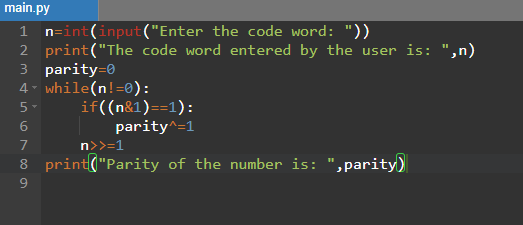
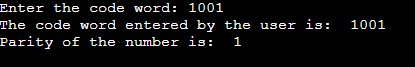
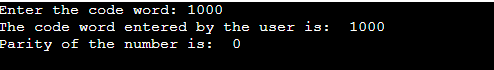
**Practical No. :-01**

**Aim:-**Checking data integrity using simple parity check

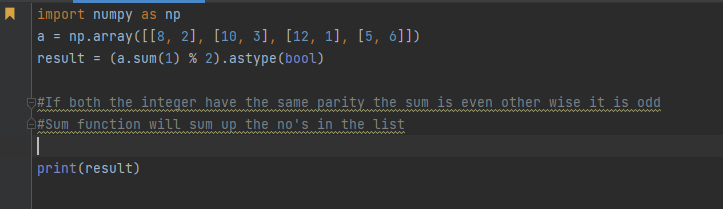


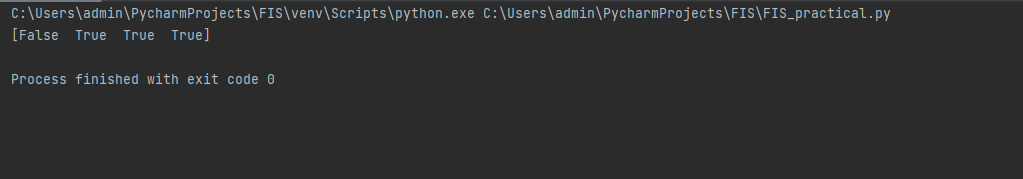




**Practical No. 02**

**Aim:-**Checking data integrity using two-dimensional parity check.

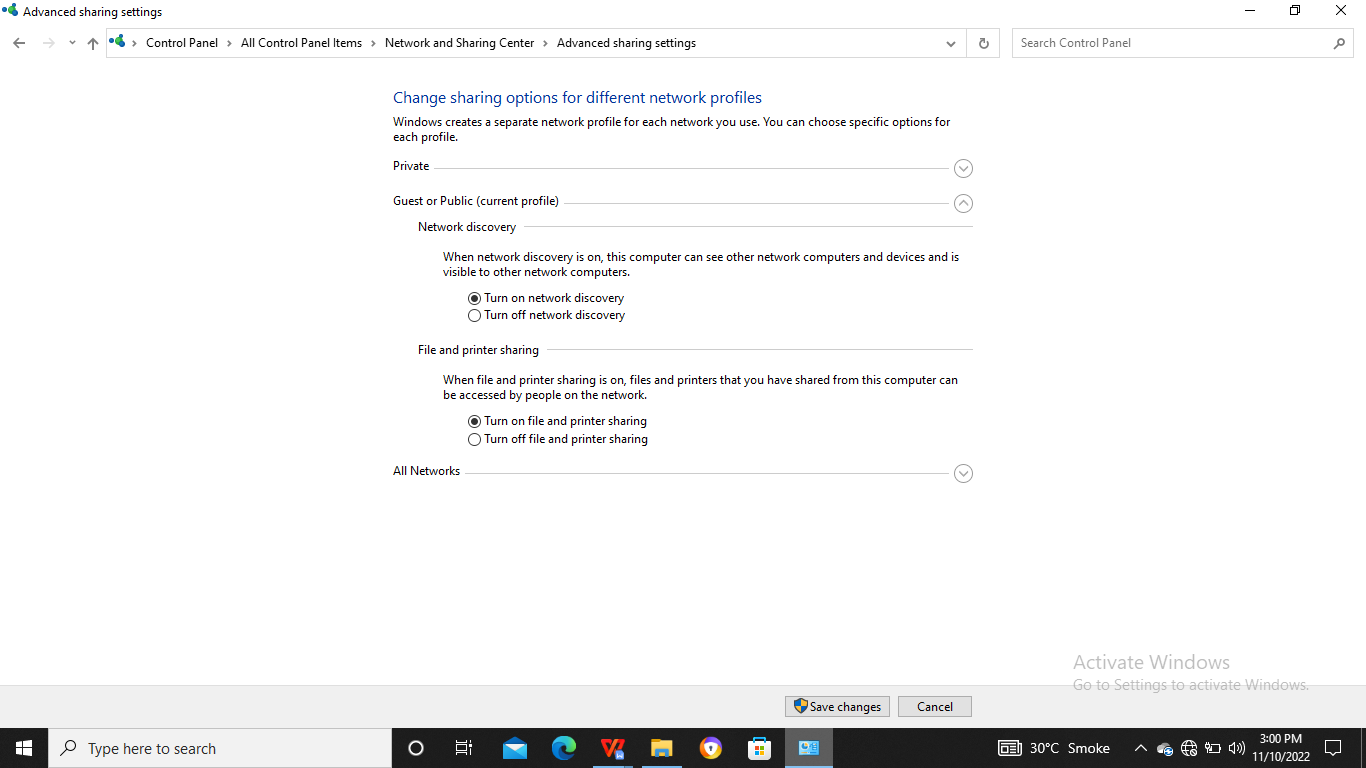


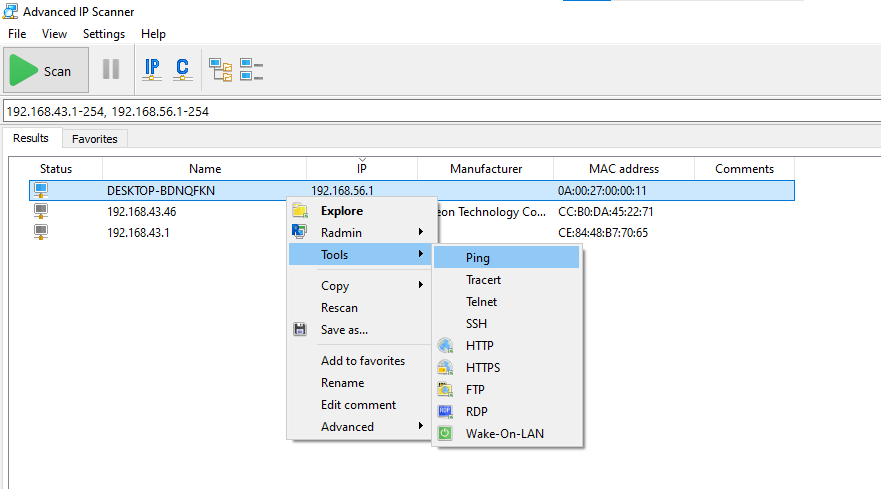


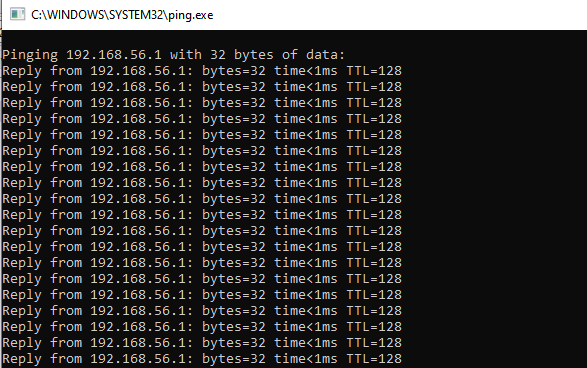
**Practical No.:03**

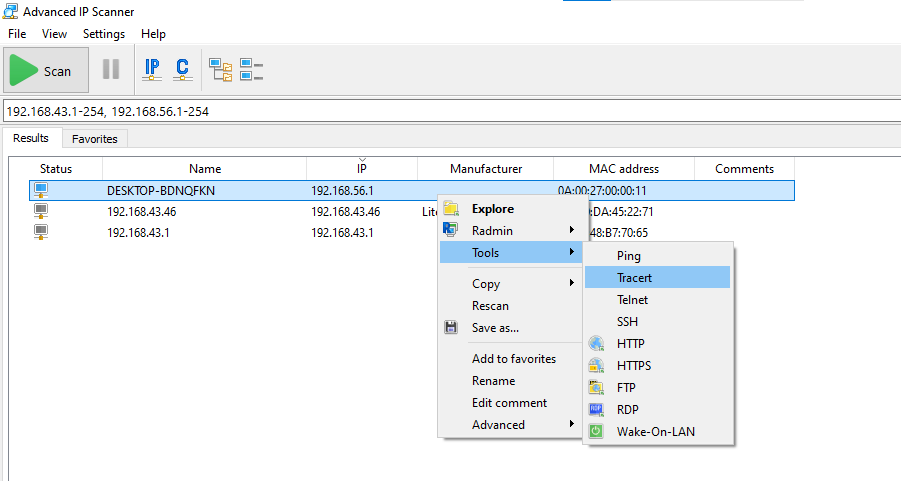
**Aim:-**Fundamental of Computers

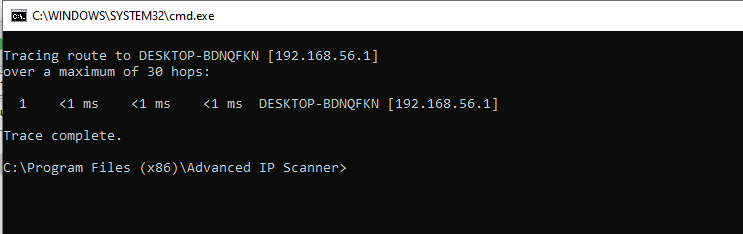
1. IP Address





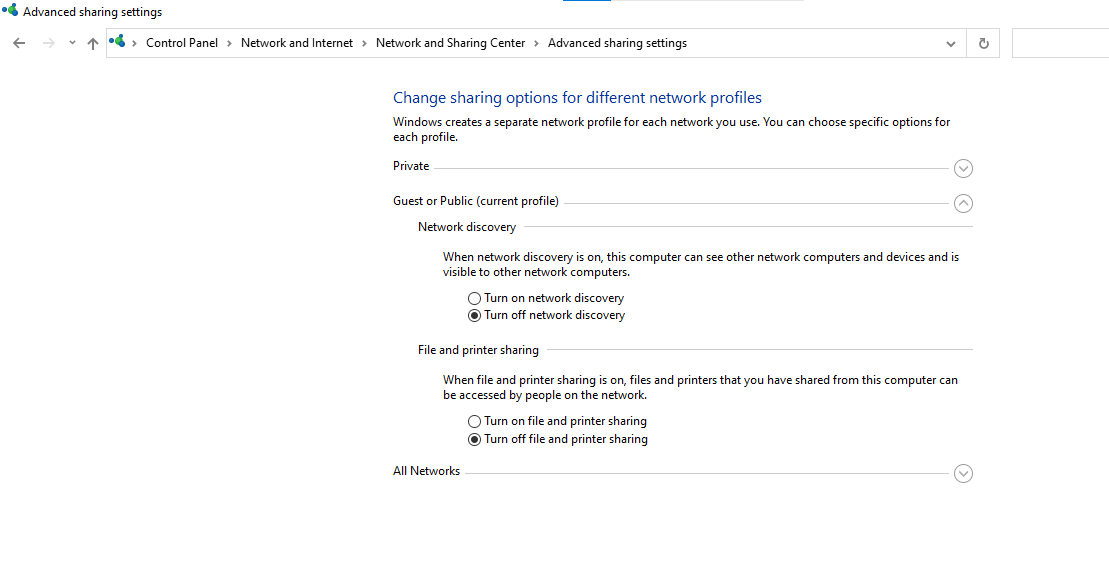


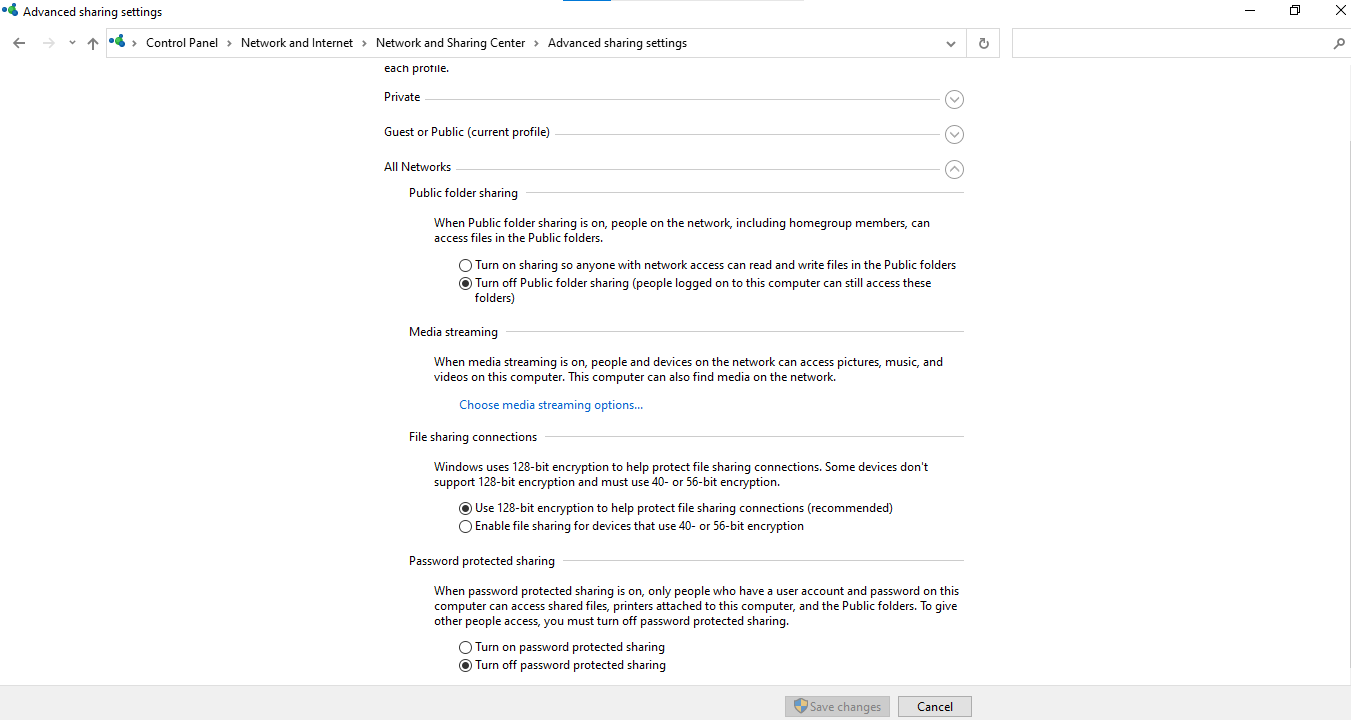


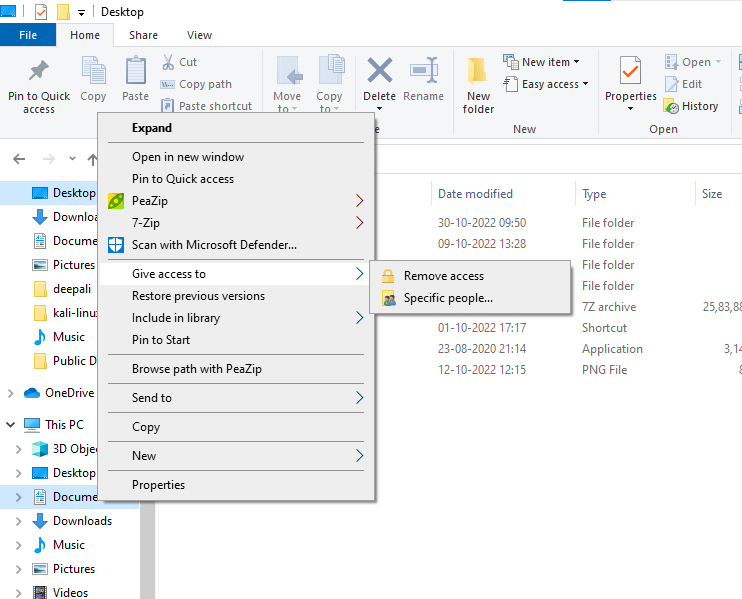


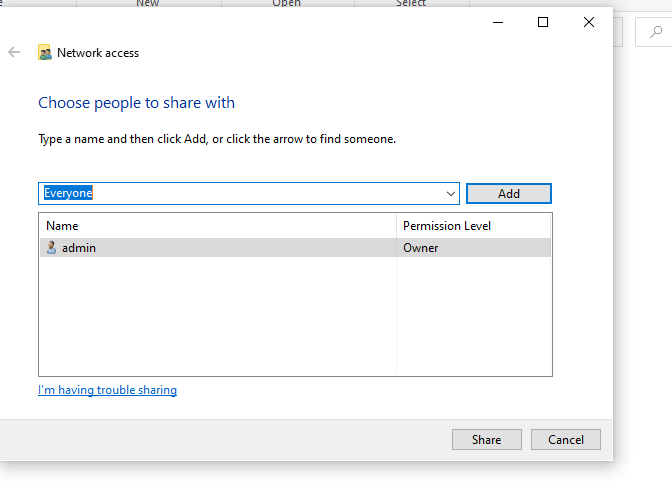
1. MAC Address (Using Advance IP Scanner)

