**CS5573**

**Assignment – 2**

Name : Pinnamwar Shruthi

Student id 16261463

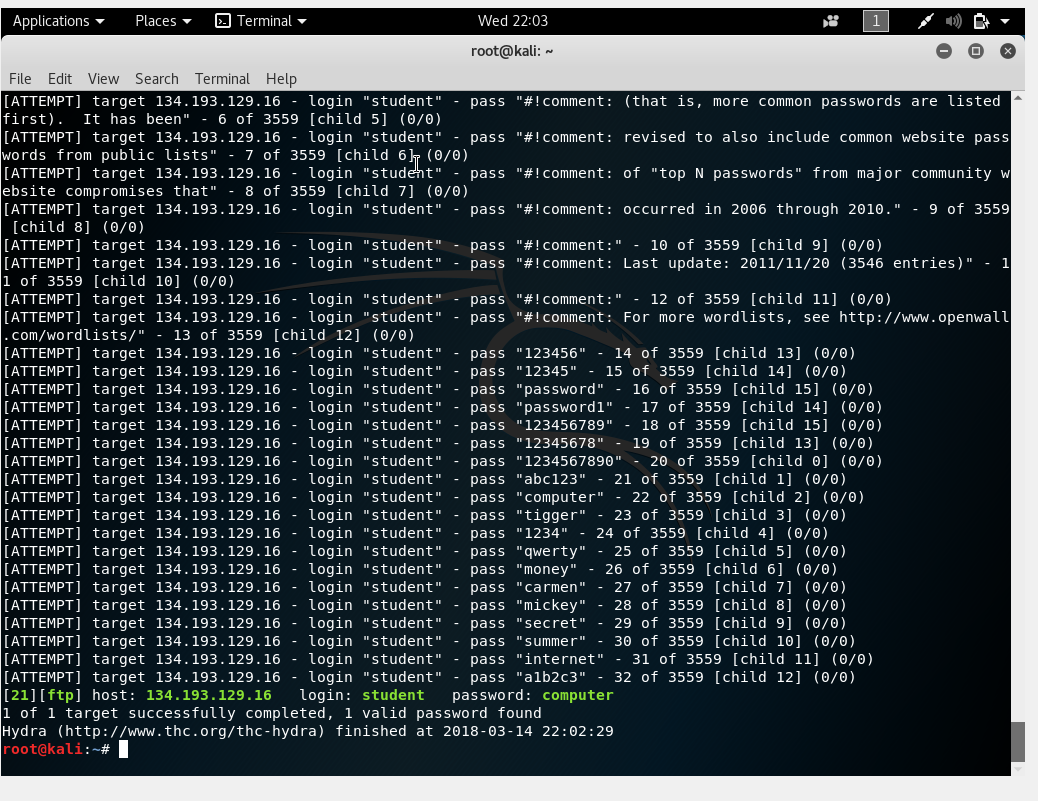
Email spdb6@mail.umkc.edu

Use the below command to crack the password of a user login account ‘student’ using dictionary attack.

Command: *hydra –l student –V –P /usr/share/john/password.lst* <ftp://134.193.129.16>

What is the password of the login account ‘student’?

Ans: Password of the login account ‘student’ on the server 134.193.129.16 is: computer



