Active Reconnaissance (Information Gathering tools)

1. Spiderfoot (https://github.com/smicallef/spiderfoot)

SpiderFoot is an open-source intelligence (OSINT) automation tool. It integrates with just about every data source available and utilizes a range of methods for data analysis, making that data easy to navigate.

SpiderFoot has an embedded web-server for providing a clean and intuitive web-based interface but can also be used completely via the command-line. It's written in Python 3 and MIT-licensed.

spiderfoot

FEATURES

- Web based UI or CLI
- Over 200 modules (see below)
- Python 3.7+
- YAML-configurable correlation engine with 37 pre-defined rules
- CSV/JSON/GEXF export
- API key export/import
- SQLite back-end for custom querying
- Highly configurable
- Fully documented
- Visualisations
- TOR integration for dark web searching
- Dockerfile for Docker-based deployments
- Can call other tools like DNSTwist, Whatweb, Nmap and CMSeeK
- Actively developed since 2012!

USES

SpiderFoot can be used offensively (e.g., in a red team exercise or penetration test) for reconnaissance of your target or defensively to gather information about what you or your organization might have exposed over the Internet.

You can target the following entities in a SpiderFoot scan:

- IP address
- Domain/sub-domain name
- Hostname
- Network subnet (CIDR)
- ASN
- E-mail address
- Phone number
- Username
- Person's name
- Bitcoin address

SpiderFoot's 200+ modules feed each other in a publisher/subscriber model to ensure maximum data extraction to do things like:

- Host/sub-domain/TLD enumeration/extraction
- Email address, phone number and human name extraction
- Bitcoin and Ethereum address extraction
- Check for susceptibility to sub-domain hijacking
- DNS zone transfers
- Threat intelligence and Blacklist queries
- API integration with SHODAN, HaveIBeenPwned, GreyNoise, AlienVault, SecurityTrails, etc.
- Social media account enumeration
- S3/Azure/Digitalocean bucket enumeration/scraping
- IP geo-location
- Web scraping, web content analysis

- Image, document and binary file meta data analysis
- Dark web searches
- Port scanning and banner grabbing
- Data breach searches
- So much more...

INSTALLING & RUNNING

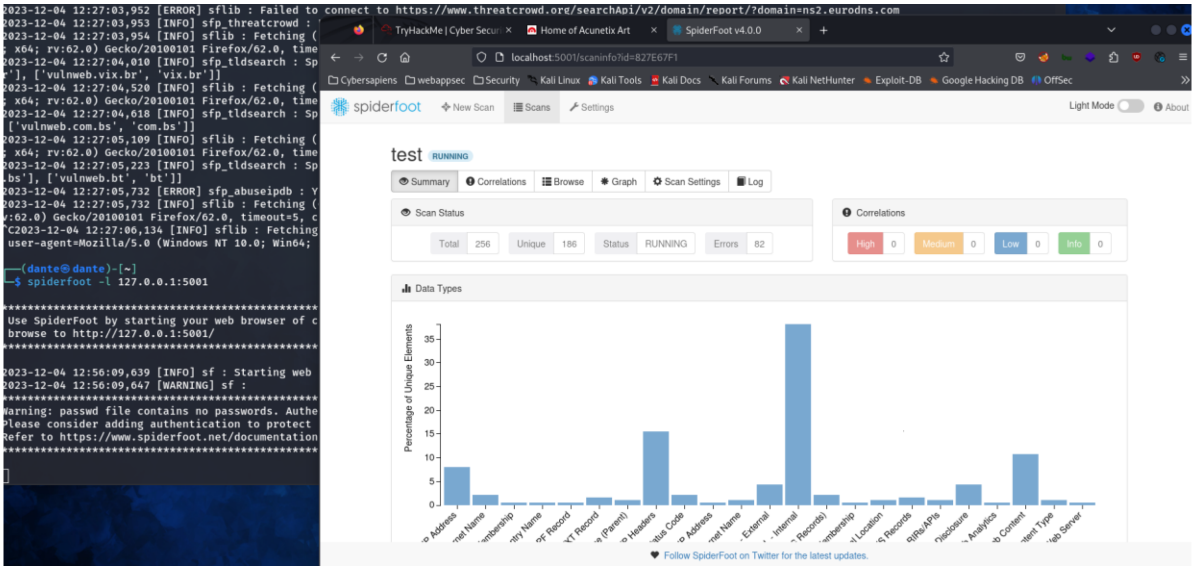
To install and run SpiderFoot, you need at least Python 3.7 and a number of Python libraries which you can install with pip. We recommend you install a packaged release since master will often have bleeding edge features and modules that aren't fully tested.

