Sri Lanka Institute of Information Technology

VULNERABILITY ASSESSMENT - WEB AUDIT

https://www.vk.com

Submitted by:

Student Registration Number	Student Name
IT1991290	**A.D. Jaliya**

Table of Contents

Acknowledgment

To start with, I would like to thank Dr. Lakmal Rupasinghe, the lecturer responsible for the Web Security Module, for his advice and contribution to the launch of the web audit at the highest level.

For the dedication and guidance they provided to us for this Web audit, I offer my heartfelt thanks to Ms. Chethna Lyanapathirana, Ms. Lanishna Rugghahakotuwa, and Ms. Udagedra.

Assessment Objectives

The security assessment of https://vk.com/ of the web security module in the second semester of the second year. This assignment aims to find vulnerabilities in the target domain and determine the risk level associated with those vulnerabilities. [1]

Introduction

A web audit scans website and its server for existing or potential weaknesses that hackers can exploit. A web audit is intended to be a thorough overview and study of the company's IT infrastructure, including core applications, plugins, themes, server settings, SSL connections, configurations, and so on.

It detects risks and bugs, revealing flaws and high-risk activities. Following the discovery of all bugs in the site audit, the next move is to conduct penetration checks,

also known as pentests. In this stage, security teams launch simulated hacking attacks against your device, simulating what could happen in the real world.

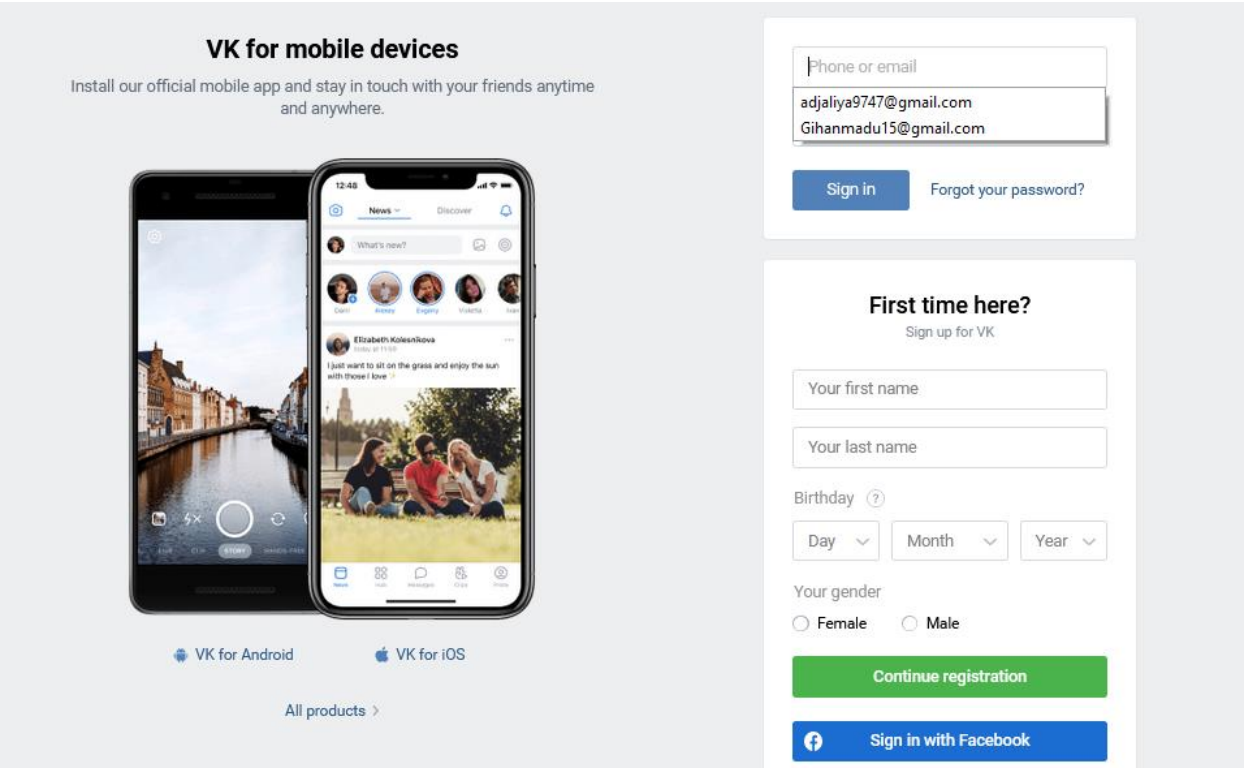
The aim of website security audits is to proactively search for and remove flaws in your website's design before hackers with malicious intent find them. [1] [2]

Scope

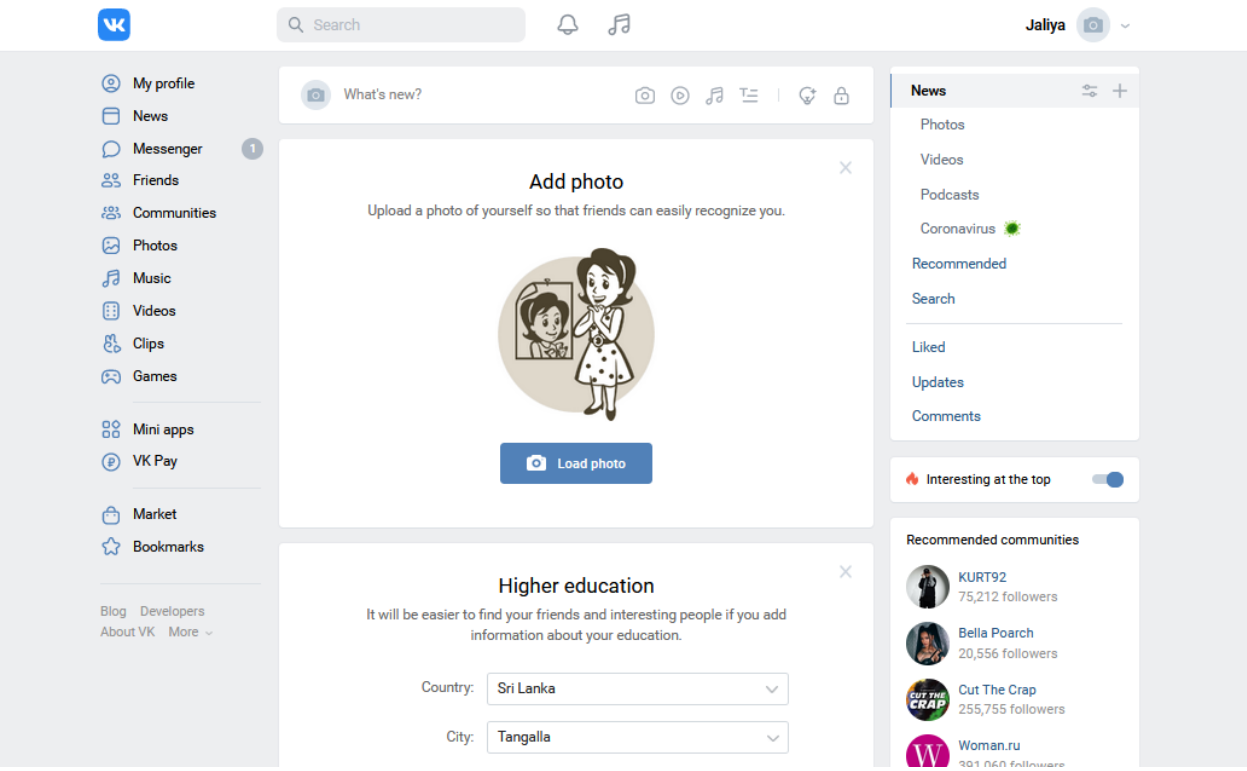
VK (*Vkontakte*) is a Russian online social media and social networking site located in Saint Petersburg. You can use VK in multiple languages but mostly used by Russian speakers. VK users can contact each other publicly or privately, form communities, public accounts, and activities, upload and tag photos, audio, and video, and play browser-based games. VK had at least 500 million users as of August 2018. It is Russia's most visited website [1]

As a cybersecurity student, I wanted to take a new challenge to find bugs in a website with the best security and huge scope. So, I choose the VK website for my web audit. Because it belongs to Russia, when it comes to cybersecurity Russia is one of the leading countries in the world and we all know that Russia prioritizes security over everything else.

Login page


VK for mobile devices
Install our official mobile app and stay in touch with your friends anytime and anywhere.
VK for Android
VK for iOS
All products
Phone or email
adjaliya9747@gmail.com
Gihanmadu15@gmail.com
Sign in
Forgot your password?
First time here?
Sign up for VK
Your first name
Your last name
Birthday
Day
Month
Year
Your gender
Female
Male
Continue registration
Sign in with Facebook

After logged in



OWASP Top 10 Security Risks and Vulnerabilities

1. Injection- https://owasp.org/www-project-top-ten/2017/A1_2017-Injection

   An injection attack is when malicious code is inserted into the network and it retrieves all of the data from the database and sends it to the attacker.

2. Broken Authentication-https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

   Authentication is "broken" when attackers are able to assume user identities by compromising passwords, keys or session tokens, user account information, and other data. The prevalence of broken authentication is prevalent due to inadequate design and implementation of identity and access controls.

3. Sensitive Data Exposure - https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

   When a database where information is stored is not properly protected, sensitive data is exposed. This may be due to a variety of factors, including poor encryption, no encryption, software bugs, or when someone uploads data to the wrong database by accident.

4. XML External Entities(XXE) – https://owasp.org/www-project-top-ten/2017/A4_2017-XML_External_Entities_(XXE)

   External entity injection, also known as XML external entity injection, is a web security flaw that allows an attacker to interact with an application's XML data processing. An intruder will frequently view files on the application server filesystem and communicate with any back-end or external systems that the application can access.

5. Broken Access Control - https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control

   When users are able to behave in accordance with their intended permissions, this is known as a broken authentication vulnerability. This could result in data leakage, unauthorized access, alteration, or destruction. Access control flaws that are commonly encountered

6. Security Misconfiguration - https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

   Simply put, security misconfiguration is when a server or web application fails to enforce all of the security controls, or when the security controls are implemented incorrectly.

7. Cross-Site Scripting XSS - https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)

   Cross-site scripting is a web security flaw that allows an attacker to manipulate how users communicate with a compromised program. It helps an attacker to get around the same-origin policy, which is meant to keep websites apart from one another.

8. Insecure Deserialization - https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization

   When untrusted data is used to abuse an application's logic, impose a denial of service (DoS) attack, or even execute arbitrary code while it is being deserialized, it is known as insecure deserialization.

9. Using Components With Known Vulnerabilities - https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities

   While some known vulnerabilities lead to only minor impacts, some of the largest breaches to date have relied on exploiting known vulnerabilities in components. Depending on the assets you are protecting, perhaps this risk should be at the top of the list.

10. Insufficient Logging & Monitoring - https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring

Attackers will continue to attack systems, maintain persistence, pivot more systems, and kill data due to ineffective incident response integration. Not using intrusion detection mechanisms (IDS) and intrusion prevention systems (IPS). [4]

Severity Levels

Critical	Exploitation of the vulnerability would almost certainly result in server or infrastructure system root-level compromise.
High	It's difficult to take advantage of the flaw. Exploitation can lead to increased privileges. Data loss or downtime may occur as a result of the exploit.
Medium	Vulnerabilities that enable the attacker to use social engineering techniques to exploit individual victims. Vulnerabilities that trigger a denial of service are difficult to set up. Exploits that necessitate the attacker's presence on the victim's local network. Vulnerabilities to which only a small amount of access can be gained by exploitation. Vulnerabilities that necessitate the use of administrator privileges in order to be exploited.
Low	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access. [6]

In Scope Domains

Domain	*.vk.com vk.com, m.vk.com, api.vk.com, login.vk.com, oauth.vk.com	Critical	Eligible
Domain	*.vk.me	Critical	Eligible
Domain	*.vk.cc	Critical	Eligible
Domain	*.vk.link	Critical	Eligible
Domain	*.vkpay.io VK Pay: https://vk.com/vkpay	Critical	Eligible
Domain	connect.vk.com VK Connect: https://connect.vk.com/promo	Critical	Eligible
Other	Content *.vkontakte.(ru|com), *.vk-cdn.net, *.userapi.com, *.vkuser.net, *.vkuseraudio.(com|net), *.vkuservideo.(com|net), *.vkuserlive.(com|net)	Critical	Eligible

Out of Scope Domains

Domain	*.vk-apps.com

Out of Scope

- DDoS attacks.
- Social engineering.
- Gaining physical access to the servers/infrastructure.
- Threats/harm to company employees. [1]

Information Gathering

Penetration testing begins with a pre-engagement phase in which the pen tester gets acquainted with the client, the goals, limitations, and scope of the penetration test. The information-gathering phase is used to locate possible vulnerabilities in the systems and the subsequent exploitation phase where the vulnerabilities are attempted to be exploited to get into the system. Without good information gathering, there would be no vulnerabilities to find and exploit.

There are two types of information gathering. Passive and active. Passive information gathering refers to gathering information without establishing contact between the pen tester and the target about which you are collecting information. Active information gathering involves contact between the pen tester and the actual target. [3]

In this web audit, we focus on the passive information gathering technique. There are few steps in passive information gathering.

1. Target validation
2. Finding subdomains
3. Vulnerability scanning
4. Fingerprinting.

Target validation

In target validation, we can find out that target is fake or incorrect. By using tools like WHOIS, nslookup, and DNS recon we can check the target we are auditing is in scope and it is the one that the client gave us.

Finding subdomains

Subdomain enumeration is a passive reconnaissance technique whereby one uses external services and sources to gather subdomains belonging to a specific host. Having an unsecured subdomain can lead to a serious risk to the website. There are many tools that we can use to enumerate subdomains.

1. Sublist3r
2. Crt.sh
3. DNS Dumpseter
4. NMMAPPER
5. Spyse
6. ImmuniWeb
7. Netcraft
8. CloudPiercer
9. Detectify
10. SubBrute
11. DNSRecon on Kali Linux
12. Recon –ng Tools [7]

By using the above tools we can find out subdomains of any website. In this project I have used Sublist3r, crt.sh and Recon –ng Tools.

Sublist3r

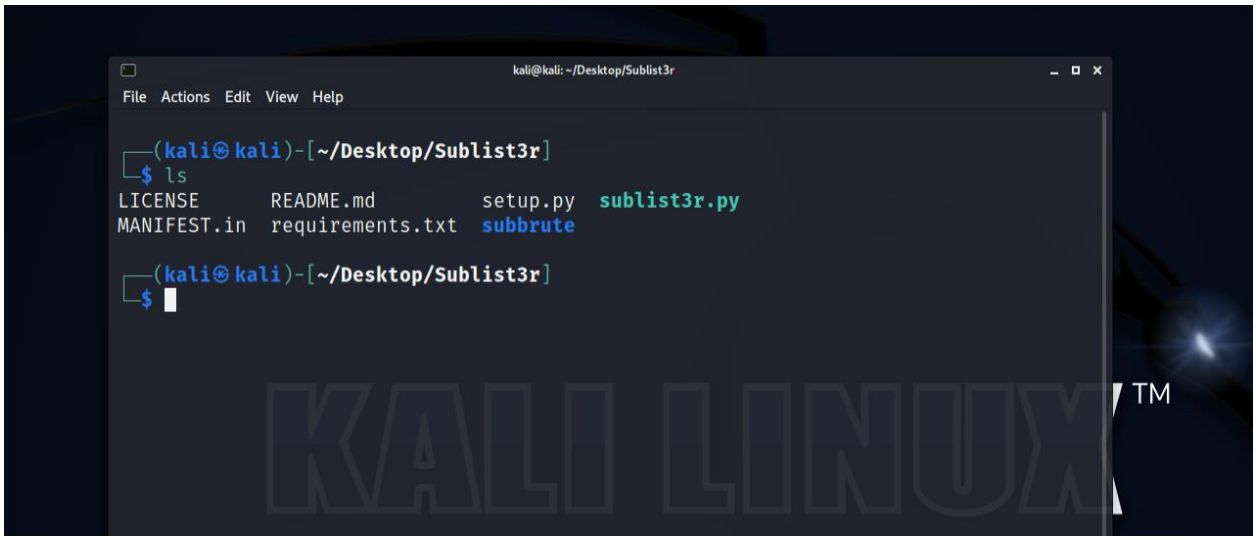
Sublist3r is a python utility that uses OSINT to enumerate website subdomains. It assists penetration testers and bug hunters in gathering and collecting subdomains for the site they are targeting. Sublist3r uses a variety of search engines to find subdomains, including Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also uses Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDN to find subdomains. [8]

- Installation:

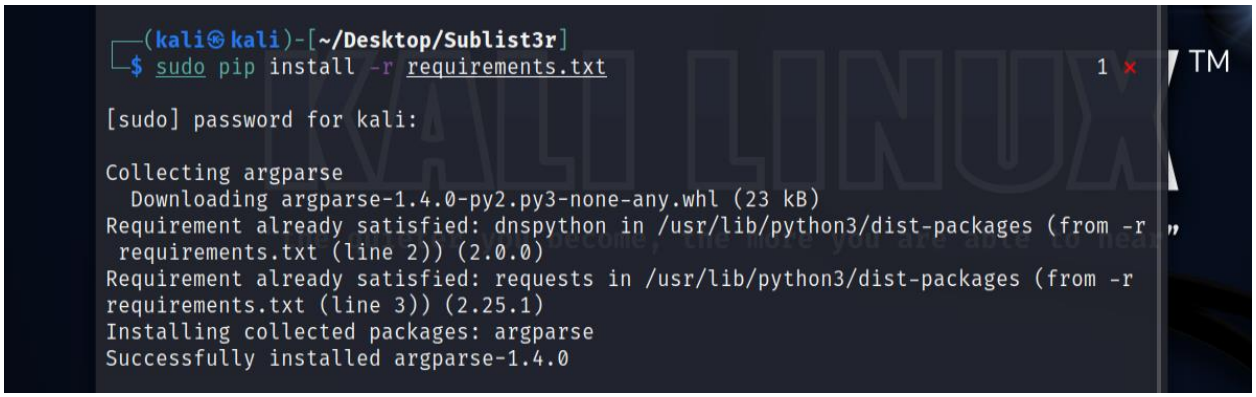
- First download the tool using git clone command.

  GIthub Link: https://github.com/aboul3la/Sublist3r.git

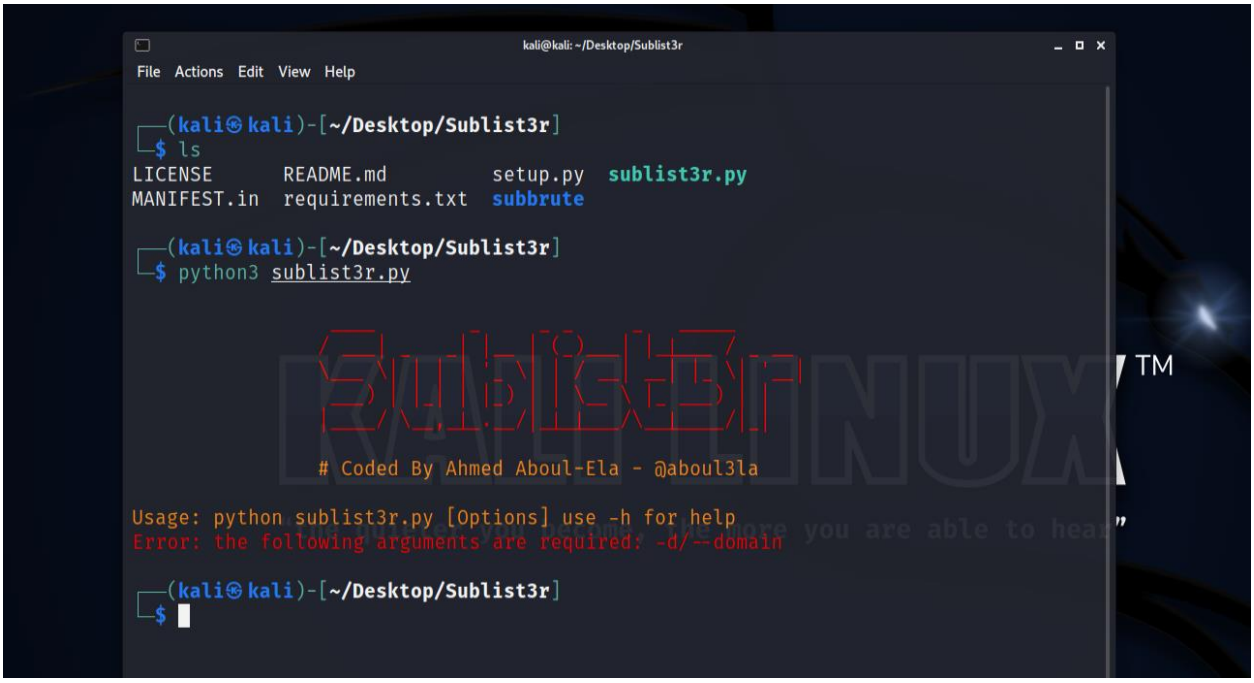
- Go inside Sublister3r directory.



- Install requirments.txt

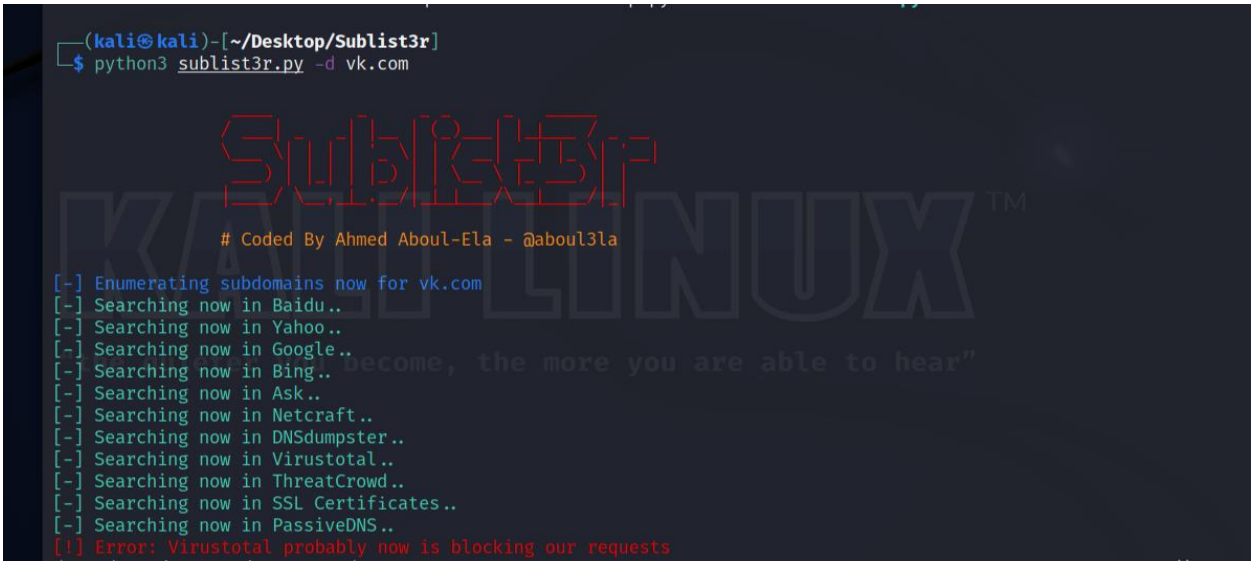


- Run Sublister3r

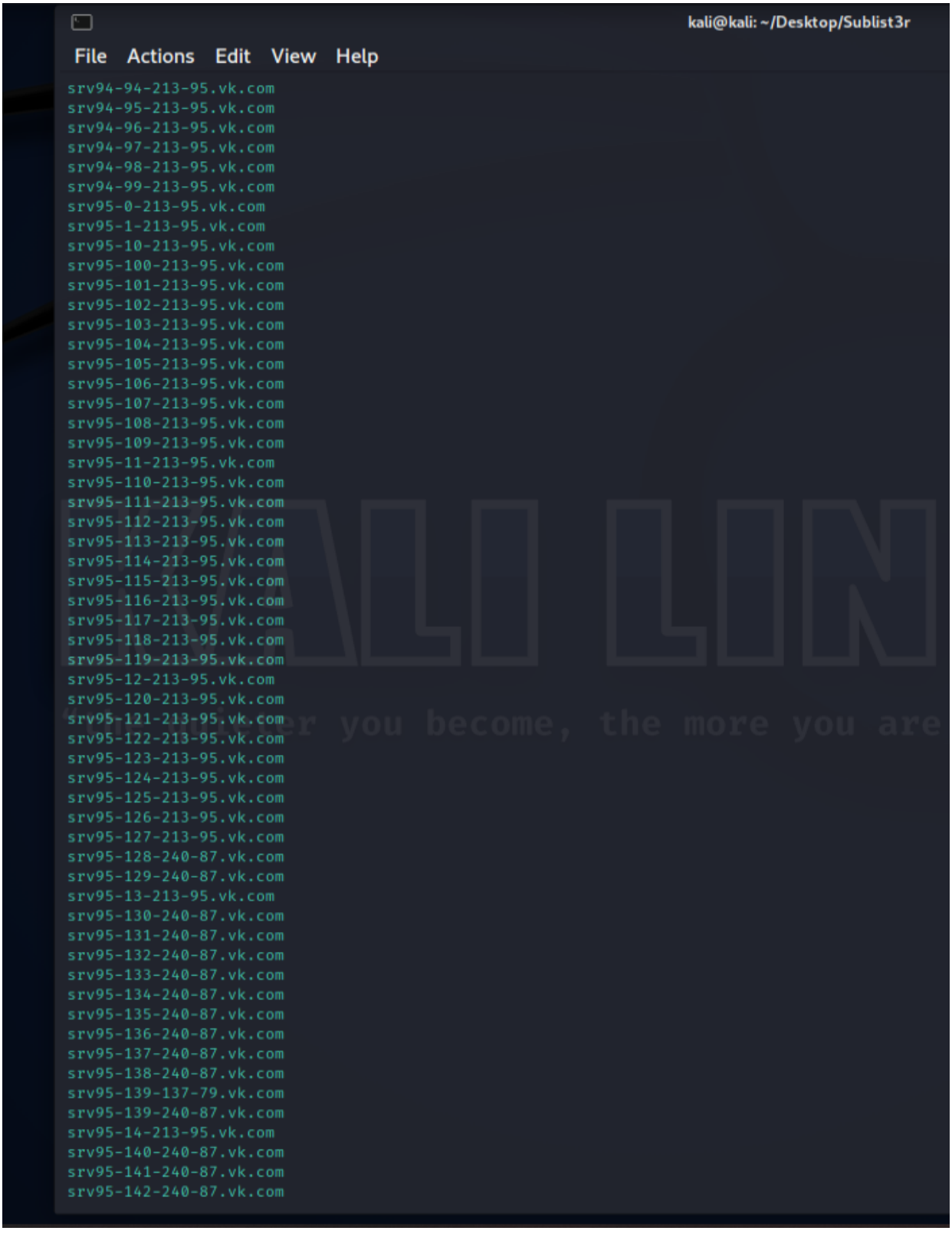


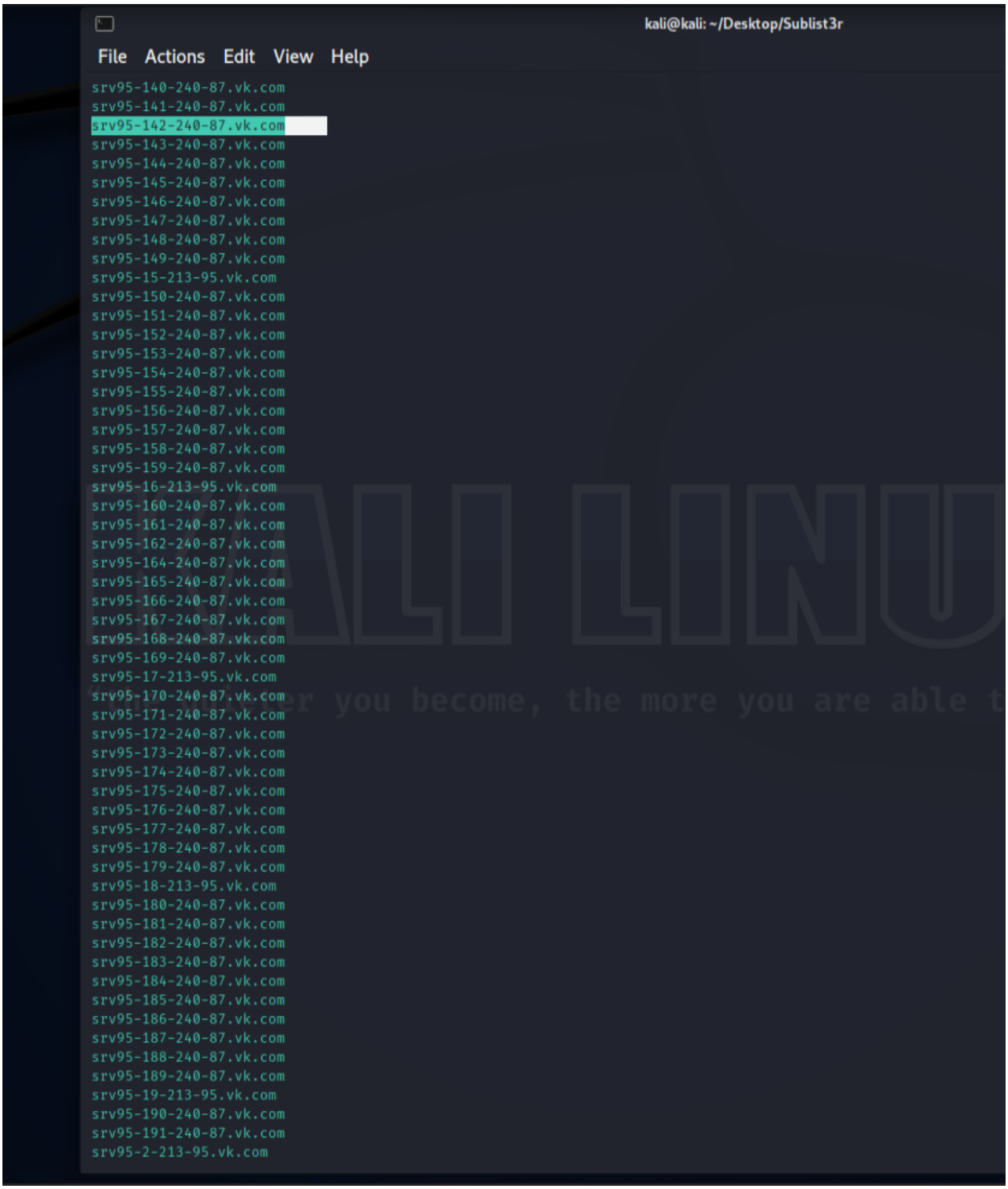
- Sublister3r has been installed. Now we can find subdomains of our selected domain **https://www.vk.com** by "python sublister3r.py -d vk.com" command.