Password cracking using bruteforce attack

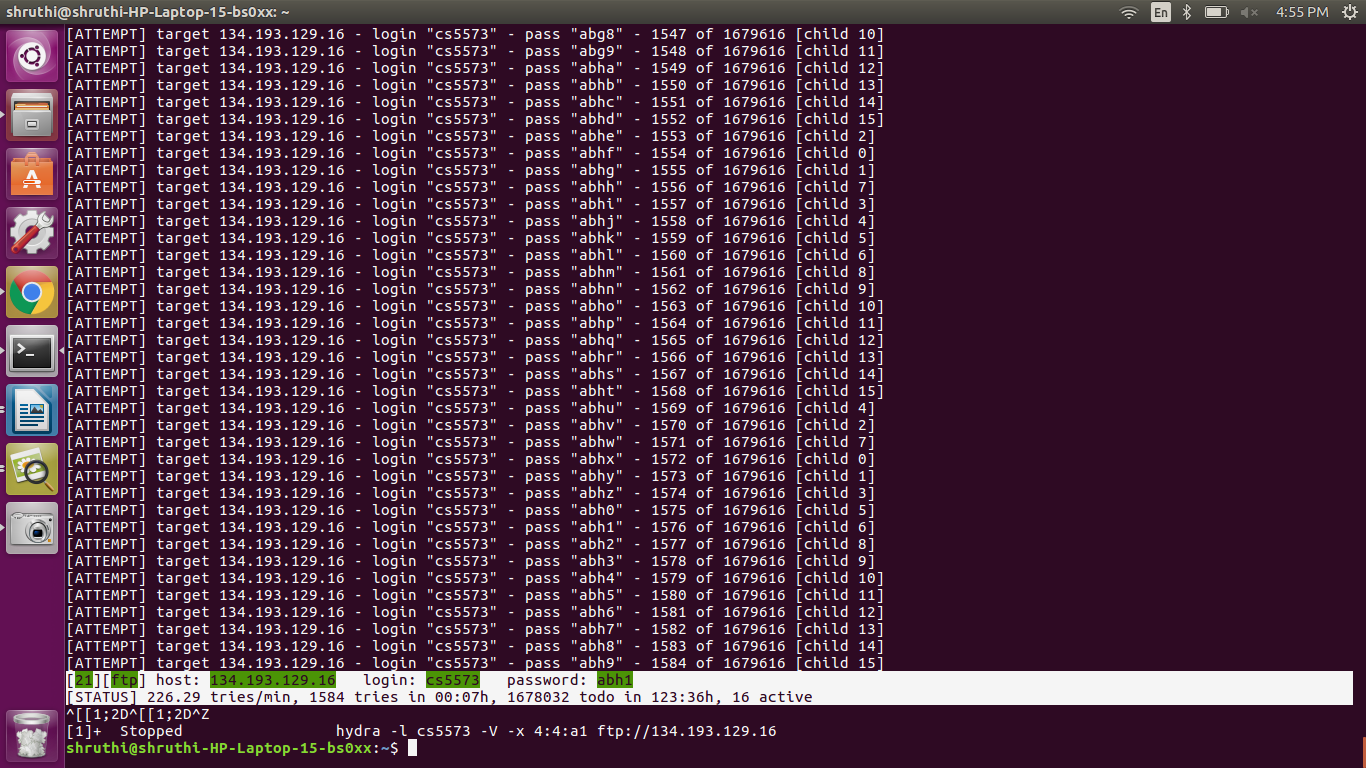
Use the below command to crack the password of a user login account ‘user’ on the server 134.193.129.16 using bruteforce attack.

Command: *hydra –l cs5573 –V –x 4:4:a1* <ftp://134.193.129.16>

1. What is the password of the login account ‘cs5573?

Ans: Password of the login account ‘cs5573 is : abhi

It took 1584 tries in 00:07h



1. Explain the process of hashing and storing the passwords in latest Ubuntu/Linux and Windows operating systems.

Ans:

Hashing: Hashing is generating a values from a string of text using a mathematical function.

Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect security of the transmission against tampering.

Hashing is also a method of sorting key values in database table in efficient manner.

In Ubuntu/Linux,

* Passwords are stored in a file called as /etc/password.
* For managing a single host, the shadow suite can be used instead of a more complex database
* This keeps the password in /etc/shadow (and only an “x” as a place-holder in /etc/passwd). The shadow file has root-only access, so utilities that manage passwords are often setUID to root.

Where as in Windows,

* Windows stores its passwords in the Security Accounts Manager database, or SAM database.
* This is a file that exists in the registry and access to it is tightly controlled while windows is running; however, local administrators who can run processes as NT AUTHORITY\SYSTEM and can access it .
* As for the hashes used, they are either the LM or NTLM hash.
* The NT hash is simply a hash. The password is hashed by using the MD4 algorithm and stored.