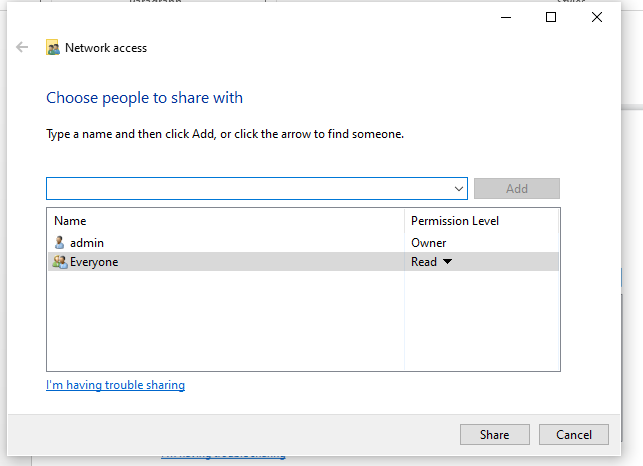


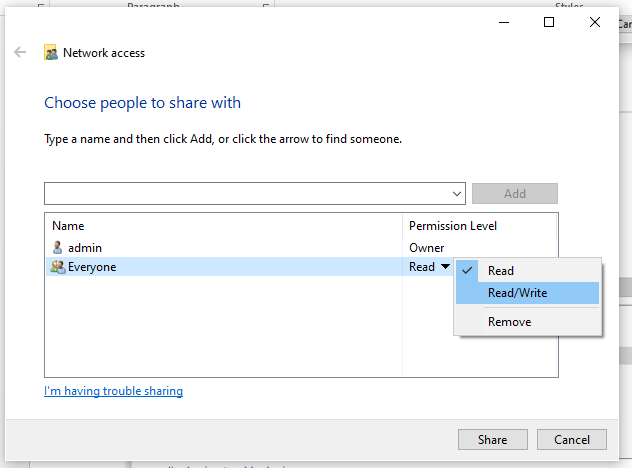


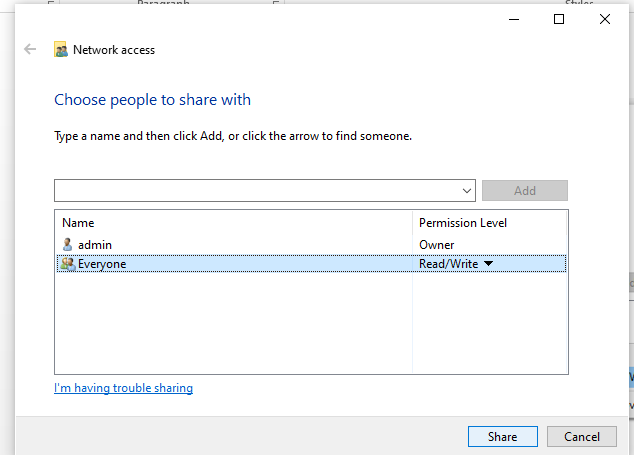


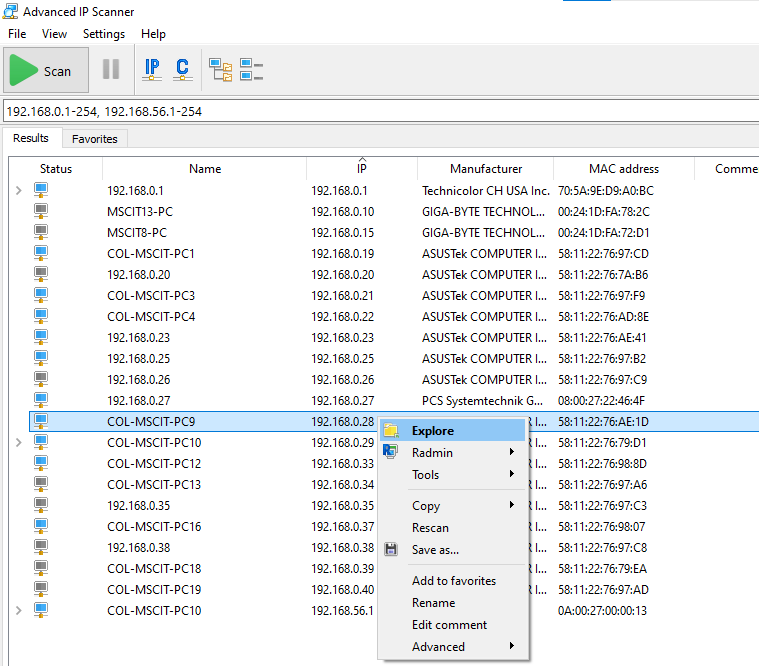


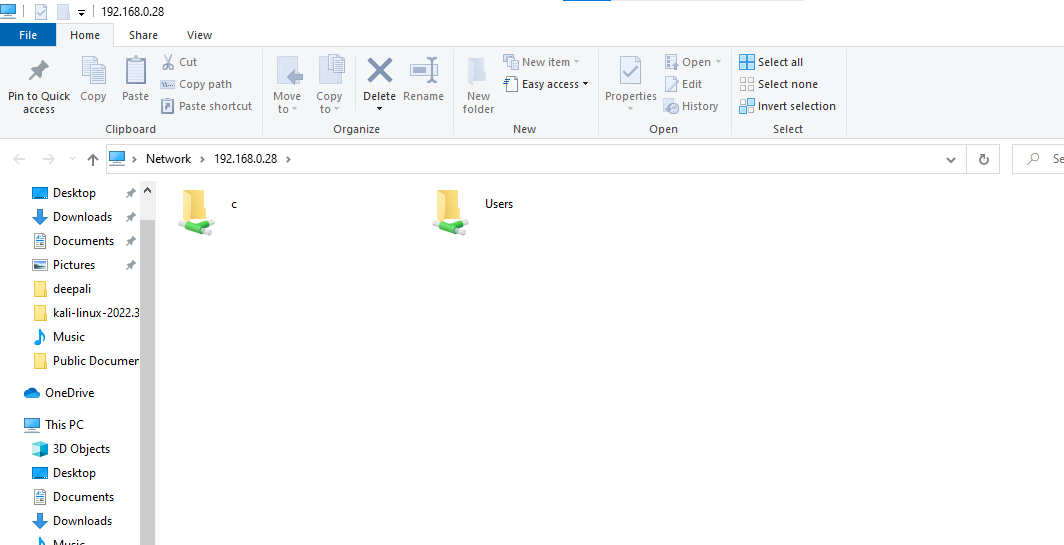


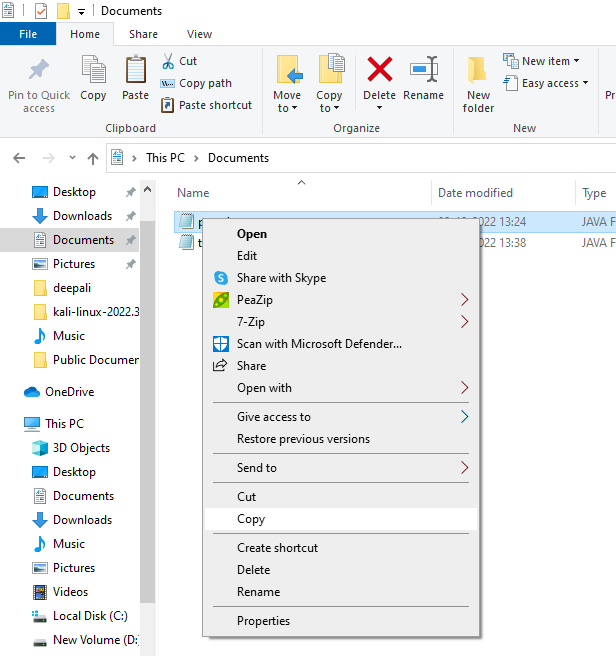


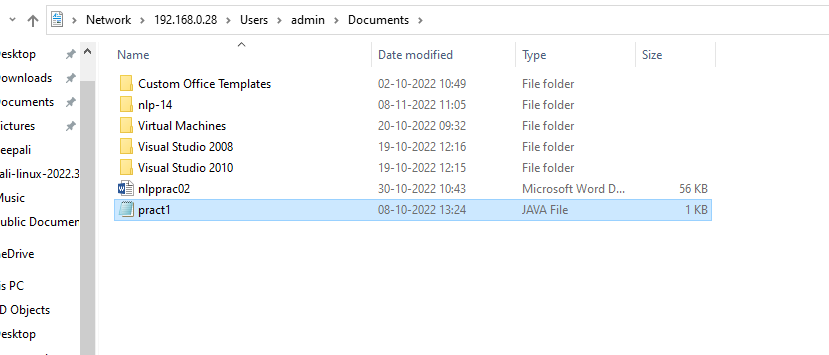








