      46891/udp   nlockmgr
|   100021  1,3,4      50871/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
```



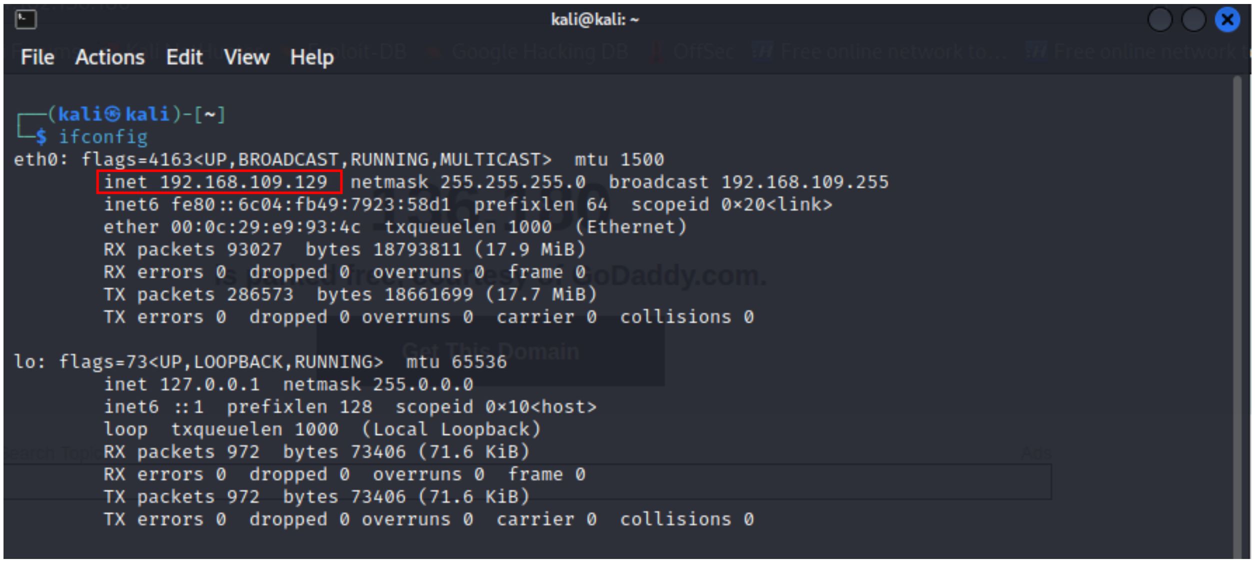
```
┌──(kali㉿kali)-[~]
└─$ nmap --script whois-ip.nse try2hack.me
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 14:31 EST
Nmap scan report for try2hack.me (31.31.79.10)
Host is up (0.19s latency).
Other addresses for try2hack.me (not scanned): 2a02:2b88:2:1::663d:1
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
2049/tcp open  nfs

Host script results:
| whois-ip: Record found at whois.ripe.net
| inetnum: 31.31.79.0 - 31.31.79.255
| netname: WEDOS-HOSTING
| descr: WEDOS hosting services
| country: CZ
| person: Petr Stastny
|_email: noc@wedos.com

Nmap done: 1 IP address (1 host up) scanned in 21.59 seconds
```

Scanning phase

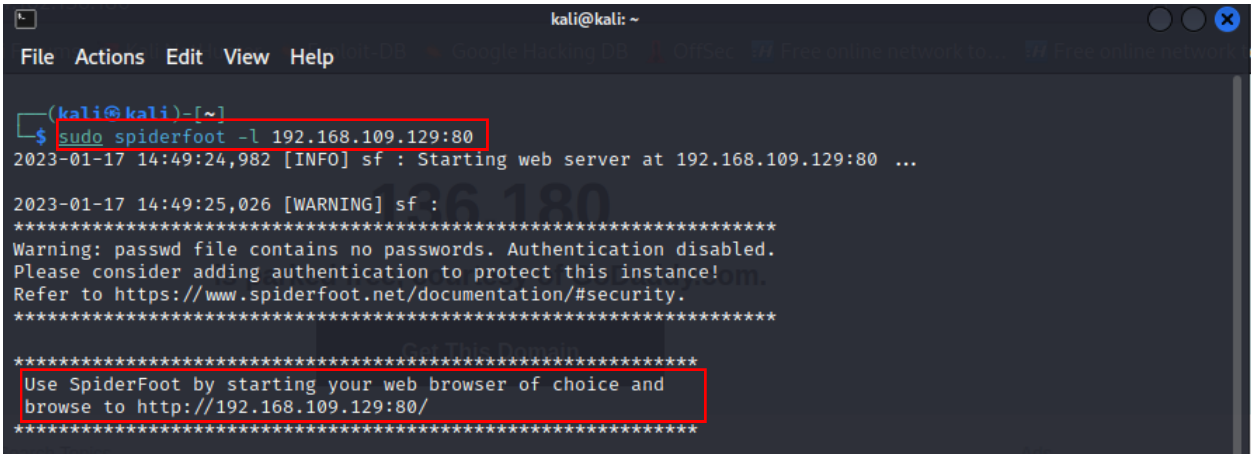
Spiderfoot

Spiderfoot is used to gather information about the target, or defensively to identify what information you or your organization are freely providing for attackers to use against you.

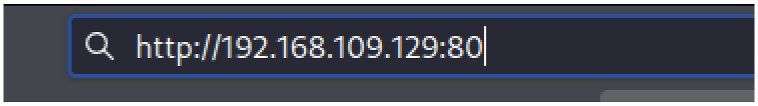
SpiderFoot is a reconnaissance tool that automatically queries over 100 public data sources to gather intelligence on IP addresses, domain names, e-mail addresses, names and more. It performs both active and passive scanning of a target.



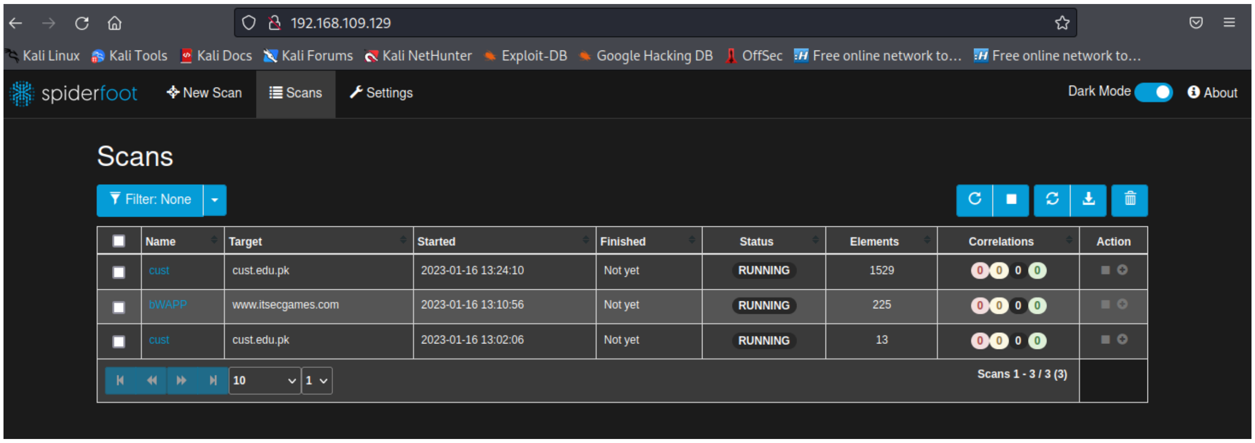
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.109.129  netmask 255.255.255.0  broadcast 192.168.109.255
        inet6 fe80::6c04:fb49:7923:58d1  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:e9:93:4c  txqueuelen 1000  (Ethernet)
        RX packets 93027  bytes 18793811 (17.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 286573  bytes 18661699 (17.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 972  bytes 73406 (71.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 972  bytes 73406 (71.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
┌──(kali㉿kali)-[~]
└─$ sudo spiderfoot -l 192.168.109.129:80
2023-01-17 14:49:24,982 [INFO] sf : Starting web server at 192.168.109.129:80 ...

2023-01-17 14:49:25,026 [WARNING] sf :
**********************************************************************
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
**********************************************************************

**************************************************************
 Use SpiderFoot by starting your web browser of choice and
 browse to http://192.168.109.129:80/
**************************************************************
```



