

# ***RECONNAISSANCE REPORT***



**Submitted By:**

**Tushar Agarwal**

**[Tushar.mittal1309@gmail.com](mailto:Tushar.mittal1309@gmail.com)**

## **Abstract**

This report uses a variety of reconnaissance scans to give a thorough reconnaissance analysis of an e-commerce company. The goal was to collect important data about the target company from a variety of sources, including open databases, network analysis, social media, search engines, website footprinting, and specialised software like Shodan.io.

A Whois Lookup was used to gather information on the domain registration, including the name of the organisation, its contact details, and the dates of registration. This information included details about the organisation that operated the e-commerce firm.

The target's domain name system configuration was then investigated using a DNS Lookup. This scan provided information on the target's infrastructure and potential attack surfaces by revealing the mail servers, IP addresses connected to the domain, and any subdomains.

# **Content**

1. Whois Lookup
2. DNS Lookup
3. Network Lookup (samspace)
4. Social media
5. Search reconnaissance (search)
6. Website footprinting
7. Footprinting using google
8. Shodan.io
9. Business Info
10. Directors/Owners

## **Reconnaissance Report on an Ecommerce Company ( [skillvertex.in](https://skillvertex.in) )**

### **❖ Reconnaissance using Google Search :-**

In this methodology we were able to perform a simple google search on the company name\_ ( [skillvertex.in](https://skillvertex.in) ) and able to get information like the company's website, google reviews, new articles and other 3rd party sites were captured from where information can be retrieved.

**Here is some google result as show in figer :-**

<https://study.skillvertex.in> :

**LMS SKILLVERTEX**

SkillVertex · About Us · Contact Us · Sign Up · Sign Up. Hi, Welcome back! Keep me signed in.

Forgot? Sign In. Don't have an account? Register Now.

- [Fig 1.1 study.skillvertex.in website captured](#)

In Fig 1.2 here we can see the google search result the company ( [skillvertex.in](https://skillvertex.in) ) have a social media account ( Instagram, linkedin) etc. and in fig1.3 we have some company reviews and details (Address, numbers, working time) etc in fig 1.4

<https://www.instagram.com/skillvertex>

### SkillVertex (@skillvertex.in) • Instagram photos and videos

An e-learning platform with a vision to upskill students for the industry and help you land your dream job/university. · 248 posts · 13.9K followers · 2 following.

<https://in.linkedin.com/company/skill-vertex>

### Skill Vertex - LinkedIn

SKILLVERTEX is a self-funded startup, we are a sophisticated Edu-tech startup that provides courses and placement programs to the Graduating Students.

---

Fig 1.2 social media account (skillvertex)

#### Reviews from the web

3.4/5 [AmbitionBox](#) · 156 reviews

#### From SkillVertex

"We are an EdTech organization where we look forward to provide upskilling and training to students and working professionals by delivering a diverse range of programs in accordance with their needs and future aspirations. With respect to the emerging... [More](#)

#### Reviews ⓘ

[Write a review](#)

[Add a photo](#)

658 [Google reviews](#)



"Really helpful **people**, best **place** to experience **team work** and personal growth."




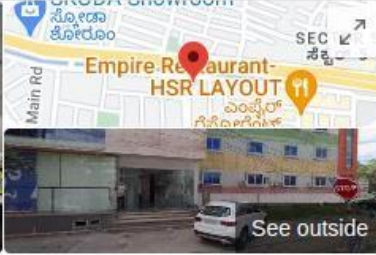
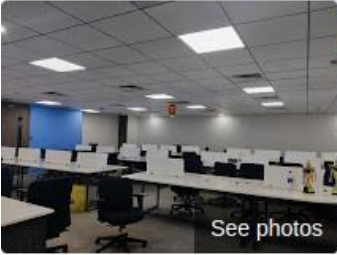
"Good company to work and friendly **environment**"



"Amazing **atmosphere**, Comfortable working **space**."




Fig 1.3 Reviews from web (Skillvertex)



[See photos](#)[See outside](#)

## SkillVertex



[Website](#)[Directions](#)[Save](#)[Call](#)

Education center in Bengaluru, Karnataka

**Service options:** Online classes · On-site services not available

**Address:** SkillVertex, 5th Main Road, 14th B Cross Rd, Sector 6, HSR Layout, Bengaluru, Karnataka 560102

**Hours:** Closed · Opens 11AM Wed ▾

**Phone:** 096060 12806

[Suggest an edit](#) · [Own this business?](#)

Fig 1.4 Address,phone,working hours (Skillvertex)

Now we have some details of SikilVertex company But this is not enough to know about company security, weakness etc. we can find out the security weakness by using [Reconnaissance](#).

