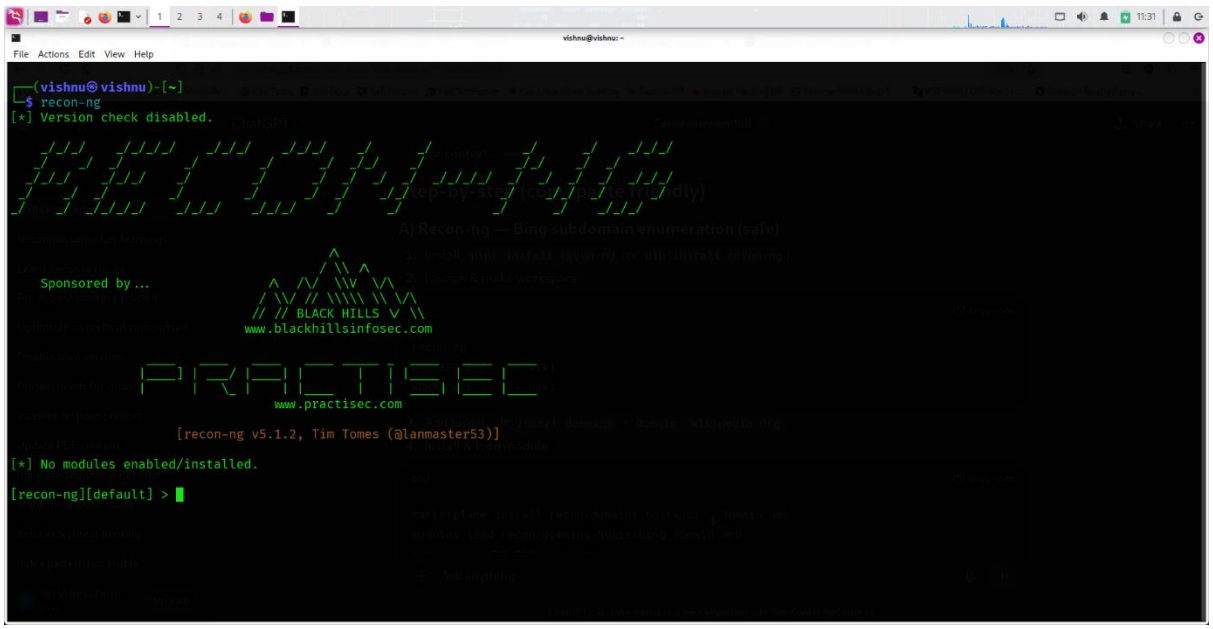
Task 1: OSINT and Recon Lab

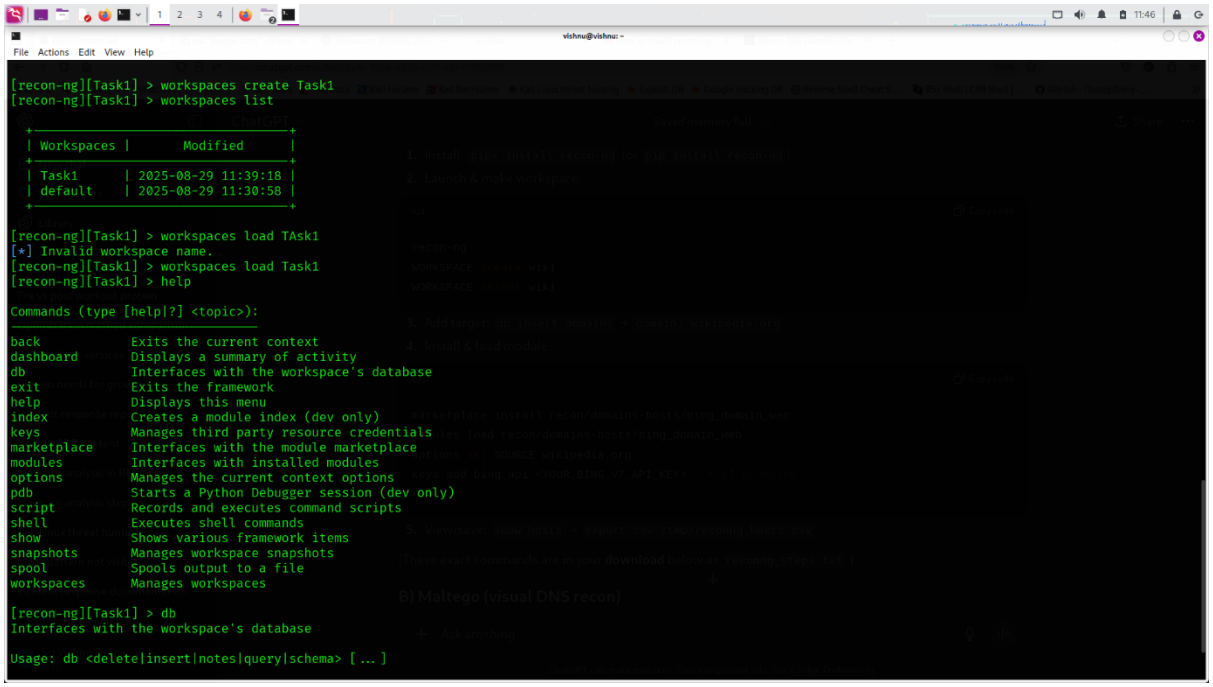
- Tasks: Enumerate subdomains and exposed services.
- Brief:
  - Subdomain Enumeration: Run Recon-ng with bing_domain_web on example.com. Log:

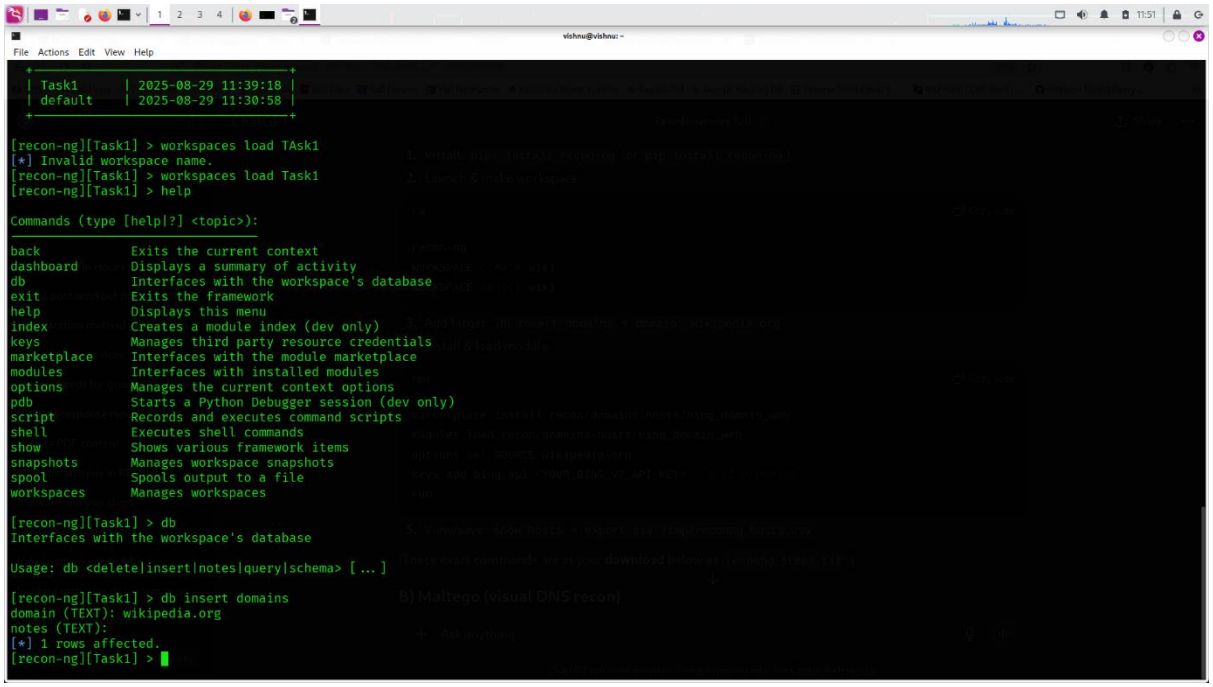
Subdomain	IP Address	Notes
www.example.com	93.184.216.34	Hosts web server
- Shodan Query: Search apache country:US; summarize 3 exposed hosts in 50 words.
- We are taking the Subdomain as ***www.wikipedia.org***.