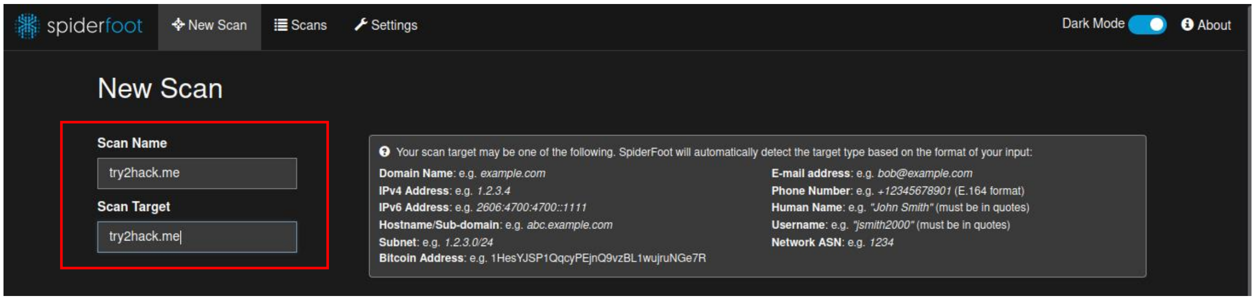
http://192.168.109.129:80



Scans

□	Name	Target	Started	Finished	Status	Elements	Correlations	Action
□	cust	cust.edu.pk	2023-01-16 13:24:10	Not yet	RUNNING	1529	0 0 0 0	■ ⊕
□	bWAPP	www.itsecgames.com	2023-01-16 13:10:56	Not yet	RUNNING	225	0 0 0 0	■ ⊕
□	cust	cust.edu.pk	2023-01-16 13:02:06	Not yet	RUNNING	13	0 0 0 0	■ ⊕

10 1 Scans 1 - 3 / 3 (3)



