Cybersecurity Footprinting and Scanning Lab

Performed using Kali Linux CLI Tools

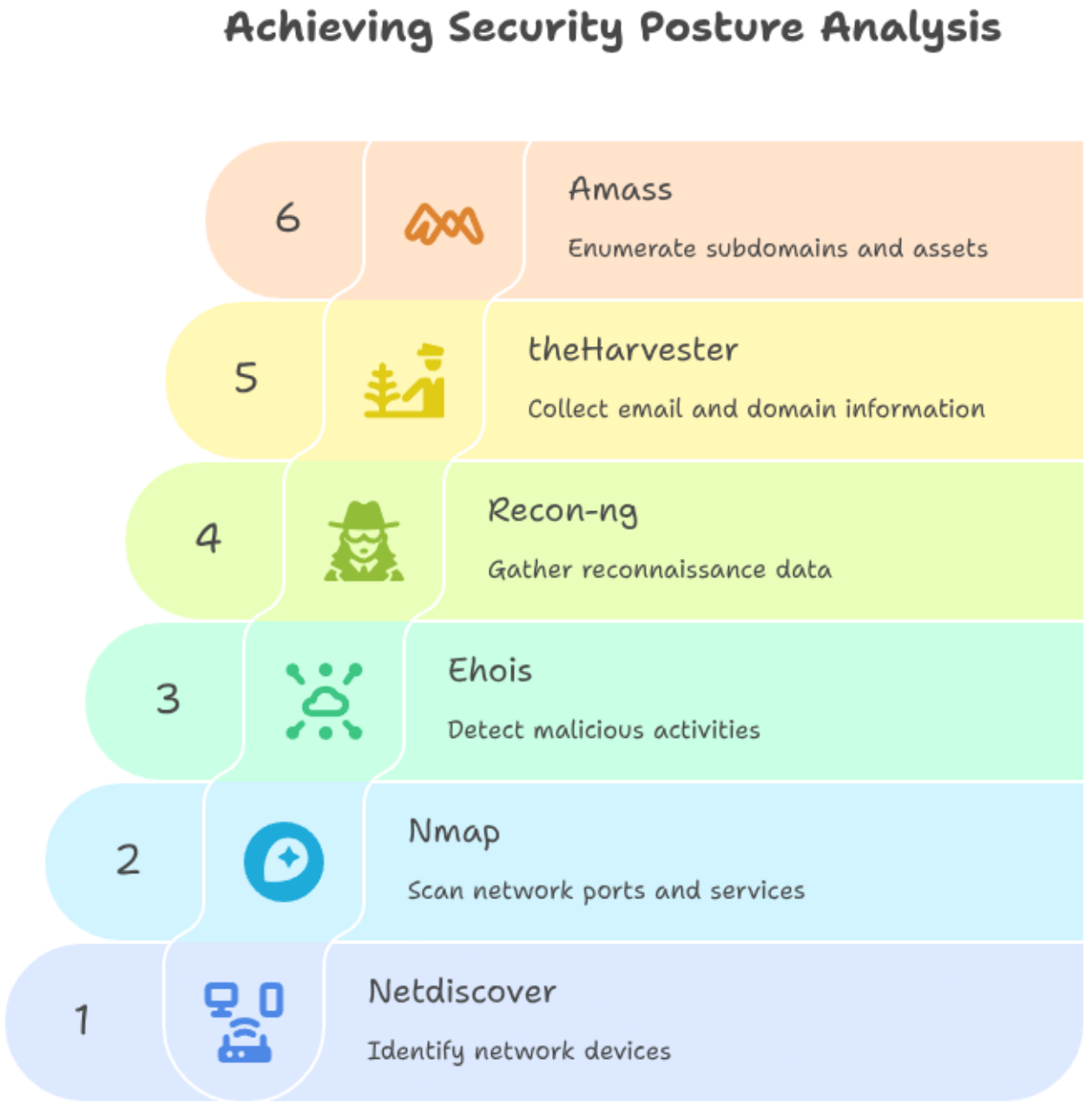
Made By: Raghunandan Sharma
Roll Number: 2023A7R020
Branch: CSE - Cybersecurity

Objective and Tools

Goal: Analyze security posture via CLI tools

Tools used:

- Netdiscover
- Nmap
- Ehois
- Recon-ng
- theHarvester
- Amass



Host Discovery using NetDiscover

Command: sudo netdiscover -r 192.168.1.0/24

Replace 192.168.1.0 with your network configuration

Usage of Command:

- Discovers live devices on a local subnet
- Helps identify internal assets

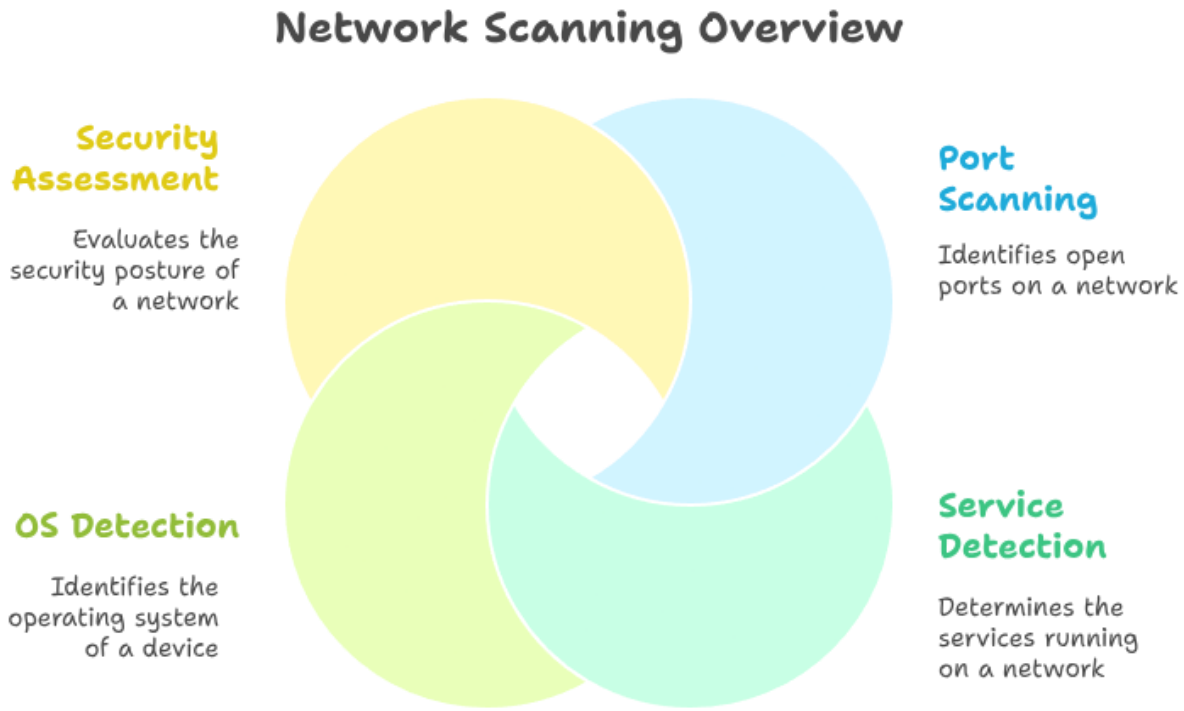
Port and Service Scanning

Commands: nmap -sS -sV –O 192.168.1.0

nmap –A 192.168.1.10

Usage of Commands:

- Scans ports, detects services and OS
- Helps assess exposed services



Domain info and OSINT

Whois command: whois example.com

Recon-ng steps:

recon-ng

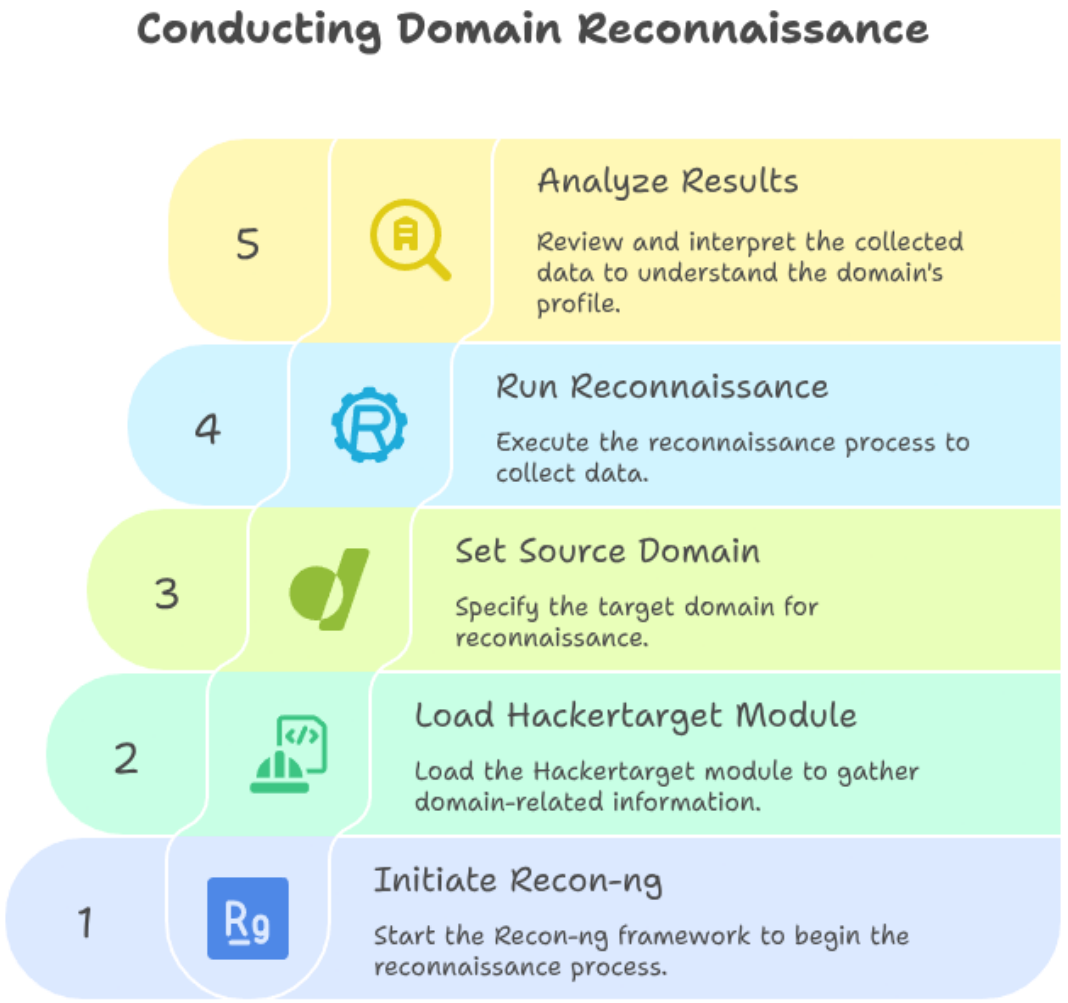
modules load recon/domains-hosts/hackertarget

