Free vps for hacking and bug bounty hunting.

loyalonlytoday

.

Follow

Published in

OSINT Team

5 min read

.

Oct 26, 2024

Listen

Share

More

>> NOTE: HERE IS THE LINK FOR NON-PAID MEMBERS → CLICKHERE <<

Hello all.

Welcome back.

In this blog will we see . 2 free vps for hacking and bug bounty things.

What is vps?

A Virtual Private Server (VPS) is a hosting solution that combines elements of both shared and dedicated hosting. It utilizes virtualization technology to partition a single physical server into multiple virtual servers, each with its own dedicated resources, such as CPU, RAM, and storage.

This setup allows users to operate their own virtual machines (VMs) that function independently from one another.

What is the advantage of vps?

- Enhanced Performance: VPS provides dedicated resources (CPU, RAM, and bandwidth) that are not shared with other users, ensuring better performance and faster loading times compared to shared hosting, where resources are pooled among multiple sites
- Scalability: VPS hosting allows for easy scaling of resources to accommodate traffic spikes or increased demand. Users can upgrade their plans with minimal downtime, which is crucial for growing websites
- Full Control and Customization: Users have root access to their VPS, allowing them to install custom software,

configure server settings, and optimize their environment according to specific needs. This level of control is not available in shared hosting

- Improved Security: VPS environments are isolated from one another, providing an added layer of security. This isolation protects users from potential threats posed by neighboring sites on a shared server
- Additionally, users can implement their own security measures, such as firewalls and intrusion detection systems.
- Cost-Effectiveness: While VPS is generally more expensive than shared hosting, it is significantly cheaper than dedicated hosting. It offers a balance of performance and cost, making it suitable for businesses that require more resources without the high costs

associated with dedicated servers

- Reliability: With dedicated resources, VPS ensures that performance is not affected by the activities of other users. This reliability is essential for businesses that require consistent uptime and performance
- Support for Resource-Intensive Applications: VPS is ideal for running applications that require significant resources, such as e-commerce platforms or resource-heavy web applications. The dedicated nature of VPS allows these applications to perform optimally under load.

So let's see our first free vps.

- Google cloud.

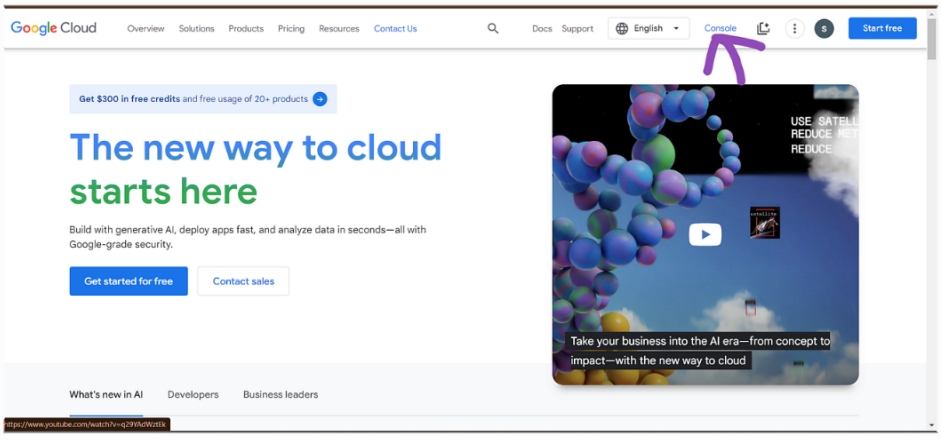
ubuntu

Click on this below link.

