Vansh Pahuja
DA1 | 50

CSS lab

Aim: a) Study the use of network reconnaissance tools like whois, dig, traceroute, nslookup. to gather information about networks and domain registration.
b) Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan, etc.
c) Setup personal firewall using iptables.

Theory:

a) Network Reconnaissance.

i) WHOIS:

It gives information about any property on internet like. whois on google gives its domain information.

2) Traceroute:

It is used to show the route data packets data take to reach their destination.

3) Dig:

The domain information groper (dig) is a flexible tool for interacting DNS name servers.

4) Nslookup:

It is used to trouble shoot DNS. It is a network administration command line tool for querying the Domain name system to obtain the mapping between domain name & IP addresses

or other DNS records.

b) NMap:

It is used to discover hosts and services on a computer network by sending packets and analyzing the responses. It provides a number of features for probing computer network including:

1) Host Discovery: identify hosts on network
2) Port scanning: Enumerating the open ports on one or more target hosts.
3) Version detection: Interrogating listening network services listening on remote devices to determine the application name & version numbers.
4) OS Detection: Remotely determining the operating system and some hardware characteristics of network devices.

→ Basic commands working in Nmap:

1) For target specifications: nmap <target URL or IP addr>
2)
2) For OS detection:
nmap -O <target URL OR IP>
3) For version detection:
nmap -sV <target host's URL or IP>

c) Firewalls:

1) All modern operating systems come equipped with a firewall software application that regulates network traffic to a computer.
2) Firewall creates a barrier between a trusted network and an untrusted network.
3) Firewalls work by using rules that govern which traffic is allowed and which is blocked.
4) The utility firewall developed for Linux system is iptables.

Steps:

1) sudo iptables -L : To check current iptables rules.
2) Login to the server as root user.
3) a) Follow the syntax below for various iptables rules.
   b) Add iptables rule to block IP Address.
   c) Add iptables rule to block ip address to access a specific port.

iptables -A input -s IP-Address-here -p tcp --destination port port-number -j Drop.

d) Drop / Remove iptable rule to unblock IP Address.
iptables -D input -s IP-Address-here -j DROP
e) DROP / Remove iptables rules to block IP Address access to a specific port.
IP tables -D Input -s IP-Address-here -ptcp --destination-port port-number -j DROP.

2) After adding/ removing any of the above rules we need to save the iptables rules by the following command iptables-save.

* Conclusion:

Thus, I have successfully implemented network reconnaissance tools, nmap and personal firewall.