New Scan

Scan Name

try2hack.me

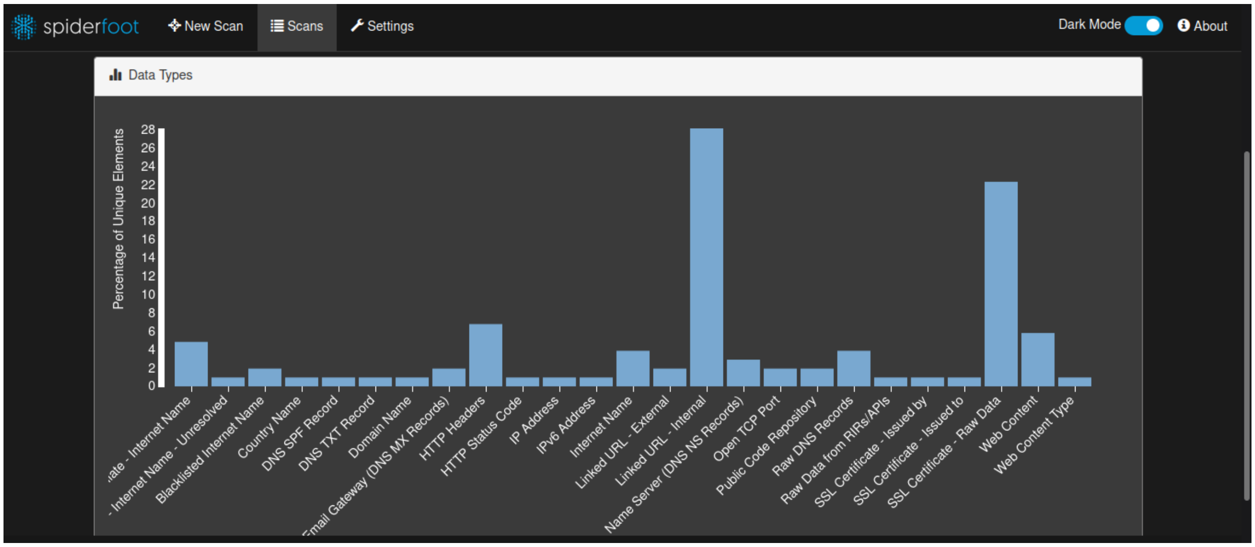
Scan Target

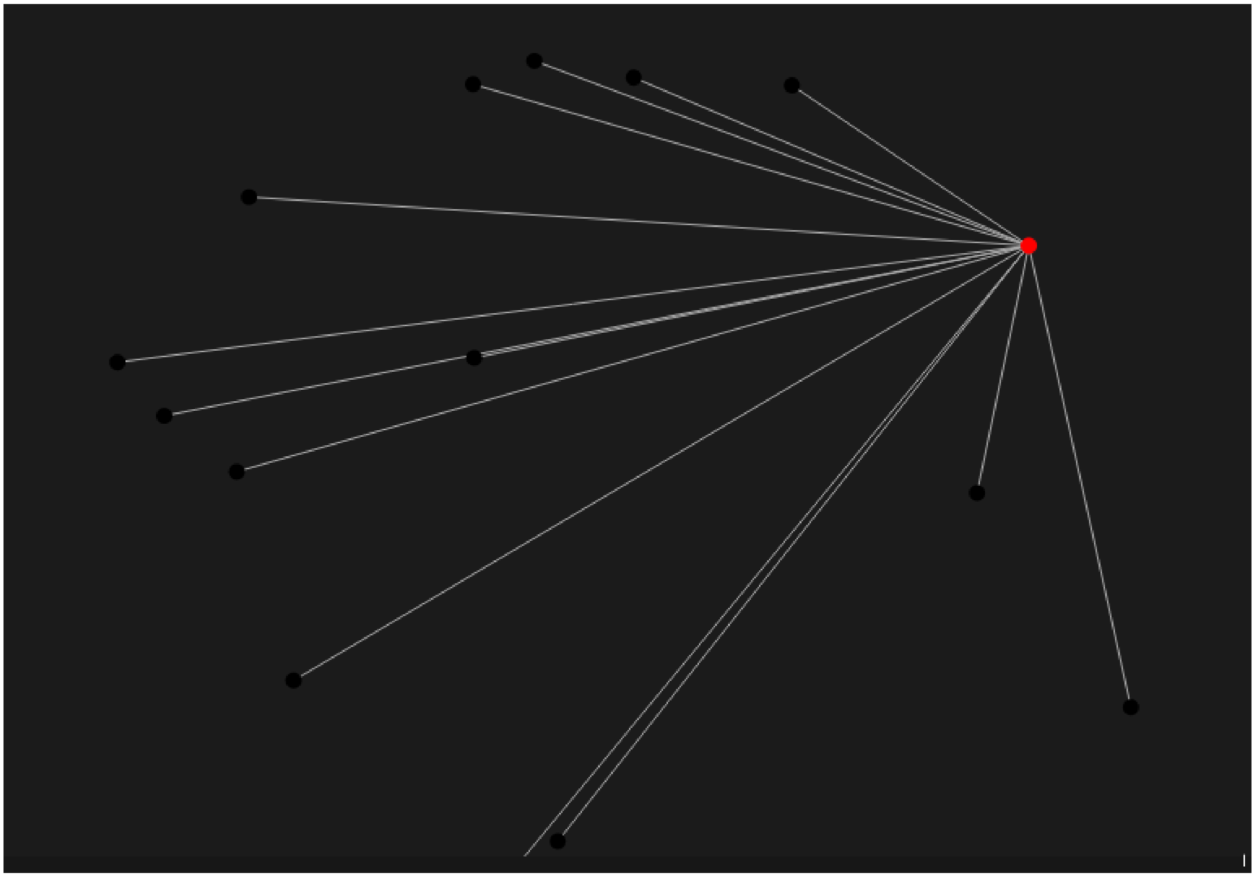
try2hack.me

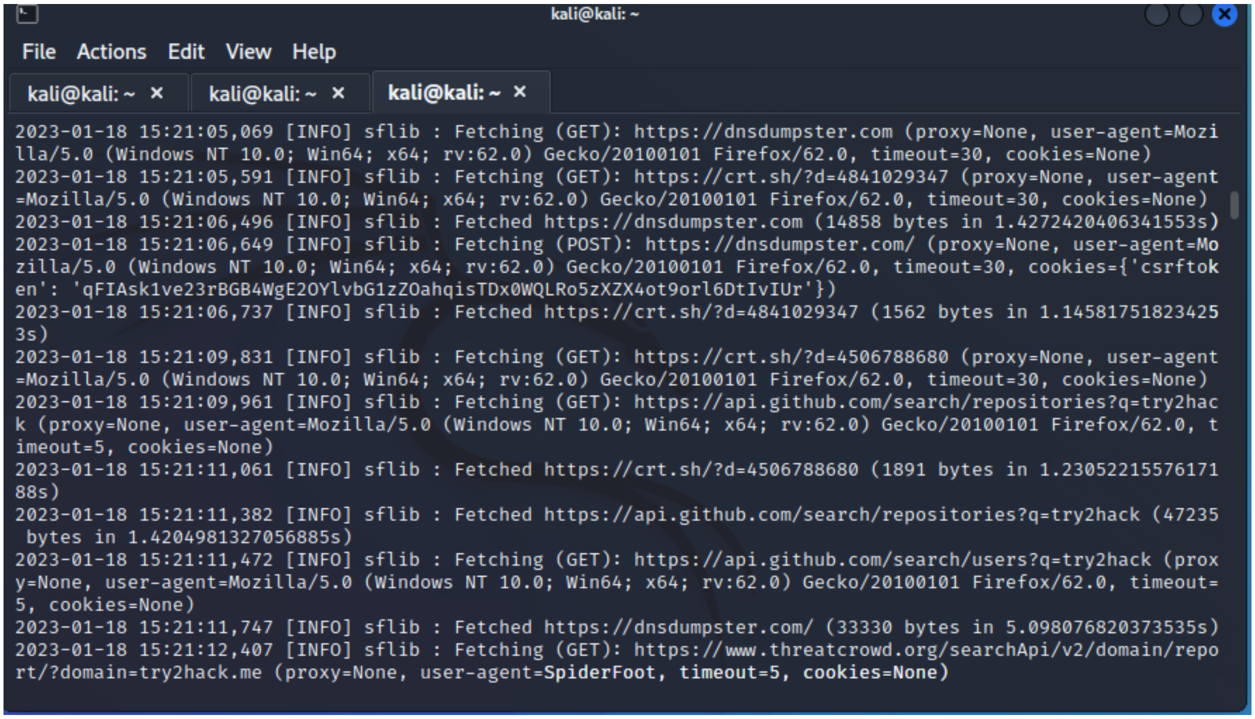
Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

Domain Name: e.g. *example.com*
IPv4 Address: e.g. *1.2.3.4*
IPv6 Address: e.g. *2606:4700:4700::1111*
Hostname/Sub-domain: e.g. *abc.example.com*
Subnet: e.g. *1.2.3.0/24*
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R

