WANMAP

An Information Gathering Web Application

How would WANMAP work ?

“**WANMAP**” would be a network mapping tool (a web interface for a very popular Information Gathering tool “NMAP”) where “NMAP” requires a setup installation before using (Generally). Where, on the other hand “**WANMAP**” would be accessible from anywhere over the Internet. No setup installation would be required to use.

Idea behind WANMAP.

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

.. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Why NMAP.

NMAP is a widely popular tool among the cyber security professionals and it is still being used tremendously in the field of Information Security or Ethical Hacking, which helps an analyst to analyze a particular target and collect as much as information, which is further used in finding the existing vulnerabilities and helps an organisation or an individual to secure their network infrastructure.

USE OF NMAP

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.

Features

- Host Discovery
- Vulnerable/Open Ports Detection.
- Script Support from NMAP API. (for extended Vulnerability scanning).
- Operating System Detection.

Technology Use

- Python
- Django
- API (NMAP)
- Web
- Socket Programming

Reference

https://drive.google.com/file/d/1OmhUKzZVmFHEE9yrtpWHVWrdnIkf232B/view?usp=sharing

THANK YOU