STEP TWO – **PORT & SERVICE USING NMAP**

Goal: To do stage scans. From quick to deeper.

1. Command Used: **nmap -sS testfire.net**

Result:-

Ports available:

PORT   STATE SERVICE
80/tcp   open http
443/tcp open https
8080/tcp open http-proxy

////////////////////////////

2. Command Used: **nmap -sV -p 22,80,443 -sC testfire.net**

Result:

PORT   STATE   SERVICE   VERSION
22/tcp filtered ssh
80/tcp open   http   Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
443/tcp open   ssl/http Apache Tomcat/Coyote JSP engine 1.1
| ssl-cert: Subject: commonName=demo.testfire.net
| Subject Alternative Name: DNS:demo.testfire.net
| Not valid before: 2025-05-21T00:00:00
|_Not valid after: 2026-06-21T23:59:59
|_http-title: Altoro Mutual
|_ssl-date: 2025-09-12T11:01:14+00:00; -1s from scanner time.

Host script results:
|_clock-skew: -1s

/////////////////////////////////

3. Command Used: **nmap -sV -p 1-65535 -sC testfire.net**

Result:

PORT   STATE SERVICE   VERSION
80/tcp   open tcpwrapped
443/tcp open tcpwrapped
| ssl-cert: Subject: commonName=demo.testfire.net
| Subject Alternative Name: DNS:demo.testfire.net

| Not valid before: 2025-05-21T00:00:00
|_Not valid after: 2026-06-21T23:59:59
8080/tcp open tcpwrapped

/////////////////////////

4. Command Used: **nmap -sV -p- testfire.net**

Result:

PORT   STATE SERVICE   VERSION
80/tcp   open tcpwrapped
443/tcp open tcpwrapped
8080/tcp open tcpwrapped

/////////////////////////

5. Command Used: **nmap -O --osscan-guess testfire.net**

Result:

ORT   STATE SERVICE
80/tcp   open http
443/tcp open https
8080/tcp open http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc|printer
Running (JUST GUESSING): Netgear embedded (87%), Brother embedded (85%)
OS CPE: cpe:/h:brother:mfc-7820n
Aggressive OS guesses: Netgear SC101 Storage Central NAS device (87%), Brother MFC-7820N printer (85%)
No exact OS matches for host (test conditions non-ideal).

/////////////////////////