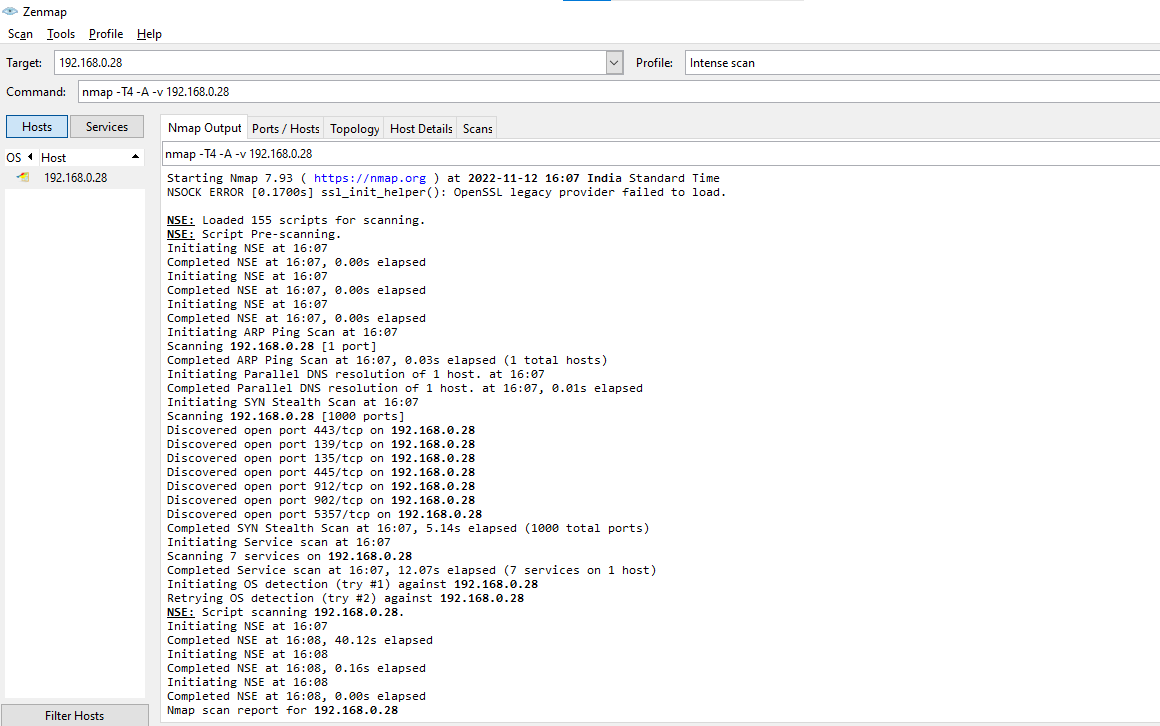


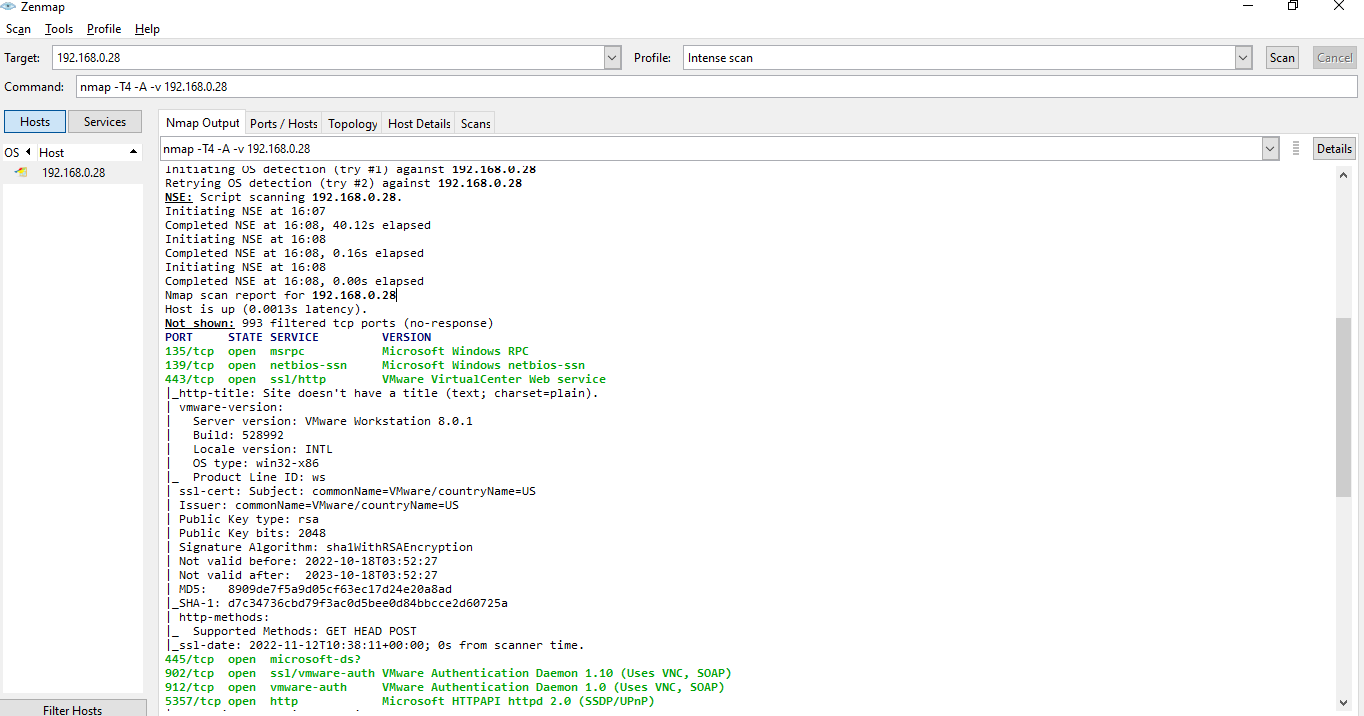


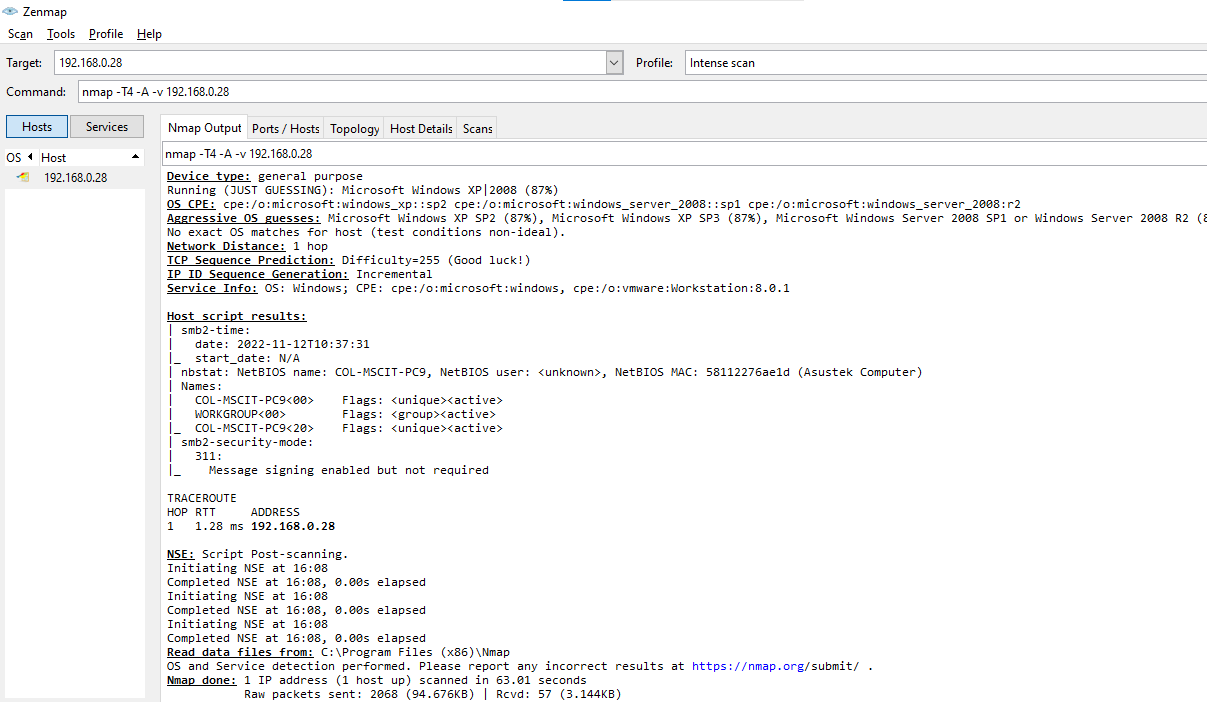
**PRACTICAL NO.:04**

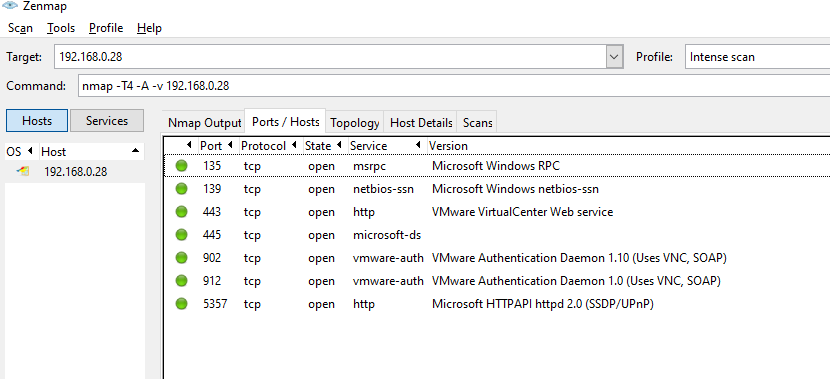
**AIM:-** Information Gathering Tool

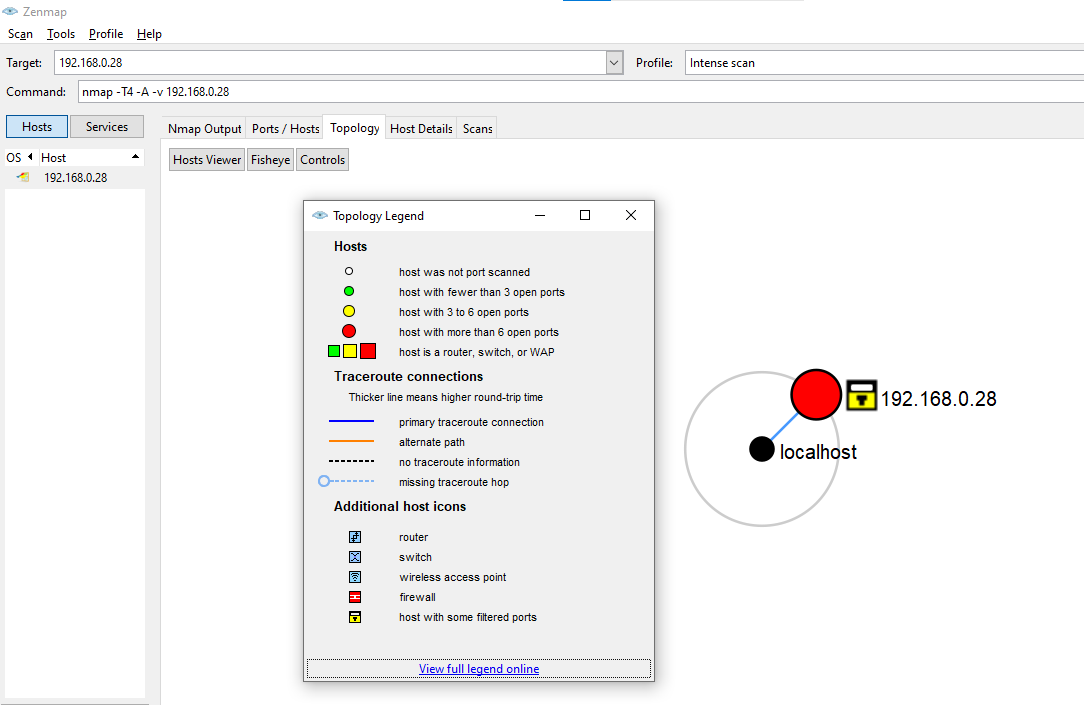
1. Opposite Pc(192.168.147.1) with profile intense scan

