**What is Nmap?**

Nmap is short for 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.

Gordon Lyon (pseudonym Fyodor) wrote Nmap as a tool to help map an entire network easily and to find its open ports and services.

Nmap has become hugely popular, being featured in movies like The Matrix and the popular series Mr. Robot.

**Why use Nmap?**

There are a number of reasons why security pros prefer Nmap over other scanning tools.

First, Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.

**Other features of Nmap include:**

Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.

Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.

Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.

During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.

Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

**How does it work?**

Nmap works by checking a network for hosts and services. Once found, the software platform sends information to those hosts and services which then respond. Nmap reads and interprets the response that comes back and uses the information to create a map of the network. The map that is created includes detailed information on what each port is doing and who (or what) is using it, how the hosts are connecting, what is and is not making it through the firewall, and listing any security issues that come up.

How is all of that accomplished? Nmap utilizes a complex system of scripts that communicate with every part of the network. The scripts act as communication tools between the network components and their human users. The scripts that Nmap uses are capable of vulnerability detection, backdoor detection, vulnerability exploitation, and network discovery. Nmap is an extremely powerful piece of software, but there does tend to be a good deal of background knowledge required to use it correctly.

Internet security companies can use Nmap to scan a system and understand what weaknesses exist that a hacker could potentially exploit. As the program is open-source and free, it is one of the more common tools used for scanning networks for open ports and other weaknesses. At Holm Security, we use this technology in a very effective way, as we provide an excellent web-based security service, which ensures that the clients’ ports remain securely closed to those not granted permission.

**Conclusion**

Whether you are a private user with important information on your system, a major corporation or a government agency protecting a wealth of highly sensitive data, Nmap can provide the level of knowledge and pre-emptive thought required to keep things safe.

VIDEO LINK

https://drive.google.com/file/d/1fkyP912ANJMvGVoqtS7-5A3PXmMwr4N\_/view?usp=sharing