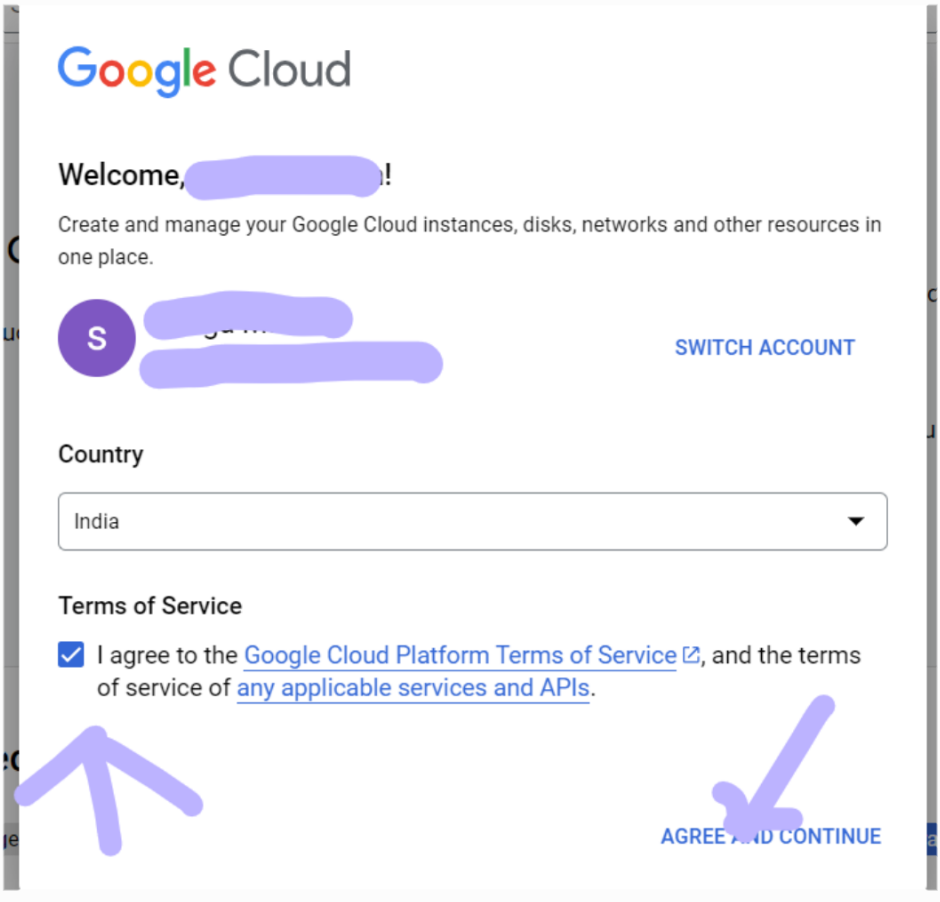
https://cloud.google.com

After you will redirects this below page.

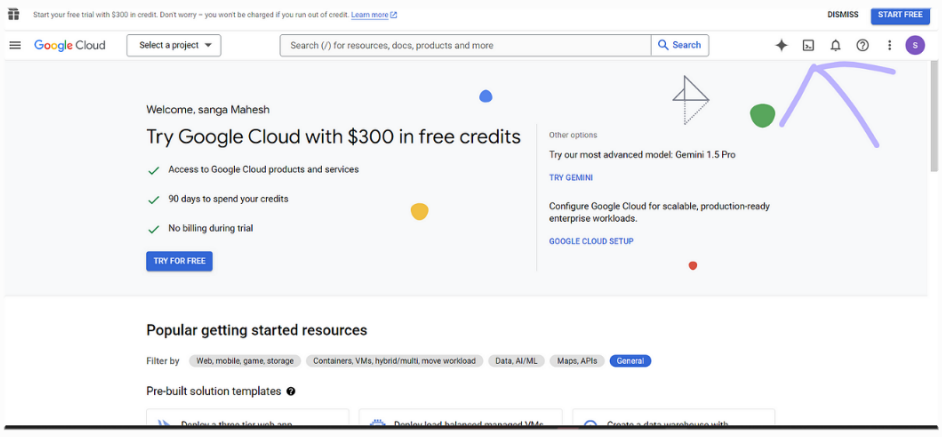
Click on console like shown in below image.