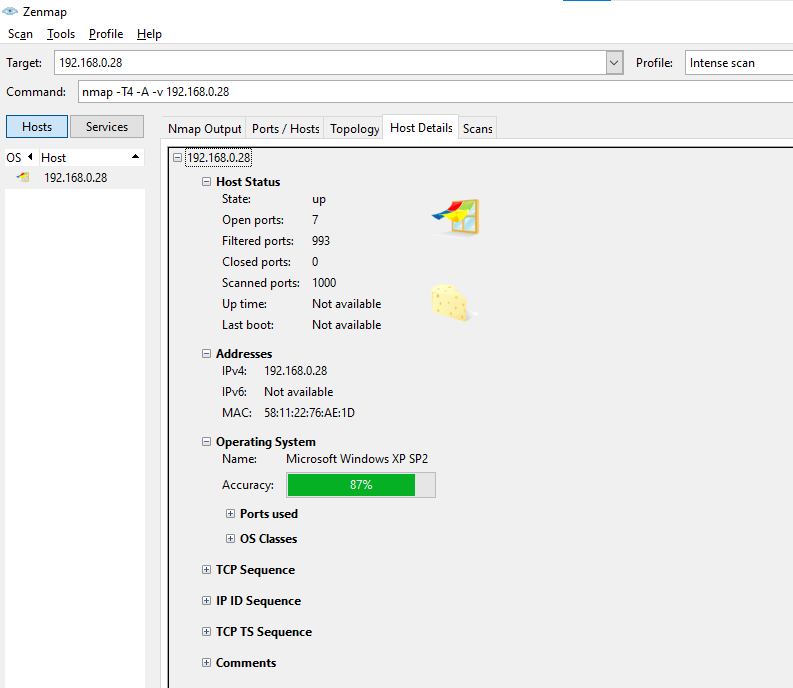


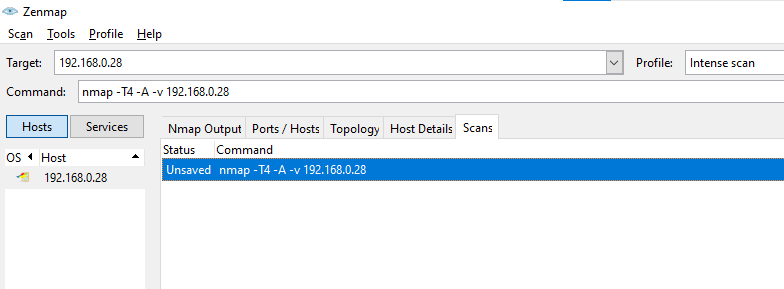




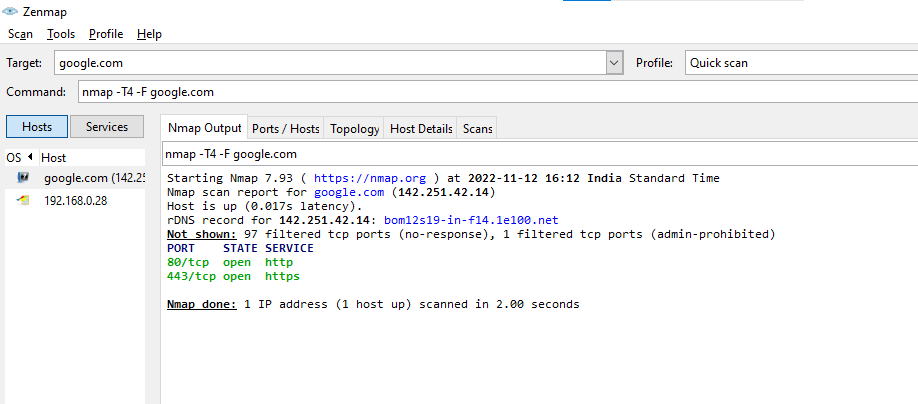


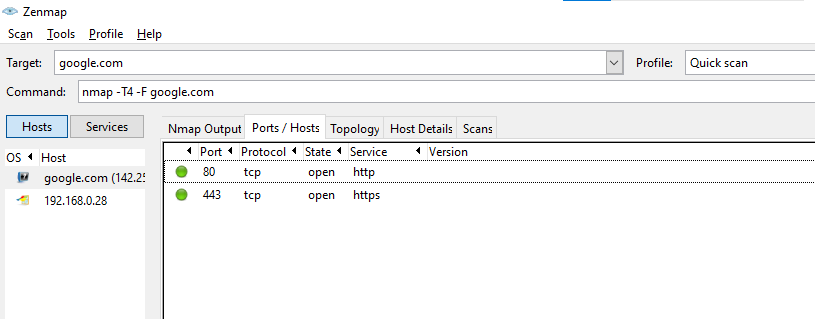


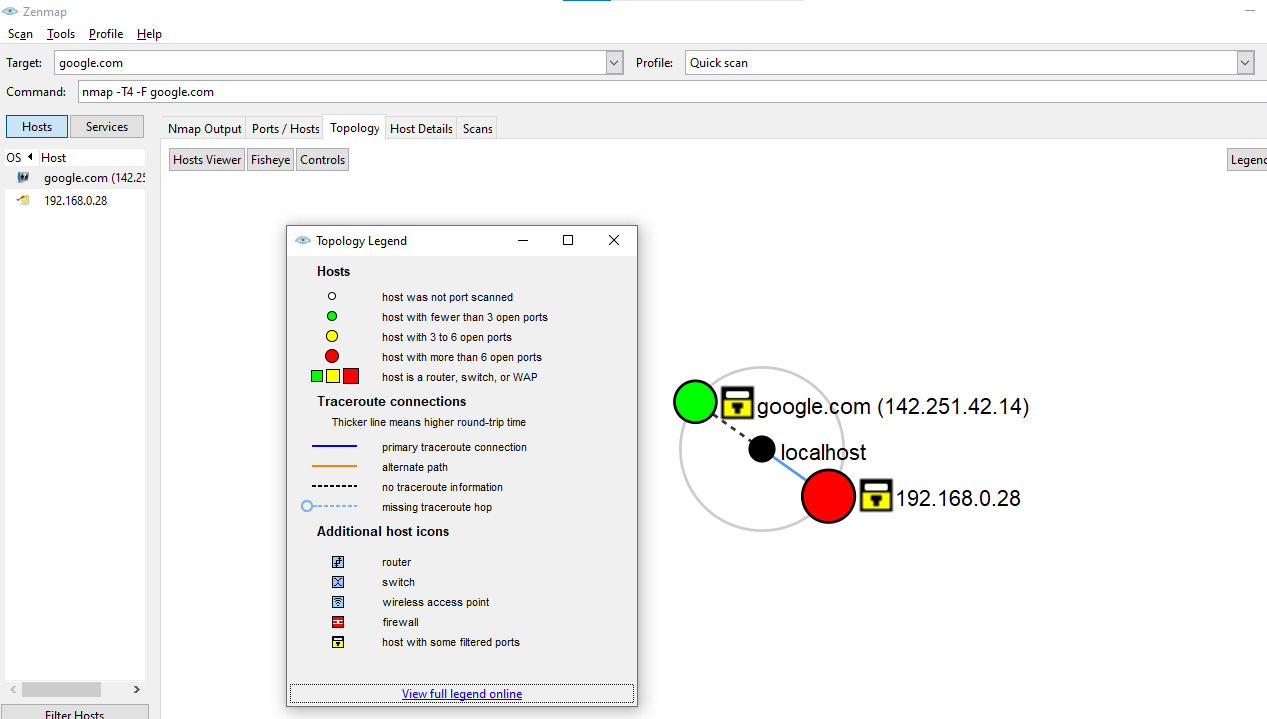


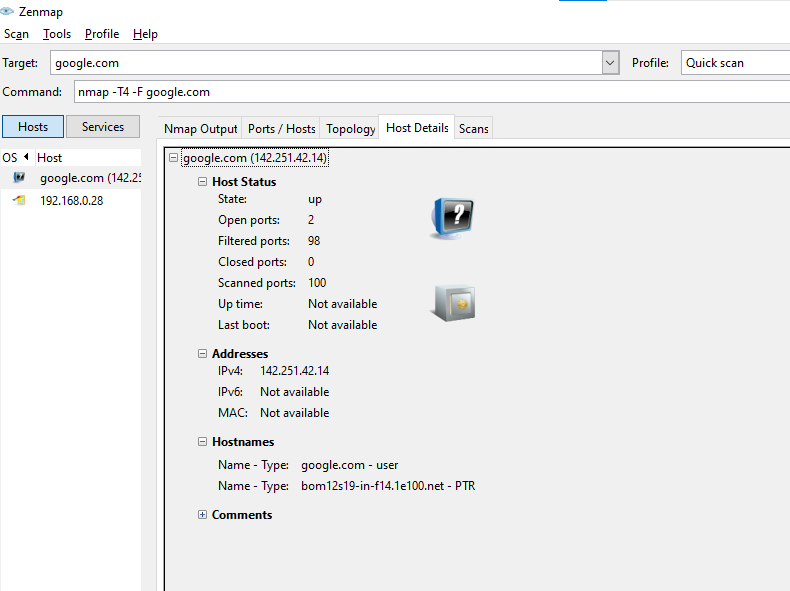


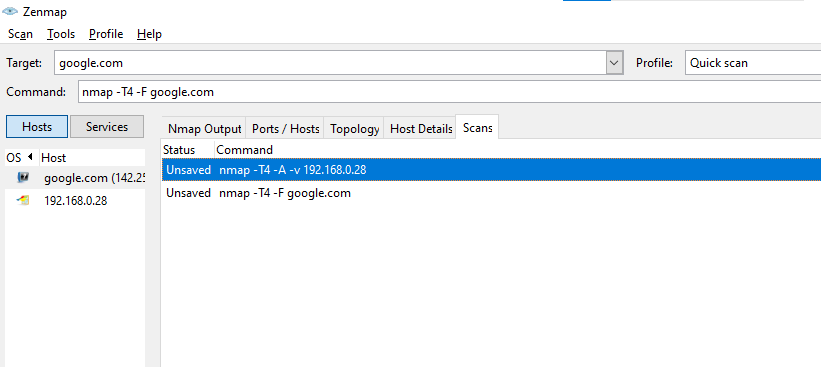
1. Google.com with profit Quick scan





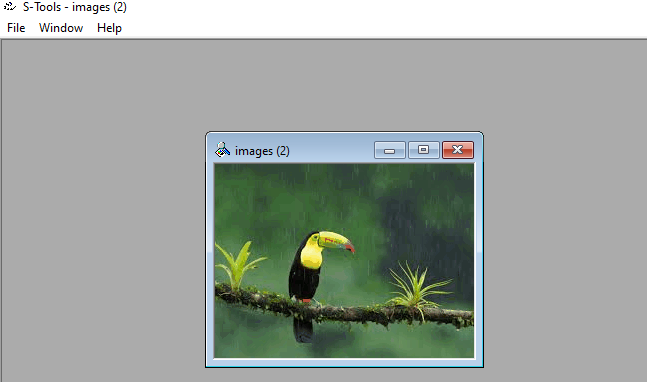


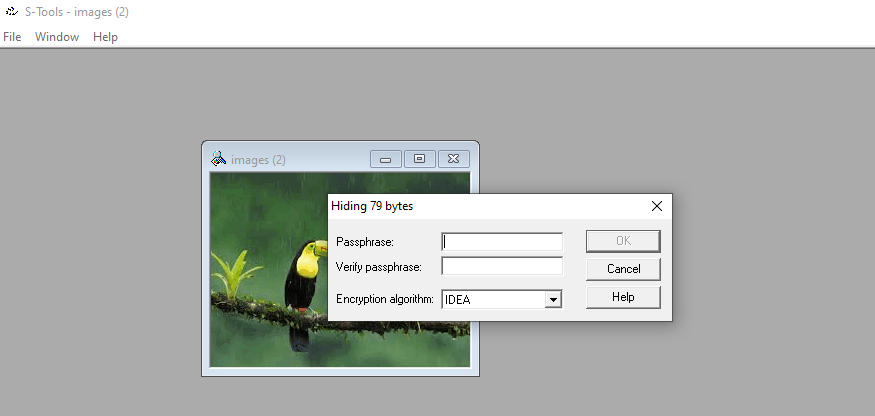


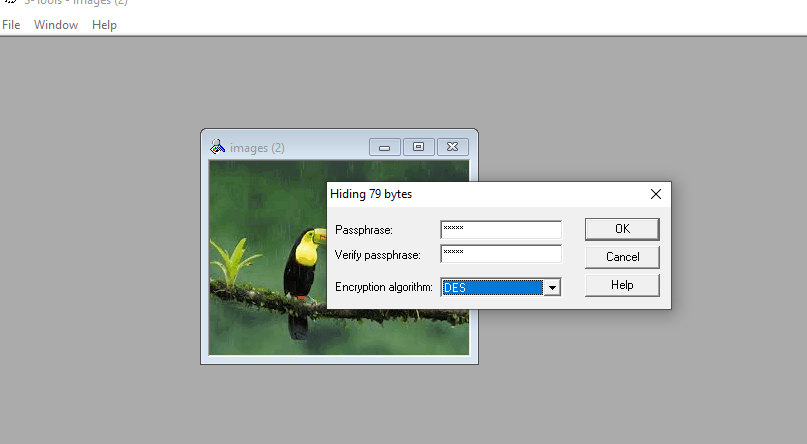


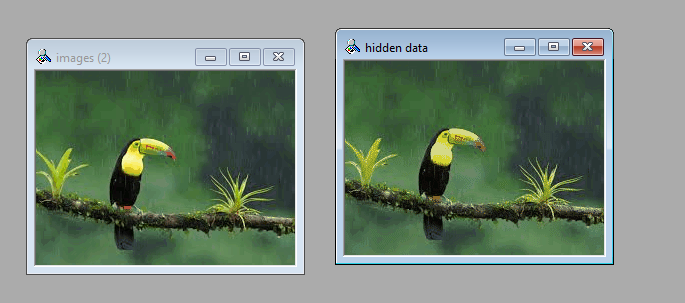
**Practical No.05**

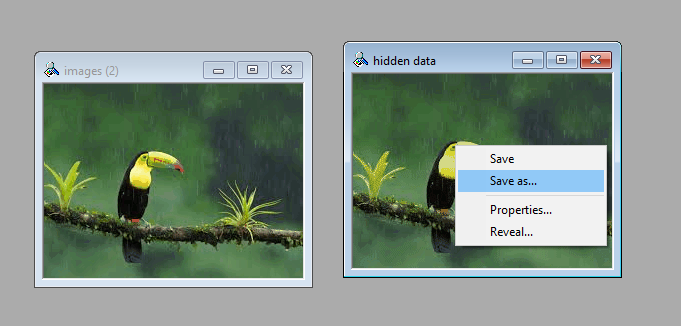
**Aim:-**Implement Steganography using tools (S-tools)

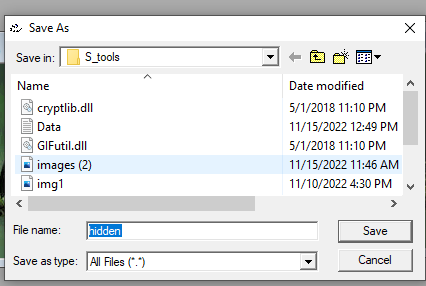


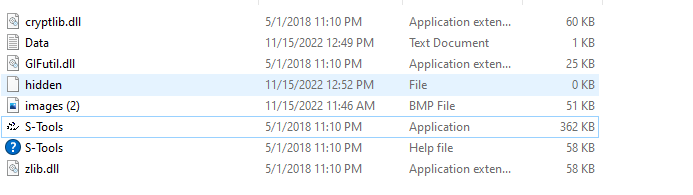


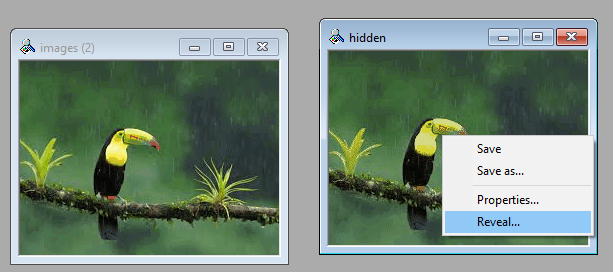


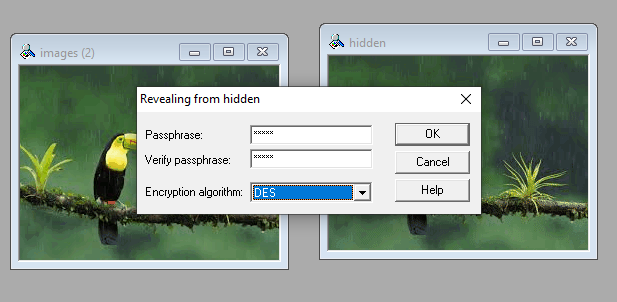


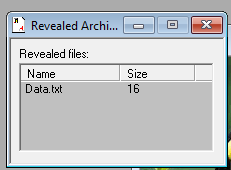
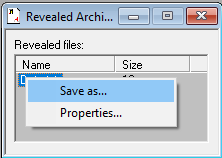