Stable build (packaged release):

- wget https://github.com/smicallef/spiderfoot/archive/v4.0.tar.gz
- tar zxvf v4.0.tar.gz
- cd spiderfoot-4.0
- pip3 install -r requirements.txt
- python3 ./sf.py -l 127.0.0.1:5001

Development build (cloning git master branch):

- git clone https://github.com/smicallef/spiderfoot.git
- cd spiderfoot
- pip3 install -r requirements.txt
- python3 ./sf.py -l 127.0.0.1:5001



```
2023-12-04 12:27:03,952 [ERROR] sflib : Failed to connect to https://www.threatcrowd.org/searchApi/v2/domain/report/?domain=ns2.eurodns.com
2023-12-04 12:27:03,953 [INFO] sfp_threatcrowd :
2023-12-04 12:27:03,954 [INFO] sflib : Fetching (
; x64; rv:62.0) Gecko/20100101 Firefox/62.0, time
2023-12-04 12:27:04,010 [INFO] sfp_tldsearch : Sp
r'], ['vulnweb.vix.br', 'vix.br']]
2023-12-04 12:27:04,520 [INFO] sflib : Fetching (
; x64; rv:62.0) Gecko/20100101 Firefox/62.0, time
2023-12-04 12:27:04,618 [INFO] sfp_tldsearch : Sp
 ['vulnweb.com.bs', 'com.bs']]
2023-12-04 12:27:05,109 [INFO] sflib : Fetching (
; x64; rv:62.0) Gecko/20100101 Firefox/62.0, time
2023-12-04 12:27:05,223 [INFO] sfp_tldsearch : Sp
.bs'], ['vulnweb.bt', 'bt']]
2023-12-04 12:27:05,732 [ERROR] sfp_abuseipdb : Y
2023-12-04 12:27:05,732 [INFO] sflib : Fetching (
v:62.0) Gecko/20100101 Firefox/62.0, timeout=5, c
^C2023-12-04 12:27:06,134 [INFO] sflib : Fetching
 user-agent=Mozilla/5.0 (Windows NT 10.0; Win64;

┌──(dante㉿dante)-[~]
└─$ spiderfoot -l 127.0.0.1:5001

************************************************
 Use SpiderFoot by starting your web browser of c
 browse to http://127.0.0.1:5001/
************************************************

2023-12-04 12:56:09,639 [INFO] sf : Starting web
2023-12-04 12:56:09,647 [WARNING] sf :
************************************************
Warning: passwd file contains no passwords. Authe
Please consider adding authentication to protect
Refer to https://www.spiderfoot.net/documentation
************************************************
```

localhost:5001/scaninfo?id=827E67F1

test RUNNING

Scan Status

Total	256	Unique	186	Status	RUNNING	Errors	82

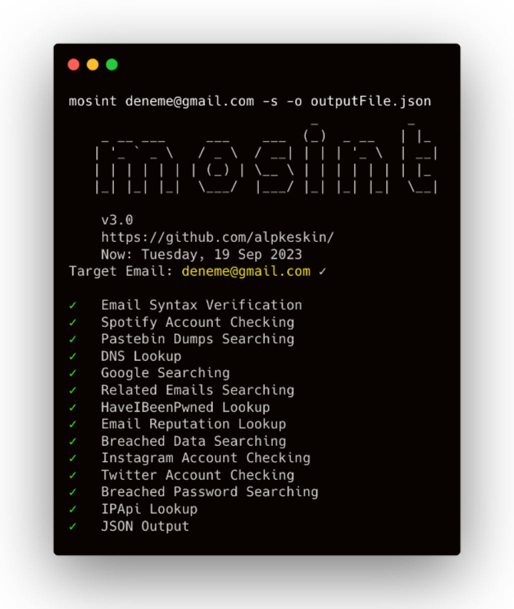
Correlations

High	0	Medium	0	Low	0	Info	0

2. MOSINT (https://github.com/alpkeskin/mosint)

Mosint is an automated email osint tool written in Go that allows you investigate for target emails in a fast and efficient manner. It consolidates numerous services, enabling security researchers to swiftly access a wealth of information.

