**EXPERIMENT NO – 11**

**AIM**: Implementation of Network Security Tools and Technologies Lab.

Windows firewall :

Windows Firewall is a stateful firewall that inspects and filters all packets for IP version 4 (IPv4) and IP version 6 (IPv6) traffic. For measuring the performance of windows firewall, first rules are created for inbound and outbound connections and then performance is measured by enablining and diseabling the firewall rule. Rule creation In firewall, firewall rules are to created to allow this computer to send traffic to or receive traffic from. Firewall rules can be created to take one of two actions for all connections that match the rule's criteria: allow the connection or block the connection. Rules can be created for either inbound traffic or outbound traffic

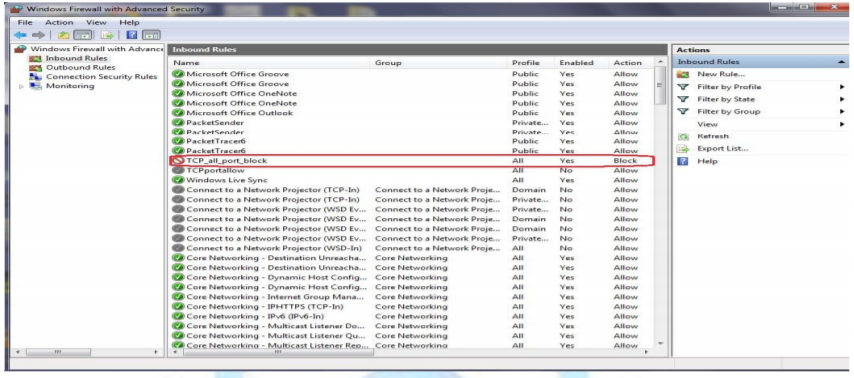
The rule can be configured to specify the computers, programs, services, ports and protocols. As IT environment changes, user might have to change, create, disable or delete rules. Rule creations involve following steps.

Step 1. Select the rule category either inbound (for incoming connection) or outbound (for outgoing connection)

Step 2. In the second step select the rule type, which type of rule would you like to create? program, port, predefined and custom

Step 3. Select any one rule. For eg. Rule for port has selected, now specified the port number (80,25,20,21) and the protocol (TCP,UDP).

Step 4. Select the action which can be performed if rule matched whether block the connection or allow the connection.

Windows firewall creation: 

Linux firewall:

Iptables is an application program that permits a system administrator to configure or manage the iptables provided by the Linux kernel firewall. It is used to setup, maintain and inspect the tables of IP chains. It is a consol based firewall service program that uses policy chains to accept or reject the network traffic. When any connection is tried to establish from any network to private network either inbound or outbound, iptables check for a rule in its stored rule base. If there is a match found then corresponding action take place, otherwise default action is applied. Iptables uses three different chains: input, forward and output.

• Input – This chain is used to control the all incoming connections from the public network. For example, if a user attempts to TELNET or SSH into your PC/server, iptables will attempt to match the IP address and port to a rule in the input chain.

• Forward – This chain is used for incoming connections that are not actually being delivered locally same as router that forwards the packets to its outgoing links

. • Output – This chain is used to control all the outgoing connections from private network to public network. If user tries to access facebook.com, iptables will check its output chain to see what the rules are stored regarding to http before making a decision to allow or deny the connection. There are three types of connection-specific Responses in Iptables

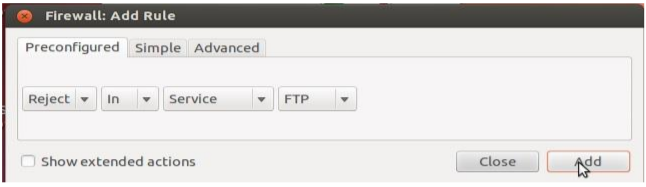
• Accept – Allow the connection.

• Drop – Drop the connection, act like it never happened. This is best when user does not want the source to realize his/her system exists.

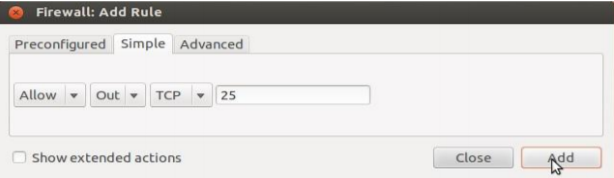
• Reject – Do not allow the connection, but send back an error to the originator. This is best if user does not want a particular source to connect to his/her system, but user wants them to know that his/her firewall blocked them.

For measuring the performance of Linux firewall, first rules are created for inbound and outbound connections and then performance is measured by enablining and diseabling the firewall.

Rule creation Gufw is a graphical uncomplicated firewall that provides user-friendly frontend to IPTables. It is used to manage the rules and policies of IPTables in easier way.Gufw allows the administarator to create preconfigured, simple and advanced rules

Creating rule to reject FTP: 

Shows a firewall rule that will allow tcp port 25 to any address on this host.



Shows ufw status that contains all the created rules.