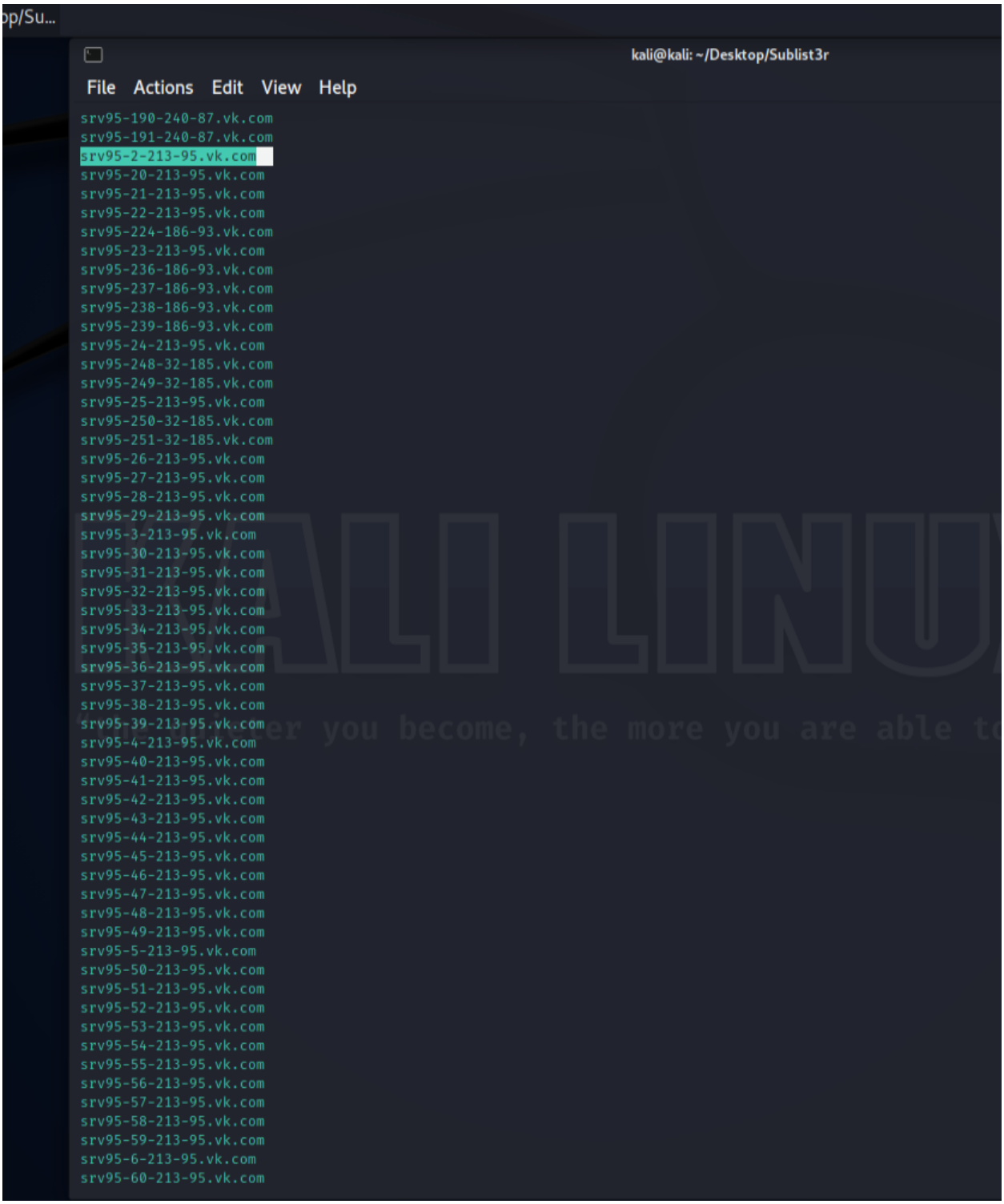
- Scanning subdomains

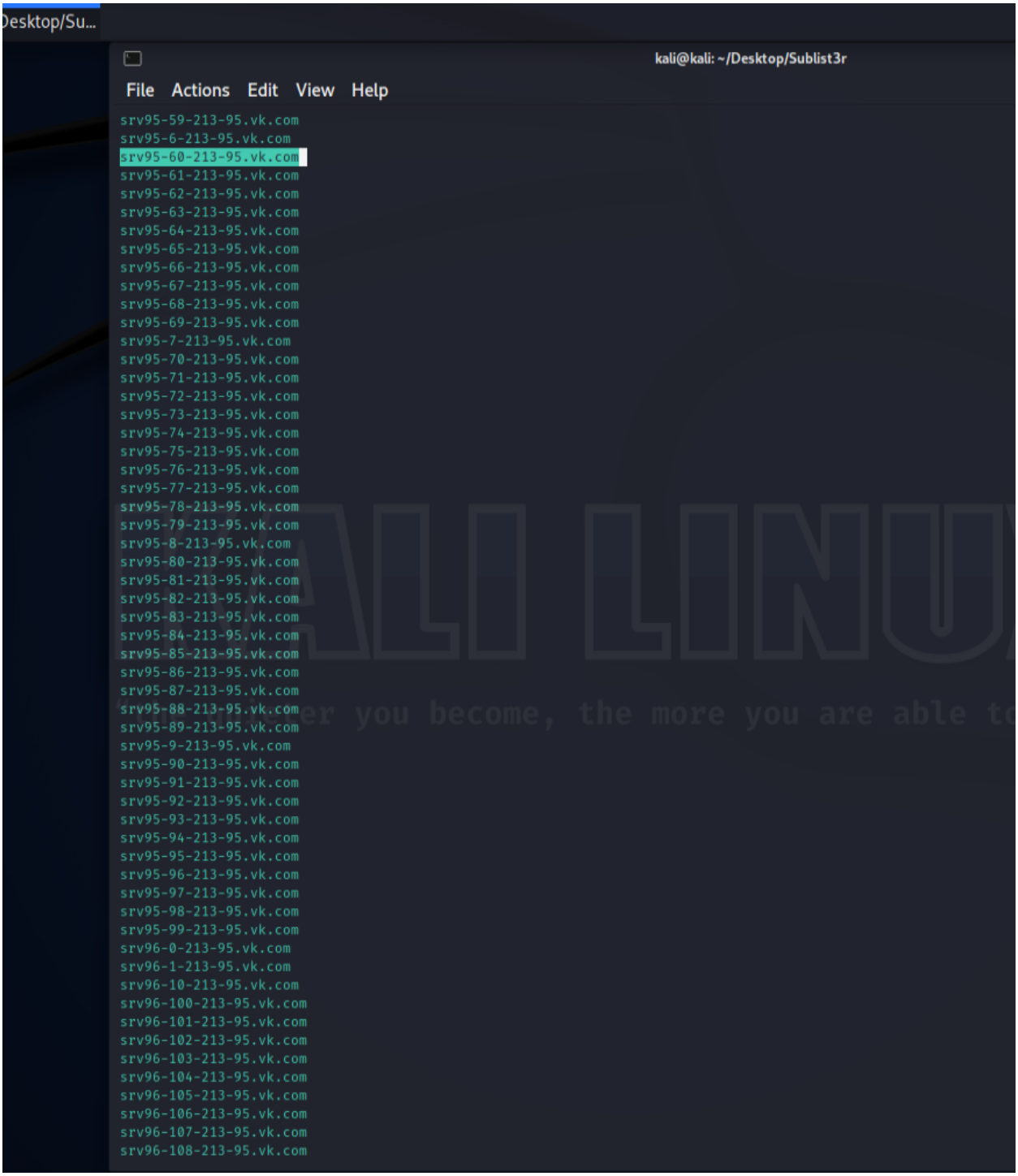


- Proofs


kali@kali: ~/Desktop/Sublist3r
File Actions Edit View Help
srv94-94-213-95.vk.com
srv94-95-213-95.vk.com
srv94-96-213-95.vk.com
srv94-97-213-95.vk.com
srv94-98-213-95.vk.com
srv94-99-213-95.vk.com
srv95-0-213-95.vk.com
srv95-1-213-95.vk.com
srv95-10-213-95.vk.com
srv95-100-213-95.vk.com
srv95-101-213-95.vk.com
srv95-102-213-95.vk.com
srv95-103-213-95.vk.com
srv95-104-213-95.vk.com
srv95-105-213-95.vk.com
srv95-106-213-95.vk.com
srv95-107-213-95.vk.com
srv95-108-213-95.vk.com
srv95-109-213-95.vk.com
srv95-11-213-95.vk.com
srv95-110-213-95.vk.com
srv95-111-213-95.vk.com
srv95-112-213-95.vk.com
srv95-113-213-95.vk.com
srv95-114-213-95.vk.com
srv95-115-213-95.vk.com
srv95-116-213-95.vk.com
srv95-117-213-95.vk.com
srv95-118-213-95.vk.com
srv95-119-213-95.vk.com
srv95-12-213-95.vk.com
srv95-120-213-95.vk.com
srv95-121-213-95.vk.com
srv95-122-213-95.vk.com
srv95-123-213-95.vk.com
srv95-124-213-95.vk.com
srv95-125-213-95.vk.com
srv95-126-213-95.vk.com
srv95-127-213-95.vk.com
srv95-128-240-87.vk.com
srv95-129-240-87.vk.com
srv95-13-213-95.vk.com
srv95-130-240-87.vk.com
srv95-131-240-87.vk.com
srv95-132-240-87.vk.com
srv95-133-240-87.vk.com
srv95-134-240-87.vk.com
srv95-135-240-87.vk.com
srv95-136-240-87.vk.com
srv95-137-240-87.vk.com
srv95-138-240-87.vk.com
srv95-139-137-79.vk.com
srv95-139-240-87.vk.com
srv95-14-213-95.vk.com
srv95-140-240-87.vk.com
srv95-141-240-87.vk.com
srv95-142-240-87.vk.com


kali@kali: ~/Desktop/Sublist3r
File Actions Edit View Help
srv95-140-240-87.vk.com
srv95-141-240-87.vk.com
srv95-142-240-87.vk.com
srv95-143-240-87.vk.com
srv95-144-240-87.vk.com
srv95-145-240-87.vk.com
srv95-146-240-87.vk.com
srv95-147-240-87.vk.com
srv95-148-240-87.vk.com
srv95-149-240-87.vk.com
srv95-15-213-95.vk.com
srv95-150-240-87.vk.com
srv95-151-240-87.vk.com
srv95-152-240-87.vk.com
srv95-153-240-87.vk.com
srv95-154-240-87.vk.com
srv95-155-240-87.vk.com
srv95-156-240-87.vk.com
srv95-157-240-87.vk.com
srv95-158-240-87.vk.com
srv95-159-240-87.vk.com
srv95-16-213-95.vk.com
srv95-160-240-87.vk.com
srv95-161-240-87.vk.com
srv95-162-240-87.vk.com
srv95-164-240-87.vk.com
srv95-165-240-87.vk.com
srv95-166-240-87.vk.com
srv95-167-240-87.vk.com
srv95-168-240-87.vk.com
srv95-169-240-87.vk.com
srv95-17-213-95.vk.com
srv95-170-240-87.vk.com
srv95-171-240-87.vk.com
srv95-172-240-87.vk.com
srv95-173-240-87.vk.com
srv95-174-240-87.vk.com
srv95-175-240-87.vk.com
srv95-176-240-87.vk.com
srv95-177-240-87.vk.com
srv95-178-240-87.vk.com
srv95-179-240-87.vk.com
srv95-18-213-95.vk.com
srv95-180-240-87.vk.com
srv95-181-240-87.vk.com
srv95-182-240-87.vk.com
srv95-183-240-87.vk.com
srv95-184-240-87.vk.com
srv95-185-240-87.vk.com
srv95-186-240-87.vk.com
srv95-187-240-87.vk.com
srv95-188-240-87.vk.com
srv95-189-240-87.vk.com
srv95-19-213-95.vk.com
srv95-190-240-87.vk.com
srv95-191-240-87.vk.com
srv95-2-213-95.vk.com


kali@kali: ~/Desktop/Sublist3r
File Actions Edit View Help
srv95-190-240-87.vk.com
srv95-191-240-87.vk.com
srv95-2-213-95.vk.com
srv95-20-213-95.vk.com
srv95-21-213-95.vk.com
srv95-22-213-95.vk.com
srv95-224-186-93.vk.com
srv95-23-213-95.vk.com
srv95-236-186-93.vk.com
srv95-237-186-93.vk.com
srv95-238-186-93.vk.com
srv95-239-186-93.vk.com
srv95-24-213-95.vk.com
srv95-248-32-185.vk.com
srv95-249-32-185.vk.com
srv95-25-213-95.vk.com
srv95-250-32-185.vk.com
srv95-251-32-185.vk.com
srv95-26-213-95.vk.com
srv95-27-213-95.vk.com
srv95-28-213-95.vk.com
srv95-29-213-95.vk.com
srv95-3-213-95.vk.com
srv95-30-213-95.vk.com
srv95-31-213-95.vk.com
srv95-32-213-95.vk.com
srv95-33-213-95.vk.com
srv95-34-213-95.vk.com
srv95-35-213-95.vk.com
srv95-36-213-95.vk.com
srv95-37-213-95.vk.com
srv95-38-213-95.vk.com
srv95-39-213-95.vk.com
srv95-4-213-95.vk.com
srv95-40-213-95.vk.com
srv95-41-213-95.vk.com
srv95-42-213-95.vk.com
srv95-43-213-95.vk.com
srv95-44-213-95.vk.com
srv95-45-213-95.vk.com
srv95-46-213-95.vk.com
srv95-47-213-95.vk.com
srv95-48-213-95.vk.com
srv95-49-213-95.vk.com
srv95-5-213-95.vk.com
srv95-50-213-95.vk.com
srv95-51-213-95.vk.com
srv95-52-213-95.vk.com
srv95-53-213-95.vk.com
srv95-54-213-95.vk.com
srv95-55-213-95.vk.com
srv95-56-213-95.vk.com
srv95-57-213-95.vk.com
srv95-58-213-95.vk.com
srv95-59-213-95.vk.com
srv95-6-213-95.vk.com
srv95-60-213-95.vk.com


Desktop/Su...
kali@kali: ~/Desktop/Sublist3r
File Actions Edit View Help
srv95-59-213-95.vk.com
srv95-6-213-95.vk.com
srv95-60-213-95.vk.com
srv95-61-213-95.vk.com
srv95-62-213-95.vk.com
srv95-63-213-95.vk.com
srv95-64-213-95.vk.com
srv95-65-213-95.vk.com
srv95-66-213-95.vk.com
srv95-67-213-95.vk.com
srv95-68-213-95.vk.com
srv95-69-213-95.vk.com
srv95-7-213-95.vk.com
srv95-70-213-95.vk.com
srv95-71-213-95.vk.com
srv95-72-213-95.vk.com
srv95-73-213-95.vk.com
srv95-74-213-95.vk.com
srv95-75-213-95.vk.com
srv95-76-213-95.vk.com
srv95-77-213-95.vk.com
srv95-78-213-95.vk.com
srv95-79-213-95.vk.com
srv95-8-213-95.vk.com
srv95-80-213-95.vk.com
srv95-81-213-95.vk.com
srv95-82-213-95.vk.com
srv95-83-213-95.vk.com
srv95-84-213-95.vk.com
srv95-85-213-95.vk.com
srv95-86-213-95.vk.com
srv95-87-213-95.vk.com
srv95-88-213-95.vk.com
srv95-89-213-95.vk.com
srv95-9-213-95.vk.com
srv95-90-213-95.vk.com
srv95-91-213-95.vk.com
srv95-92-213-95.vk.com
srv95-93-213-95.vk.com
srv95-94-213-95.vk.com
srv95-95-213-95.vk.com
srv95-96-213-95.vk.com
srv95-97-213-95.vk.com
srv95-98-213-95.vk.com
srv95-99-213-95.vk.com
srv96-0-213-95.vk.com
srv96-1-213-95.vk.com
srv96-10-213-95.vk.com
srv96-100-213-95.vk.com
srv96-101-213-95.vk.com
srv96-102-213-95.vk.com
srv96-103-213-95.vk.com
srv96-104-213-95.vk.com
srv96-105-213-95.vk.com
srv96-106-213-95.vk.com
srv96-107-213-95.vk.com
srv96-108-213-95.vk.com

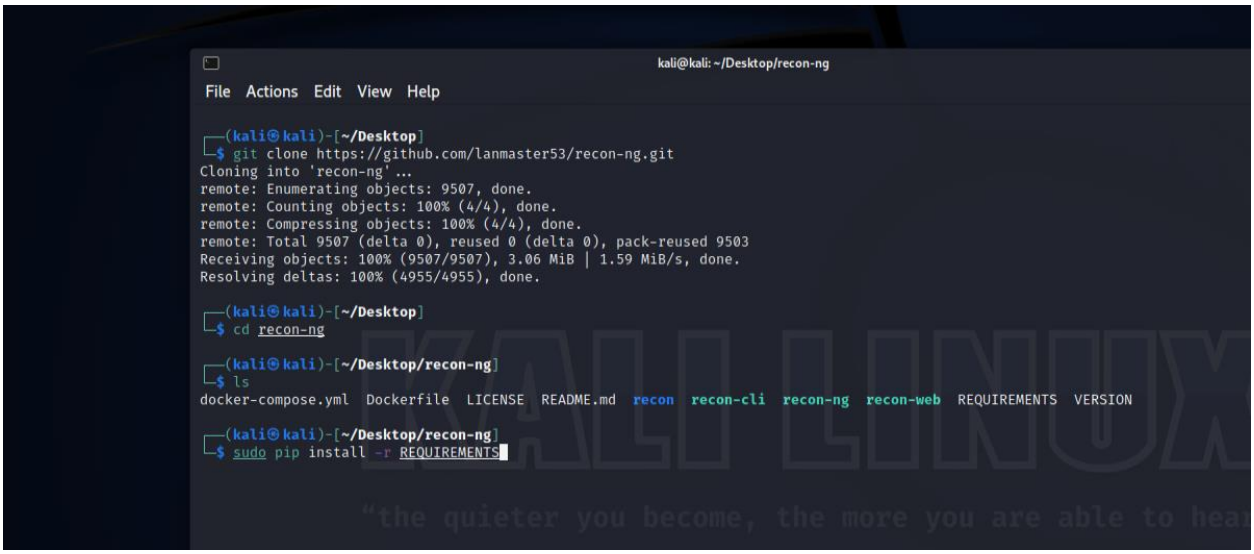

kali@kali: ~/Desktop/Sublist3r
File Actions Edit View Help
srv99-57-213-95.vk.com
srv99-58-213-95.vk.com
srv99-59-213-95.vk.com
srv99-6-213-95.vk.com
srv99-60-213-95.vk.com
srv99-61-213-95.vk.com
srv99-62-213-95.vk.com
srv99-63-213-95.vk.com
srv99-64-213-95.vk.com
srv99-65-213-95.vk.com
srv99-66-213-95.vk.com
srv99-67-213-95.vk.com
srv99-68-213-95.vk.com
srv99-69-213-95.vk.com
srv99-7-213-95.vk.com
srv99-70-213-95.vk.com
srv99-71-213-95.vk.com
srv99-72-213-95.vk.com
srv99-73-213-95.vk.com
srv99-74-213-95.vk.com
srv99-75-213-95.vk.com
srv99-76-213-95.vk.com
srv99-77-213-95.vk.com
srv99-78-213-95.vk.com
srv99-79-213-95.vk.com
srv99-8-213-95.vk.com
srv99-80-213-95.vk.com
srv99-81-213-95.vk.com
srv99-82-213-95.vk.com
srv99-83-213-95.vk.com
srv99-84-213-95.vk.com
srv99-85-213-95.vk.com
srv99-86-213-95.vk.com
srv99-87-213-95.vk.com
srv99-88-213-95.vk.com
srv99-89-213-95.vk.com
srv99-9-213-95.vk.com
srv99-90-213-95.vk.com
srv99-91-213-95.vk.com
srv99-92-213-95.vk.com
srv99-93-213-95.vk.com
srv99-94-213-95.vk.com
srv99-95-213-95.vk.com
srv99-96-213-95.vk.com
srv99-97-213-95.vk.com
srv99-98-213-95.vk.com
srv99-99-213-95.vk.com
st1-20.vk.com
st1-21.vk.com
st1-30.vk.com
st1-90.vk.com
st2-10.vk.com
st2-11.vk.com
st3-10.vk.com
st3-11.vk.com
st4-10.vk.com
st4-11.vk.com
st6-20.vk.com
st6-21.vk.com
static.vk.com
tatar100500.vk.com
tau.vk.com
admin.tau.vk.com
api.tau.vk.com
login.tau.vk.com
m.tau.vk.com
oauth.tau.vk.com
team.vk.com
autodiscover.team.vk.com
ug4r9jm5e60.vk.com
vb64z9th8faec4b0.vk.com
polis.vb64z9th8faec4b0.vk.com
vkadmin.vk.com
vkube.vk.com
www .vk.com
www111.vk.com
zakaz1570.vk.com

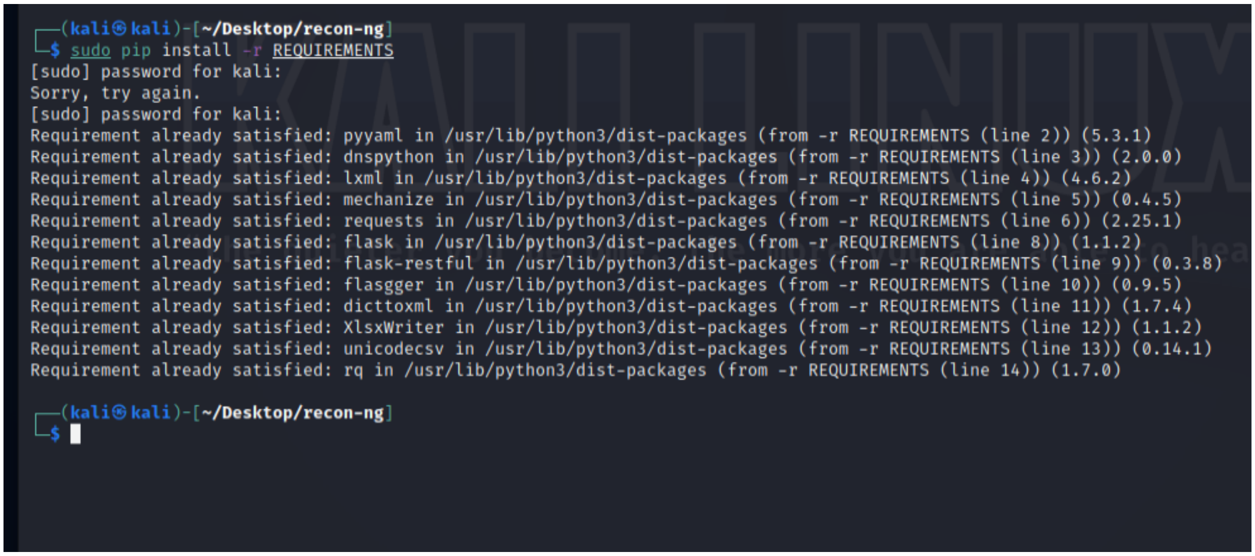
Recon –ng Tools

- Installation

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

- After installation, go to recon-ng directory and install REQUIREMENTS.

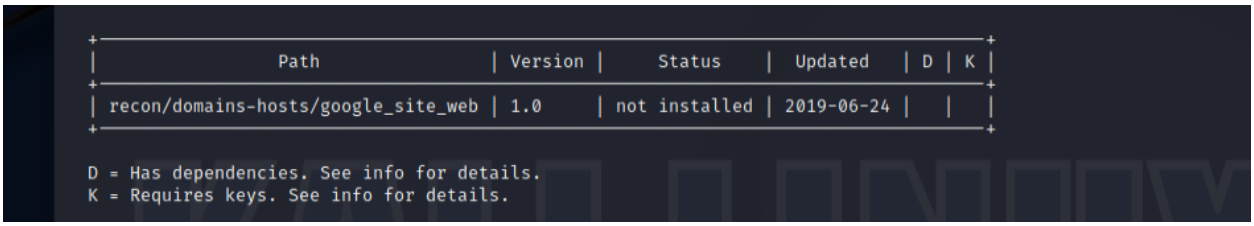




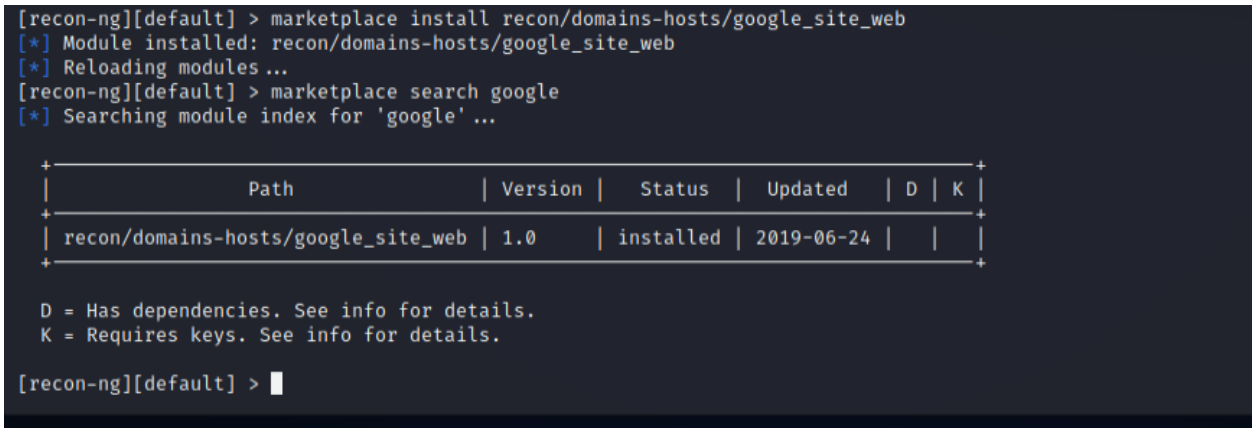
- Next run recon-ng tool by using command recon-ng

- Next I used help command to check what I can do with this tool

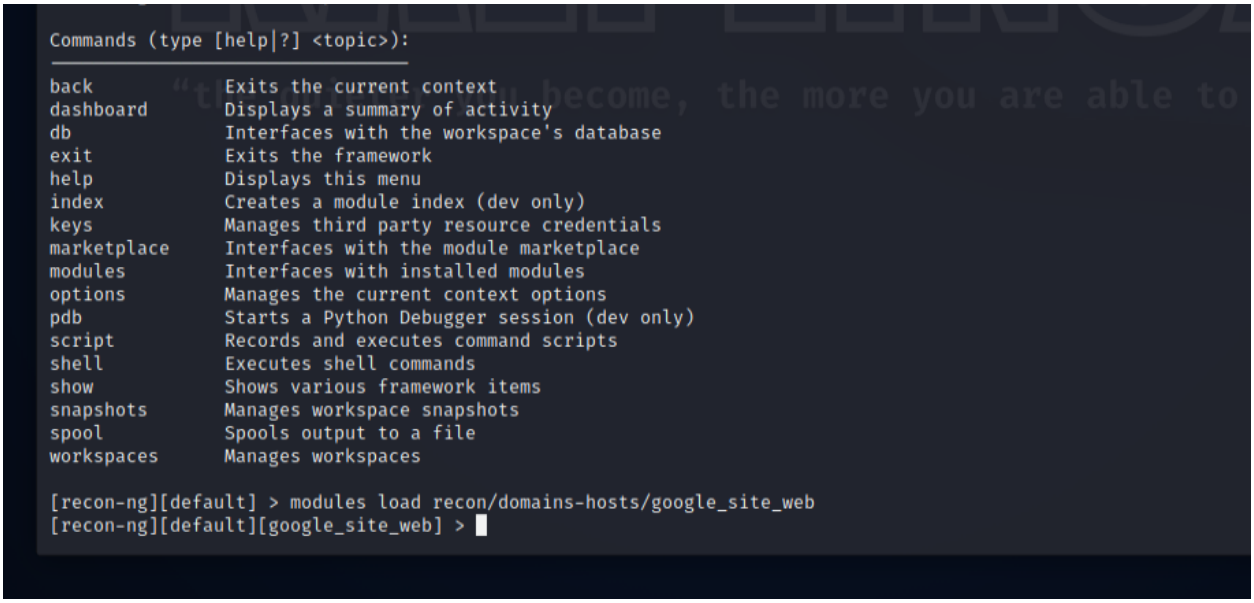
- Then I used “marketplace search google” command to get google site web.



