Sri Lanka Institute of Information Technology

Final Assignment- Web Audit Report

IE2062 – Web Security

Submitted by:

Student Registration Number	Student Name
IT20618872	Thisitha K.L.D

Date of submission

06/5/2022

Table of Contents

Bug Bounty Hunting

Trojan horse bounty looking is a reputed field in cyber security area. It wishes a whole lot of experience And sharp competencies to carry out such activities related with bug bounty looking. More regularly, bug Bounties are completed by means of people. And for those worm looking's they'll be rewarded with Cash. Worm bounty systems will offer the desired internet programs for enumerate.

What is Bug Bounty?

It's far a continual safety exam that permits firms to protect in opposition to cyber assaults, Information theft, and misuse. Security trying out is accomplished with the aid of ethical hackers who're compensated for Identifying flows and vulnerabilities in services and alertness with a coin's prize.

In malicious program bounty schemes, the ethical hacker is rewarded simplest if he or she discovers a Meaningful vulnerability within the machine. By way of comparison, the company must pay for the Penetration check although no security vulnerability is discovered.

In preference to pen-testing, that is restricted to a single moral hacker or a small organization of Testers, trojan horse bounty trying out isn't constrained to a single moral hacker or a small group of testers. Your Product is examined within the worm bounty program by means of tens of loads of moral hackers who compete Against each other to find the fault first and earn a fee. However, the disadvantage of bug bounty schemes is, in maximum situations, their public nature.

It establishes that moral hackers can check most effective publicly to be had quantities of websites, Programs, or user interfaces inside many situations. Normally, applications with No outside get right of entry to cannot be tested. Then again, the option to permit hackers to test the Manufacturing or trying out surroundings is absolutely as much as the enterprise.

Likewise, there are cos and professionals in malicious program bounty programs.

Cos & execs in worm Bounty

Advantages	**Disadvantages**
Output is varied over a longer period of time	Only software/hardware which is available online can be tested by hunters
Will detect rare vulnerabilities. And weird scenarios.	Less complexity in compare with penetration tests.
Hunters will be varied, from education skill, continent this will help to cover vast area of the application.	Hunters may report false vulnerabilities in order to gain amends.
Continuous testing will available as new hunters will attempt everyday.	If the reward is low, bounty hunters will not interact much.
Possibility of testing in production and/or test environment.	Cannot be guaranteed the reports and attacks.
Low prices owners have the authority to make the values for sorted vulnerabilities.	The area specified by the company may not be enough for security strengthen.

Penetration trying out of high high-quality are high-priced and time-ingesting. They're completed by using Security professionals whose time is treasured and constrained. Moreover, they require Widespread guidance – each formal and technical – for the established order of test instances as they're typically tested in a look at surroundings in place of a production surroundings.

They do but offer a thorough image of the present-day degree of safety for online Undertaking and the infrastructure that supports it. Typically, a protection company takes 1-2 weeks to carry out A pen-check, and its result is a manually checked document containing vulnerabilities, their locations, And the potential effect of misuse. The gain is that it allows testing of formerly Unpublished web sites, apps, and goods.

Trojan horse praise programs, however, are more cost powerful. They are expected to Take an extended quantity of time (at least numerous months), to spread the cost of paying White hat hackers across time. It is as much as the company or agency to determine what will be examined and How an awful lot money may be paid for security faults.

But a time without determined vulnerabilities is feasible - whilst rewards Are located in an unattractive way for ethical hackers. On the other side, reasonably exceptional

Vulnerability output, that's frequently the end result of sizeable guide testing, is beneficial to a Agency. That is a critical difference from much less luxurious automatic scanning — the computer virus Bounty program enlists a large group of ethical hackers from across the world with varying Levels of expertise and training. Additionally, they are able to find unusual security flaws that Even the most pricey penetration examinations may also miss.

Web Audit & Vulnerability Assessment

Security audits and vulnerability exams each precaution are taken to make sure the Vigilance of the internet software. To make certain the vulnerability unfastened surroundings might be kept in the packages these approaches should be followed and necessary steps ought to be taken Periodically. Both tests ought to be executed time and again, it is not sufficient if it runs one Time, and results have been best, no longer to observe up once more. Because as cyber space is changing hastily and on the identical time more vulnerabilities will evolve and arise.

Security Audit

A safety audit is the first phase in securing IT infrastructure and may be characterized as a rigorous exam of the safety of business's IT infrastructure. Protection professionals Will grade the diploma to which, security methods adhere to a list of targeted criteria in Order to validate its protection aspect.

IT infrastructure safety audits should be complete and systematic with a view to Protect corporations or firms’ statistics and IT assets. In case your quarter is noticeably regulated, partaking in This pastime may also assist enterprise by making sure compliance with guidelines together with GDPR, HIPPA, SOX, and PCI-DSS.

Standardized evaluation of a Web Audit:

- Email
- Information handling processes
- Hardware configurations
- Data and access-related details
- User practices
- Networks

Any of the subsequent need to be evaluated in light of previous and potential destiny problems. Which means that your safety body of workers need to be informed at the modern-day protection trends and the Responses made via different firms.

Vulnerability Assessment

Vulnerability evaluation is a manner that makes use of computerized testing gear to identify risks and threats. Due to the reality that safety flaws would possibly permit cyber attackers to breach an employer's
Records generation systems, it's far important to discover and restore vulnerabilities before their Being infiltrated and exploited. Vulnerability evaluation is critical because it informs a business enterprise Approximately its vulnerabilities and gives solutions for assessing them.
Vulnerability assessment responsibilities consist of figuring out, quantifying, and classifying regarded Security flaws in packages, hardware and software program systems, and network infrastructure. Moreover, it illustrates the ramifications of a hypothetical situation the usage of the discovered security Weak spot.
Additionally, vulnerability evaluation generates and refines an approach and sensible Technique for responding to threats. Eventually, it's miles responsible for making recommendations to Improve an agency's safety procedures.

Vulnerability assessment has four predominant additives, the ones are,

1.Initial assessment
2.Defining system baseline
3.Vulnerability scanning
4.Vulnerability Assessment report

Experiences

This become the very first time I tried to do this kind of pastime which turned into honestly a laugh and Exciting, a long way greater higher it become very useful to benefit new abilities. On the other hand, it changed into a superb Assist to run through numerous articles and reports, because it became no longer the most favored manner of Operating as youngers. We use generation for every type of things and have become lazy to examine. But because of this I needed to undergo wide variety of articles the ones have been written by nicely reputed ethical Hackers. Because of this I had the threat to get stimulated by using the best humans running in the Domain.

Nevertheless, in case of locating insects I needed to move slowly via lot of web sites. As active scans Are greater alarming and it's going to block the Ip cope within case we get stuck, I generally tend to observe passive
Scanning lots extra. As for passive scanning there are ardent equipment, there are wonderful number of Complete gears have evolved for every specialized task, consequently passive scanning is lot Simpler and more fruitful than walking lively scans on websites. And I've discovered lot of tools and Command with the intention to be high-quality asset for my destiny endeavors.

There are lot of systems based totally on how the internet utility has been evolved, I am getting the Risk to have a slighter concept approximately this massive region by way of interacting this mission.

I decided on Tinder.com corporation's subdomains as the subjected website. Before that I tried Western Union websites, grasp Card, and lot more. Amongst those site credit card required a unique manner to Run audits and scans on its subdomains. I needed to create a bug crowd email and log in to the MasterCard page on bug crowd. I attempted to this but lamentably, I failed to log in to this web site Efficaciously.

So, after numerous failed tries i was compelled to pick out some other domain that's OLX.Com Company's domains. The main hassle I came throughout with website online is it changed into surely already near to Ideal, as i used to be a new one too, it turned into very difficult to find insects. But being thankful to "Netsparker" which runs complete automated web scanner I used to be capable of find some
Insects, and as for my marvel a essential computer virus as well.

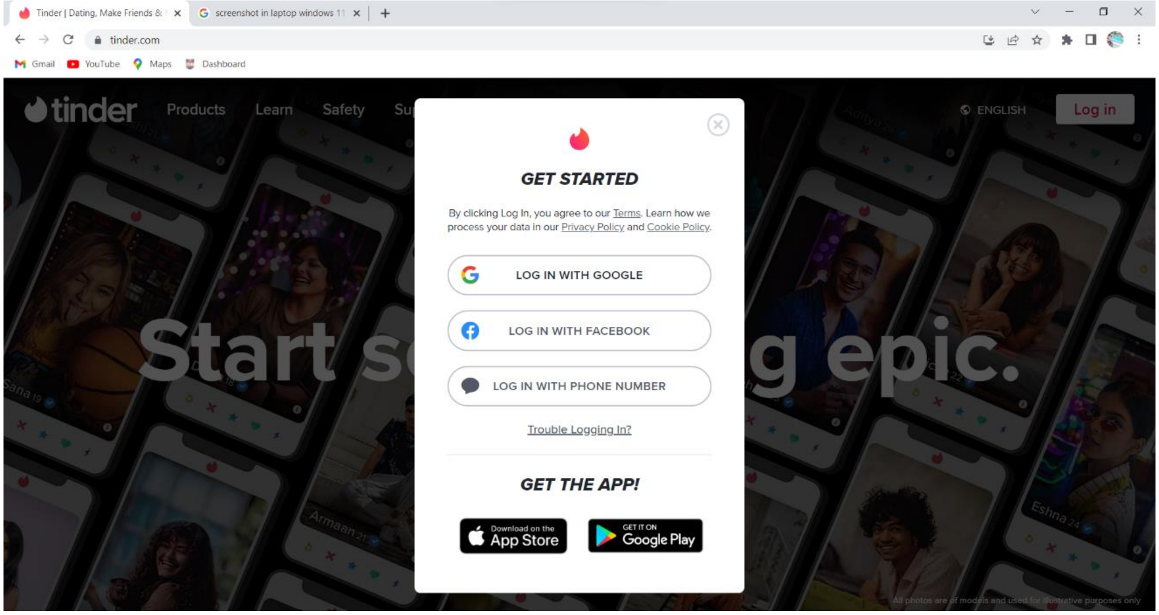
After appearing that I grew to become to find those insects manually before that I should acquire all Sort of data. More technical smart reconnaissance segment. I did this part as I've noted Above, the usage of massive range of tools and direct scans. The vital fact is that huge wide variety of tools are doing passive scans they move slowly through google and experiment the consequences which can be related to the use of that knowledge they acquire data. It's miles more secure than guide scanning as it's far immediately Handling the unique sites. And single mistake could damage to the gadget as well.

Introduction of web site

Web link - https://tinder.com/

It is a social media platform and online dating application.

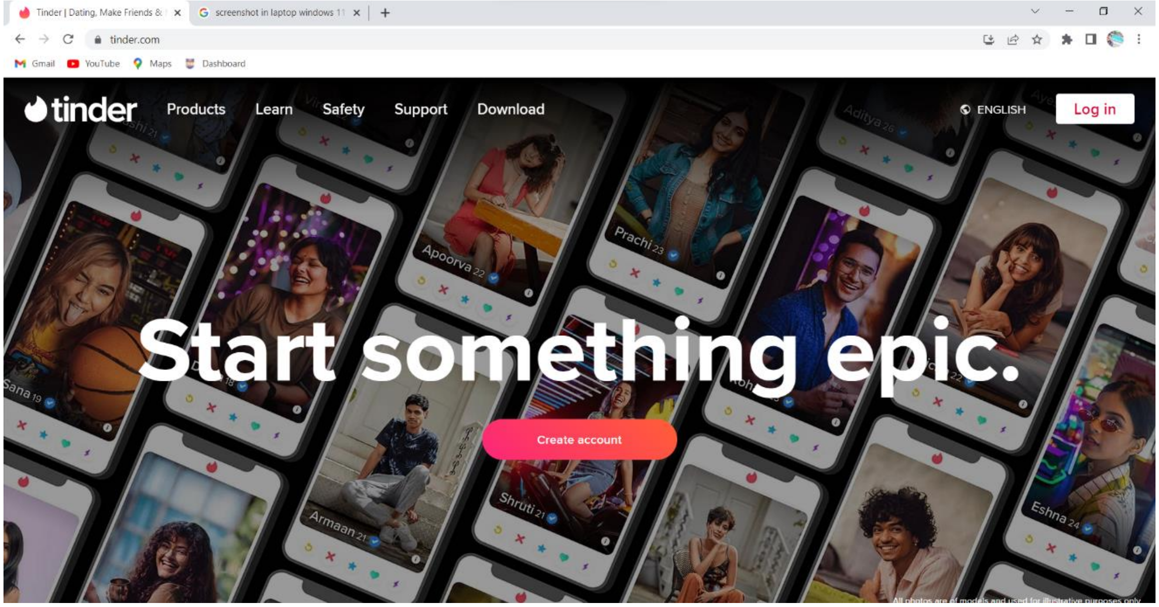
1.Logging page



By clicking Log In, you agree to our Terms. Learn how we process your data in our Privacy Policy and Cookie Policy.