options set SOURCE example.com

run

Usage of Commands:

- **Whois:** reveals domain ownership
- **Recon-ng:** modular framework for recon



Subdomain and Email Discovery

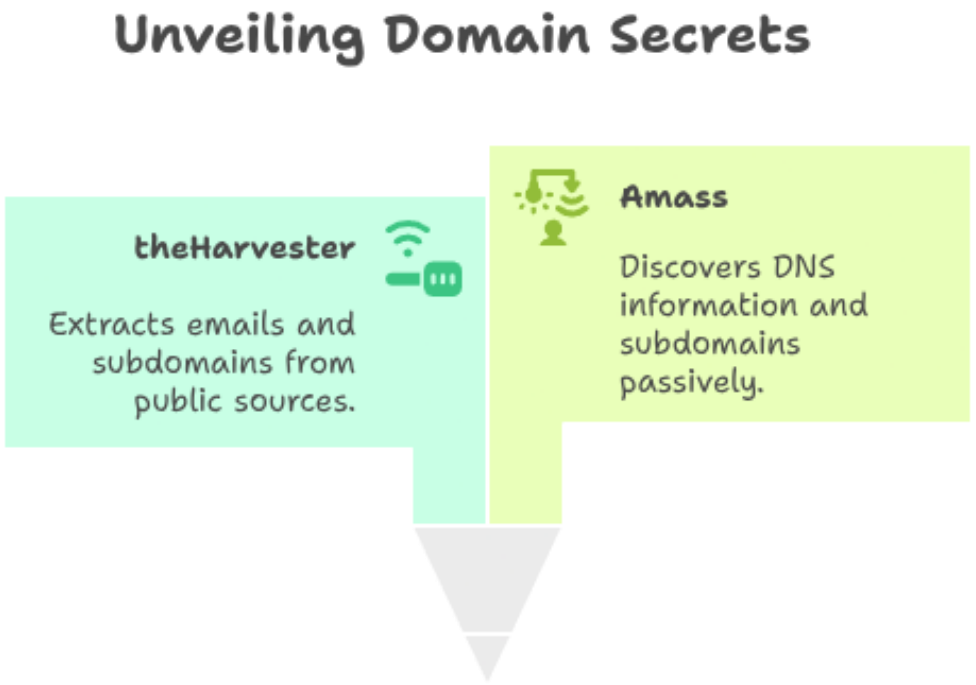
Commands:

theHarvester -d example.com -b google

amass enum -passive -d example.com

Usage of Commands:

- **theHarvester:** finds emails, subdomains from public sources
- **Amass:** discovers DNS info and subdomains



Open Ports and Mitigation

IP	Port	Service	Risk	Mitigation
192.168.1.10	22	SSH	Brute-Force	Key auth, Fail2bin
192.168.1.10	80	Apache	RCE vuln	Patch/Update Apache

Conclusion and Learning Outcomes

- Used only free CLI tools in Kali Linux.
- Discovered hosts, services, and domain info.
- Learned how attackers gather OSINT.
- Gained experience in scanning and mitigation techniques
- Hands-on commands and output:

https://drive.google.com/file/d/14Y7WCaP-qXBewhSMoy4_FpIt4W5VIXsm/view?usp=sharing