Penetration Test Report on Taregt-IP 10.10.77.53

1. Executive Summary

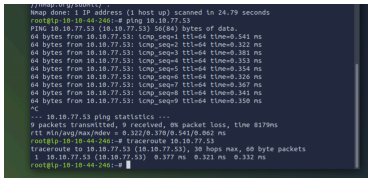
This penetration test was conducted to identify vulnerabilities in the target system (10.10.77.53) with permission. Testing focused on open HTTP services on ports 80 and 3000.

2. Methodology

Basic ping & traceroute

ping -c 4 10.10.77.53
traceroute 10.10.77.53

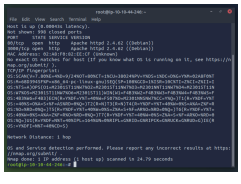
Screenshot Placeholder: Basic ping & traceroute

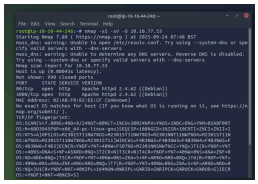


Nmap service discovery

nmap -sS -sV -O 10.10.77.53

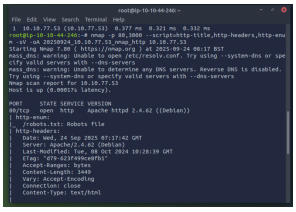
Screenshot Placeholder: Nmap service discovery

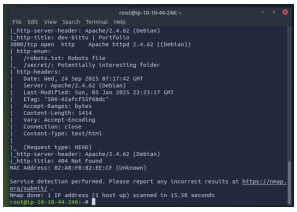




Nmap HTTP enumeration

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

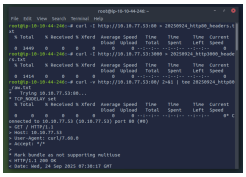


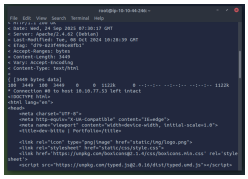


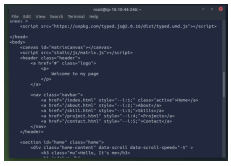
Curl to grab headers and default page

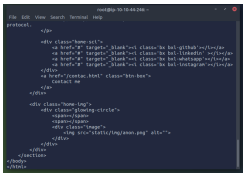
curl -I http://10.10.77.53:80
curl -I http://10.10.77.53:3000

Screenshot Placeholder: Curl to grab headers and default page





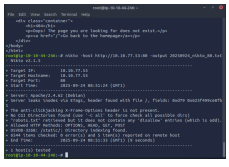


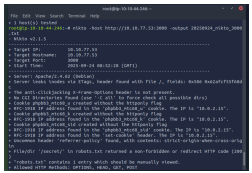


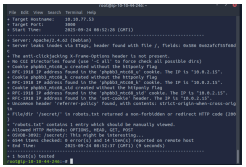
Safe web scanner & headers check

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



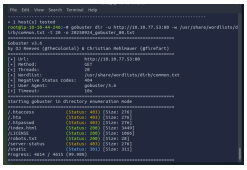


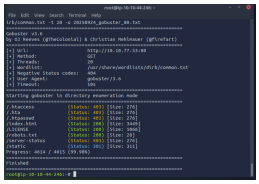


Enumeration (web-oriented)

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)

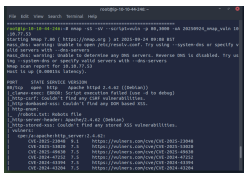


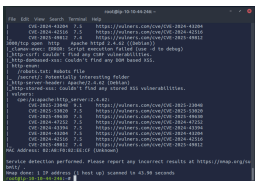


Vulnerability scanning (non-exploitative)

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.