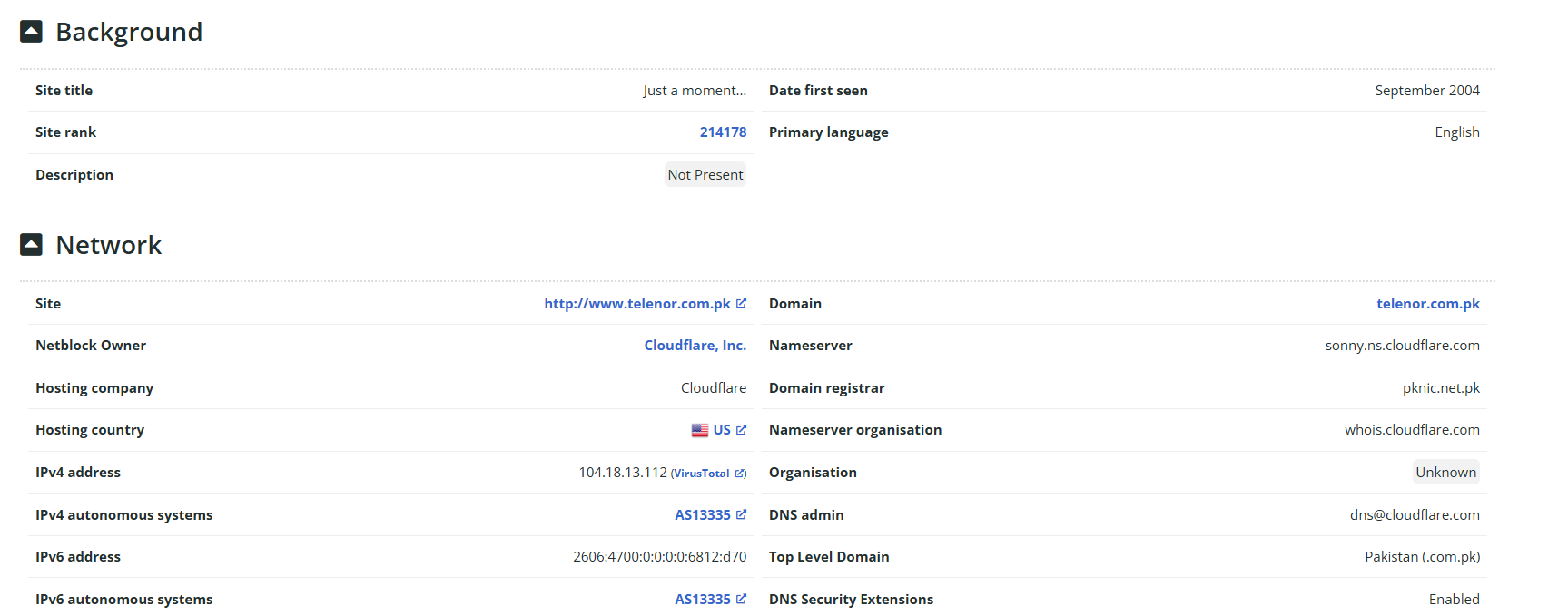
**Information Gathering:**

**LAB:**

* Download the application **xmind** from (<https://xmind.app>)
* Using OSINT, gather information about “Telenor Pakistan”
  + Company Name
  + Key Services/Product
  + Scope of Services
  + Website
    - Fully Qualified Domain Name
    - Hosting Country/Company
    - Age
    - IP Address
    - Geo Location of Web Server (longitude/latitude)
    - Technologies
    - Load Balancer / Web Application Firewall (WAF), if any
* Content Delivery Network (if any)
* Sub-domains
* Domain Registrar
* Shared Hosting (if any)