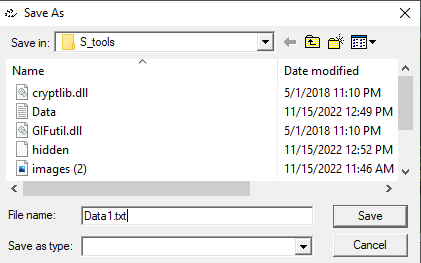


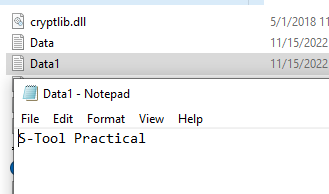


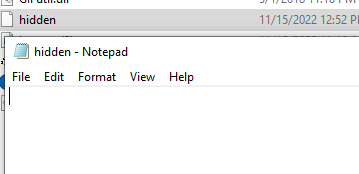






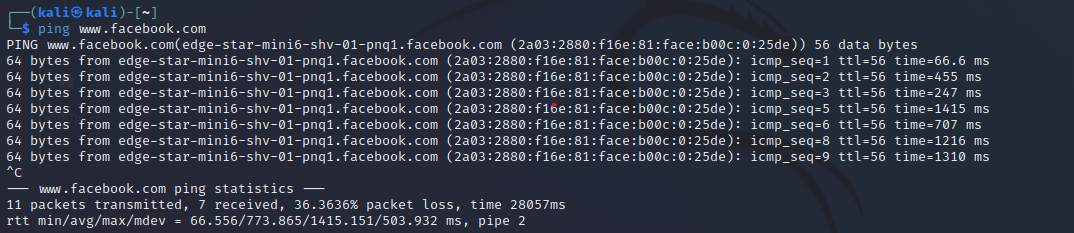




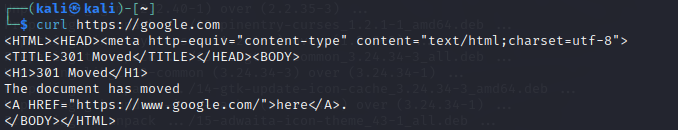
**PRACTICAL NO.:-06**

**Aim:-** Implementation of Networking Tools

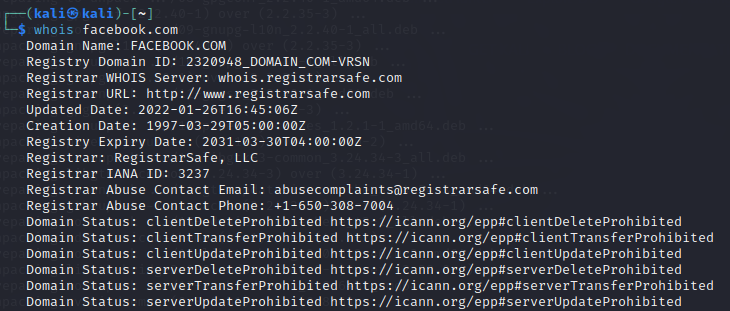
1. PING,TRACERT, IFCONFIG, IPCONFIG, NSLOOKUP, WHOIS, NETSTAT…
2. Ping:-

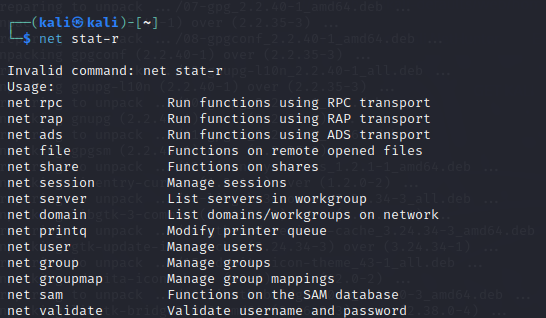


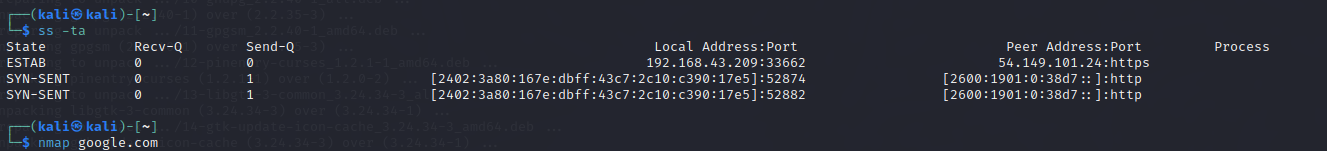
1. Curl:-



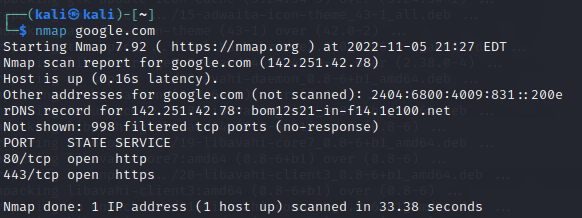
1. Whois:-



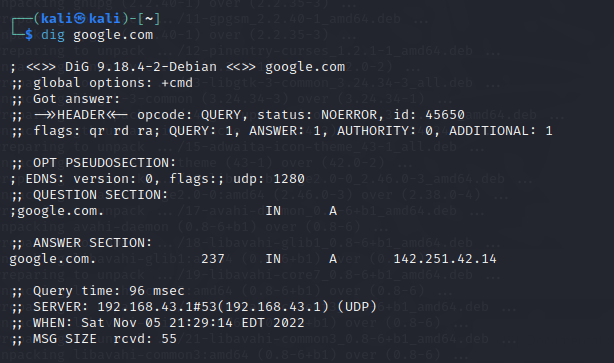
1. net stat -r:-
2. Ss -ta:-



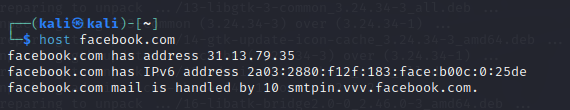
1. Nmap:-



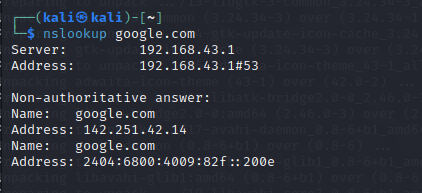
1. Dig:-



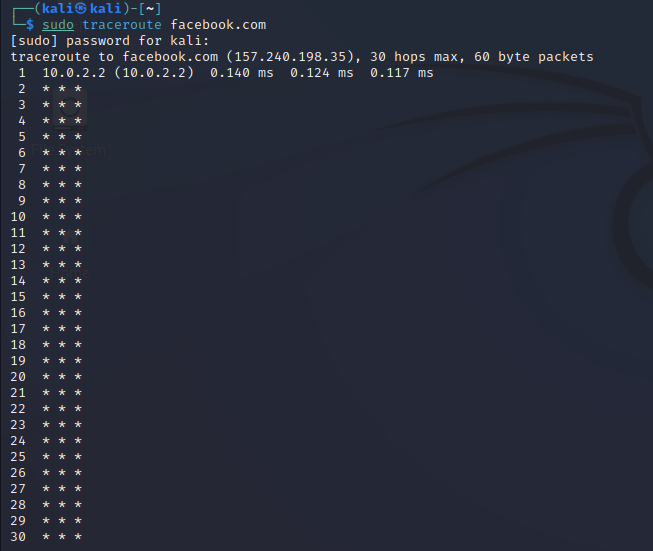
1. Host:-



9. Nslookup:-



10. Traceroute

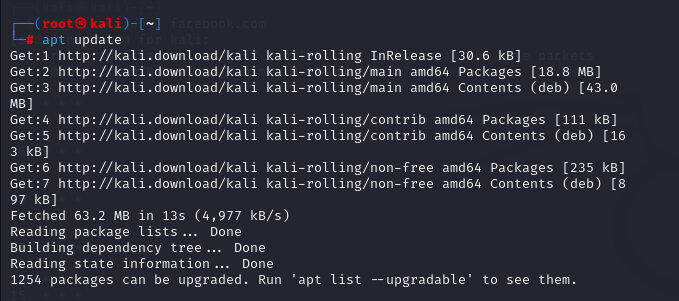


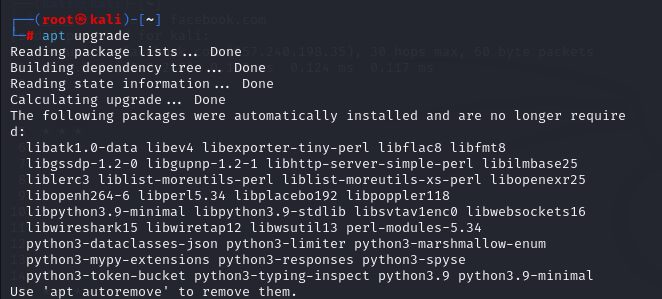
1. Mtr:-

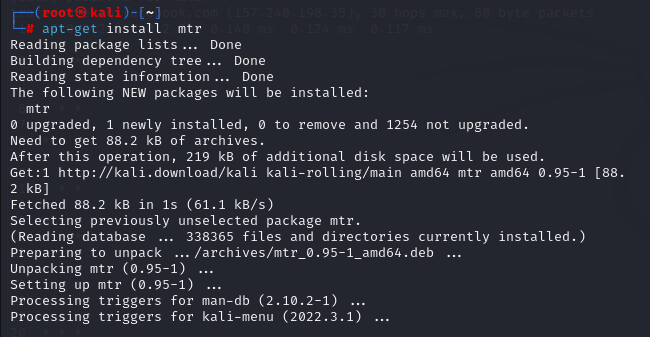
Step 1: apt Update

Step 2: apt Upgrade

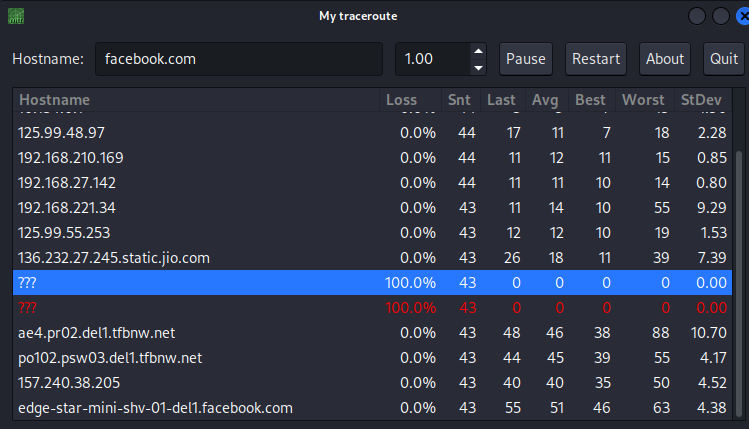
Step 3: apt-get Install mtr

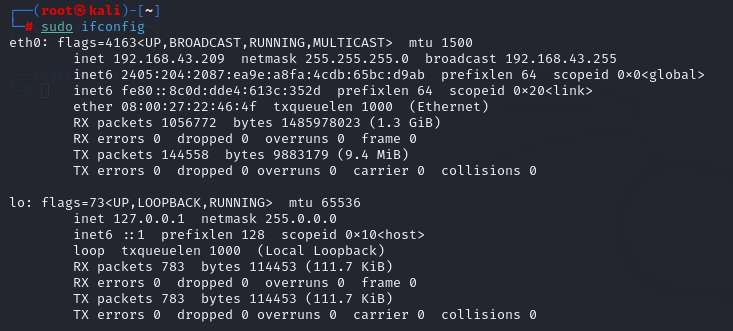
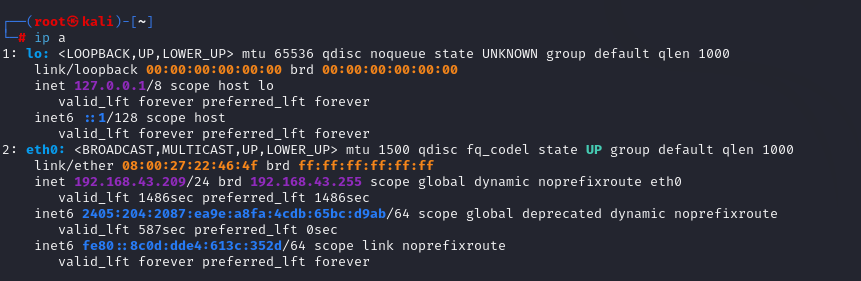




