Experiment 02

Aim:

To use an OSINT (Open-Source Intelligence) tool such as **TheHarvester** to gather valuable information like email addresses, subdomains, hosts, employee names, open ports, and banners from public sources such as search engines and PGP key servers.

Theory:

1) What are OSINT Tools?

Open-Source Intelligence (OSINT) tools are specialized applications used to collect data from publicly accessible sources on the internet. These tools are widely used by cybersecurity professionals, researchers, investigators, and ethical hackers for:

- Reconnaissance in penetration testing
- Threat intelligence and analysis
- Investigative journalism
- Risk assessment
- Competitive intelligence

Popular OSINT Tools

1. **Maltego** – A graphical link analysis tool used to map relationships between people, domains, and metadata.
2. **TheHarvester** – Used for gathering emails, subdomains, hosts, and employee details.
3. **Shodan** – A search engine for internet-connected devices and associated vulnerabilities.
4. **Censys** – Provides information about exposed internet devices and services.
5. **FOCA** – Extracts metadata from files and documents.
6. **SpiderFoot** – Automates OSINT tasks including scanning social media, DNS records, and more.
7. **OSINT Framework** – A categorized directory of OSINT tools and resources.
8. **Ghidra** – A reverse engineering suite developed by the NSA.
9. **Snort** – An open-source intrusion detection and prevention system (IDS/IPS).
10. **Metasploit** – A framework for penetration testing and exploiting vulnerabilities.

2) What is TheHarvester?

TheHarvester is a Python-based OSINT tool used for gathering information in the early stages of a penetration test. It can extract data from public sources like search engines, PGP key servers, and even platforms like Shodan and LinkedIn.

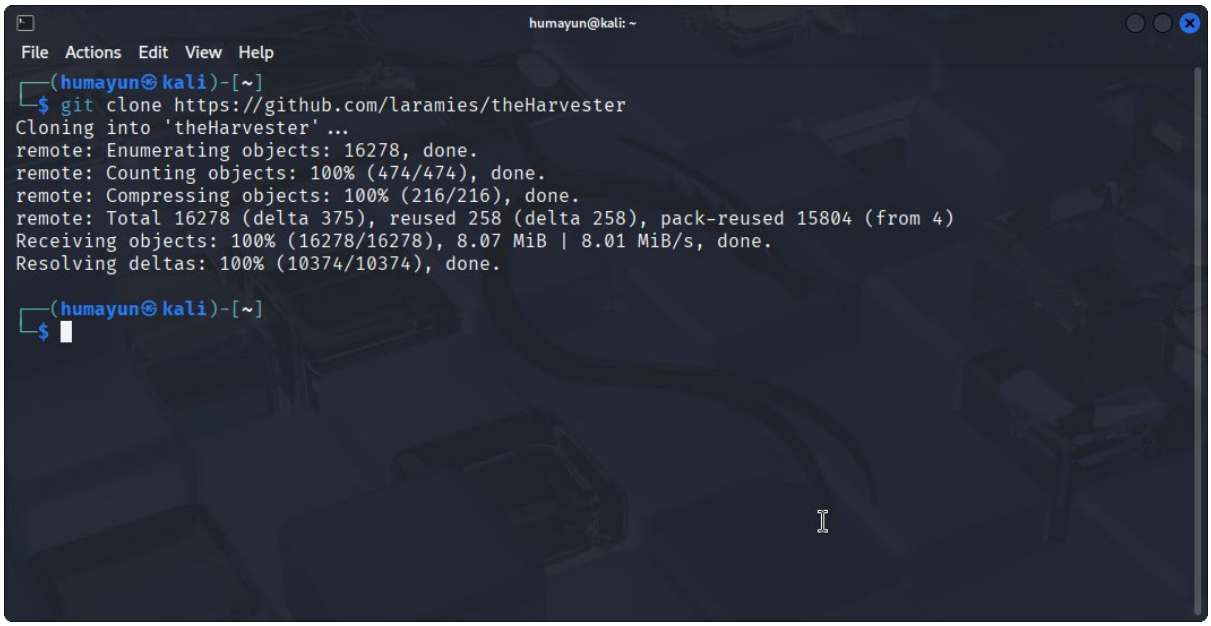
TheHarvester can collect:

- Email addresses
- Subdomains and domains
- Hostnames
- Open ports and service banners
- Names of employees

Installation in Kali Linux

Step 1: Clone the Repository

```
>> git clone https://github.com/laramies/theHarvester
```



Step 2: Install Python PIP (if not already installed)

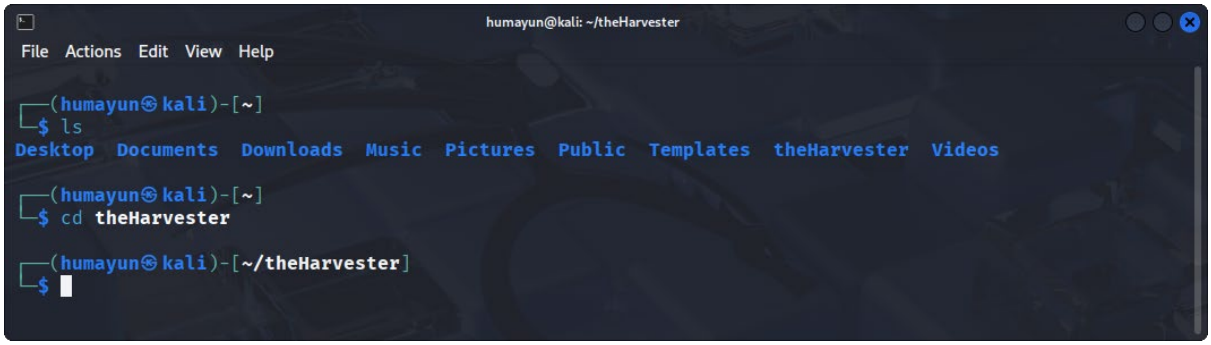
```
>> sudo apt install python3-pip
```

Step 3: Install Required Libraries

Navigate to the theHarvester directory:

```
>> cd theHarvester
```

```
>> python3 -m pip install -r requirements/dev.txt
```



Step 4: Verify Installation

```
>> python3 theHarvester.py -h
```

How to Use TheHarvester

Basic Syntax:

```
>> python3 theHarvester.py -d <domain> -l <limit> -b <source>
```

Common Options:

- -d : Target domain (e.g., microsoft.com)
- -l : Limit on number of results
- -b : Data source (e.g., google, bing, linkedin)
- -v : Enable DNS resolution for virtual hosts
- -n : Perform reverse DNS queries
- -c : Enable DNS brute force
- -f : Save results to a file (XML, JSON)
- -s : Use Shodan for device information

Example:

```
>> python3 theHarvester.py -d microsoft.com -l 500 -b google
```

Conclusion:

In this experiment, we successfully utilized TheHarvester, a powerful open-source intelligence gathering tool, to extract critical data such as emails, subdomains, hostnames, employee names, open ports, and service banners. This validated the importance of OSINT in cybersecurity assessments and highlighted how attackers and defenders alike can use publicly available data for reconnaissance and analysis.