

Passive Reconnaissance - OSINT

ACCA7033

Dr. Ayman El Hajjar

2026/27

STOP and READ

Before you start your work in the lab you need to ensure the following steps when setting up your lab environment if you are using university labs devices:

1. Do not delete the 7Z files.
2. Delete all Virtual machines that already exist inside VirtualBox to ensure that you are starting your labs from a clean state.
3. For this lab we will be using several machines. You can download them by following the instructions available in the lab folder on Moodle.
4. Make sure you save the extracted files of the VMs in C:\VirtualMachines folder

Requirements and Notes

- **NOTE**- In this activity you need **only** your Kali Linux machine to be connected to the internet.
- In this lab, you need the following VM machines
 1. Kali Linux

For this section of the lab, you need to make sure that your kali Linux machine is connected to the Internet (NAT)

- This is not a HACKING TUTORIAL and YOU ARE RESPONSIBLE FOR YOUR ACTS OUTSIDE THIS LAB

Passive Reconnaissance: Open Source Intelligence (OSINT)

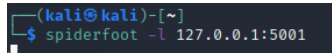


PLEASE READ BEFORE YOU START THIS SECTION

- Reconnaissance and information gathering both form an essential stage in every penetration test or auditing activity;
- The more information we have about our target, the more options we will have when it comes to finding vulnerabilities and/or exploiting them.
- For any other sections, if you need to be connected to the Internet, to install an application or for any other reasons, this will be made clear to you.
- OSINT can be carried out by conducting different activities on the internet to search for information. Tools are there to put all of those activities in one place and to automate them.
- There are many tools to use to conduct your OSINT. We will be using some, but feel free to explore others.
- You can see what type of sources can be used in OSINT investigation using the [OSINT Framework](#)
- Feel free to use [cwscenario.site](#) domain for all your OSINT investigations. This is a domain I own and only use for testing.

TheHarvester

- Since [TheHarvester](#) searches for information already are online, it means your search will go unnoticed and will not raise any alarm. This is passive reconnaissance



```
(kali㉿kali)-[~]
└─$ spiderfoot -l 127.0.0.1:5001
```

Figure 1: Starting spiderfoot on localhost port 5001

and you are not actually searching the web server of the company but public information about them that are available on the Internet.

- There are many options to use with theHarvester tool, if you type **theHarvester -h** on an open terminal, you will see a collection of different options you can use.
- We will focus on **-d** option to specify the domain, **-b** option to specify the data source (yahoo, linkedin, bing, twitter, etc..) . We also need to use **-l** option for certain sources as they block your request if the number of requests is not set. **Google was remove few years ago and it will give invalid sources if used.**
- Lets see an example below

theHarvester -d westminster.ac.uk -b yahoo -l 100

- you can also specify all sources

theHarvester -d cwscenario.site -b all

- It is useful to save the output of your OSINT so that you can use it to carry further attacks at a later stage. You can use the **-f** option to specify the filename to save the output to. I will save them in an html format so that I can open them in a browser.

theHarvester -d cwscenario.site -b all -f myresults.html

- Visit [TheHarvester](#) website and see how you can leverage OSINT tools and methods for your benefit.

SpiderFoot

- Another OSINT you should explore is Spiderfoot.
- SpiderFoot is preinstalled on Kali.
- To start you need to open a terminal and run it. You need to specify the server address and the port number to use for its application.

spiderfoot -l 127.0.0.1:5001

- While Spiderfoot is running on the terminal, open a new browser and point it to 127.0.0.1:5001 (you can specify any other port number you want. I suggest you use a number larger than 5000)

The screenshot shows the SpiderFoot web interface. At the top, there's a navigation bar with links like 'Kali Linux', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. Below this is a 'New Scan' form. The form has a 'Scan Name' field (annotated with a red circle and '3') and a 'Scan Target' field (annotated with a red circle and '4'). The 'Scan Target' field contains 'cwsenario.site'. To the right of the 'Scan Target' field, there's a list of supported target types: Domain Name, IPv4 Address, IPv6 Address, Hostname/Sub-domain, Subnet, Bitcoin Address, E-mail address, Phone Number, Human Name, Username, and Network ASN. Below the 'Scan Target' field, there are three radio buttons: 'All' (selected), 'Footprint', and 'Investigate'. The 'All' option is described as 'Get anything and everything about the target.' The 'Footprint' option is described as 'Understand what information this target exposes to the Internet.' The 'Investigate' option is described as 'Best for when you suspect the target to be malicious but need more information.' Below these, there's a 'Passive' radio button (annotated with a red circle and '5') described as 'When you don't want the target to even suspect they are being investigated.' At the bottom of the form is a 'Run Scan Now' button (annotated with a red circle and '6').