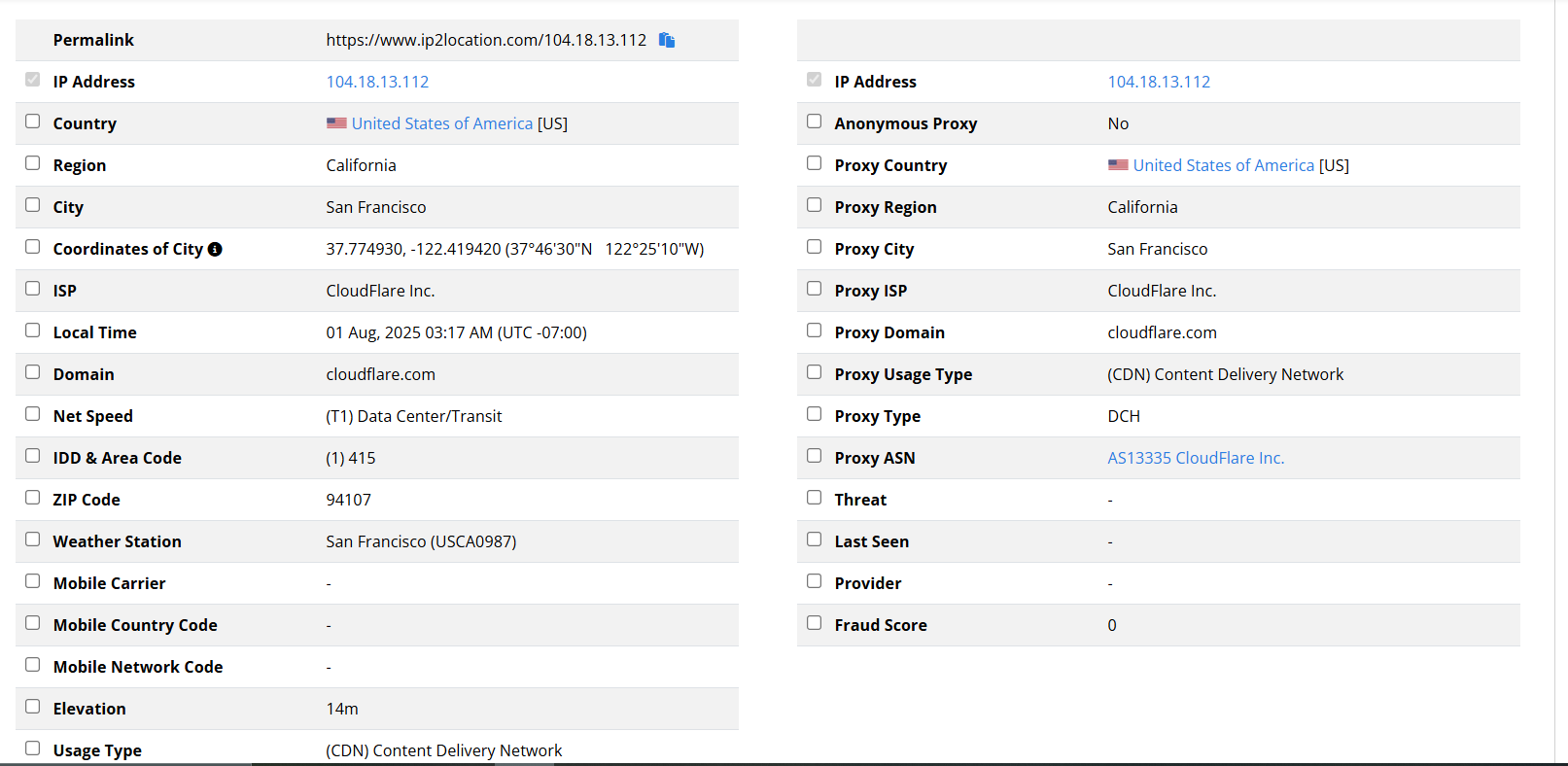
Now where to gather this information?

If you have Company name, go to **Wikipedia** for information like **“**Key services/Products, Scope of Services and its Fully Quantified Domain Name**”**. Now go to the site **Netcraft > Resources > Research tools > Site Report**. Enter the name of the domain like [www.telenor.com.pk](http://www.telenor.com.pk).



This site will tell you information like Hosting Country, Company, IP Address and some other info.

To find Geolocation, go to the site named **IP2Location**, put the IP there and it will tell you the Country, Region, City and Coordinates and some other info.