All photos are of models and used for illustrative purposes only

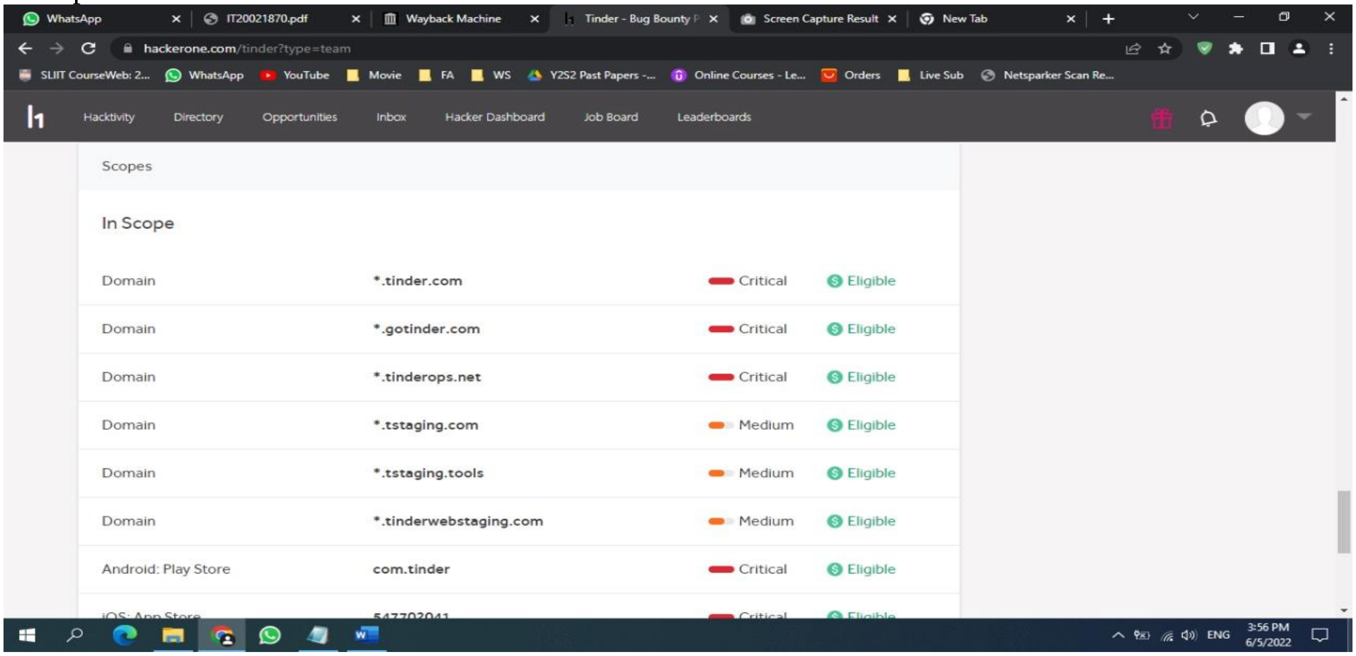
2.After logged



All photos are of models and used for illustrative purposes only

Scopes

Inscope

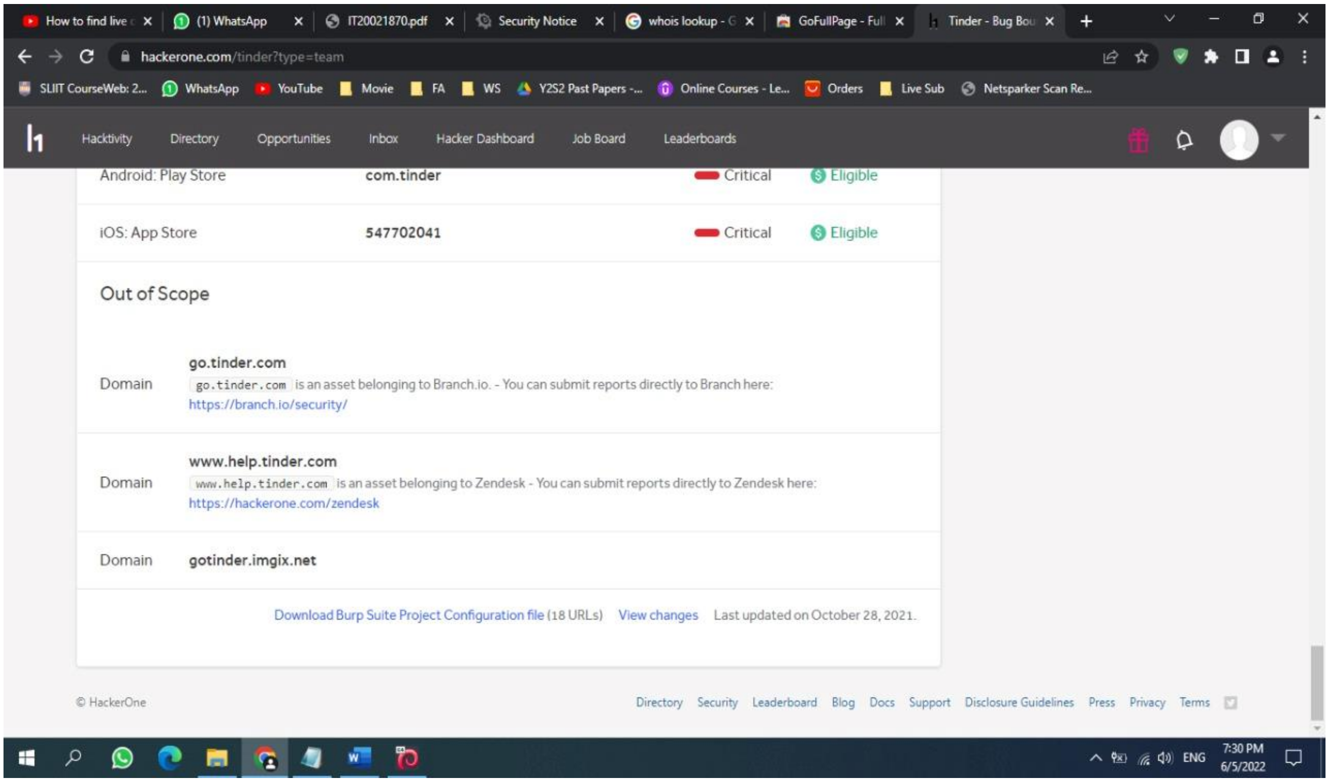


Scopes

In Scope

Domain	*.tinder.com	Critical	Eligible
Domain	*.gotinder.com	Critical	Eligible
Domain	*.tinderops.net	Critical	Eligible
Domain	*.tstaging.com	Medium	Eligible
Domain	*.tstaging.tools	Medium	Eligible
Domain	*.tinderwebstaging.com	Medium	Eligible
Android: Play Store	com.tinder	Critical	Eligible
iOS: App Store	547702041	Critical	Eligible

Out of scope



Android: Play Store	com.tinder	Critical	Eligible
iOS: App Store	547702041	Critical	Eligible

Out of Scope

Domain — **go.tinder.com**
`go.tinder.com` is an asset belonging to Branch.io. - You can submit reports directly to Branch here: https://branch.io/security/

Domain — **www.help.tinder.com**
`www.help.tinder.com` is an asset belonging to Zendesk - You can submit reports directly to Zendesk here: https://hackerone.com/zendesk

Domain — **gotinder.imgix.net**

Download Burp Suite Project Configuration file (18 URLs) View changes Last updated on October 28, 2021.

© HackerOne

FIND SUBDOMAINS

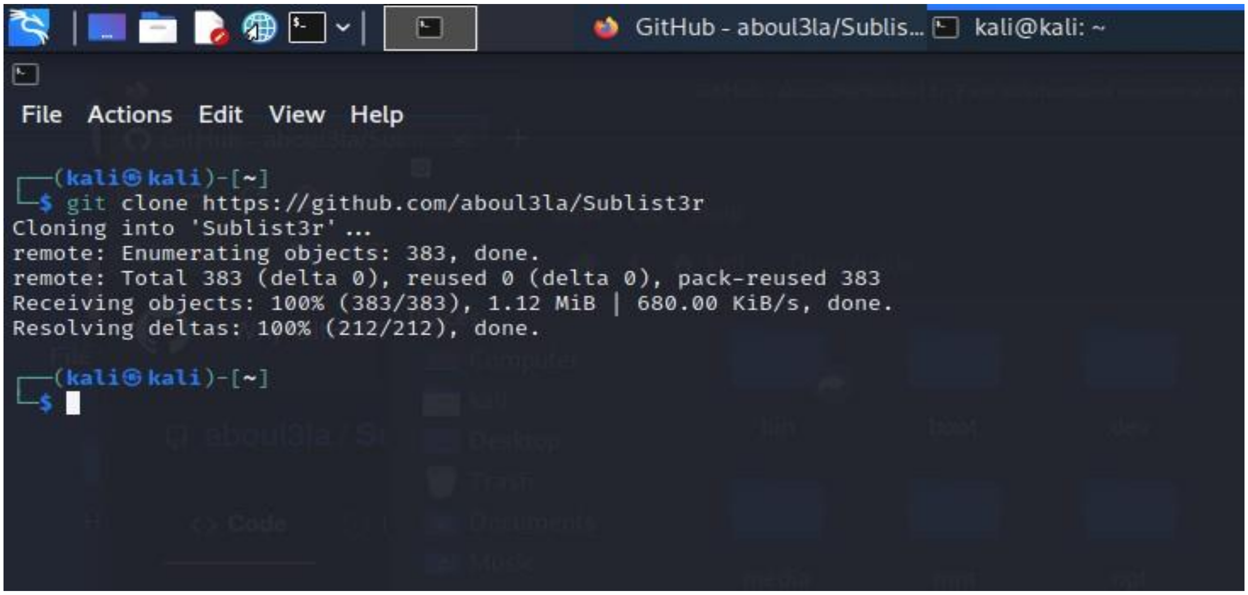
There are several tools for using finding subdomains.

1. Sublist3r
2. Recon-ng
3. Amass
4. SubBrute
5. Knock
6. DNSRecon
7. AltDNS
8. Axiom
9. Haktrails

Sublist3r tool

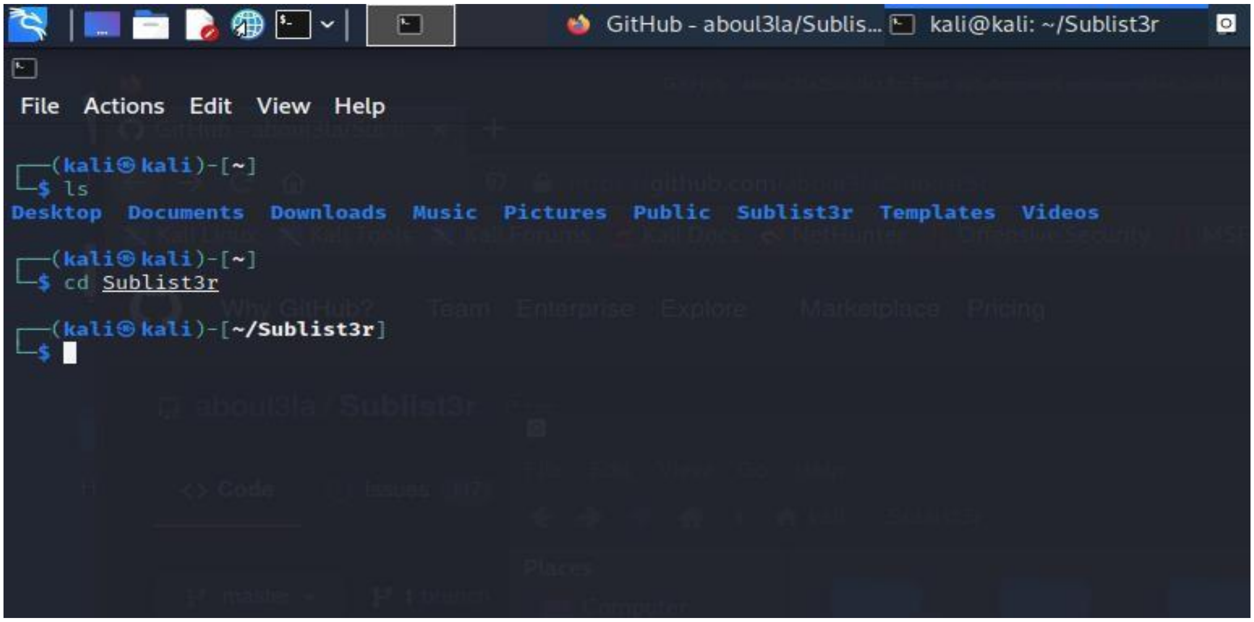
Download link- - https://github.com/aboul3la/Sublist3r.git

Download sublist3r tool from git clone



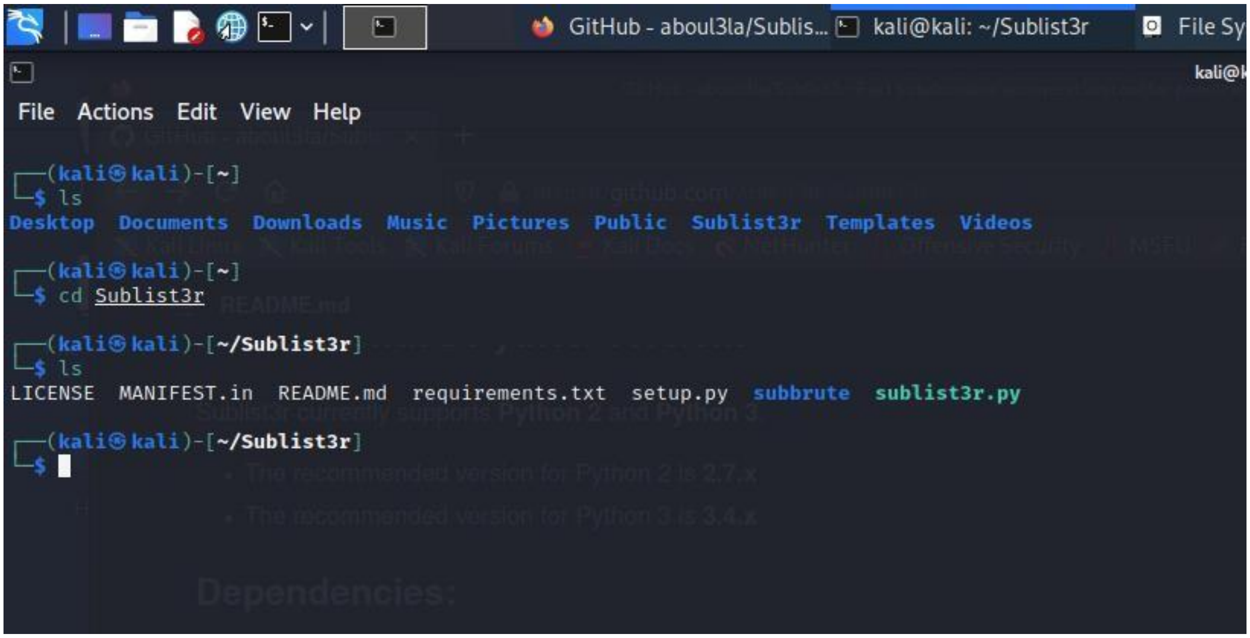
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/aboul3la/Sublist3r
Cloning into 'Sublist3r'...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383
Receiving objects: 100% (383/383), 1.12 MiB | 680.00 KiB/s, done.
Resolving deltas: 100% (212/212), done.

┌──(kali㉿kali)-[~]
└─$ 
```

Secondly downloaded folder



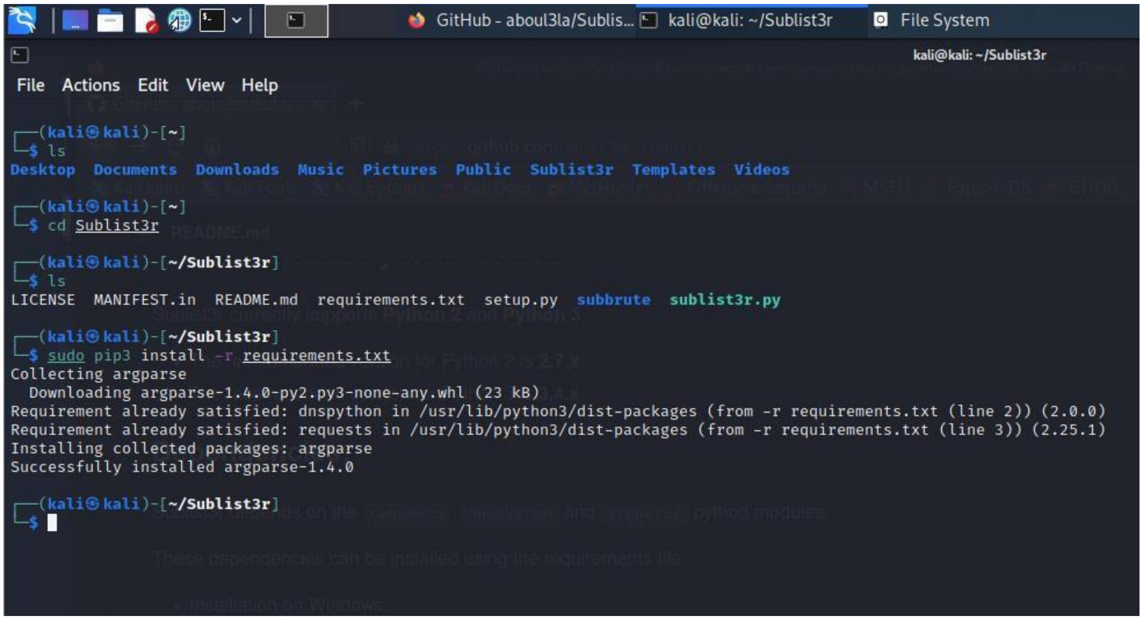
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Sublist3r  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd Sublist3r

┌──(kali㉿kali)-[~/Sublist3r]
└─$ 
```

Check sublist3r folder using this command



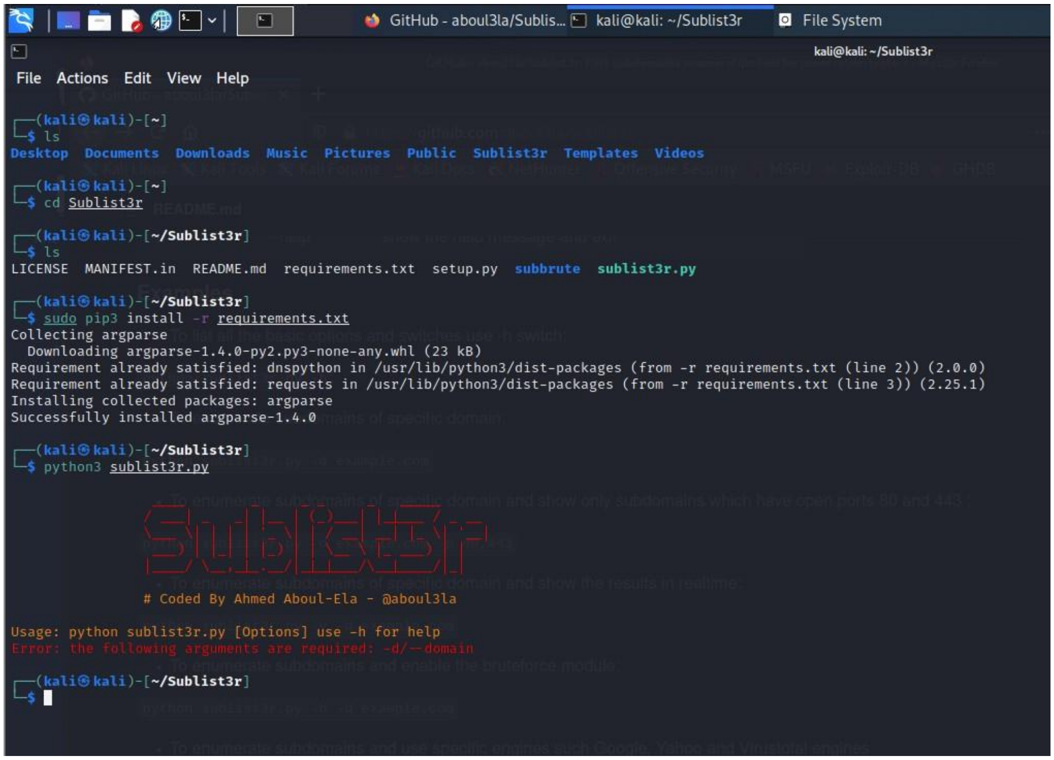
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Sublist3r  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd Sublist3r

