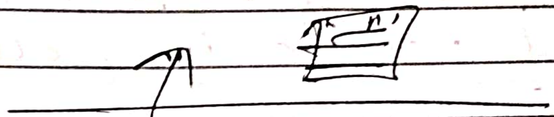
DDOS Protection System for Cloud Aws. (Testing).

EC2-Instance — Public IPv4 addr.— 13.61.188.105.

✓ Private IPv4 addr— ·172.31.24.80.

1. flask. → Hosting Site.

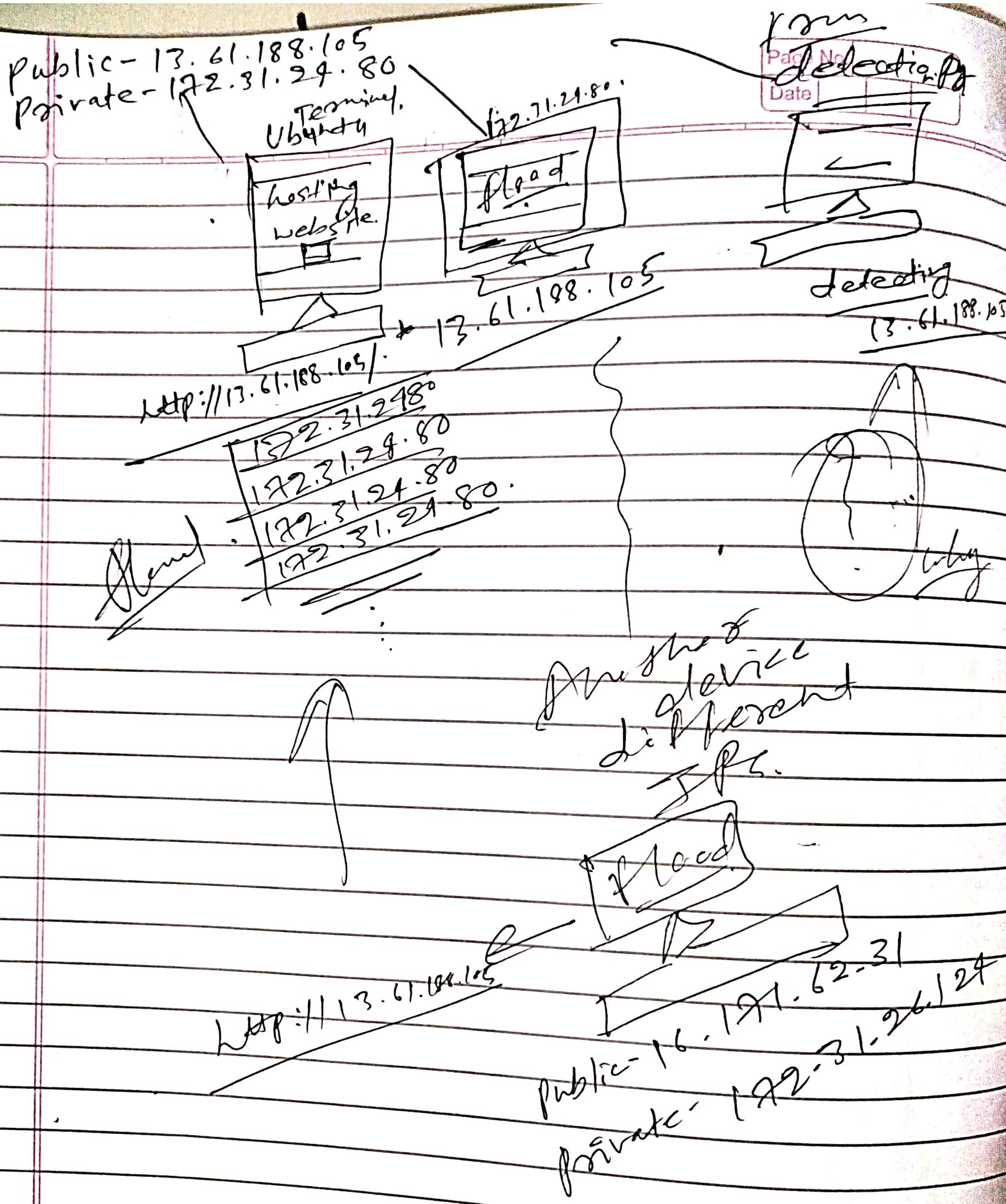


2. Sending flood. to the Side which i have hosted (hping3.)
Target is — 13.61.188.105

3. python protection Code run then — Detection (Analysis). then the ip Comes— ·172.31.24.80.

If I Create 1 more instance I Got new ip (public & private)

new Instance — (for flood) public IPv4 — 16.171.62.31
private IPv4 — 172.31.26.124.


Public- 13.61.188.105
Private- 172.31.24.80
Terminal,
Ubuntu
hosting
website.
172.31.24.80.
flood
from
detecting
13.61.188.105
http://13.61.188.105/
172.31.24.80
172.31.24.80
172.31.24.80
172.31.24.80.
172.31.24.80
flood
detecting
13.61.188.105
why
Another device
different
IPs.
flood
http://13.61.188.105
public- 16.171.62.31
private- 172.31.26.124

AWS- hosting a website — Gym fitness

http://52.21.182.90

/var/log/apache2/ — access.log.