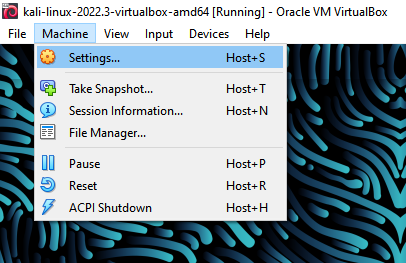


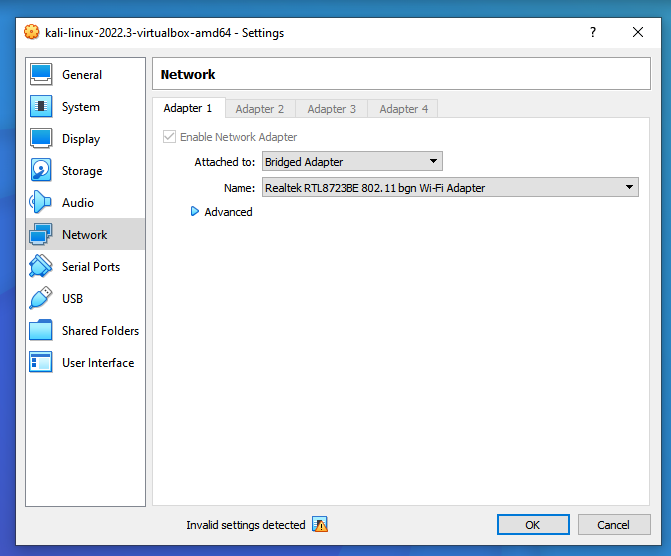


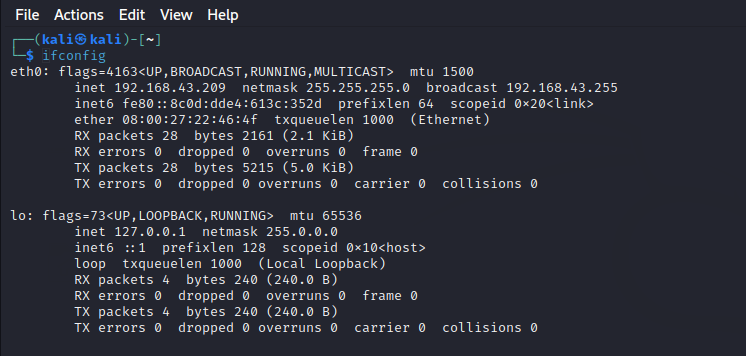


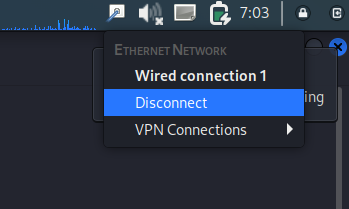
12. Ifconfig:-13. Ipconfig:-

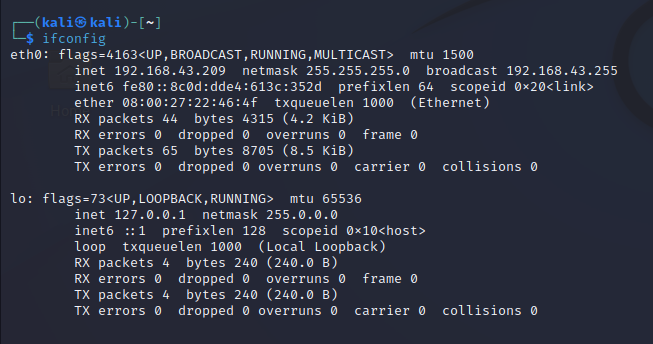
1. Kali and Putty



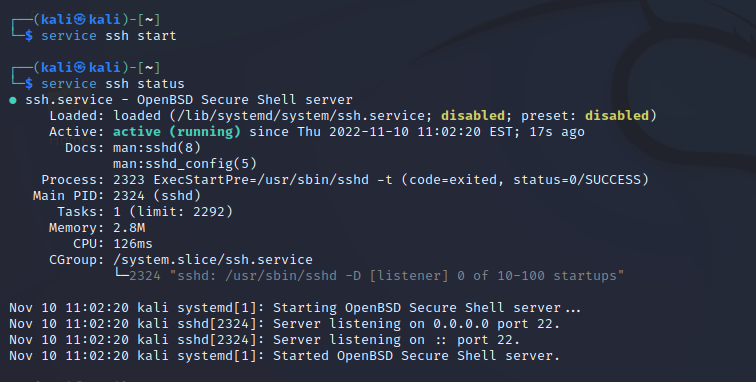


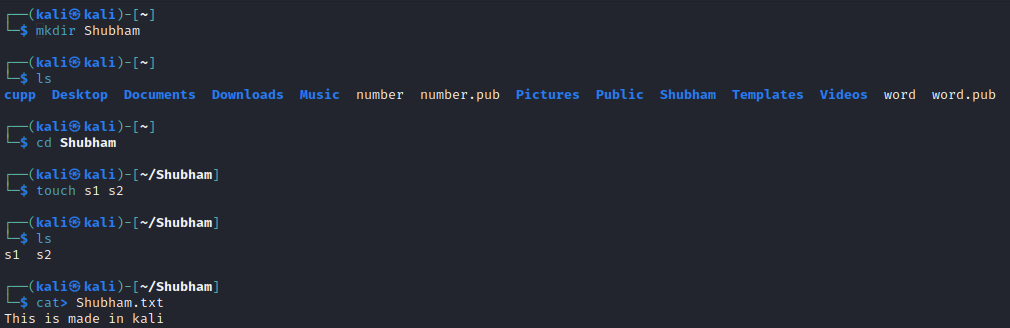


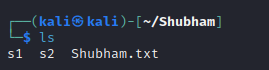


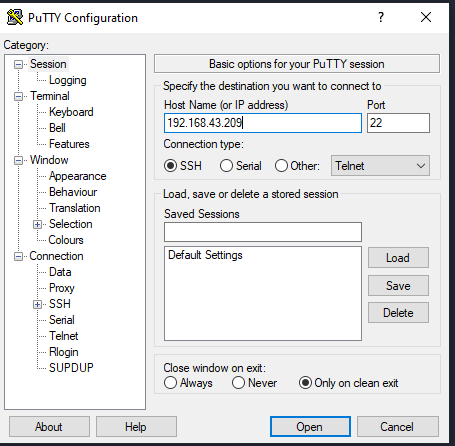


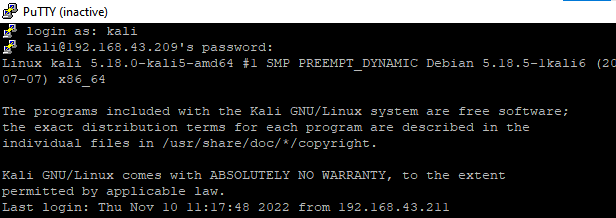


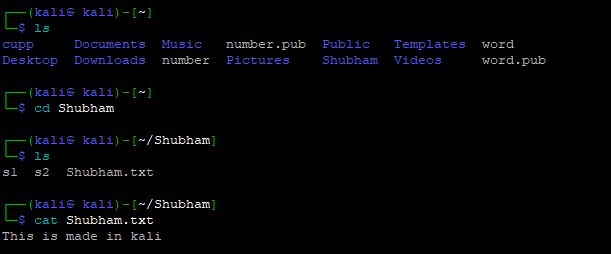


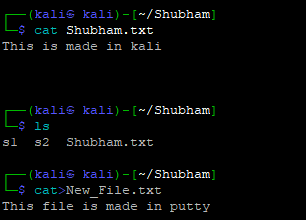


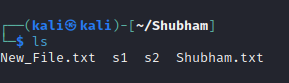


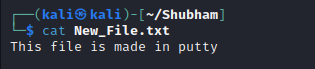










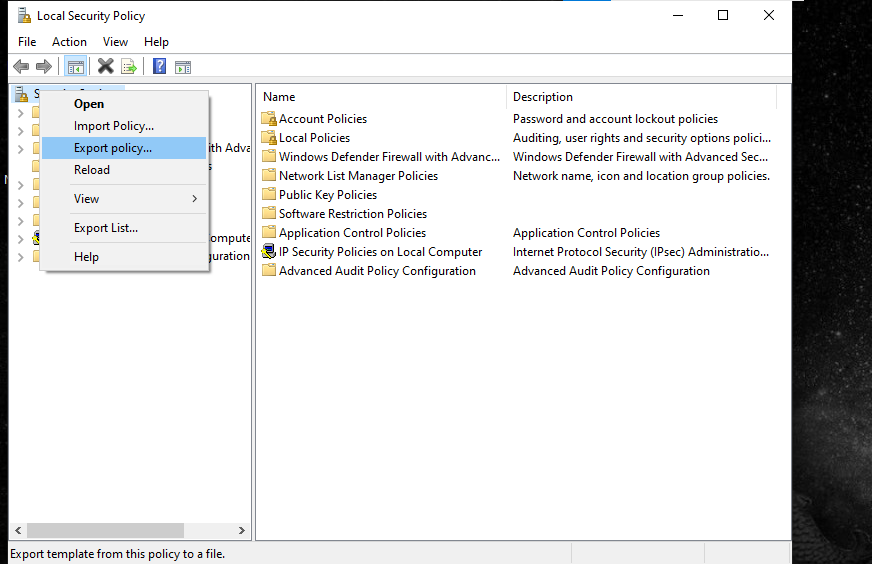


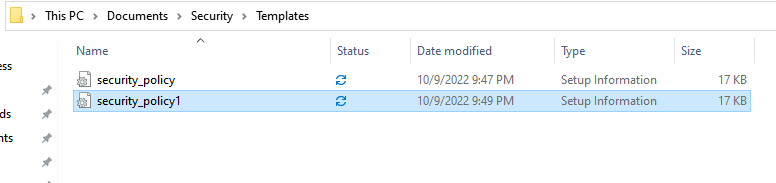
**PRACTICAL NO.:-07**

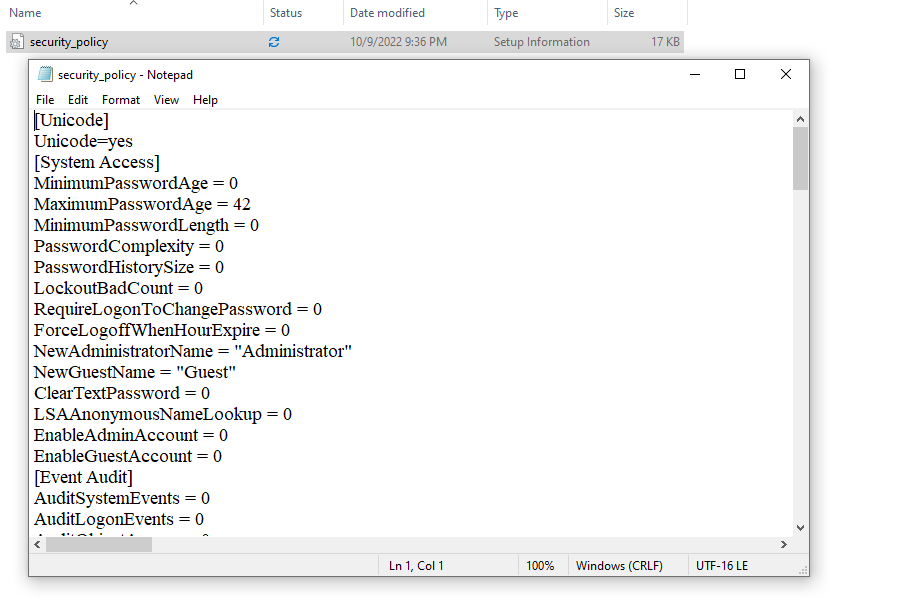
**AIM**:- Implementing Linux Policy using Commands

