Recon-ng Basics and Information Gathering Tools

Recon-ng Basics Seekhne ke Liye Steps

1. Install Recon-ng

- Recon-ng Python-based framework hai. Tum ise apne system par install kar sakte ho:

  git clone https://github.com/lanmaster53/recon-ng.git

  cd recon-ng

  pip install -r REQUIREMENTS

- Kali Linux ke saath ye pre-installed bhi aata hai.

2. Recon-ng Commands Aur Modules

Recon-ng me modules hote hain jo specific tasks ke liye hote hain. Tumhe ye commands aur modules use karne seekhne honge:

- workspace: Information gathering ke liye alag-alag workspaces create karne ke liye.

  workspace create <name>

- Marketplace: Naye modules install karne ke liye.

  marketplace install <module>

- API Configuration: Recon-ng kaafi API-driven hai, jaise:

  - Shodan

  - VirusTotal

  - Censys

  API keys ko set karne ka command:

  keys add <service> <api_key>

- Module Execution:

  use <module>

  run

3. Commonly Used Recon-ng Modules

- recon/domains-hosts/brute_hosts: Domain ki host information gather karna.

- recon/hosts-hosts/resolve: Hosts ki IP address ko resolve karna.

- recon/profiles-profiles/profiler: Social media profiles ka analysis.

4. Practical Labs

- Recon-ng practice ke liye public domains ka use karo (apne domain ya legal permission ke bina testing illegal hai).

- Example:

  - example.com ka subdomain enumeration karo.

  - Email addresses aur contacts gather karo.

Information Gathering ke Tools

1. Web Reconnaissance Tools

- Nmap: Network scanning aur open ports find karne ke liye.

- Nikto: Web servers me vulnerabilities scan karne ke liye.

- WhatWeb: Website ka backend technology analyze karne ke liye.

2. OSINT (Open-Source Intelligence) Tools

- Maltego: Graph-based OSINT tool, relationships analyze karne ke liye.

- theHarvester: Emails, subdomains, IPs gather karne ke liye.

- Shodan: Publicly available IoT aur devices search karne ke liye.

- Google Dorking: Google search tricks se sensitive data find karna.

3. DNS and Network Tools

- DNSRecon: DNS information gather karne ke liye.

- Fierce: Subdomains aur DNS vulnerabilities ke liye.

- Traceroute: Packet path analysis ke liye.

4. Email and Social Media Gathering

- Social-Engineer Toolkit (SET): Email phishing aur social engineering tools.

- Spiderfoot: Automated reconnaissance tool.

5. Wireless Reconnaissance Tools

- Aircrack-ng: Wi-Fi password cracking aur sniffing.

- Wireshark: Packet capture aur analysis ke liye.

Recommended Devices and Setups

1. Kali Linux OS: Pre-installed penetration testing tools ke saath aata hai.

2. Parrot Security OS: Lightweight alternative for ethical hacking.

3. Wi-Fi Pineapple: Wireless network reconnaissance ke liye.

4. Virtual Machines (VMs): Lab setup ke liye (VMware ya VirtualBox).

5. Raspberry Pi: Portable hacking device banane ke liye.

Resources jo Helpful Hain

1. Books:

- "The Hacker Playbook" series.

- "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman.

2. Online Courses:

- TryHackMe (Recon-related rooms).

- Hack The Box (Beginner to Advanced Labs).

- Udemy courses on Ethical Hacking and Recon-ng.

3. Practice Platforms:

- CTF platforms: OverTheWire, TryHackMe, Hack The Box.

- Bug Bounty Platforms: HackerOne, Bugcrowd.