1. Steps in cracking network :

* INFORMATION GATHERING about the target , publicly available information and social engineering.
* PORT SCANNING in order to identify all the open ports on a target system.This will indicate which ports are open and which applications can be targeted.
* NETWORK ENUMERATION Thereafter the hacker would attempt to discover which applications or OS are being ran.Hacker can also attempt to distinguish workstations from servers.
* GAINING AND KEEPING ROOT/ADMINISTRATOR ACCESS : After gathering all that information hacker will attempt to gain access to the user account.
* Used the gained access ,leaving backdoor and covering the tracks.

1. SECURITY POLICY is the philosophical and structure of organisations security efforts.

* Security policy defines the acceptable use of computing resources.
* Who has access to what
* It acts as a security contact with the employees

1. FIREWALL

* There is a first firewall the intercepts all the web traffic.
* It is simply a software that is loaded up either on a workstation or a server.

PACKET FILTERING FIREWALL

* Provides NAT FEATURE.
* As packet arrives it determines which port it is supposed to be sent to.
* Device uses an internal table to map whicj port the packet would need to be directed to.
* We can download zone labs firewall to install it on the workstation.

STATEFUL FIREWALL

There are two major drawbacks to packet filtering firewall.

It doesn't examine the actual payload.

Once the packet is passed through the firewall the firewall has no track of what occured with previous packets.

Does it matter what a packet does once it’s been approved by the firewall? Indeed it does. Some system crackers can design packets that

change the port to which they are destined after they pass through a firewall. For example, a packet might be addressed to port 80 so that it

can pass through a firewall that has port 25 (SMTP) closed. Once the packet is onto the local network, it changes its port so that it can access

the e-mail server and leave a virus or other malware behind.

* Keeps track of all the incoming and outgoing TCP sessions.
* When a packet originates from local network STATEFUL firewall keeps track of the destination address and allows traffic back from the destination to the local network.
* If a packet that appears as a response to an internal request but it doesn't correspond to an existing TCP SESSION will be blocked as well.
* In addition, a stateful firewall monitors the port used by packets once they enter the local network, and blocks packets that attempt to change their ports.
* Like packet filtering firewalls, stateful firewalls work at levels 3 and 4 of the TCP/IP protocol stack and are therefore relatively independent of the application to which packets are destined.

APPLICATION PROXY FIREWALL

* Operates at application layer of TCP/IP model.
* Sits between app and the external world , monitors the traffic.
* Provides a high degree of logging and security.
* Major limitation is that we need a separate proxy for each application.

1. SERVICES.MSC

Windows has a lot of unwanted services running in windows that have to be manually disabled in order to make the system more secure.

In Linux we use /etc/services

1. Netstat -an

gives list of all the ports that are running on the host.

1. BASIC DIG SYNTAX :

dig example.com

QUERY A SPECIFIC SERVER

dig @8.8.8.8 example.com

1. Network mapper user ICMP packets which is extension to the IP that defines packets carrying error ,control and information messages.