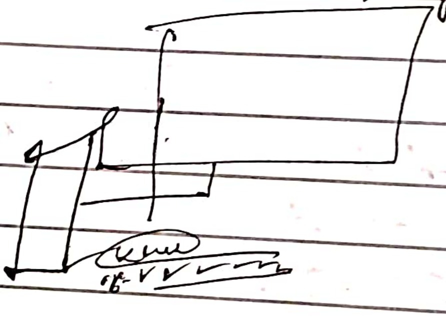
X every visit showing these

But flood data Not showing and website is well working

After this capturing data through ip a

```
Sudo tcpdump -i enX0 port 80
```

http



Terminal

Sending flood Not effecting in this site.

```
Sudo hping3 -S --flood -p 80 <target-ip>.
```

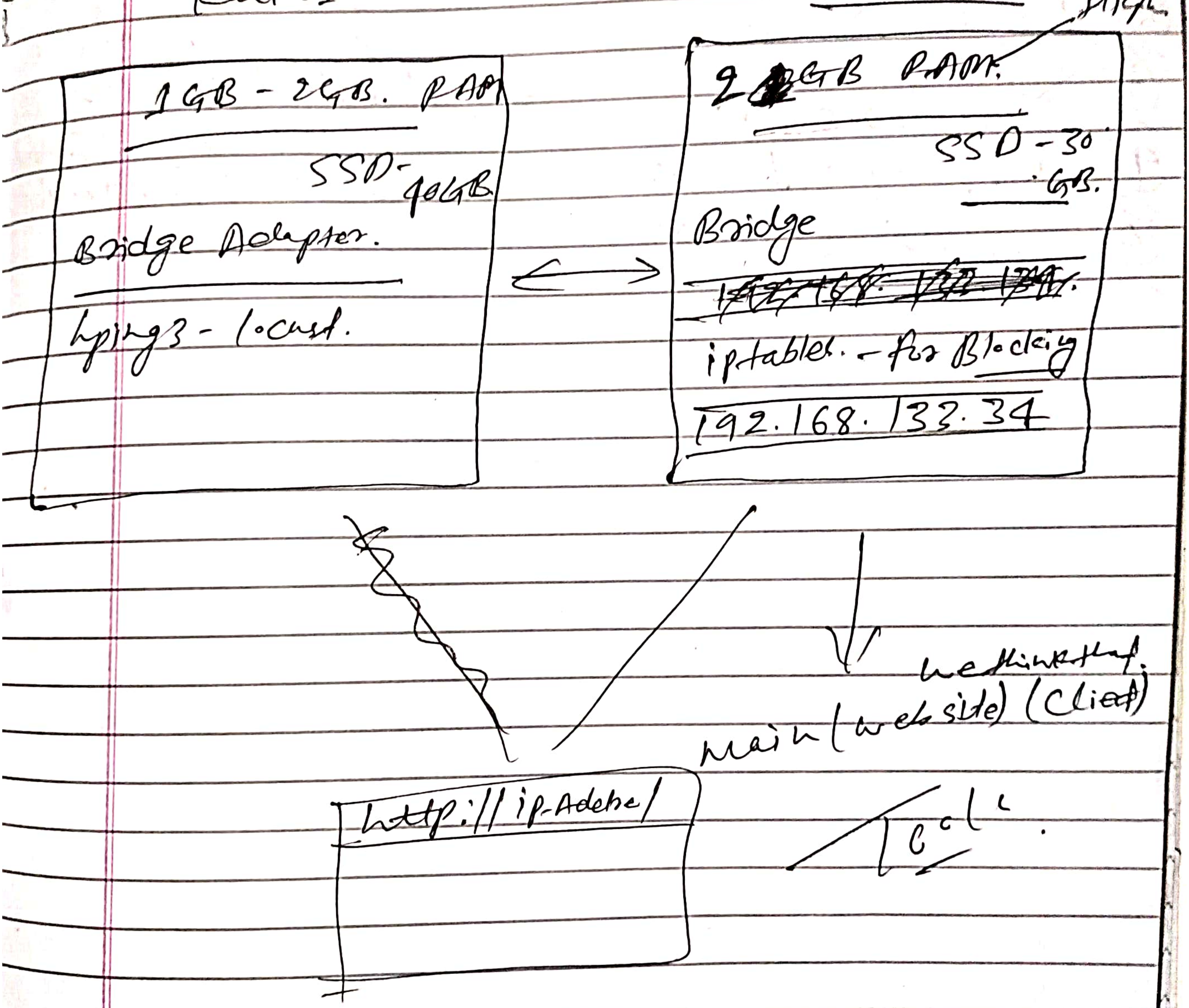
when sending flood S. the ip is 192.168.1.1 and when checking in the website tcpdump there is another link comming. 172.0.1140

Testing on localhost

flood — Attacker machine.

Kali 01

— Hosting website Apache 2.
— protect from there also.
Kali 02.