The steps should be performed in an orderly manner as follows:-

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing tracks

We have some tools to gether information :-

- [1] Whois Lookup
- [2] Geo-IP Lookup
- [3] Grab Banners
- [4] Subnet Calculator
- [5] NMAP Port Scan
- [6] Subdomain Scanner
- [7] Reverse IP Lookup & CMS Detection
- [8] SQLi Scanner (Finds Links With Parameter And Scans For Error Based SQLI )

The main goal of this report will be solely based on “Reconnaissance”. The purpose of Reconnaissance is to gather information. Information gathering and getting to know more about the target system is the first process that is involved in ethical hacking. There are mainly two types of Reconnaissance that could be performed which are known as “active” and “passive” This Report will focus on both the passive method and the active method of gathering information. Passive reconnaissance is a method through which attempts are made to gather information about the target and its network without actively being involved with the system. Active reconnaissance is a method in which attempts are made to gather information through actively engaging with the system. With the advancements that have taken there has been an increase in the usage of the internet nowadays due to which passive method has also become common and is being performed by many people

### **[1] Whois Lookup :-**

A Whois record contains all of the contact information associated with the person, group, or company that registers a particular domain name. Typically, each Whois record will contain information such as the name and contact information of the Registrant (who owns the domain), the name and contact information of the registrar

Registrar (the organization or commercial entity that registered the domain name), the registration dates, the name servers, the most recent update, and the expiration date. Whois records may also provide the administrative and technical contact information (which is often, but not always, the registrant).

Here we have some ( [skillvertex.in](https://skillvertex.in) ) website details like the site owner, Registrant, Dates when was site was create, updated, expires date etc. as shown fig 2.1 and fig 2.2

### Whois Record for SkillVertex.in




— Domain Profile	
Registrant	REDACTED FOR PRIVACY
Registrant Org	N/A
Registrant Country	in
Registrar	Endurance Digital Domain Technology LLP IANA ID: 801217 URL: <a href="https://publicdomainregistry.com/">https://publicdomainregistry.com/</a> Whois Server: —
Registrar Status	clientTransferProhibited
Dates	680 days old Created on 2021-02-23 Expires on 2023-02-23 Updated on 2022-07-05
Name Servers	NS1.SKILLVERTEX.IN (has 3 domains) NS2.SKILLVERTEX.IN (has 3 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) x (f) x
IP Address	216.10.247.147 - 3 other sites hosted on this server
IP Location	 - Delhi - Delhi - P.d.r Solutions Fzc
ASN	 AS394695 PUBLIC-DOMAIN-REGISTRY, US (registered Nov 24, 2015)
IP History	2 changes on 2 unique IP addresses over 2 years
Hosting History	2 changes on 3 unique name servers over 2 years
— Website	
Website Title	 500 SSL negotiation failed:
Response Code	500

Fig 2.1 :- whois Record for skillvertex.in



**Whois Record** ( last updated on 2023-01-04 )

```
Domain Name: skillvertex.in
Registry Domain ID: DC6E9747B127A44EDBA212643CBBC4F1E-IN
Registrar WHOIS Server:
Registrar URL: https://publicdomainregistry.com/
Updated Date: 2022-07-05T10:32:34Z
Creation Date: 2021-02-23T21:09:55Z
Registry Expiry Date: 2023-02-23T21:09:55Z
Registrar: Endurance Digital Domain Technology LLP
Registrar IANA ID: 801217
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhi
bited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: N/A
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Jharkhand
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns2.skillvertex.in
Name Server: ns1.skillvertex.in
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

For more information on Whois status codes, please visit https://icann.org/epp
```

*Fig 2.2 :- whois Record for skillvertex.in*

## [2] Geo-IP Lookup :-

IP Geo-location involves attempting to discover the location of an IP address in the real world. IP addresses are assigned to an organization, and as these are ever-changing associations, it can be difficult to determine exactly where in the world an IP address is located.

```
[S] Scan Type : GEO-IP Lookup  
[GEO-IP] IP Address: 216.10.247.147  
[GEO-IP] Country: India  
[GEO-IP] State:  
[GEO-IP] City:  
[GEO-IP] Latitude: 21.9974  
[GEO-IP] Longitude: 79.0011
```

