NMAP Command Options

Ravindra Dagale · Follow
2 min read · 5 days ago

Listen Share

Open in app ↗ Sign up Sign in

Medium Search

1. `-sS` : TCP SYN Scan The `-sS` option initiates a TCP SYN scan, often referred to as a "stealth scan," to determine which ports on a target system are open. This scan technique can help identify potential entry points for attackers while minimizing the risk of detection.

2. `-sU` : UDP Scan UDP scans, facilitated by the `-sU` option, are used to discover open UDP ports on a target system. Since UDP is connectionless and lacks the reliability of TCP, identifying open UDP ports is essential for comprehensively assessing network security.

3. `-O` : Operating System Detection By enabling the `-O` option, Nmap can attempt to determine the operating system running on a target host based on subtle differences in how systems respond to network probes. This information is invaluable for understanding the diversity of devices in your network and tailoring security measures accordingly.

4. `-A` : Aggressive Scan For a comprehensive assessment of a target system, the `-A` option activates aggressive scanning techniques, including OS detection, version detection, script scanning, and traceroute. While more intrusive, this approach provides a wealth of information for thorough network analysis.

5. `-p` : Port Specification The `-p` option allows you to specify which ports to scan, either individually or as port ranges. This flexibility enables targeted scans, focusing only on relevant ports and reducing scan times.

6. `-v` : Verbosity Level Increasing the verbosity level with the `-v` option provides more detailed output during the scan, allowing for better visibility into the scanning process and its results. This can be particularly useful for diagnosing complex network issues.

7. `-T` : Timing Template The `-T` option sets the timing template for the scan, ranging from "paranoid" to "insane." Choosing an appropriate timing template balances the thoroughness of the scan with its impact on network performance and potential for detection.

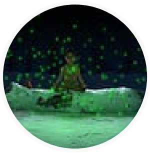
8. `-F` : Fast Scan When time is of the essence, the `-F` option facilitates a fast scan by only scanning the 100 most common ports. This abbreviated scan can provide quick insights into a target system's most critical services.

9. `-sn` : Ping Scan The `-sn` option conducts a ping scan to determine which hosts on the network are online, without actively scanning ports. This preliminary step helps streamline the scanning process by focusing on reachable hosts.

Thank You For Reading, Hope You Liked It…!!! 😊

Ravindra Dagale 🙆
Security Researcher | *Information Security*
Connect at : **Instagram** | **YouTube**

Nmap Commands Information Security Bug Bounty Vulnerability



Follow

Written by Ravindra Dagale

462 Followers

Security Researcher | Information Security

More from Ravindra Dagale

Ravindra Dagale

E: Package ‘libgtkglext1’ has no installation candidate | anydesk : Depends: libgtkglext1 but it is...

Follow the below steps for possible solution of errors:

1 min read · Feb 9, 2024

14 2