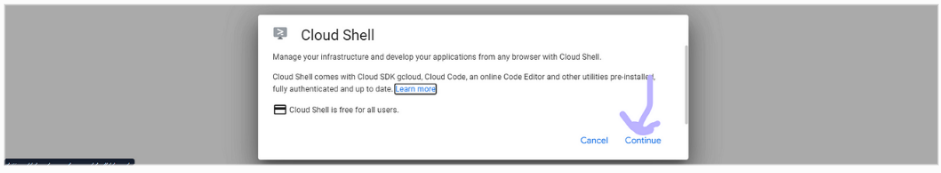
After accepting terms&conditions click on Agree&continue.



After click on console. like shown in below image.

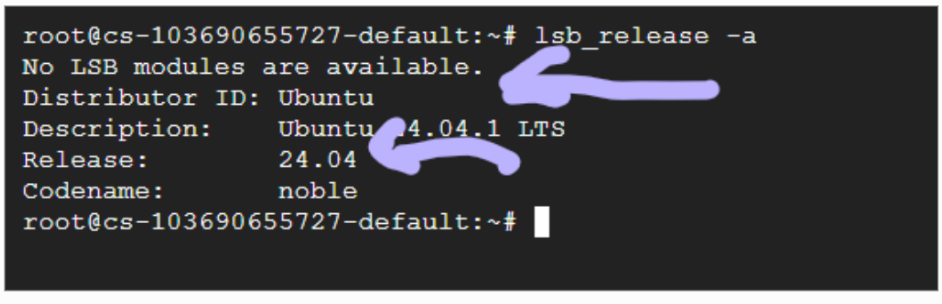
- 

Click on continue.

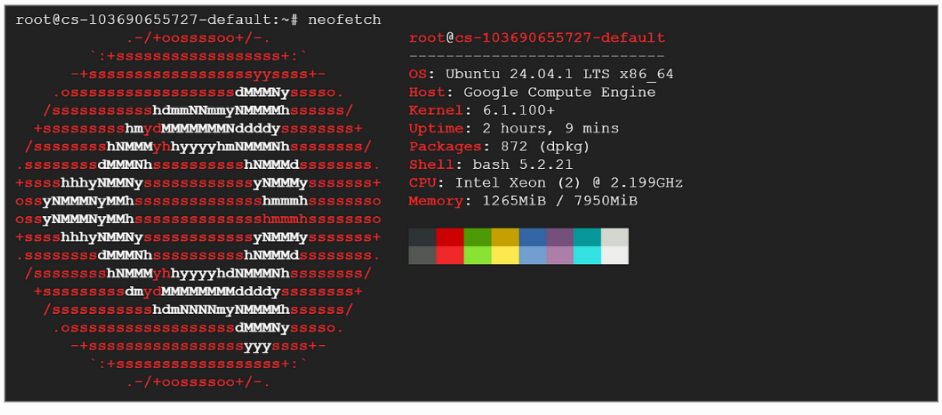
- 

run **sudo su** to root.

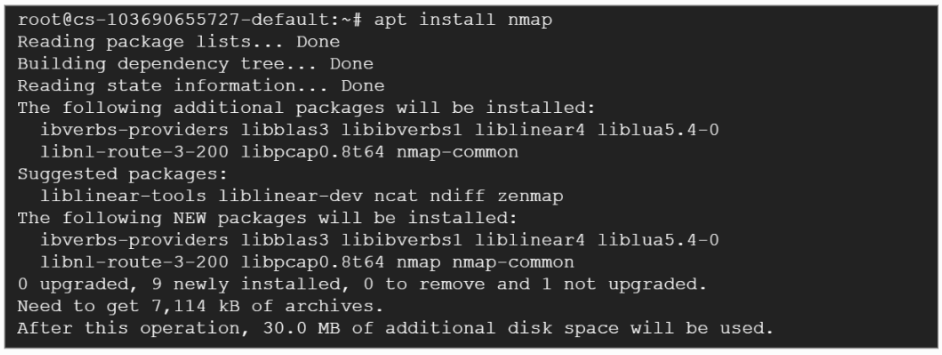
After enter this **lsb_release -a** to check version and os. this is a ubuntu os.