┌──(kali㉿kali)-[~/Sublist3r]
└─$ ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py

┌──(kali㉿kali)-[~/Sublist3r]
└─$ 
```

Install requirements.txt file



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Sublist3r  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd Sublist3r

┌──(kali㉿kali)-[~/Sublist3r]
└─$ ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py

┌──(kali㉿kali)-[~/Sublist3r]
└─$ sudo pip3 install -r requirements.txt
Collecting argparse
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.0.0)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.25.1)
Installing collected packages: argparse
Successfully installed argparse-1.4.0

┌──(kali㉿kali)-[~/Sublist3r]
└─$ 
```

It is working



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Sublist3r  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd Sublist3r

┌──(kali㉿kali)-[~/Sublist3r]
└─$ ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py

┌──(kali㉿kali)-[~/Sublist3r]
└─$ sudo pip3 install -r requirements.txt
Collecting argparse
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.0.0)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.25.1)
Installing collected packages: argparse
Successfully installed argparse-1.4.0

┌──(kali㉿kali)-[~/Sublist3r]
└─$ python3 sublist3r.py

                # Coded By Ahmed Aboul-Ela - @aboul3la

Usage: python sublist3r.py [Options] use -h for help
Error: the following arguments are required: -d/--domain

┌──(kali㉿kali)-[~/Sublist3r]
└─$ 
```

Our tool is ready. Then, Use the following command to find subdomains.

“ Python3 sublist3r.py tinder.com “

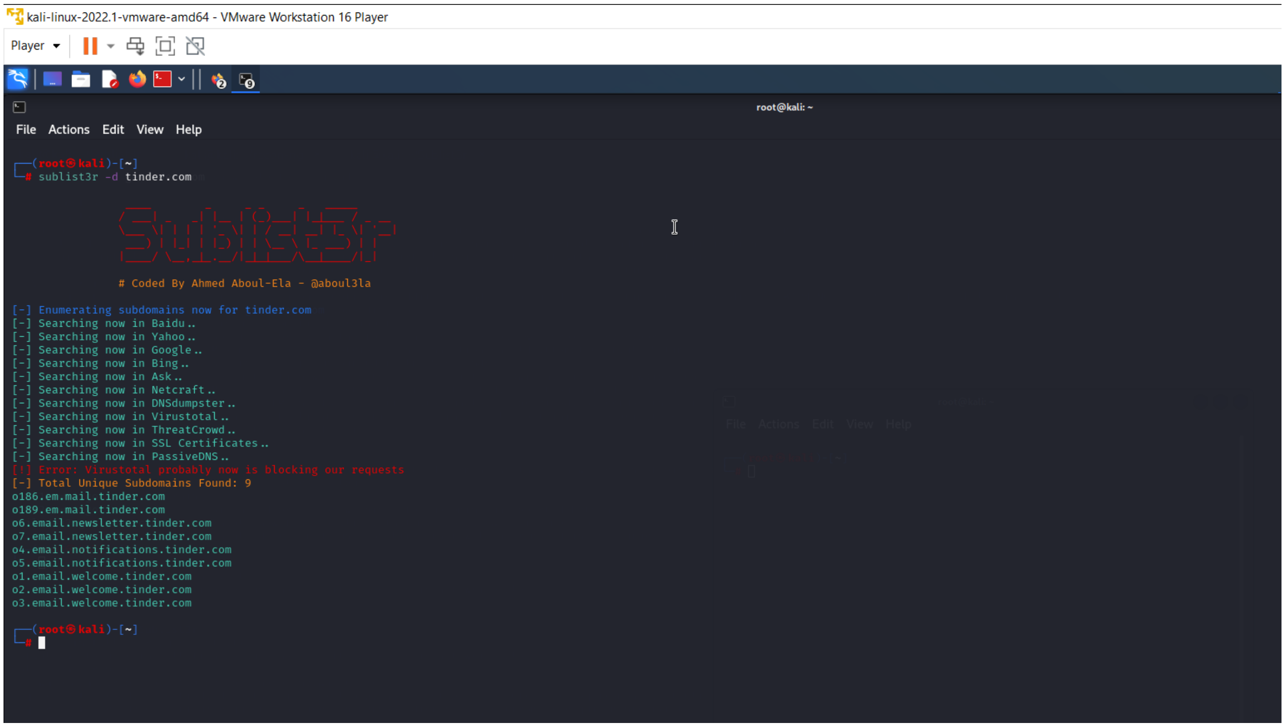
Now, you can see how the

subdomains are scanning.

My domain name is

http://www.tinder.com.

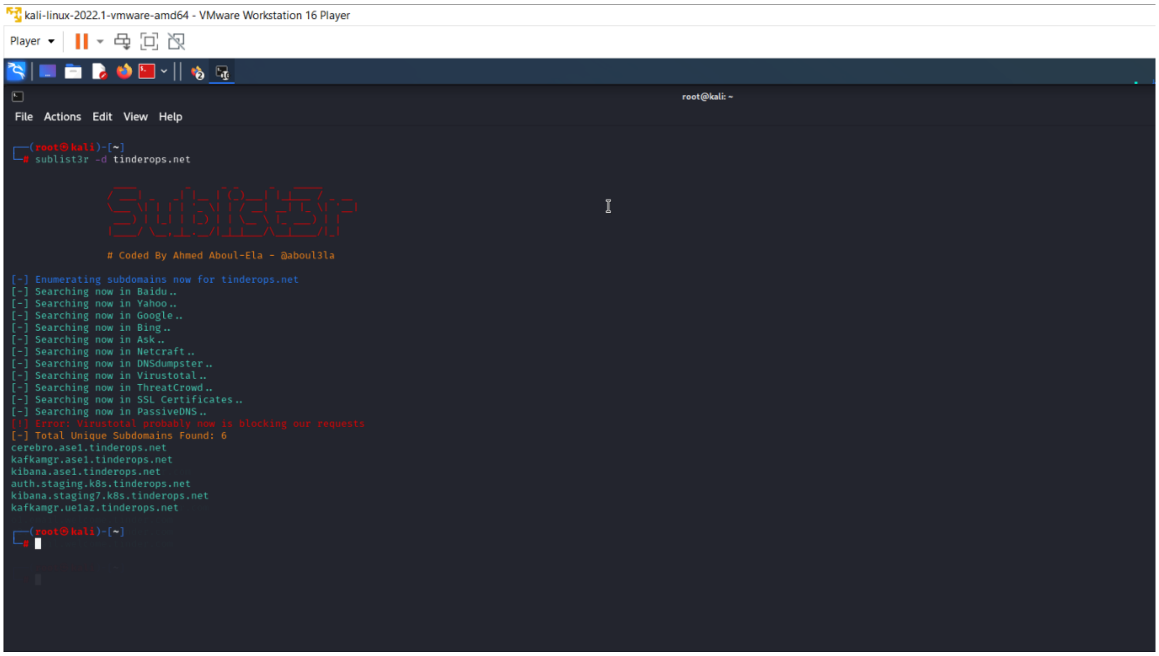
It has 9 sub domains


kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player
Player
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# sublist3r -d tinder.com

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tinder.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..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 9
o186.em.mail.tinder.com
o189.em.mail.tinder.com
o6.email.newsletter.tinder.com
o7.email.newsletter.tinder.com
o4.email.notifications.tinder.com
o5.email.notifications.tinder.com
o1.email.welcome.tinder.com
o2.email.welcome.tinder.com
o3.email.welcome.tinder.com

┌──(root㉿kali)-[~]
└─# 
```

Domain name is tinderops.net

It has 6 domains

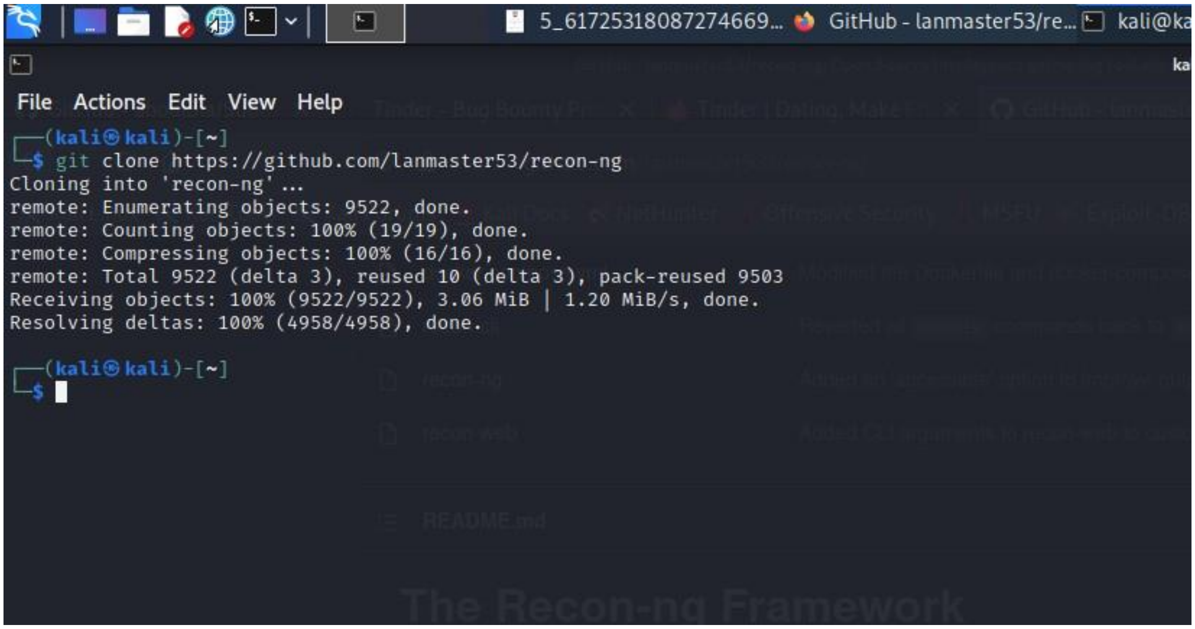

kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player
Player
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# sublist3r -d tinderops.net

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tinderops.net
[-] 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..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 6
cerebro.ase1.tinderops.net
kafkamgr.ase1.tinderops.net
kibana.ase1.tinderops.net
auth.staging.k8s.tinderops.net
kibana.staging7.k8s.tinderops.net
kafkamgr.ue1az.tinderops.net

┌──(root㉿kali)-[~]
└─# 
```

Recon-ng Tool

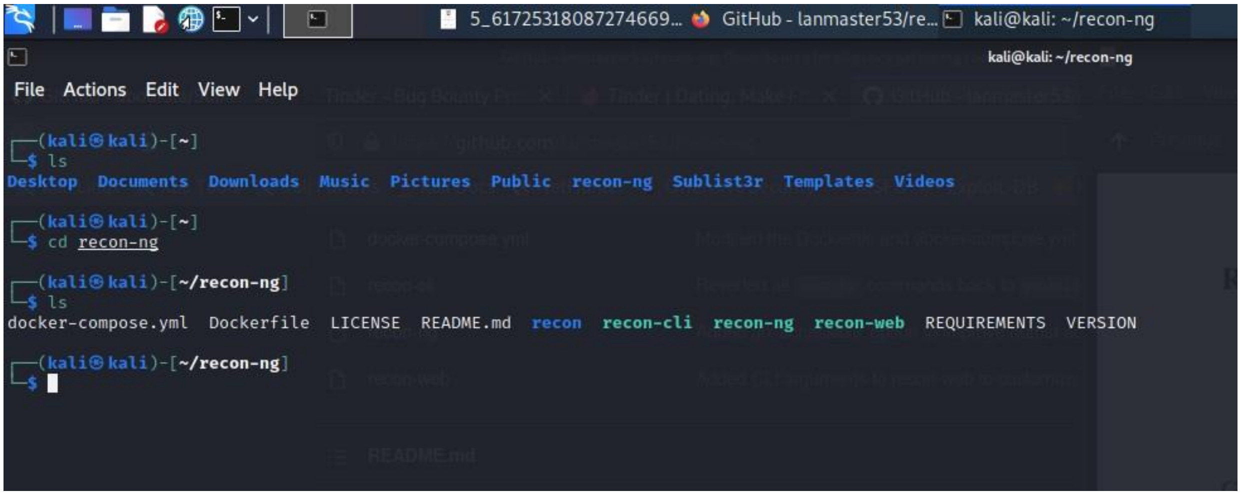
Link - https://github.com/lanmaster53/recon-ng

1.Download tool from this link



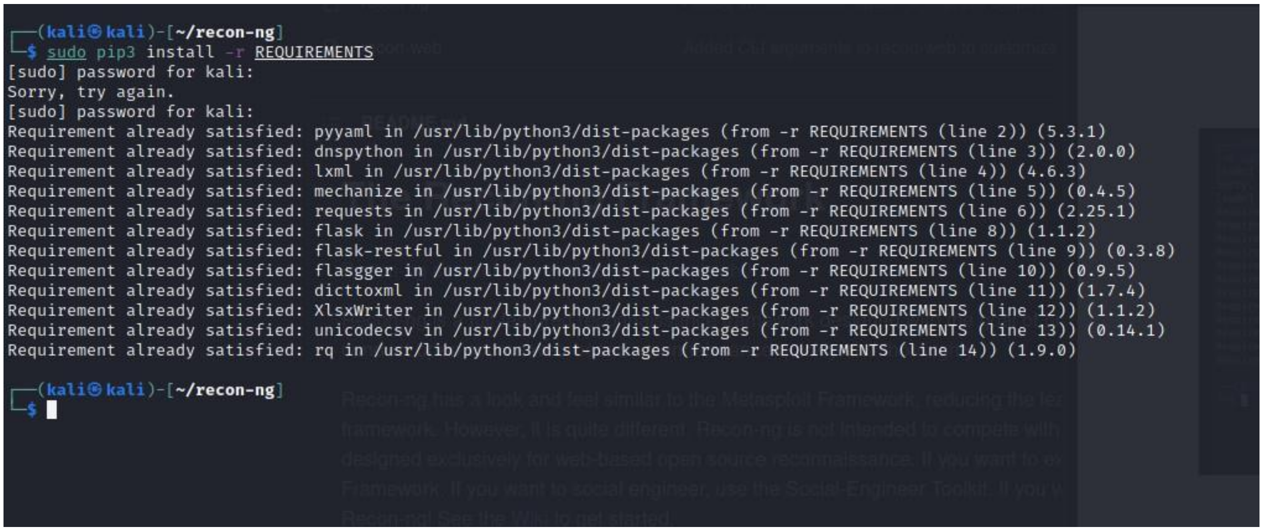
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/lanmaster53/recon-ng
Cloning into 'recon-ng'...
remote: Enumerating objects: 9522, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 9522 (delta 3), reused 10 (delta 3), pack-reused 9503
Receiving objects: 100% (9522/9522), 3.06 MiB | 1.20 MiB/s, done.
Resolving deltas: 100% (4958/4958), done.

┌──(kali㉿kali)-[~]
└─$ 
```