- Open the terminal.
- Install: ***sudo apt-get update && apt-get install recon-ng.***
- *After installation of the recon-ng tool, launch the tool.* [Command: ***recon-ng***]

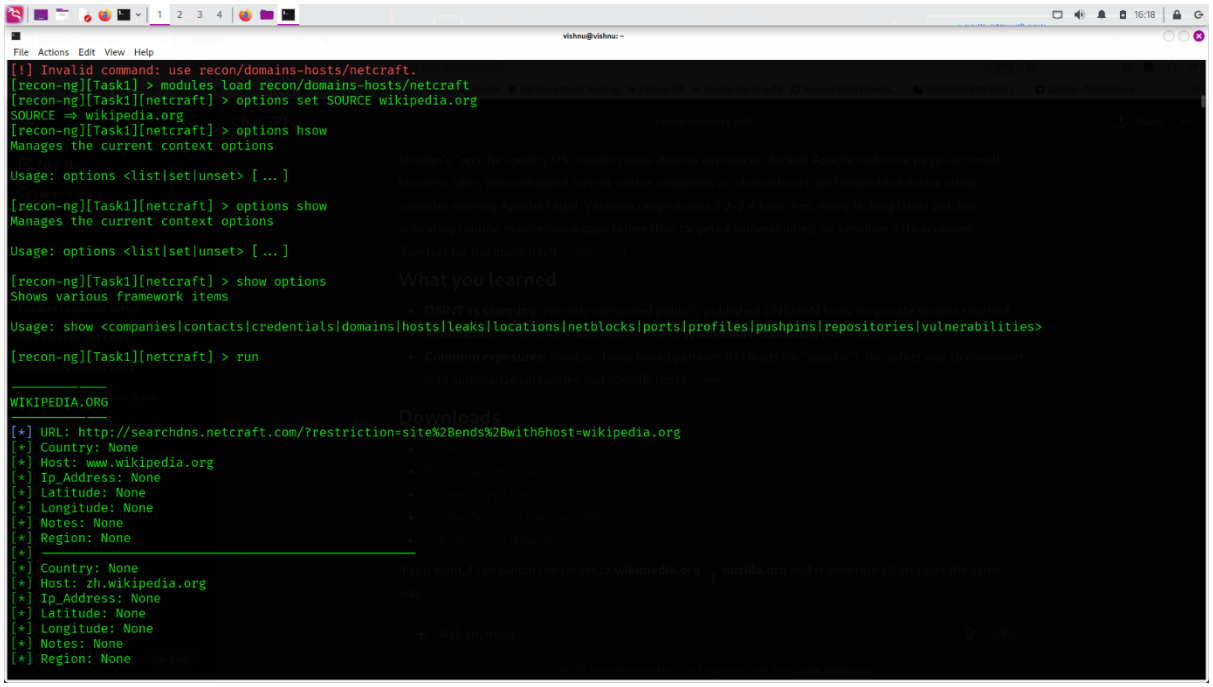


- Now, create a workspace. [Command: ***workspaces create Task1***].
- Load the workspace. [Command: workspaces load Task1].
- You can use the command ***help to list the commands that are used for the tool.***
- Command to add the target: [Command: db insert domains] --> Click Enter.
- Then add the domain name: wikipedia.org, --> Click Enter, and Click Enter again, leave the notes blank, or you could give a note to it.