Fig 2.3 GEO-IP Lookup

Here we have a site IP-Address ( 216.10.247.147 ) we have scan this IP to discover the location of an IP address in the real world. And we got a latitude and longitude we can search on google-map for finding state and City in **fig 2.4**

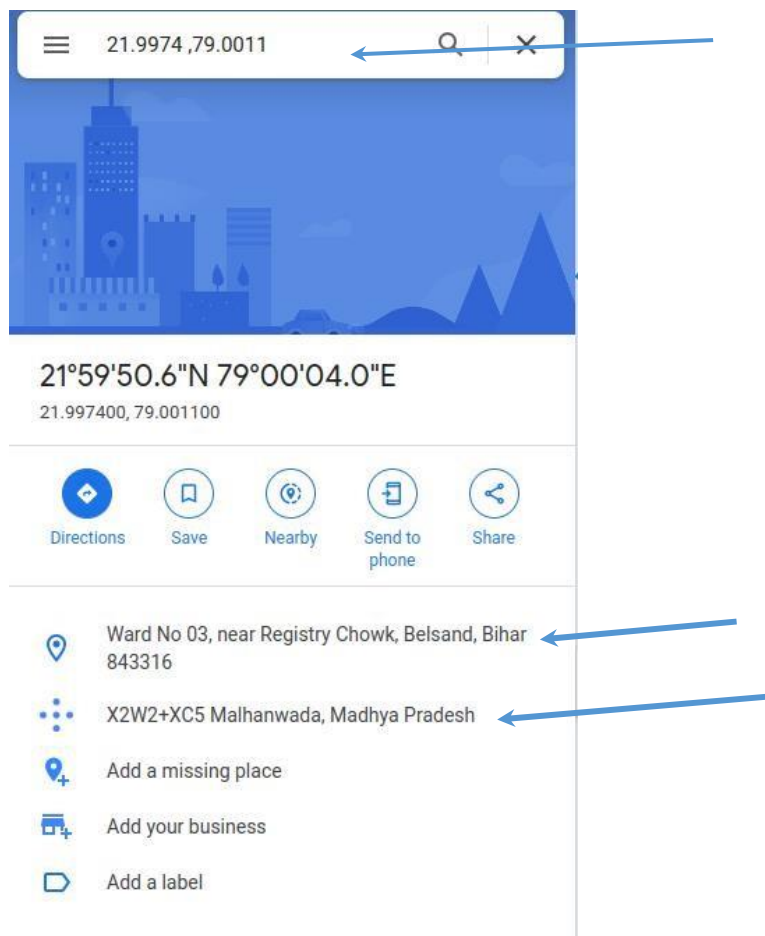
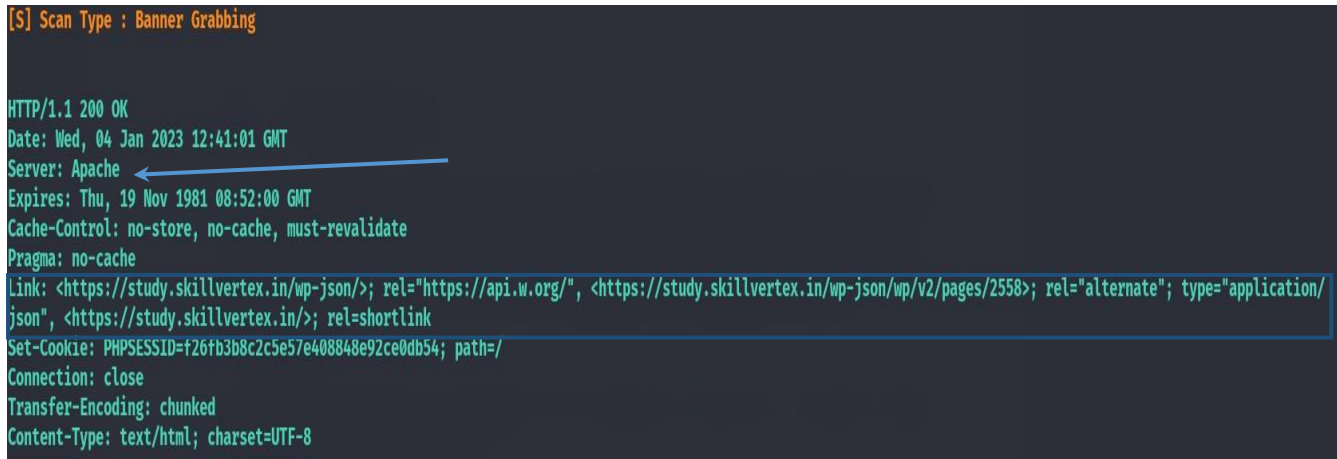


Fig 2.4 Google Map result.