2. Check files



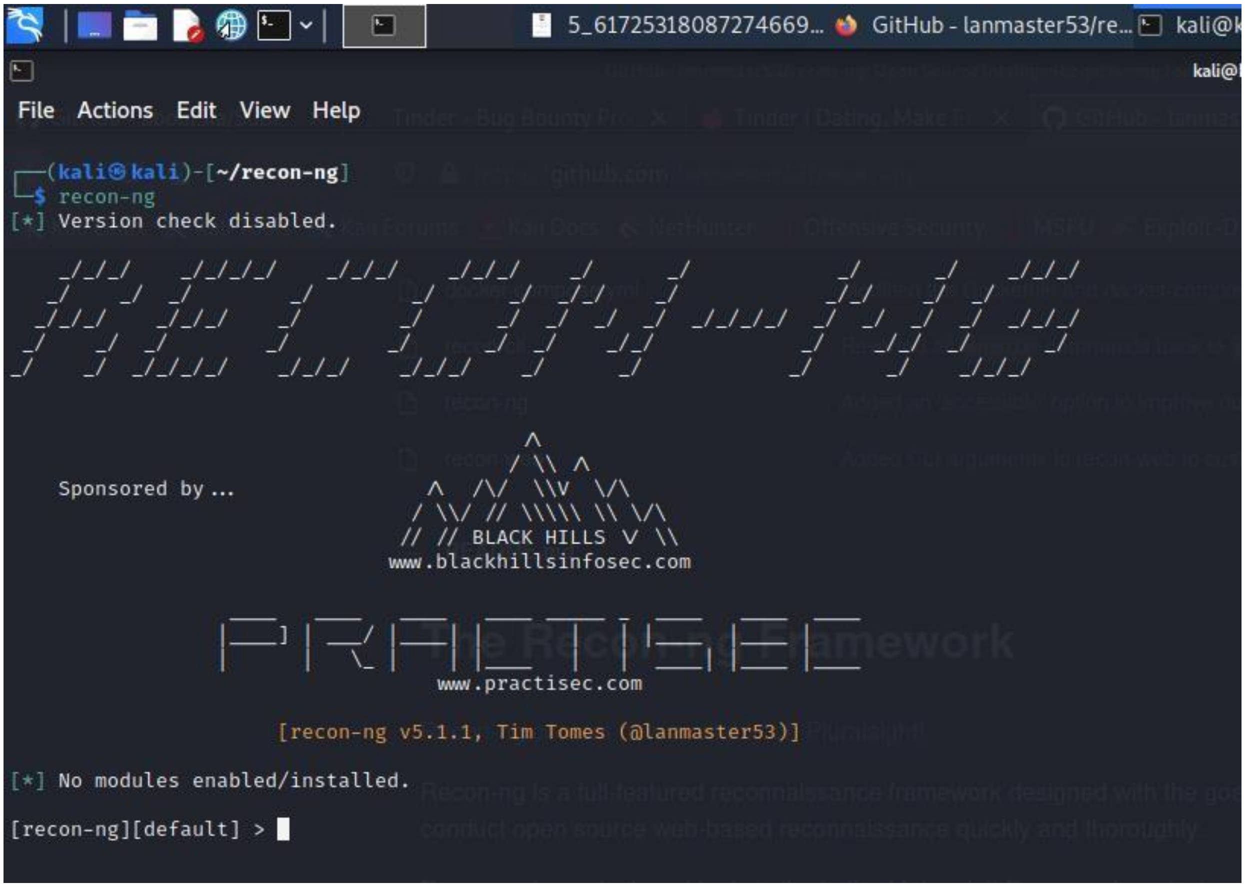
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  recon-ng  Sublist3r  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd recon-ng

┌──(kali㉿kali)-[~/recon-ng]
└─$ ls
docker-compose.yml  Dockerfile  LICENSE  README.md  recon  recon-cli  recon-ng  recon-web  REQUIREMENTS  VERSION

┌──(kali㉿kali)-[~/recon-ng]
└─$ 
```

Install requirements



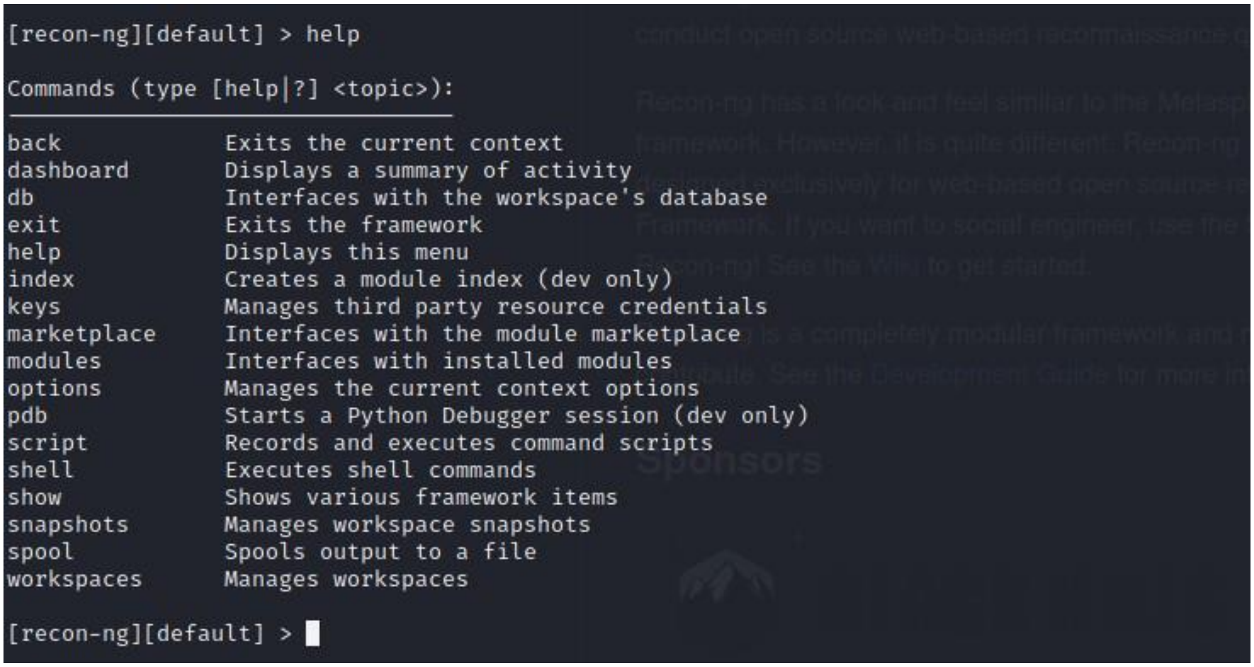
```
┌──(kali㉿kali)-[~/recon-ng]
└─$ sudo pip3 install -r REQUIREMENTS
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Requirement already satisfied: pyyaml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 2)) (5.3.1)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 3)) (2.0.0)
Requirement already satisfied: lxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 4)) (4.6.3)
Requirement already satisfied: mechanize in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 5)) (0.4.5)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 6)) (2.25.1)
Requirement already satisfied: flask in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 8)) (1.1.2)
Requirement already satisfied: flask-restful in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 9)) (0.3.8)
Requirement already satisfied: flasgger in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 10)) (0.9.5)
Requirement already satisfied: dicttoxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 11)) (1.7.4)
Requirement already satisfied: XlsxWriter in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 12)) (1.1.2)
Requirement already satisfied: unicodecsv in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 13)) (0.14.1)
Requirement already satisfied: rq in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 14)) (1.9.0)

┌──(kali㉿kali)-[~/recon-ng]
└─$ 
```

4.open tool



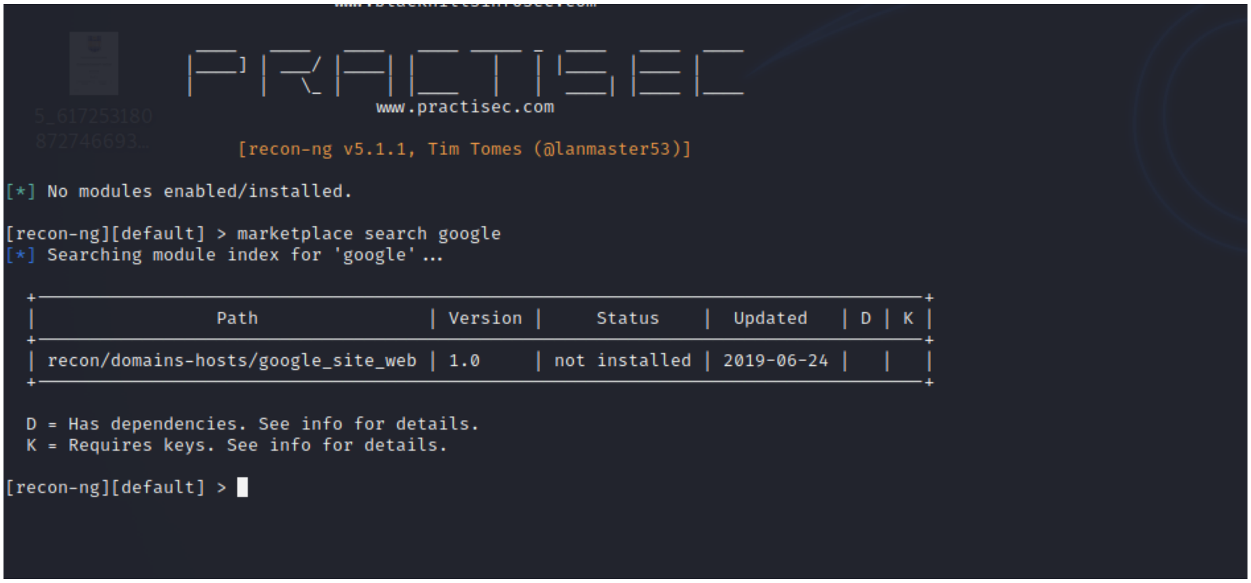
```
┌──(kali㉿kali)-[~/recon-ng]
└─$ recon-ng
[*] Version check disabled.

    Sponsored by ...

                    // // BLACK HILLS  V  \\
                   www.blackhillsinfosec.com

                        www.practisec.com

             [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > 
```

5.Use help command



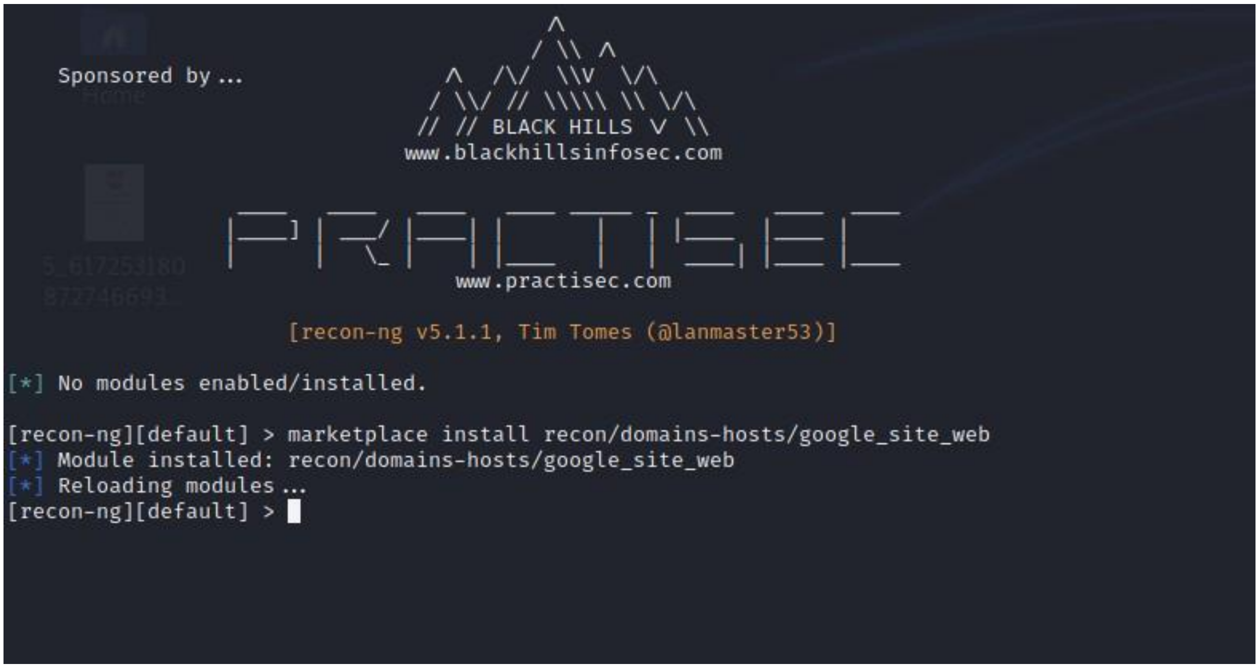
```
[recon-ng][default] > help

Commands (type [help|?] <topic>):
_________________________________
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces

[recon-ng][default] >
```

6. Google module



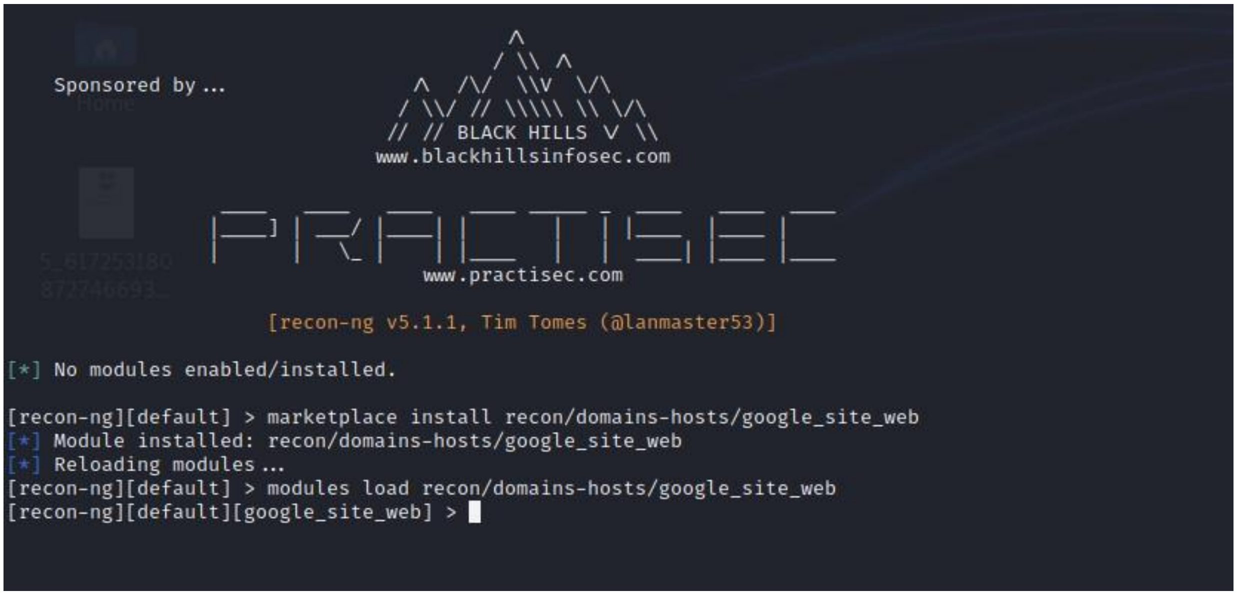
```
                       www.practisec.com

              [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > marketplace search google
[*] Searching module index for 'google'...