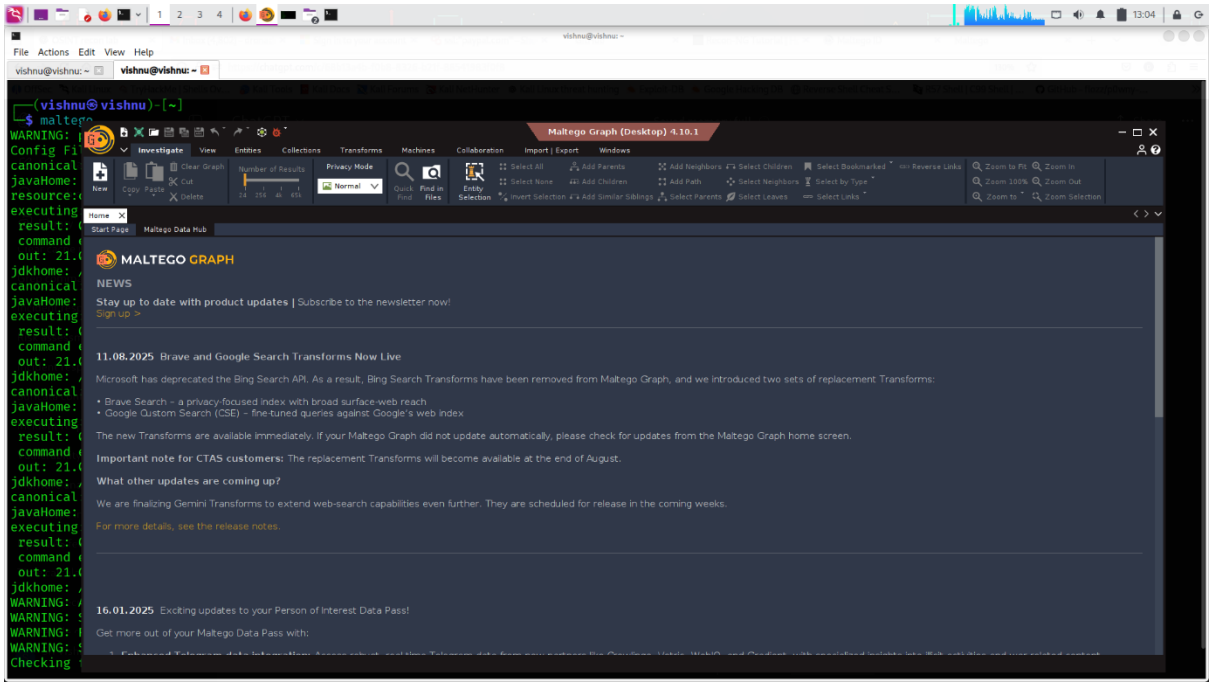


- Install this module. ***[Command: marketplace install recon/domains-hosts/netcraft].***
- Load the module. ***[Command: modules load recon/domains-hosts/netcraft].***
- Set the source. ***[Command: options set SOURCE wikipedia.org].***
- ***Then run.***



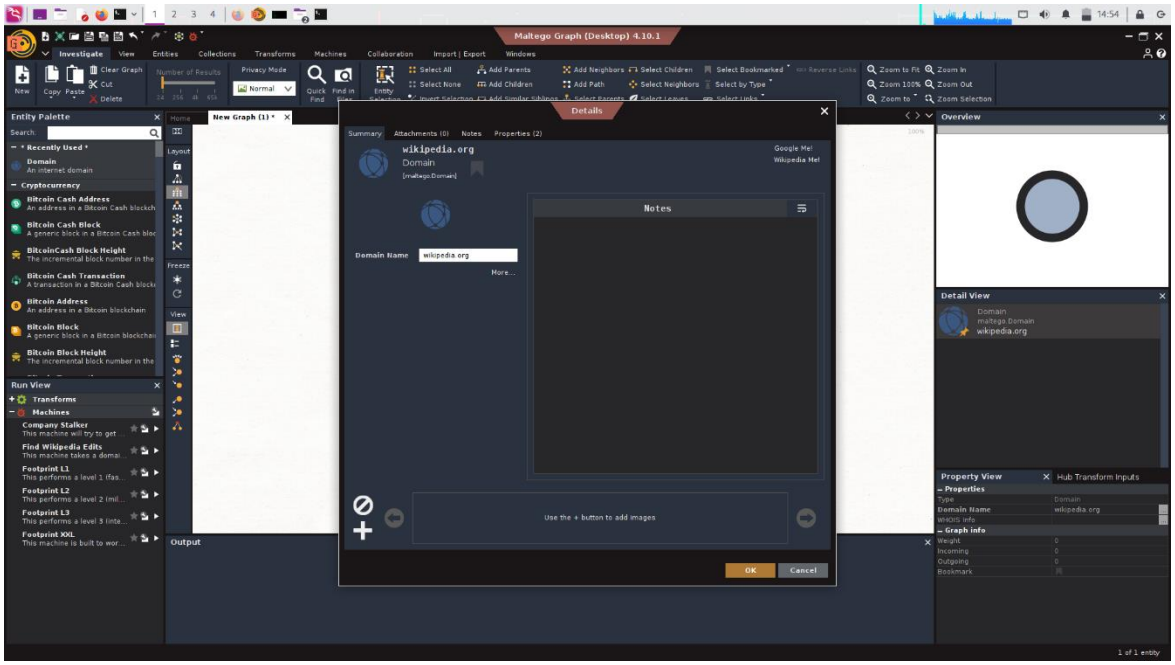
Found 213 hosts…

Maltego



- Click ***NEW*** in the top-left corner. It will create a graph board for you.
- After that, in the left Entity Palette, search for the ***domain***, [Drag it into the graph].
- Double-click on the Domain, ***Domain Name: Wikipedia.org.***

- Click ***Okay***.



