Hacking & Cracking Information Gathering ke liye OSINT Basics

OSINT (Open-Source Intelligence) Basics Seekhne ke Liye Roadmap

OSINT kya hai?

OSINT ka matlab hai public domain (open sources) se information gather karna. Ye ethical hacking aur penetration testing me kaafi important hota hai. OSINT tools aur techniques ka use karke kisi bhi target (individual, company, ya system) ke baare me data gather kiya jata hai.

OSINT ke Liye Seekhne Wale Areas:

1. **Google Dorking:**
   - Google ke advanced search operators ka use karke sensitive data find karna.
   - Example:
     - `filetype:pdf site:example.com`
     - `intitle:index of`

2. **Social Media Intelligence:**
   - Social media platforms se information gather karna.
   - Tools:
     - **Sherlock**: Username enumeration ke liye.
     - **Maltego**: Graph-based relationship analysis.

3. **Domain Information Gathering:**
   - Target website aur domain ke baare me technical details find karna.

- Tools:
  - **Whois**: Domain registration details.
  - **DNSDumpster**: DNS aur subdomain enumeration.
  - **theHarvester**: Emails, subdomains, aur IP gather karne ke liye.

4. **Geolocation Analysis:**
   - Geo-tagged images aur locations track karna.
   - Tools:
     - **ExifTool**: Metadata extraction ke liye.
     - **Google Maps API**: Location analysis.

5. **Network Scanning:**
   - Open ports aur vulnerabilities find karna.
   - Tools:
     - **Nmap**: Network scanning ke liye.
     - **Shodan**: Publicly accessible devices aur systems.

6. **Email Analysis:**
   - Email headers aur spoofed emails ka analysis.
   - Tools:
     - **Emailrep.io**: Email reputation check.
     - **Spiderfoot**: Automated reconnaissance tool.

7. **Dark Web OSINT:**
   - TOR aur dark web ka analysis.
   - Tools:
     - **OnionScan**: Dark web vulnerabilities find karne ke liye.

Recommended Tools for OSINT:

1. **Maltego:** Social media, domain aur relationship analysis ke liye.

2. **theHarvester:** Email, subdomain aur IP address gather karne ke liye.

3. **Shodan:** IoT devices aur open systems search karne ke liye.

4. **Spiderfoot:** Automated OSINT framework.

5. **Google Dorking:** Manual OSINT process ke liye sabse powerful.

Practice Platforms:

1. TryHackMe: OSINT specific labs.

2. Hack The Box: OSINT challenges.

3. Intelligence X: Public data archives.

Books aur Resources:

1. "OSINT Techniques" by Michael Bazzell.

2. "The Art of Invisibility" by Kevin Mitnick.

3. OSINT ke liye GitHub repositories explore karo.

Kuch Practical Steps OSINT Seekhne ke Liye:

1. Public domain ka analysis karo.

2. Tools ka hands-on practice karo.

3. Legal aur ethical rules ka dhyan rakho.