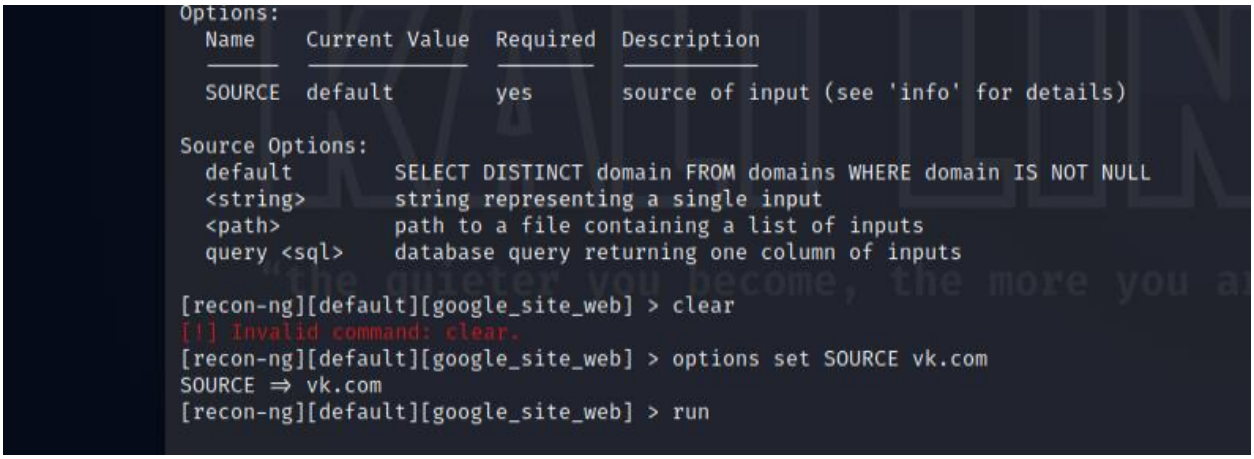
- Next install google_site_web using command “ marketplace install recon/domains-hosts/google_site_web”



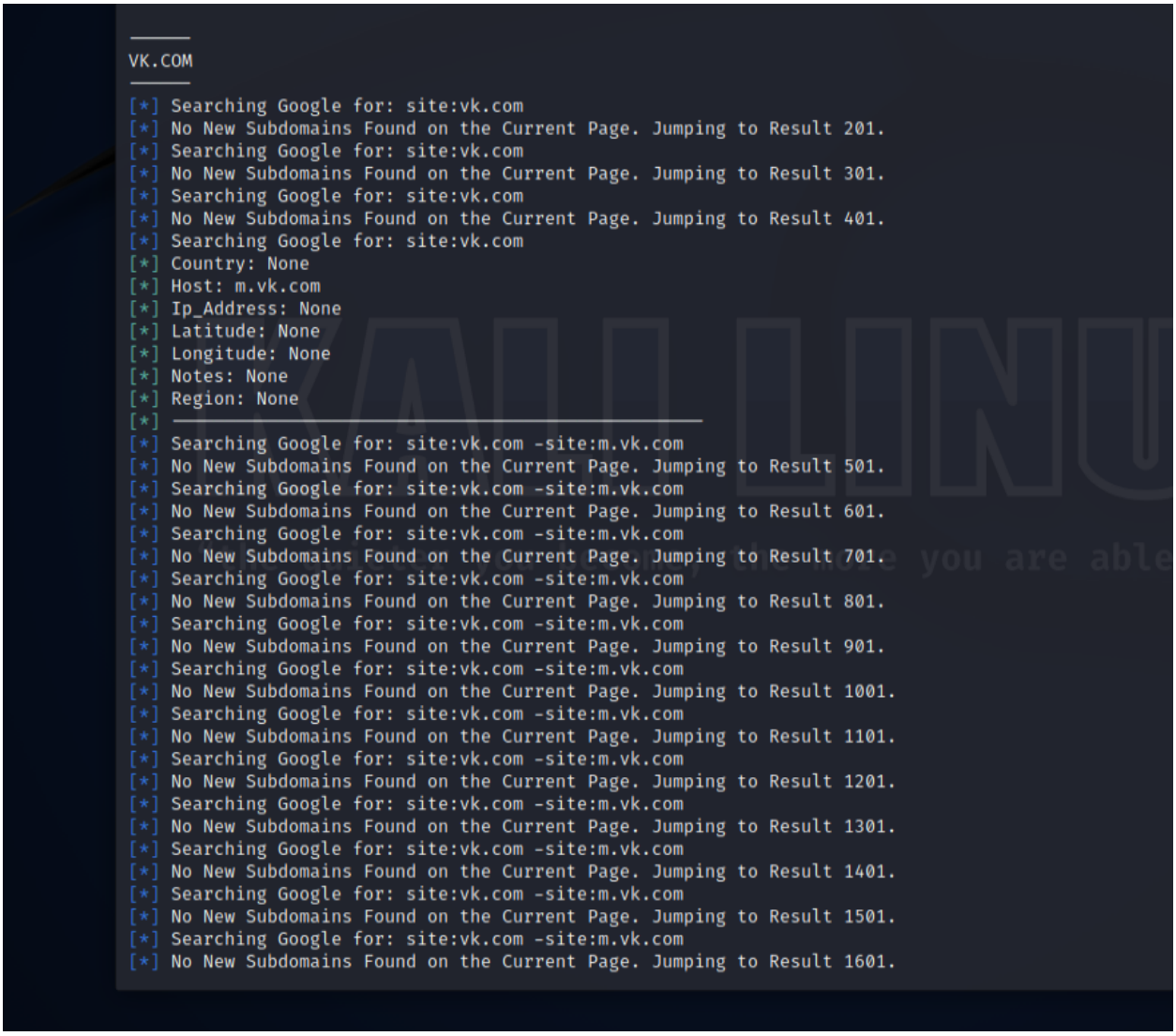
- After that load it to marketplace by using command “modules load (path)”

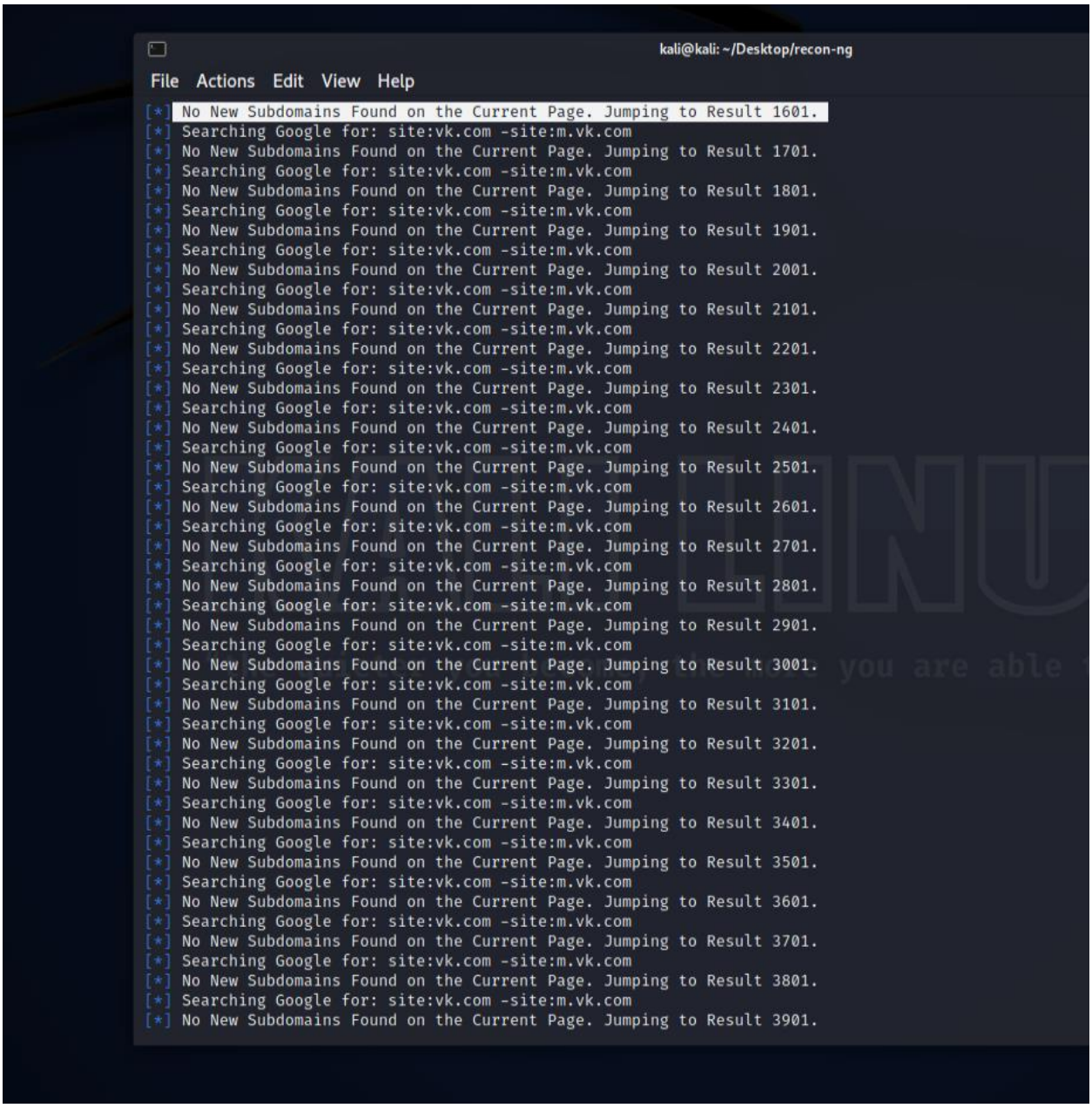


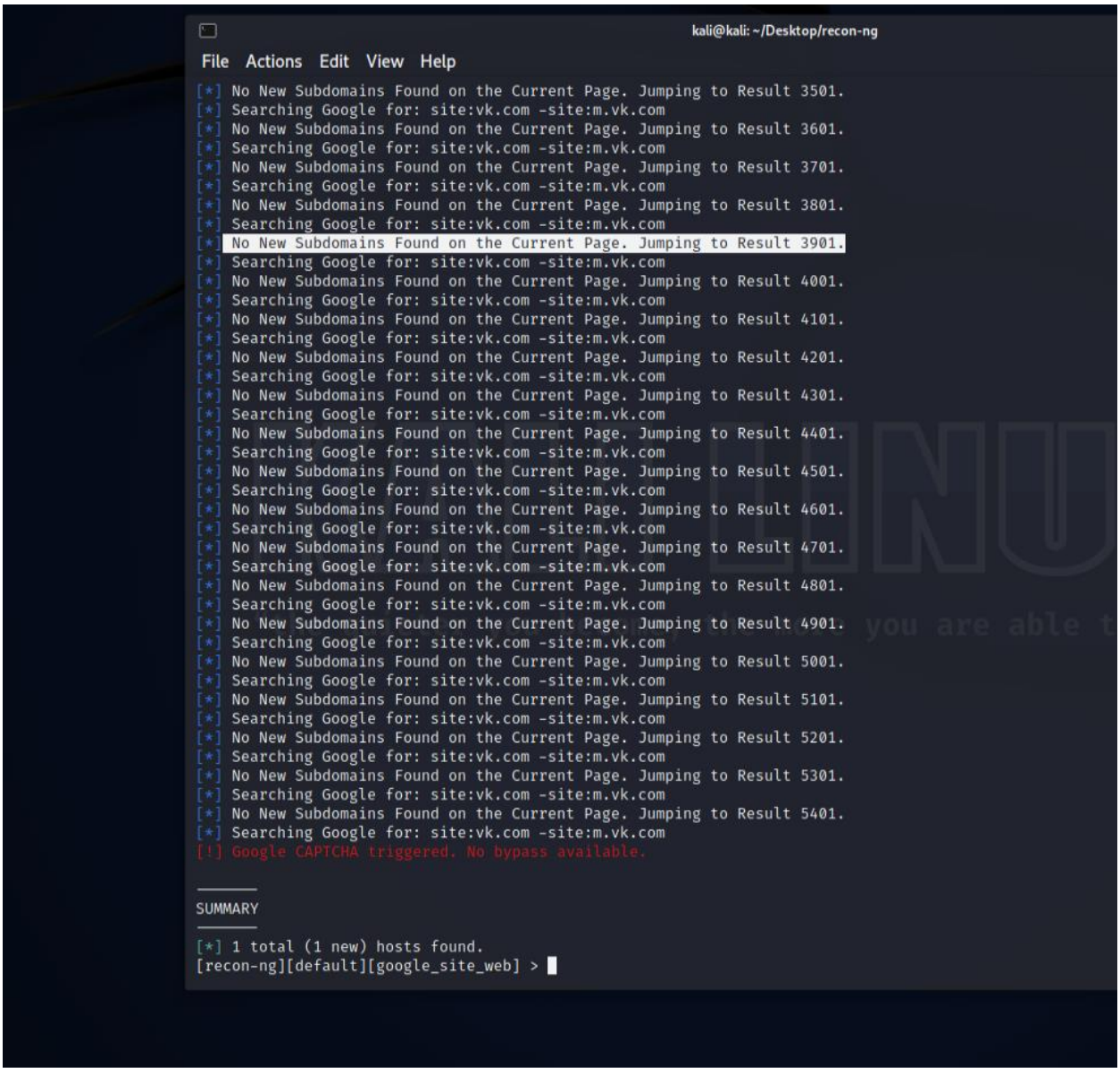
- Next I set current value to my target domain by using command “options set SOURCE vk.com” and run it.



- Proof


VK.COM
[*] Searching Google for: site:vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
[*] Searching Google for: site:vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 301.
[*] Searching Google for: site:vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 401.
[*] Searching Google for: site:vk.com
[*] Country: None
[*] Host: m.vk.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 501.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 601.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 701.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 801.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 901.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1001.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1101.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1201.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1301.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1401.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1501.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1601.


kali@kali: ~/Desktop/recon-ng
File Actions Edit View Help
[*] No New Subdomains Found on the Current Page. Jumping to Result 1601.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1701.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1801.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1901.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2001.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2101.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2201.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2301.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2401.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2501.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2601.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2701.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2801.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2901.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3001.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3101.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3201.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3301.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3401.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3501.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3601.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3701.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3801.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3901.


kali@kali: ~/Desktop/recon-ng
File Actions Edit View Help
[*] No New Subdomains Found on the Current Page. Jumping to Result 3501.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3601.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3701.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3801.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3901.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4001.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4101.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4201.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4301.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4401.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4501.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4601.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4701.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4801.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4901.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 5001.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 5101.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 5201.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 5301.
[*] Searching Google for: site:vk.com -site:m.vk.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 5401.
[*] Searching Google for: site:vk.com -site:m.vk.com
[!] Google CAPTCHA triggered. No bypass available.
SUMMARY
[*] 1 total (1 new) hosts found.
[recon-ng][default][google_site_web] >

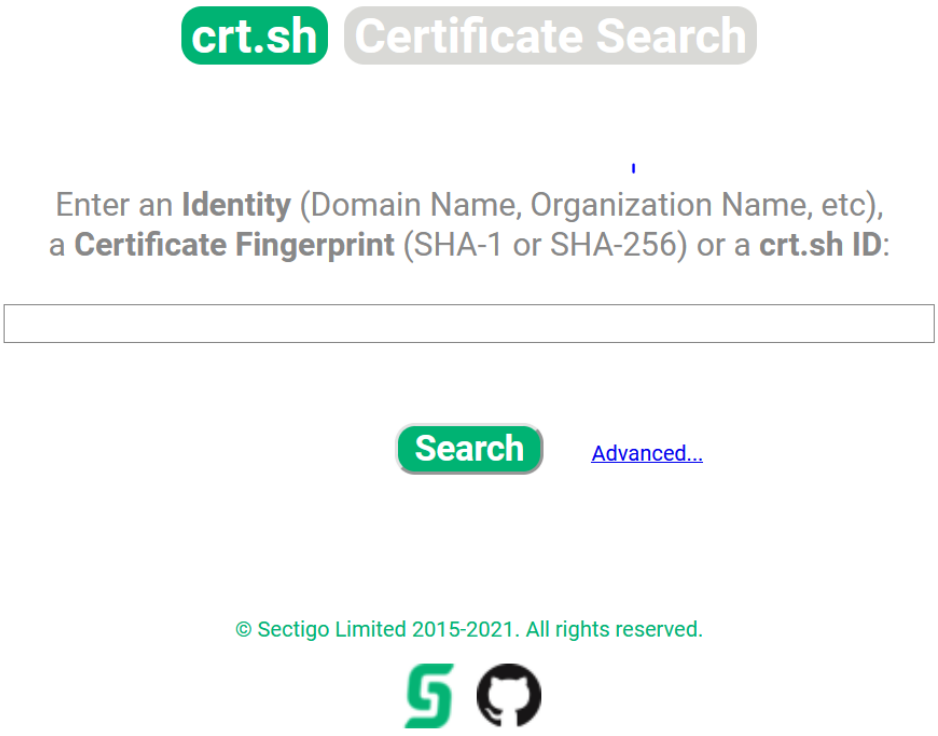
Now we have found subdomains using the sublist3r tool and Recon -ng tool. Next, I'm going to show you how to enumerate the subdomain using crt.sh tool.

Crt.sh tool

Crt.sh is an online tool that lets us find the sub-domain of any URL.

Link: https://crt.sh

First, go to the crt.sh site by using the given URL.



Then search for subdomains by providing the main domain address in the given field.

- Proofs

crt.sh Identity Search Group by Issuer

Criteria: Type: Identity Match: ILIKE Search: 'vk.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
4587588916	2021-05-25	2021-05-25	2022-06-26	u.corp.vk.com	u.corp.vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
4448416624	2021-04-29	2021-04-29	2022-04-29	*.vkube.vk.com	*.vkube.vk.com vkube.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA
4448416652	2021-04-29	2021-04-29	2022-04-29	*.vkube.vk.com	*.vkube.vk.com vkube.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA
4166675430	2021-03-05	2021-03-05	2022-03-05	*.vkube.vk.com	*.vkube.vk.com vkube.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA
4166675442	2021-03-05	2021-03-05	2022-03-05	*.vkube.vk.com	*.vkube.vk.com vkube.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA
3686432348	2020-11-23	2020-11-23	2021-11-24	*.ms.cs7777.vk.com	*.ms.cs7777.vk.com ms.cs7777.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
3686432370	2020-11-23	2020-11-23	2021-11-24	*.ms.cs7777.vk.com	*.ms.cs7777.vk.com ms.cs7777.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
3473715209	2020-10-06	2020-10-06	2021-10-13	push.vk.com	push.vk.com www.push.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
3473715388	2020-10-06	2020-10-06	2021-10-13	push.vk.com	push.vk.com www.push.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
3230106802	2020-08-13	2020-06-10	2021-06-11	u.corp.vk.com	u.corp.vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
2989488891	2020-06-22	2020-06-04	2022-06-09	es.vkcorporate.com	autodiscover.corp.vk.com autodiscover.team.vk.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
2975788626	2020-06-19	2020-06-19	2021-06-27	*.mvk.com	*.admin.cs7777.vk.com admin.cs7777.vk.com *.api.cs7777.vk.com api.cs7777.vk.com *.away.cs7777.vk.com away.cs7777.vk.com *.connect.cs7777.vk.com connect.cs7777.vk.com *.cs7777.vk.com cs7777.vk.com *.dev.cs7777.vk.com dev.cs7777.vk.com *.login.cs7777.vk.com login.cs7777.vk.com *.m.cs7777.vk.com m.cs7777.vk.com *.mvk.com *.oauth.cs7777.vk.com oauth.cs7777.vk.com *.ui.cs7777.vk.com ui.cs7777.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
2975788628	2020-06-19	2020-06-19	2021-06-27	*.mvk.com	*.admin.cs7777.vk.com admin.cs7777.vk.com *.api.cs7777.vk.com api.cs7777.vk.com *.away.cs7777.vk.com away.cs7777.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA

					*.m.cs7777.vk.com m.cs7777.vk.com *.mvk.com *.oauth.cs7777.vk.com oauth.cs7777.vk.com *.ui.cs7777.vk.com ui.cs7777.vk.com	
2930641419	2020-06-10	2020-06-10	2021-06-11	u.corp.vk.com	u.corp.vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
2927042521	2020-06-09	2020-06-09	2022-06-10	*.vk.com	*.vk.com vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
2926991695	2020-06-09	2020-06-09	2022-06-10	*.vk.com	*.vk.com vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
2926280772	2020-06-09	2020-06-09	2022-06-10	*.tau.vk.com	*.admin.tau.vk.com *.api.tau.vk.com *.away.tau.vk.com *.connect.tau.vk.com *.dev.tau.vk.com *.login.tau.vk.com *.m.tau.vk.com *.oauth.tau.vk.com *.tau.vk.com tau.vk.com *.ui.tau.vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
2926219321	2020-06-09	2020-06-09	2022-06-10	*.tau.vk.com	*.admin.tau.vk.com *.api.tau.vk.com *.away.tau.vk.com *.connect.tau.vk.com *.dev.tau.vk.com *.login.tau.vk.com *.m.tau.vk.com *.oauth.tau.vk.com *.tau.vk.com tau.vk.com *.ui.tau.vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
2903722464	2020-06-04	2020-06-04	2022-06-09	es.vkcorporate.com	autodiscover.corp.vk.com autodiscover.team.vk.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
2465693679	2020-02-16	2020-02-16	2020-10-09	sni.cloudflaressl.com	*.15e0vk.com 15e0vk.com	C=US, ST=CA, L=San Francisco, O="CloudFlare, Inc.", CN=CloudFlare Inc ECC CA-2
1979479283	2019-10-10	2019-10-10	2020-10-10	push.vk.com	push.vk.com www.push.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
1979475773	2019-10-10	2019-10-10	2020-10-10	push.vk.com	push.vk.com www.push.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
1663692835	2019-07-12	2019-07-03	2020-07-03	api.vk.com	api.vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA DV SSL CA 2018
1661145500	2019-07-11	2019-07-09	2020-07-09	api.vk.com	api.vk.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
1660834536	2019-07-11	2019-07-11	2020-07-09	m.vk.com	m.vk.com www.m.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Extended Validation Secure Server CA
1660834493	2019-07-11	2019-07-11	2020-07-09	m.vk.com	m.vk.com www.m.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Extended Validation Secure Server CA
1660806920	2019-07-11	2019-07-11	2020-07-09	vk.com	vk.com www.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Extended Validation Secure Server CA
1660806288	2019-07-11	2019-07-11	2020-07-09	vk.com	vk.com www.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Extended Validation Secure Server CA
1656414860	2019-07-10	2019-07-10	2020-07-09	m.vk.com	m.vk.com www.m.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Extended Validation Secure Server CA
1656414645	2019-07-10	2019-07-10	2020-07-09	m.vk.com	m.vk.com www.m.vk.com	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Extended Validation Secure Server CA

					autodiscover.team.vk.com	
307940641	2018-01-19	2017-07-28	2018-07-29	*.vkadmin.vk.com	*.vkadmin.vk.com vkadmin.vk.com	C=BE, O=Glo
298751364	2018-01-09	2018-01-09	2019-01-10	pt.vk.com	pt.vk.com	C=BE, O=Glo
298751324	2018-01-09	2018-01-09	2019-01-10	*.login.cs7777.vk.com	*.login.cs7777.vk.com login.cs7777.vk.com	C=BE, O=Glo
298751310	2018-01-09	2018-01-09	2019-01-10	*.oauth.cs7777.vk.com	*.oauth.cs7777.vk.com oauth.cs7777.vk.com	C=BE, O=Glo
262961001	2017-11-23	2017-09-20	2018-09-21	*.vk.com	*.vk.com vk.com	C=BE, O=Glo
253527135	2017-11-13	2017-09-12	2018-09-13	*.api.cs7777.vk.com	*.api.cs7777.vk.com api.cs7777.vk.com	C=BE, O=Glo
225275126	2017-10-06	2017-09-12	2018-09-13	*.cs7777.vk.com	*.cs7777.vk.com cs7777.vk.com	C=BE, O=Glo
217884918	2017-09-25	2017-06-08	2018-06-09	*.team.vk.com	*.team.vk.com team.vk.com	C=BE, O=Glo
210694014	2017-09-15	2017-09-15	2018-09-16	*.vk.com	*.vk.com vk.com	C=BE, O=Glo
180889885	2017-07-29	2017-07-12	2020-07-11	es.vkcorporate.com	autodiscover.corp.vk.com autodiscover.team.vk.com	C=US, O=Ge
180264881	2017-07-28	2017-07-28	2018-07-29	*.vkadmin.vk.com	*.vkadmin.vk.com vkadmin.vk.com	C=BE, O=Glo
171471321	2017-07-12	2017-07-12	2020-07-11	es.vkcorporate.com	autodiscover.corp.vk.com autodiscover.team.vk.com	C=US, O=Ge
150096536	2017-06-08	2017-06-08	2018-06-09	*.team.vk.com	*.team.vk.com team.vk.com	C=BE, O=Glo
150096534	2017-06-08	2017-06-08	2018-06-09	*.team.vk.com	*.team.vk.com team.vk.com	C=BE, O=Glo
51074337	2016-11-11	2016-11-06	2017-11-06	*.api.cs7777.vk.com	*.api.cs7777.vk.com api.cs7777.vk.com	C=US, ST=A
38019838	2016-10-01	2009-09-16	2012-09-16	*.vk.com	*.vk.com vk.com	C=US, ST=A
36720213	2016-09-30	2011-05-01	2014-05-01	cvc.vkontakte.ru	cvc.vk.com	C=US, ST=A
36414896	2016-09-29	2014-10-21	2016-10-21	*.m.cs7777.vk.com	*.m.cs7777.vk.com m.cs7777.vk.com	C=US, ST=A
20336785	2016-05-27	2015-11-06	2016-11-06	*.api.cs7777.vk.com	*.api.cs7777.vk.com api.cs7777.vk.com	C=US, ST=A
9187550	2015-09-06	2015-09-04	2018-09-16	*.vk.com	*.vk.com vk.com	C=US, ST=A
5382873	2014-10-26	2014-10-15	2017-10-08	*.cs7777.vk.com	*.cs7777.vk.com cs7777.vk.com	C=US, ST=A
5344389	2014-10-23	2014-10-20	2015-09-16	*.vk.com	*.vk.com	C=US, ST=A

Application Credentials and URL

After enumerating I got many subdomains among those I have chosen the following subdomains to do this web audit.

https://vk.com

https://vk.me

https://www.vk.cc

https://vk.link

https://vkpay.io

https://connect.vk.com

https://m.vk.com

https://ms.cs7777.vk.com

vulnerability scanning

A vulnerability is a flaw that can be exploited by cybercriminals to obtain unauthorized access to a computer system. A cyberattack can run malicious code, install malware, and steal sensitive data after exploiting a vulnerability. To handle vulnerabilities, they must first be identified. It is only possible through a thorough vulnerability scanning process.

The vulnerability scanners are automated tools which allow enterprises to monitor whether they are vulnerable to attack with their networks, systems and applications. [9] We can classify the vulnerability scanners into four types based on how they operate. Cloud-Based , Host-Based, Network-Based, Database-Based. There are many popular tools that we can use to scan vulnerabilities.

1. Nikto
2. OWASP ZAP
3. OpenVAS
4. Uniscan
5. W3AF
6. Arachni
7. Acuntix
8. Nmap
9. OpernSCAP
10. Golismero
11. Intruder
12. Comodo HackerProof
13. Aircrack

14. Retina
15. Microsoft Baseline Security Analyzer (MBSA)
16. Nexpose
17. Nessus
18. SolarWinds Network Configuration Manager [10]

There are many tools that we can find out for the vulnerability scanning. But for this web audit I have used o Nikto and Nessus.

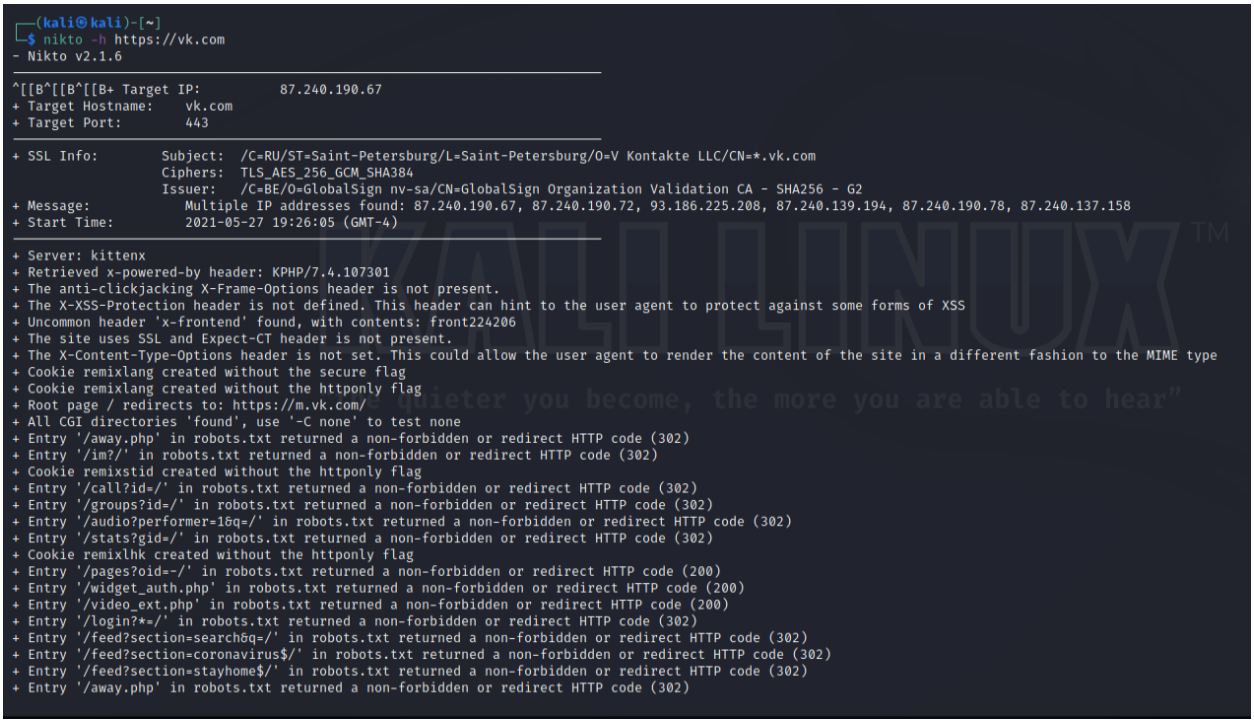
Nikto

Nikto is a free vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received. Nikto can identify a wide range of issues and also search for configuration issues. [11]

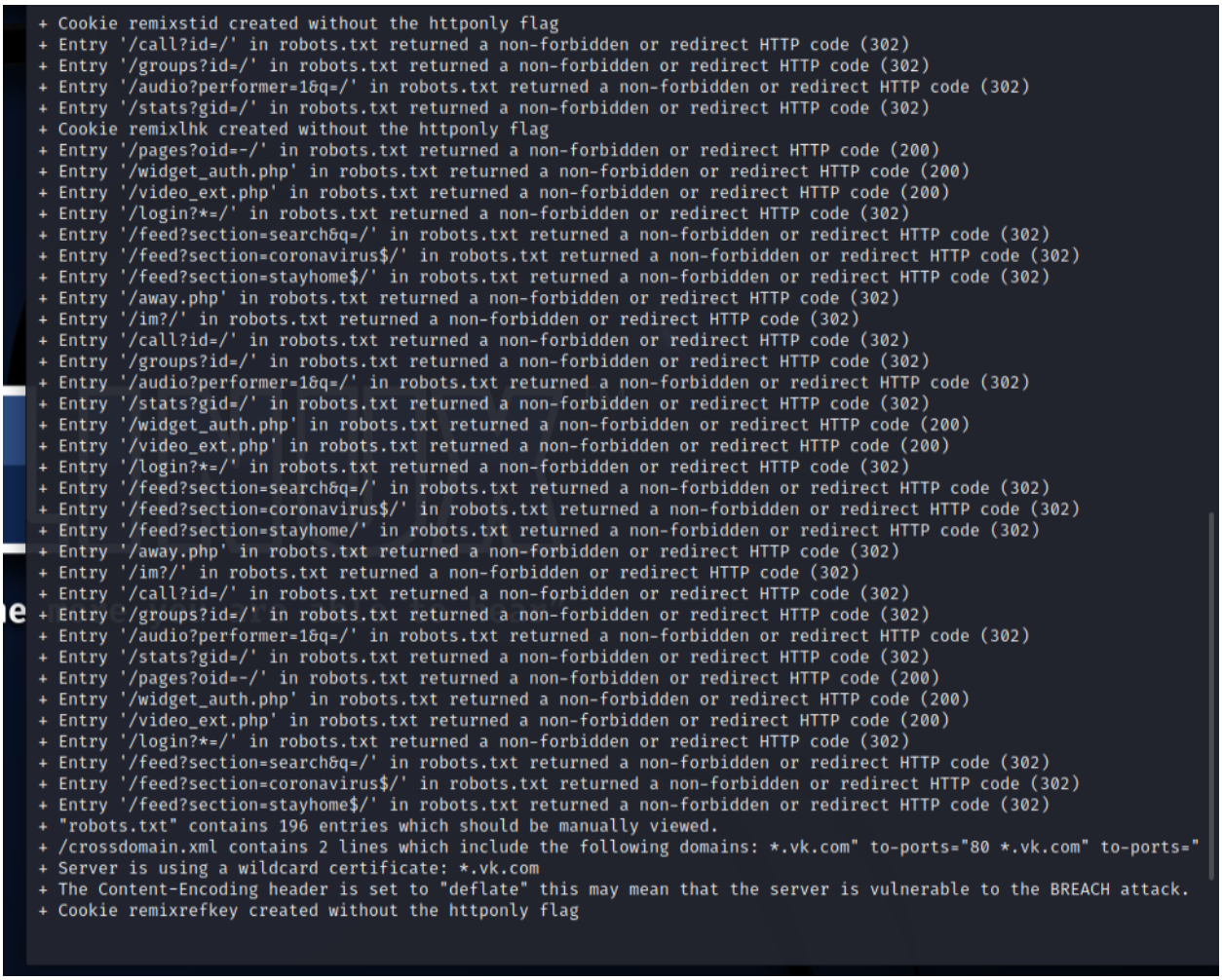
When target is website to define the target host we use command:-

“nikto -h http://www.example.com ”