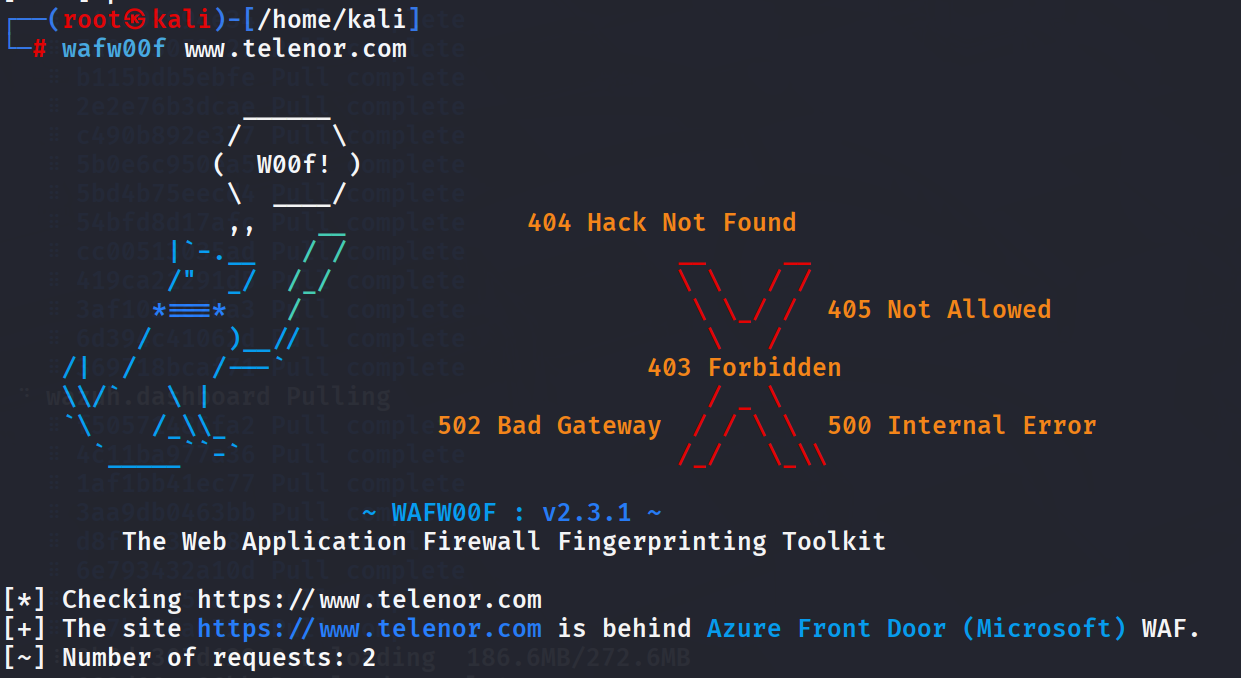


For information about Technologies like which technology are they using, use the **Wapplyzer extension**.

To find about Web Application Firewall and Load Balancers, we have built-in tools in Kali Linux.

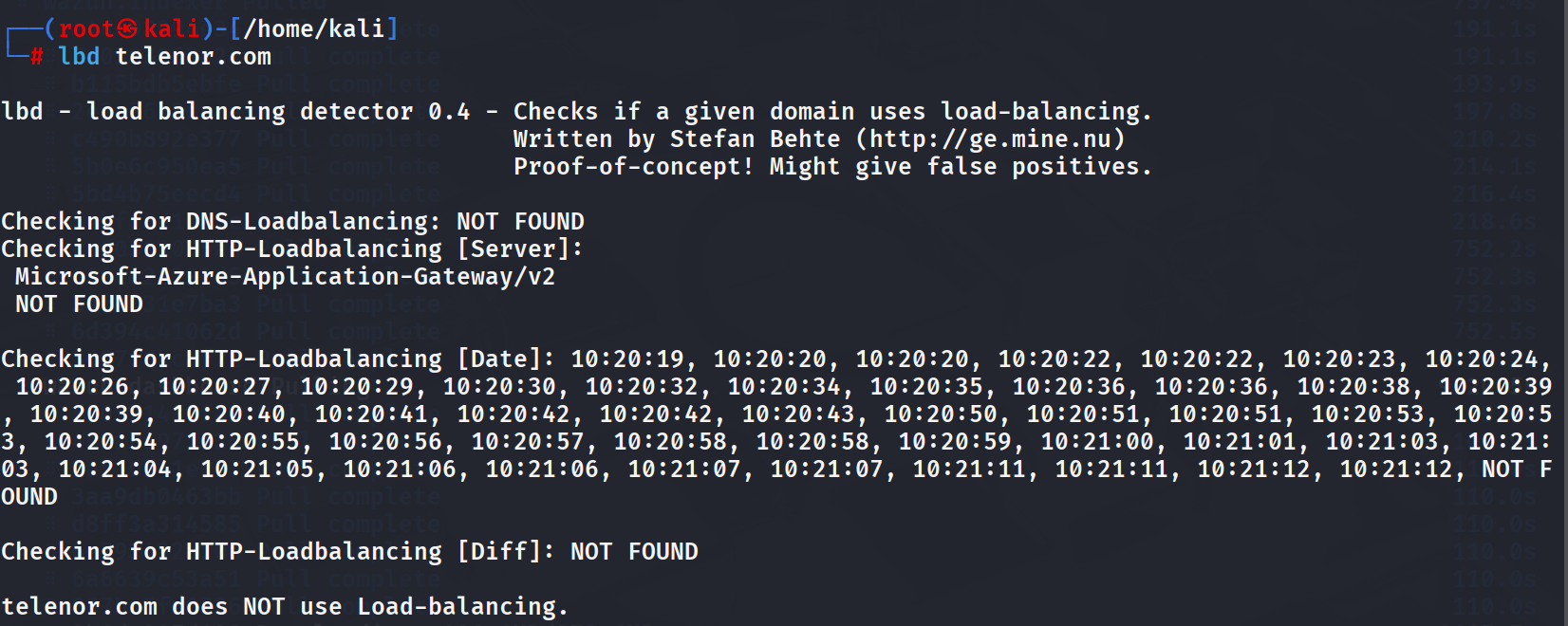
Type this in terminal to find info about WAF:

**wafw00f** [**www.telenor.com**](http://www.telenor.com) (It will tell you if they are using WAF)



Type this in terminal to find info about Load Balancer:

**lbd Telenor.com** (It will tell you if they are using Load Balancer)



**Note:** There are other tools for cross-checking like **WMtips**, **Webcheck**, **URLscan.io** (This one is more authentic)

**Finding Sub-Domains:**

**Tools for finding Sub-domains:**

* Subdomain finder (Web-based)
* Assetfinder (Linux-based)
  + Install it by typing **apt install assetfinder**
* Subfinder (Linux-based)
  + Install it by typing **apt install subfinder**
* Crt.sh (Web-based)
* Amass

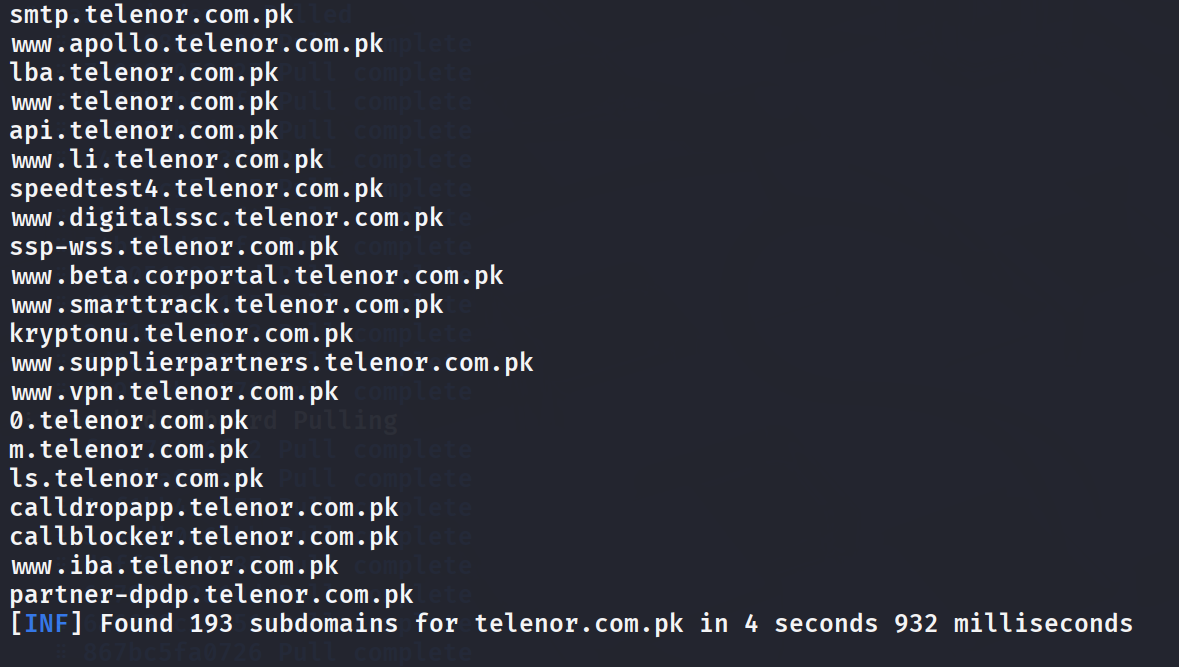
**LAB:**

* Find out sub-domains of **Telenor.com.pk** using tools mentioned above.
* Validate active sub-domains using **httprobe, httpx**(requires golang dependency)**,** & **httpx-toolkit**.
* Compare the output(active-domains) using an appropriate tool to build a final list for sub-domains.