  +--------------------------------------------------------------------------------+
  |                Path                | Version |     Status    |  Updated   | D | K |
  +--------------------------------------------------------------------------------+
  | recon/domains-hosts/google_site_web | 1.0     | not installed | 2019-06-24 |   |   |
  +--------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default] >
```

7.Then install module



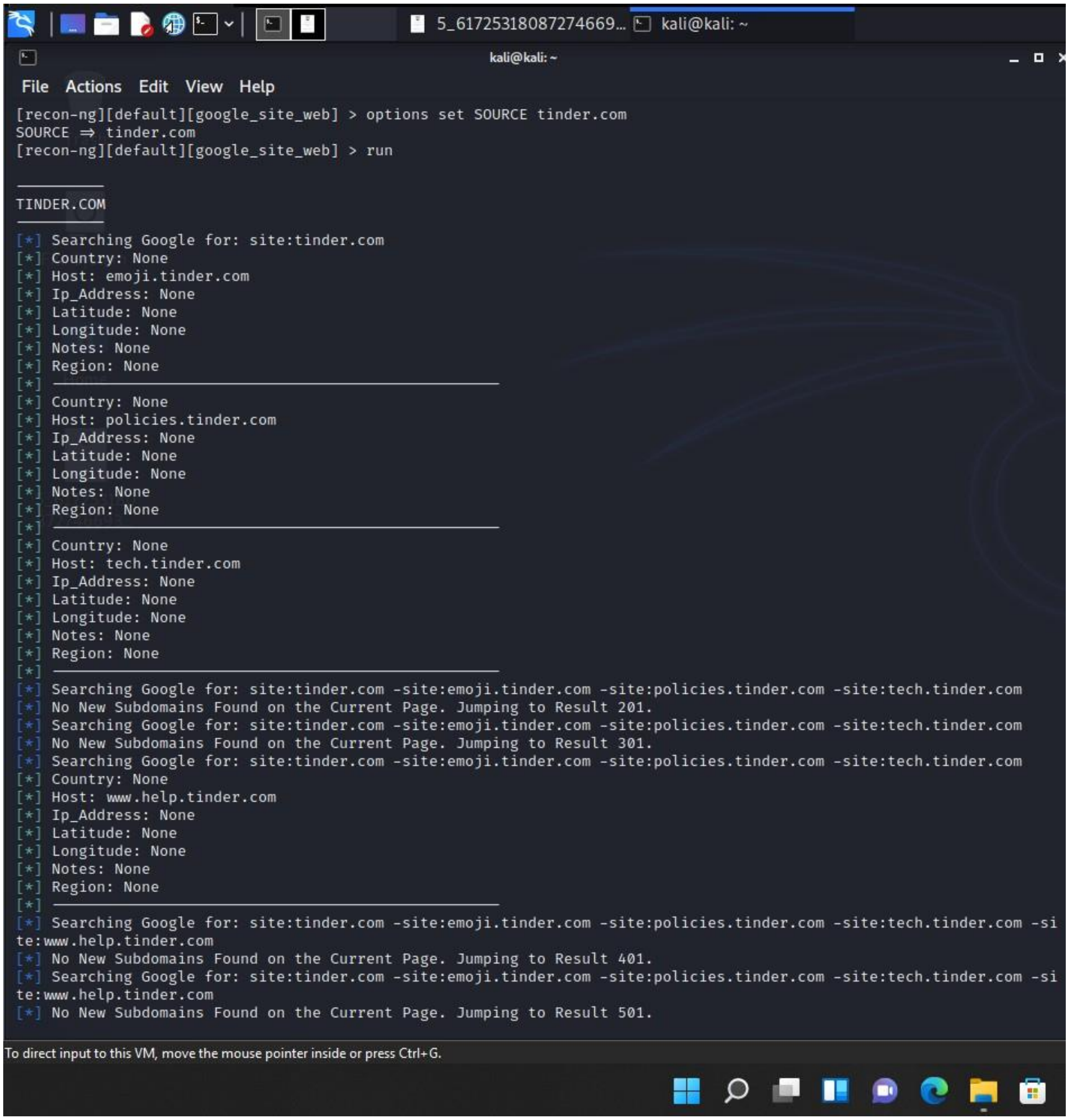
```
                              ^
                             / \\ ^
    Sponsored by ...      ^  /\/  \\V  \/\
                         / \\/ // \\\\\ \\ \/\
                        // // BLACK HILLS \/ \\
                       www.blackhillsinfosec.com

                            www.practisec.com

                [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] >
```

8.Load module



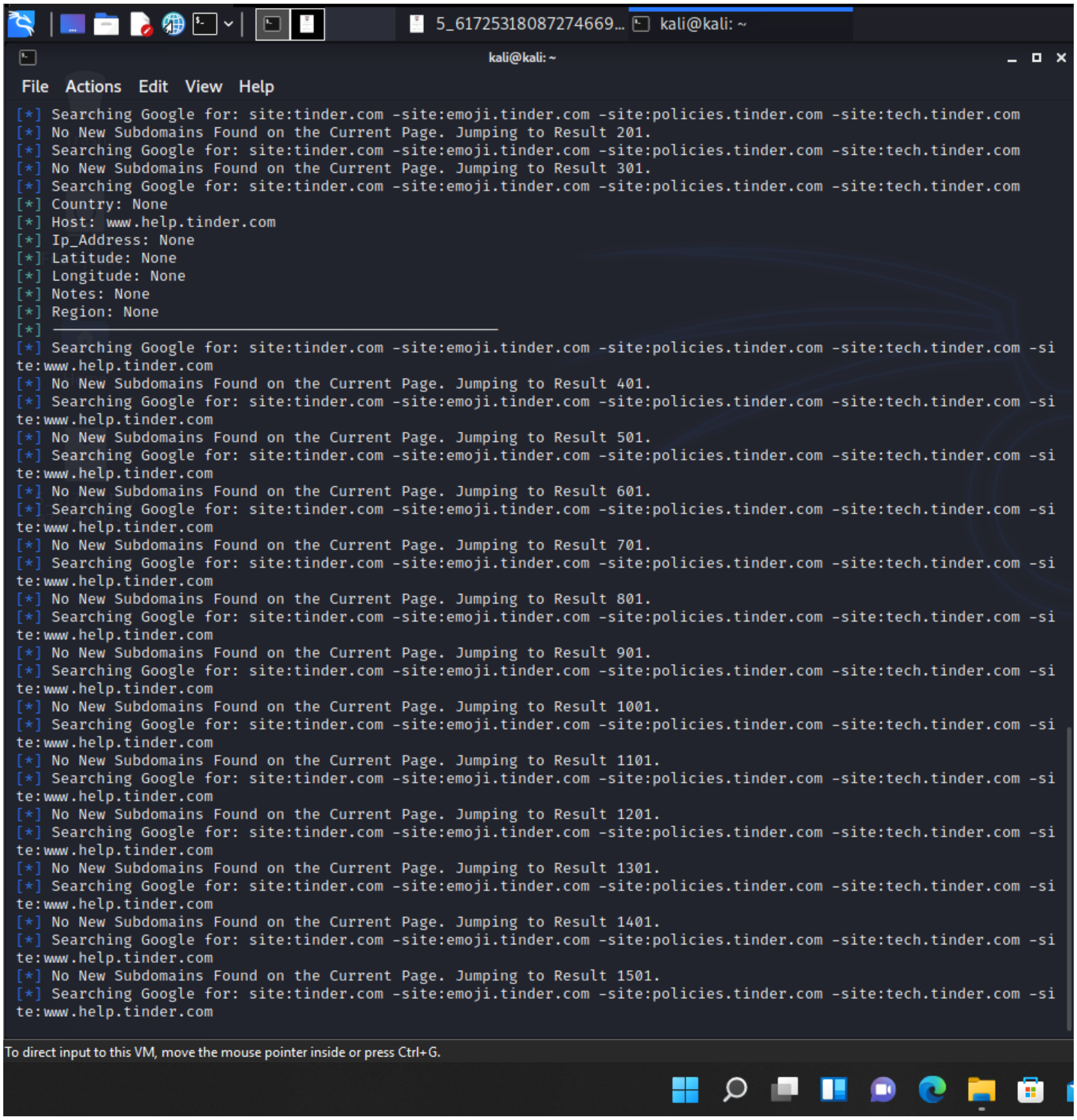
```
                              ^
                             / \\ ^
    Sponsored by ...      ^  /\/  \\V  \/\
                         / \\/ // \\\\\ \\ \/\
                        // // BLACK HILLS \/ \\
                       www.blackhillsinfosec.com

                            www.practisec.com

                [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] >
```

Scan



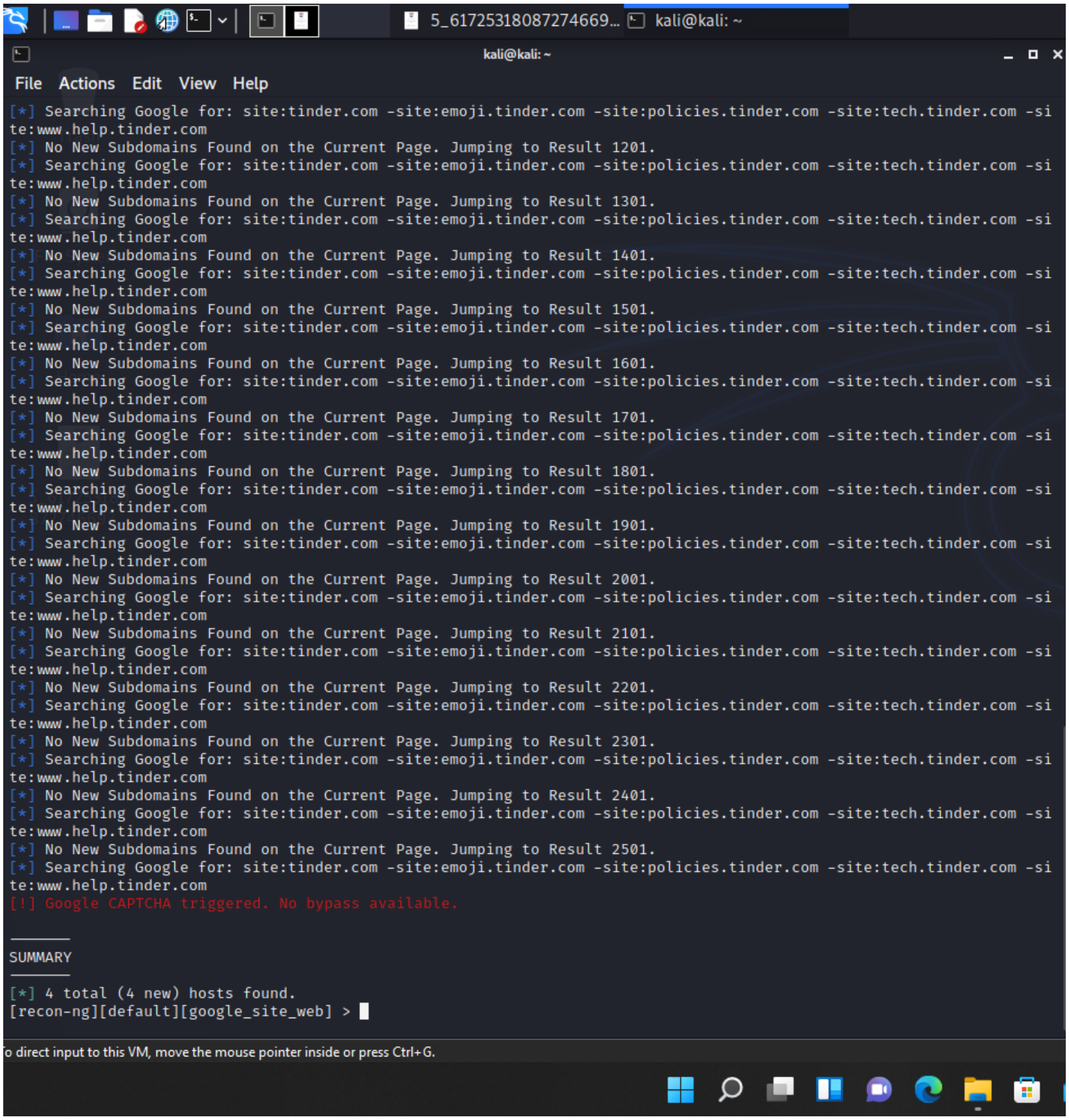
```
[recon-ng][default][google_site_web] > options set SOURCE tinder.com
SOURCE ⇒ tinder.com
[recon-ng][default][google_site_web] > run

──────────
TINDER.COM
──────────
[*] Searching Google for: site:tinder.com
[*] Country: None
[*] Host: emoji.tinder.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: policies.tinder.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: tech.tinder.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 301.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com
[*] Country: None
[*] Host: www.help.tinder.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 401.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 501.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 301.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com
[*] Country: None
[*] Host: www.help.tinder.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 401.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 501.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 601.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 701.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 801.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 901.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1001.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1101.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1201.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1301.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1401.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1501.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1201.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1301.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1401.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1501.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1601.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1701.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1801.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1901.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2001.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2101.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2201.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2301.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2401.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2501.
[*] Searching Google for: site:tinder.com -site:emoji.tinder.com -site:policies.tinder.com -site:tech.tinder.com -si
te:www.help.tinder.com
[!] Google CAPTCHA triggered. No bypass available.