Figure 2: Creating new scan on my testing domain name. Feel free to use this domain for testing.

- Spiderfoot is module based, some of the modules requires the use of API keys. In some cases, these modules will not function without properly setting up the API keys first. In other modules, the API keys are only to speed up the scanning. Check this [website](#) for more information on the modules. Ignore the installation part.
- At the beginning, and since we are conducting an OSINT investigation, at least at this stage.
- Click on "New Scan"
- Choose "Passive scan" and give a name for the scan and for ip address you can choose either an IP address or a domain name to investigate.
- Give it some time until it finishes running. Results will come gradually until the scan finishes.
- Once it is done, explore the obtained results.

SIGIT - Simple Information Gathering Toolkit

- Let us now clone the SIGIT tool, another powerful information gathering tool.
- To clone it and install, we type:
 - `sudo git clone https://github.com/termuxhackers-id/SIGIT.git`

- **cd SIGIT**
 - * we navigate to folder
 - **chmod a+x install.sh**
 - * we make the Kali installer "install.sh" executable
 - **sudo ./install.sh**
 - * we execute the installer
- Let's run it now and see what information we can obtain. To run it open a terminal and type:
python3 sigit.py
 - SIGIT brings an interface with a number of options you can use.
 - Choose the one you need and put its number. For example **01** for usernames
 - Try for example your username (01), or the username you usually use for many services online and see if it can find it.
 - You can also try to find a specific email with specific names and many other information.

```

[ 3.1.0.17 ]
Simple Information Gathering Toolkit
Author by @Termuxhackers.id

Choose number or type exit for exiting

01 Userrecon      Username reconnaissance
02 Facedumper    Dump facebook information
03 Mailfinder     Find email with name
04 Godorker       Dorking with google search
05 Phoneinfo      Phone number information
06 DNSlookup      Domain name system lookup
07 Whoislookup    Identify who is on domain
08 Sublookup      Subnetwork lookup
09 Hostfinder     Find host domain
10 DNSfinder      Find host domain name system
11 RIPLookup      Reverse IP lookup
12 IPlocation     IP to location tracker

> choose: 

```

Figure 3: SIGIT - Simple Information Gathering Toolkit

Recon-ng

Recon-Ng

This tool will only work outside the university or if you are connected to EduRoam.

It is currently blocked if you are conducting the lab on a university machine.

- Recon-ng is an information-gathering tool that uses many different sources to gather data, for example, on Google, Twitter, and Shodan.
- Let's try to gather public information about our target.
- Let's start recon-ng by typing:

recon-ng

- You notice that recon-ng throws a warning that no modules are install.
- let us install the hackertarget first. Hackertarget is a module that search for subdomains on any given domains.

marketplace install hackertarget

- To search for hackertarget module. We type :

modules search hackertarget

- To use hackertarget module. We type :

modules load recon/domains-hosts/hackertarget

- Now we need to set the target to use for our investigation:

options set source cwsenario.site

- Let's run the module now:

run

- **Note:** my domain will not bring a lot of results, you can use any other website as these are public information and we are not touching the server.
- There are many other modules that you can explore, for example you can install all marketplace modules by typing:

marketplace install all

- to search the module use

marketplace search

- I really suggest you explore recon-ng in depth. It is not only used for passive reconnaissance but we can also use it for active reconnaissance and part of our information gathering phase.
- I also suggest that you try to run recon-web at the same time. Recon-web will run on port 5000 and will show a graphical interface of everything captured on recon-ng tool
- There are many sites that give examples of recon-ng usage:
 - Tutorial [recon-ng usage example](#)

- Tutorial [recon-ng](#)
- [Tutorial on Hackersploit](#)

Sock Puppet Accounts

- **Where to Collect Social Media Information:** To succeed in gathering social media intelligence (SOCMINT), start by identifying relevant information and objectives for your search. You should explore various platforms and public databases that aid comprehensive investigations ¹.

¹[Check this link for more on Social Media Intelligence from Maltego](#)