**Procedure:**

1. Find the sub-domains about the target using tools.

e.g: **subfinder -d Telenor.com.pk**

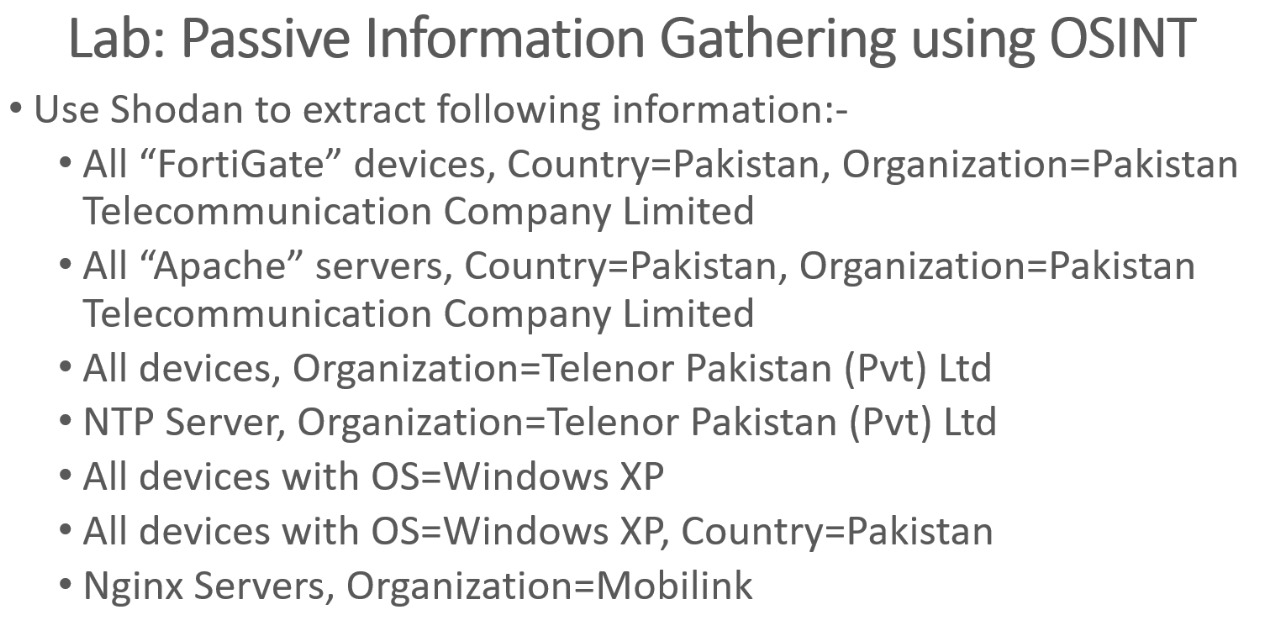


2. Copy these sub-domains and save them in a file. Suppose filename is sub-domains.txt

3. Now verify the active sub-domains using tool **httprobe** using this command:

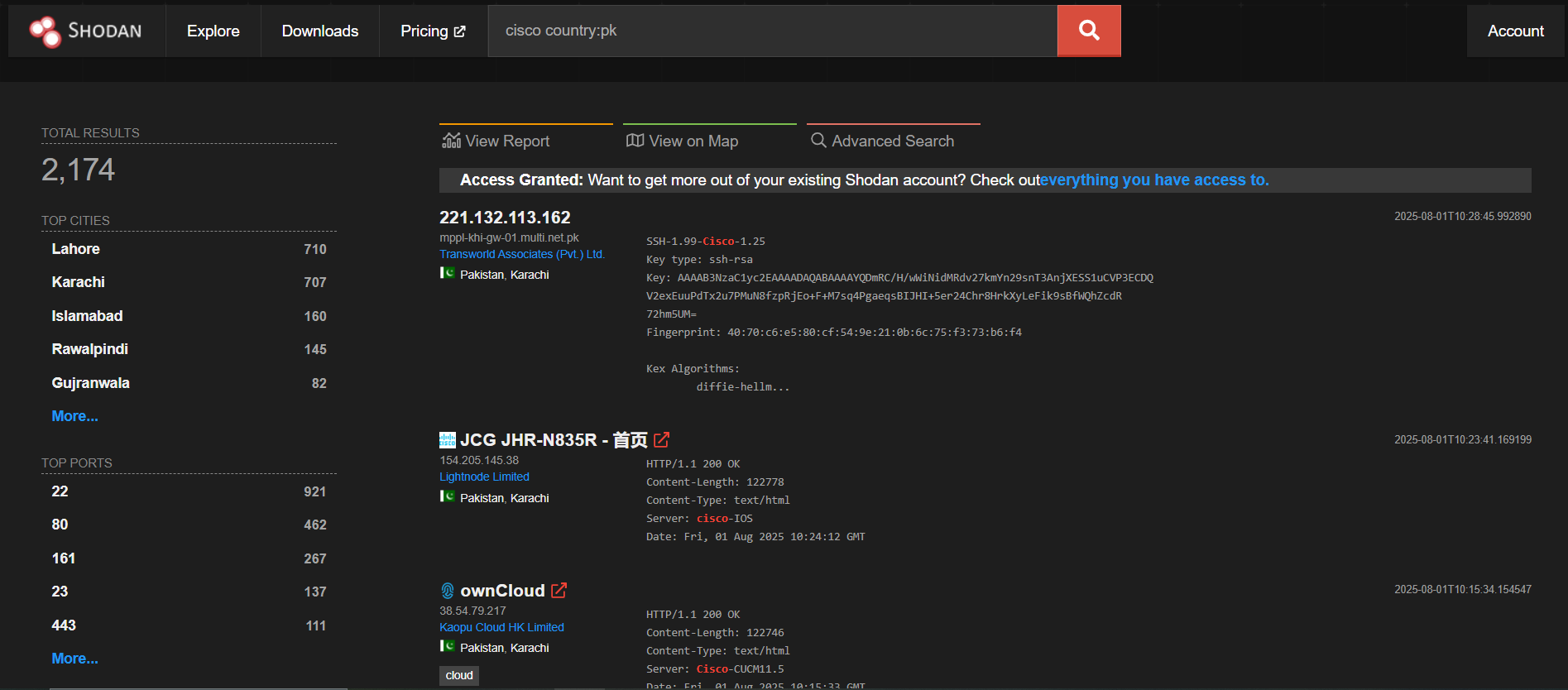
**cat sub-domains.txt | httprobe**

4. This will send probe request to every sub-domain and if he gets response he will list active sub-domains.



