**Practical 4**

Use nmap scanner to perform

Ack is used to map our fireball toolset determining wether they are state full or not and which port are filtered . back is used to map out the fireball tool set. It never determine open port Even open\_filterport

syn(steath) scan (-sS)

Cmd:- namp -p22, 113, 139

Scanme.nmap.org

Sync scan is the default and the most popular scan option for good reason. It can be performed quickly scanning thousand of code ports per second on a fast network not hamper by impressive fireball .

**1)Fin Scan :-**

**cPMMAMD**

**NMAP\_SF\_T4 PARA**

**2)Null scan:-**

dOES NOT SET ANY BIT(TCP black header)

CMD:- namp -sN-p 22 scanme.nmap.org

**3) XMS scan**

Set the fin , urg , psh ,flash, lighting the packets up using the christmas tree

Command

Nmap -sx\_T4 scanme.nmap.org

**4) DISCOVERY SCAN**

-sp(ping)

S-sL(ping)

-sD (protocol)

-T-connect-sS

-sN

-XX(xmas)

-sAck(acknowledgement)

-sW(windows)

Trace -n (do not look up dns)