1. Nmap: Network Mapper (Nmap) is a very powerful and versatile open-source tool for network exploration or security auditing. It can be used to scan a wide range of ports, or a specific port, like 8585.

nmap -p 8585 <target-ip>

1. Netcat (nc): Netcat is a simple Unix utility that reads and writes data across network connections, using the TCP or UDP protocol. You can use it to check if a particular port is open:

nc -zv <target-ip> 8585

1. Telnet: While not as comprehensive as Nmap or Netcat, Telnet can also be used for basic port scanning:

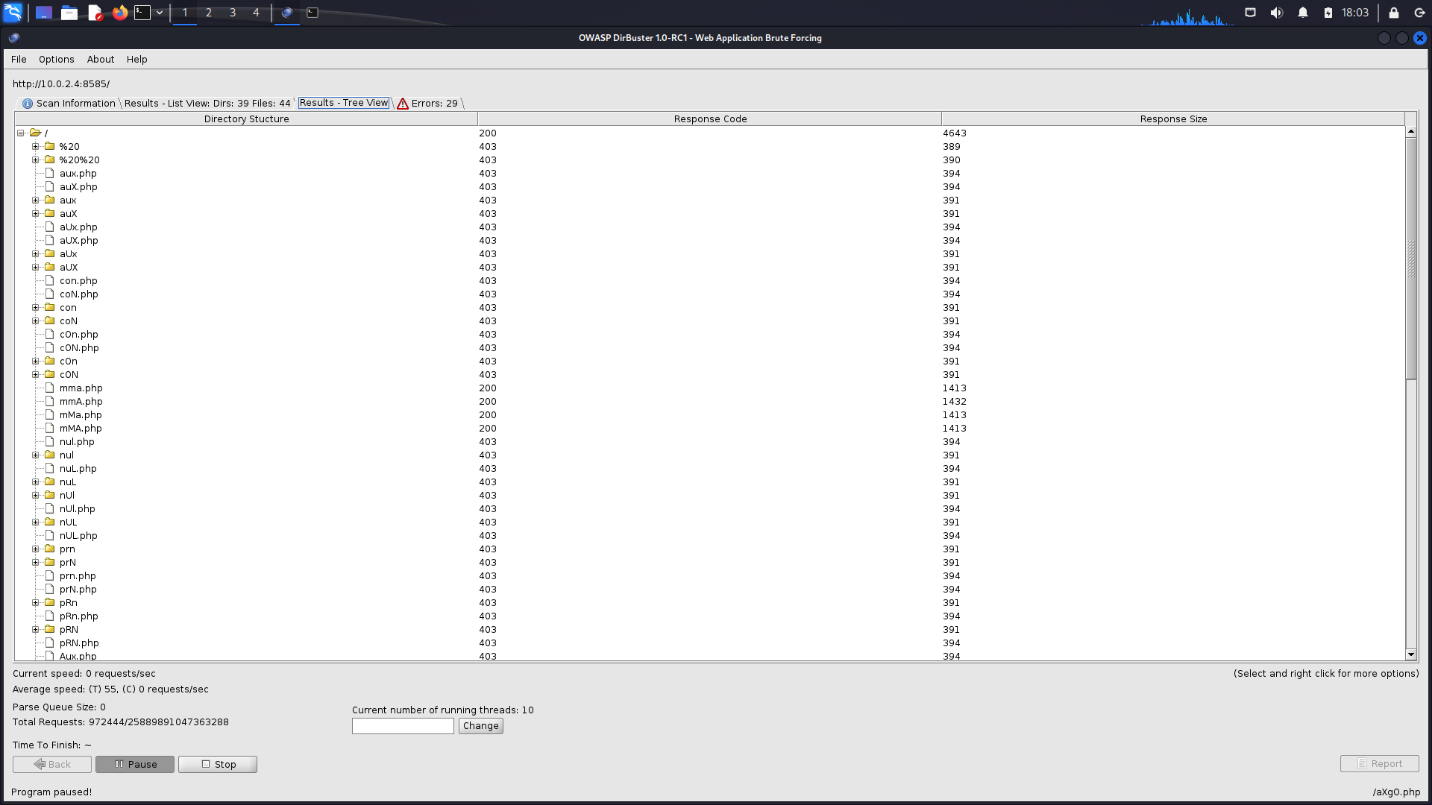
telnet <target-ip> 8585

1. Masscan: Masscan is known as the fastest Internet port scanner. It can scan the entire Internet in under 6 minutes, transmitting 10 million packets per second. It's useful for large-scale scans, but can also be used for a specific port on a specific target:

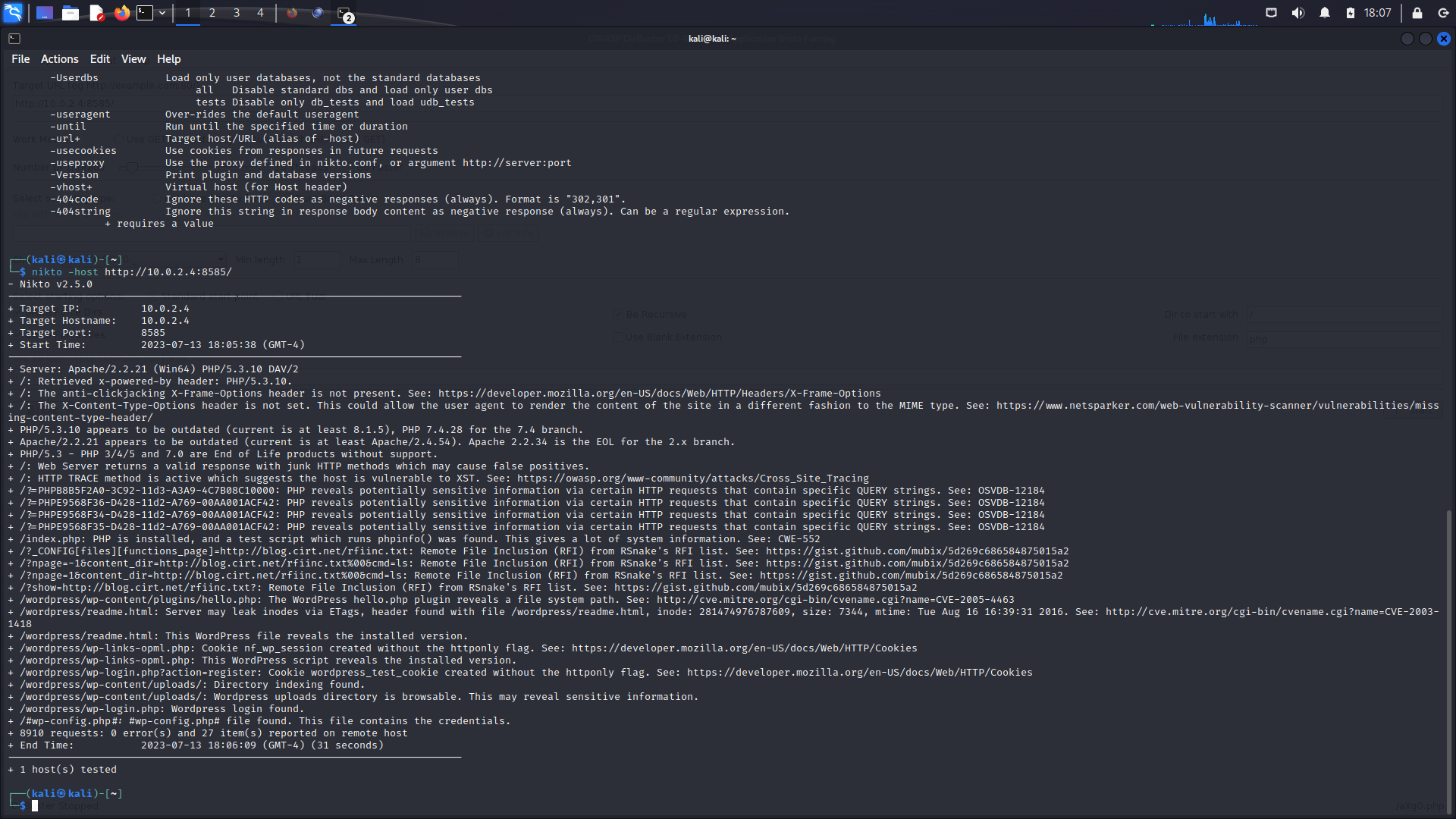
masscan -p8585 <target-ip> --rate=1000

1. Angry IP Scanner: This is a cross-platform port and IP scanner. It can scan IP addresses in any range and any port. It's simple, lightweight, and doesn't require any installation. Just specify the IP and port range, and it'll do the rest.
2. Packet Sender: This is an open-source utility that allows you to send and receive TCP, UDP, and SSL packets. It's very useful for testing network systems and devices.
3. Wireshark: Although primarily a packet sniffing tool, Wireshark can be used to see if there is traffic going to a specific port, effectively making it a way to 'scan' for port activity.