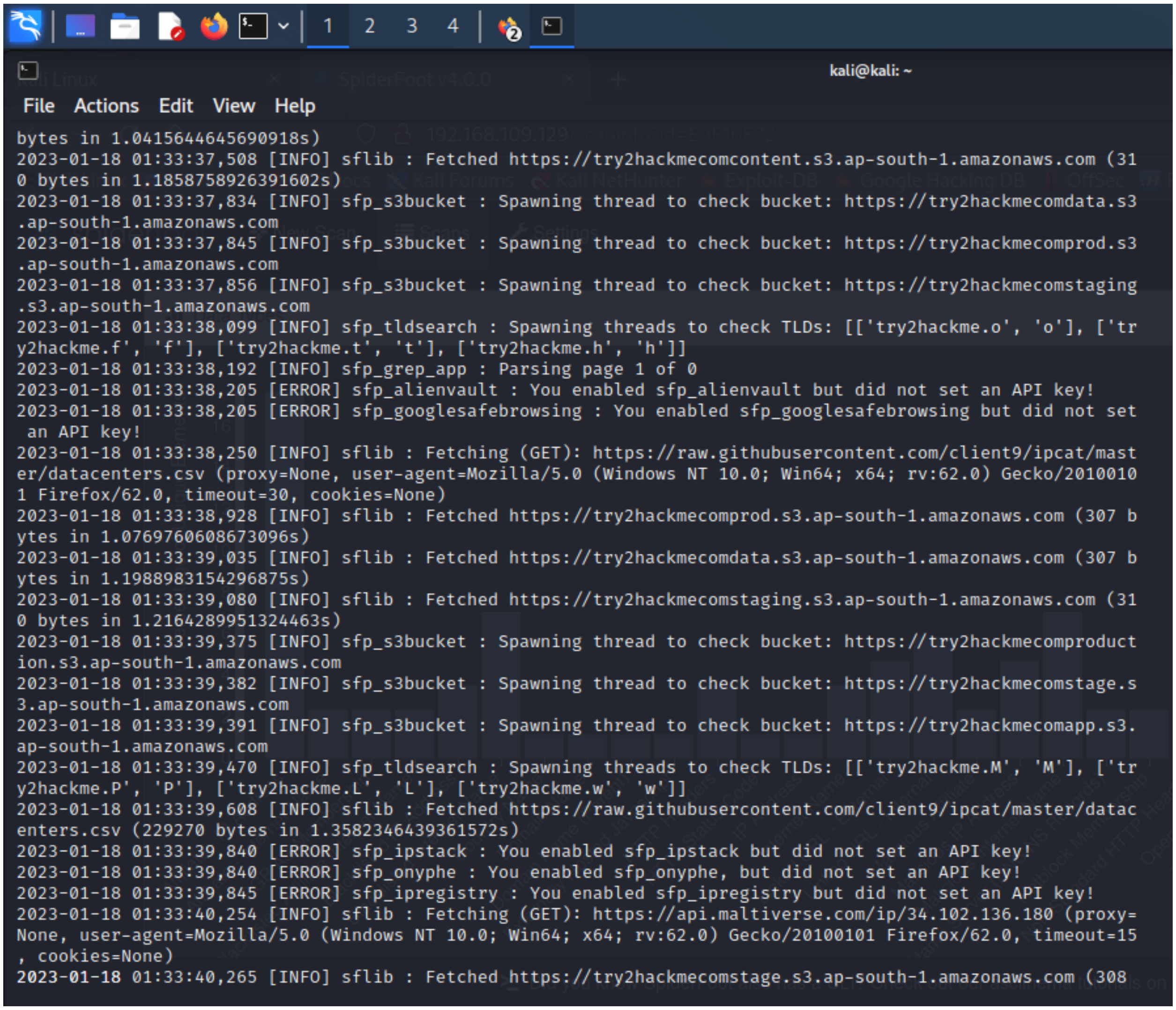
E-mail address: e.g. *bob@example.com*
Phone Number: e.g. *+12345678901* (E.164 format)
Human Name: e.g. *"John Smith"* (must be in quotes)
Username: e.g. *"jsmith2000"* (must be in quotes)
Network ASN: e.g. *1234*



