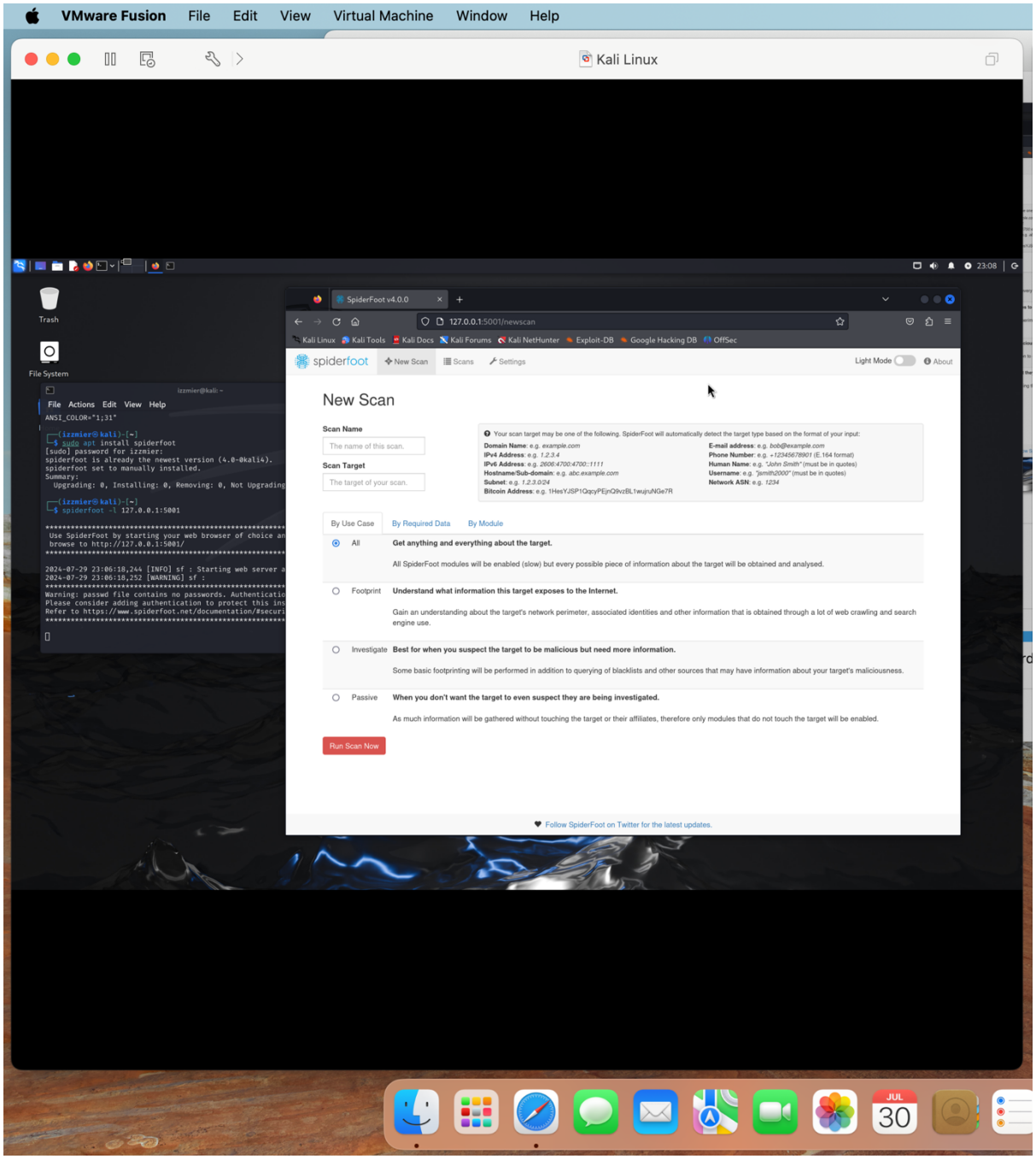
SPIDERFOOT THE MOST POWERFUL OSINT TOOL FOR CYBERSECURITY INVESTIGATIONS

BY IZZMIER IZZUDDIN


VMware Fusion File Edit View Virtual Machine Window Help
Kali Linux
Trash
File System
SpiderFoot v4.0.0
127.0.0.1:5001/newscan
spiderfoot
New Scan
Scans
Settings
Light Mode
About
New Scan
Scan Name
The name of this scan.
Scan Target
The target of your scan.
By Use Case
By Required Data
By Module
All
Get anything and everything about the target.
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.
Footprint
Understand what information this target exposes to the Internet.
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.
Investigate
Best for when you suspect the target to be malicious but need more information.
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.
Passive
When you don't want the target to even suspect they are being investigated.
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.
Run Scan Now
Follow SpiderFoot on Twitter for the latest updates.