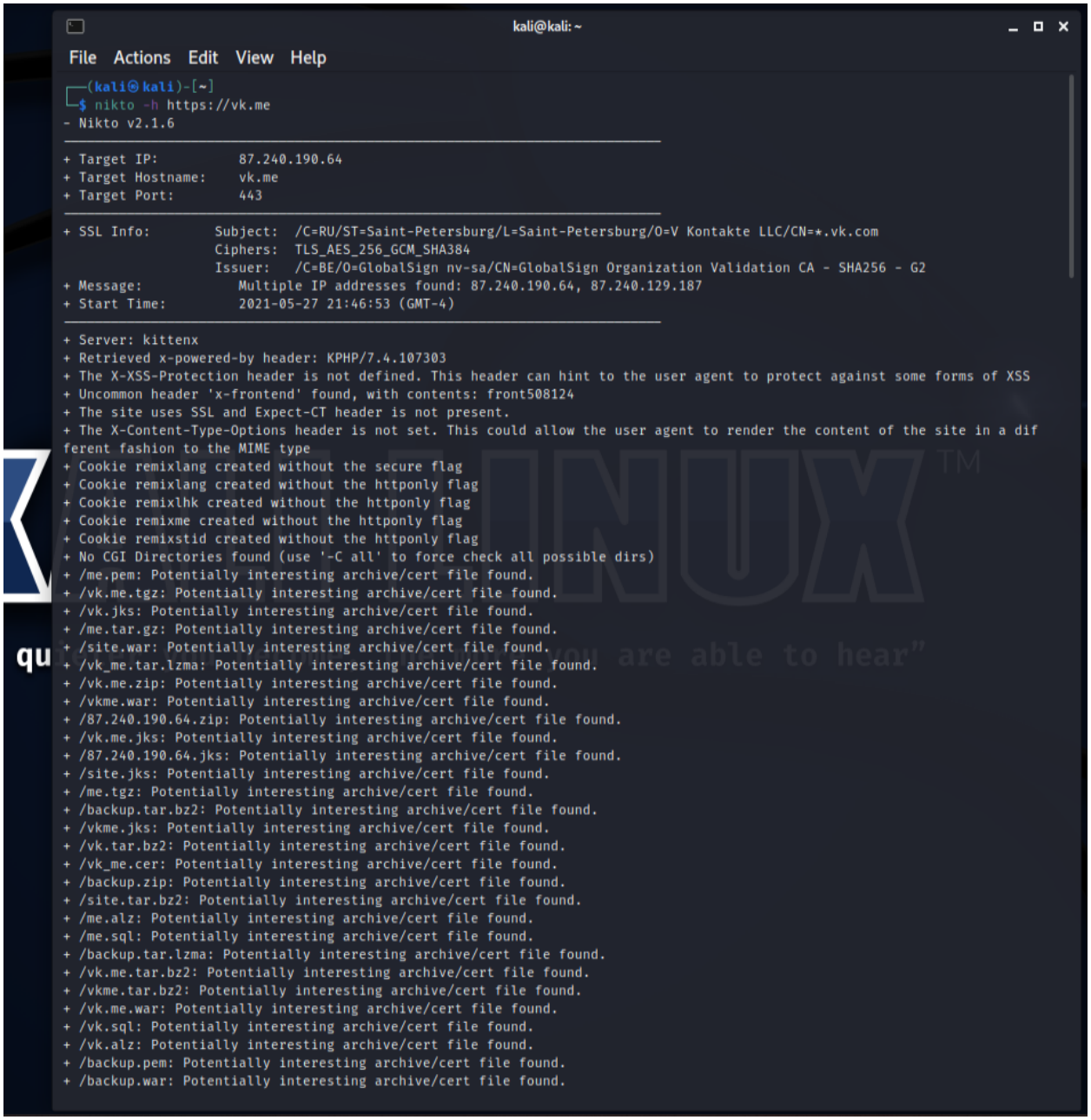
- https://vk.com



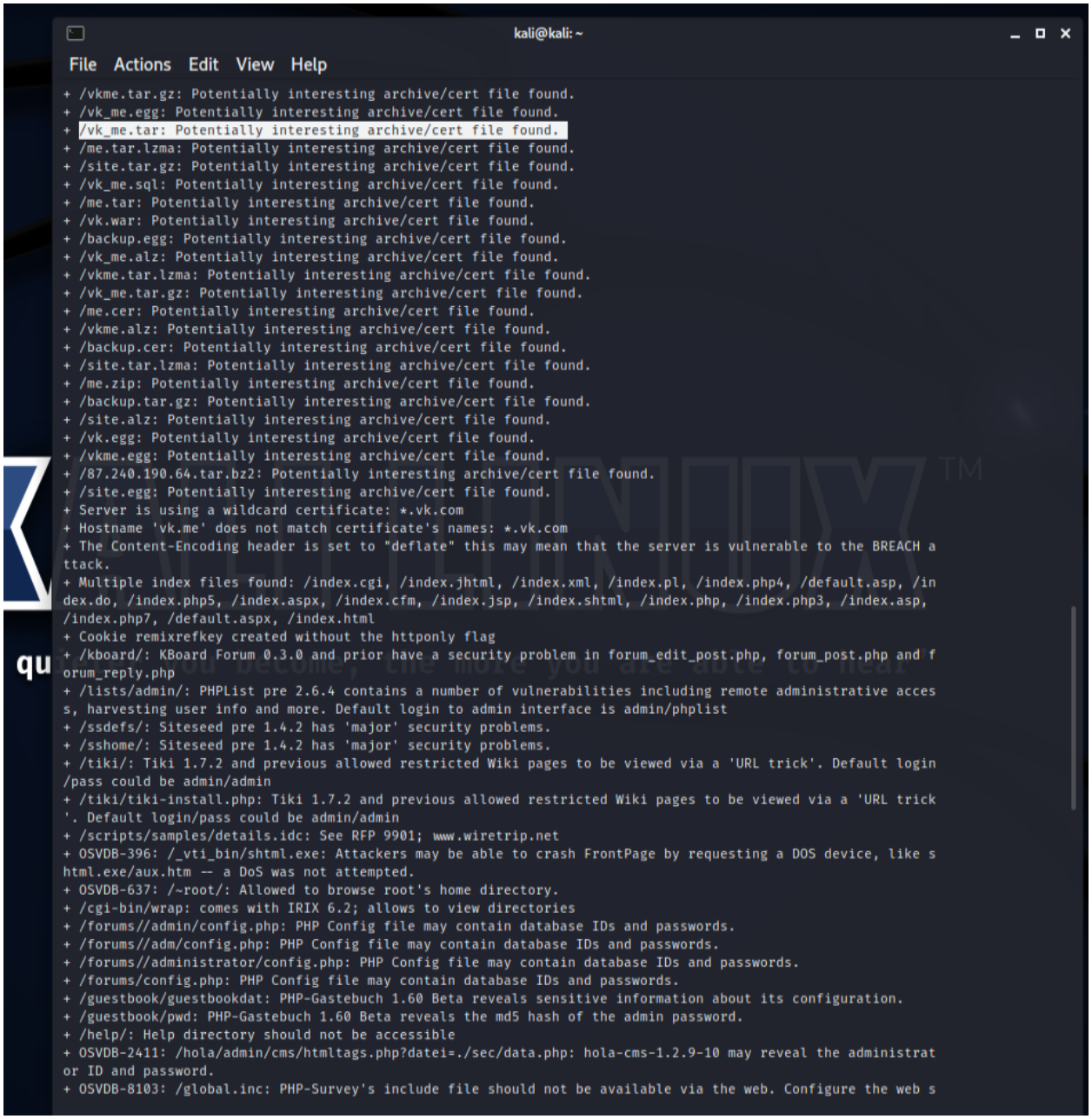
```
┌──(kali㉿kali)-[~]
└─$ nikto -h https://vk.com
- Nikto v2.1.6
---------------------------------------------------------------------------
^[[B^[[B^[[B+ Target IP:          87.240.190.67
+ Target Hostname:    vk.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=RU/ST=Saint-Petersburg/L=Saint-Petersburg/O=V Kontakte LLC/CN=*.vk.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validation CA - SHA256 - G2
+ Message:            Multiple IP addresses found: 87.240.190.67, 87.240.190.72, 93.186.225.208, 87.240.139.194, 87.240.190.78, 87.240.137.158
+ Start Time:         2021-05-27 19:26:05 (GMT-4)
---------------------------------------------------------------------------
+ Server: kittenx
+ Retrieved x-powered-by header: KPHP/7.4.107301
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-frontend' found, with contents: front224206
+ 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
+ Cookie remixlang created without the secure flag
+ Cookie remixlang created without the httponly flag
+ Root page / redirects to: https://m.vk.com/
+ All CGI directories 'found', use '-C none' to test none
+ Entry '/away.php' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/im?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Cookie remixstid created without the httponly flag
+ Entry '/call?id=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/groups?id=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/audio?performer=1&q=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/stats?gid=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Cookie remixlhk created without the httponly flag
+ Entry '/pages?oid=-/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/widget_auth.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/video_ext.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/login?*=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=search&q=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=coronavirus$/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=stayhome$/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/away.php' in robots.txt returned a non-forbidden or redirect HTTP code (302)
```


+ Cookie remixstid created without the httponly flag
+ Entry '/call?id=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/groups?id=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/audio?performer=1&q=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/stats?gid=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Cookie remixlhk created without the httponly flag
+ Entry '/pages?oid=-/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/widget_auth.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/video_ext.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/login?*=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=search&q=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=coronavirus$/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=stayhome$/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/away.php' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/im?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/call?id=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/groups?id=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/audio?performer=1&q=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/stats?gid=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/widget_auth.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/video_ext.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/login?*=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=search&q=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=coronavirus$/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=stayhome/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/away.php' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/im?/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/call?id=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/groups?id=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/audio?performer=1&q=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/stats?gid=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/pages?oid=-/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/widget_auth.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/video_ext.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/login?*=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=search&q=/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=coronavirus$/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/feed?section=stayhome$/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 196 entries which should be manually viewed.
+ /crossdomain.xml contains 2 lines which include the following domains: *.vk.com" to-ports="80 *.vk.com" to-ports="
+ Server is using a wildcard certificate: *.vk.com
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Cookie remixrefkey created without the httponly flag

- https://vk.me

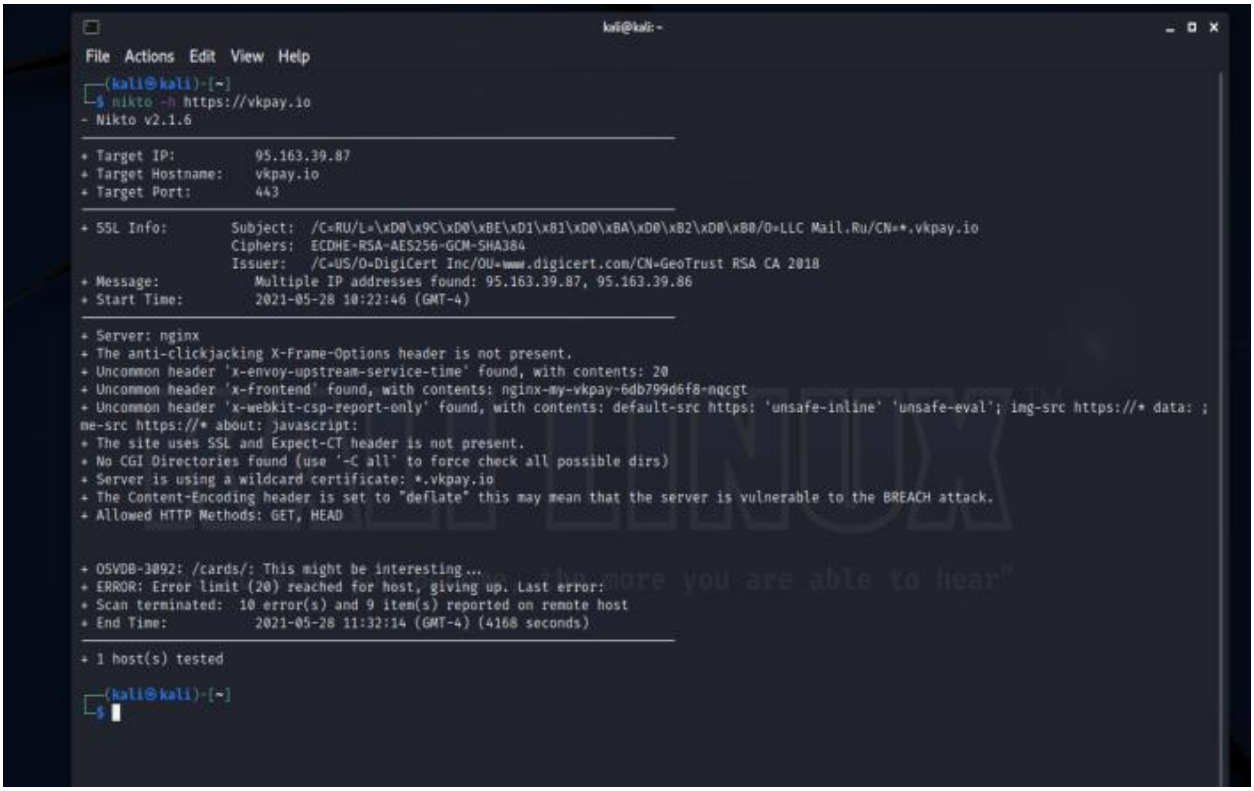

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nikto -h https://vk.me
- Nikto v2.1.6
+ Target IP: 87.240.190.64
+ Target Hostname: vk.me
+ Target Port: 443
+ SSL Info: Subject: /C=RU/ST=Saint-Petersburg/L=Saint-Petersburg/O=V Kontakte LLC/CN=*.vk.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validation CA - SHA256 - G2
+ Message: Multiple IP addresses found: 87.240.190.64, 87.240.129.187
+ Start Time: 2021-05-27 21:46:53 (GMT-4)
+ Server: kittenx
+ Retrieved x-powered-by header: KPHP/7.4.107303
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-frontend' found, with contents: front508124
+ 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 dif
ferent fashion to the MIME type
+ Cookie remixlang created without the secure flag
+ Cookie remixlang created without the httponly flag
+ Cookie remixlhk created without the httponly flag
+ Cookie remixme created without the httponly flag
+ Cookie remixstid created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /me.pem: Potentially interesting archive/cert file found.
+ /vk.me.tgz: Potentially interesting archive/cert file found.
+ /vk.jks: Potentially interesting archive/cert file found.
+ /me.tar.gz: Potentially interesting archive/cert file found.
+ /site.war: Potentially interesting archive/cert file found.
+ /vk_me.tar.lzma: Potentially interesting archive/cert file found.
+ /vk.me.zip: Potentially interesting archive/cert file found.
+ /vkme.war: Potentially interesting archive/cert file found.
+ /87.240.190.64.zip: Potentially interesting archive/cert file found.
+ /vk.me.jks: Potentially interesting archive/cert file found.
+ /87.240.190.64.jks: Potentially interesting archive/cert file found.
+ /site.jks: Potentially interesting archive/cert file found.
+ /me.tgz: Potentially interesting archive/cert file found.
+ /backup.tar.bz2: Potentially interesting archive/cert file found.
+ /vkme.jks: Potentially interesting archive/cert file found.
+ /vk.tar.bz2: Potentially interesting archive/cert file found.
+ /vk_me.cer: Potentially interesting archive/cert file found.
+ /backup.zip: Potentially interesting archive/cert file found.
+ /site.tar.bz2: Potentially interesting archive/cert file found.
+ /me.alz: Potentially interesting archive/cert file found.
+ /me.sql: Potentially interesting archive/cert file found.
+ /backup.tar.lzma: Potentially interesting archive/cert file found.
+ /vk.me.tar.bz2: Potentially interesting archive/cert file found.
+ /vkme.tar.bz2: Potentially interesting archive/cert file found.
+ /vk.me.war: Potentially interesting archive/cert file found.
+ /vk.sql: Potentially interesting archive/cert file found.
+ /vk.alz: Potentially interesting archive/cert file found.
+ /backup.pem: Potentially interesting archive/cert file found.
+ /backup.war: Potentially interesting archive/cert file found.


kali@kali: ~
File Actions Edit View Help
+ /backup.war: Potentially interesting archive/cert file found.
+ /vkme.pem: Potentially interesting archive/cert file found.
+ /site.pem: Potentially interesting archive/cert file found.
+ /vk_me.pem: Potentially interesting archive/cert file found.
+ /vkme.sql: Potentially interesting archive/cert file found.
+ /87.240.190.64.tar.gz: Potentially interesting archive/cert file found.
+ /vk.me.egg: Potentially interesting archive/cert file found.
+ /me.tar.bz2: Potentially interesting archive/cert file found.
+ /vkme.tgz: Potentially interesting archive/cert file found.
+ /site.sql: Potentially interesting archive/cert file found.
+ /vk.me.tar: Potentially interesting archive/cert file found.
+ /site.tgz: Potentially interesting archive/cert file found.
+ /vk.tgz: Potentially interesting archive/cert file found.
+ /vk.me.sql: Potentially interesting archive/cert file found.
+ /vk.me.tar.gz: Potentially interesting archive/cert file found.
+ /vk.me.alz: Potentially interesting archive/cert file found.
+ /backup.sql: Potentially interesting archive/cert file found.
+ /87.240.190.64.tar.lzma: Potentially interesting archive/cert file found.
+ /vk.pem: Potentially interesting archive/cert file found.
+ /me.jks: Potentially interesting archive/cert file found.
+ /vk.tar.gz: Potentially interesting archive/cert file found.
+ /backup.tgz: Potentially interesting archive/cert file found.
+ /87.240.190.64.sql: Potentially interesting archive/cert file found.
+ /site.cer: Potentially interesting archive/cert file found.
+ /87.240.190.64.war: Potentially interesting archive/cert file found.
+ /87.240.190.64.tar: Potentially interesting archive/cert file found.
+ /backup.alz: Potentially interesting archive/cert file found.
+ /vkme.cer: Potentially interesting archive/cert file found.
+ /vk_me.jks: Potentially interesting archive/cert file found.
+ /me.egg: Potentially interesting archive/cert file found.
+ /vk_me.tgz: Potentially interesting archive/cert file found.
+ /site.tar: Potentially interesting archive/cert file found.
+ /87.240.190.64.tgz: Potentially interesting archive/cert file found.
+ /vk.zip: Potentially interesting archive/cert file found.
+ /vkme.zip: Potentially interesting archive/cert file found.
+ /vkme.tar: Potentially interesting archive/cert file found.
+ /vk.me.tar.lzma: Potentially interesting archive/cert file found.
+ /vk.cer: Potentially interesting archive/cert file found.
+ /vk_me.zip: Potentially interesting archive/cert file found.
+ /site.zip: Potentially interesting archive/cert file found.
+ /vk.tar: Potentially interesting archive/cert file found.
+ /me.war: Potentially interesting archive/cert file found.
+ /87.240.190.64.egg: Potentially interesting archive/cert file found.
+ /vk_me.tar.bz2: Potentially interesting archive/cert file found.
+ /vk_me.war: Potentially interesting archive/cert file found.
+ /87.240.190.64.alz: Potentially interesting archive/cert file found.
+ /vk.tar.lzma: Potentially interesting archive/cert file found.
+ /backup.tar: Potentially interesting archive/cert file found.
+ /87.240.190.64.pem: Potentially interesting archive/cert file found.
+ /87.240.190.64.cer: Potentially interesting archive/cert file found.
+ /vk.me.cer: Potentially interesting archive/cert file found.
+ /vk.me.pem: Potentially interesting archive/cert file found.
+ /backup.jks: Potentially interesting archive/cert file found.
+ /vkme.tar.gz: Potentially interesting archive/cert file found.
+ /vk_me.egg: Potentially interesting archive/cert file found.
+ /vk_me.tar: Potentially interesting archive/cert file found.


kali@kali: ~
File Actions Edit View Help
+ /vkme.tar.gz: Potentially interesting archive/cert file found.
+ /vk_me.egg: Potentially interesting archive/cert file found.
+ /vk_me.tar: Potentially interesting archive/cert file found.
+ /me.tar.lzma: Potentially interesting archive/cert file found.
+ /site.tar.gz: Potentially interesting archive/cert file found.
+ /vk_me.sql: Potentially interesting archive/cert file found.
+ /me.tar: Potentially interesting archive/cert file found.
+ /vk.war: Potentially interesting archive/cert file found.
+ /backup.egg: Potentially interesting archive/cert file found.
+ /vk_me.alz: Potentially interesting archive/cert file found.
+ /vkme.tar.lzma: Potentially interesting archive/cert file found.
+ /vk_me.tar.gz: Potentially interesting archive/cert file found.
+ /me.cer: Potentially interesting archive/cert file found.
+ /vkme.alz: Potentially interesting archive/cert file found.
+ /backup.cer: Potentially interesting archive/cert file found.
+ /site.tar.lzma: Potentially interesting archive/cert file found.
+ /me.zip: Potentially interesting archive/cert file found.
+ /backup.tar.gz: Potentially interesting archive/cert file found.
+ /site.alz: Potentially interesting archive/cert file found.
+ /vk.egg: Potentially interesting archive/cert file found.
+ /vkme.egg: Potentially interesting archive/cert file found.
+ /87.240.190.64.tar.bz2: Potentially interesting archive/cert file found.
+ /site.egg: Potentially interesting archive/cert file found.
+ Server is using a wildcard certificate: *.vk.com
+ Hostname 'vk.me' does not match certificate's names: *.vk.com
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Multiple index files found: /index.cgi, /index.jhtml, /index.xml, /index.pl, /index.php4, /default.asp, /index.do, /index.php5, /index.aspx, /index.cfm, /index.jsp, /index.shtml, /index.php, /index.php3, /index.asp, /index.php7, /default.aspx, /index.html
+ Cookie remixrefkey created without the httponly flag
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phplist
+ /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /scripts/samples/details.idc: See RFP 9901; www.wiretrip.net
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted.
+ OSVDB-637: /~root/: Allowed to browse root's home directory.
+ /cgi-bin/wrap: comes with IRIX 6.2; allows to view directories
+ /forums//admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//adm/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//administrator/config.php: PHP Config file may contain database IDs and passwords.
+ /forums/config.php: PHP Config file may contain database IDs and passwords.
+ /guestbook/guestbookdat: PHP-Gastebuch 1.60 Beta reveals sensitive information about its configuration.
+ /guestbook/pwd: PHP-Gastebuch 1.60 Beta reveals the md5 hash of the admin password.
+ /help/: Help directory should not be accessible
+ OSVDB-2411: /hola/admin/cms/htmltags.php?datei=./sec/data.php: hola-cms-1.2.9-10 may reveal the administrator ID and password.
+ OSVDB-8103: /global.inc: PHP-Survey's include file should not be available via the web. Configure the web s

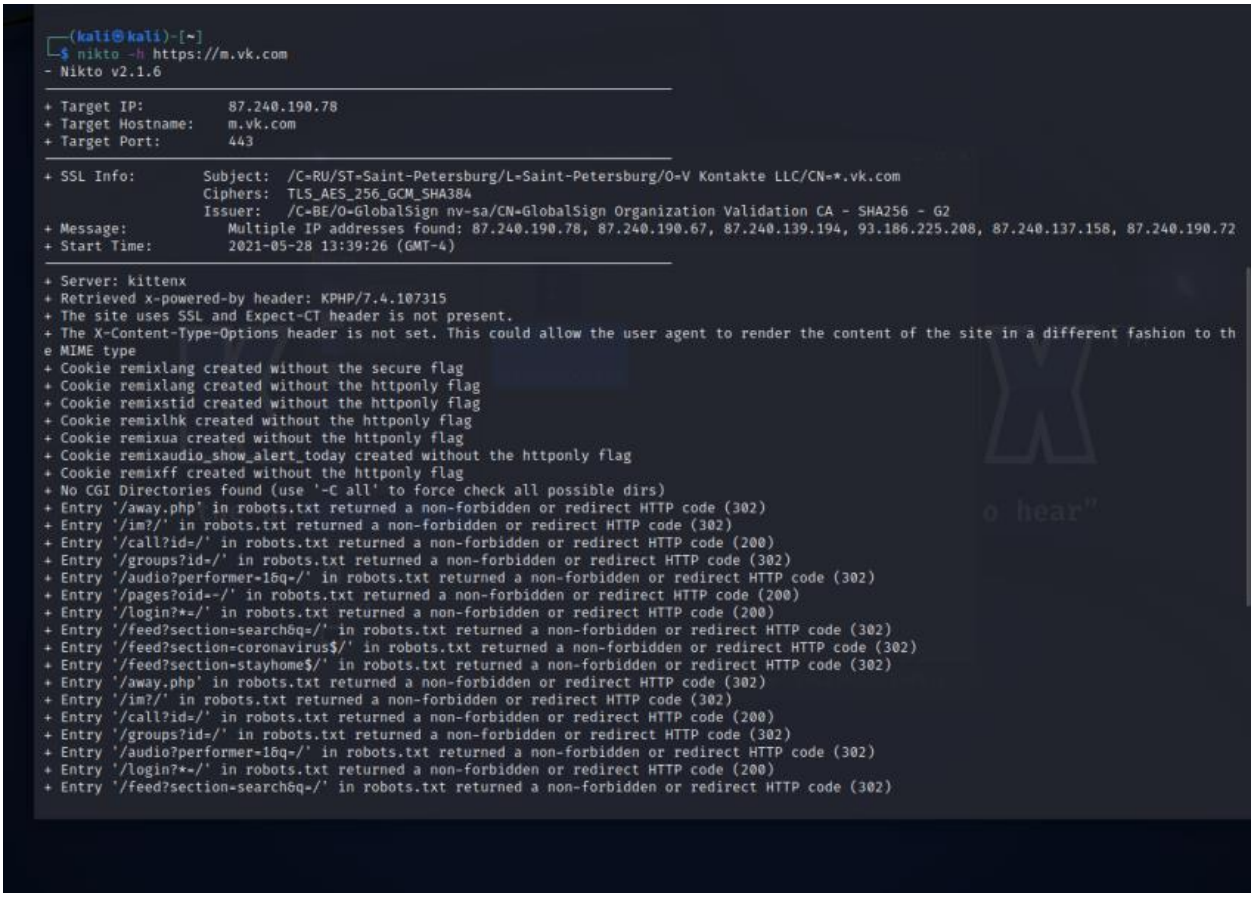

kali@kali: ~
File Actions Edit View Help
+ OSVDB-2411: /hola/admin/cms/htmltags.php?datei=./sec/data.php: hola-cms-1.2.9-10 may reveal the administrator ID and password.
+ OSVDB-8103: /global.inc: PHP-Survey's include file should not be available via the web. Configure the web server to ignore .inc files or change this to global.inc.php
+ OSVDB-59620: /inc/common.load.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
+ OSVDB-59619: /inc/config.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
+ OSVDB-59618: /inc/dbase.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
+ OSVDB-2703: /geeklog/users.php: Geeklog prior to 1.3.8-1sr2 contains a SQL injection vulnerability that lets a remote attacker reset admin password.
+ OSVDB-8204: /gb/index.php?login=true: gBook may allow admin login by setting the value 'login' equal to 'true'.
+ /guestbook/admin.php: Guestbook admin page available without authentication.
+ /getaccess: This may be an indication that the server is running getAccess for SSO
+ /cfdocs/expeval/openfile.cfm: Can use to expose the system/server path.
+ /tsweb/: Microsoft TSAC found. http://www.dslwebserver.com/main/fr_index.html?/main/sbs-Terminal-Services-Advanced-Client-Configuration.html
+ /vgn/performance/TMT: Vignette CMS admin/maintenance script available.
+ /vgn/performance/TMT/Report: Vignette CMS admin/maintenance script available.
+ /vgn/performance/TMT/Report/XML: Vignette CMS admin/maintenance script available.
+ /vgn/performance/TMT/reset: Vignette CMS admin/maintenance script available.
+ /vgn/ppstats: Vignette CMS admin/maintenance script available.
+ /vgn/previewer: Vignette CMS admin/maintenance script available.
+ /vgn/record/previewer: Vignette CMS admin/maintenance script available.
+ /vgn/stylepreviewer: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Deleting: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Editing: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Saving: Vignette CMS admin/maintenance script available.
+ /vgn/vr/Select: Vignette CMS admin/maintenance script available.
+ /scripts/iisadmin/bdir.htr: This default script shows host info, may allow file browsing and buffer a overrun in the Chunked Encoding data transfer mechanism, request /scripts/iisadmin/bdir.htr??c:\<dirs> . https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/MS02-028. http://www.cert.org/advisories/CA-2002-09.html.
+ /scripts/iisadmin/ism.dll: Allows you to mount a brute force attack on passwords
+ /scripts/tools/ctss.idc: This CGI allows remote users to view and modify SQL DB contents, server paths, doc root and more.
+ /bigconf.cgi: BigIP Configuration CGI
+ /wp-content/plugins/nextgen-gallery/products/photocrati_nextgen/modules/nextgen_addgallery_page/static/jquery.filetree/connectors/jqueryFileTree.php: NextGEN Gallery LFI, see https://security.dxw.com/advisories/directory-traversal-in-nextgen-gallery-2-0-0/
+ /wordpresswp-content/plugins/nextgen-gallery/products/photocrati_nextgen/modules/nextgen_addgallery_page/static/jquery.filetree/connectors/jqueryFileTree.php: NextGEN Gallery LFI, see https://security.dxw.com/advisories/directory-traversal-in-nextgen-gallery-2-0-0/
+ 7792 requests: 1 error(s) and 165 item(s) reported on remote host
+ End Time: 2021-05-27 23:48:48 (GMT-4) (7315 seconds)
+ 1 host(s) tested
(kali㉿kali)-[~]
$