- 

Lets's try and run nmap in this

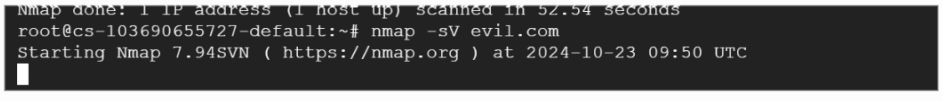
- 

apt install nmap

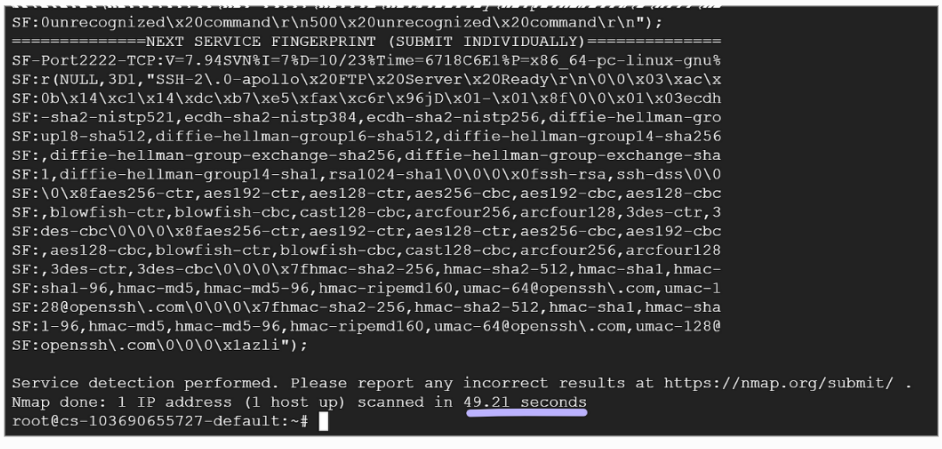
- 
```
root@cs-103690655727-default:~# apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ibverbs-providers libblas3 libibverbs1 liblinear4 liblua5.4-0
  libnl-route-3-200 libpcap0.8t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  ibverbs-providers libblas3 libibverbs1 liblinear4 liblua5.4-0
  libnl-route-3-200 libpcap0.8t64 nmap nmap-common
0 upgraded, 9 newly installed, 0 to remove and 1 not upgraded.
Need to get 7,114 kB of archives.
After this operation, 30.0 MB of additional disk space will be used.
```

running a scan on evil.com with nmap

in vps

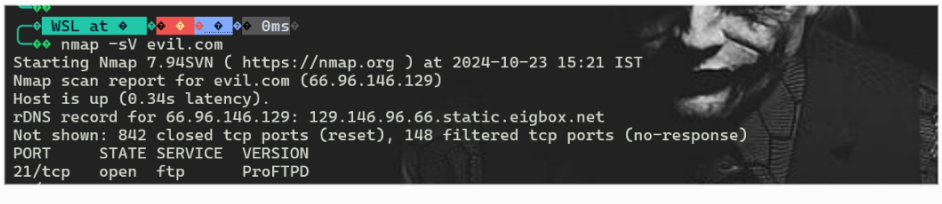
- 
```
Nmap done: 1 IP address (1 host up) scanned in 52.54 seconds
root@cs-103690655727-default:~# nmap -sV evil.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 09:50 UTC
```

in 49 seconds.