-------
SUMMARY
-------
[*] 4 total (4 new) hosts found.
[recon-ng][default][google_site_web] >
```

o direct input to this VM, move the mouse pointer inside or press Ctrl+G.

VULNERABILITY SCANNING

I choose these subdomains for my assignment

https://www.tinder.com

https://lite.tinder.com

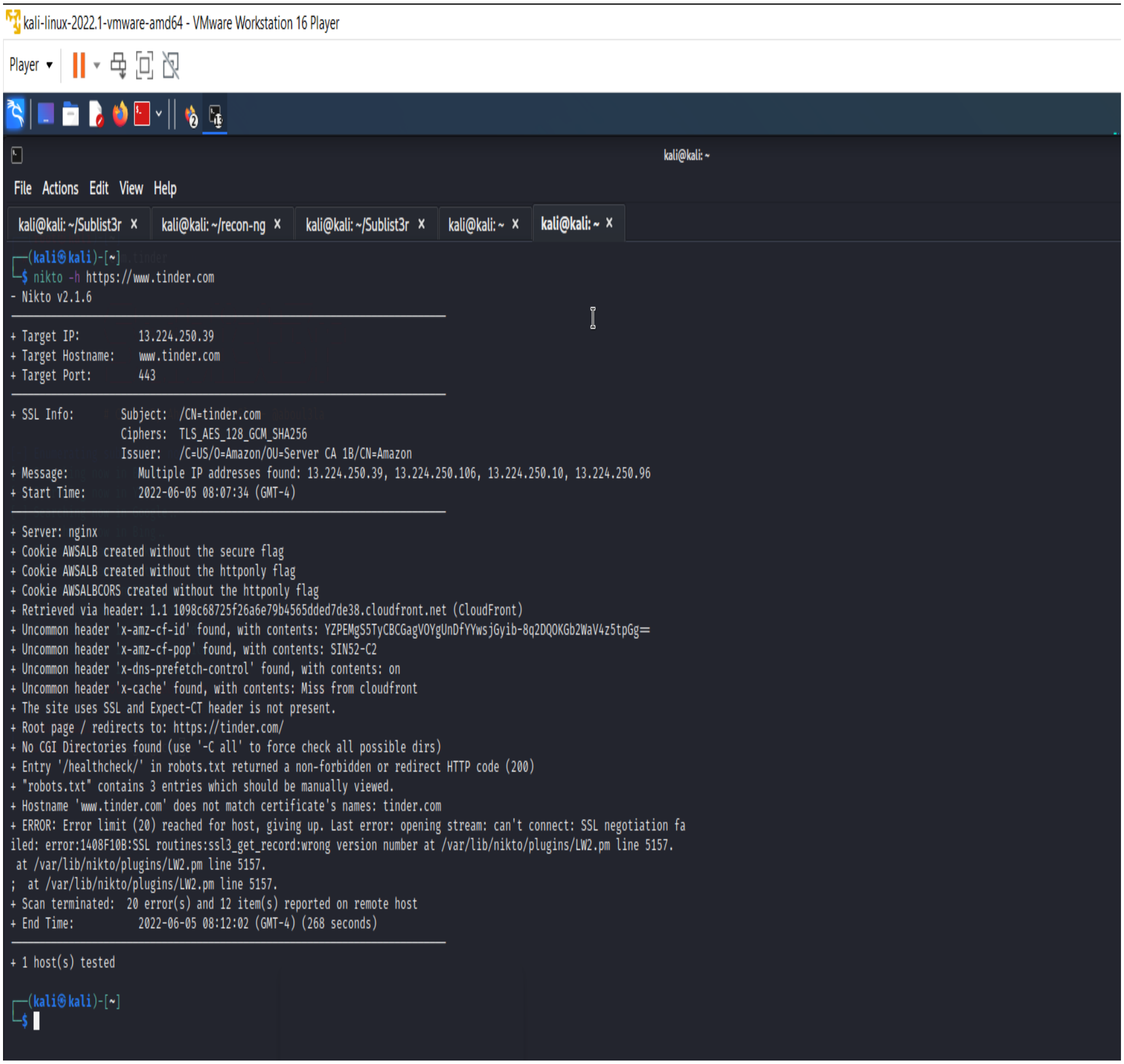
https://open.tinder.com

https://tech.tinder.com

https://polls.tinder.com

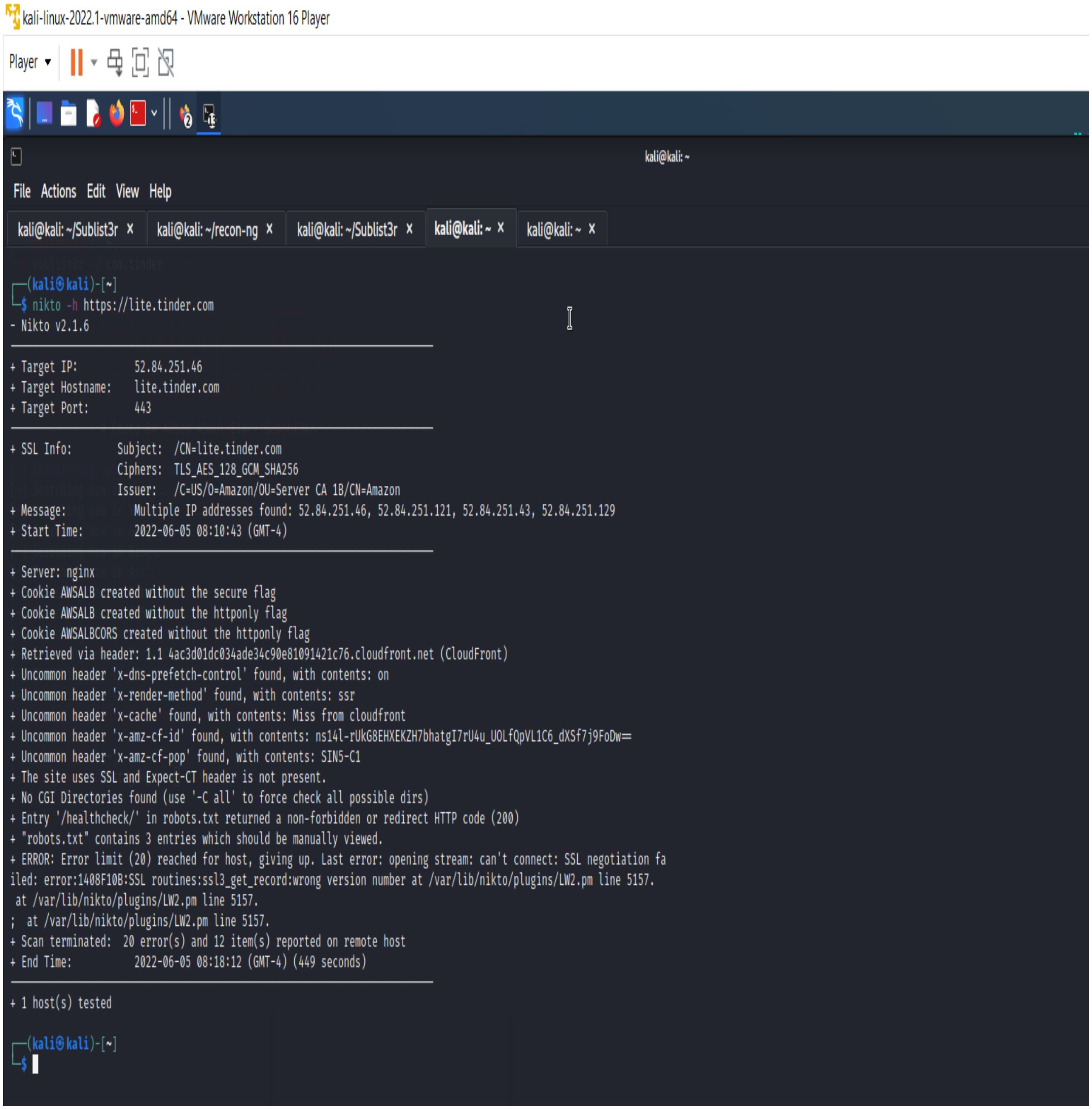
Scan with Nikto Tool

https://www.tinder.com



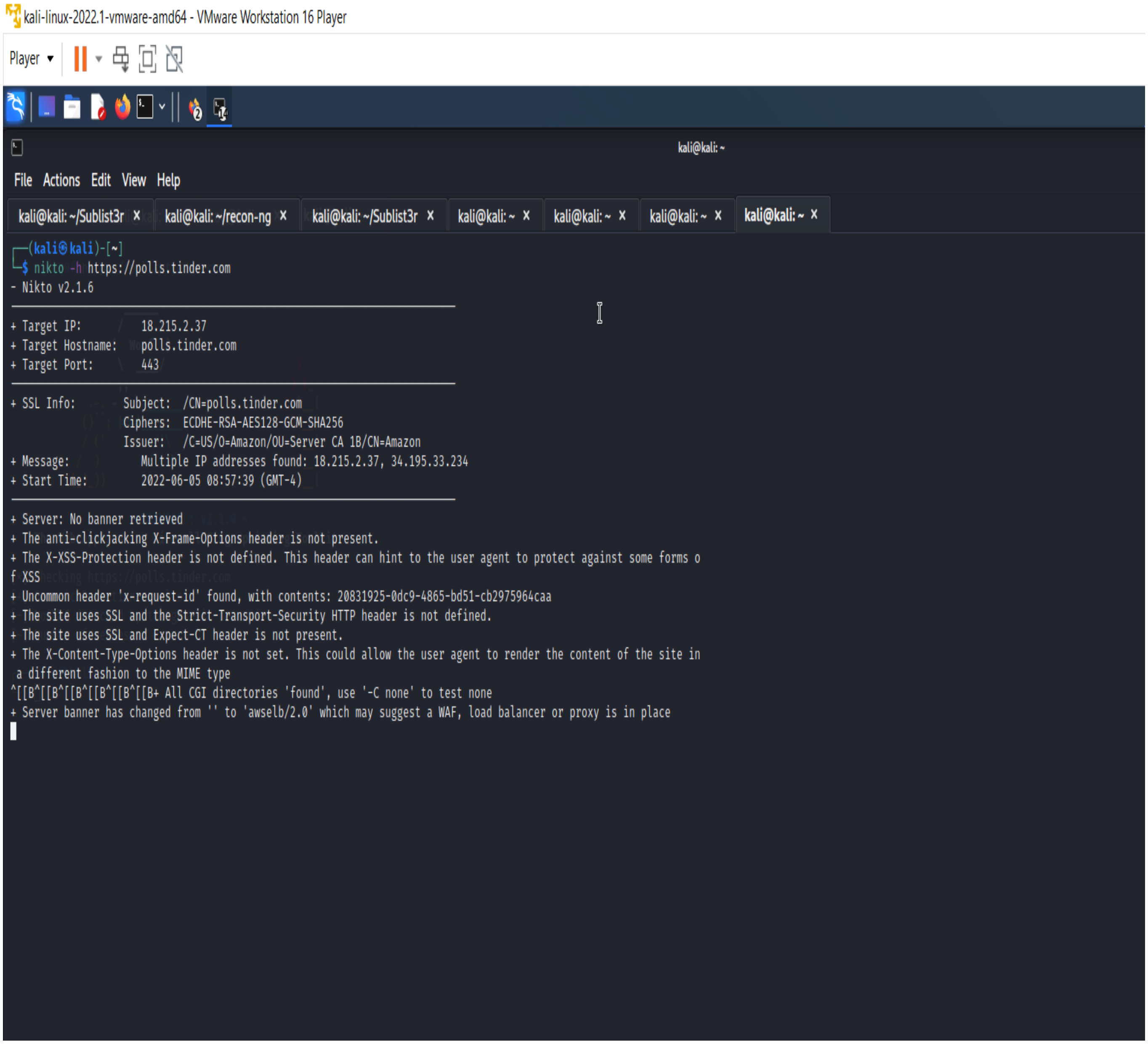
```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://www.tinder.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          13.224.250.39
+ Target Hostname:    www.tinder.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=tinder.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message:            Multiple IP addresses found: 13.224.250.39, 13.224.250.106, 13.224.250.10, 13.224.250.96
+ Start Time:         2022-06-05 08:07:34 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ Cookie AWSALB created without the secure flag
+ Cookie AWSALB created without the httponly flag
+ Cookie AWSALBCORS created without the httponly flag
+ Retrieved via header: 1.1 1098c68725f26a6e79b4565dded7de38.cloudfront.net (CloudFront)
+ Uncommon header 'x-amz-cf-id' found, with contents: YZPEMgS5TyCBCGagVOYgUnDfYYwsjGyib-8q2DQOKGb2WaV4z5tpGg==
+ Uncommon header 'x-amz-cf-pop' found, with contents: SIN52-C2
+ Uncommon header 'x-dns-prefetch-control' found, with contents: on
+ Uncommon header 'x-cache' found, with contents: Miss from cloudfront
+ The site uses SSL and Expect-CT header is not present.
+ Root page / redirects to: https://tinder.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/healthcheck/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 3 entries which should be manually viewed.
+ Hostname 'www.tinder.com' does not match certificate's names: tinder.com
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation fa
iled: error:1408F10B:SSL routines:ssl3_get_record:wrong version number at /var/lib/nikto/plugins/LW2.pm line 5157.
 at /var/lib/nikto/plugins/LW2.pm line 5157.
;  at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated:  20 error(s) and 12 item(s) reported on remote host
+ End Time:           2022-06-05 08:12:02 (GMT-4) (268 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```

https://lite.tinder.com



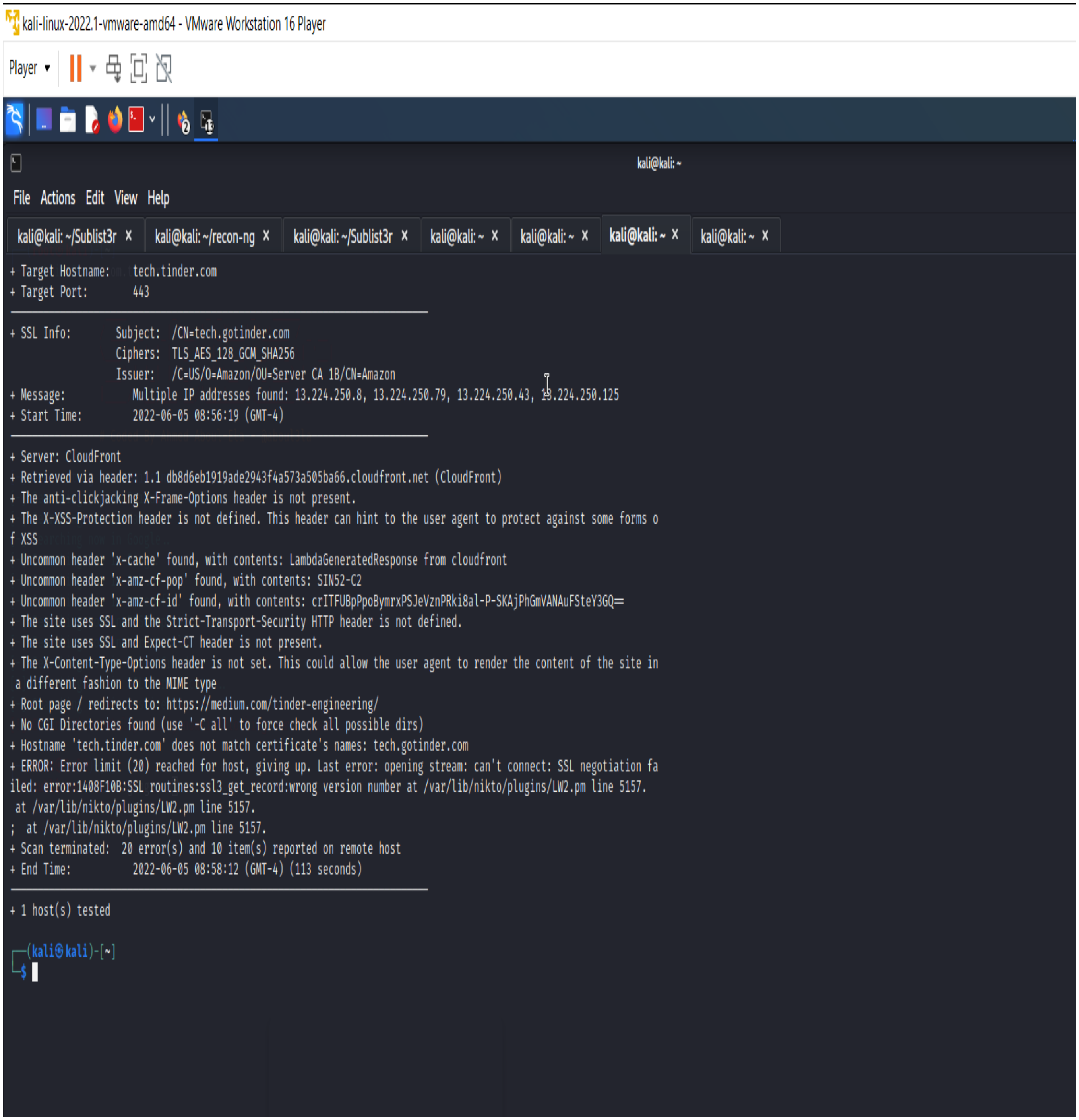
```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://lite.tinder.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          52.84.251.46
+ Target Hostname:    lite.tinder.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=lite.tinder.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message:            Multiple IP addresses found: 52.84.251.46, 52.84.251.121, 52.84.251.43, 52.84.251.129
+ Start Time:         2022-06-05 08:10:43 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ Cookie AWSALB created without the secure flag
+ Cookie AWSALB created without the httponly flag
+ Cookie AWSALBCORS created without the httponly flag
+ Retrieved via header: 1.1 4ac3d01dc034ade34c90e81091421c76.cloudfront.net (CloudFront)
+ Uncommon header 'x-dns-prefetch-control' found, with contents: on
+ Uncommon header 'x-render-method' found, with contents: ssr
+ Uncommon header 'x-cache' found, with contents: Miss from cloudfront
+ Uncommon header 'x-amz-cf-id' found, with contents: ns14l-rUkG8EHXEKZH7bhatgI7rU4u_UOLfQpVL1C6_dXSf7j9FoDw==
+ Uncommon header 'x-amz-cf-pop' found, with contents: SIN5-C1
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/healthcheck/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 3 entries which should be manually viewed.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation fa
iled: error:1408F10B:SSL routines:ssl3_get_record:wrong version number at /var/lib/nikto/plugins/LW2.pm line 5157.
 at /var/lib/nikto/plugins/LW2.pm line 5157.
;  at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated:  20 error(s) and 12 item(s) reported on remote host
+ End Time:           2022-06-05 08:18:12 (GMT-4) (449 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```

https://polls.tinder.com



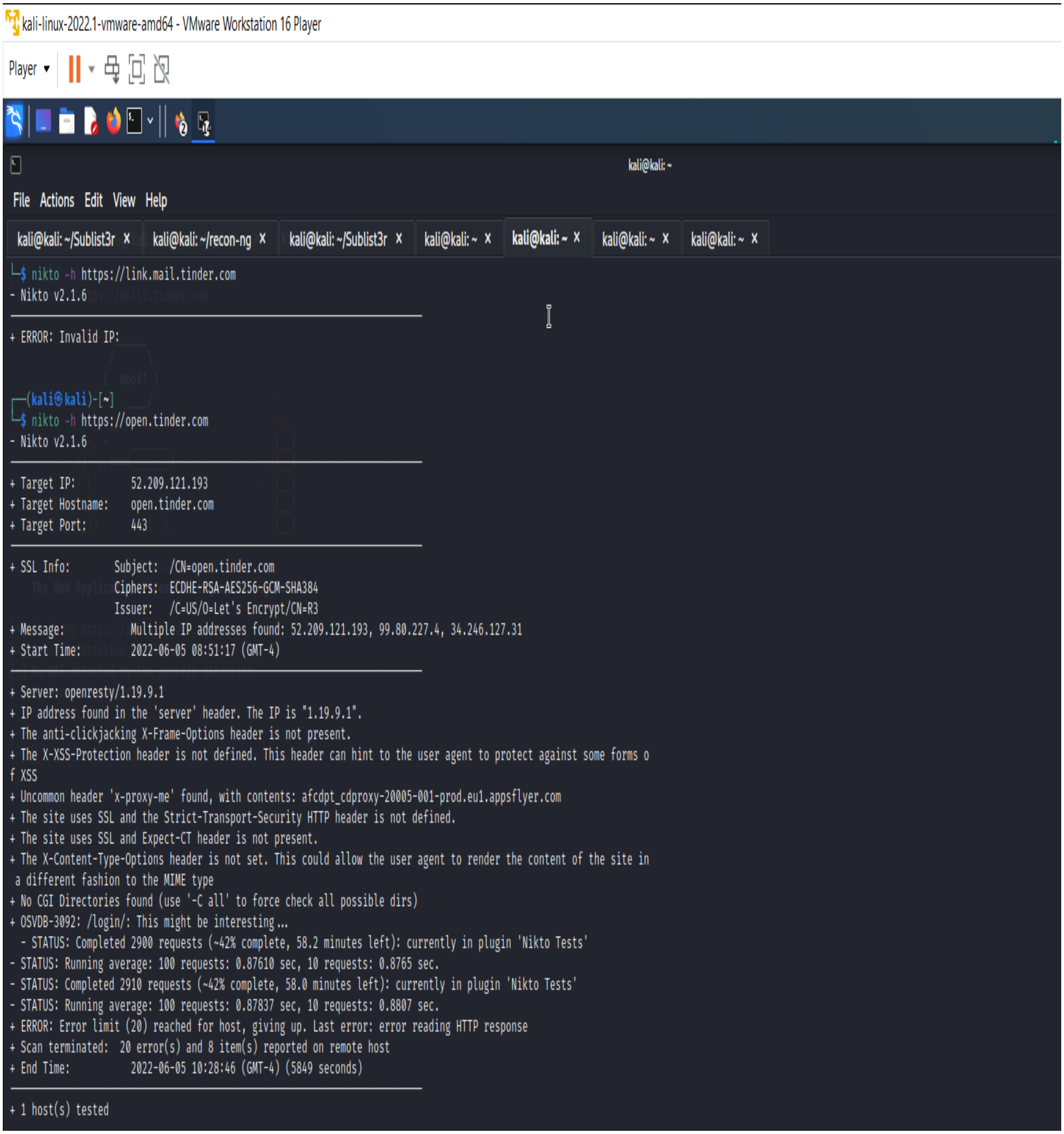
```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://polls.tinder.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          18.215.2.37
+ Target Hostname:    polls.tinder.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=polls.tinder.com
                   Ciphers:  ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message:            Multiple IP addresses found: 18.215.2.37, 34.195.33.234
+ Start Time:         2022-06-05 08:57:39 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ 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 o
f XSS
+ Uncommon header 'x-request-id' found, with contents: 20831925-0dc9-4865-bd51-cb2975964caa
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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 to the MIME type
^[[B^[[B^[[B^[[B^[[B^[[B+ All CGI directories 'found', use '-C none' to test none
+ Server banner has changed from '' to 'awselb/2.0' which may suggest a WAF, load balancer or proxy is in place
```

https://tech.tinder.com