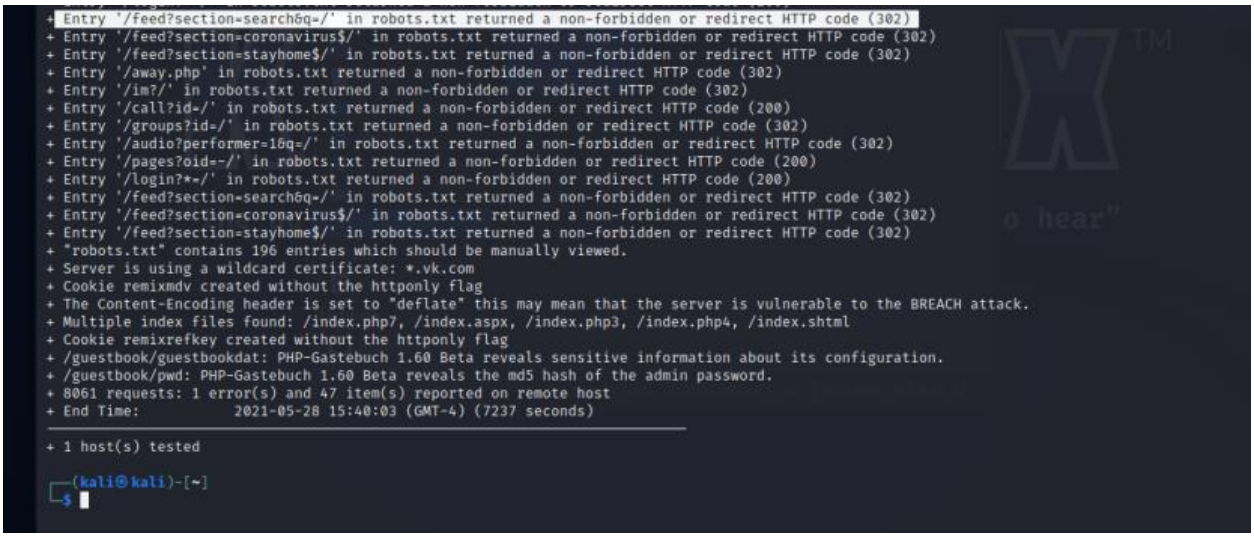
- https://vkpay.io



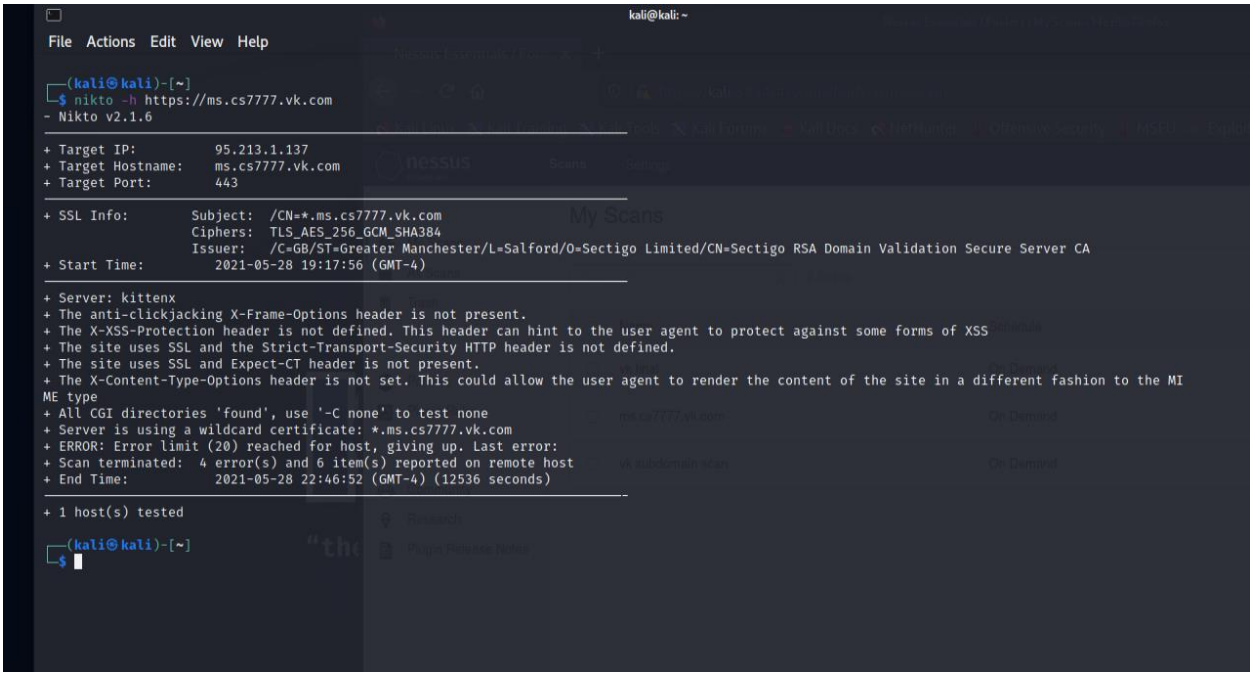
- https://connect.vk.com

- https://m.vk.com





- https://ms.cs7777.vk.com

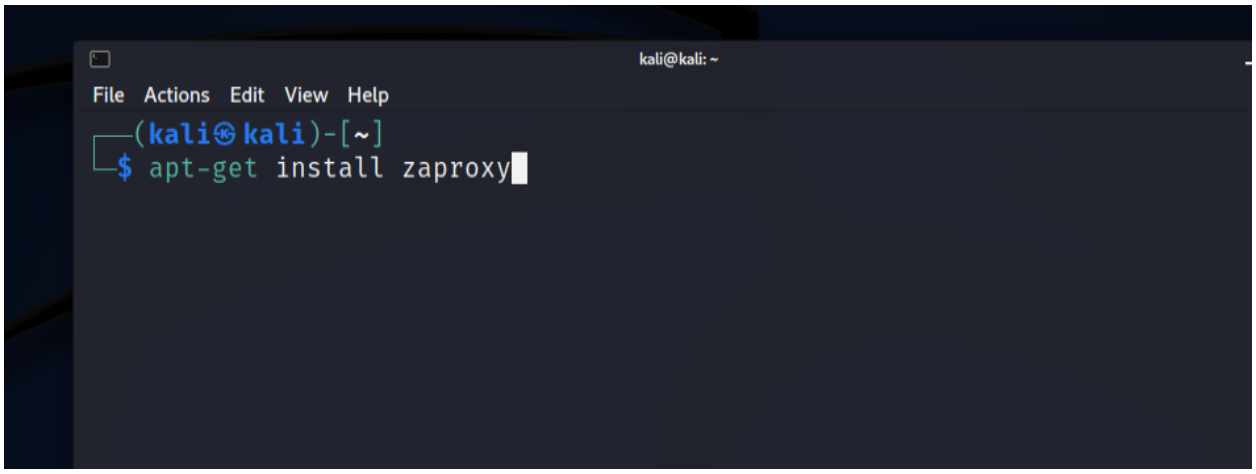


OWASP ZAP

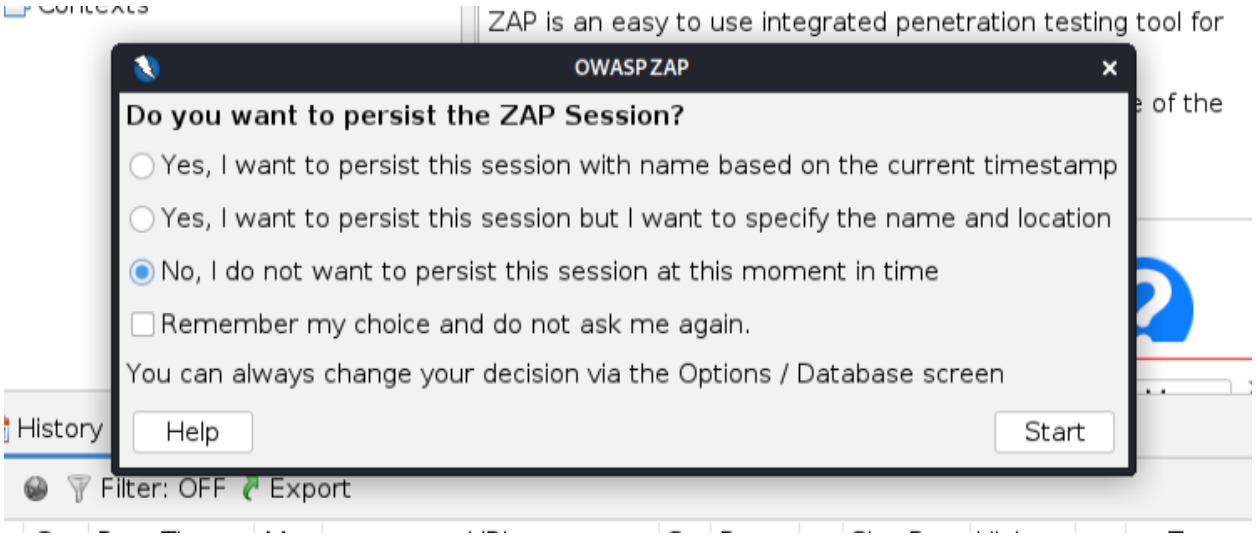
Under the auspices of the Open Web Application Security Project, Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool (OWASP). ZAP is a web application testing framework that is both flexible and extendable.

ZAP is a so-called "man-in-the-middle proxy" at its core. It sits between the tester's browser and the web application, intercepting and inspecting messages transmitted between the two, modifying the contents if necessary, and then forwarding those packets on to their intended destination. It can be run as a standalone program or as a daemon process. [12]

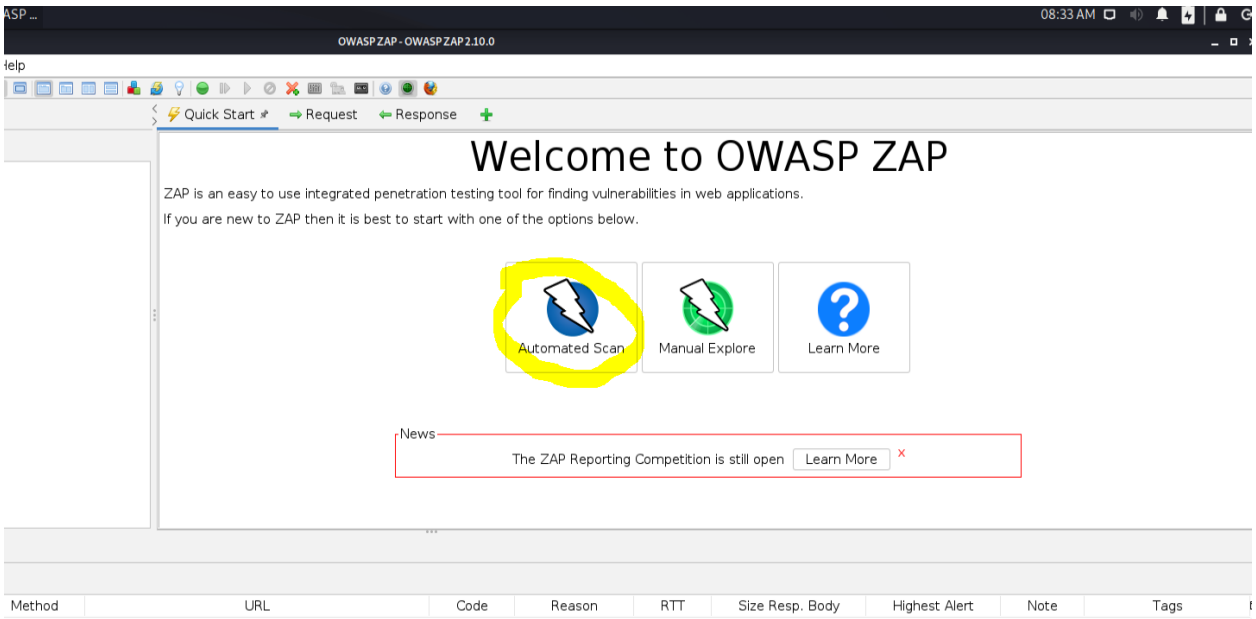
- **Installation**



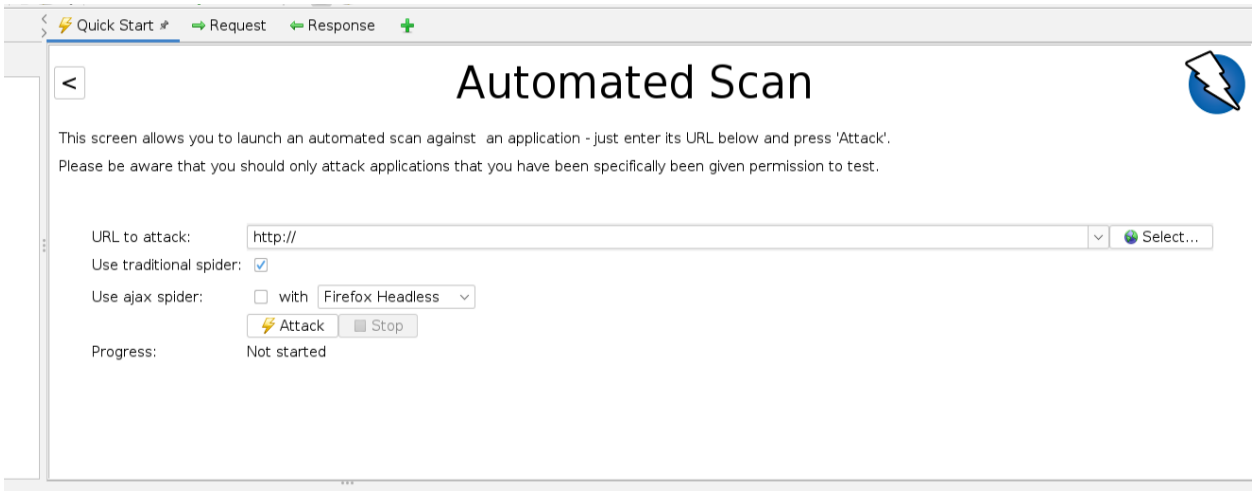
- **After installation open the tool bar you will able to see it.**



- **Click on the automated scan button**

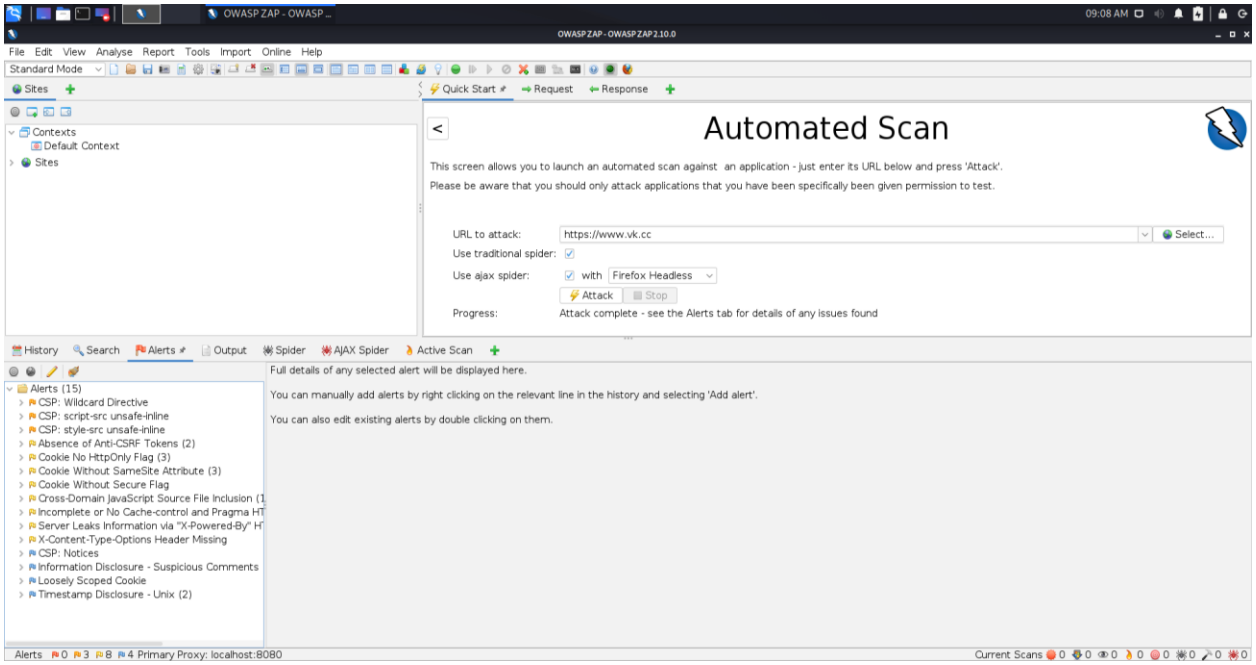


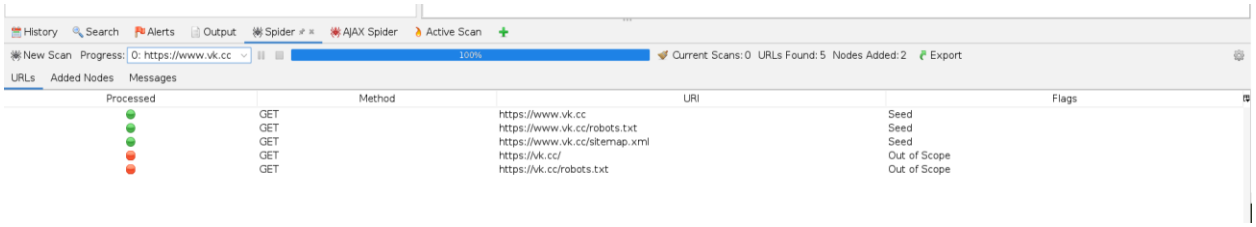
- **In the url box enter the full url of the web site that you want to attack and click the attack.**

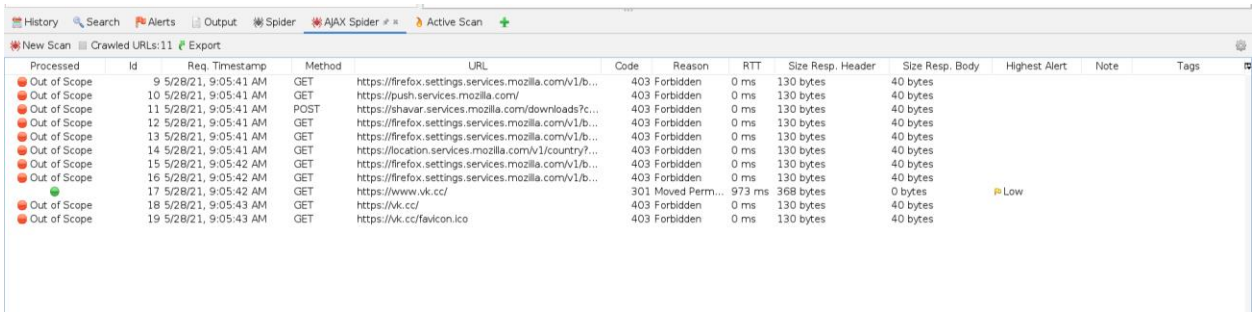


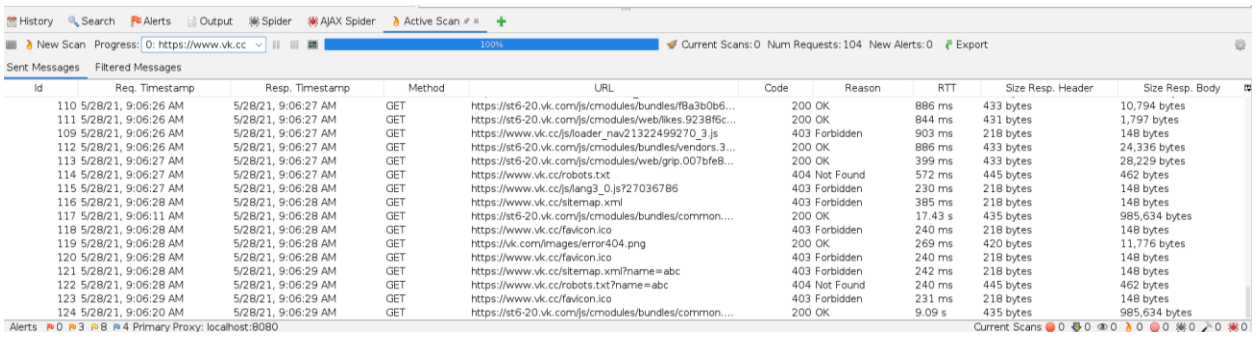
ZAP will then use its spider to crawl the web application and passively scan each page it discovers. The active scanner will then be used by ZAP to attack all of the pages, functionality, and parameters that have been found. You can use any or both of the spiders provided by ZAP to crawl web applications from this screen. The classic ZAP spider, which finds links by inspecting the HTML of web application responses. This spider is quick, but it isn't always successful when researching an AJAX web application that uses JavaScript to produce links.

- https://www.vk.cc







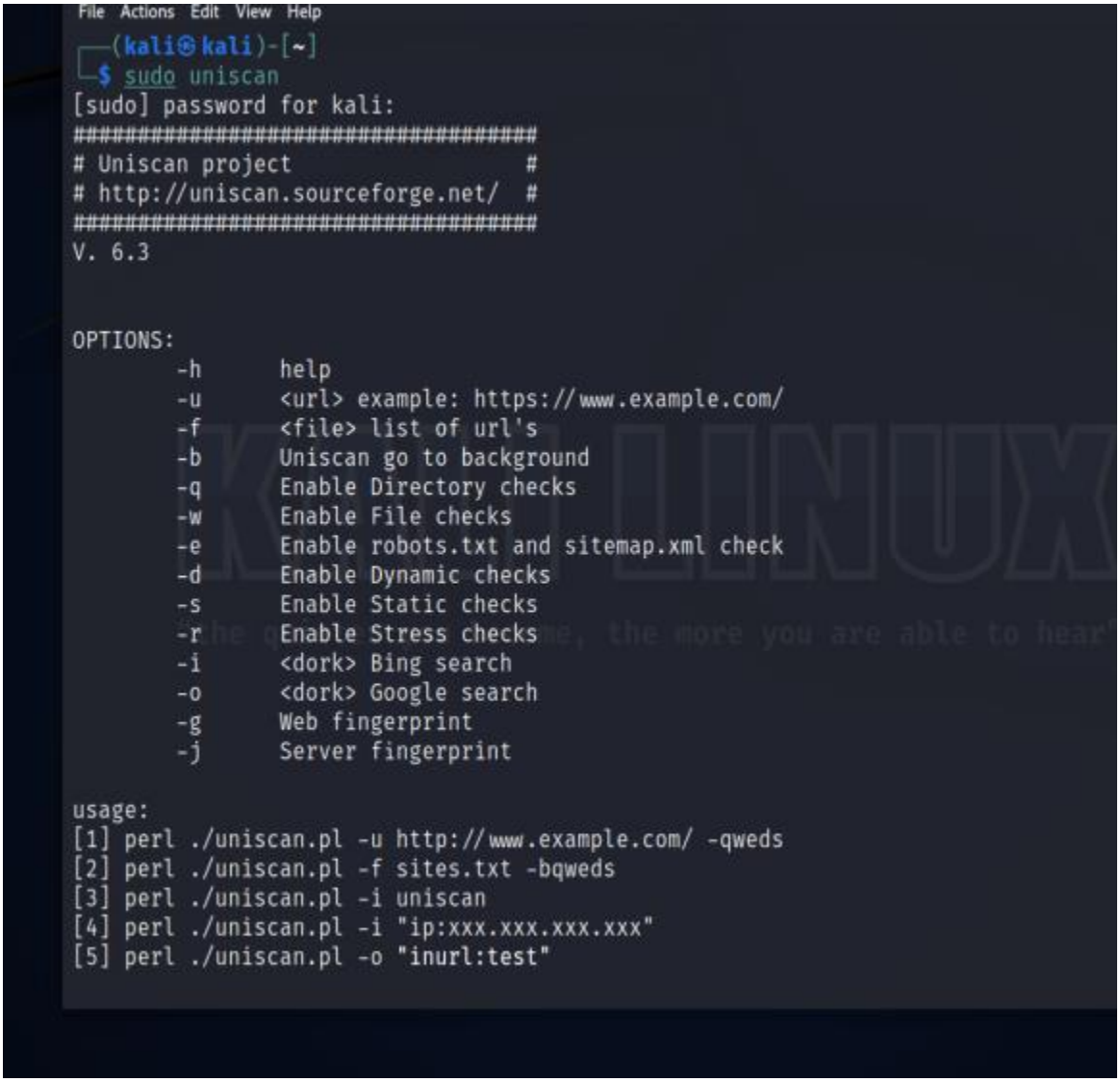


Uniscan

Uniscan is an open source program that can scan web applications for significant vulnerabilities like sql injection, blind sql injection, cross site scripting, remote file inclusion, web shell vulnerabilities, and hidden backdoors. Uniscan can search Bing and Google for websites on shared IP addresses in addition to vulnerability evaluation. [13]

Installation:

- **First run uniscan by command “sudo uniscan”**



- https://vk.link

HTML report saved in: report/vk.link.html

SCAN TIME

Scan Started: 28/5/2021 9:53:40

TARGET

Domain https://vk.link/

Server Banner: kittenx

Target IP: 87.240.190.64

CRAWLING

Directory check:
Skipped because https://vk.link/uniscan57/ did not return the code 404

File check:
Skipped because https://vk.link/uniscan107/ did not return the code 404

Check robots.txt:

Check sitemap.xml:

Crawling finished, found: 7 URL's

Timthumb:

Source Code Disclosure:

FCKeditor File Upload:

File Upload Forms:

PHPinfo() Disclosure:

External hosts:
https://www.googletagmanager.com

E-mails:

Web Backdoors:

Ignored Files:

DYNAMIC TESTS

Learning New Directories: 1 New directories added.

FCKeditor tests:
Skipped because https://vk.link/css/al/testing123 did not return the code 404

Timthumb < 1.33 vulnerability:

Backup Files:
Skipped because https://vk.link/css/al/testing123 did not return the code 404

Blind SQL Injection:

Local File Include:

PHP CGI Argument Injection:

Remote Command Execution:

Remote File Include:

SQL Injection:

Cross-Site Scripting (XSS):

Web Shell Finder:

STATIC TESTS

Local File Include:

Remote Command Execution:

Remote File Include:

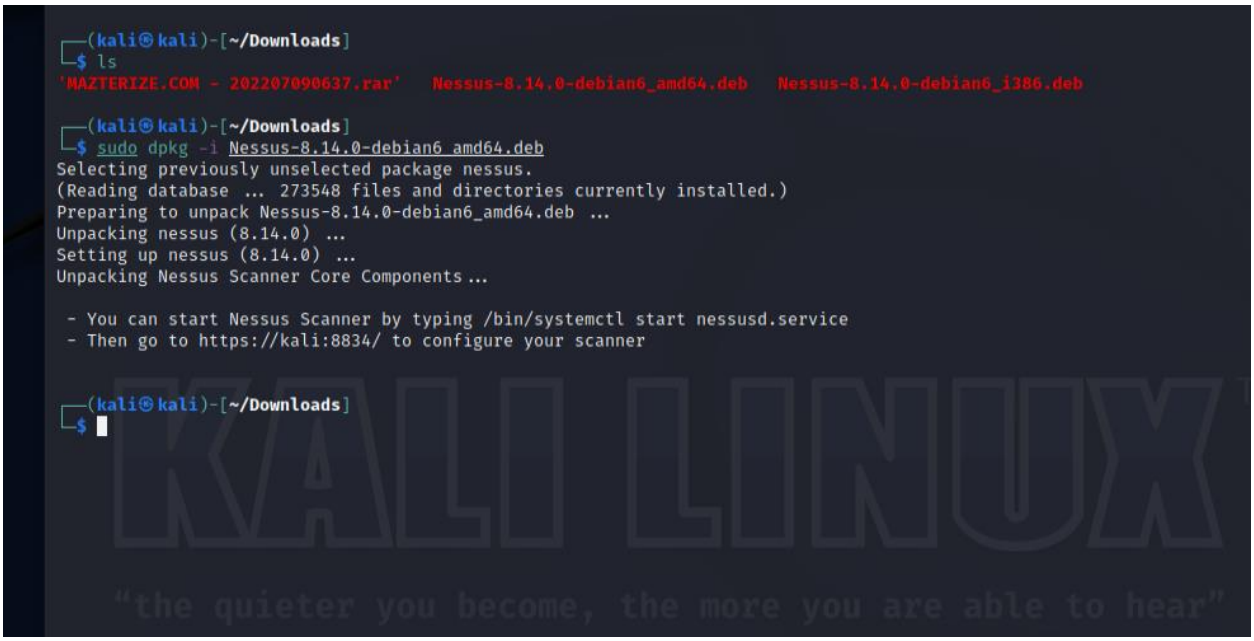
SCAN TIME

Scan Finished: 28/5/2021 9:58:36

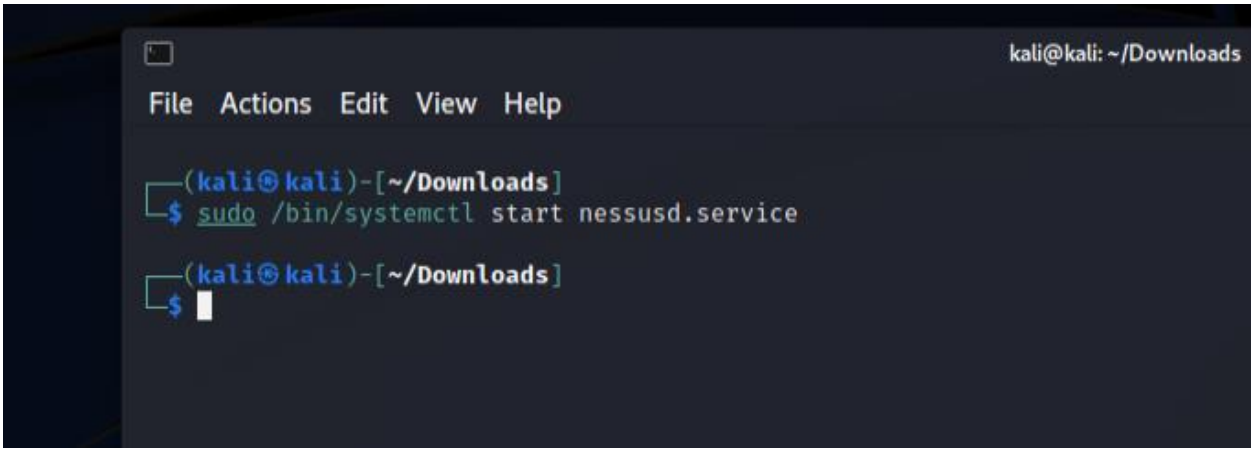
Nessus

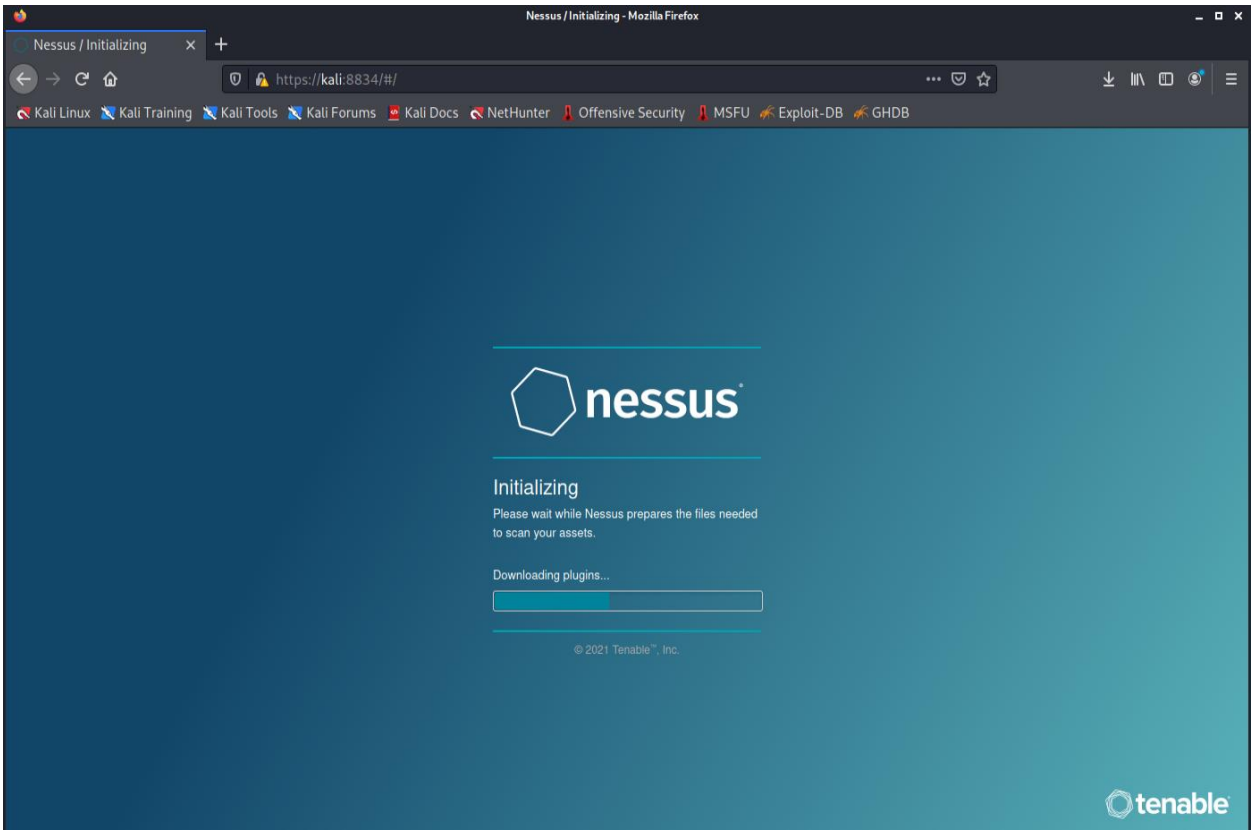
Nessus is a remote security scanning application that examines a computer and sends out an alert if it finds any vulnerabilities that malevolent hackers could exploit to obtain access to any computer on your network. [14]

- Download Nessus using https://www.tenable.com/products/nessus/nessus-essentials and install it to your kali machine.