Suppose you want to know how many or which devices Ptcl has on its premises. This is the procedure:

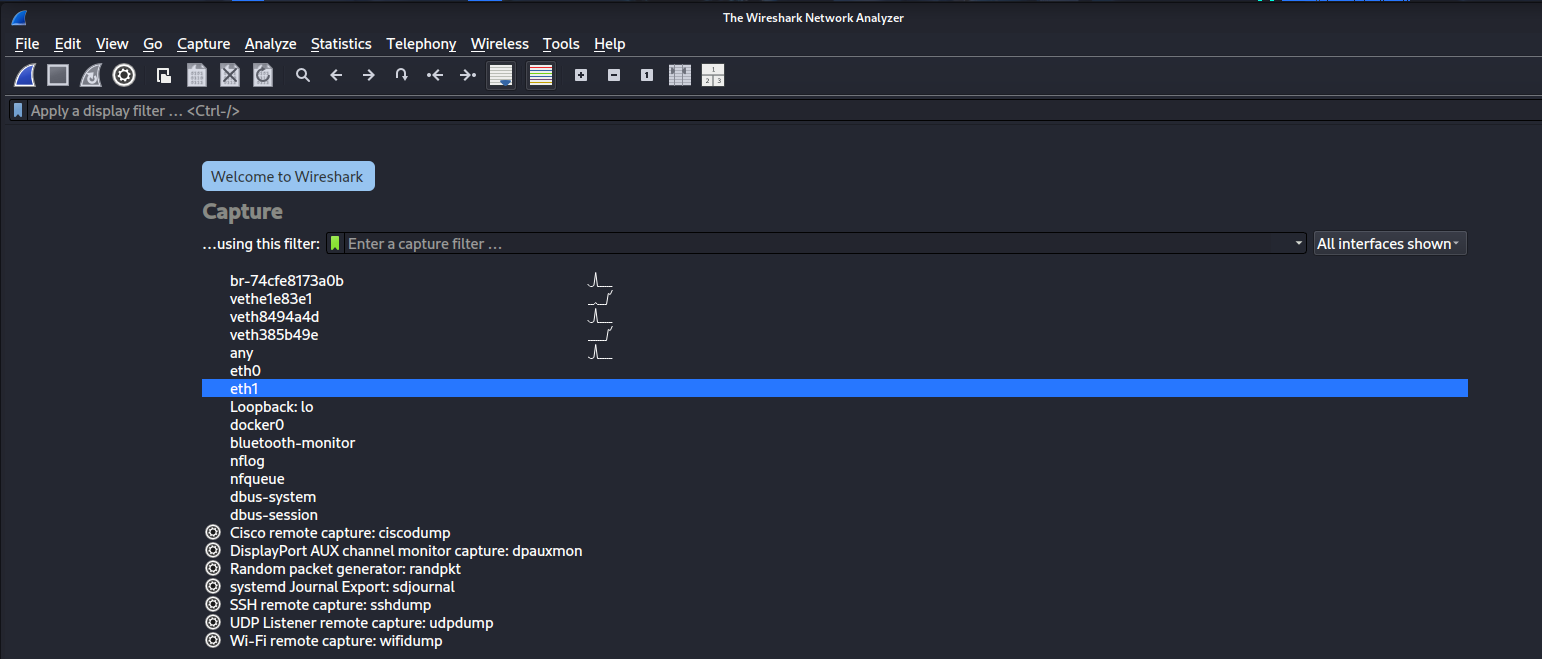
* Go to Shodan.io
* Search like this **cisco country:pk**. This will tell you how many cisco devices are in Pakistan. Then we can also check devices in specific cities.
* Similarly, type **fortigate country:pk**. It will tell you how many fortigate products are in Pakistan with their IP.