SPIDERFOOT TUTORIAL ON KALI LINUX

Here's a step-by-step guide on how to install and use SpiderFoot on Kali Linux (For latest Kali Linux 2024.2 already installed):

Step 1: Install SpiderFoot

1. **Update Your System:** Open your terminal and update your system to ensure all packages are up-to-date.
   sudo apt update && sudo apt upgrade -y

2. **Install SpiderFoot:** SpiderFoot can be installed from the official repositories or cloned from its GitHub repository.
   sudo apt install spiderfoot

   Alternatively, you can clone it from GitHub:
   git clone https://github.com/smicallef/spiderfoot.git
   cd spiderfoot
   sudo python3 setup.py install

Step 2: Running SpiderFoot

1. **Start SpiderFoot:** Run SpiderFoot with the following command:
   spiderfoot

STEP-BY-STEP GUIDE TO ACCESS THE SPIDERFOOT WEB INTERFACE

1. Open Terminal

First, open your terminal on Kali Linux.

2. Start SpiderFoot

Start SpiderFoot by specifying the IP address and port you want it to listen on. The default localhost IP (127.0.0.1) and port (5001) are commonly used.

spiderfoot -l 127.0.0.1:5001

3. Open a Web Browser

Open your preferred web browser on Kali Linux. This can be Firefox, Chromium, or any other browser installed on your system.

4. Navigate to the SpiderFoot Web Interface

In the address bar of your web browser, enter the following URL and press Enter:

http://127.0.0.1:5001

Troubleshooting

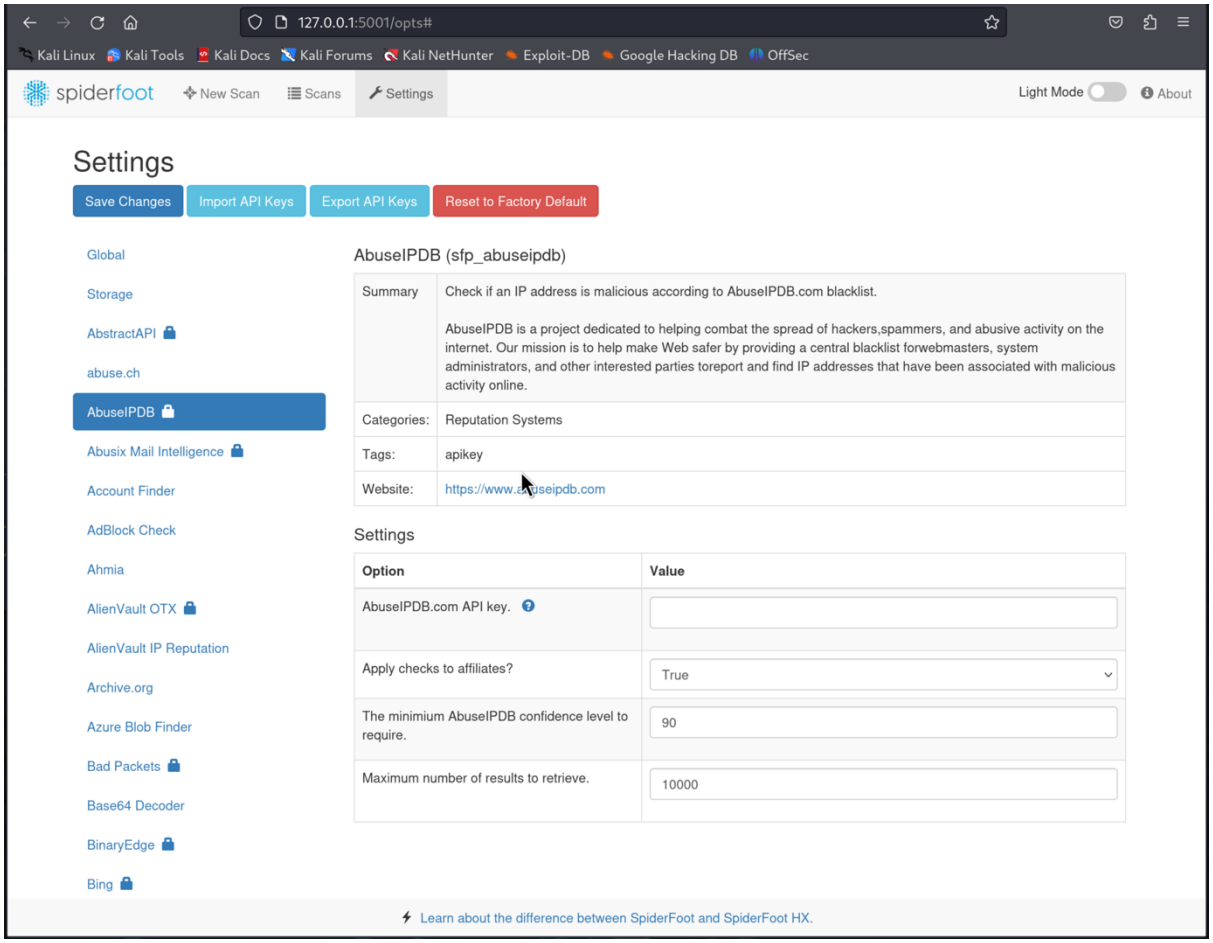
- **If the Web Interface Does Not Load:**
  - Ensure SpiderFoot is running in your terminal and there are no errors.
  - Verify that you are using the correct IP address and port.
  - Check for any firewall rules that might be blocking the connection.
  - Make sure no other service is using the same port.
- **To Change the Port:** If port 5001 is in use by another service or you want to use a different port, you can specify a different port number:

  spiderfoot -l 127.0.0.1:8080

  Then, access the interface using:

  http://127.0.0.1:8080

SPIDERFOOT CONFIGURATIONS



When you access the SpiderFoot web UI and click the Settings button, you'll notice that modules such as AbuseIPDB and AlienVault OTX are locked. To obtain the full information, you'll need to first unlock these modules before running the scan.

Step-By-Step Guide To Enable Abuseipdb In Spiderfoot

Step 1: Obtain an API Key

1. **Sign Up for AbuseIPDB:**
    - Go to AbuseIPDB and sign up for an account.
    - Once you have an account, log in and navigate to the API section.
    - Generate an API key. This key will be used to enable the module in SpiderFoot.

Step 2: Configure SpiderFoot with the API Key

1. **Open Settings:**
    - In the SpiderFoot web interface, click on the gear icon (settings) at the top right corner.
2. **Select the Modules Tab:**
    - In the settings menu, navigate to the "Modules" tab.

    - Scroll down or use the search bar to find the AbuseIPDB module (sfp_abuseipdb).
3. **Configure AbuseIPDB Module:**
    - Click on the AbuseIPDB module to open its settings.
    - You will see a field for the API key.
    - Paste the API key you obtained from AbuseIPDB into the API key field.
4. **Save Settings:**
    - After entering the API key, click on the "Save" button to apply the changes.

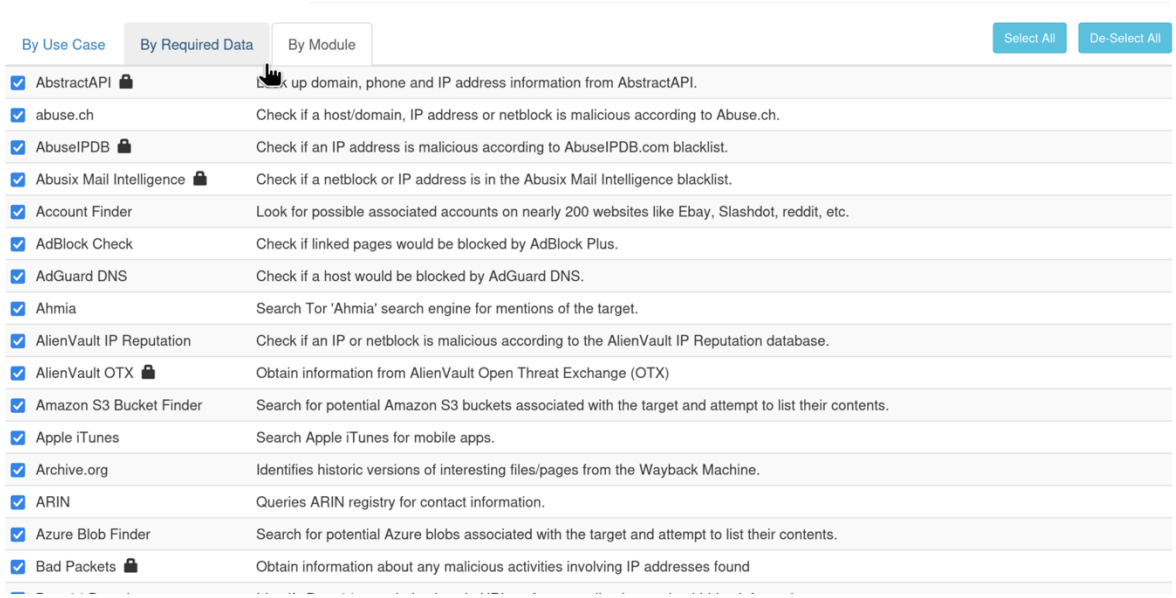
Example Configuration:

1. **Obtain API Key:**
    - API Key: 1234567890abcdef1234567890abcdef
2. **Configure Module:**
    - Go to Settings > Modules > sfp_abuseipdb
    - Enter API Key: 1234567890abcdef1234567890abcdef
    - Save Settings

SIMULATION OF USING SPIDERFOOT

(The results are just a simulation; the real results are too long to screenshot. Please try running the scan using the malicious IP you have identified.)

SIMULATION 1: BY MODULE



Step 1: Configure a New Scan in SpiderFoot

1. **New Scan:**
   - Open the SpiderFoot web interface.
   - Click on "New Scan."
2. **Configure Scan:**
   - **Name:** Enter a name for your scan, e.g., "Malicious IP Investigation."
   - **Target:** Enter the IP address to investigate, e.g., 45.33.32.156.
   - **Use Case:** Select "Investigate" from the drop-down menu to pre-select modules for detailed intelligence gathering.
   - **Select Additional Modules:** Customize the scan by adding modules like sfp_abuseipdb, sfp_dnsresolve, sfp_whois, etc.

Step 2: Run the Scan

1. **Start the Scan:**
   - Click "Run Scan" to initiate the scan.
2. **Monitor Progress:**
   - Monitor the scan progress in the SpiderFoot web interface.

Step 3: Analysing the Results

Results for IP Address 45.33.32.156

1. **DNS Information:**
    - **Reverse DNS:** li752-156.members.linode.com
2. **Web Server Information:**
    - **IP Address:** 45.33.32.156
    - **Server Location:** Fremont, United States
3. **WHOIS Information:**
    - **Registrar:** Linode, LLC
    - **Registration Date:** 23-07-2013
    - **Expiry Date:** 23-07-2023
4. **IP Information:**
    - **Geolocation:** Fremont, United States
    - **Associated Domains:**
        - example.com
        - example.org
5. **Malware and Phishing Information:**
    - **Reports from Malware Databases:**
        - The IP address is flagged in multiple malware databases.
        - Detected as a malicious site by several antivirus engines.
6. **AbuseIPDB Data:**
    - **AbuseIPDB Reports:**
        - The associated IP address has a high abuse score.
        - Multiple reports of malicious activity, including spam and DDoS attacks.

Analysis and Next Steps

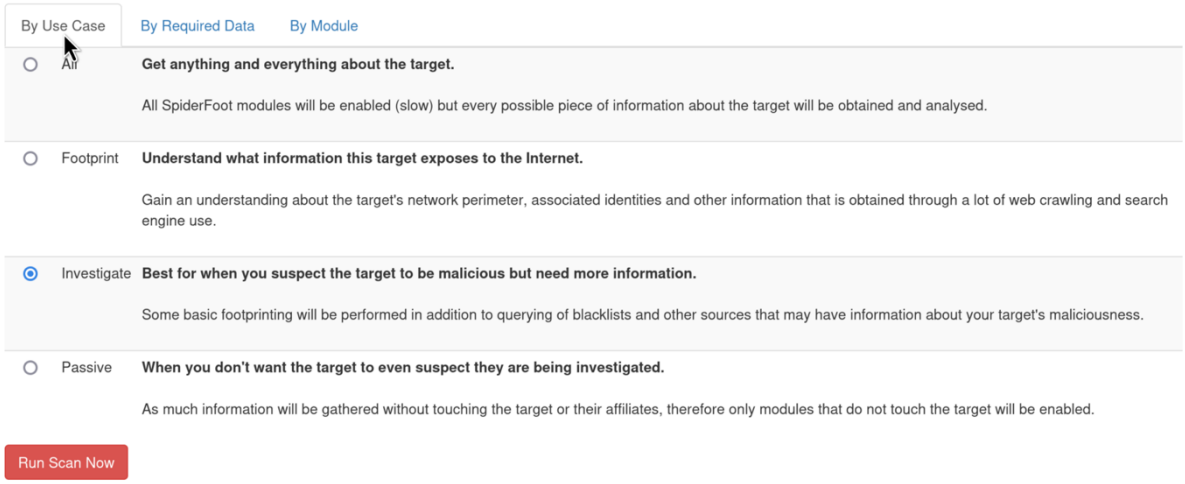
1. **Subdomains:**
    - No subdomains identified.
2. **WHOIS Information:**
    - **Registrar:** Linode, LLC
    - **Creation Date:** 2013-07-23
    - **Expiry Date:** 2023-07-23
3. **IP Information:**
    - **IP Address:** 45.33.32.156
    - **Location:** Fremont, United States
4. **Malware and Phishing Reports:**
    - The IP address is reported in multiple phishing databases.
    - Detected as a malicious site by several antivirus engines.
5. **AbuseIPDB Data:**
    - The associated IP address has a high abuse score, with multiple reports of malicious activity.