```
+ Target Hostname:    tech.tinder.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=tech.gotinder.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message:            Multiple IP addresses found: 13.224.250.8, 13.224.250.79, 13.224.250.43, 13.224.250.125
+ Start Time:         2022-06-05 08:56:19 (GMT-4)
---------------------------------------------------------------------------
+ Server: CloudFront
+ Retrieved via header: 1.1 db8d6eb1919ade2943f4a573a505ba66.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 o
f XSS
+ Uncommon header 'x-cache' found, with contents: LambdaGeneratedResponse from cloudfront
+ Uncommon header 'x-amz-cf-pop' found, with contents: SIN52-C2
+ Uncommon header 'x-amz-cf-id' found, with contents: crITFUBpPpoBymrxPSJeVznPRki8al-P-SKAjPhGmVANAuFSteY3GQ==
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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 to the MIME type
+ Root page / redirects to: https://medium.com/tinder-engineering/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname 'tech.tinder.com' does not match certificate's names: tech.gotinder.com
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation fa
iled: error:1408F10B:SSL routines:ssl3_get_record:wrong version number at /var/lib/nikto/plugins/LW2.pm line 5157.
 at /var/lib/nikto/plugins/LW2.pm line 5157.
;  at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated:  20 error(s) and 10 item(s) reported on remote host
+ End Time:           2022-06-05 08:58:12 (GMT-4) (113 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$
```

https://open.tinder.com



```
└─$ nikto -h https://link.mail.tinder.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: Invalid IP:


┌──(kali㉿kali)-[~]
└─$ nikto -h https://open.tinder.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          52.209.121.193
+ Target Hostname:    open.tinder.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=open.tinder.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Message:            Multiple IP addresses found: 52.209.121.193, 99.80.227.4, 34.246.127.31
+ Start Time:         2022-06-05 08:51:17 (GMT-4)
---------------------------------------------------------------------------
+ Server: openresty/1.19.9.1
+ IP address found in the 'server' header. The IP is "1.19.9.1".
+ 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 o
f XSS
+ Uncommon header 'x-proxy-me' found, with contents: afcdpt_cdproxy-20005-001-prod.eu1.appsflyer.com
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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 to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3092: /login/: This might be interesting...
  - STATUS: Completed 2900 requests (~42% complete, 58.2 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.87610 sec, 10 requests: 0.8765 sec.
- STATUS: Completed 2910 requests (~42% complete, 58.0 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.87837 sec, 10 requests: 0.8807 sec.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 8 item(s) reported on remote host
+ End Time:           2022-06-05 10:28:46 (GMT-4) (5849 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Fingerprinting

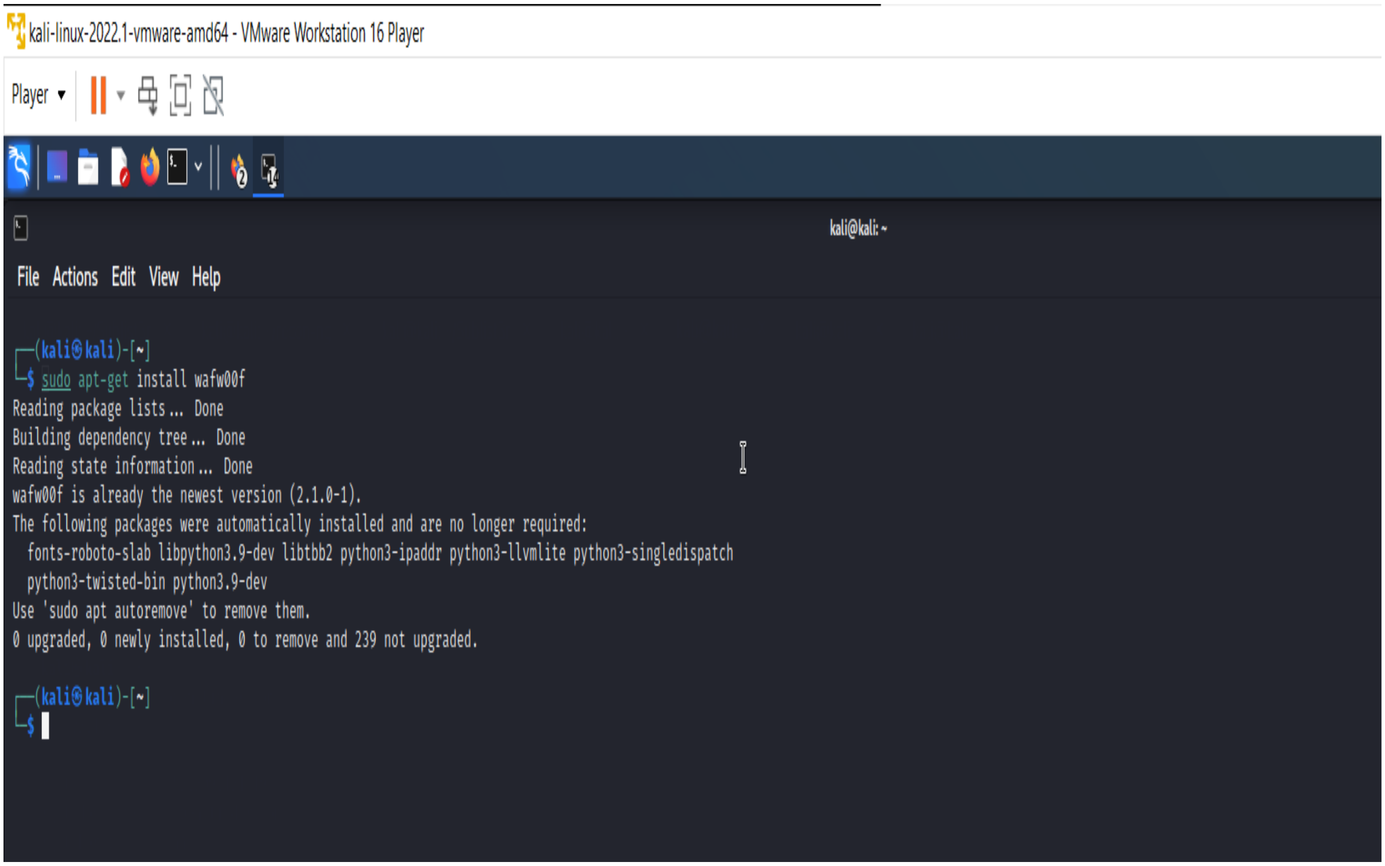
In data gathering system, we need to find open ports, firewalls, iptcpdum[addresses, active ports, open ports, filtered ports, active devices, operating system etc.

Fingerprinting tools

- Wafw00f
- Nmap
- PacketFence
- Netcat
- P0f
- Uniscan
- Tcpdump
- Wireshark
- Amap
- Cessation

Wafwoof tool

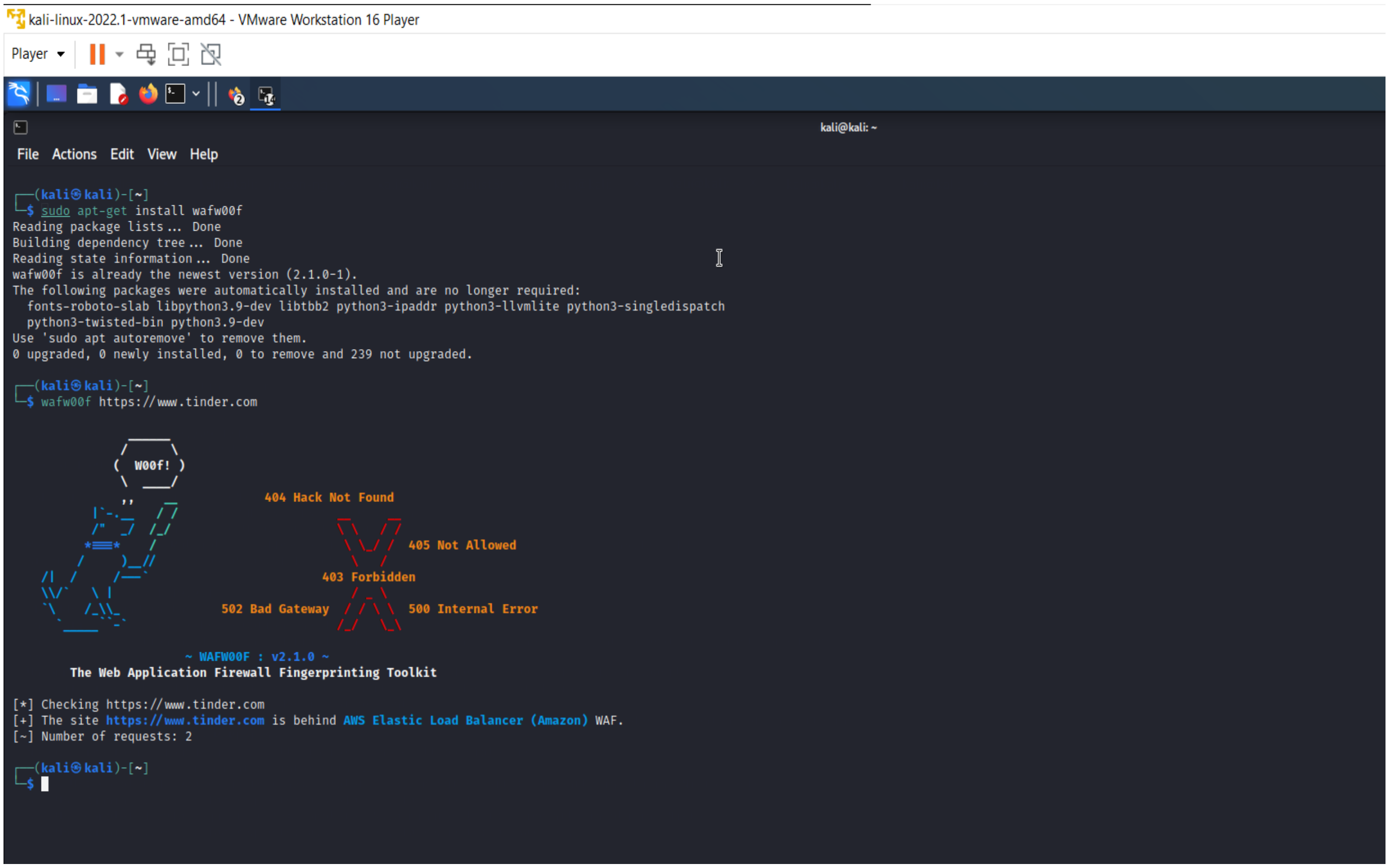
Use to install command - sudo apt-get install wafw00f



kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player
Player
kali@kali: ~
File Actions Edit View Help

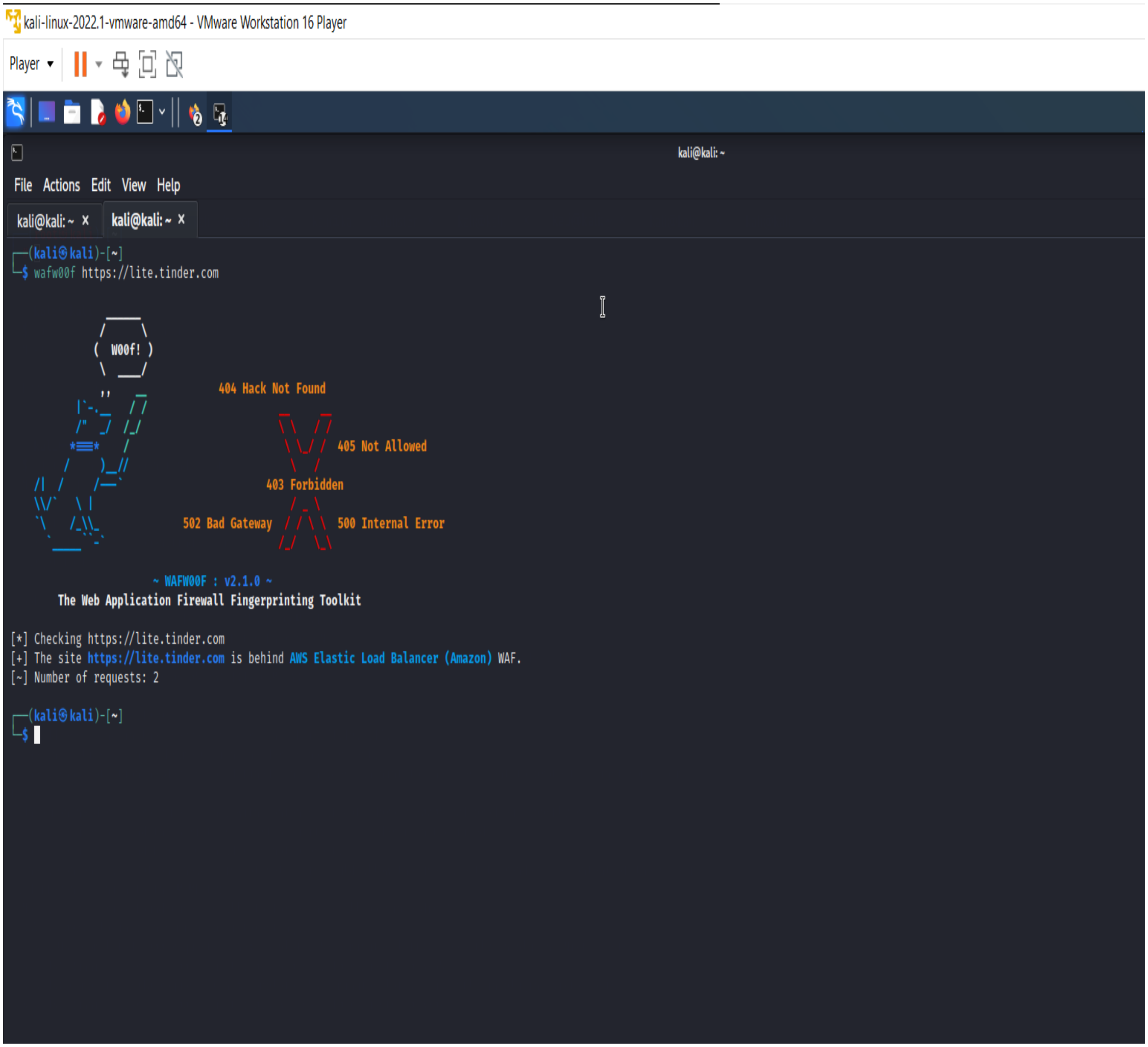
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install wafw00f
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wafw00f is already the newest version (2.1.0-1).
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libpython3.9-dev libtbb2 python3-ipaddr python3-llvmlite python3-singledispatch
  python3-twisted-bin python3.9-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 239 not upgraded.