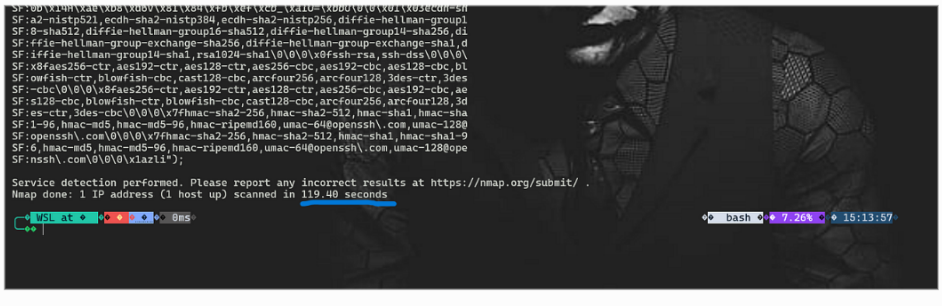
- 
```
SF:0unrecognized\x20command\r\n500\x20unrecognized\x20command\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port2222-TCP:V=7.94SVN%I=7%D=10/23%Time=6718C6E1%P=x86_64-pc-linux-gnu%
SF:r(NULL,3D1,"SSH-2\.0-apollo\x20FTP\x20Server\x20Ready\r\n\0\0\x03\xac\x
SF:0b\x14\xc1\x14\xdc\xb7\xe5\xfax\xc6r\x96jD\x01-\x01\x8f\0\0\x01\x03ecdh
SF:-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-gro
SF:up18-sha512,diffie-hellman-group16-sha512,diffie-hellman-group14-sha256
SF:,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha
SF:1,diffie-hellman-group14-sha1,rsa1024-sha1\0\0\0\x0fssh-rsa,ssh-dss\0\0
SF:\0\x8faes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,aes128-cbc
SF:,blowfish-ctr,blowfish-cbc,cast128-cbc,arcfour256,arcfour128,3des-ctr,3
SF:des-cbc\0\0\0\x8faes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc
SF:,aes128-cbc,blowfish-ctr,blowfish-cbc,cast128-cbc,arcfour256,arcfour128
SF:,3des-ctr,3des-cbc\0\0\0\x7fhmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-
SF:sha1-96,hmac-md5,hmac-md5-96,hmac-ripemd160,umac-64@openssh\.com,umac-1
SF:28@openssh\.com\0\0\0\x7fhmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha
SF:1-96,hmac-md5,hmac-md5-96,hmac-ripemd160,umac-64@openssh\.com,umac-128@
SF:openssh\.com\0\0\0\x1azli");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.21 seconds
root@cs-103690655727-default:~#
```

in wsl.

- 
```
WSL at  0ms
nmap -sV evil.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 15:21 IST
Nmap scan report for evil.com (66.96.146.129)
Host is up (0.34s latency).
rDNS record for 66.96.146.129: 129.146.96.66.static.eigbox.net
Not shown: 842 closed tcp ports (reset), 148 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD
```

in 119 seconds.

- 
```
SF:a2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group1
SF:8-sha512,diffie-hellman-group16-sha512,diffie-hellman-group14-sha256,di
SF:ffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,d
SF:iffie-hellman-group14-sha1,rsa1024-sha1\0\0\0\x0fssh-rsa,ssh-dss\0\0\0\
SF:x8faes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,aes128-cbc,bl
SF:owfish-ctr,blowfish-cbc,cast128-cbc,arcfour256,arcfour128,3des-ctr,3des
SF:-cbc\0\0\0\x8faes256-ctr,aes192-ctr,aes128-ctr,aes256-cbc,aes192-cbc,ae
SF:s128-cbc,blowfish-ctr,blowfish-cbc,cast128-cbc,arcfour256,arcfour128,3d
SF:es-ctr,3des-cbc\0\0\0\x7fhmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha
SF:1-96,hmac-md5,hmac-md5-96,hmac-ripemd160,umac-64@openssh\.com,umac-128@
SF:openssh\.com\0\0\0\x7fhmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-9
SF:6,hmac-md5,hmac-md5-96,hmac-ripemd160,umac-64@openssh\.com,umac-128@ope
SF:nssh\.com\0\0\0\x1azli");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 119.40 seconds
WSL at  0ms
bash  7.26%  15:13:57
```

You can see the time diffrence.

Now let’s see our second free vps.