1. Mention the salt value, hash algorithm and hashed password value of the account ‘root’ of your Kali Linux system. (Open the shadow file in your kali linux and locate the username ‘root’ and provide the above details)

Ans: The owner of the /etc/shadow file is usually the user **root**.

Password is not stored in /etc/passwd, but in /etc/shadow

Password is a combination of the hashing algorithm, optional salt applied, and the hashed password itself

* The first field is a numerical number that tell's you the hashing algorithm that's being used.

$1 = MD5 hashing algorithm.

$2 =Blowfish Algorithm is in use.

$2a=eksblowfish Algorithm

$5 =SHA-256 Algorithm

$6 =SHA-512 Algorithm

* The second field is the salt value
* The last field is the hash value of salt+user password

In our case

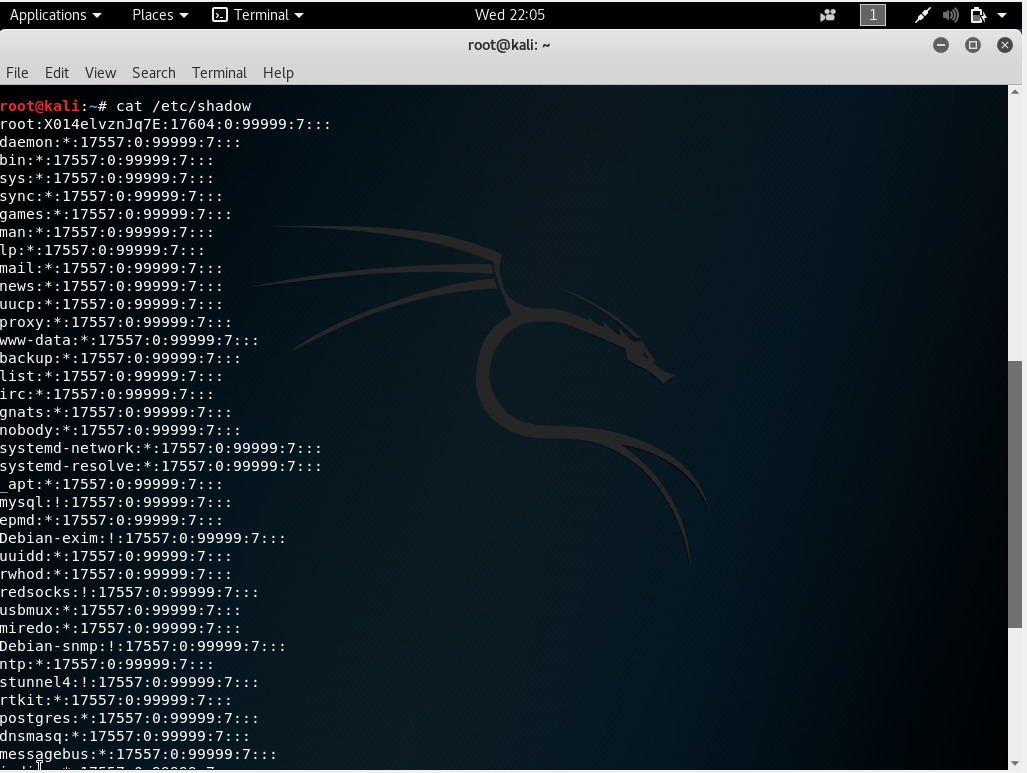
$6$DJJJejmh$bGWxX9AYTT7.Z4up43vo4uGjxQ.LTlXrh9772pJ7.dTzJ4j2ETYJdgtEywJBvOUsUttJHx1d3j7Ly15/VCj3q.:17558:0:99999:7:::