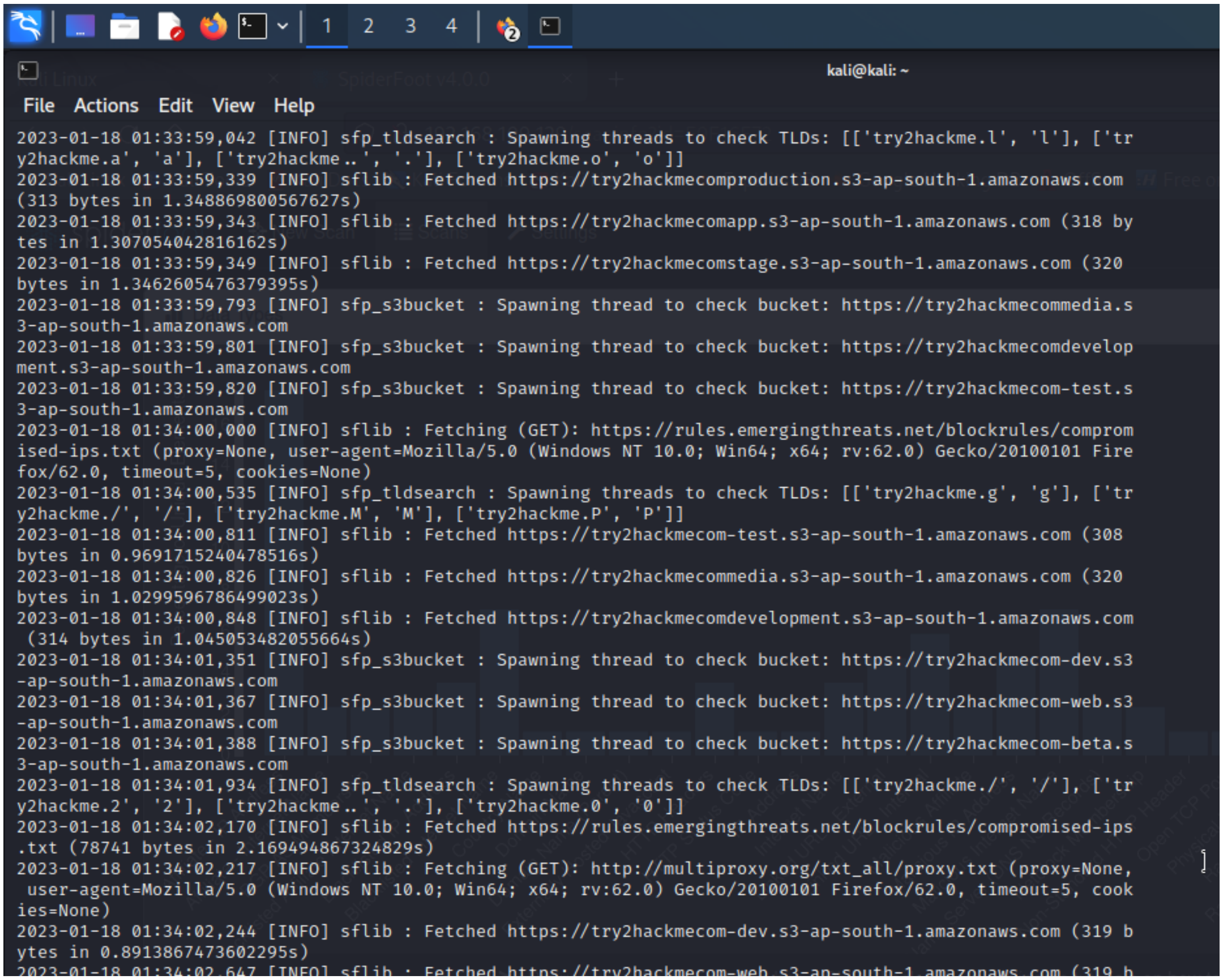




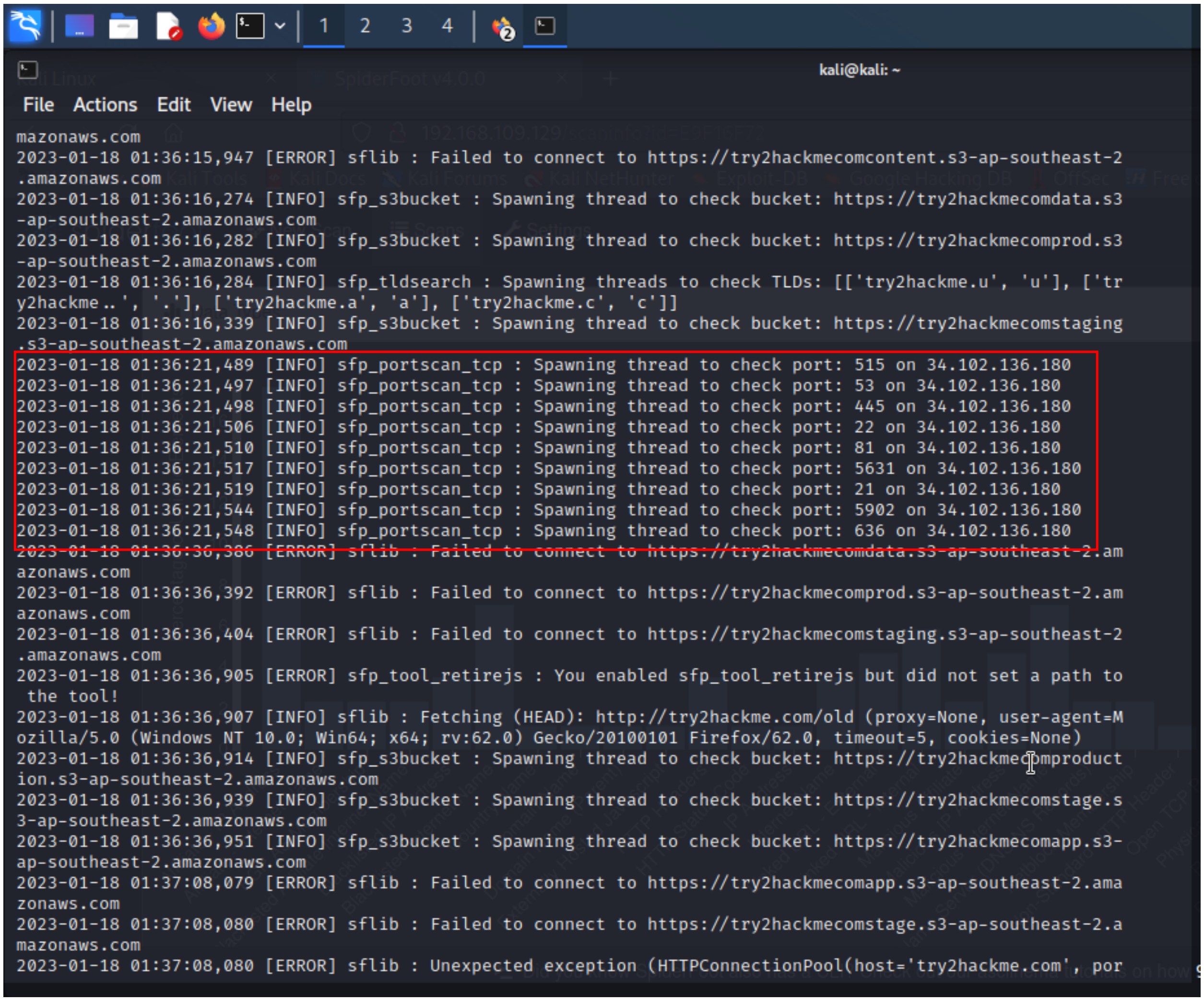
```
2023-01-18 15:21:05,069 [INFO] sflib : Fetching (GET): https://dnsdumpster.com (proxy=None, user-agent=Mozi
lla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=30, cookies=None)
2023-01-18 15:21:05,591 [INFO] sflib : Fetching (GET): https://crt.sh/?d=4841029347 (proxy=None, user-agent
=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=30, cookies=None)
2023-01-18 15:21:06,496 [INFO] sflib : Fetched https://dnsdumpster.com (14858 bytes in 1.4272420406341553s)
2023-01-18 15:21:06,649 [INFO] sflib : Fetching (POST): https://dnsdumpster.com/ (proxy=None, user-agent=Mo
zilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=30, cookies={'csrftok
en': 'qFIAsk1ve23rBGB4WgE2OYlvbG1zZOahqisTDx0WQLRo5zXZX4ot9orl6DtIvIUr'})
2023-01-18 15:21:06,737 [INFO] sflib : Fetched https://crt.sh/?d=4841029347 (1562 bytes in 1.14581751823425
3s)
2023-01-18 15:21:09,831 [INFO] sflib : Fetching (GET): https://crt.sh/?d=4506788680 (proxy=None, user-agent
=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=30, cookies=None)
2023-01-18 15:21:09,961 [INFO] sflib : Fetching (GET): https://api.github.com/search/repositories?q=try2hac
k (proxy=None, user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, t
imeout=5, cookies=None)
2023-01-18 15:21:11,061 [INFO] sflib : Fetched https://crt.sh/?d=4506788680 (1891 bytes in 1.23052215576171
88s)
2023-01-18 15:21:11,382 [INFO] sflib : Fetched https://api.github.com/search/repositories?q=try2hack (47235
 bytes in 1.4204981327056885s)
2023-01-18 15:21:11,472 [INFO] sflib : Fetching (GET): https://api.github.com/search/users?q=try2hack (prox
y=None, user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=
5, cookies=None)
2023-01-18 15:21:11,747 [INFO] sflib : Fetched https://dnsdumpster.com/ (33330 bytes in 5.098076820373535s)
2023-01-18 15:21:12,407 [INFO] sflib : Fetching (GET): https://www.threatcrowd.org/searchApi/v2/domain/repo
rt/?domain=try2hack.me (proxy=None, user-agent=SpiderFoot, timeout=5, cookies=None)
```



```
bytes in 1.0415644645690918s)
2023-01-18 01:33:37,508 [INFO] sflib : Fetched https://try2hackmecomcontent.s3.ap-south-1.amazonaws.com (31
0 bytes in 1.1858758926391602s)
2023-01-18 01:33:37,834 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomdata.s3
.ap-south-1.amazonaws.com
2023-01-18 01:33:37,845 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomprod.s3
.ap-south-1.amazonaws.com
2023-01-18 01:33:37,856 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomstaging
.s3.ap-south-1.amazonaws.com
2023-01-18 01:33:38,099 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['try2hackme.o', 'o'], ['tr
y2hackme.f', 'f'], ['try2hackme.t', 't'], ['try2hackme.h', 'h']]
2023-01-18 01:33:38,192 [INFO] sfp_grep_app : Parsing page 1 of 0
2023-01-18 01:33:38,205 [ERROR] sfp_alienvault : You enabled sfp_alienvault but did not set an API key!
2023-01-18 01:33:38,205 [ERROR] sfp_googlesafebrowsing : You enabled sfp_googlesafebrowsing but did not set
 an API key!
2023-01-18 01:33:38,250 [INFO] sflib : Fetching (GET): https://raw.githubusercontent.com/client9/ipcat/mast
er/datacenters.csv (proxy=None, user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/2010010
1 Firefox/62.0, timeout=30, cookies=None)
2023-01-18 01:33:38,928 [INFO] sflib : Fetched https://try2hackmecomprod.s3.ap-south-1.amazonaws.com (307 b
ytes in 1.0769760608673096s)
2023-01-18 01:33:39,035 [INFO] sflib : Fetched https://try2hackmecomdata.s3.ap-south-1.amazonaws.com (307 b
ytes in 1.198898315429687 5s)
2023-01-18 01:33:39,080 [INFO] sflib : Fetched https://try2hackmecomstaging.s3.ap-south-1.amazonaws.com (31
0 bytes in 1.2164289951324463s)
2023-01-18 01:33:39,375 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomproduct
ion.s3.ap-south-1.amazonaws.com
2023-01-18 01:33:39,382 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomstage.s