- Right-click on the domain search for ***DNS.***
- Select ***[Utilities] To DNS Name [Find common DNS names].***
  mail, mx, ns, ftp, webmail, web, gateway, secure, intranet, extranet, smtp, pop, ns1, mx1, email, admin, dmz, blog, dns, forum, ntp, pub, route, sql, ssh, webaccess, xml, imap
- The above, which are highlighted, are the DNS names to test. Click run.
- You can try everything listed here:

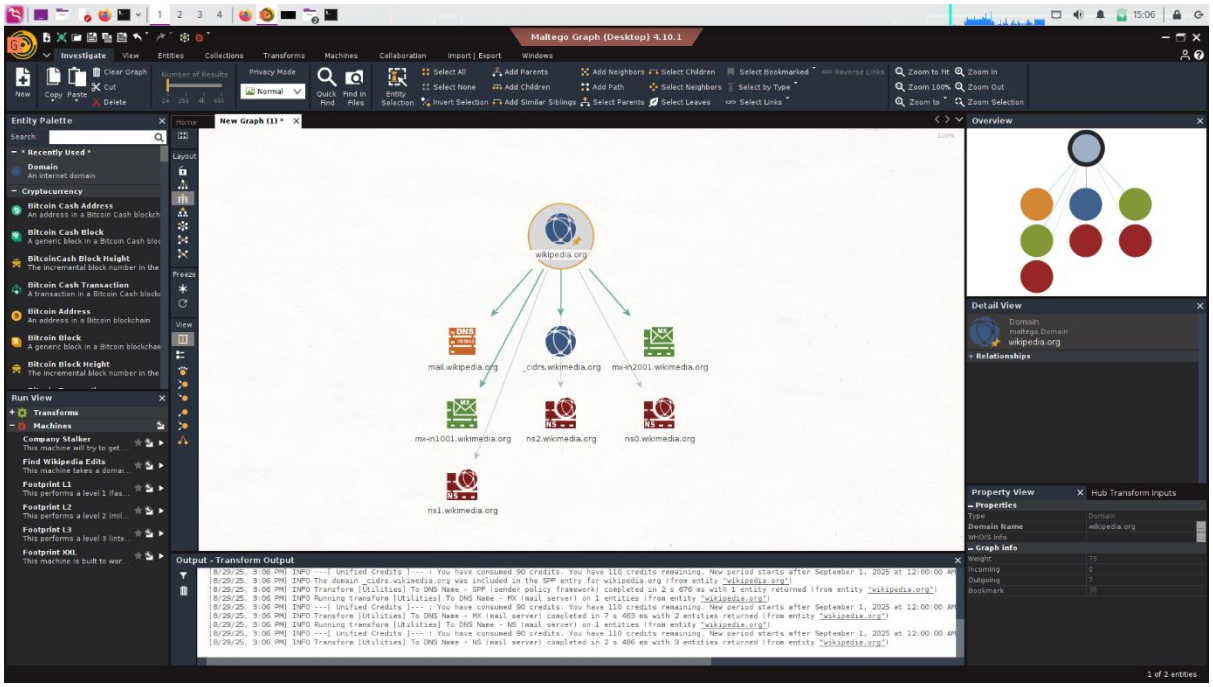
 To DNS Names → finds subdomains.

 To DNS A Record → resolves IPv4.

 To DNS AAAA Record → resolves IPv6.

 To DNS MX Record → finds mail servers.

 To DNS NS Record → finds nameservers.



