Entry-Level Reconnaissance Project

This project demonstrates foundational skills in *cybersecurity reconnaissance* using publicly available tools. It focuses on passive information gathering (OSINT) to simulate real-world ethical hacking practices without active intrusion.

🛠️ Tools Used

- theHarvester – Email, subdomain, and host harvesting
- WHOIS – Domain registration and ownership details
- nslookup – DNS resolution and record queries
- Shodan – Publicly exposed device and service scanner
- Google Dorking – Advanced search query techniques

Project Steps

1. Target Definition
- Simulated domain: exampletarget.com

a. Email and Subdomain Collection
bash
theHarvester -d exampletarget.com -b google

b. Domain registration and ownership details
bash
Whois exampletarget.com

c. DNS resolution and record queries
bash
nslookup -type=any exampletarget.com

d. Shodan Recon
bash
shodan host <target_ip>

e. Google Dorking advanced search query techniques
text
exampletarget.com

Objectives

- Gather basic target intelligence from public sources

- Identify potential emails, IPs, domains, and technologies used
- Lay the groundwork for more advanced phases (e.g., vulnerability scanning)

Findings

- Emails: admin@exampletarget.com, support@exampletarget.com
- Subdomains: mail.exampletarget.com, blog.exampletarget.com
- Open services: Port 80 (HTTP), 443 (HTTPS), 21 (FTP)
- WHOIS: Registrar data exposed including location
- Public documents: 3 PDF files indexed on Google

———

Lessons Learned

- How to collect and organize OSINT from multiple sources
- How to use recon tools without triggering alerts on target systems
- Importance of reconnaissance before any active engagement
- Better understanding of passive vs active recon