AIM:-Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars

Theory:-

Network reconnaissance is the process through which threat actors collect information about target networks before mounting an attack. It typically involves the use of techniques such as networking scanning and probing to identify potentially exploitable vulnerabilities.

Network Reconnaissance involves identifying and mapping network assets to locate potential entry points. It is often the first stage in Automated Penetration Testing scenarios.

Network reconnaissance is important because it provides actionable information on network vulnerabilities and security posture.

For threat actors, this is essential as it enables them to establish a plan of attack.

For defenders, understanding these methods is equally important because it enables them to identify and mitigate exploitable vulnerabilities through vulnerability management practices, which systematically prioritize and address network weaknesses.

The purpose of network reconnaissance is to learn technical details about open ports, IPs, security, active services, security mechanisms, and more. This information helps threat actors establish a clear understanding of IT infrastructure and network topology so as to map out potential entry points and attack paths. For defenders, this information enables the anticipation of certain attack vectors so that defenses can be strengthened preemptively through automated penetration testing methods.

During this process, threat actors employ a variety of different techniques to help them uncover network vulnerabilities. These include the following:

Whois

ipconfig:

Displays current IP address, subnet mask, default gateway, and other network configuration details. Using ipconfig /all provides more comprehensive information including MAC address and DHCP status.

Ipconfig

ipconfig/all

Ipconfig displaydns

ping:

Verifies connectivity to a target host by sending ICMP echo requests and measuring response times.

Ping

Ping destination

Ping -t destination

tracert:

Maps the route packets take to reach a destination, showing the hops (routers) involved and their respective response times.

netstat:

Displays active network connections, listening ports, routing tables, and network interface statistics. Options like netstat -a show all connections, netstat -b (requires administrator privileges) shows associated executables, and netstat -n displays numerical addresses without name resolution.

nslookup:

Queries DNS servers to resolve hostnames to IP addresses and vice versa, and to retrieve other DNS records.

arp:

Displays and modifies the Address Resolution Protocol (ARP) cache, showing the mapping between IP addresses and MAC addresses of devices on the local network.

route:

Manages network routing tables, allowing display and modification of routes.