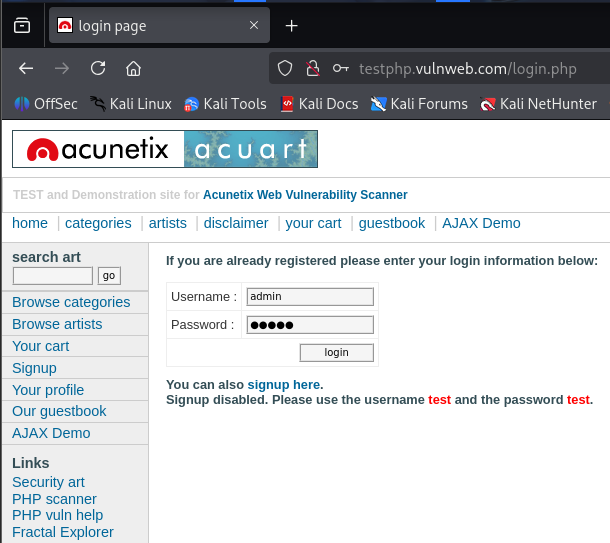
**Packet Analysis using Wireshark:**

We will be capturing packets from the **Login page** of **Vulnerable web**.

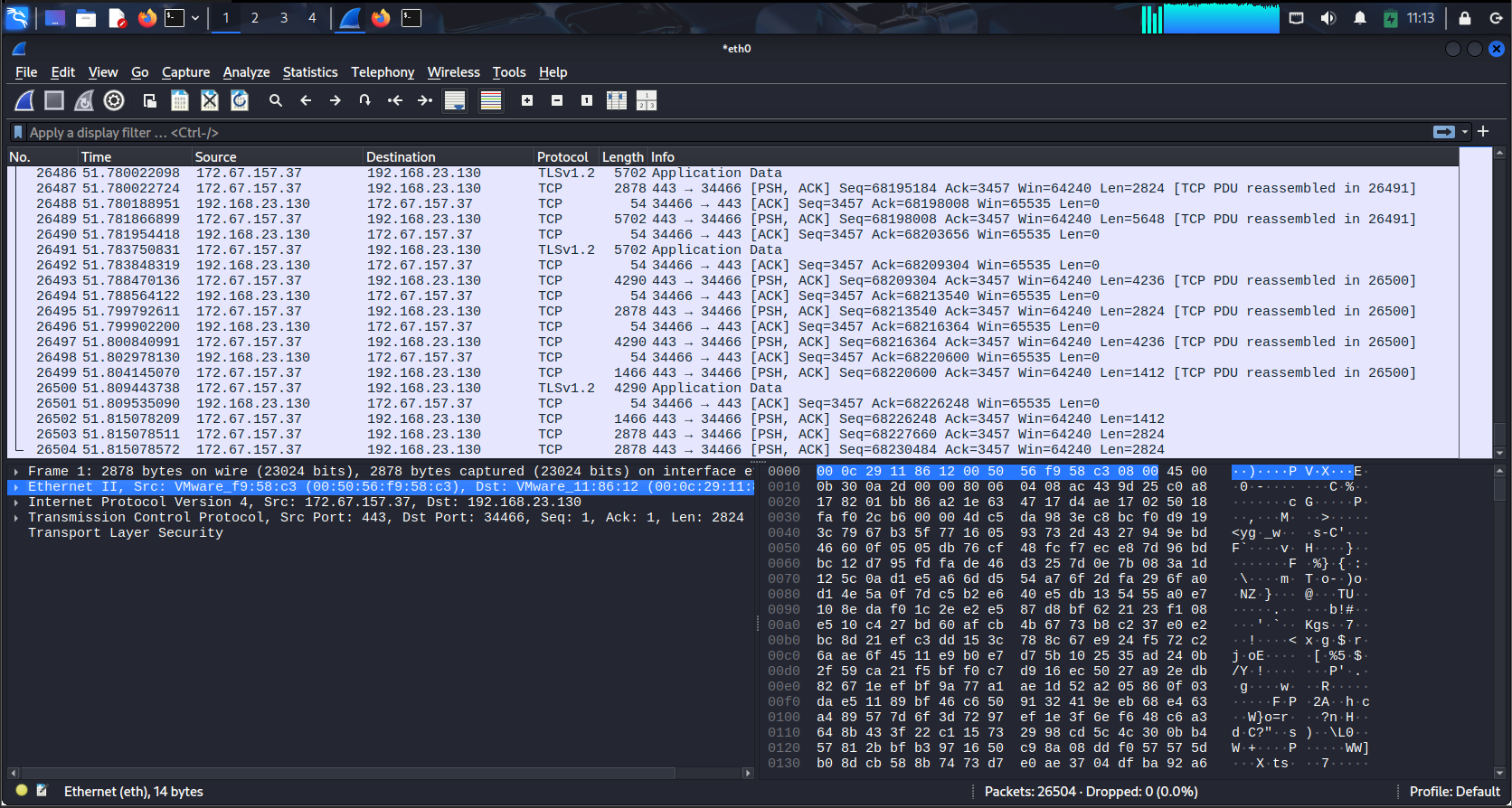
* Open Wireshark and start capturing packets.