┌──(kali㉿kali)-[~]
└─$ 
```

https://www.tinder.com


kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player
Player
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install wafw00f
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wafw00f is already the newest version (2.1.0-1).
The following packages were automatically installed and are no longer required:
  fonts-roboto-slab libpython3.9-dev libtbb2 python3-ipaddr python3-llvmlite python3-singledispatch
  python3-twisted-bin python3.9-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 239 not upgraded.

┌──(kali㉿kali)-[~]
└─$ wafw00f https://www.tinder.com

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,    __            404 Hack Not Found
           |`-.__   / /                      __     __
           /"  _/  /_/                       \ \   / /
          *===*    /                          \ \_/ /  405 Not Allowed
         /     )__//                           \   /
    /|  /     /---`                        403 Forbidden
    \\/`   \ |                                 / _ \
    `\    /_\\_              502 Bad Gateway  / / \ \  500 Internal Error
      `_____``-`                             /_/   \_\

                        ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.tinder.com
[+] The site https://www.tinder.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[~] Number of requests: 2

┌──(kali㉿kali)-[~]
└─$
```

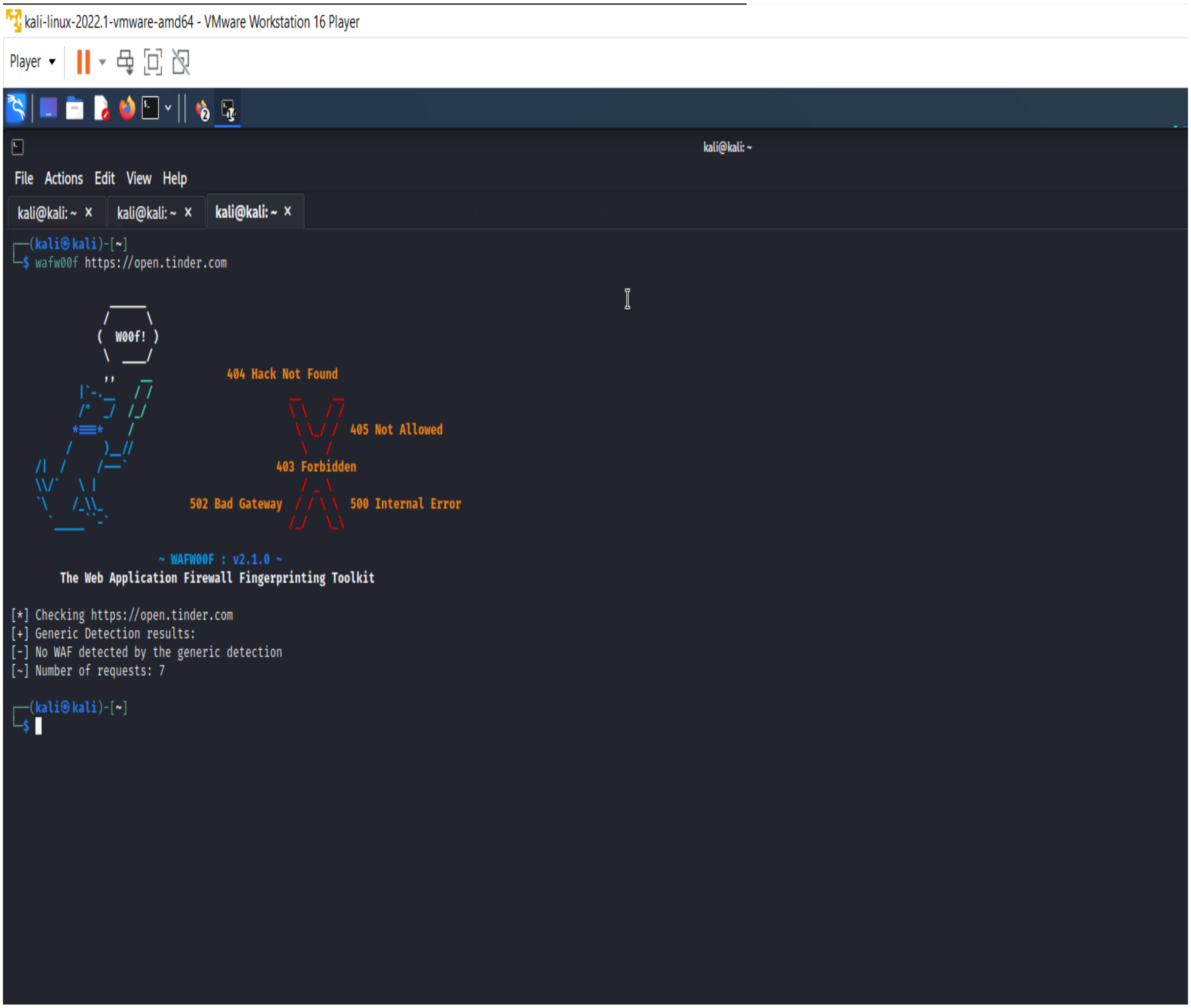
https://lite.tinder.com



kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player
Player
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ wafw00f https://lite.tinder.com

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,    __            404 Hack Not Found
           |`-.__   / /                      __     __
           /"  _/  /_/                       \ \   / /
          *===*    /                          \ \_/ /  405 Not Allowed
         /     )__//                           \   /
    /|  /     /---`                        403 Forbidden
    \\/`    \ |                                 / _ \
    `\    /_\\_               502 Bad Gateway  / / \ \  500 Internal Error
      `_____``-`                              /_/   \_\

                        ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://lite.tinder.com
[+] The site https://lite.tinder.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[~] Number of requests: 2

┌──(kali㉿kali)-[~]
└─$ 
```

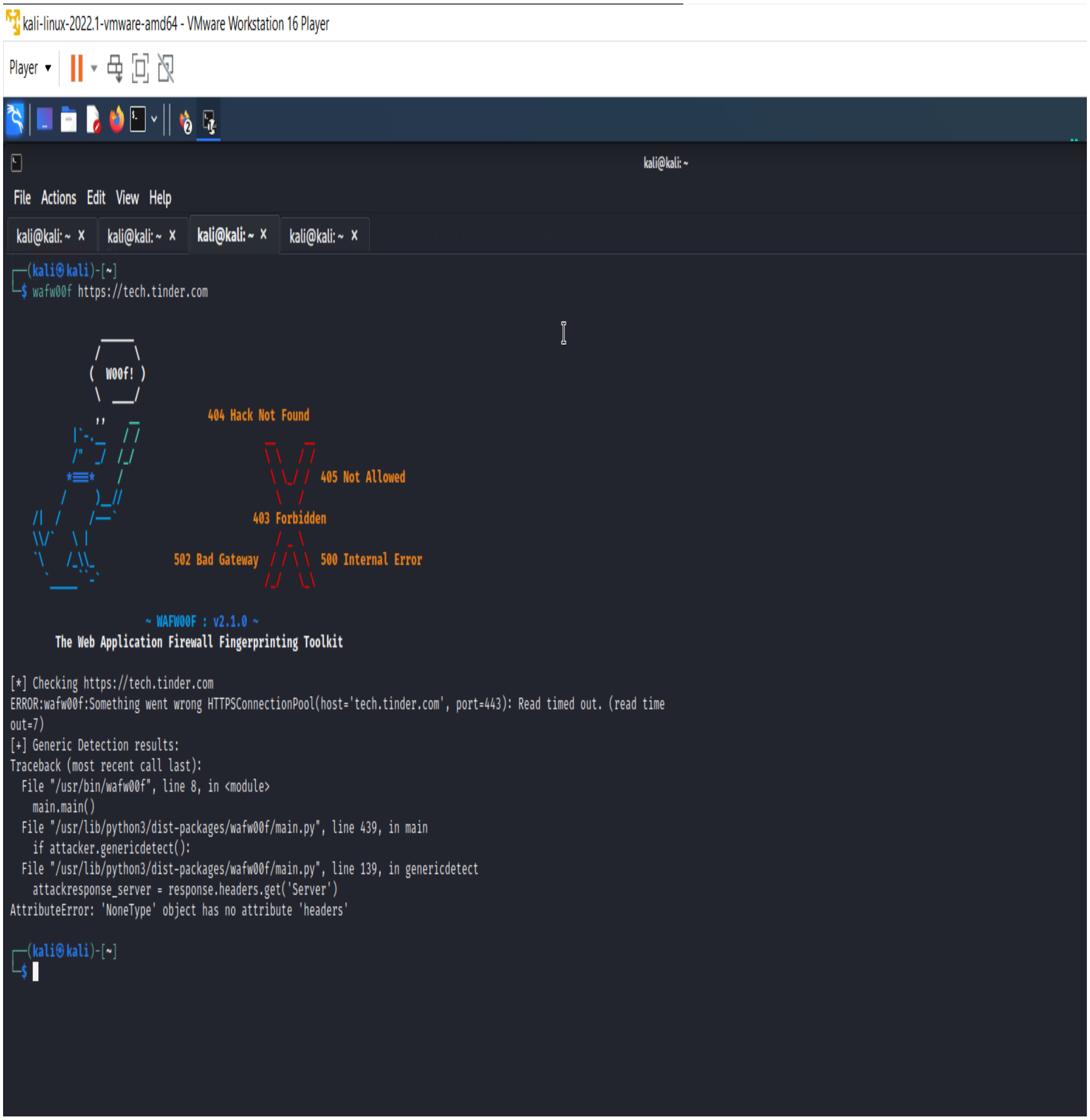
https://open.tinder.com



kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player
Player
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~

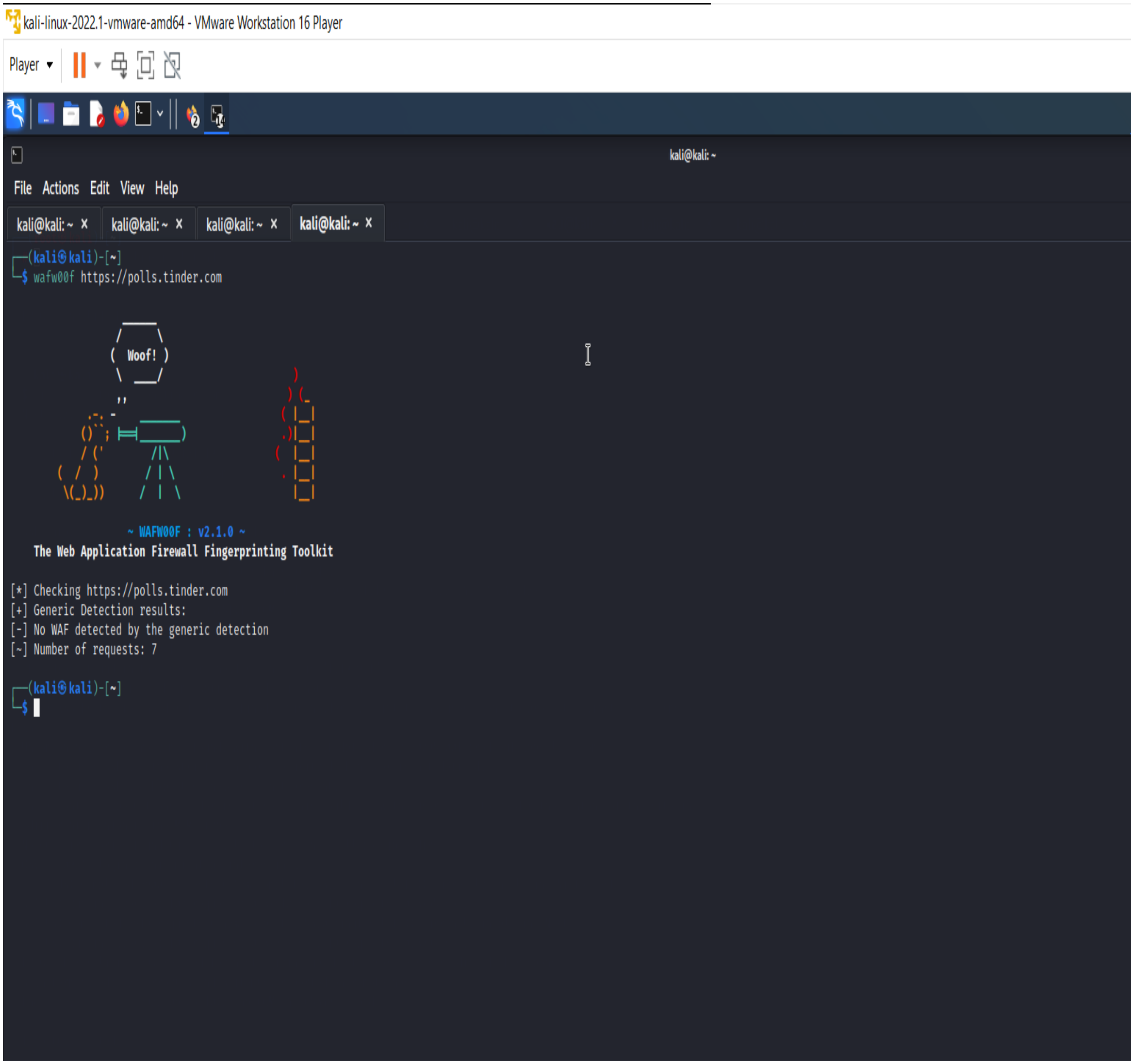
```
┌──(kali㉿kali)-[~]
└─$ wafw00f https://open.tinder.com

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,    __            404 Hack Not Found
           |`-.__   / /                      __     __
           /"  _/  /_/                       \ \   / /
          *===*    /                          \ \_/ /  405 Not Allowed
         /     )__//                           \   /
    /|  /     /---`                     403 Forbidden
    \\/`    \ |                                / _ \
    `\    /_\\_              502 Bad Gateway  / / \ \  500 Internal Error
      `_____``-`                             /_/   \_\

                        ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://open.tinder.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7

┌──(kali㉿kali)-[~]
└─$ 
```

https://tech.tinder.com


kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player
Player
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ X
kali@kali: ~ X
kali@kali: ~ X
kali@kali: ~ X

```
┌──(kali㉿kali)-[~]
└─$ wafw00f https://tech.tinder.com

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,    __            404 Hack Not Found
           |`-.__   / /                      __     __
           /"  _/  /_/                       \ \   / /
          *===*    /                          \ \_/ /  405 Not Allowed
         /     )__//                           \   /
    /|  /     /---`                        403 Forbidden
    \\/`    \ |                                 / _ \
    `\    /_\\_              502 Bad Gateway  / / \ \  500 Internal Error
      `_____``-`                             /_/   \_\

                        ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://tech.tinder.com
ERROR:wafw00f:Something went wrong HTTPSConnectionPool(host='tech.tinder.com', port=443): Read timed out. (read time
out=7)
[+] Generic Detection results:
Traceback (most recent call last):
  File "/usr/bin/wafw00f", line 8, in <module>
    main.main()
  File "/usr/lib/python3/dist-packages/wafw00f/main.py", line 439, in main
    if attacker.genericdetect():
  File "/usr/lib/python3/dist-packages/wafw00f/main.py", line 139, in genericdetect
    attackresponse_server = response.headers.get('Server')
AttributeError: 'NoneType' object has no attribute 'headers'

┌──(kali㉿kali)-[~]
└─$ 
```

https://polls.tinder.com


kali-linux-2022.1-vmware-amd64 - VMware Workstation 16 Player
Player
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
Woof!

```
┌──(kali㉿kali)-[~]
└─$ wafw00f https://polls.tinder.com

                ~ WAFW00F : v2.1.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://polls.tinder.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7

┌──(kali㉿kali)-[~]
└─$
```

VULNERABILITY ANALYZING

Vulnerability

Vulnerability is troubles/troubles or weaknesses within the web sites, net programs, software. Hackers can exploit that matters the usage of those vulnerabilities.

4 principal kinds of vulnerabilities. There are

1. Faulty defenses
2. Insecure connections
3. Resource management not adequate
4. End user errors and misuse

We can use these tools to scan vulnerabilities.

1. Uniscan
2. Nessus
3. Owasap
4. Nikto

Then I founded these vulnerabilities of selected my subdomains.

1.The website makes use of SSL and the stern-shipping-security HTTP header isn't defined.
2. The web site uses SSL and expect-CT header isn't always present.
3. The X-content-kind-option header isn't always set/
4. The anti-clickjacking X-frame-options header isn't present.
5. The X-XSS-safety header isn't described.

Conclusion

This internet audit has proven the vulnerabilities and essential suggestions for http://www.tinder.com domain. I've commenced via listing subdomains. After I’ve seemed thru every subdomain for weaknesses/vulnerabilities. I’ve Big descriptions of what i use the tools I used all through each phase of my protection assessment's vulnerability evaluation. In the end, I pointed out a way to deal with such risks.