ACTIVE RECON REPORT – Assignment 4

Target: testfire.net

IP: 65.61.137.117

---

1. Host Discovery

Command Used

nmap -sn testfire.net

Result

- Host is **alive**

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:05 EST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.29s latency).
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```

Ping Confirmation

ping testfire.net

From the ping output, the IP was identified as **65.61.137.117**

```
┌──(kali㉿kali)-[~]
└─$ ping testfire.net
PING testfire.net (65.61.137.117) 56(84) bytes of data.
64 bytes from 65.61.137.117: icmp_seq=1 ttl=111 time=566 ms
64 bytes from 65.61.137.117: icmp_seq=2 ttl=111 time=325 ms
64 bytes from 65.61.137.117: icmp_seq=3 ttl=111 time=273 ms
64 bytes from 65.61.137.117: icmp_seq=4 ttl=111 time=374 ms
^C
── testfire.net ping statistics ──
5 packets transmitted, 4 received, 20% packet loss, time 4008ms
rtt min/avg/max/mdev = 272.532/384.465/566.095/110.814 ms
```

---

2. Port & Service Scan (Nmap)

2.1 TCP SYN Scan

nmap -sS testfire.net

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:05 EST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.10% done; ETC: 09:06 (0:01:03 remaining)
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.28s latency).
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 31.11 seconds
```

2.2 Service & Version Detection (Common Ports)

nmap -sV -p 22,80,443 -sC testfire.net

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -p 80,443,8080,8443 testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:09 EST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.65s latency).

PORT     STATE  SERVICE   VERSION
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
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
| 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
|_ssl-date: 2025-11-27T14:09:40+00:00; +2s from scanner time.
8080/tcp open   http      Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
8443/tcp closed https-alt

Host script results:
|_clock-skew: 1s

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.03 seconds
```

2.3 Full Port Scan

nmap -sV -p- -sC testfire.net

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:10 EST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.0050s latency).
Not shown: 63407 filtered tcp ports (no-response), 2125 filtered tcp ports (host-unreach)
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
8080/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.84 seconds
```

2.4 Full Range Port Scan (1–65535) + NSE Scripts

nmap -sV -p 1-65535 -sC testfire.net

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 1-65535 -sC testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:09 EST
Nmap scan report for testfire.net (65.61.137.117)
Host is up (0.042s latency).
Not shown: 63430 filtered tcp ports (no-response), 2102 filtered tcp ports (host-unreach)
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
|_http-title: Altoro Mutual
443/tcp  open  tcpwrapped
8080/tcp open  tcpwrapped
|_http-title: Altoro Mutual

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 125.55 seconds
```

2.5 OS Detection

nmap -O --osscan-guess 65.61.137.117

```
┌──(kali㉿kali)-[~]
└─$ nmap -O --osscan-guess testfire.net
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:11 EST
Failed to resolve "testfire.net".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 12.25 seconds
```

Issue Noticed

- When running some scans with the domain name, Nmap showed: "Failed to resolve testfire.net". Switching to the IP address resolved the issue.

```
┌──(kali㉿kali)-[~]
└─$ nmap -O --osscan-guess 65.61.137.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:34 EST
Nmap scan report for 65.61.137.117
Host is up (0.27s latency).
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
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|3.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3
Aggressive OS guesses: Linux 4.4 (88%), Linux 3.2 - 3.8 (87%), Linux 3.11 - 4.9 (
86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.12 seconds
```

Summary of Findings

- Host up
- Open ports discovered
- Services detected
- NSE script outputs gathered
- OS fingerprint guessed