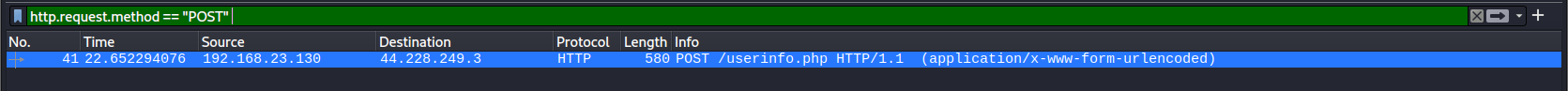
* Go to the login page of the site and enter any credentials.



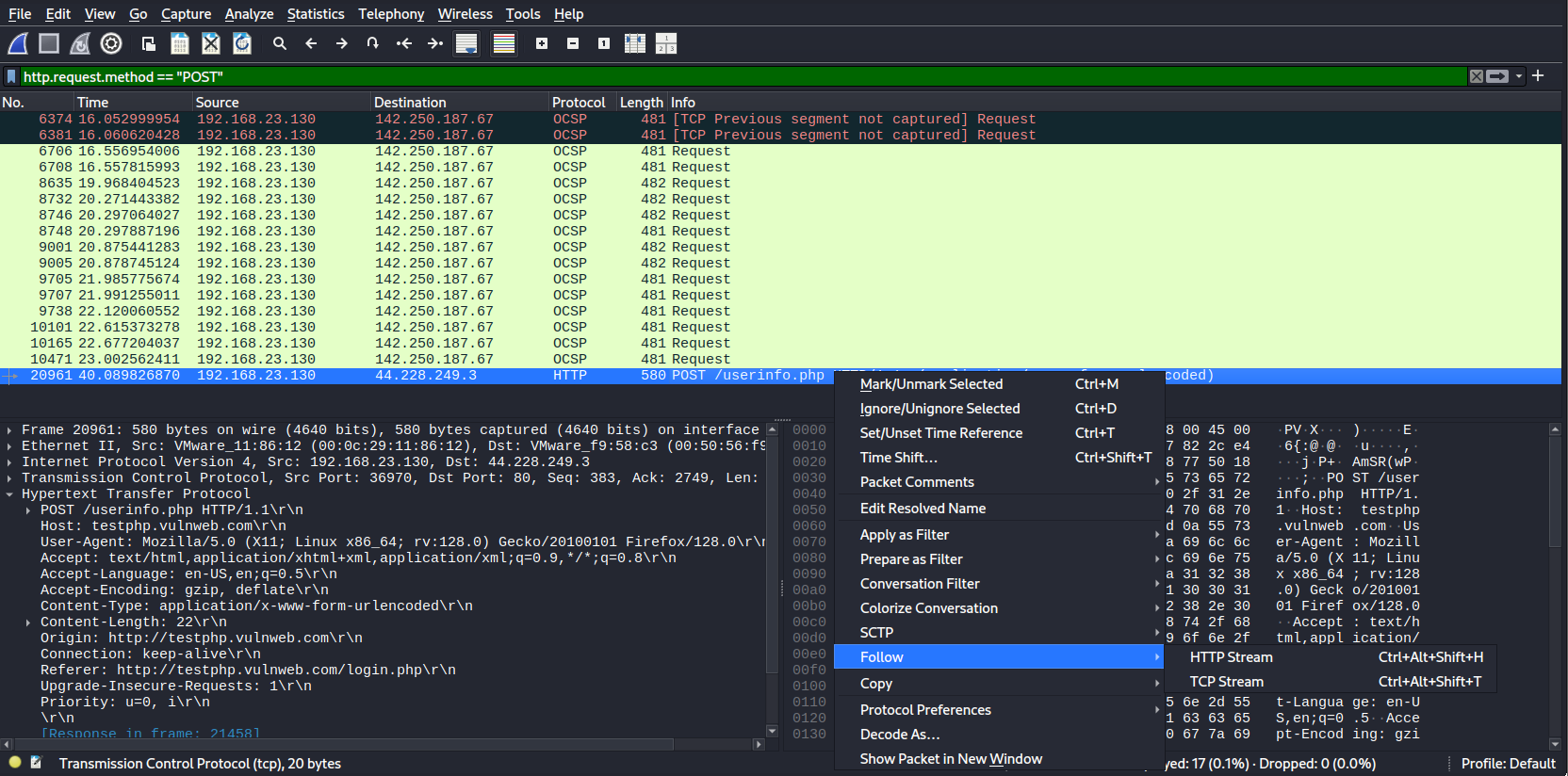
* You will see wireshark will start capturing packets.



* Apply a filter to filter out ‘**POST**’ request.



* Right click on it and follow HTTP stream.



* Scroll down until you see credentials.