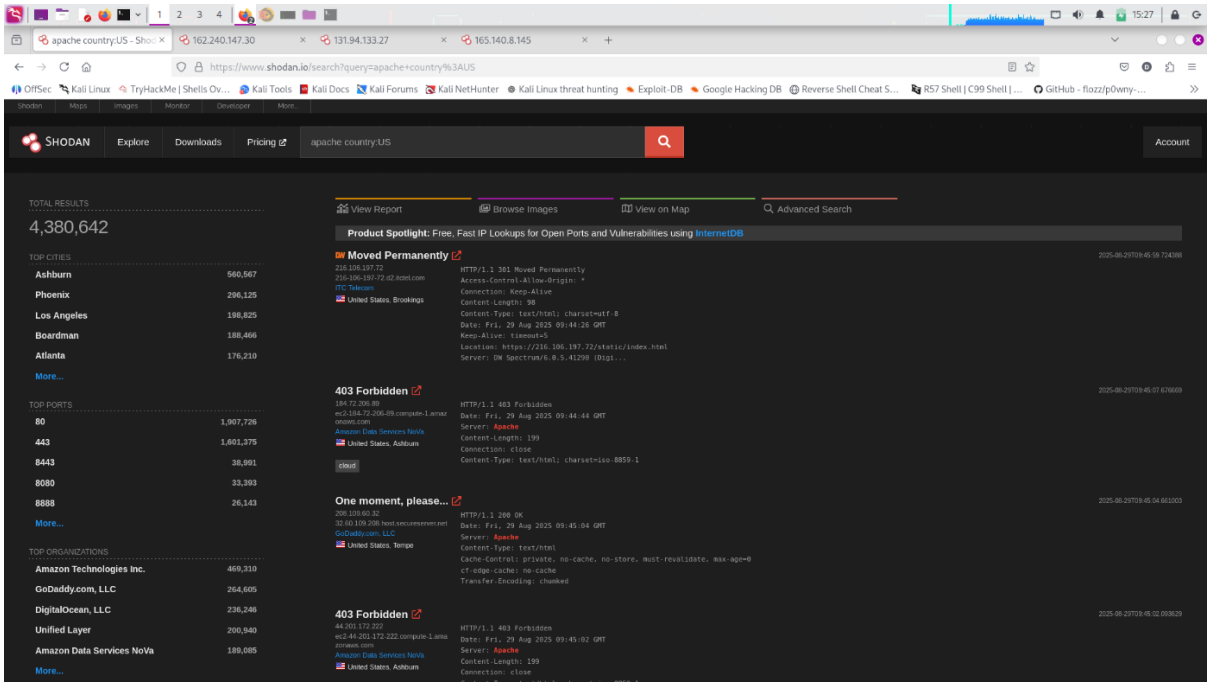
- Right-click on the DNS Name Entities ***example: mail.wikipedia.org***, then click on the ***[Utilities] To IP Address [DNS]***.

- You can save it into your system by ***Ctrl + S***.

Shodan

Shadon is a search engine that allows users to search for devices connected to the internet. This website helps to find the vulnerable devices in the network.

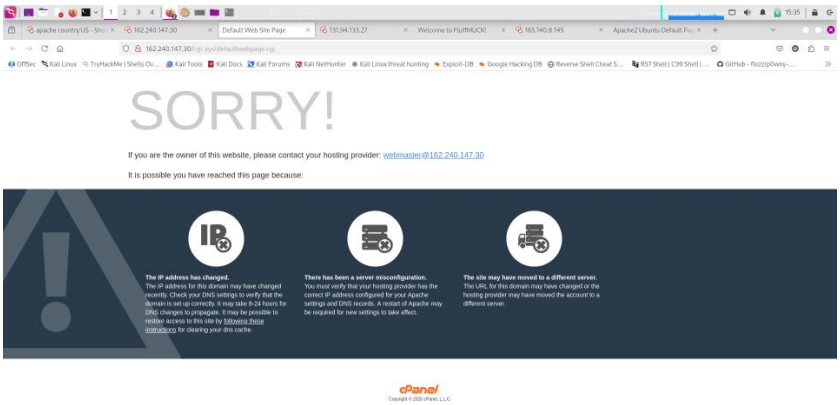
- Create an account in Shodan so that we can use the queries in the search bar.
- I have searched ***apache country:US***



- I have selected 3 exposed hosts from the above search.