---

3. HTTP Enumeration (DIRB)

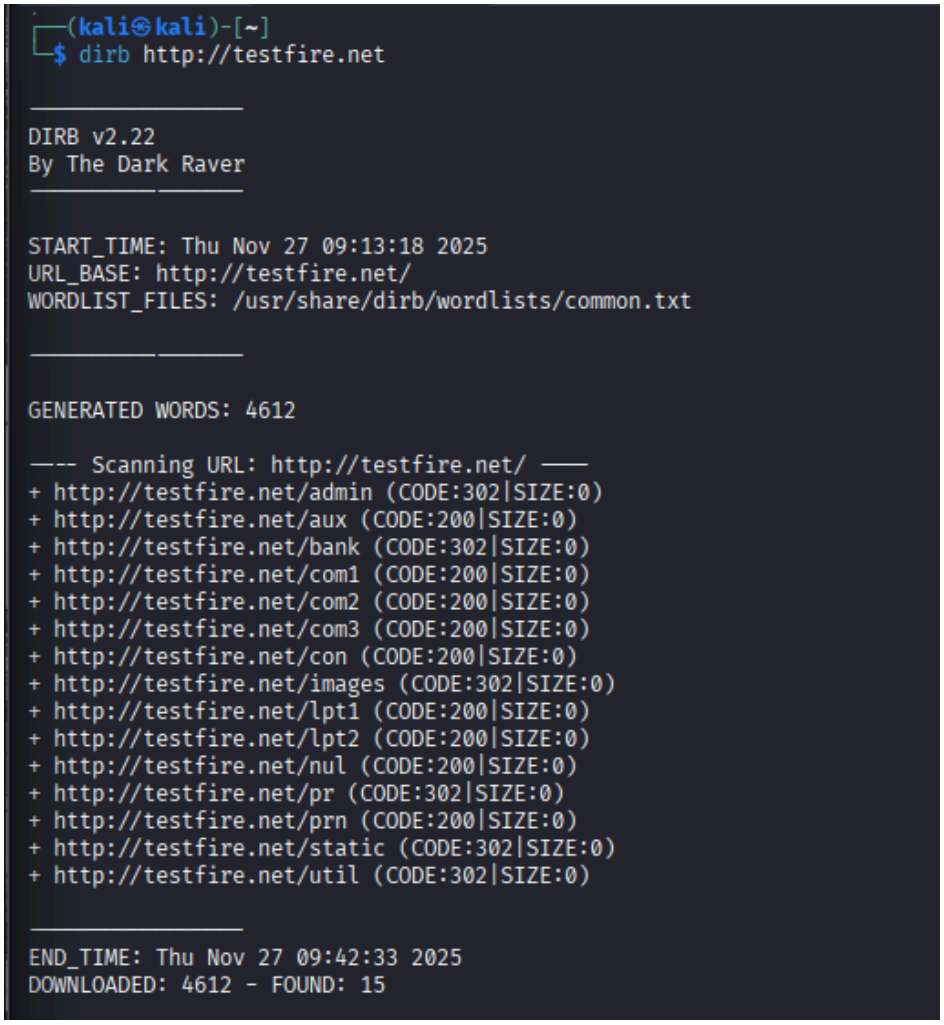
Command

dirb http://testfire.net

Discovered Paths

Directory	Status
/admin	302
/aux	200
/bank	302
/com1	200
/com2	200
/com3	200
/con	200
/images	302
/lpt1	200
/lpt2	200
/nul	200
/pr	302
/prn	200
/static	302
/util	302

Total: 15 findings



---

4. Web Fingerprinting (WhatWeb)

Command

whatweb http://testfire.net

Findings

- Detected technologies
- Server information
- Frameworks / cookies / headers

```
┌──(kali㉿kali)-[~]
└─$ whatweb http://testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Country[UNITED STATES][
US], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], IP[65.61.137.117], Java
, Title[Altoro Mutual]
```

---

5. Web Vulnerability Scan (Nikto)

Command

nikto -h http://testfire.net -o nikto.txt

Findings

- Outdated server components
- Directory/file disclosure Possible misconfigurations
- Insecure headers

```
┌──(kali㉿kali)-[~]
└─$ cat nikto.txt
- Nikto v2.5.0/
+ Target Host: testfire.net
+ Target Port: 80
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing
-content-type-header/:
+ OPTIONS OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ GET HTTP method ('Allow' Header): 'PUT' method could allow clients to save file
s on the web server.
+ GET HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on
 the web server.
+ EJIUHTLA /: Web Server returns a valid response with junk HTTP methods which ma
y cause false positives.
```

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://testfire.net -o nikto.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2025-11-27 09:15:12 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://de
veloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agen
t to render the content of the site in a different fashion to the MIME type. See:
 https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-con
tent-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on
 the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the
 web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause f
alse positives.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 1 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-11-27 09:30:18 (GMT-5) (906 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

---

6. Final Summary

Detail	Result
Target	testfire.net
IP	65.61.137.117
Host Status	UP
Open Ports	80, 443, 8080
OS Guess	Linux Kernel 3.x / 4.x
Confidence	87–88%

- Host discovery was successful

- Domain name failed only during some scans, switching to IP resolved the error.
- Staged Nmap scans completed
- 15 useful directories discovered with DIRB
- Web technologies fingerprinted via WhatWeb
- Basic vulnerability indicators collected using Nikto