- Then start Nessus service and go to https://kali:8834/ link using your browser.

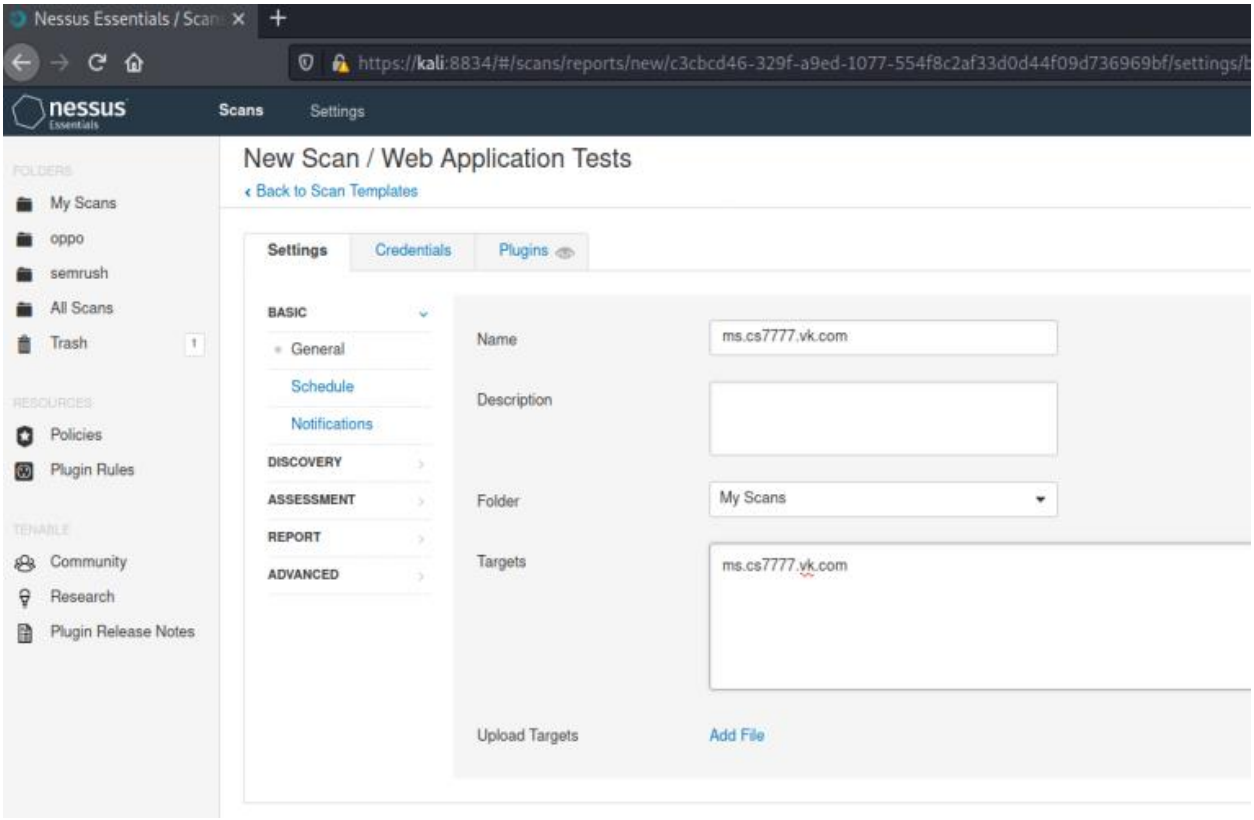




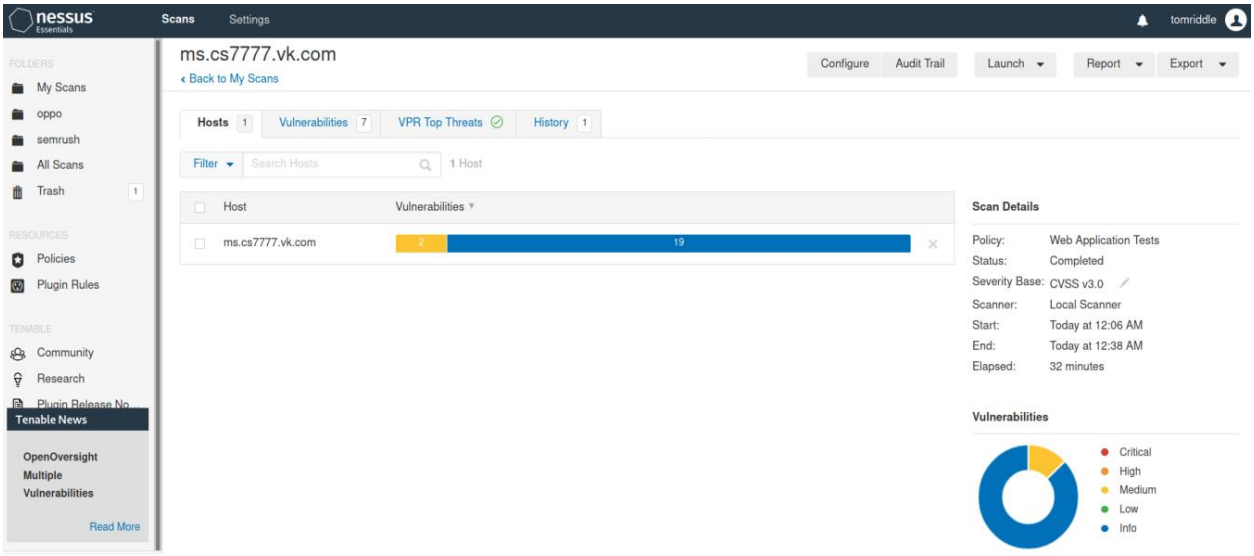
- https://ms.cs7777.vk.com

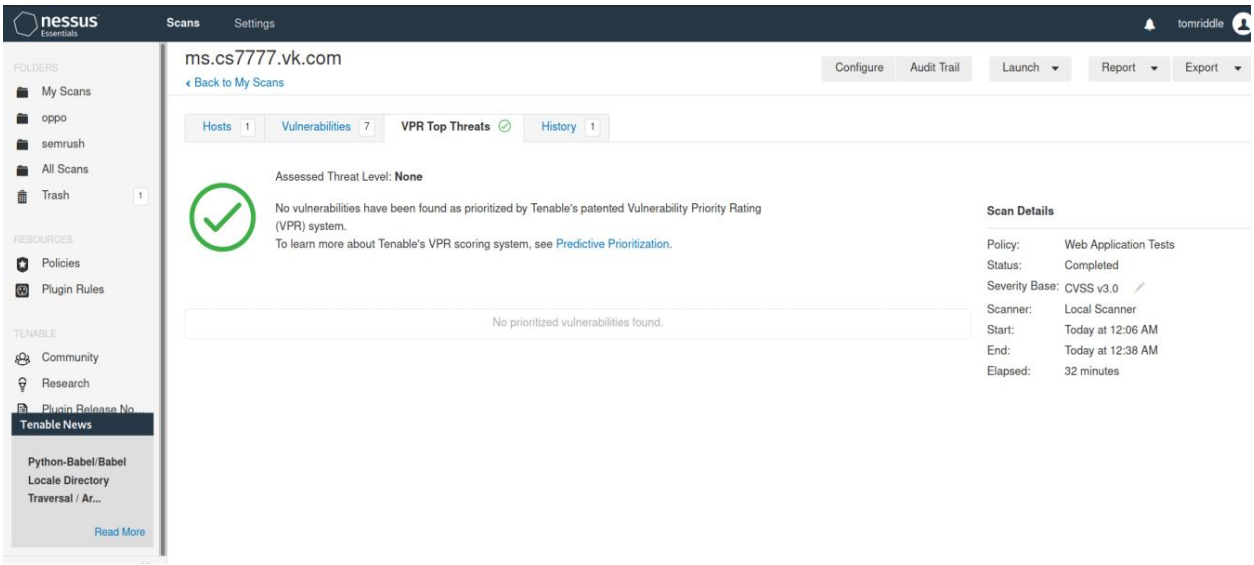
Add new scan > web application tests >

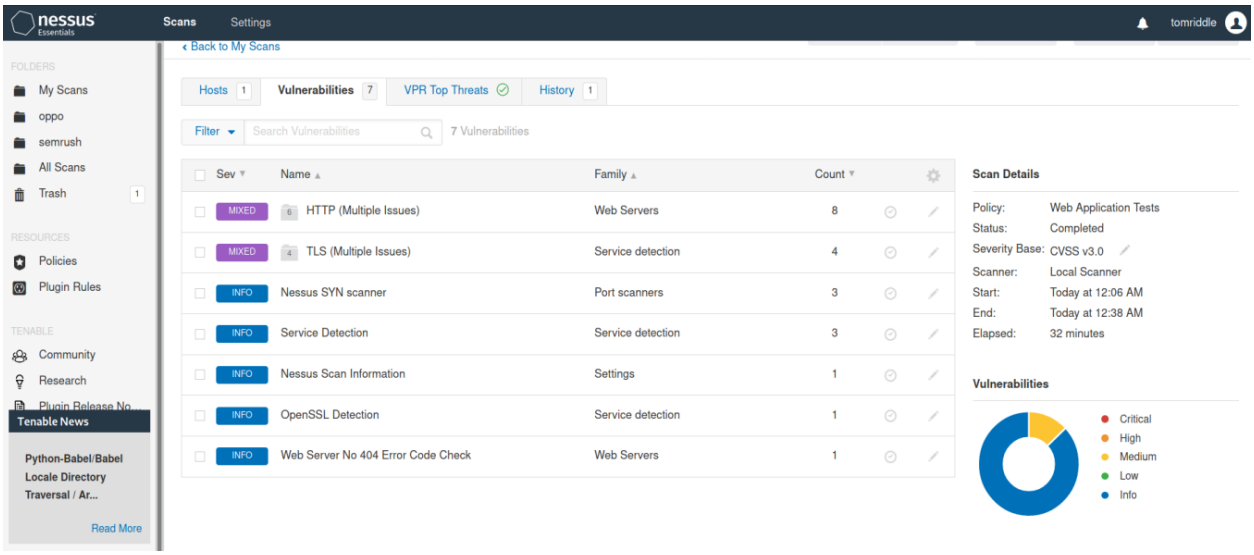
Then save your name and target web address and run it.

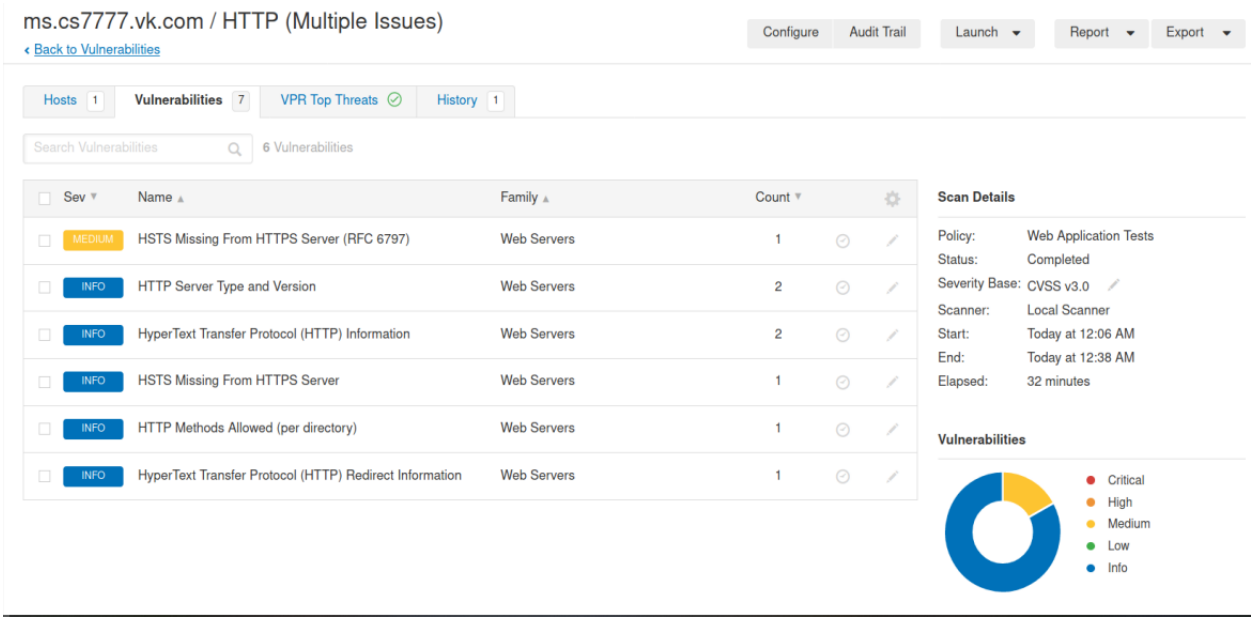


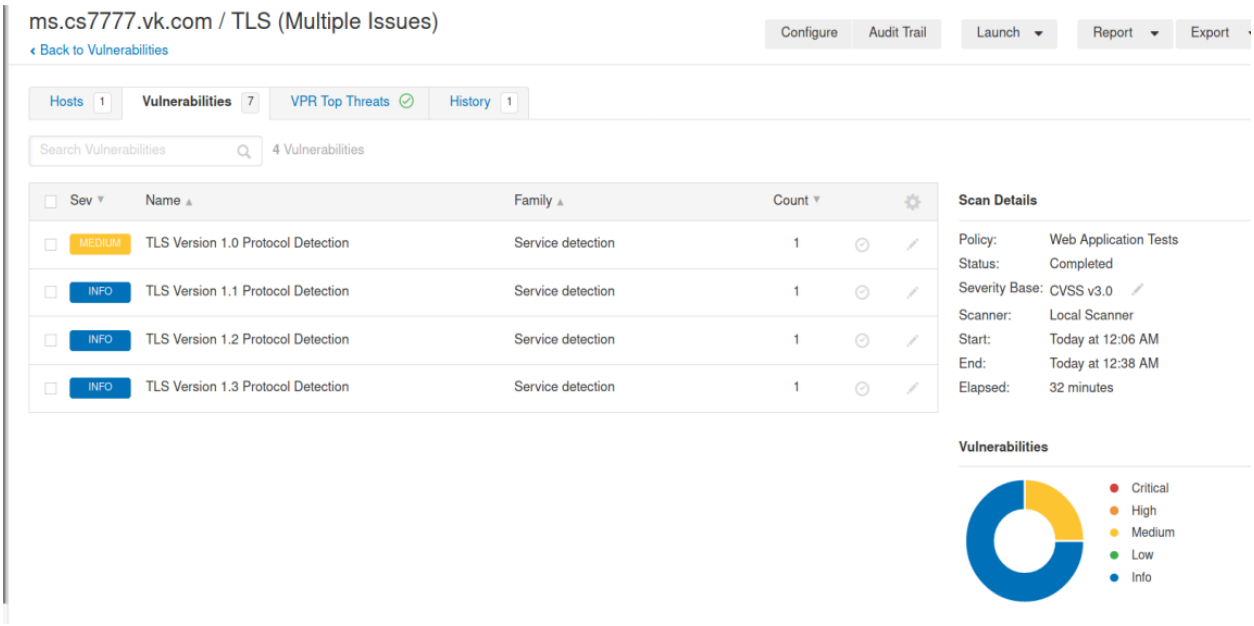
Proof (after web application test complete)



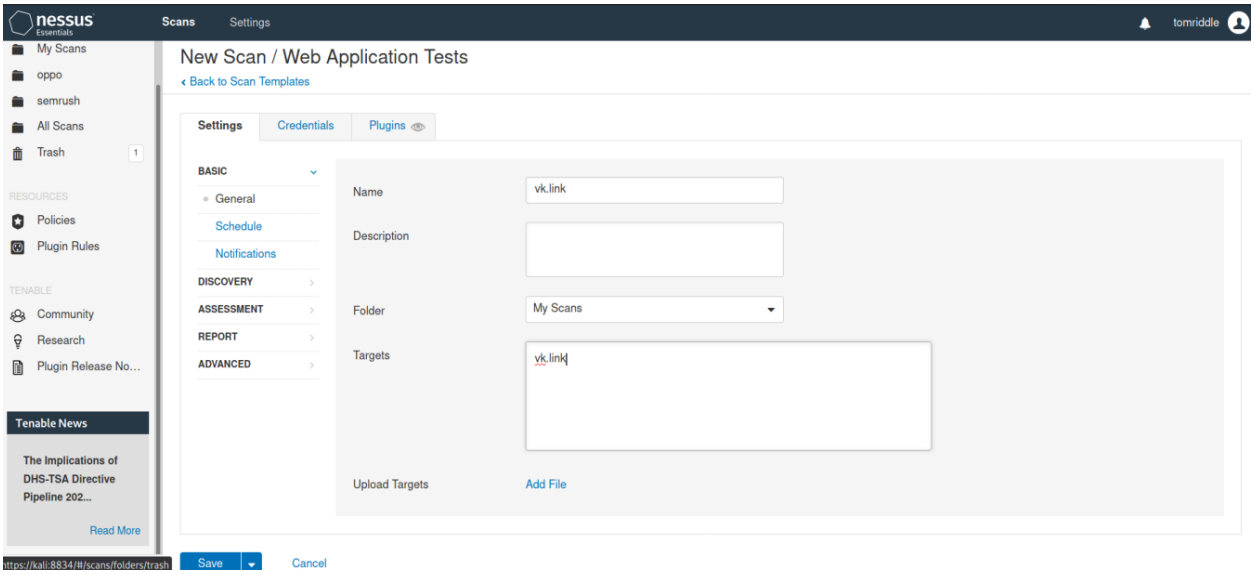


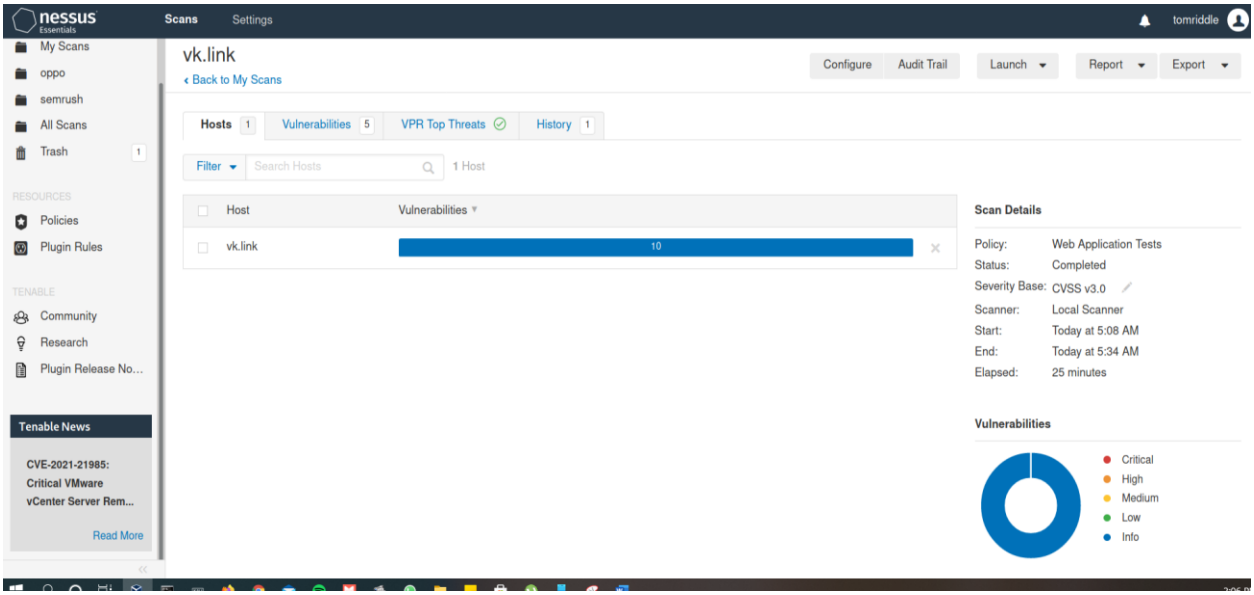

nessus
Essentials
Scans
Settings
tomriddle
FOLDERS
My Scans
oppo
semrush
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Tenable News
Python-Babel/Babel Locale Directory Traversal / Ar...
Read More
Back to My Scans
Hosts 1
Vulnerabilities 7
VPR Top Threats
History 1
Filter
Search Vulnerabilities
7 Vulnerabilities
Sev
Name
Family
Count
MIXED HTTP (Multiple Issues) Web Servers 8
MIXED TLS (Multiple Issues) Service detection 4
INFO Nessus SYN scanner Port scanners 3
INFO Service Detection Service detection 3
INFO Nessus Scan Information Settings 1
INFO OpenSSL Detection Service detection 1
INFO Web Server No 404 Error Code Check Web Servers 1
Scan Details
Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:06 AM
End: Today at 12:38 AM
Elapsed: 32 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

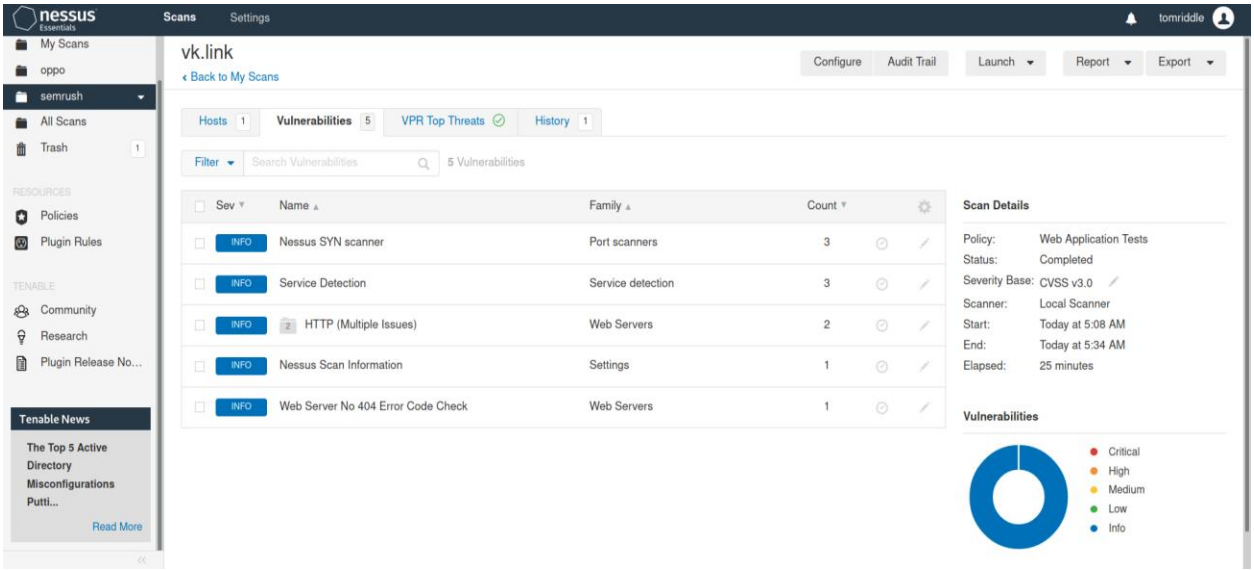

ms.cs7777.vk.com / HTTP (Multiple Issues)
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 7
VPR Top Threats
History 1
Search Vulnerabilities
6 Vulnerabilities
Sev
Name
Family
Count
MEDIUM HSTS Missing From HTTPS Server (RFC 6797) Web Servers 1
INFO HTTP Server Type and Version Web Servers 2
INFO HyperText Transfer Protocol (HTTP) Information Web Servers 2
INFO HSTS Missing From HTTPS Server Web Servers 1
INFO HTTP Methods Allowed (per directory) Web Servers 1
INFO HyperText Transfer Protocol (HTTP) Redirect Information Web Servers 1
Scan Details
Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:06 AM
End: Today at 12:38 AM
Elapsed: 32 minutes
Vulnerabilities
Critical
High
Medium
Low
Info



- https://vk.link







Here I found only some informational vulnerabilities so I'm not going to attach screenshots of those.

Fingerprinting

A fingerprint is a collection of data that can be used to identify software, network protocols, operating systems, and hardware. Fingerprinting, also known as Footprinting, is the process of correlating data sets to identify network services, operating system numbers and versions, software programs, databases, and configurations, among other things.

There are 2 main types of fingerprinting, they are passive and active. Active fingerprinting consists of sending packets to the target and wait for it to reply then analyzing the response. Passive fingerprinting consists of monitoring the target's network traffic without any direct involvements. [12]

Tools use for fingerprinting

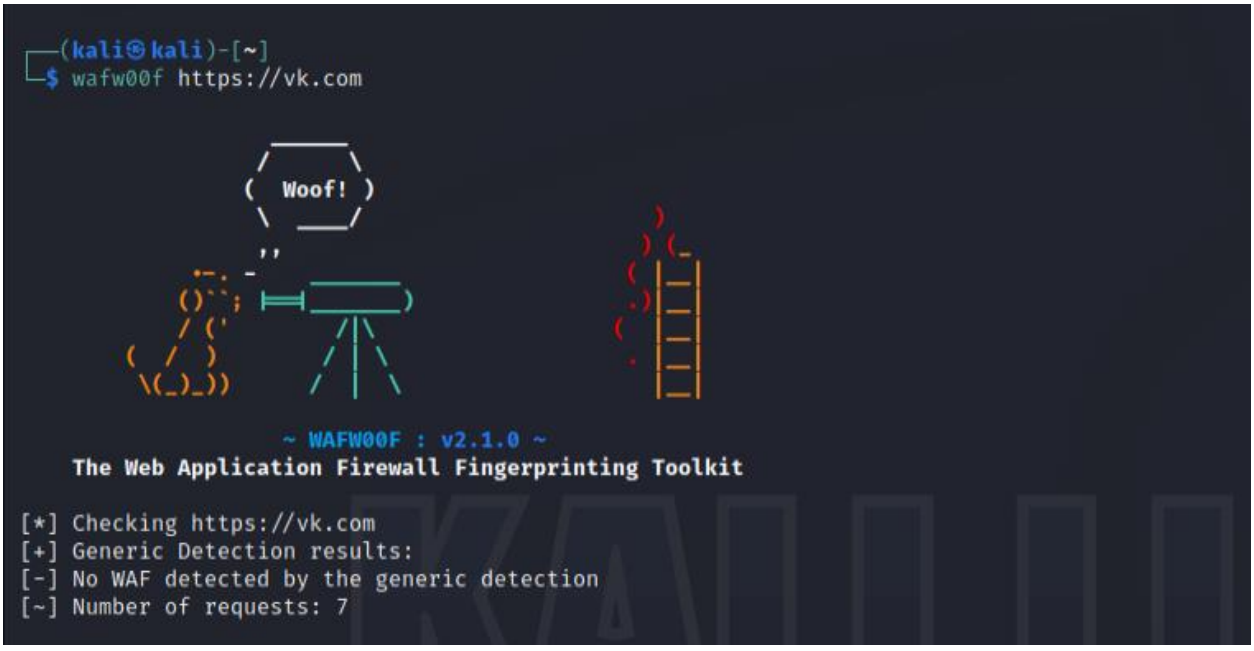
- Nmap
- Ettercap
- Wafw00f
- PacketFence
- Netcat

Finding the target domain has firewall protection

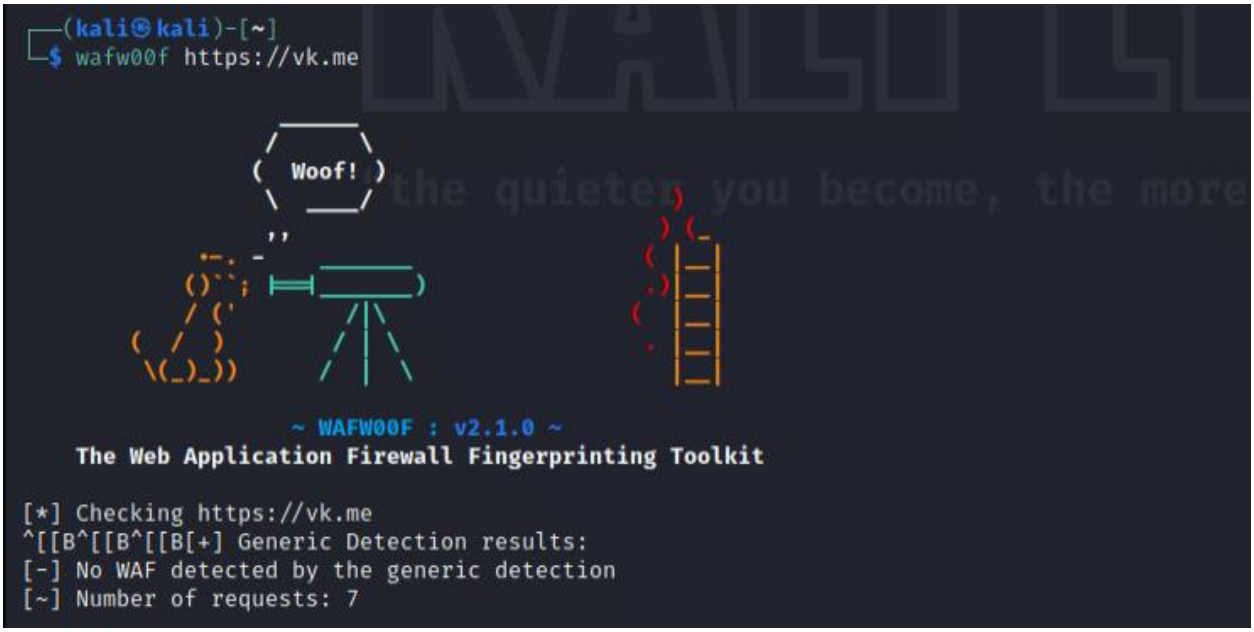
- **Wafw00f**

WAFW00f is the inbuilt tool in Kali distribution or else you can install it manually. It can detect around Top 22 web application firewall, so wafw00f is a phase of information gathering initially. [9] Here I used this tool to detect firewalls of chosen subdomains.