### [3] Grab Banners :-

Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. However, an intruder can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.

Here Grab (grabbing) Banners has find out some details like mutiple like, server-info, Transfer-Encoding, content-type etc. in fig 3.1



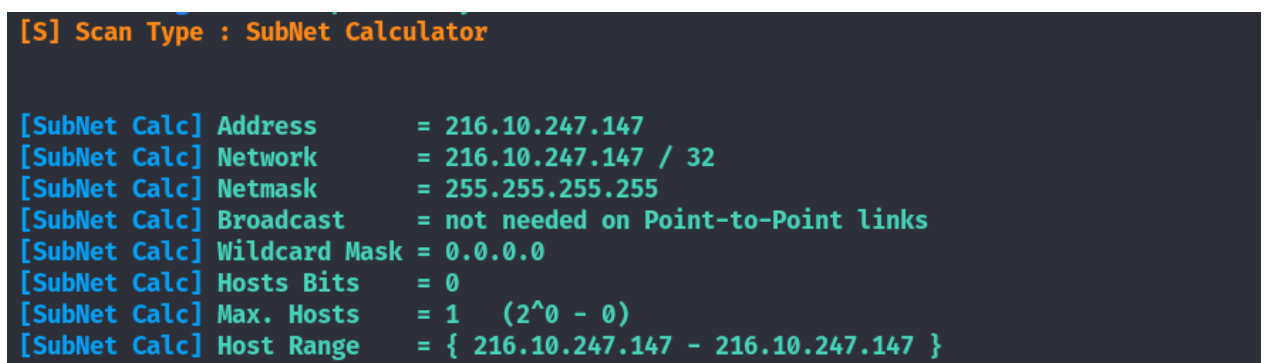
```
[S] Scan Type : Banner Grabbing

HTTP/1.1 200 OK
Date: Wed, 04 Jan 2023 12:41:01 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Link: <https://study.skillvertex.in/wp-json/>; rel="https://api.w.org/", <https://study.skillvertex.in/wp-json/wp/v2/pages/2558>; rel="alternate"; type="application/json", <https://study.skillvertex.in/>; rel=shortlink
Set-Cookie: PHPSESSID=f26fb3b8c2c5e57e408848e92ce0db54; path=/
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Fig 3.1 Banner Grabbing search result.

### [4] Subnet Calculator :-

The subnet calculator is a handy tool for finding the number of possible subnets for any given network address block. You can choose the combination of subnets and number of hosts per subnet that suits your network and get the host address range and broadcast address for any given subnet mask in fig 3.2.



```
[S] Scan Type : SubNet Calculator

[SubNet Calc] Address      = 216.10.247.147
[SubNet Calc] Network     = 216.10.247.147 / 32
[SubNet Calc] Netmask      = 255.255.255.255
[SubNet Calc] Broadcast    = not needed on Point-to-Point links
[SubNet Calc] Wildcard Mask = 0.0.0.0
[SubNet Calc] Hosts Bits   = 0
[SubNet Calc] Max. Hosts   = 1 (2^0 - 0)
[SubNet Calc] Host Range   = { 216.10.247.147 - 216.10.247.147 }
```

Fig 3.2 subnet calculator search result

## [5] NMAP Port Scan :-

Nmap is used to actively probe the target network for active hosts(host discovery), port scanning, OS detection, version details, and active services running on the hosts that are up. In fig 4.1.

```
(balwant@balwant)-[~]$ nmap study.skillvertex.in
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-04 18:56 IST
Nmap scan report for study.skillvertex.in (216.10.247.147)
Host is up (0.020s latency).
rDNS record for 216.10.247.147: 216-10-247-147.webhostbox.net
Not shown: 583 closed tcp ports (conn-refused), 403 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 125.46 seconds
```

Fig 4.1 Nmap search result

Port Scanning was conducted on the target website. Port number 80 and port 443 are open. This shows that the website is secure as HTTPS (HyperText Transfer Protocol Secure) is open. However, this needs to be monitored so that the open ports are not exploited. And there are lot of port that open ftp,ssh etc.

In this report, the focus is on the important process known as reconnaissance which is a vital step in the website hacking process. Different types of reconnaissance processes are involved to gather the essential information.

THANK YOU