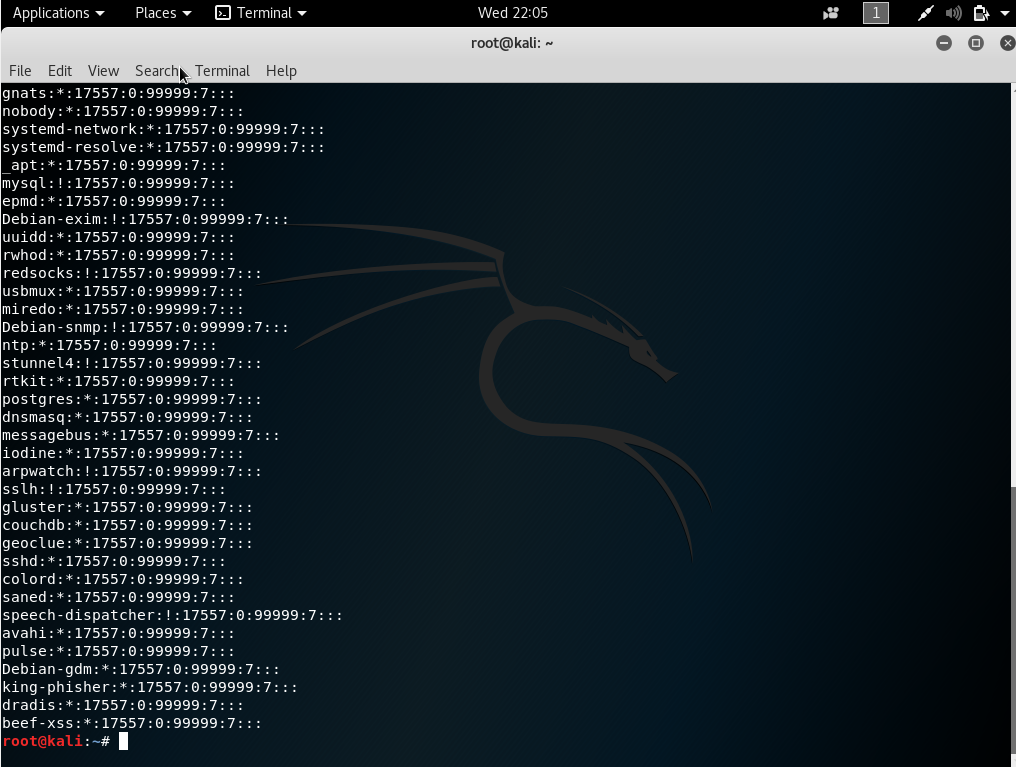
$6 =SHA-512 Algorithm

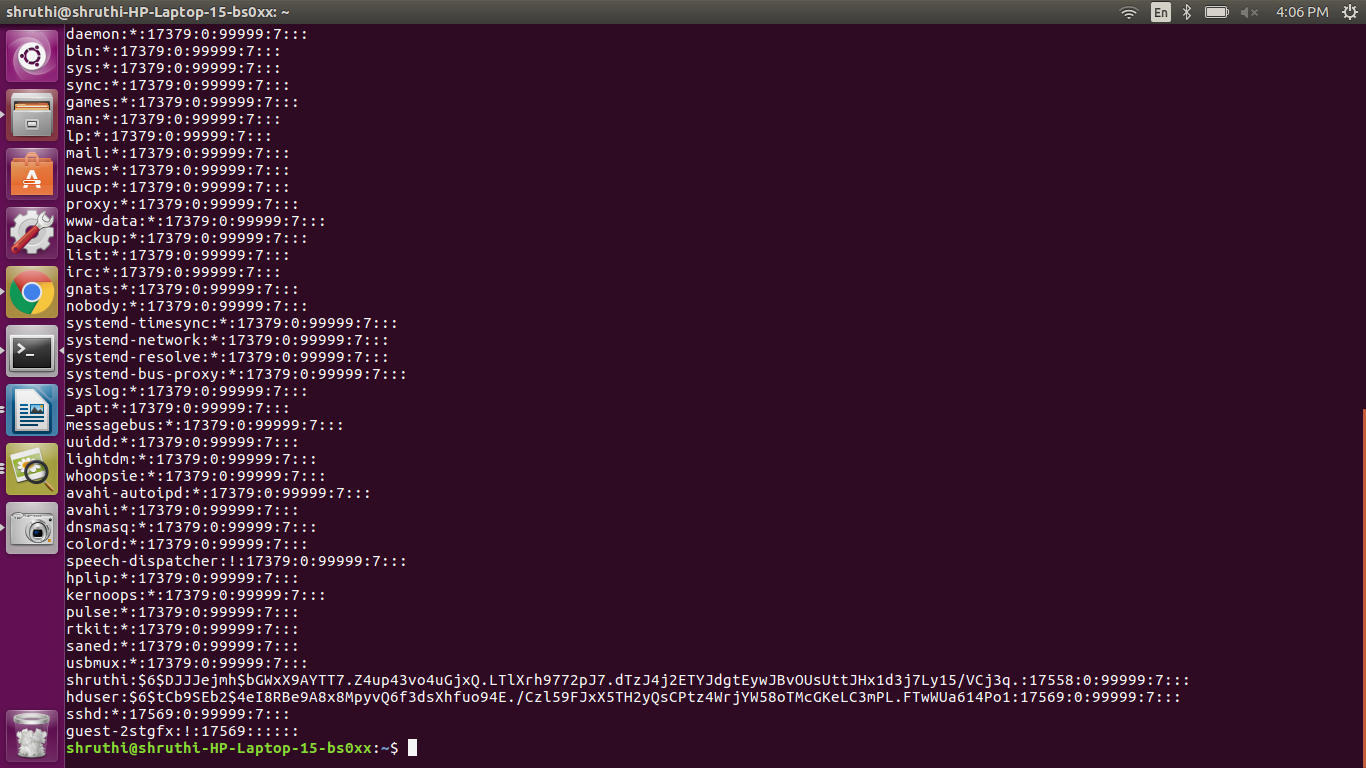
Salt value : DJJJejmh

Hashed Password Value and how long its been created : bGWxX9AYTT7.Z4up43vo4uGjxQ.LTlXrh9772pJ7.dTzJ4j2ETYJdgtEywJBvOUsUttJHx1d3j7Ly15

VCj3q.:17558:0:99999:7:::