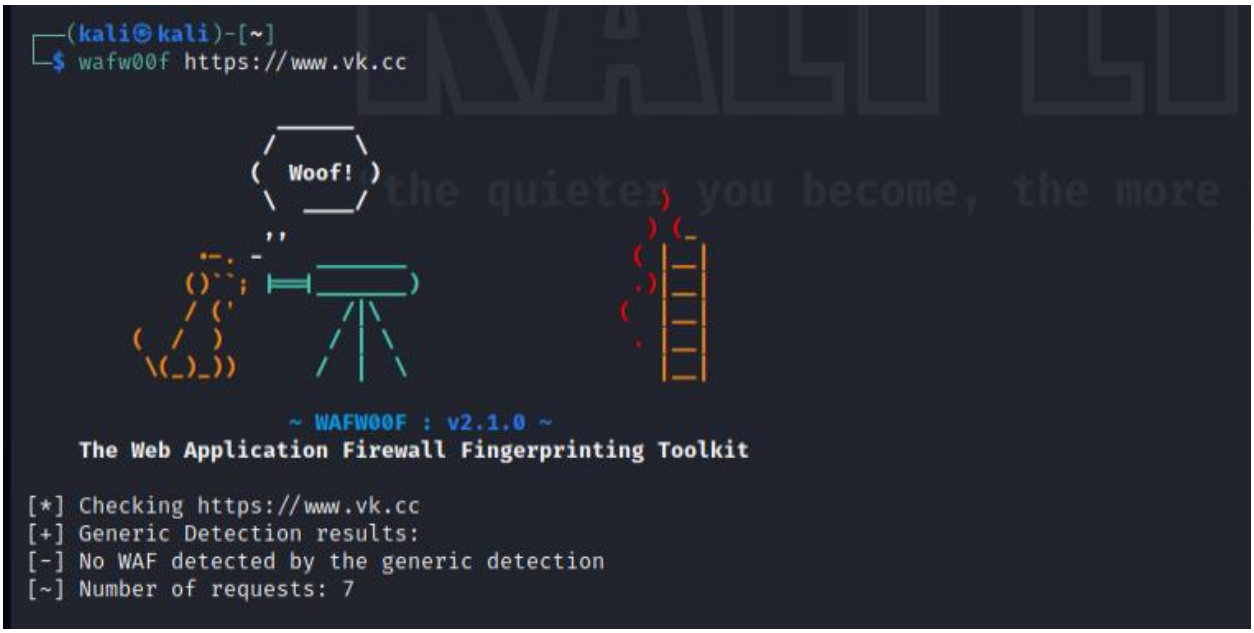
https://vk.com



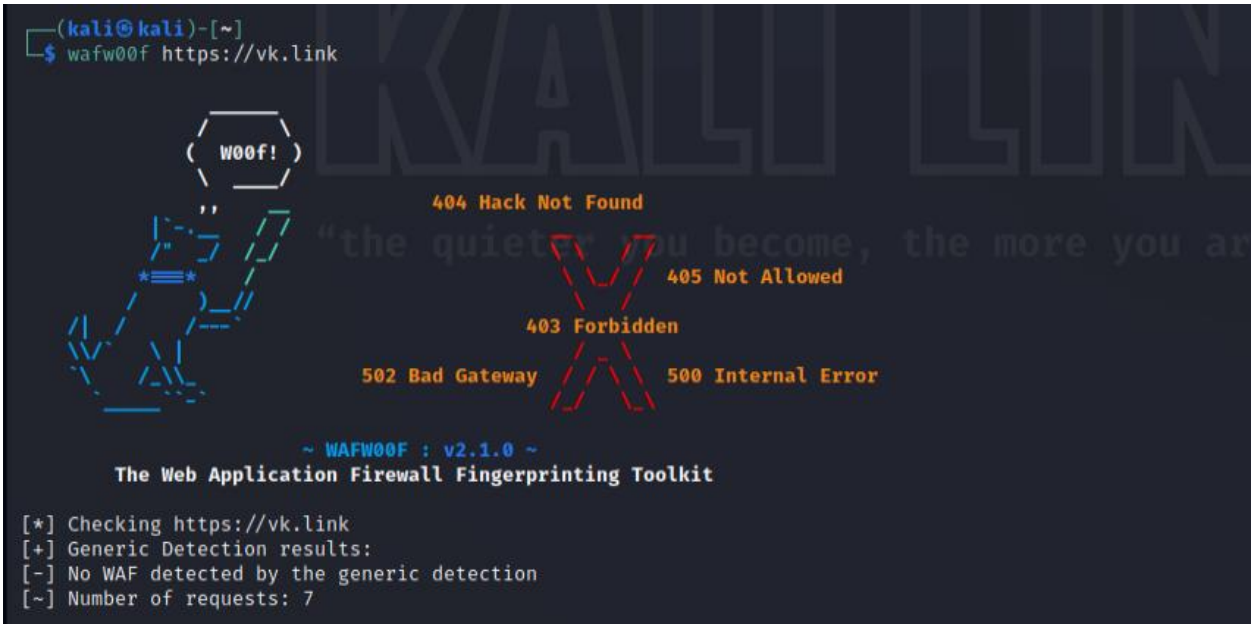
https://vk.me



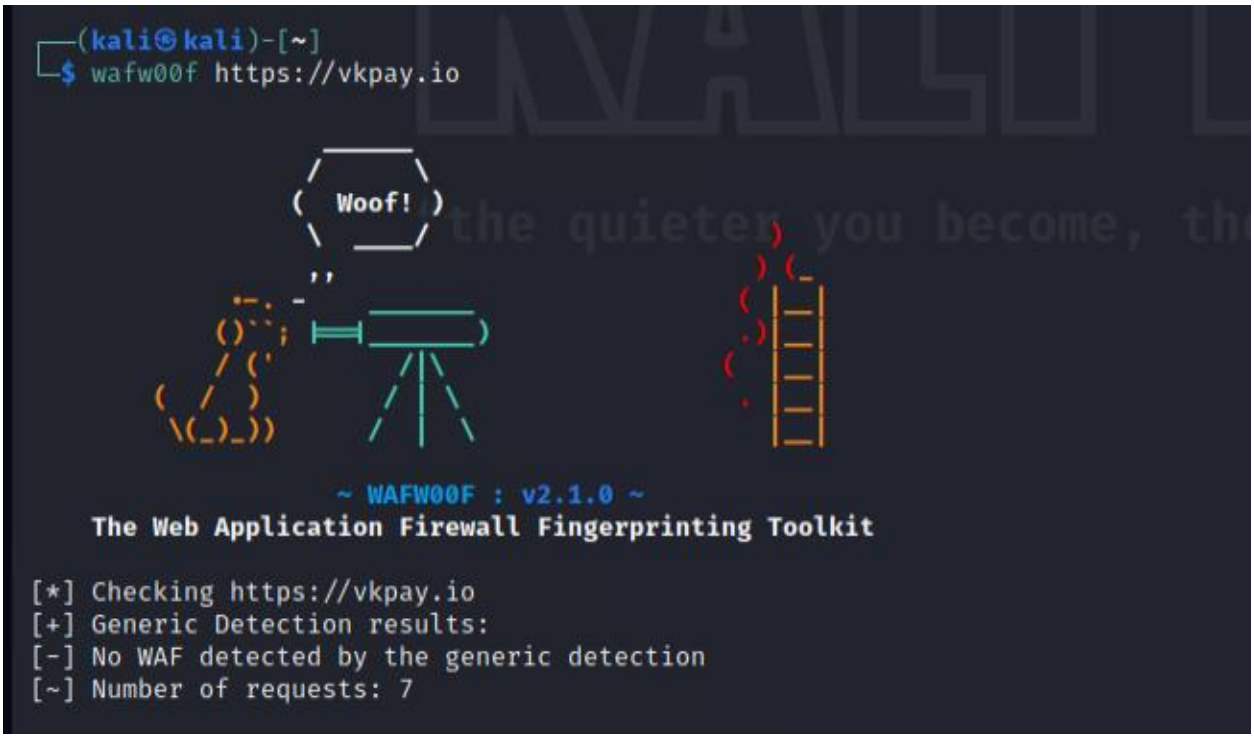
https://www.vk.cc



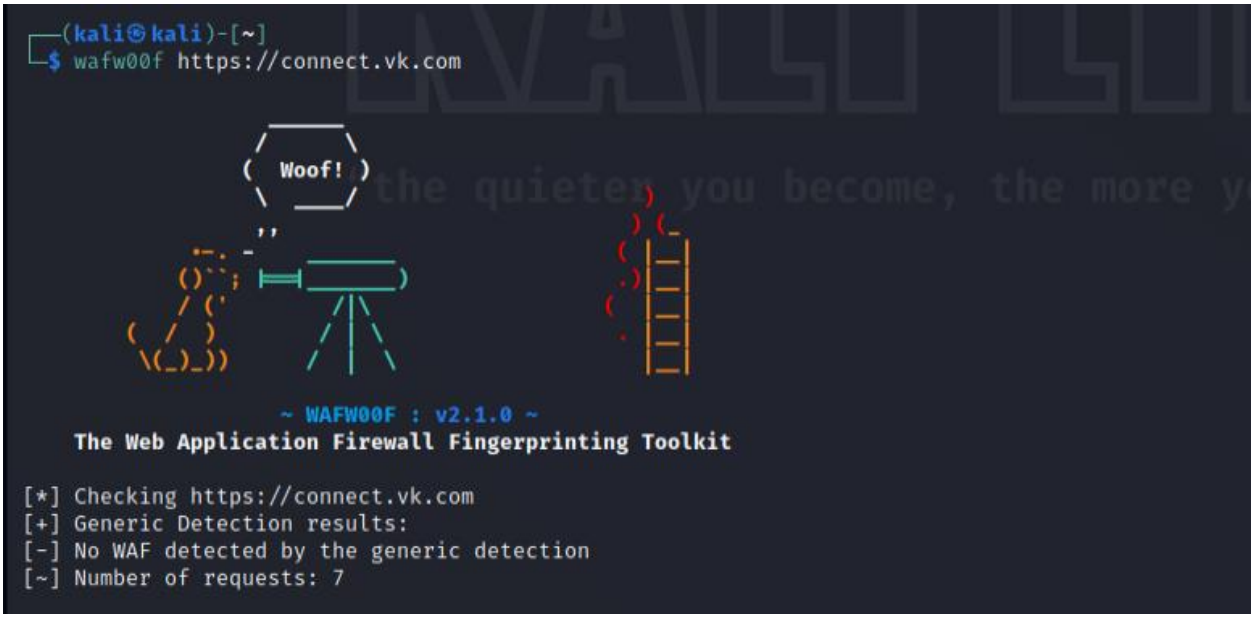
https://vk.link



https://vkpay.io

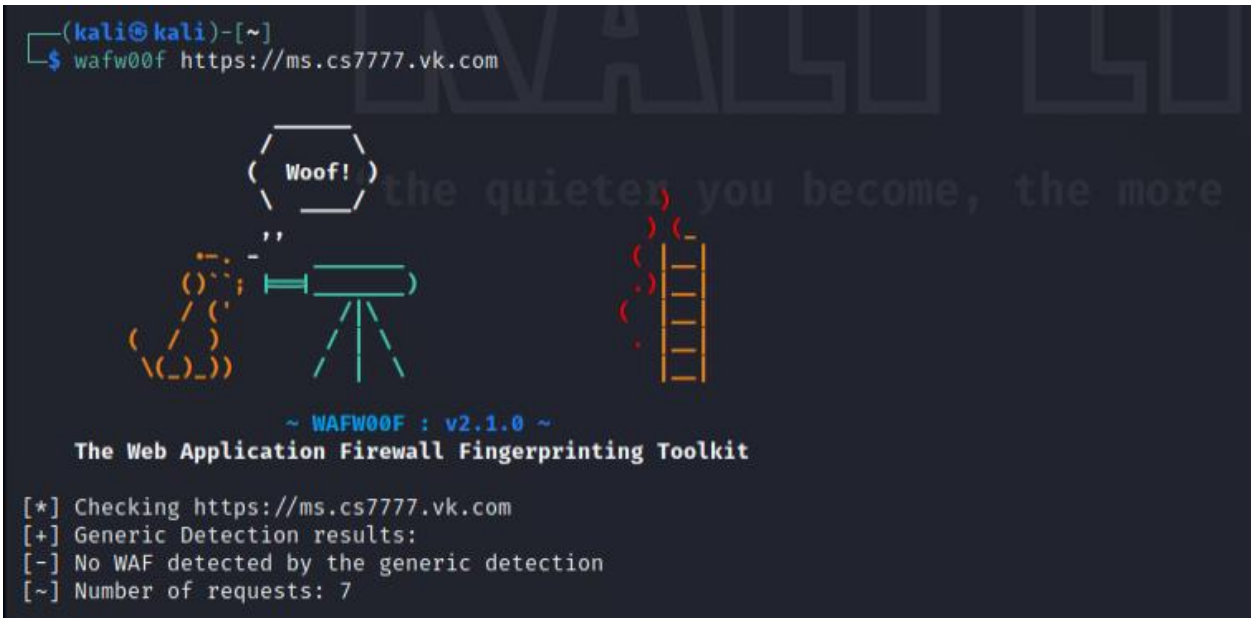


https://connect.vk.com



https://m.vk.com

https://ms.cs7777.vk.com

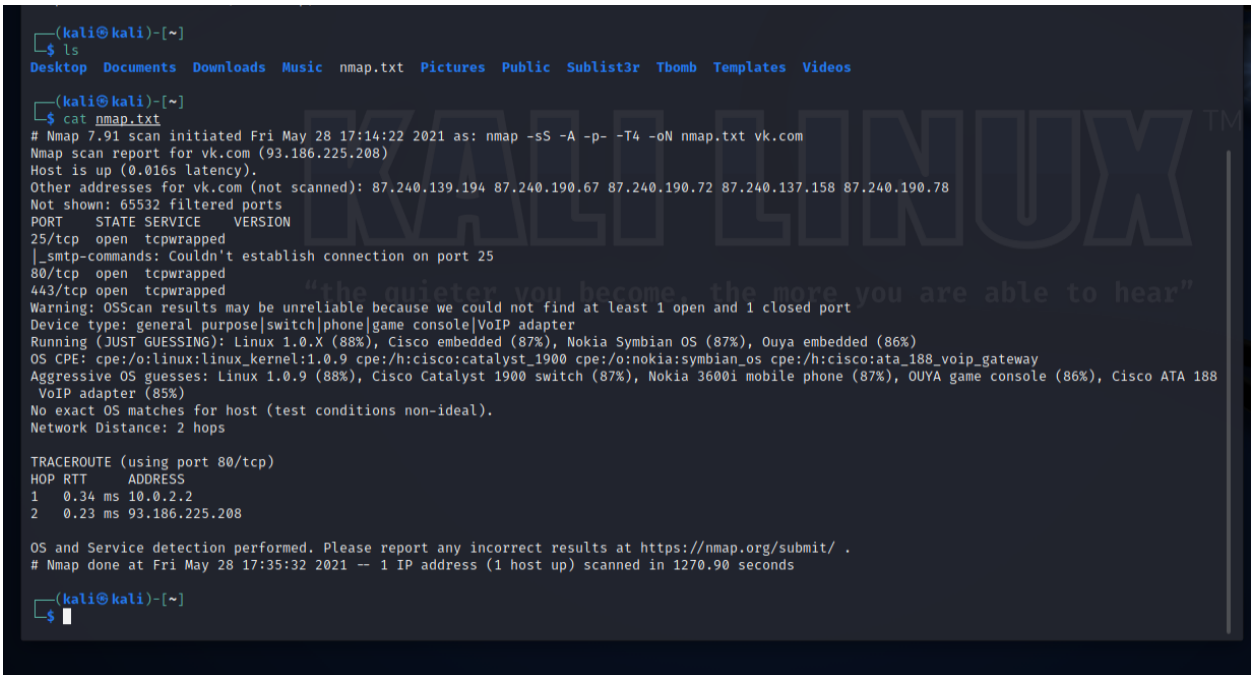


Find Open ports and running devices on the target network

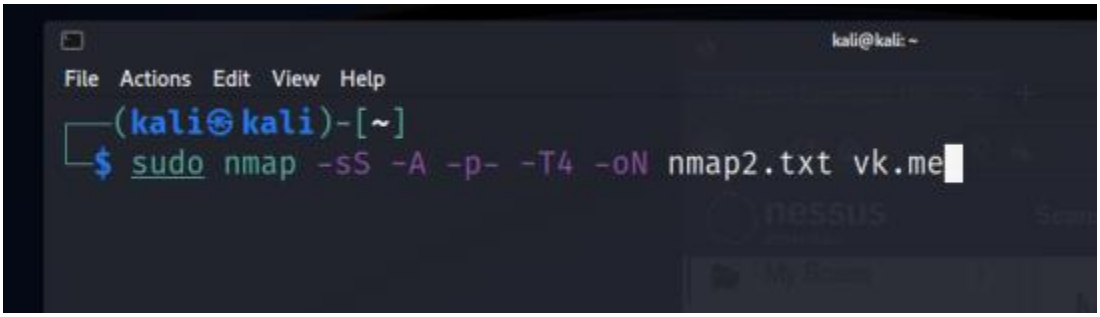
- **Nmap**

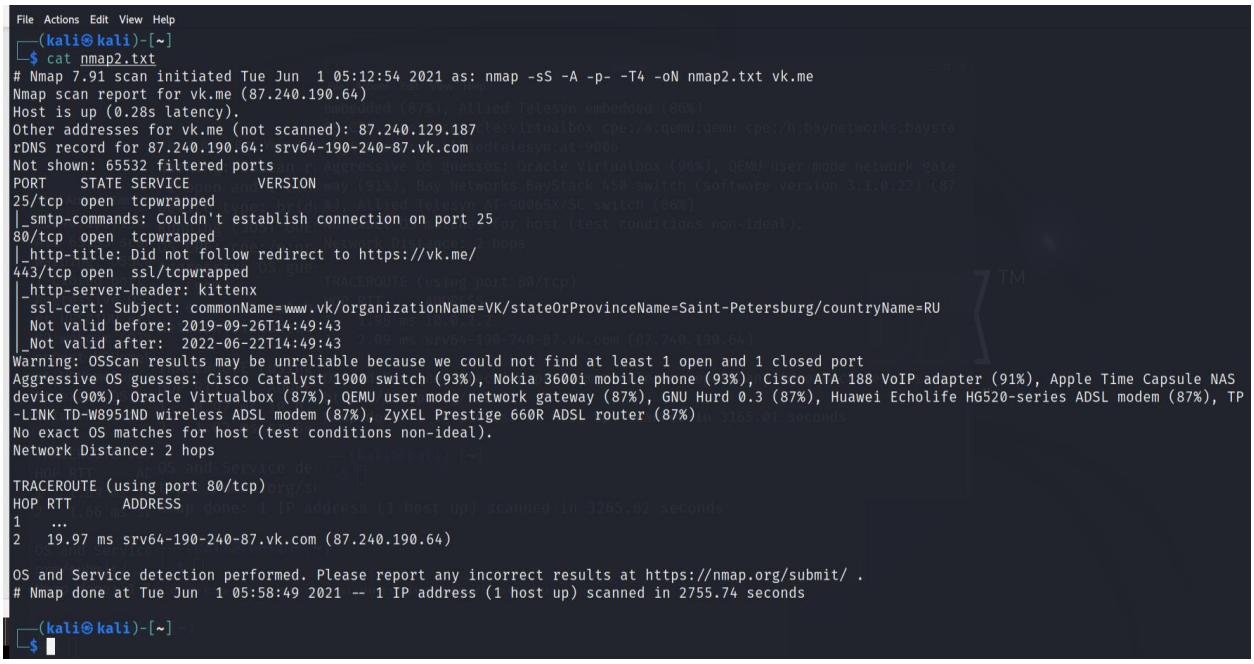
Nmap is the most popular port security network scanner in the world. The Nmap hosted security utility can assist you in determining the state of your firewall and security settings. Here I used Nmap to find open ports of chosen subdomains.

- https://vk.com

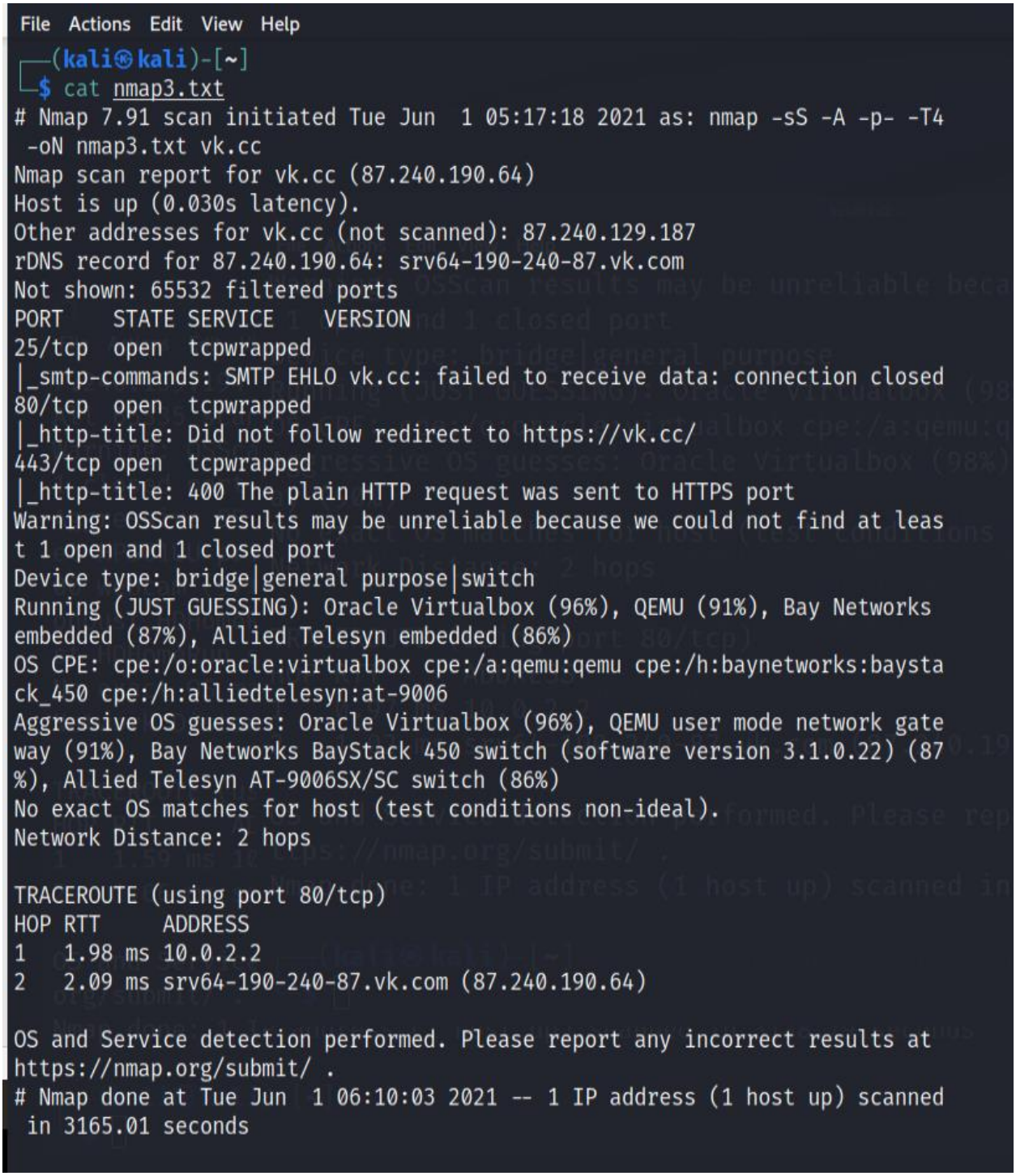


- https://vk.me

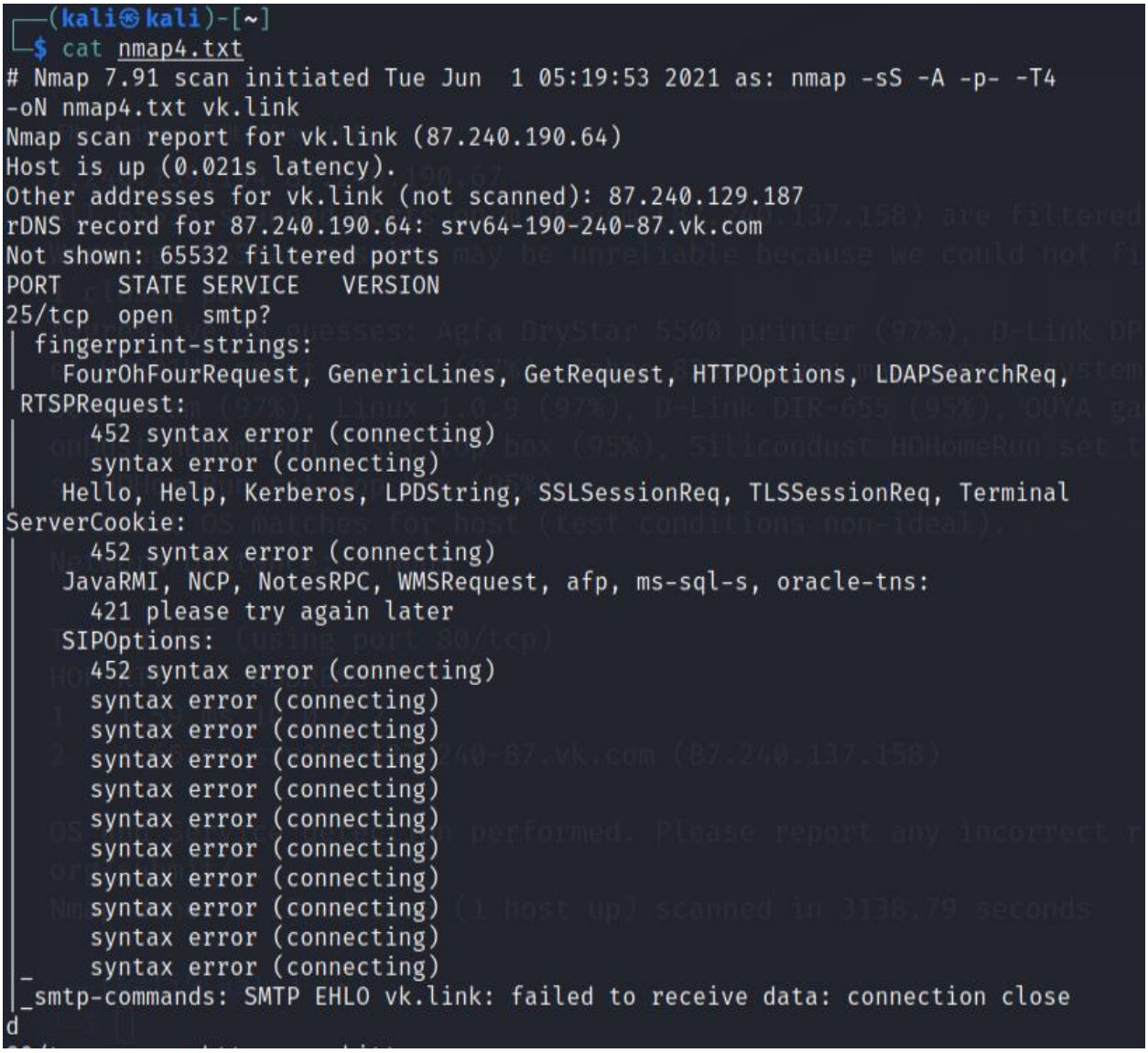

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -sS -A -p- -T4 -oN nmap2.txt vk.me

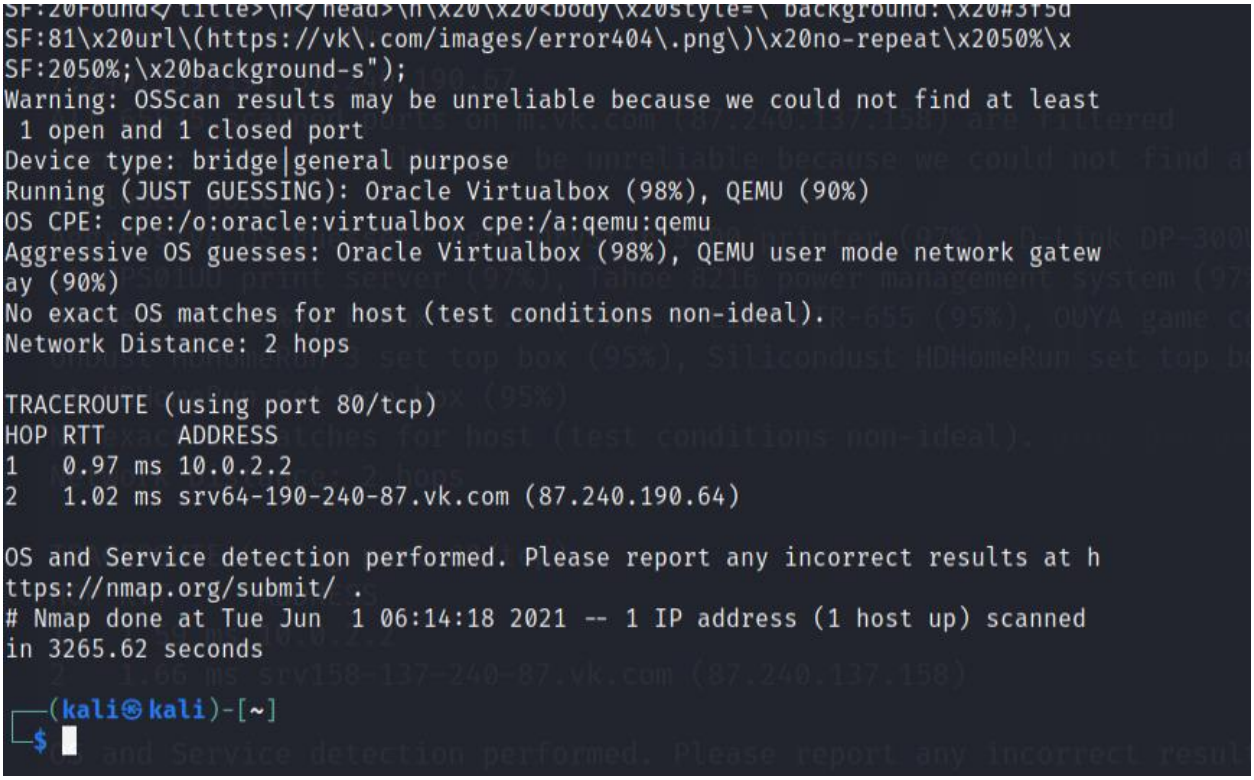

File Actions Edit View Help
(kali㉿kali)-[~]
$ cat nmap2.txt
Nmap 7.91 scan initiated Tue Jun 1 05:12:54 2021 as: nmap -sS -A -p- -T4 -oN nmap2.txt vk.me
Nmap scan report for vk.me (87.240.190.64)
Host is up (0.28s latency).
Other addresses for vk.me (not scanned): 87.240.129.187
rDNS record for 87.240.190.64: srv64-190-240-87.vk.com
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
25/tcp open tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp open tcpwrapped
|_http-title: Did not follow redirect to https://vk.me/
443/tcp open ssl/tcpwrapped
|_http-server-header: kittenx
| ssl-cert: Subject: commonName=www.vk/organizationName=VK/stateOrProvinceName=Saint-Petersburg/countryName=RU
| Not valid before: 2019-09-26T14:49:43
|_Not valid after: 2022-06-22T14:49:43
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Cisco Catalyst 1900 switch (93%), Nokia 3600i mobile phone (93%), Cisco ATA 188 VoIP adapter (91%), Apple Time Capsule NAS device (90%), Oracle Virtualbox (87%), QEMU user mode network gateway (87%), GNU Hurd 0.3 (87%), Huawei Echolife HG520-series ADSL modem (87%), TP-LINK TD-W8951ND wireless ADSL modem (87%), ZyXEL Prestige 660R ADSL router (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 ...
2 19.97 ms srv64-190-240-87.vk.com (87.240.190.64)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jun 1 05:58:49 2021 -- 1 IP address (1 host up) scanned in 2755.74 seconds
(kali㉿kali)-[~]
$

