OSINT & Recon Lab

Objective

Identify exposed assets belonging to the target organization using OSINT techniques.

Tools Used

Recon-ng, Shodan, Maltego, WHOIS Lookup

Commands Executed

recon-ng
workspaces create week3
add domains example.com
modules load recon/domains-hosts/bing_domain_web
run
show hosts

Findings

Subdomain	IP Address	Technology	Risk	Notes
www.example.com	93.184.216.34	Apache HTTP	Medium	Public web services
mail.example.com		SMTP	High	Exposed E-mail Server
dev.example.com		PHP	Critical	Might contain test apps

Shodan Query

apache port:80 country:US

IP	Ports	Service	Risk	Issue
(Shodan result)	80	Apache 2.4.6	Critical	Outdated version
(Shodan result)	22,80	SSH + HTTP	High	Direct SSH exposure

Summary

Using Recon-ng, multiple subdomains were discovered including development and mail servers running outdated software. Shodan revealed web servers exposing Apache versions vulnerable to multiple CVEs including directory traversal attacks. Exposed SSH services increase brute-force risk. Passive recon was completed without any direct intrusion. This intelligence helps attackers build a precise exploitation plan targeting weak systems, outdated services, and insecure configurations.