3.ap-south-1.amazonaws.com
2023-01-18 01:33:39,391 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomapp.s3.
ap-south-1.amazonaws.com
2023-01-18 01:33:39,470 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['try2hackme.M', 'M'], ['tr
y2hackme.P', 'P'], ['try2hackme.L', 'L'], ['try2hackme.w', 'w']]
2023-01-18 01:33:39,608 [INFO] sflib : Fetched https://raw.githubusercontent.com/client9/ipcat/master/datac
enters.csv (229270 bytes in 1.3582346439361572s)
2023-01-18 01:33:39,840 [ERROR] sfp_ipstack : You enabled sfp_ipstack but did not set an API key!
2023-01-18 01:33:39,840 [ERROR] sfp_onyphe : You enabled sfp_onyphe, but did not set an API key!
2023-01-18 01:33:39,845 [ERROR] sfp_ipregistry : You enabled sfp_ipregistry but did not set an API key!
2023-01-18 01:33:40,254 [INFO] sflib : Fetching (GET): https://api.maltiverse.com/ip/34.102.136.180 (proxy=
None, user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=15
, cookies=None)
2023-01-18 01:33:40,265 [INFO] sflib : Fetched https://try2hackmecomstage.s3.ap-south-1.amazonaws.com (308
```



```
2023-01-18 01:33:59,042 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['try2hackme.l', 'l'], ['tr
y2hackme.a', 'a'], ['try2hackme..', '.'], ['try2hackme.o', 'o']]
2023-01-18 01:33:59,339 [INFO] sflib : Fetched https://try2hackmecomproduction.s3-ap-south-1.amazonaws.com
(313 bytes in 1.348869800567627s)
2023-01-18 01:33:59,343 [INFO] sflib : Fetched https://try2hackmecomapp.s3-ap-south-1.amazonaws.com (318 by
tes in 1.307054042816162s)
2023-01-18 01:33:59,349 [INFO] sflib : Fetched https://try2hackmecomstage.s3-ap-south-1.amazonaws.com (320
bytes in 1.3462605476379395s)
2023-01-18 01:33:59,793 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecommedia.s
3-ap-south-1.amazonaws.com
2023-01-18 01:33:59,801 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomdevelop
ment.s3-ap-south-1.amazonaws.com
2023-01-18 01:33:59,820 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecom-test.s
3-ap-south-1.amazonaws.com
2023-01-18 01:34:00,000 [INFO] sflib : Fetching (GET): https://rules.emergingthreats.net/blockrules/comprom
ised-ips.txt (proxy=None, user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Fire
fox/62.0, timeout=5, cookies=None)
2023-01-18 01:34:00,535 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['try2hackme.g', 'g'], ['tr
y2hackme./', '/'], ['try2hackme.M', 'M'], ['try2hackme.P', 'P']]
2023-01-18 01:34:00,811 [INFO] sflib : Fetched https://try2hackmecom-test.s3-ap-south-1.amazonaws.com (308
bytes in 0.9691715240478516s)
2023-01-18 01:34:00,826 [INFO] sflib : Fetched https://try2hackmecommedia.s3-ap-south-1.amazonaws.com (320
bytes in 1.0299596786499023s)
2023-01-18 01:34:00,848 [INFO] sflib : Fetched https://try2hackmecomdevelopment.s3-ap-south-1.amazonaws.com
 (314 bytes in 1.045053482055664s)
2023-01-18 01:34:01,351 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecom-dev.s3
-ap-south-1.amazonaws.com
2023-01-18 01:34:01,367 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecom-web.s3
-ap-south-1.amazonaws.com
2023-01-18 01:34:01,388 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecom-beta.s
3-ap-south-1.amazonaws.com
2023-01-18 01:34:01,934 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['try2hackme./', '/'], ['tr
y2hackme.2', '2'], ['try2hackme..', '.'], ['try2hackme.0', '0']]
2023-01-18 01:34:02,170 [INFO] sflib : Fetched https://rules.emergingthreats.net/blockrules/compromised-ips
.txt (78741 bytes in 2.169494867324829s)
2023-01-18 01:34:02,217 [INFO] sflib : Fetching (GET): http://multiproxy.org/txt_all/proxy.txt (proxy=None,
 user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=5, cook
ies=None)
2023-01-18 01:34:02,244 [INFO] sflib : Fetched https://try2hackmecom-dev.s3-ap-south-1.amazonaws.com (319 b
ytes in 0.8913867473602295s)
2023-01-18 01:34:02,647 [INFO] sflib : Fetched https://try2hackmecom-web.s3-ap-south-1.amazonaws.com (319 b
```

