

# TRAINING DAY 19 REPORT:

- **Introduction to theHarvester Tool**

**theHarvester** is a powerful **open-source reconnaissance tool** that is used during the **information gathering (footprinting) phase** of ethical hacking or penetration testing.

**Purpose:**

To gather information like:

- Emails
- Subdomains
- IP addresses
- Hostnames
- URLs
- Open ports (using Shodan)

**Sources Supported:**

1. Search engines: Google, Bing, Yahoo
2. Public databases: LinkedIn, VirusTotal
3. Shodan (for internet-connected devices)
4. DNS servers

**Installed by default in Kali Linux**

Or install using:

```
sudo apt install theharvester
```

- **Working of theHarvester Tool**

**Basic Syntax:**

```
theHarvester -d <domain_name> -b <source>
```

- d: The target domain (e.g., example.com)
- b: The source to search from (e.g., google, bing, shodan)

### **Example:**

```
theHarvester -d microsoft.com -b bing
```

### **Output:**

- List of email addresses
- Subdomains found on the web
- Associated IP addresses
- DNS data

### **Use Case:**

Before launching attacks, hackers or ethical testers gather all available passive information using tools like this.

## • **Working of theHarvester Tool Part-2**

### **Advanced Usage:**

You can combine options to increase efficiency and depth of information.

### **Saving output to file:**

```
theHarvester -d example.com -b bing -f report
```

Generates files like:

```
report.xml
```

```
report.html
```

### **Using multiple sources:**

```
theHarvester -d example.com -b google,bing,shodan
```

### **API Integration:**

You can link **Shodan** and **Hunter.io API keys** to get more data.

## **GUI Mode (optional):**

theHarvester also comes with a web interface in some versions.

- **Introduction to Shodan**

**Shodan** is often called the "**Google for Hackers.**"

Unlike Google (which indexes websites), Shodan indexes devices connected to the internet.

### **It Finds:**

- Webcams
- Routers
- Traffic lights
- Industrial control systems
- Printers, Smart TVs, etc.

### **Data Collected:**

- Open ports
- Banner information
- SSL certificates
- HTTP headers
- Device metadata

- **Shodan Part-1**

### **Website Interface:**

Search Bar example:

apache port:80 country:IN

### **Filters you can use:**

port: – e.g., port:22 for SSH

country: – e.g., country:IN

city: – e.g., city:Delhi

org: – e.g., org:BSNL

### **You Can Discover:**

- Misconfigured servers
- Vulnerable IoT devices
- IP addresses of running services

## • **Shodan – Webcam Part-2**

### **Focus on Webcam Search:**

Using Shodan to find insecure webcams across the globe.

### **Example Searches:**

```
webcamxp  
port:8080  
has_screenshot:true
```

### **Caution:**

1. Many webcams lack authentication
2. Ethical hackers use this to **raise awareness** and report misconfigured devices

**Note:** Never access private or unauthorized systems. This is illegal and unethical.

**By : Brahmjot Kaur**

**URN : 2302501**

**CRN : 2315045**