



## **Lab Focus – Module 02: Footprinting & Reconnaissance**

### **Lab Title: Passive Footprinting with FOCA, Shodan & Photon**

#### **Objective**

Perform deep passive reconnaissance using modern CEH v13 tools to collect information without interacting directly with the target's system. This lab simulates the information-gathering phase of an ethical hack.

#### **Tools Required**

- **FOCA** (Windows)
- **Shodan** (web interface)
- **Photon** (Python-based crawler)
- **ShellGPT**
- **Optional:** theHarvester, dnsrecon
- **Markdown** template or PDF report for documentation

### **Lab Step 1: Extract Metadata Using FOCA**

#### ◆ **Purpose:**

Reveal file metadata that may expose usernames, software versions, internal paths.

#### ◆ **Instructions:**

1. Download a PDF or DOCX from the target's website
2. Open FOCA > Load the document
3. Extract metadata from the file

#### ✓ **Output to Capture:**

- Screenshot of extracted metadata
- Note exposed usernames, document creators, software versions

## Lab Step 2: Identify Exposed Services Using Shodan

### ◆ Purpose:

Find internet-connected assets (e.g., servers, webcams, apps) tied to the organization.

### ◆ Instructions:

1. Go to <https://www.shodan.io>
2. Search using:
  - Domain name (e.g., "hostname:example.com")
  - Technology (e.g., "Apache", "IIS", "port:21")

### ✓ Output to Capture:

- Screenshot of Shodan results
- List exposed ports, services, software versions
- Highlight anything outdated or risky

## Lab Step 3: Crawl the Site Using Photon

### ◆ Purpose:

Discover hidden files, folders, endpoints, and internal links.

### ◆ Command:

```
photon -u https://example.com -o output/
```

### ◆ Output:

- Review `output/files`, `output/endpoints`, and `output/robots.txt`
- Note any login pages, forgotten directories, or admin panels

### ✓ Output to Capture:

- Screenshot of folder output
- List of interesting files or URLs found

## Lab Step 4: Use ShellGPT to Generate a Recon Report Template

### ◆ Prompt:

ShellGPT: Create a passive recon report template based on metadata, DNS, social media, and file discovery.

### ✓ Output to Capture:

- Screenshot of ShellGPT-generated structure
- Export or adapt into your own markdown/PDF report

## Lab Report Template

| Section      | What to Include                                     |
|--------------|-----------------------------------------------------|
| Target       | Domain or company investigated                      |
| Tools Used   | FOCA, Shodan, Photon, ShellGPT                      |
| Findings     | Metadata, exposed IPs/services, internal links      |
| Screenshots  | Minimum 3 (FOCA, Shodan, Photon)                    |
| Observations | What security risks or exposures were observed?     |
| Next Steps   | What will you scan or test next based on this info? |

### CEH Tip:

Passive recon doesn't touch the target's infrastructure , yet it can expose emails, paths, ports, usernames, and open doors.

### End of Lab

You've now completed a full passive recon using CEH v13 tools.