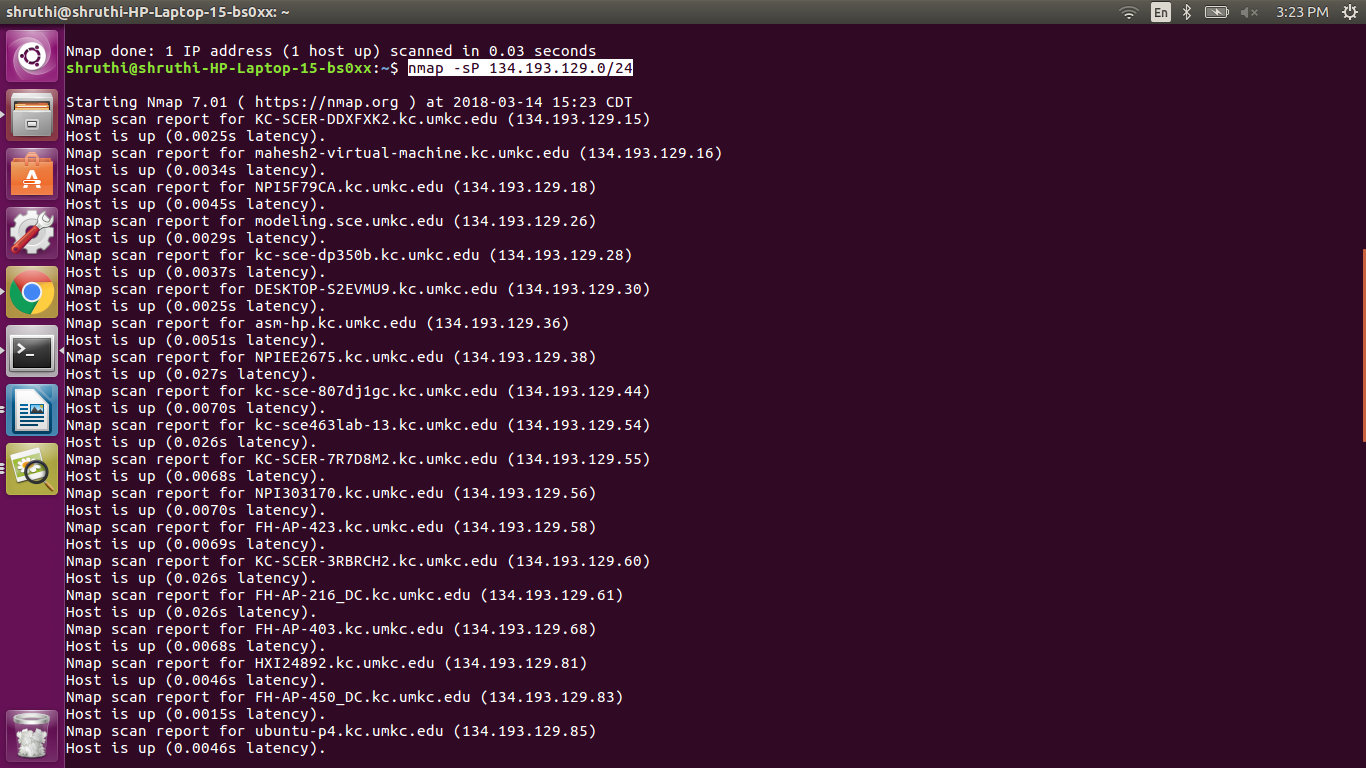


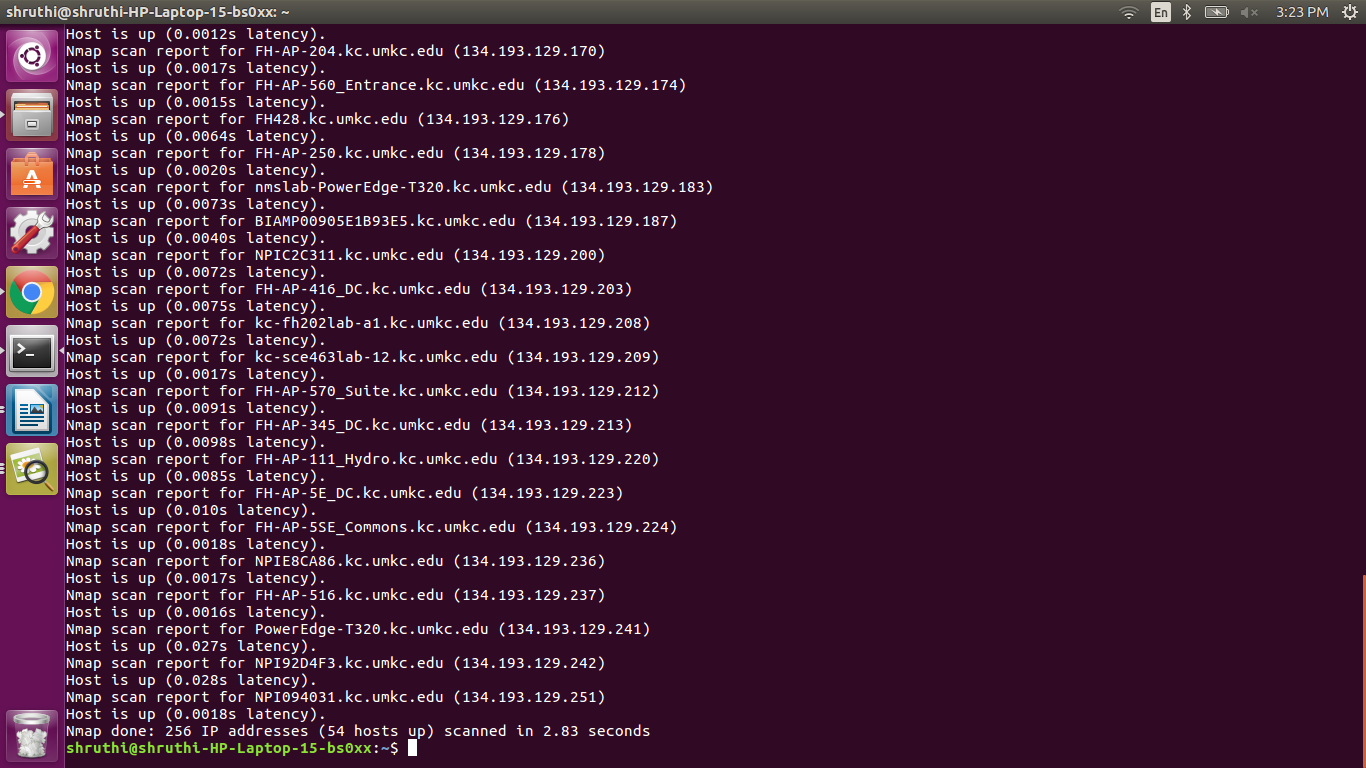




1. List the **live systems** of the network 134.193.129.0/24 using nmap tool.

Ans: 266 IP Addresses 54 hosts up scanned

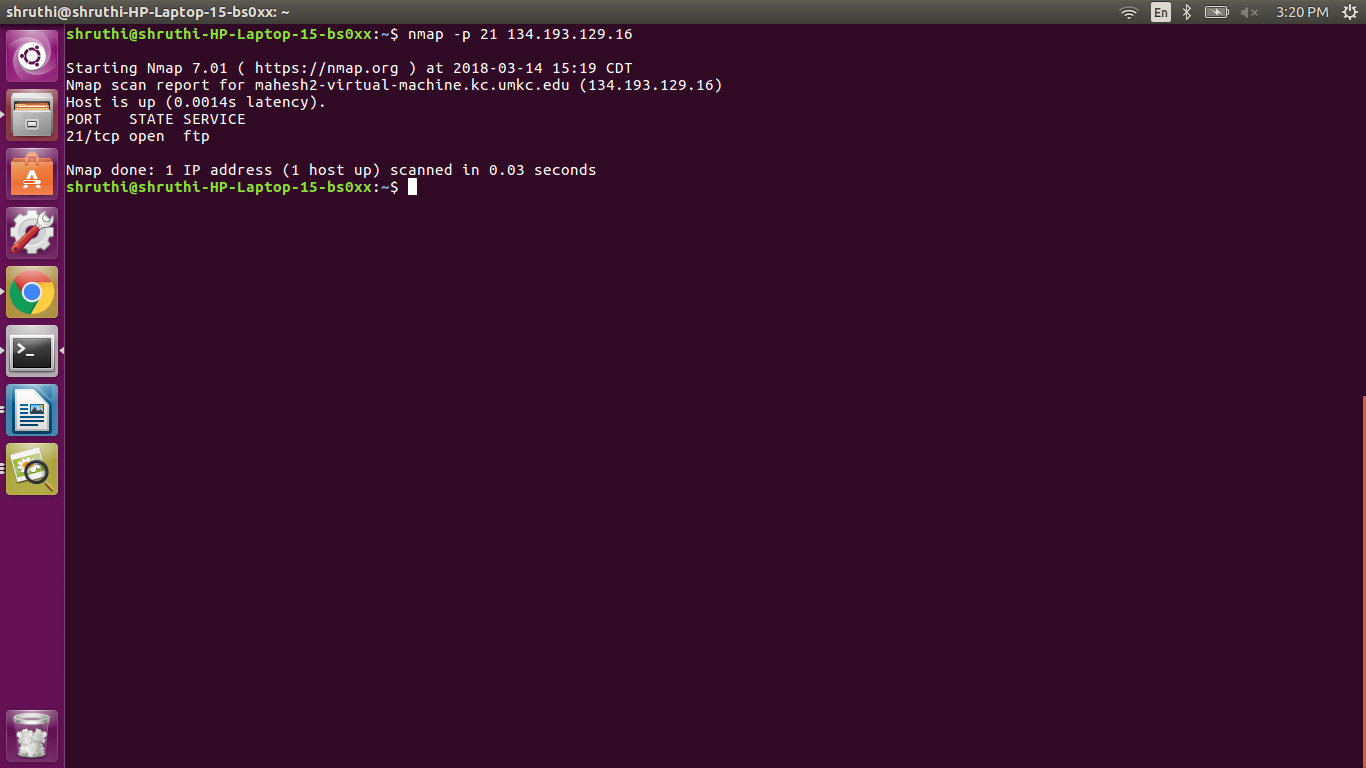




