What did I do?

I conducted Nmap scanning for my home network using my IP address 38.50.238.86. Nmap scanning refers to the process of using the Nmap (Network Mapper) tool to explore and analyze network hosts, services, and associated vulnerabilities. Nmap is a popular and powerful open-source network scanning tool that is widely used for security assessments and audits, system administration tasks, and network inventory purposes.

When performing Nmap scan, the tool sends specially crafted packets to target hosts or IP addresses and analyzes the responses received. These packets can be used to determine various aspects of a network, including the status of hosts (whether they are up or down), open ports, running services, operating systems, and even potential security vulnerabilities.

The scan started with NSE (Nmap Script Engine) pre-scanning, which involves loading scripts for scanning. Conducted a Ping Scan to check the host's status and latency, It determines if the host is up and responds to network requests. a Parallel DNS resolution is performed to resolve the hostname associated with the IP address. Performed a SYN Stealth Scan on 1000 ports of the target IP address to determine open, closed, filtered, etc ports, identifying port 3001/tcp as open. It is a stealthy scanning technique that sends SYN packets to establish a connection with the target ports and determines their state. Conducted a Service scan to gather information about the specific service running on the open port. Initiated OS detection to identify the running operating system on the IP address, (Linux 3.X or 4.X). Conducted a Traceroute to measure network distance. Executed NSE script scanning for additional information.

What are the results?

Based on the Nmap scanning output, the following results were obtained: The host at IP address 38.50.238.86 is up with a latency of 0.0036s. Port 3001/tcp is open and running an SSL/nessus? service. Detailed information about the SSL certificate, including its subject, issuer, validity dates, and cryptographic details, was provided. The target device is identified as a general-purpose device. The host is running a Linux operating system with a kernel version between 3.2 and 4.9. Uptime guess suggests the host has been up for approximately 0.421 days. The network distance between the scanning machine and the target IP is one hop.

What did I learn?

From the Nmap scanning process and analysis, I learnt that Nmap scanning provides valuable insights into the network infrastructure, including live hosts, open ports, and running services. This knowledge helps in understanding the organization's or home digital network and its components. The scan output allows for an assessment of the attack surface presented by the network. By identifying open ports and services, it becomes possible to evaluate potential vulnerabilities and areas that may be targeted by cyberattacks. Nmap scanning highlights the significance of implementing strong security measures to protect the network and its components. The presence of open ports or services can serve as entry points for attackers, emphasizing the need for robust security configurations and ongoing monitoring. By detecting potential vulnerabilities or misconfigurations, Nmap scanning emphasizes the importance of proactive vulnerability management. Regular scanning and assessment can help organizations or individual identify and address weaknesses before they can be exploited by malicious actors. The Nmap scanning process demonstrates the value of continuous network monitoring. Regular scans allow organizations and individual to track changes in the network, identify new systems or services, and ensure that security measures remain effective over time.

Overall, the Nmap scanning process and analysis provide valuable insights into the network's components, potential vulnerabilities, and the importance of proactive security measures. It underscores the need for organizations to continually assess and strengthen their security posture to protect against cyber threats.