a.Implementing security using commands

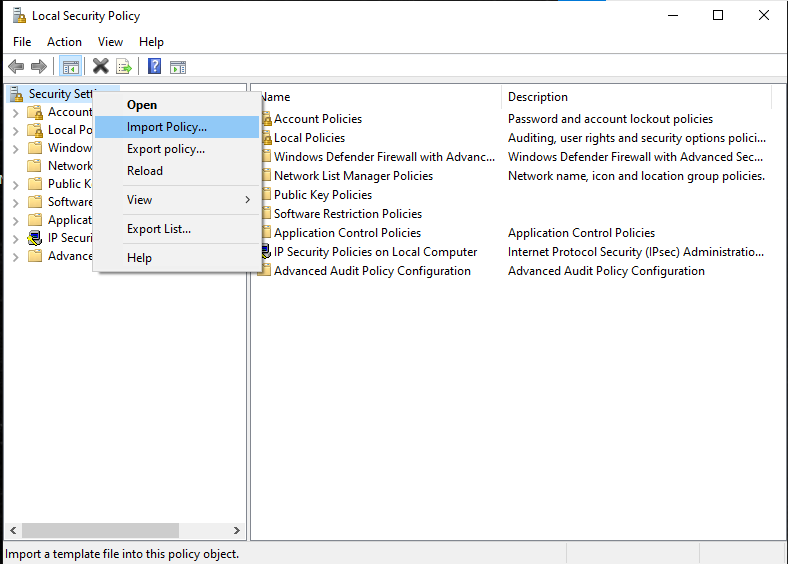


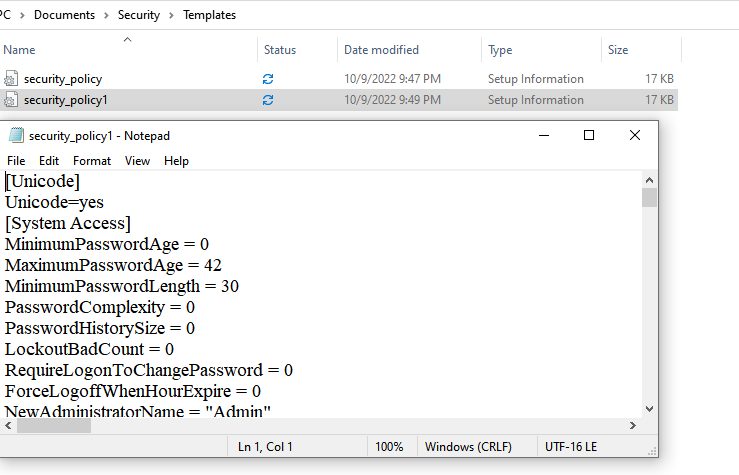






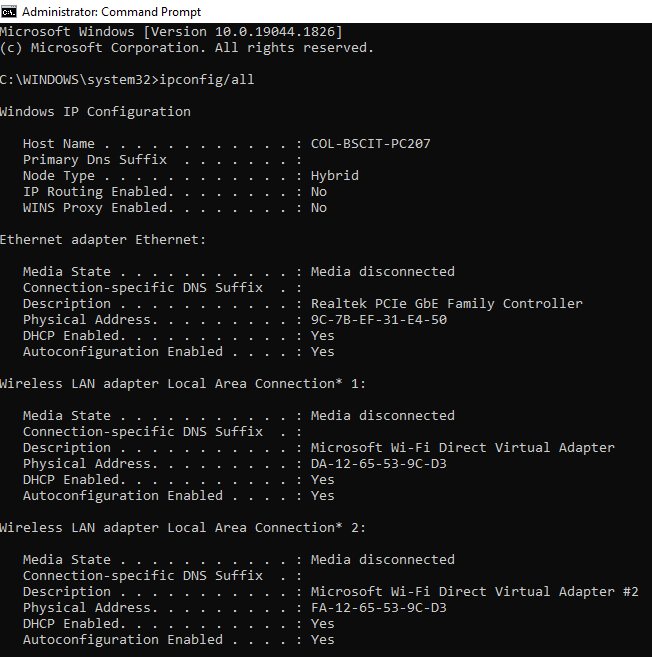


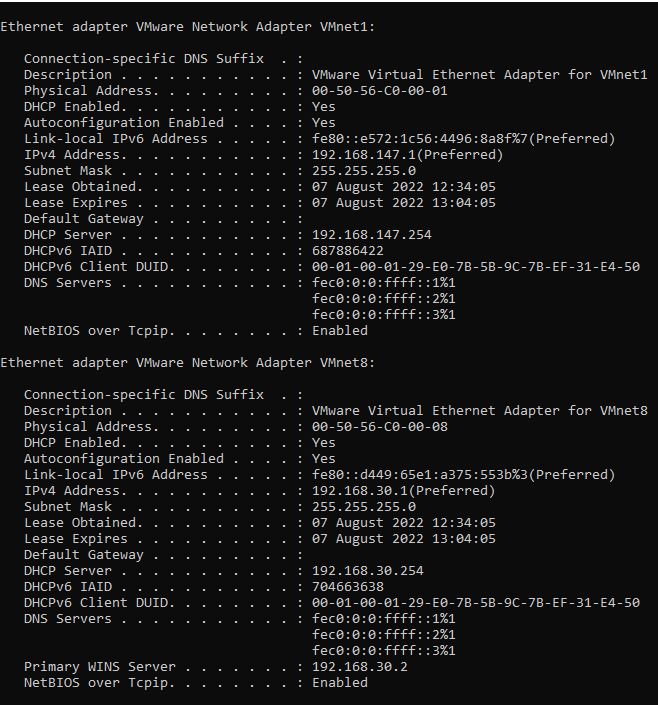


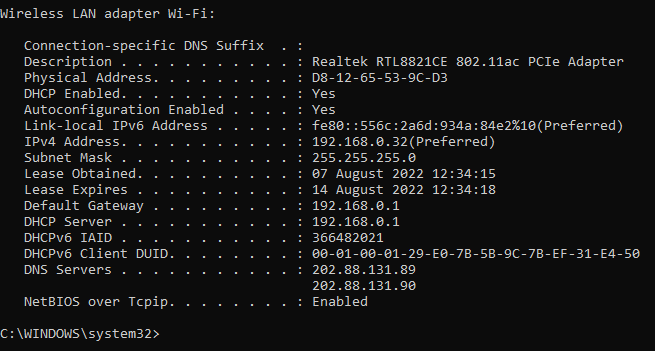


**b) Monitoring security using commands**

1) CIP gateway DNS & other information: ipconfig/all



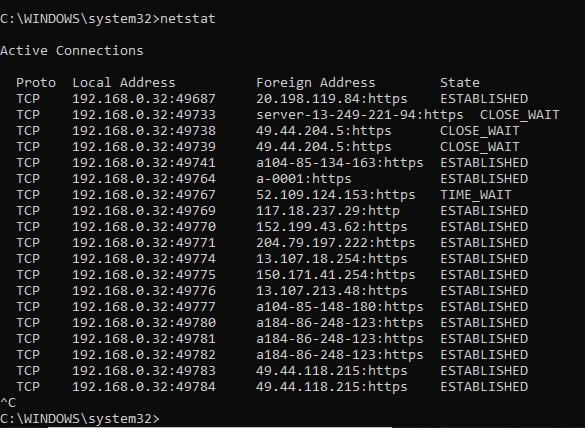




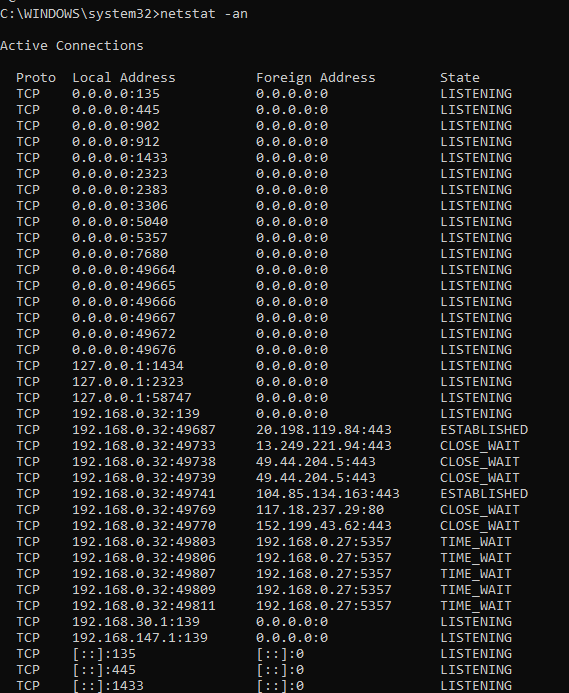
2) a) See connection status: netstat (Network statistics)

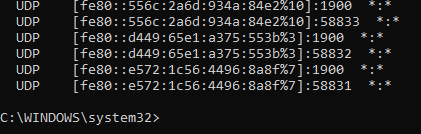
Command line monitoring tool for monitoring network connections

All network connections that are open and port information (on which port it is currently listening )

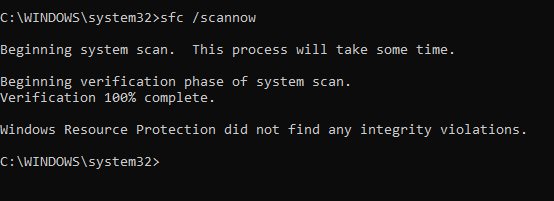


b) For monitoring: netstat -an



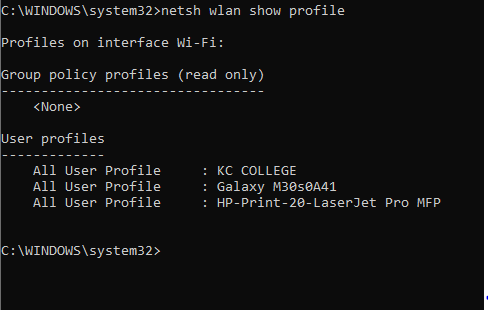


3) System file checker : sfc /scannow

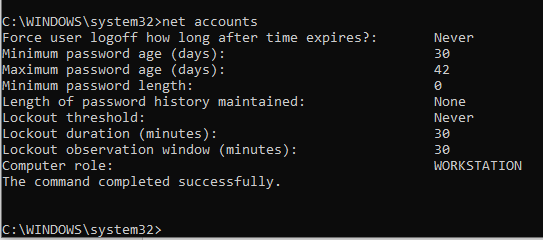


4) Wifi password: netsh wlan show profile

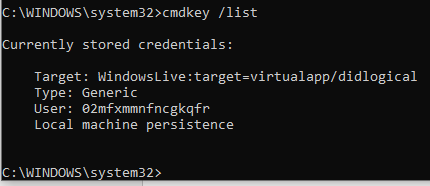
Shows our PC Wi-Fi information which is connected to Wi-Fi till date



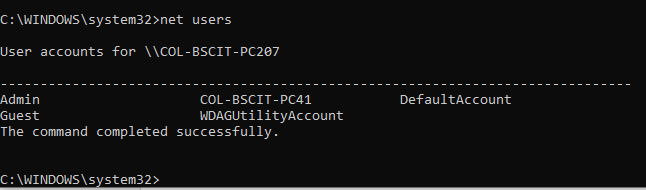
5) To check password policies of account : net accounts



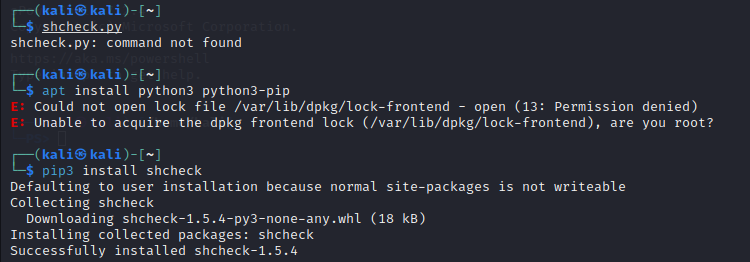
6) List all the credentials of your system : cmdkey /list

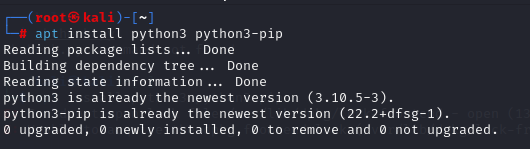


7) Display all the users of your system : net users

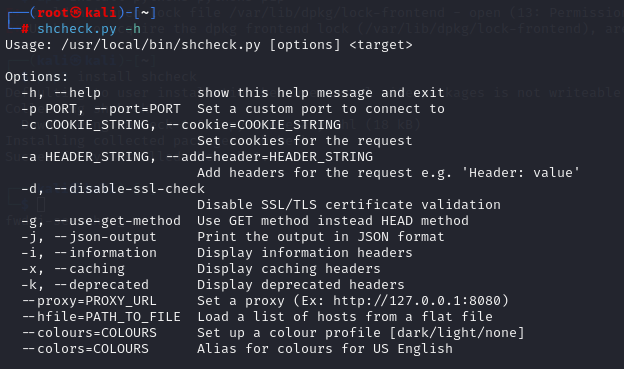


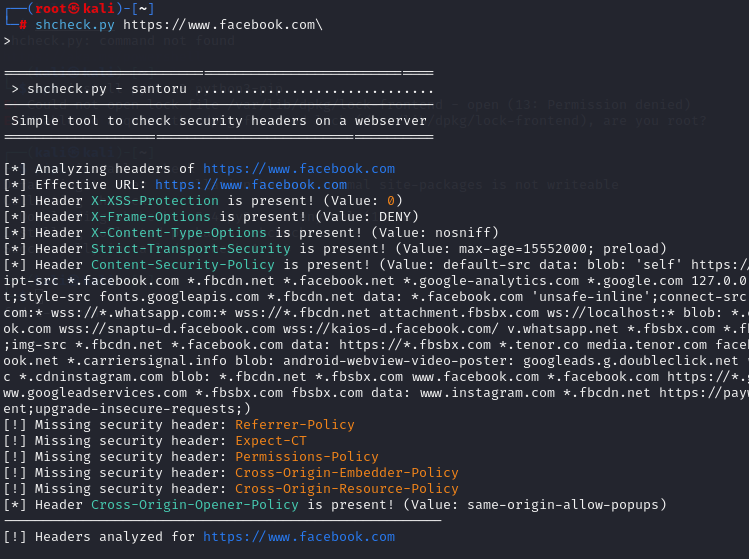
1. Shcheck-Tool to check Security Headers in Kali Linux