Next Steps:

1. **Block the IP Address:** Given its high abuse score and association with malicious activity, consider blocking the IP address in your network.

2. **Investigate Associated Domains:** Further investigate domains associated with the IP address for additional threats.
3. **Review Logs:** Check your network logs for any interactions with the IP address and assess any potential impacts on your systems.

SIMULATION 2: BY USE CASE (INVESTIGATE)



Step 1: Configure a New Scan in SpiderFoot

1. **New Scan:**
   - Open the SpiderFoot web interface.
   - Click on "New Scan."
2. **Configure Scan:**
   - **Name:** Enter a name for your scan, e.g., "Malicious IP Investigation."
   - **Target:** Enter the IP address to investigate, e.g., 45.33.32.156.
   - **Use Case:** Select "Investigate" from the drop-down menu. This pre-selects a set of modules aimed at gathering detailed intelligence about the target.
   - **Select Additional Modules:** Customize the scan by adding or modifying modules based on your needs, for instance:
     - sfp_abuseipdb
     - sfp_dnsresolve
     - sfp_whois
     - sfp_virustotal
     - sfp_shodan

Step 2: Run the Scan

1. **Start the Scan:**
   - Click "Run Scan" to initiate the scan.
2. **Monitor Progress:**
   - Monitor the scan progress in the SpiderFoot web interface.

Step 3: Analysing the Results

Results for IP Address 45.33.32.156

1. **DNS Information:**

    - **Reverse DNS:** li752-156.members.linode.com
2. **Web Server Information:**
    - **IP Address:** 45.33.32.156
    - **Server Location:** Fremont, United States
3. **WHOIS Information:**
    - **Registrar:** Linode, LLC
    - **Registration Date:** 2013-07-23
    - **Expiry Date:** 2023-07-23
4. **IP Information:**
    - **Geolocation:** Fremont, United States
    - **Associated Domains:**
        - malicious-site.com
        - example-malware.org
5. **Malware and Phishing Information:**
    - **Reports from Malware Databases:**
        - The IP address is flagged in multiple malware databases.
        - Detected as a malicious site by several antivirus engines.
6. **AbuseIPDB Data:**
    - **AbuseIPDB Reports:**
        - The associated IP address has a high abuse score.
        - Multiple reports of malicious activity, including spam and DDoS attacks.
7. **Shodan Data:**
    - **Open Ports:**
        - Port 80 (HTTP)
        - Port 22 (SSH)
    - **Service Information:**
        - Running a web server with outdated software versions.
8. **VirusTotal Data:**
    - **Malware Reports:**
        - Several detections from different antivirus vendors indicating malicious activity.

Analysis and Next Steps

1. **Subdomains:**
    - No subdomains identified.
2. **WHOIS Information:**
    - **Registrar:** Linode, LLC
    - **Creation Date:** 2013-07-23
    - **Expiry Date:** 2023-07-23
3. **IP Information:**
    - **IP Address:** 45.33.32.156
    - **Location:** Fremont, United States
4. **Malware and Phishing Reports:**
    - The IP address is reported in multiple phishing databases.
    - Detected as a malicious site by several antivirus engines.

5. **AbuseIPDB Data:**
    - The associated IP address has a high abuse score, with multiple reports of malicious activity.
6. **Shodan Data:**
    - The IP address has open ports with potentially vulnerable services.
7. **VirusTotal Data:**
    - Multiple antivirus engines detect the IP address as associated with malicious activity.

Next Steps:

1. **Block the IP Address:** Given its high abuse score and association with malicious activity, consider blocking the IP address in your network.
2. **Investigate Associated Domains:** Further investigate domains associated with the IP address for additional threats.
3. **Review Logs:** Check your network logs for any interactions with the IP address and assess any potential impacts on your systems.
4. **Update Security Measures:** Ensure that your security measures are updated to detect and block similar threats in the future.