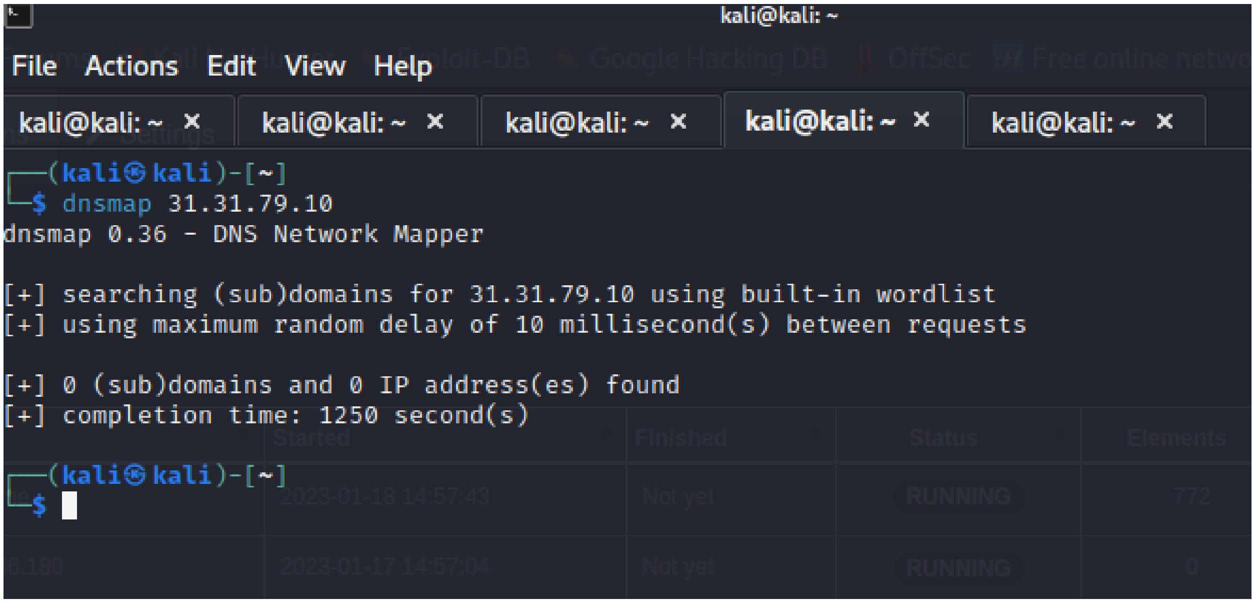


```
mazonaws.com
2023-01-18 01:36:15,947 [ERROR] sflib : Failed to connect to https://try2hackmecomcontent.s3-ap-southeast-2
.amazonaws.com
2023-01-18 01:36:16,274 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomdata.s3
-ap-southeast-2.amazonaws.com
2023-01-18 01:36:16,282 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomprod.s3
-ap-southeast-2.amazonaws.com
2023-01-18 01:36:16,284 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['try2hackme.u', 'u'], ['tr
y2hackme..', '.'], ['try2hackme.a', 'a'], ['try2hackme.c', 'c']]
2023-01-18 01:36:16,339 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomstaging
.s3-ap-southeast-2.amazonaws.com
2023-01-18 01:36:21,489 [INFO] sfp_portscan_tcp : Spawning thread to check port: 515 on 34.102.136.180
2023-01-18 01:36:21,497 [INFO] sfp_portscan_tcp : Spawning thread to check port: 53 on 34.102.136.180
2023-01-18 01:36:21,498 [INFO] sfp_portscan_tcp : Spawning thread to check port: 445 on 34.102.136.180
2023-01-18 01:36:21,506 [INFO] sfp_portscan_tcp : Spawning thread to check port: 22 on 34.102.136.180
2023-01-18 01:36:21,510 [INFO] sfp_portscan_tcp : Spawning thread to check port: 81 on 34.102.136.180
2023-01-18 01:36:21,517 [INFO] sfp_portscan_tcp : Spawning thread to check port: 5631 on 34.102.136.180
2023-01-18 01:36:21,519 [INFO] sfp_portscan_tcp : Spawning thread to check port: 21 on 34.102.136.180
2023-01-18 01:36:21,544 [INFO] sfp_portscan_tcp : Spawning thread to check port: 5902 on 34.102.136.180
2023-01-18 01:36:21,548 [INFO] sfp_portscan_tcp : Spawning thread to check port: 636 on 34.102.136.180
2023-01-18 01:36:36,386 [ERROR] sflib : Failed to connect to https://try2hackmecomdata.s3-ap-southeast-2.am
azonaws.com
2023-01-18 01:36:36,392 [ERROR] sflib : Failed to connect to https://try2hackmecomprod.s3-ap-southeast-2.am
azonaws.com
2023-01-18 01:36:36,404 [ERROR] sflib : Failed to connect to https://try2hackmecomstaging.s3-ap-southeast-2
.amazonaws.com
2023-01-18 01:36:36,905 [ERROR] sfp_tool_retirejs : You enabled sfp_tool_retirejs but did not set a path to
 the tool!
2023-01-18 01:36:36,907 [INFO] sflib : Fetching (HEAD): http://try2hackme.com/old (proxy=None, user-agent=M
ozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=5, cookies=None)
2023-01-18 01:36:36,914 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomproduct
ion.s3-ap-southeast-2.amazonaws.com
2023-01-18 01:36:36,939 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomstage.s
3-ap-southeast-2.amazonaws.com
2023-01-18 01:36:36,951 [INFO] sfp_s3bucket : Spawning thread to check bucket: https://try2hackmecomapp.s3-
ap-southeast-2.amazonaws.com
2023-01-18 01:37:08,079 [ERROR] sflib : Failed to connect to https://try2hackmecomapp.s3-ap-southeast-2.ama
zonaws.com
2023-01-18 01:37:08,080 [ERROR] sflib : Failed to connect to https://try2hackmecomstage.s3-ap-southeast-2.a
mazonaws.com
2023-01-18 01:37:08,080 [ERROR] sflib : Unexpected exception (HTTPConnectionPool(host='try2hackme.com', por
```

