demo.testfire.net

*Ping Scan : Check target is live or not

```
┌──(root㉿kali)-[~]
└─# nmap -sn demo.testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 21:03 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.042s latency).
Other addresses for demo.testfire.net (not scanned): 64:ff9b::413d:8975
Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds
```

*Basic Scan : Lists open ports and basic service information.

```
┌──(root㉿kali)-[~]
└─# nmap demo.testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 13:02 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.10s latency).
Other addresses for demo.testfire.net (not scanned): 64:ff9b::413d:8975
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8080/tcp open   http-proxy
8443/tcp closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 33.02 seconds
```

*Service Version Detection : Detects the versions of running services.

```
┌──(root㉿kali)-[~]
└─# nmap -sV demo.testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 13:07 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.086s latency).
Other addresses for demo.testfire.net (not scanned): 64:ff9b::413d:8975
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE   VERSION
80/tcp   open   http      Apache Tomcat/Coyote JSP engine 1.1
443/tcp  open   ssl/http  Apache Tomcat/Coyote JSP engine 1.1
8080/tcp open   http      Apache Tomcat/Coyote JSP engine 1.1
8443/tcp closed https-alt

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.69 seconds
```

*Operating System Detection : Tries to identify the target's OS using TCP/IP fingerprinting

```
┌──(root㉿kali)-[~]
└─# nmap -O demo.testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 13:09 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.27s latency).
Other addresses for demo.testfire.net (not scanned): 64:ff9b::413d:8975
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8080/tcp open   http-proxy
8443/tcp closed https-alt
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.76 seconds
```

*Scan All Ports : Scans all 65,535 ports to detect any open ones not in the default 1–1000 range.

```
┌──(root㉿kali)-[~]
└─# nmap -p- demo.testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 13:10 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.045s latency).
Other addresses for demo.testfire.net (not scanned): 64:ff9b::413d:8975
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8080/tcp open   http-proxy
8443/tcp closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 430.27 seconds
```

*Version scan : Print version

```
┌──(root㉿kali)-[~]
└─# nmap -V demo.testfire.net
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.4.1 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

* TCP SYN scan – Sends SYN, waits for SYN-ACK

```
┌──(root㉿kali)-[~]
└─# nmap -sS demo.testfire.net

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 21:08 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.10s latency).
Other addresses for demo.testfire.net (not scanned): 64:ff9b::413d:8975
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8080/tcp open   http-proxy
8443/tcp closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 20.86 seconds
```

* TCP Connect scan for a specified port number

```
┌──(root㉿kali)-[~]
└─# nmap -sT demo.testfire.net -p21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 21:33 EDT
Nmap scan report for demo.testfire.net (65.61.137.117)
Host is up (0.19s latency).
Other addresses for demo.testfire.net (not scanned): 64:ff9b::413d:8975

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```