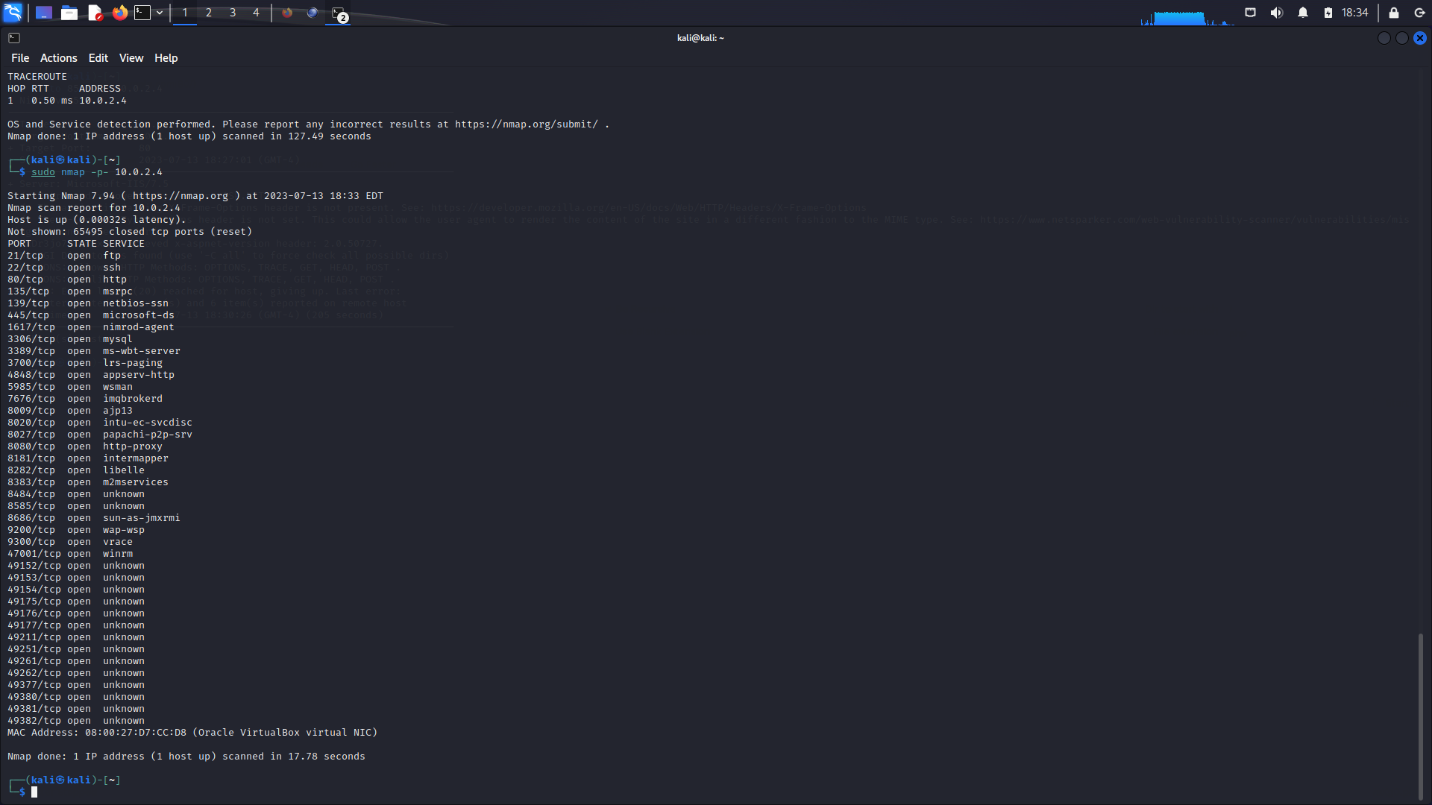
DIRBUSTER



NIKTO



NMAP



Find specialized scanner for the web

WPScan:

WPScan is a free, for non-commercial use, black box WordPress vulnerability scanner written for security professionals and blog maintainers to test the security of their sites. It checks for known vulnerabilities in WordPress itself, its themes, and plugins. WPScan also checks for weak passwords, user enumeration, and other common security issues.

Wordfence Scan:

Wordfence includes an endpoint firewall and malware scanner that were built from the ground up to protect WordPress. The Threat Defense Feed arms Wordfence with the newest firewall rules, malware signatures and malicious IP addresses it needs to keep your website safe.

Sucuri SiteCheck:

Sucuri SiteCheck is another popular tool. It scans for known malware, blacklisting status, website errors, and out-of-date software. While it's not specifically only for WordPress, it does a good job of detecting issues with WordPress sites.

NinjaScanner:

A lightweight, fast and powerful Antimalware scanner for WordPress which includes many features to help you scan your blog for malware and virus.