With the help of this tool, we found the **phone numbers, email addresses, IP Addresses, IPv6 Addresses, Internet Name, Open TCP Port, DNS TXT Records, Domain Name of the target**. With the help of this tool, we can create graphs of scanning done by Spiderfoot. We simply specified the target we wanted to investigate, picked which modules to enable and then used SpiderFoot will collect data.

Dnsmap

Dnsmap tells the subdomain of the website. DNSMAP, as the name suggests, is DNS Network Mapper, which is used for multiple purposes. Basically, DNSMAP is a passive Network Mapper, often called a sub domain brute force tool. This tool is mainly used by penetration testers and hackers for DNS and sub domain information gathering. It is similar to most other DNS information gathering tools.

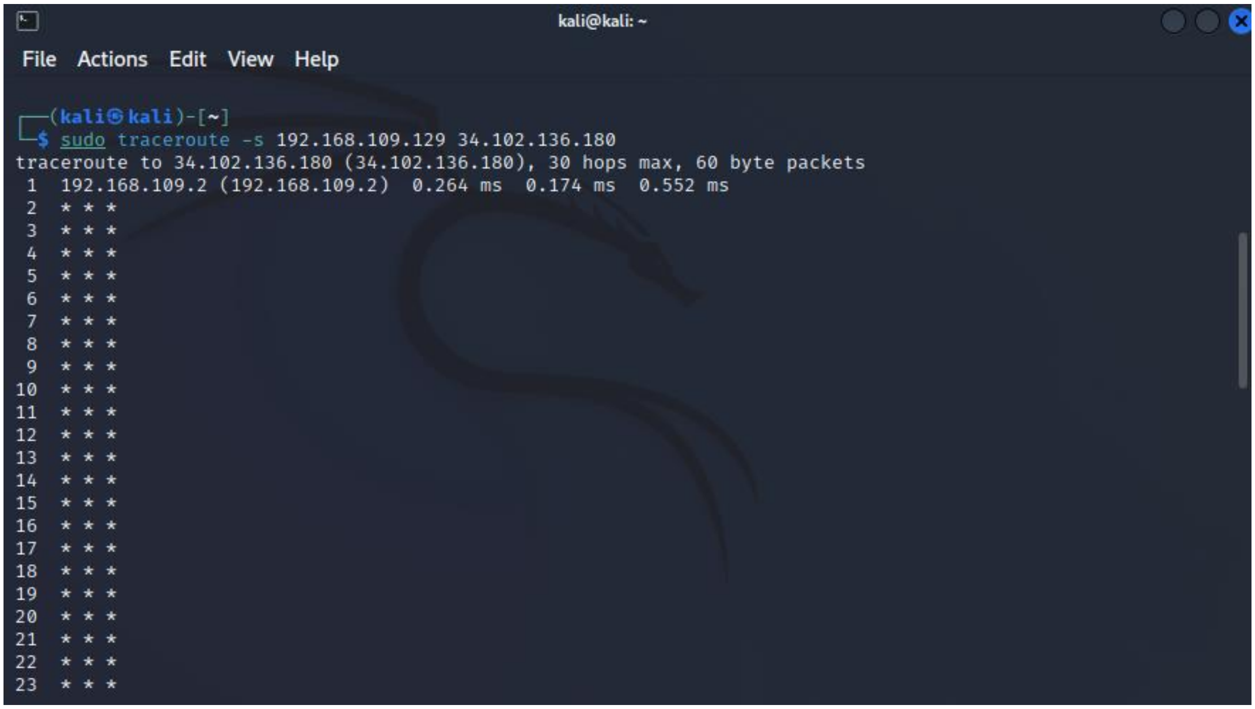


```
┌──(kali㉿kali)-[~]
└─$ dnsmap 31.31.79.10
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for 31.31.79.10 using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

[+] 0 (sub)domains and 0 IP address(es) found
[+] completion time: 1250 second(s)

┌──(kali㉿kali)-[~]
└─$ 
```

The above image says 0 (sub)domains found which means there is **no subdomain of the website** Try2Hack.me

Traceroute

The traceroute command is used to determine the path between two connections. Often a connection to another device will have to go through multiple routers.



```
┌──(kali㉿kali)-[~]
└─$ sudo traceroute -s 192.168.109.129 34.102.136.180
traceroute to 34.102.136.180 (34.102.136.180), 30 hops max, 60 byte packets
 1  192.168.109.2 (192.168.109.2)  0.264 ms  0.174 ms  0.552 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
```

The Traceroute command provided with the information about how many hops are required to reach from one IP to the other.

CONCLUSION AND FINDINGS:

Summarizing our applied project, we got to learn about many new tools of Kali Linux which were very helpful in scanning and finding vulnerabilities of the website we chose. Try2Hack.Me is a website where we can test and practice our ethical hacking skills. The information we gathered can be used to access the website. Moreover, any data found about the website can be uploaded on Dark Web, which can be dangerous for the website owners. For instance, we can use the emails and other information found to perform any kind of social engineering attacks. Moreover, this project can be very helpful for website owners to enhance their security system.

FINDINGS:

- Domain name
- IP Address
- DNS Servers
- Employee Data
- Email Addresses
- Open Ports

TOOLS USED:

- Whois
- Nmap
- Spiderfoot
- Dnsmap
- Traceroute