- https://www.vk.cc



- https://vk.link



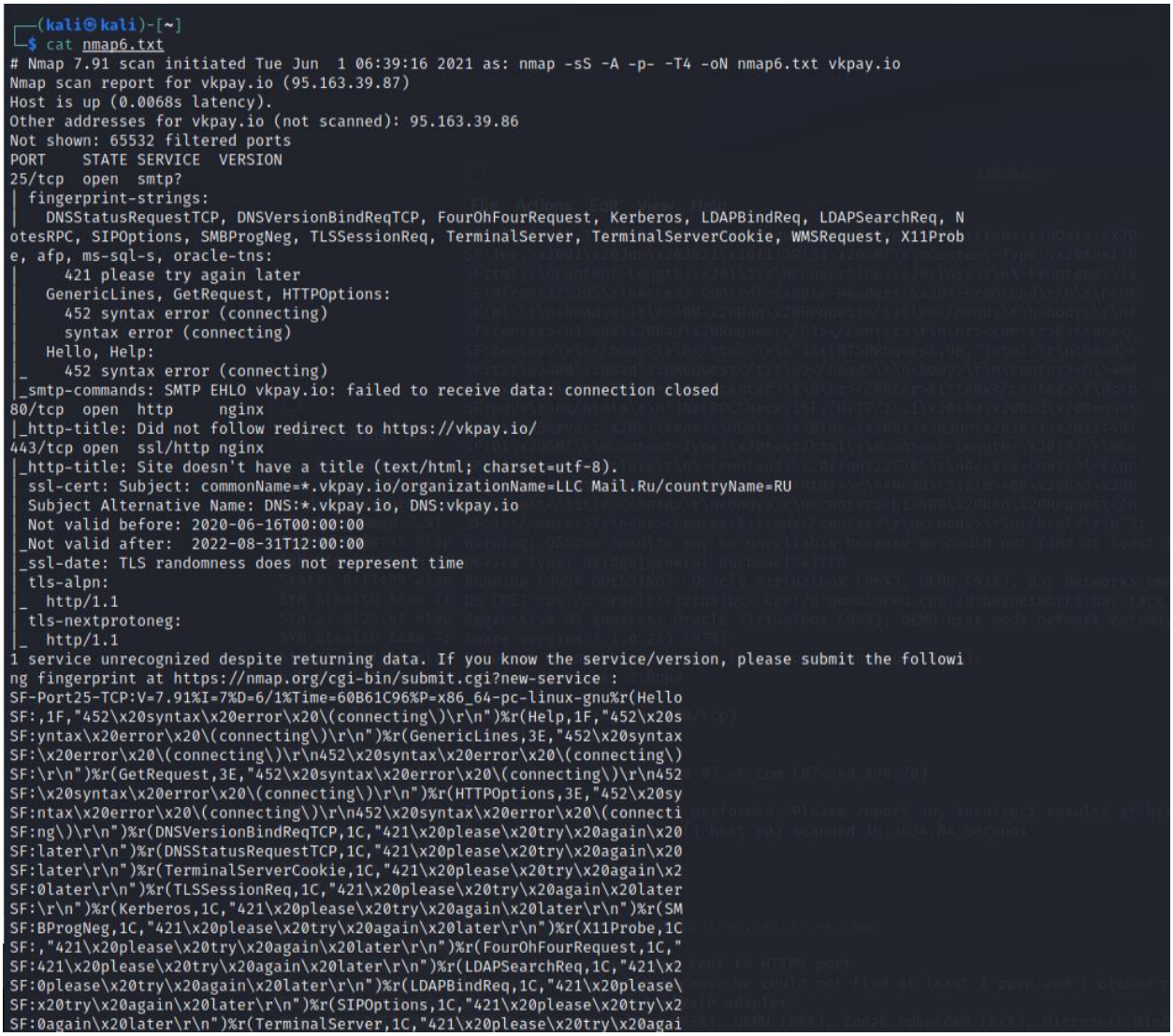

SF:20Found</title>\n</head>\n\x20\x20<body\x20style=\"background:\x20#3f5d
SF:81\x20url\(https://vk\.com/images/error404\.png\)\x20no-repeat\x2050%\x
SF:2050%;\x20background-s");
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gatew
ay (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.97 ms 10.0.2.2
2 1.02 ms srv64-190-240-87.vk.com (87.240.190.64)
OS and Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done at Tue Jun 1 06:14:18 2021 -- 1 IP address (1 host up) scanned
in 3265.62 seconds
(kali㉿kali)-[~]
$

- https://m.vk.com

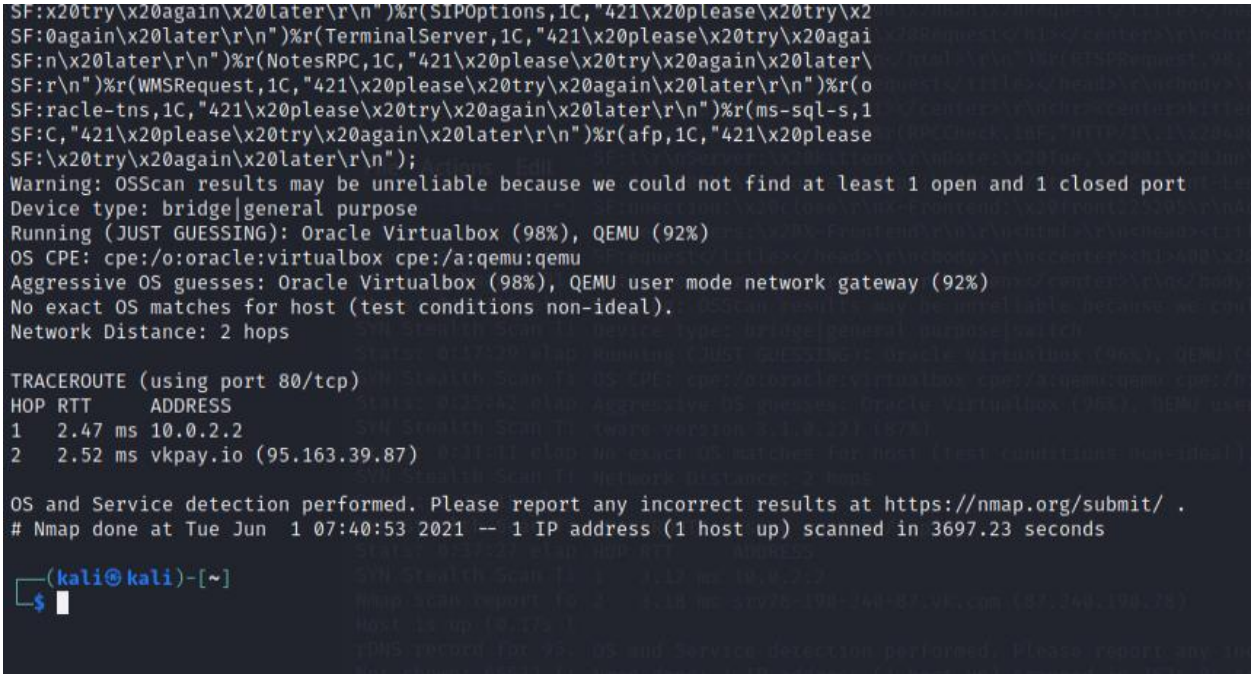
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A -p- -T4 -oN nmap5.txt m.vk.com
```

```
┌──(kali㉿kali)-[~]
└─$ cat nmap5.txt
# Nmap 7.91 scan initiated Tue Jun  1 05:22:27 2021 as: nmap -sS -A -p- -T4 -oN nmap5.txt m.vk.com
Nmap scan report for m.vk.com (87.240.137.158)
Host is up (0.0078s latency).
Other addresses for m.vk.com (not scanned): 93.186.225.208 87.240.190.72 87.240.190.78 87.240.139.194 87.
240.190.67
All 65535 scanned ports on m.vk.com (87.240.137.158) are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Agfa DryStar 5500 printer (97%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print
server (97%), Tahoe 8216 power management system (97%), TRENDnet TV-IP100 webcam (97%), Linux 1.0.9 (97%)
, D-Link DIR-655 (95%), OUYA game console (95%), SiliconDust HDHomeRun 3 set top box (95%), Silicondust H
DHomeRun set top box (95%), SiliconDust HDHomeRun set top box (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.59 ms 10.0.2.2
2   1.66 ms srv158-137-240-87.vk.com (87.240.137.158)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun  1 06:14:45 2021 -- 1 IP address (1 host up) scanned in 3138.79 seconds

┌──(kali㉿kali)-[~]
```

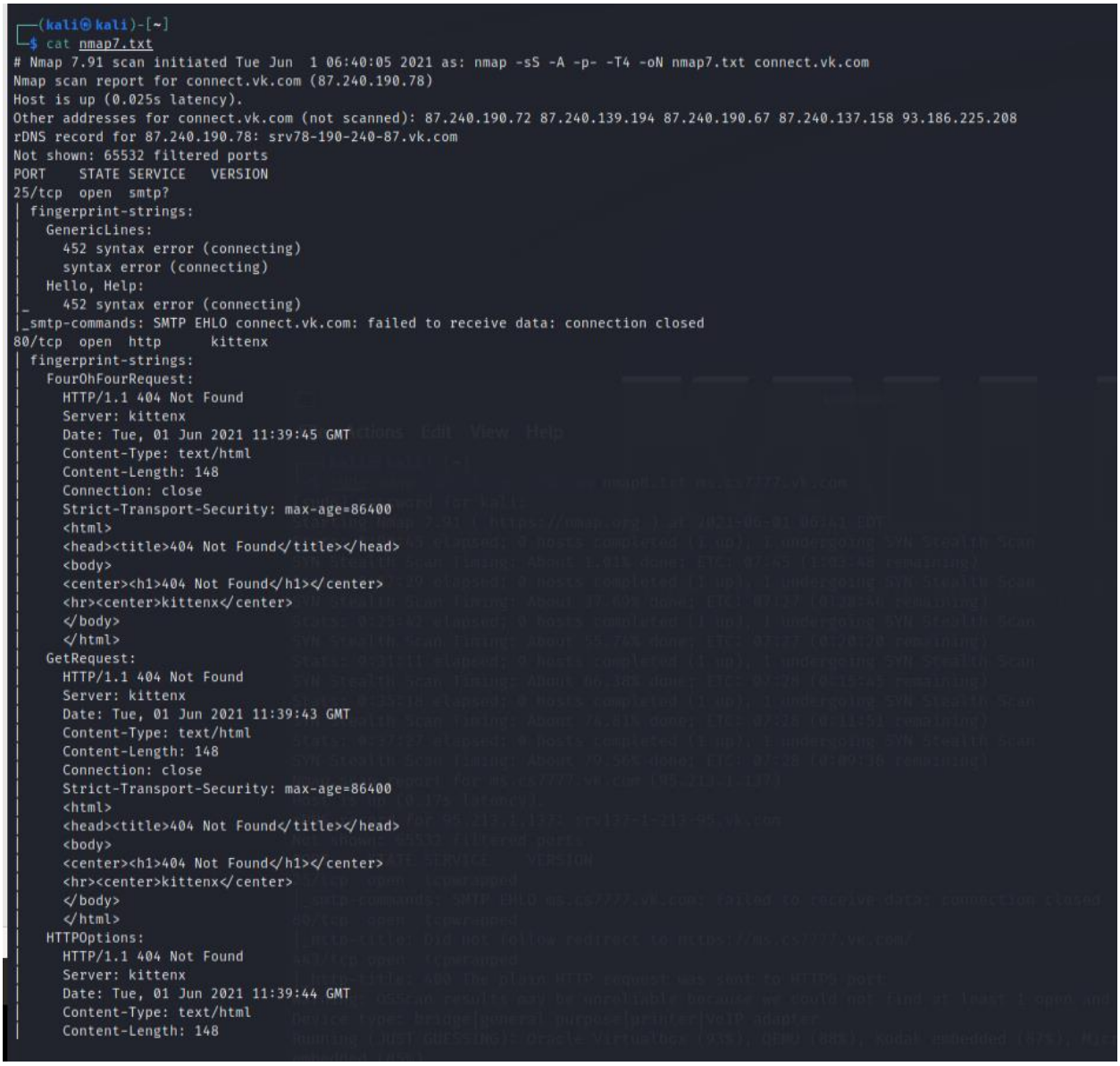
- https://vkpay.io



```
┌──(kali㉿kali)-[~]
└─$ cat nmap6.txt
# Nmap 7.91 scan initiated Tue Jun  1 06:39:16 2021 as: nmap -sS -A -p- -T4 -oN nmap6.txt vkpay.io
Nmap scan report for vkpay.io (95.163.39.87)
Host is up (0.0068s latency).
Other addresses for vkpay.io (not scanned): 95.163.39.86
Not shown: 65532 filtered ports
PORT    STATE SERVICE  VERSION
25/tcp  open  smtp?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, Kerberos, LDAPBindReq, LDAPSearchReq, N
otesRPC, SIPOptions, SMBProgNeg, TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Prob
e, afp, ms-sql-s, oracle-tns:
|     421 please try again later
|   GenericLines, GetRequest, HTTPOptions:
|     452 syntax error (connecting)
|     syntax error (connecting)
|   Hello, Help:
|_    452 syntax error (connecting)
|_smtp-commands: SMTP EHLO vkpay.io: failed to receive data: connection closed
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://vkpay.io/
443/tcp open  ssl/http nginx
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| ssl-cert: Subject: commonName=*.vkpay.io/organizationName=LLC Mail.Ru/countryName=RU
| Subject Alternative Name: DNS:*.vkpay.io, DNS:vkpay.io
| Not valid before: 2020-06-16T00:00:00
|_Not valid after:  2022-08-31T12:00:00
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the followi
ng fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.91%I=7%D=6/1%Time=60B61C96%P=x86_64-pc-linux-gnu%r(Hello
SF:,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Help,1F,"452\x20s
SF:yntax\x20error\x20\(connecting\)\r\n")%r(GenericLines,3E,"452\x20syntax
SF:\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting\)
SF:\r\n")%r(GetRequest,3E,"452\x20syntax\x20error\x20\(connecting\)\r\n452
SF:\x20syntax\x20error\x20\(connecting\)\r\n")%r(HTTPOptions,3E,"452\x20sy
SF:ntax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecti
SF:ng\)\r\n")%r(DNSVersionBindReqTCP,1C,"421\x20please\x20try\x20again\x20
SF:later\r\n")%r(DNSStatusRequestTCP,1C,"421\x20please\x20try\x20again\x20
SF:later\r\n")%r(TerminalServerCookie,1C,"421\x20please\x20try\x20again\x2
SF:0later\r\n")%r(TLSSessionReq,1C,"421\x20please\x20try\x20again\x20later
SF:\r\n")%r(Kerberos,1C,"421\x20please\x20try\x20again\x20later\r\n")%r(SM
SF:BProgNeg,1C,"421\x20please\x20try\x20again\x20later\r\n")%r(X11Probe,1C
SF:,"421\x20please\x20try\x20again\x20later\r\n")%r(FourOhFourRequest,1C,"
SF:421\x20please\x20try\x20again\x20later\r\n")%r(LDAPSearchReq,1C,"421\x2
SF:0please\x20try\x20again\x20later\r\n")%r(LDAPBindReq,1C,"421\x20please\
SF:x20try\x20again\x20later\r\n")%r(SIPOptions,1C,"421\x20please\x20try\x2
SF:0again\x20later\r\n")%r(TerminalServer,1C,"421\x20please\x20try\x20agai
```


SF:x20try\x20again\x20later\r\n")%r(SIPOptions,1C,"421\x20please\x20try\x2
SF:0again\x20later\r\n")%r(TerminalServer,1C,"421\x20please\x20try\x20agai
SF:n\x20later\r\n")%r(NotesRPC,1C,"421\x20please\x20try\x20again\x20later\
SF:r\n")%r(WMSRequest,1C,"421\x20please\x20try\x20again\x20later\r\n")%r(o
SF:racle-tns,1C,"421\x20please\x20try\x20again\x20later\r\n")%r(ms-sql-s,1
SF:C,"421\x20please\x20try\x20again\x20later\r\n")%r(afp,1C,"421\x20please
SF:\x20try\x20again\x20later\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.47 ms 10.0.2.2
2 2.52 ms vkpay.io (95.163.39.87)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jun 1 07:40:53 2021 -- 1 IP address (1 host up) scanned in 3697.23 seconds
┌──(kali㉿kali)-[~]
└─$

- https://connect.vk.com



```
┌──(kali㉿kali)-[~]
└─$ cat nmap7.txt
# Nmap 7.91 scan initiated Tue Jun  1 06:40:05 2021 as: nmap -sS -A -p- -T4 -oN nmap7.txt connect.vk.com
Nmap scan report for connect.vk.com (87.240.190.78)
Host is up (0.025s latency).
Other addresses for connect.vk.com (not scanned): 87.240.190.72 87.240.139.194 87.240.190.67 87.240.137.158 93.186.225.208
rDNS record for 87.240.190.78: srv78-190-240-87.vk.com
Not shown: 65532 filtered ports
PORT    STATE SERVICE   VERSION
25/tcp  open  smtp?
| fingerprint-strings:
|   GenericLines:
|     452 syntax error (connecting)
|     syntax error (connecting)
|   Hello, Help:
|_    452 syntax error (connecting)
|_smtp-commands: SMTP EHLO connect.vk.com: failed to receive data: connection closed
80/tcp  open  http      kittenx
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Server: kittenx
|     Date: Tue, 01 Jun 2021 11:39:45 GMT
|     Content-Type: text/html
|     Content-Length: 148
|     Connection: close
|     Strict-Transport-Security: max-age=86400
|     <html>
|     <head><title>404 Not Found</title></head>
|     <body>
|     <center><h1>404 Not Found</h1></center>
|     <hr><center>kittenx</center>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.1 404 Not Found
|     Server: kittenx
|     Date: Tue, 01 Jun 2021 11:39:43 GMT
|     Content-Type: text/html
|     Content-Length: 148
|     Connection: close
|     Strict-Transport-Security: max-age=86400
|     <html>
|     <head><title>404 Not Found</title></head>
|     <body>
|     <center><h1>404 Not Found</h1></center>
|     <hr><center>kittenx</center>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Server: kittenx
|     Date: Tue, 01 Jun 2021 11:39:44 GMT
|     Content-Type: text/html
|     Content-Length: 148
```

```
SF:equest</title></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h
SF:1></center>\r\n<hr><center>kittenx</center>\r\n</body>\r\n</html>\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (87%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   3.12 ms 10.0.2.2
2   3.18 ms srv78-190-240-87.vk.com (87.240.190.78)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun  1 07:40:40 2021 -- 1 IP address (1 host up) scanned in 3634.84 seconds

┌──(kali㉿kali)-[~]
└─$
```

- https://ms.cs7777.vk.com

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A -p- -T4 -oN nmap8.txt ms.cs7777.vk.com
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-01 06:41 EDT
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.01% done; ETC: 07:45 (1:03:48 remaining)
Stats: 0:17:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.69% done; ETC: 07:27 (0:28:46 remaining)
Stats: 0:25:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.74% done; ETC: 07:27 (0:20:20 remaining)
Stats: 0:31:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 66.38% done; ETC: 07:28 (0:15:45 remaining)
Stats: 0:35:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.81% done; ETC: 07:28 (0:11:51 remaining)
Stats: 0:37:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.56% done; ETC: 07:28 (0:09:36 remaining)
Nmap scan report for ms.cs7777.vk.com (95.213.1.137)
Host is up (0.17s latency).
rDNS record for 95.213.1.137: srv137-1-213-95.vk.com
Not shown: 65532 filtered ports
PORT    STATE SERVICE    VERSION
25/tcp  open  tcpwrapped
|_smtp-commands: SMTP EHLO ms.cs7777.vk.com: failed to receive data: connection closed
80/tcp  open  tcpwrapped
|_http-title: Did not follow redirect to https://ms.cs7777.vk.com/
443/tcp open  tcpwrapped
|_http-title: 400 The plain HTTP request was sent to HTTPS port
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|printer|VoIP adapter
Running (JUST GUESSING): Oracle Virtualbox (93%), QEMU (88%), Kodak embedded (87%), Microsoft Windows XP (86%), Vegastream
embedded (85%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:kodak:esp_5210 cpe:/o:microsoft:windows_xp::sp3 cpe:/h:vegastream:
vega_400
Aggressive OS guesses: Oracle Virtualbox (93%), QEMU user mode network gateway (88%), Kodak ESP 5210 printer (87%), Microso
ft Windows XP SP3 (86%), Kodak ESP C310 printer (86%), Vegastream Vega 400 VoIP Gateway (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   151.16 ms 10.0.2.2
2   151.16 ms srv137-1-213-95.vk.com (95.213.1.137)

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 3054.72 seconds

┌──(kali㉿kali)-[~]
└─$
```

Vulnerability Analyzing

A vulnerability is a system or device code weakness or error which can endanger the confidentiality, availability and integrity of the data stored on a device or system via unauthorized access, privilege or dos when exploited. An exploit is called a code or program used to use a vulnerability.

Here I used Nikto, OWASP ZAP, Uniscan and Nessus to scan vulnerabilities of chosen subdomains. After scanning I have found.

1. The anti-clickjacking X-frame-option header is not present
2. The x-xss-protection header is not defined
3. The site uses SSL and Expect-CT header is not present.
4. The X-Content-Type-Options header is not set.
5. Cookie remixlang created without the secure flag.
6. Cookie remixlang created without the httponly flag
7. Wildcard certificate
8. BREACH Attack.
9. HSTS Missing From HTTPS Server.
10. TLS Version 1.0 Protocol Detection

After identifying vulnerabilities, we must analyze them and take actions to prevent the risk associated with those weaknesses.

1. The anti-clickjacking X-frame-option header is not present

Scan detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

X-Frame-Option

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Clicckjacking Attack

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly

download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Remediation

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

- X-Frame-Options: DENY

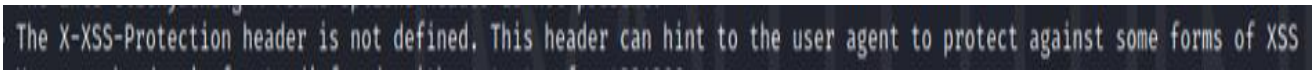
  It completely denies to be loaded in frame/iframe.
- X-Frame-Options: SAMEORIGIN

  It allows only if the site which wants to load has a same origin.
- X-Frame-Options: ALLOW-FROM *URL*

  It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

2. The x-xss-protection header is not defined



Modern browsers support the HTTP 'X-XSS-Protection' response header, which allows websites to regulate their XSS auditors. Because the server isn't set up to return a 'X-XSS-Protection' header,

every page on this site could be vulnerable to a Cross-Site Scripting (XSS) attack. This URL has been marked as an example. If older browser support is not required, Content-Security-Policy without permitting unsafe-inline scripts should be used instead.

Remediation

Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages.

3. The site uses SSL and Expect-CT header is not present.

The Expect-CT header allows sites to opt in to reporting and or enforcement of Certificate Transparency requirements, which prevents the use of misissued certificates for that site from going unnoticed. This URL is flagged as a specific example.

Remediation

Configure your web server to include an 'Expect-CT' header with a value of 'maxage' defined therein.

4. The X-Content-Type-Options header is not set.

The missing "X-Content-Type-Options" header enables a browser to perform MIME type sniffing when the Content-Type header is not set or its value seems inappropriate. In other words, when the browser gets the response from the server it tries to figure out on its own what is the type of the content and how to handle it. In certain circumstances that can lead to serious security issues (XSS attack).

For example, if we have an application that allows an upload of jpg files, an attacker may upload a file with jpg extension being in fact an html file with malicious js script inside. Some other user may want to display the image in his browser. The browser gets the file with Content-Type=image/jpg and finds out that content type is inappropriate. If the MIME type sniffing is enabled, the browser handles the file as html and executes the malicious js script. On the other hand, if the MIME type sniffing is disabled by setting the "X-Content-Type-Options" header, the browser displays an error message and the script is not executed. [17]

Remediation

Your server should be configured to include the header.

X-Content-Type-Options=nosniff

5. Cookie remixlang created without the secure flag.

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

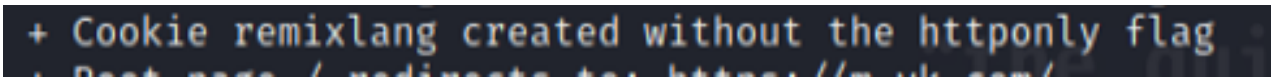
To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common

defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure. [18]

Remediation

The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

6. Cookie remixlang created without the httponly flag



If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as

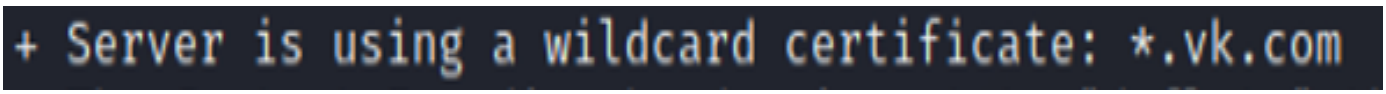
cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing. [19]

7. Wildcard certificate



A wildcard certificate is a public key certificate that can be used with several sub-domains of a domain in terms of networking and web security. The most common application is for safeguarding websites with HTTPS, but it also has uses in a variety of other industries. A wildcard certificate can be less expensive and more convenient than a certificate for each sub-domain when

compared to traditional certificates. By safeguarding many domains and associated sub-domains, multi-domain wildcard certificates decrease complexity and costs.

Using a wildcard certificate on a publicly accessible web server raises the danger of cybercriminals using the server to host malicious websites in phishing campaigns.

- Compromised web server.

  If you use a wildcard certificate on public-facing web servers, you risk cybercriminals exploiting that server to host malicious websites for phishing campaigns. .

- Stolen private key.

  If cybercriminals obtain access to the private key of a wildcard certificate, they may be able to impersonate any domain that is covered by that certificate.

- Fake certificates.

  Cybercriminals can utilize wildcard certificates to construct subdomains and set up phishing sites if they mislead a CA into issuing a wildcard certificate for a fictional firm. [20]

Remediation

To fix this you need to list the additional subdomain levels you'd like to encrypt in the SAN fields of your certificate signing request (CSR). Keep in mind that as you go to higherTo fix this, in the SAN fields of your certificate signing request, mention the additional subdomain levels you'd like to encrypt (CSR). Keep in mind that the complexity of protecting higher subdomain levels with individual wildcards grows. subdomain levels, the complexity of securing them with individual wildcards increases. [21] [22]

8. BREACH Attack

Severity: Medium

Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext attack is possible on this website. Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website. Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.An attacker can monitor the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server even if the connection is SSL/TLS protected (by using invisible frames). An attacker could steal information from the website and accomplish the following by following these steps: Inject some of the plaintext they've discovered into a victim's queries. Calculate the amount of encrypted traffic.

Even if you use an SSL/TLS protected connection, an attacker can still view the victim’s encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server. Following these

steps, an attacker could steal information from the website and do the following; Inject partial plaintext they have uncovered into a victim's requests, Measure the size of encrypted traffic.

Remediation

- If possible, disable HTTP level compression
- Separate sensitive information from user input
- Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
- Hide the length of the traffic by adding a random number of bytes to the responses.
- Add in a rate limit, so that the page maximum is reached five times per minute. [23]

9. HSTS Missing From HTTPS Server

Output

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

Port ▲	Hosts
443 / tcp / www	ms.cs7777.vk.com

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Remediation

Configure the remote web server to use HSTS.

10. TLS Version 1.0 Protocol Detection

Output

```
TLSv1 is enabled and the server supports at least one cipher.
```

Port ▲	Hosts
443 / tcp / www	ms.cs7777.vk.com

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Remediation

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Conclusion

The vulnerabilities and essential recommendations for the http://www.vk.com domain have been demonstrated in this web audit. First, I have enumerated subdomains. After I've inspected each subdomain for vulnerabilities. In addition, I have detailed descriptions of the tools I utilized for each reconnaissance and vulnerability analysis phase of this security assessment. Finally, I discussed how to mitigate such risks.

References

[1] "hackerone," [Online]. Available: https://hackerone.com/vkcom?type=team.

[2] "WEBSCOOT," [Online]. Available: https://webscoot.io/blog/website-security-audit/.

[3] "CYFOR," [Online]. Available: https://cyfor.co.uk/cyber-security/cyber-security-audit/.

[4] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/VK_(service).

[5] "OWASP," [Online]. Available: https://owasp.org/www-project-top-ten/.

[6] "Atlassian," [Online]. Available: https://www.atlassian.com/trust/security/security-severity-levels.

[7] "geekflare," [Online]. Available: https://geekflare.com/find-subdomains/.

[8] "github," [Online]. Available: https://github.com/aboul3la/Sublist3r.

[9] CSO. [Online]. Available: https://www.csoonline.com/article/3537230/what-are-vulnerability-scanners-and-how-do-they-work.html.

[10] "phoenixnap," [Online]. Available: https://phoenixnap.com/blog/vulnerability-assessment-scanning-tools.

[11] "tools.kali.org," [Online]. Available: https://tools.kali.org/information-gathering/nikto.

[12] www.zaproxy.org. [Online]. Available: https://www.zaproxy.org/getting-started/.

[13] "latesthackingnews," [Online]. Available: https://latesthackingnews.com/2018/09/20/uniscan-web-applications-penetration-testing-tool/.

[14] "linuxhint.com," [Online]. Available: https://linuxhint.com/nessus_installation_kali_linux/.

[15] "whitehatsec," [Online]. Available: https://www.whitehatsec.com/glossary/content/fingerprintingfootprinting.

[16] "GBHackers on Security," [Online]. Available: https://gbhackers.com/web-application-firewall-detection-using-kali-linux-wafw00f/.

[17] "scanrepeat.com," [Online]. Available: https://scanrepeat.com/web-security-knowledge-base/x-content-type-options-header-missing.

[18] "portswigger," [Online]. Available: https://portswigger.net/kb/issues/00500200_tls-cookie-without-secure-flag-set.

[19] "portswigger," [Online]. Available: https://portswigger.net/kb/issues/00500600_cookie-without-httponly-flag-set.

[20] "venaf," [Online]. Available: https://www.venafi.com/blog/wildcard-certificates-make-encryption-easier-but-less-secure.

[21] "cheapsslsecurity," [Online]. Available: https://cheapsslsecurity.com/p/what-an-ssl-common-name-wildcard-error-is-and-how-to-fix-it/.

[22] ssl. [Online]. Available: https://www.ssl.com/faqs/what-is-a-wildcard-ssl-certificate/.

[23] "netsparker.," [Online]. Available: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/breach-attack-detected/.

[24] "INFOSEC," [Online]. Available: https://resources.infosecinstitute.com/topic/information-gathering/.

[25] "upguard," [Online]. Available: https://www.upguard.com/blog/vulnerability.