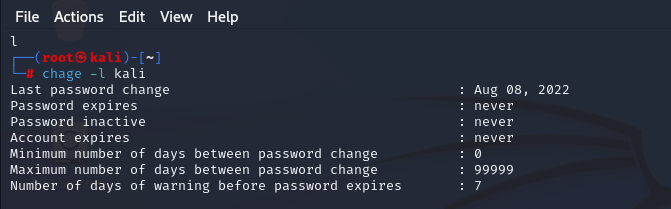




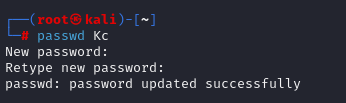


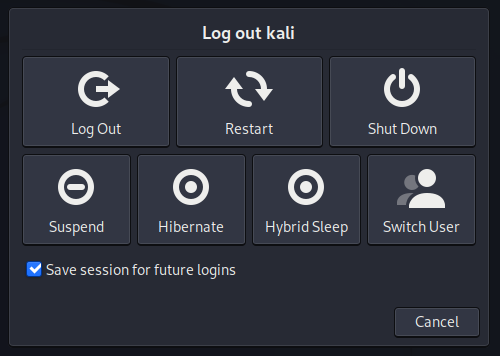


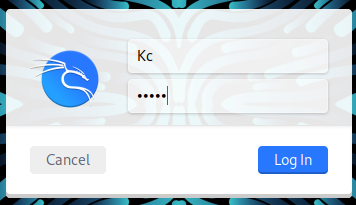
### d.Using Aging Policy

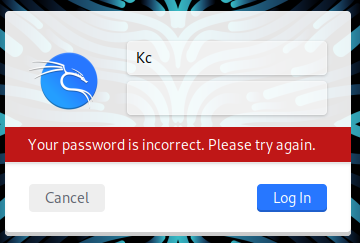


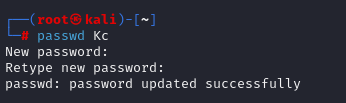


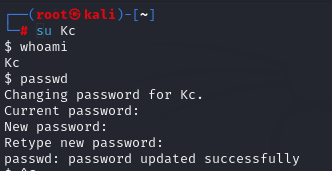


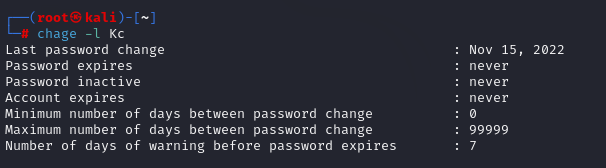




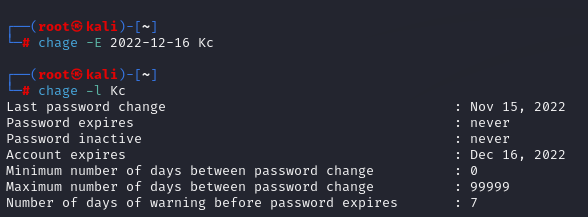


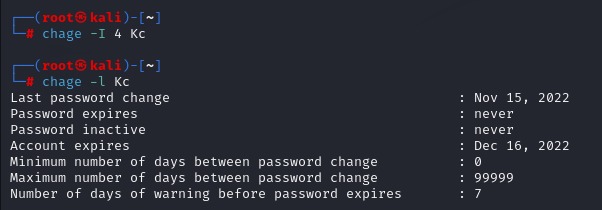


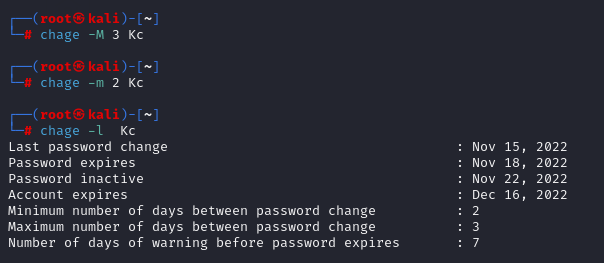


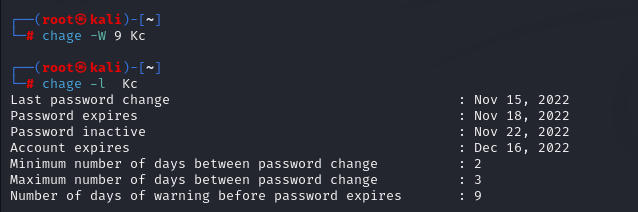




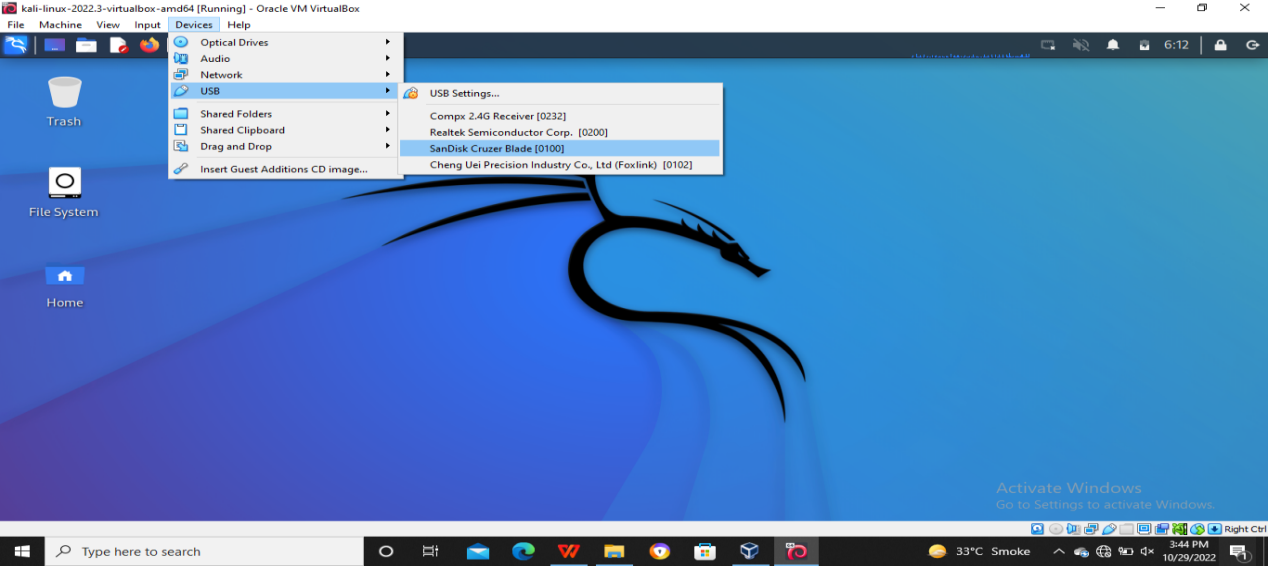


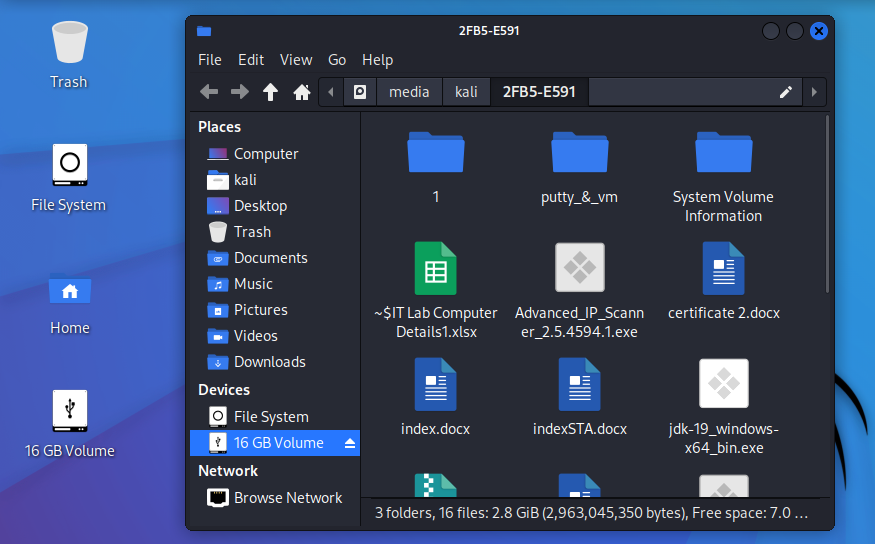


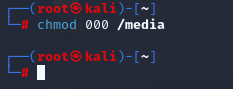




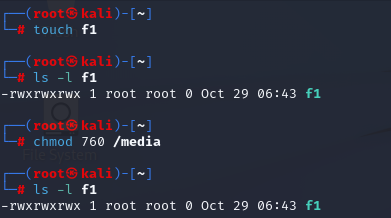
e.Disable booting from external device

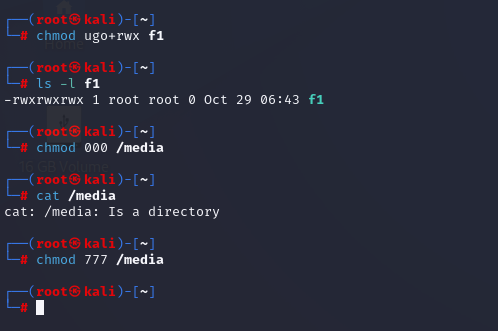






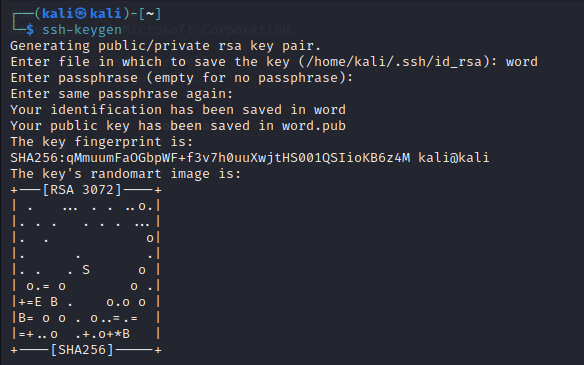


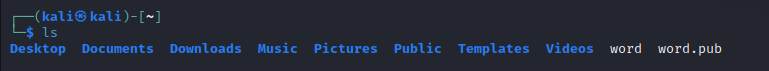


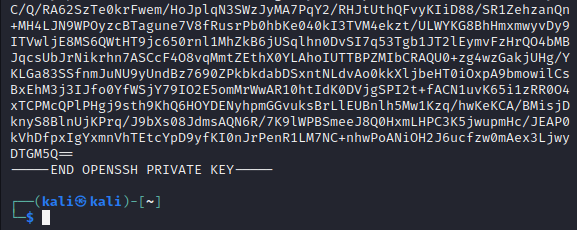
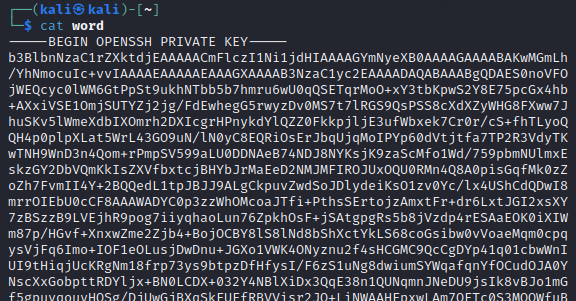


f. Generate SSH Key Pair

Keygen:public and private key



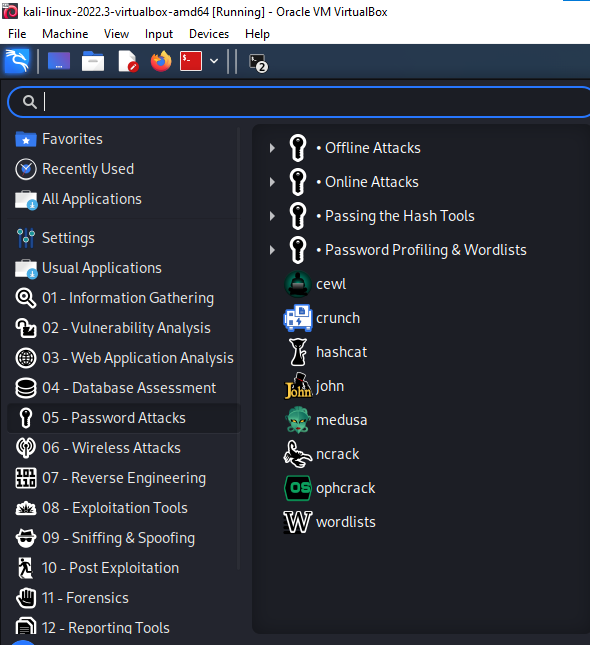


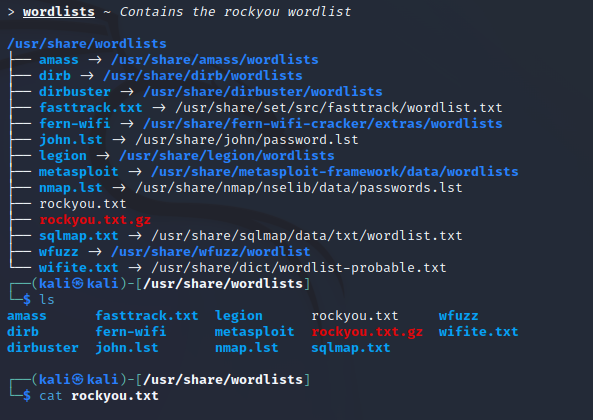


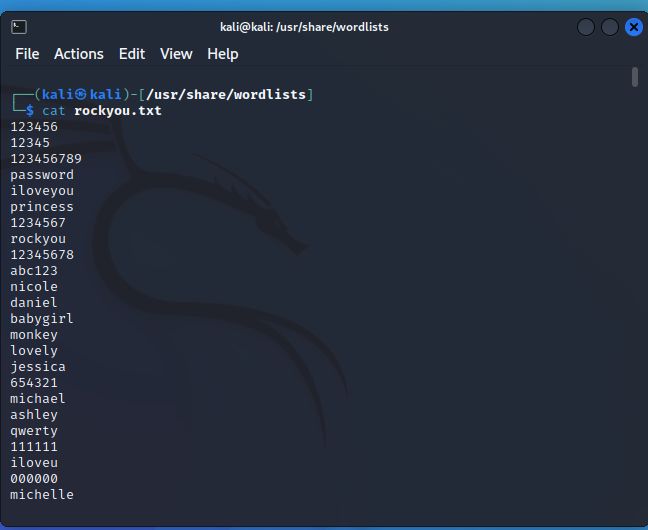
**Practical No.:-08**

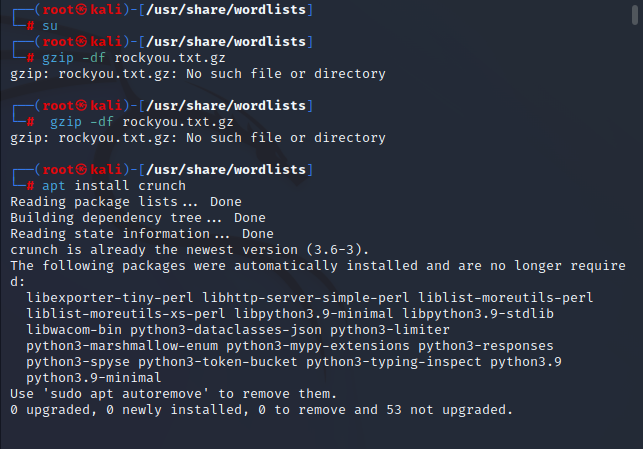
**Aim:-**Password Attack

a) Locate wordlist in kali.

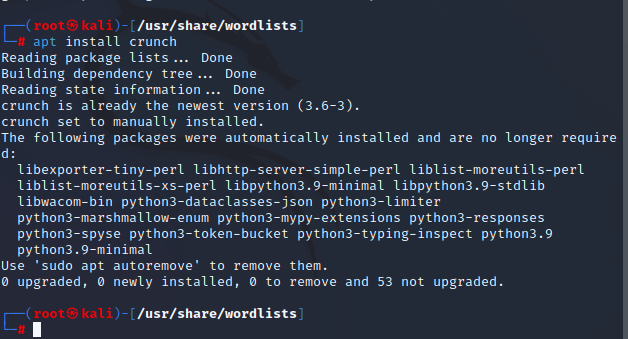


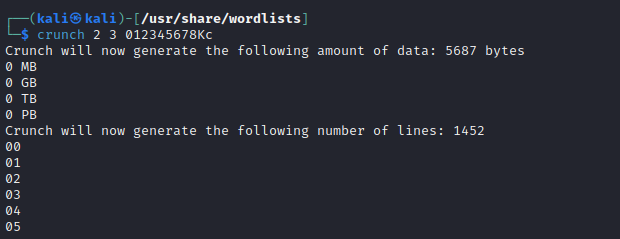


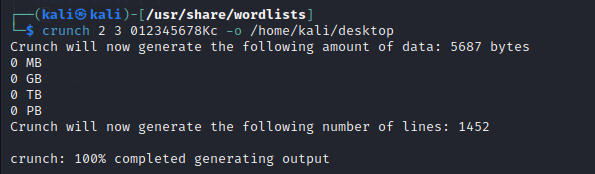




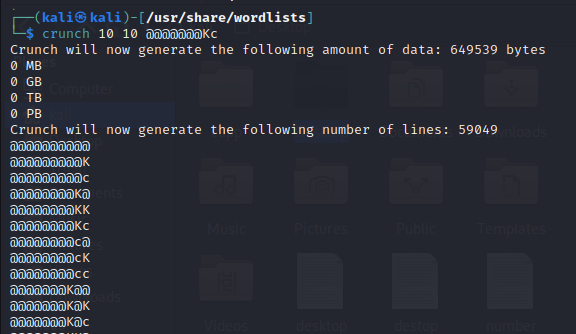
b) Create Wordlist using crunch.











C.Create wordlist for bruteforce attack using cupp.