1. List all the **open ports** available on the system[134.193.129.16](ftp://134.193.129.16) using nmap tool.

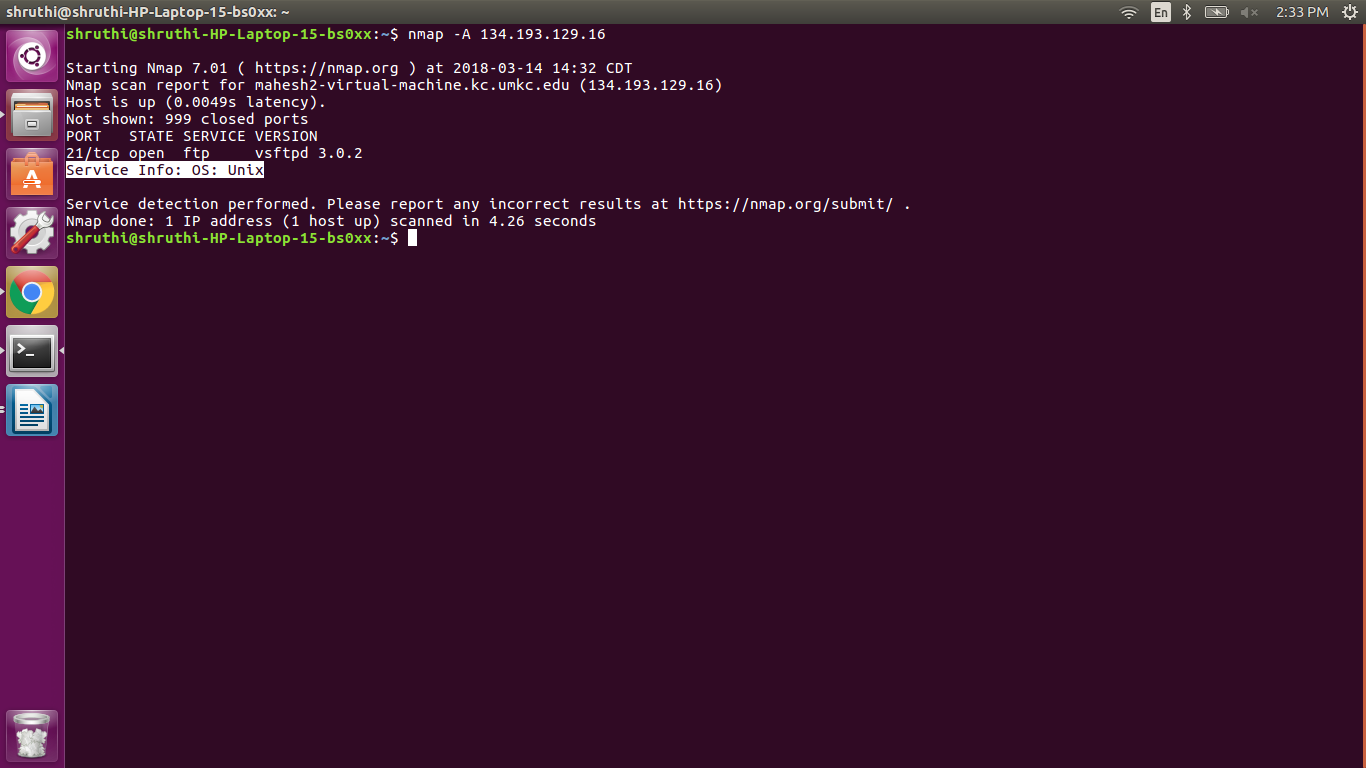
Ans: tcp open

Command : nmap -p 21 134.193.129.16



1. Find out the **Operating System** on the system 134.193.129.16 using nmap tool.

Ans: OS : Unix



1. What is the **FTP server version** on the system 134.193.129.16?

(Use banner grabbing method – telnet with port 21)

Ans: Service name: vsftpd(Very Secure FTP Daemon)

Version number: 3.0.2

