Aim: knowing about CyberSecurity tools.

1. Nmap

Nmap is short form of Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Nmap helps you to quickly map out a Network without sophisticated commands (or) configurations. It also supports simple commands and complex scripting through the Nmap scripting Engine

We use Nmap in our kali linux Command-d promt.

Let's take a command of Nmap.

Syntax

nmap <ipaddress>

nmap 192.10.0.11

port	state	service
22/tcp	open	ssh

25/tcp	filtered	smtp
30/tcp	open	http

. . .

Zenmap

Zenmap is the official Nmap security scanner GUI. It is a multi-platform free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved & viewed later. Saved scan results can be compared with one another to see how they differ.

Commands

Open zenmap and then set Target Ip address 10.0.8.1/24 and set profile to Quick scan plus and then click on scan it starts scanning and then click on topology to we can see a diagram.

We can observe the image with colors. The colour changing says they are dead hosts or live hosts and servers.

Task Manager

Task Manager shows the services that a system performs
so to see the services open task Manager and click on services option
It shows all the services that are going in the system up to present
it gives Name, PID, Description, and the type of service it provides.

Angry ip Scanner

It is an open source and cross-platform network scanner designed to be fast, and simple to use. It scans IP address and ports as well as has many other features. It is widely used by network administrators and just curious users around the world, including Large and small enterprises, banks, and Govt Agenc -ies. It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.

Open Angry ip Scanner and set the Ip range and then set IP^ value and click on start to start the scanning.

The Result comes below

The Balls which are Red in colour are dead and Balls of Blue are live and Balls of Green are the servers.

We can Open the services of green in google chrome to check out their Website

for Example from Ip range

14.97.0.0 to 14.97.255.255

We have many websites like

Ip 14.97.1.22 has DBMS i.e., Mysql Website

Ip 14.97.0.27 is the website some spy cams etc.,

We have many of them some off them does not open so that indi-cates the protection of those Website by the Firewalls.

Advanced Ip Scanner

Advanced Ip scanner is a free network scanner that can locate and analyze all computers available on your wireless or wired local network. With its help, you can get remote Acess to all pcs, such that you can copy and share files present on the sha -red folders and turn off systems remotely. The Application is portable and can be used bynetwork admins anytime, any where. The primary purpo -se of a network scanner is to Help administrators manage devices conne -cted to a local network.

Commands

Open Advanced Ip Scanner and then give the Ip address in the consent column and then Click on Scan. It gives all the systems internal things likes the directories of the other system to access and down -load files.

Global Network Inventory

It is a powerful and flexible software and hardware inventory system that can be used as an audit scanner in an agent-free and zero dep -loyment enviroments. If used as an audit scannar; it only requires full administrator rights to the remote computers you can wish to scan. Global Network Inventory can audit remote computers and even network printers, document centers etc.,

Global Network Inventory agent can also be deployed to perform regular audits initiated through the domain logic script when your users log on the Network.

Commands

Open Global Network Inventory and click the default settings.