

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
```



```
humayun@kali: ~  
File Actions Edit View Help  
(humayun@kali)~  
$ git clone https://github.com/laramies/theHarvester  
Cloning into 'theHarvester' ...  
remote: Enumerating objects: 16278, done.  
remote: Counting objects: 100% (474/474), done.  
remote: Compressing objects: 100% (216/216), done.  
remote: Total 16278 (delta 375), reused 258 (delta 258), pack-reused 15804 (from 4)  
Receiving objects: 100% (16278/16278), 8.07 MiB | 8.01 MiB/s, done.  
Resolving deltas: 100% (10374/10374), done.  
(humayun@kali)~  
$
```


A screenshot of a terminal window titled 'humayun@kali: ~/theHarvester'. The window displays a list of 35 Microsoft subdomains. The background of the terminal has a dark blue theme with a faint, stylized image of a city skyline. The subdomains listed are: account.microsoft.com, admin.microsoft.com, answers.microsoft.com, apps.microsoft.com, azure.microsoft.com, bingapp.microsoft.com, blogs.microsoft.com, careers.microsoft.com, cdn-dynmedia-1.microsoft.com, dotnet.microsoft.com, edge.payments.microsoft.com, fpt.microsoft.com, go.microsoft.com, holidays.microsoft.com, intune.microsoft.com, jobs.careers.microsoft.com, learn.microsoft.com, mathsolver.microsoft.com, mvp.microsoft.com, myaccount.microsoft.com, myapplications.microsoft.com, myapps.microsoft.com, myprofile.microsoft.com, mysignins.microsoft.com, news.microsoft.com, ov-df.microsoft.com, paymentinstruments-int.mp.microsoft.com, paymentinstruments.mp.microsoft.com, pmservices.cp.microsoft.com, research.microsoft.com, serviceshub.microsoft.com, support.microsoft.com, techcommunity.microsoft.com, visualstudio.microsoft.com, and vlscppe.microsoft.com.

```
humayun@kali: ~/theHarvester
File Actions Edit View Help
account.microsoft.com
admin.microsoft.com
answers.microsoft.com
apps.microsoft.com
azure.microsoft.com
bingapp.microsoft.com
blogs.microsoft.com
careers.microsoft.com
cdn-dynmedia-1.microsoft.com
dotnet.microsoft.com
edge.payments.microsoft.com
fpt.microsoft.com
go.microsoft.com
holidays.microsoft.com
intune.microsoft.com
jobs.careers.microsoft.com
learn.microsoft.com
mathsolver.microsoft.com
mvp.microsoft.com
myaccount.microsoft.com
myapplications.microsoft.com
myapps.microsoft.com
myprofile.microsoft.com
mysignins.microsoft.com
news.microsoft.com
ov-df.microsoft.com
paymentinstruments-int.mp.microsoft.com
paymentinstruments.mp.microsoft.com
pmservices.cp.microsoft.com
research.microsoft.com
serviceshub.microsoft.com
support.microsoft.com
techcommunity.microsoft.com
visualstudio.microsoft.com
vlscppe.microsoft.com
```

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.