2.Segfault.

kali-linux

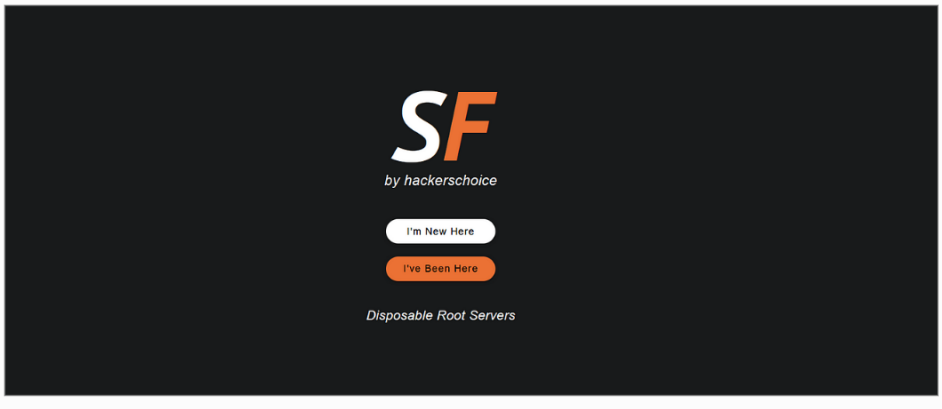
Click on this below link.

SegFault

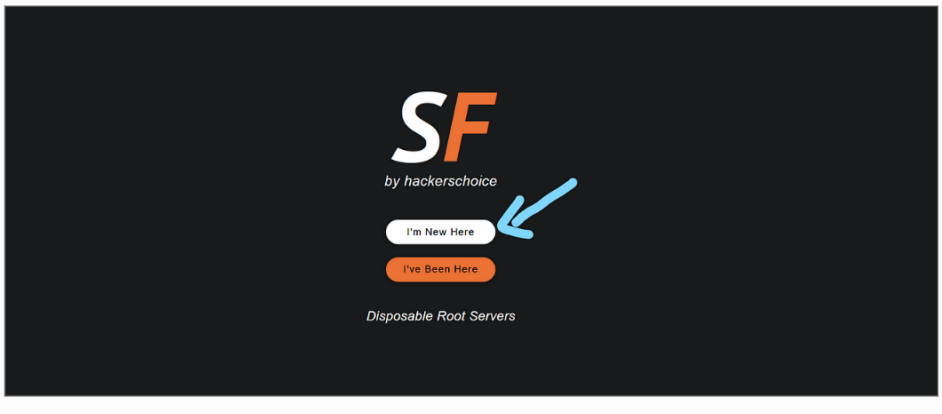
SFUI - Free root shells, powered by thc.org/segfault

shell.segfault.net

You will be redirects this page like shown in below.

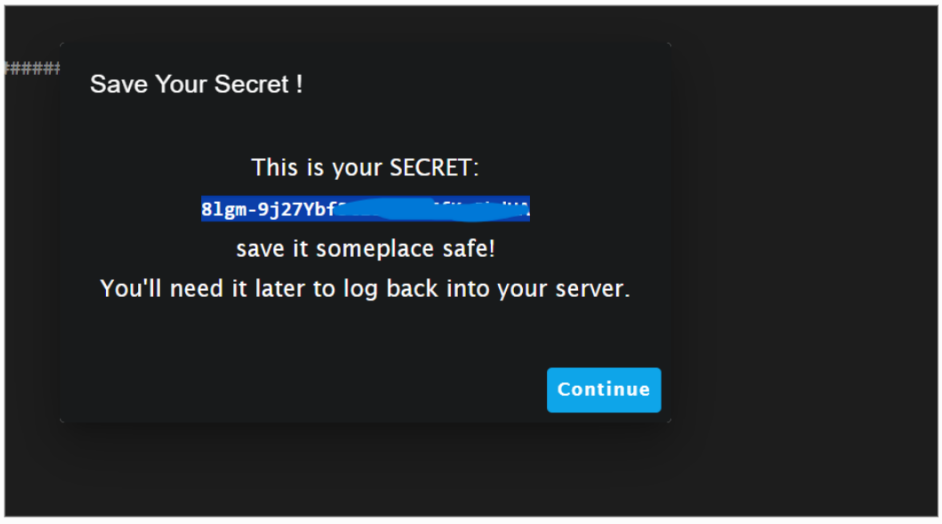
- 

Click on i’m New Here.