Features



```
mosint deneme@gmail.com -s -o outputFile.json
                             _            _
    _ __ ___     ___    ___ (_)  _ __    | |_
   | '_ ` _ \   / _ \  / __|| | | '_ \   | __|
   | | | | | | | (_) | \__ \| | | | | |  | |_
   |_| |_| |_|  \___/  |___/|_| |_| |_|   \__|

    v3.0
    https://github.com/alpkeskin/
    Now: Tuesday, 19 Sep 2023
Target Email: deneme@gmail.com ✓

✓   Email Syntax Verification
✓   Spotify Account Checking
✓   Pastebin Dumps Searching
✓   DNS Lookup
✓   Google Searching
✓   Related Emails Searching
✓   HaveIBeenPwned Lookup
✓   Email Reputation Lookup
✓   Breached Data Searching
✓   Instagram Account Checking
✓   Twitter Account Checking
✓   Breached Password Searching
✓   IPApi Lookup
✓   JSON Output
```

- Fast and simple email-based scanning
- Optimized for ease of use and **lightweight** on resources
- Email verification and validation
- Checking **Social Media** Accounts
- Checking **data breaches** and **password leaks**
- Finding **related** emails and domains
- Scanning **pastebin dumps**

- Google Search
- DNS/IP Lookup
- Output to **JSON** file
- Print coffee with --coffee flag!

Installation

go install -v github.com/alpkeskin/mosint/v3/cmd/mosint@latest

Services

Service	Function	Status
ipapi.co - Public	More Information About Domain	✅
hunter.io - Public	Related Emails	✅ 🔑
emailrep.io - Public	Breached Sites Names	✅ 🔑
scylla.so - Public	Database Leaks	🚧
psbdmp.ws - Public	Pastebin Dumps	✅ 🔑
Intelligence X	Password Leaks	✅ 🔑
BreachDirectory	Password Leaks	✅ 🔑
HaveIBeenPwned	Password Leaks	✅ 🔑

🔑 API key required

Configuration file

Mosint supports config file as default located at $HOME/.mosint.yaml. It allows you to define API keys for services.

You must set the config file for mosint to run! To specify a configuration file located in a directory other than the home directory, you can use the --config flag.

Usage

```
mosint example@email.com
```

Call the help (-h) flag for more information on usage.

Reference:

https://github.com/smicallef/spiderfoot

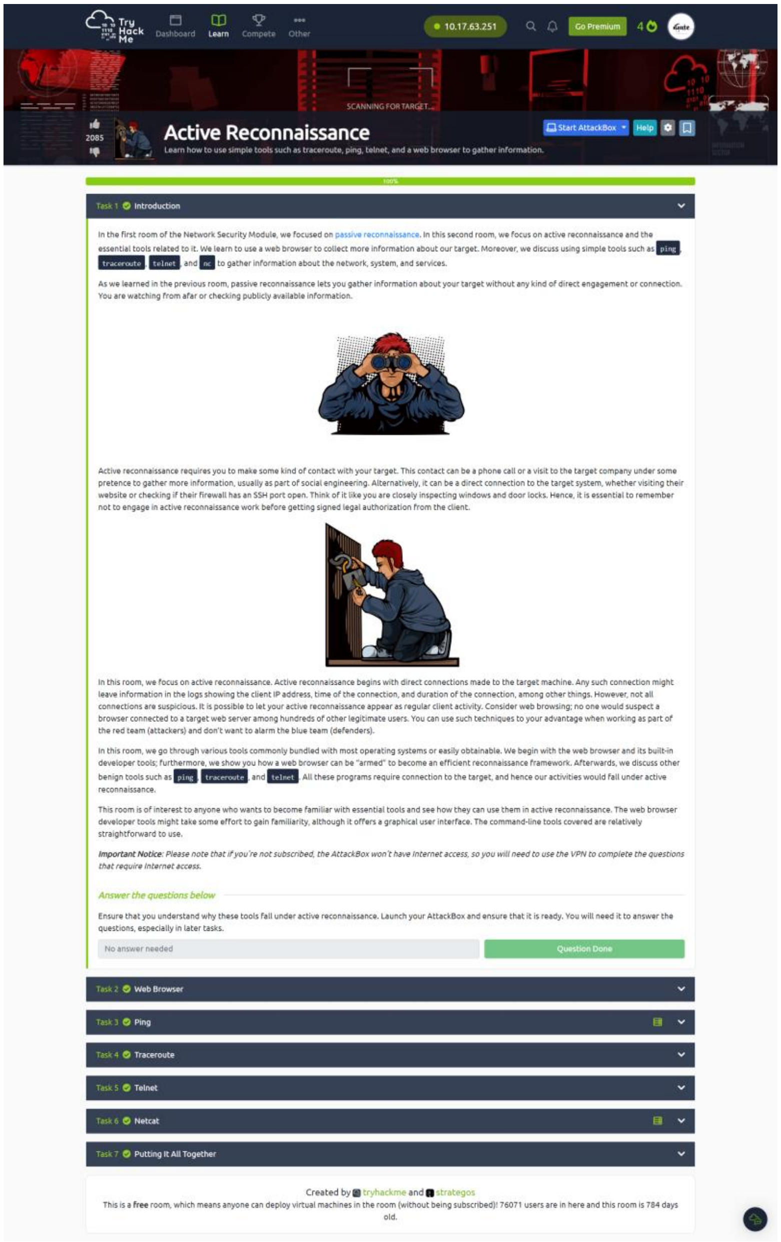
https://github.com/alpkeskin/mosint

https://intel471.com/solutions/attack-surface-protection

https://intel471.com/attack-surface-documentation

Practical Section

https://tryhackme.com/room/activerecon



Active Reconnaissance

Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information.

Task 1 Introduction

In the first room of the Network Security Module, we focused on passive reconnaissance. In this second room, we focus on active reconnaissance and the essential tools related to it. We learn to use a web browser to collect more information about our target. Moreover, we discuss using simple tools such as `ping`, `traceroute`, `telnet`, and `nc` to gather information about the network, system, and services.

As we learned in the previous room, passive reconnaissance lets you gather information about your target without any kind of direct engagement or connection. You are watching from afar or checking publicly available information.

Active reconnaissance requires you to make some kind of contact with your target. This contact can be a phone call or a visit to the target company under some pretence to gather more information, usually as part of social engineering. Alternatively, it can be a direct connection to the target system, whether visiting their website or checking if their firewall has an SSH port open. Think of it like you are closely inspecting windows and door locks. Hence, it is essential to remember not to engage in active reconnaissance work before getting signed legal authorization from the client.

In this room, we focus on active reconnaissance. Active reconnaissance begins with direct connections made to the target machine. Any such connection might leave information in the logs showing the client IP address, time of the connection, and duration of the connection, among other things. However, not all connections are suspicious. It is possible to let your active reconnaissance appear as regular client activity. Consider web browsing; no one would suspect a browser connected to a target web server among hundreds of other legitimate users. You can use such techniques to your advantage when working as part of the red team (attackers) and don't want to alarm the blue team (defenders).

In this room, we go through various tools commonly bundled with most operating systems or easily obtainable. We begin with the web browser and its built-in developer tools; furthermore, we show you how a web browser can be "armed" to become an efficient reconnaissance framework. Afterwards, we discuss other benign tools such as `ping`, `traceroute`, and `telnet`. All these programs require connection to the target, and hence our activities would fall under active reconnaissance.

This room is of interest to anyone who wants to become familiar with essential tools and see how they can use them in active reconnaissance. The web browser developer tools might take some effort to gain familiarity, although it offers a graphical user interface. The command-line tools covered are relatively straightforward to use.

Important Notice: *Please note that if you're not subscribed, the AttackBox won't have Internet access, so you will need to use the VPN to complete the questions that require Internet access.*

Answer the questions below

Ensure that you understand why these tools fall under active reconnaissance. Launch your AttackBox and ensure that it is ready. You will need it to answer the questions, especially in later tasks.

No answer needed | Question Done

Task 2 Web Browser

Task 3 Ping

Task 4 Traceroute

Task 5 Telnet

Task 6 Netcat

Task 7 Putting It All Together

Created by tryhackme and strategos

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 76071 users are in here and this room is 784 days old.

Priyesh Singh

Cyber Security Intern