

# Penetration Test Report on Target-IP

## 10.10.77.53

### 1. Executive Summary

This penetration test was conducted to identify vulnerabilities in the target system (10.10.77.53) with permission. Testing focused on open HTTP services on ports 80 and 3000.

### 2. Methodology

#### Basic ping & traceroute

ping -c 4 10.10.77.53

traceroute 10.10.77.53

Screenshot Placeholder: Basic ping & traceroute

```
root@kali:~# ping -c 4 10.10.77.53
PING 10.10.77.53 (10.10.77.53) 56(84) bytes of data.
64 bytes from 10.10.77.53: icmp_seq=1 ttl=64 time=0.341 ms
64 bytes from 10.10.77.53: icmp_seq=2 ttl=64 time=0.322 ms
64 bytes from 10.10.77.53: icmp_seq=3 ttl=64 time=0.335 ms
64 bytes from 10.10.77.53: icmp_seq=4 ttl=64 time=0.333 ms
64 bytes from 10.10.77.53: icmp_seq=5 ttl=64 time=0.334 ms
64 bytes from 10.10.77.53: icmp_seq=6 ttl=64 time=0.331 ms
64 bytes from 10.10.77.53: icmp_seq=7 ttl=64 time=0.367 ms
64 bytes from 10.10.77.53: icmp_seq=8 ttl=64 time=0.331 ms
64 bytes from 10.10.77.53: icmp_seq=9 ttl=64 time=0.359 ms
...
... 10.10.77.53 ping statistics ...
9 packets transmitted, 9 packets received, 0% packet loss, time 8179ms
rtt min/avg/max/mdev = 0.322(0.379) / 0.561(0.062) ms
root@kali:~# traceroute 10.10.77.53
traceroute to 10.10.77.53 (10.10.77.53), 30 hops max, 60 byte packets
 1  10.10.77.53 (10.10.77.53)  0.377 ms  0.321 ms  0.332 ms
root@kali:~#
```

#### Nmap service discovery

nmap -sS -sV -O 10.10.77.53

Screenshot Placeholder: Nmap service discovery

```
root@kali:~# nmap -sS -sV -O 10.10.77.53
Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-24 07:45 AST
Nmap scan type: Service detection
Nmap probe: Scriptable
Nmap threads: 10 threads
Nmap timing: 0.50s per host, 0.50s per port
Nmap scan timeout: 20.00s
Nmap scan mode: Service detection
Nmap service detection performed. Please report any incorrect results at https://nmap.org/submit/bug.html
Nmap done at 2019-09-24 07:46 (local)
```

```
root@kali:~# nmap -sS -sV -O 10.10.77.53
Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-24 07:47 AST
Nmap scan type: Service detection
Nmap probe: Scriptable
Nmap threads: 10 threads
Nmap timing: 0.50s per host, 0.50s per port
Nmap scan timeout: 20.00s
Nmap scan mode: Service detection
Nmap service detection performed. Please report any incorrect results at https://nmap.org/submit/bug.html
Nmap done at 2019-09-24 07:48 (local)
```

## Nmap HTTP enumeration

```
nmap -p 80,3000 --script=http-title,http-headers,http-enum -sV -oA  
20250924_10.10.77.53_nmap_http 10.10.77.53
```

The image shows two terminal windows side-by-side. The left window is for port 80 and the right is for port 3000. Both use the 'root@IP-10-10-44-246:' prompt. The Nmap command is identical for both: `nmap -p 80,3000 --script=http-title,http-headers,http-enum -sV -oA 20250924_10.10.77.53_nmap_http 10.10.77.53`. The output for port 80 includes results for the robots.txt file and the Apache version. The output for port 3000 includes results for the robots.txt file and the Apache version.

## Curl to grab headers and default page

```
curl -I http://10.10.77.53:80  
curl -I http://10.10.77.53:3000
```

Screenshot Placeholder: Curl to grab headers and default page

The image shows four terminal windows. The first two are for port 80 and the last two are for port 3000. Each window shows a curl command being run against the respective port. The output shows the received headers and the default web pages for each port.

## Safe web scanner & headers check

```
nikto -host http://10.10.77.53:80 -output 20250924_nikto_80.txt  
nikto -host http://10.10.77.53:3000 -output 20250924_nikto_3000.txt  
curl -v http://10.10.77.53:80/ 2>&1 | tee 20250924_10.10.77.53_http80_raw.txt
```

Screenshot Placeholder: Safe web scanner & headers check

The image shows three terminal windows. The first window shows a nikto scan for port 80, the second shows a nikto scan for port 3000, and the third shows the raw curl output for port 80. The nikto scans identify various vulnerabilities and exposures, while the curl output shows the raw HTTP traffic exchanged between the scanner and the target server.

## Enumeration (web-oriented)

```
gobuster dir -u http://10.10.77.53:80 -w /usr/share/wordlists/dirb/common.txt -t 50 -o  
20250924_gobuster_80.txt
```

## Screenshot Placeholder: Enumeration (web-oriented)

## Vulnerability scanning (non-exploitative)

```
nmap -sS -sV --script=vuln -p 80,3000 -oA 20250924_nmap_vuln 10.10.77.53
```

Screenshot Placeholder: Vulnerability scanning (non-exploitative)

### 3. Recommendations

1. Patch Apache and OS updates
  2. Restrict access to sensitive directories
  3. Implement security headers and cookie flags
  4. Disable directory indexing
  5. Monitor logs for suspicious activity

## 4. Conclusion

The penetration test identified high-severity vulnerabilities, misconfigured directories, and security header issues. Immediate remediation is recommended.