I want to Send flood ~~before~~ 02 until website not Stop.

① Host

② main Tool. for protection

Kali 01 to overlay

① hping3 Yes > /dev/null &

hping3 -S --flood -p 80 192.168.133.34 X

② LOIC X

③ Slowloris X

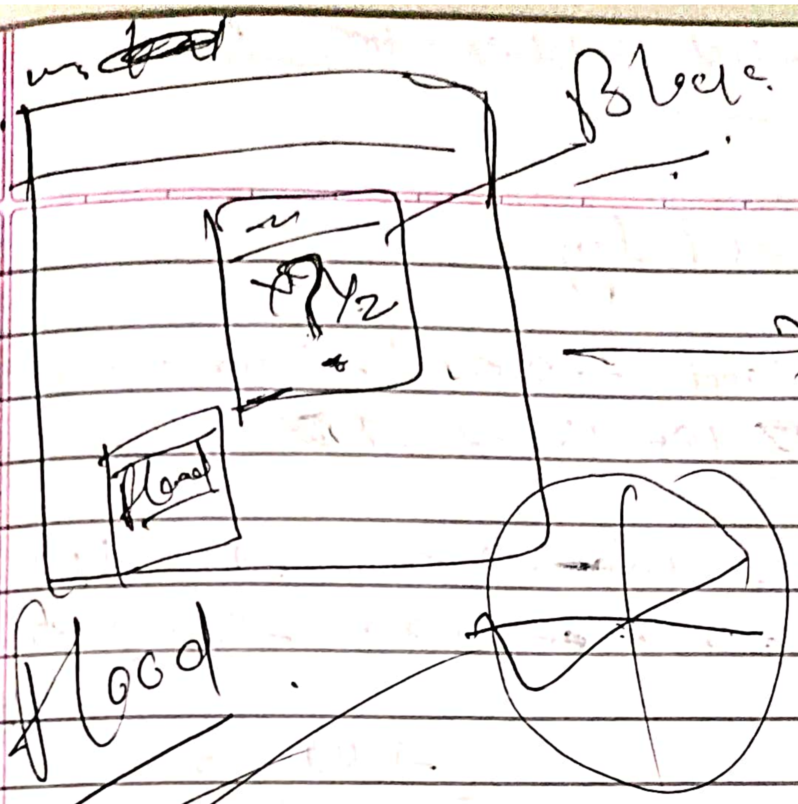
④ Metasploid X

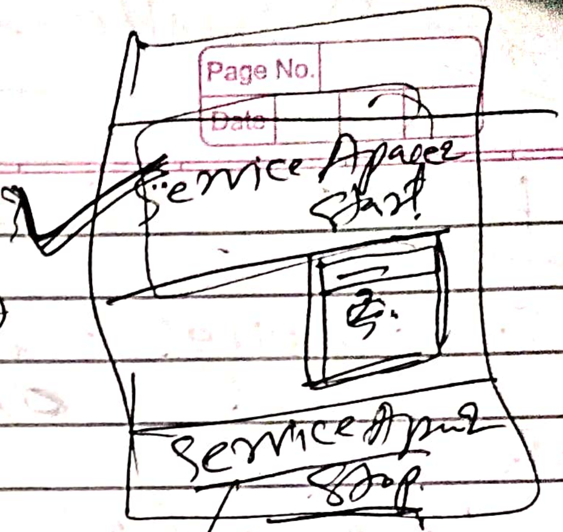
⑤ GoldenEye X

http:// Kali 02

192.168.133.34/

→ I have to that the hosted website terminal down (80p) crash. (Shutdown).





website hosted

pont of

100 [illegible]

iptables

firewall

firewall. Iptables --list --linenumber.

flood : Successfully.

```
Sudo hping3 --flood --rand-source -s -p 80
     ~~d~~ 192.168.2.34
```

Imp.

```
hping3 --flood --rand-source -1 <ip>
hping3 --flood --rand-source -S -p 80 -i u1
                                           <ip>
```

Imp

-i u1   microsecond

status.   firewall . iptables.

```
Sudo iptables -L -n -v.
```

Blocked.

```
Sudo iptables -A INPUT -s <ip> -j DROP.
```

remove   -I

```
Sudo iptables -D INPUT -s <ip> -j DROP
```

It takes To much times
to responed in blocking

fail2ban   /etc./fail2ban/

fail2ban proxychain Tor.

Page No.
Date

kali-linux-2024.3-virtual amd64.

ApacheBenchmark

Ab -n -c -k .ip

proxychain Tor.

192.168.2.136.

test-hosting

~~Apache~~

hosting Apache2.

protecting - fail2Ban

192.168.2.91

Sudo Service fail2Ban start.

Before Blocking ips. iptables.

Sudo hping3 -S -p80 192.168.235.91 -c 100

Before Blocking there is no packet received.

Sudo hping3 iu1. ~~-S -p80~~ <ip>.

for Blocking

Sudo iptables -I INPUT -S <ip> -j DROP

↕

UnBlocking -D

Tshark Stored ips

```
tshark -r test.pcap
```

```
ab -n 1000 -c 100 http://34.207.91.9/
```

Page No.

Date