- 

Save your secret code.

After click on continue.

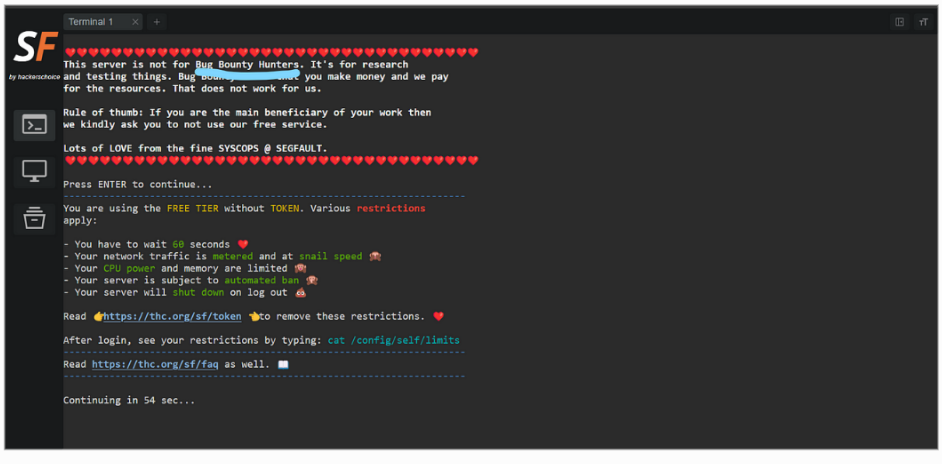
- 

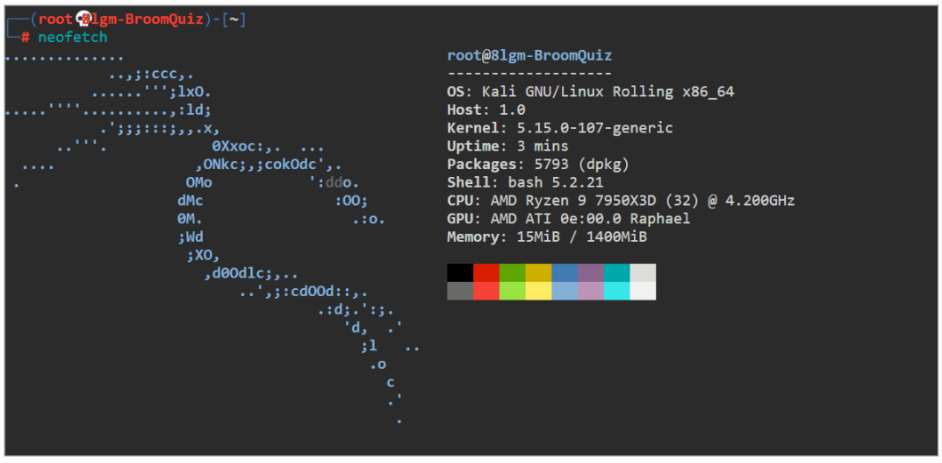
After enter any key to continue.

after wait for 60 seconds.

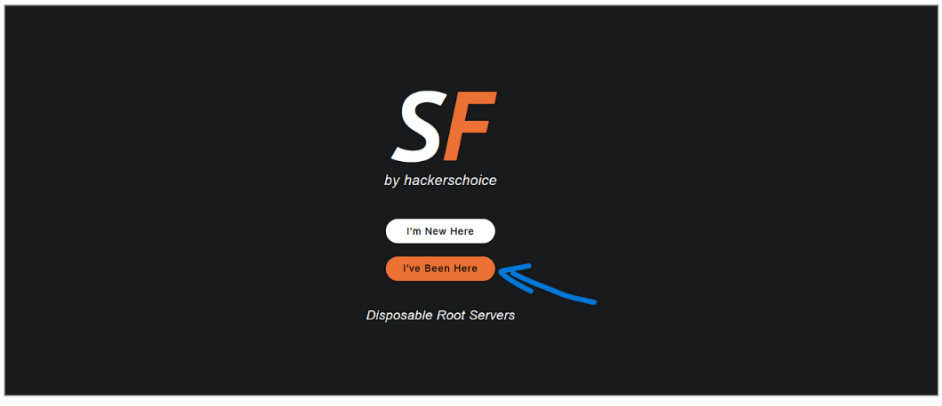
they are telling this server is not for bug hunters . any way you can use this for your bug bounty things.

