1. theHarvester

- **Purpose**: `theHarvester` is an OSINT (Open Source Intelligence) tool used for gathering information about a domain from various public sources.
- **Usage**:
    - The command `theHarvester -d DOMAIN -l LIMIT -b SOURCE` is used to search for information related to a specific domain (`DOMAIN`) using a specified data source (`SOURCE`).
    - The `-l LIMIT` option limits the number of search results.
    - Common sources include search engines, PGP key servers, and social networks.
- **Ethical Considerations**:
    - Ensure that the domain you are investigating is one you have permission to research.
    - Only gather information that is publicly available and does not infringe on privacy laws.

2. Nmap

- **Purpose**: `Nmap` (Network Mapper) is a tool used for network discovery and security auditing.
- **Usage**:
    - The command `nmap -sn kali.org` performs a ping scan (`-sn`) to determine which hosts are up on the network without performing port scanning.
    - This is useful for network mapping to identify active hosts.
- **Ethical Considerations**:
    - Only scan networks or hosts for which you have explicit permission.
    - Avoid scanning networks that could disrupt services or violate terms of service agreements.

Documentation and Ethical Boundaries

- **Methodology**:
    - Clearly document the tools used, commands executed, and the rationale behind each step.
    - Include screenshots or logs of the commands and outputs.
- **Findings**:

    - Categorize the information gathered, such as IP addresses, open ports, and domain-related data.
    - Analyze the findings to understand the network structure and potential vulnerabilities.
- **Ethical Guidelines**:
    - Obtain proper authorization before conducting any reconnaissance activities.
    - Respect privacy and legal boundaries.
    - Use the gathered information responsibly and ethically, focusing on improving security rather than exploiting vulnerabilities.

Example of Ethical Reconnaissance Report

1. **Introduction**:
    - State the purpose of the reconnaissance.
    - Mention the tools used and the ethical guidelines followed.
2. **Methodology**:
    - Detail the steps taken, including the commands used for `theHarvester` and `Nmap`.
3. **Findings**:
    - Present the data gathered, such as domain information and network maps.
    - Include visual aids like diagrams or charts if applicable.
4. **Analysis**:
    - Interpret the findings to identify potential security issues.
    - Provide recommendations for improving security based on the findings.
5. **Conclusion**:
    - Summarize the key findings and their implications.
    - Reiterate the importance of ethical reconnaissance.