✓ 1st exposed IP: **162.240.147.30**

On the first exposed IP, we could observe that in the image below:

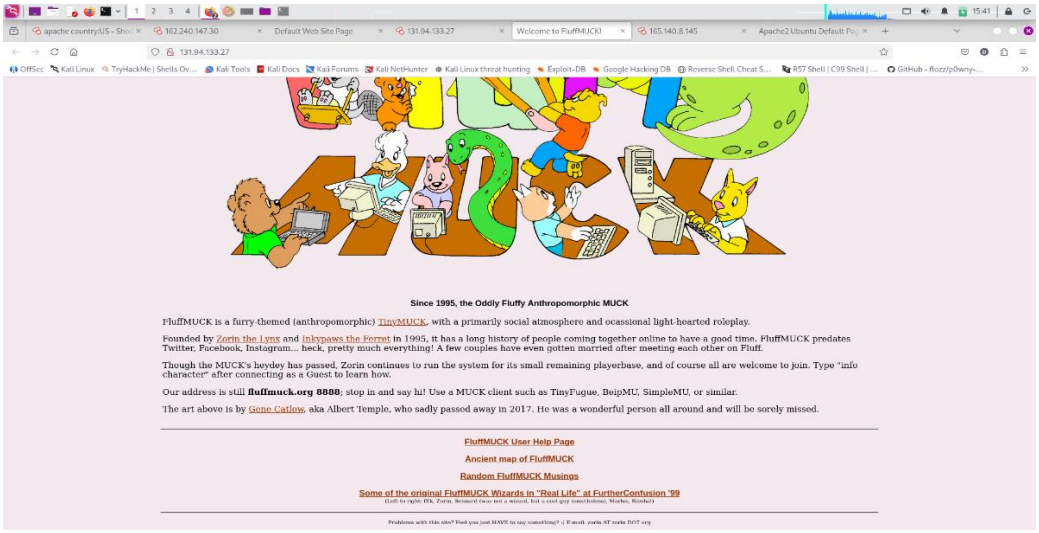


The page is a default page landing page generated by cPanel/Apache when a domain is pointing to the server, but no content (website files) is deployed.
It mentions causes such as:

1. IP address recently changed.
2. The server is misconfigured or has not yet been displayed.
3. Site moved to a different server.

✓ 2nd exposed IP: **131.94.133.27**

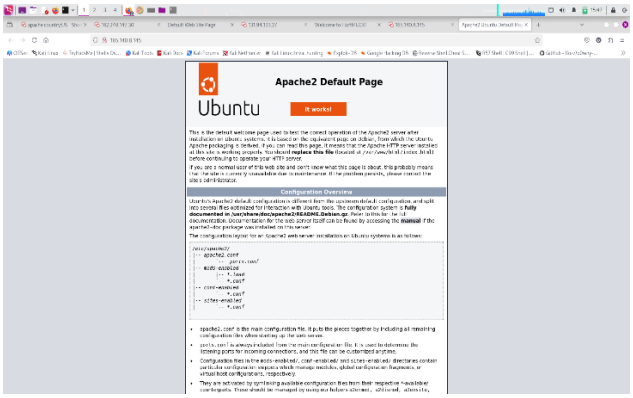
On the second exposed IP, we could observe that in the image below:



1. The page is for Furry Muck, an old text-based multiplayer game server.
2. The website runs on an Apache web server and hosts a public-facing informational page with links to community history and instructions for connecting.
3. The page also contains some references to Telnet/MUCK servers, which could indicate legacy/unsecured services running in parallel.

✓ 3rd exposed IP: **165.140.8.145**

On the second exposed IP, we could observe that in the image below:



1. The page is the default Apache2 index page on Ubuntu after installation.\
2. It confirms the server is running Apache2 correctly, but has not been configured with a real website yet.
3. The page also reveals details about the configuration structure on Ubuntu systems (/etc/apache2/ sites-enabled/, mods-enabled/).

Finally, I could say:

◈ Image 1 – cPanel Default Page

Possible Attack:

- Brute-force / credential stuffing attacks against the cPanel login (if accessible).
- Attackers often look for exposed cPanel to gain full hosting account access.

◈ Image 2 – Furry MUCK Page (Legacy Game Site)

Possible Attack:

- Exploitation of outdated services (e.g., Apache vulnerabilities or Telnet service exploitation).
- Could allow remote code execution (RCE) or man-in-the-middle attacks if Telnet is still running (since Telnet sends data in plaintext).

◈ Image 3 – Ubuntu Apache2 Default Page

Possible Attack:

- Information disclosure → targeted exploits.
- Since it reveals Ubuntu + Apache2, attackers can launch version-specific exploits (e.g., CVE-2017-5638 Apache Struts RCE, Apache path traversal, DoS, etc.).