If you find any bugs using this vps pls make donate some money from your finding

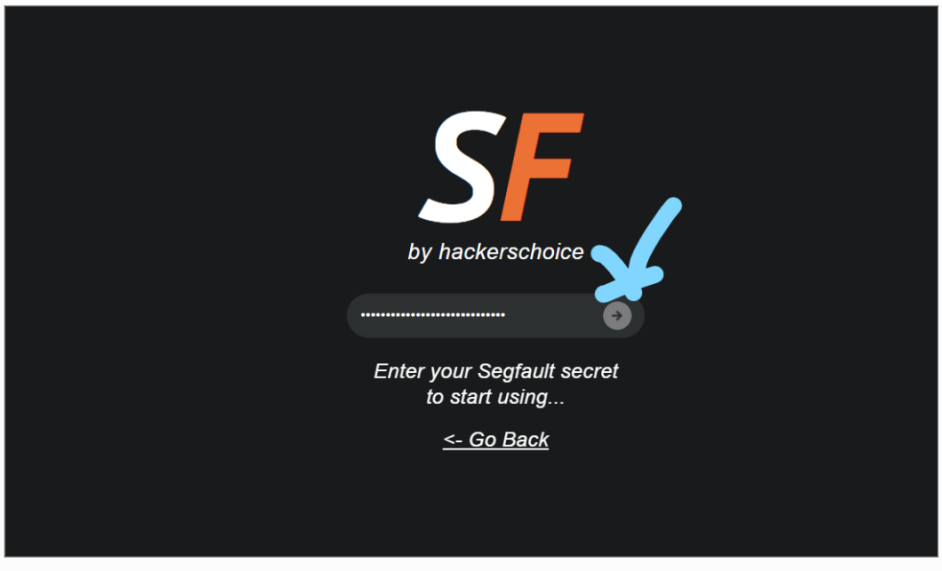
- 

- 

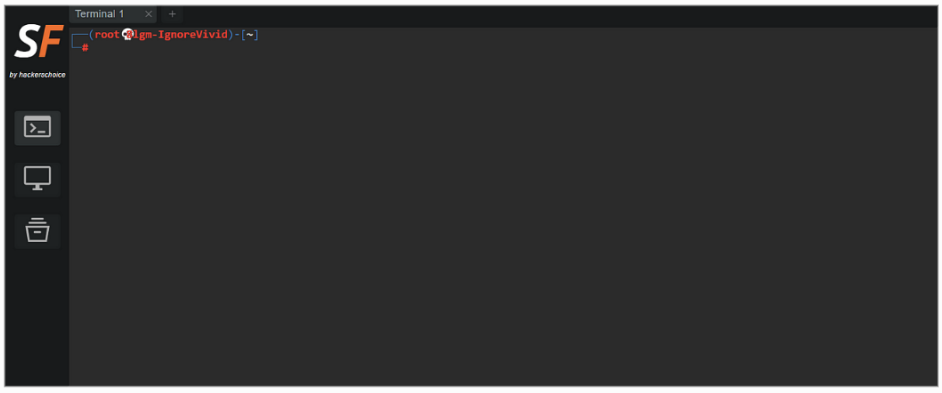
After closing . this you want to use this by your secret code.
Click on i’ve Been Here.

- 

paste your secret and click arrow sign .like shown in below image

- 

After login.

- 

That’s all for this blog.
I hope this blog will very helpful in your bug bounty journey.
If it’s really helpful . do clap . share my medium link to your friends.
It you have any doubts ask in comments.
Thanks for reading.

-