

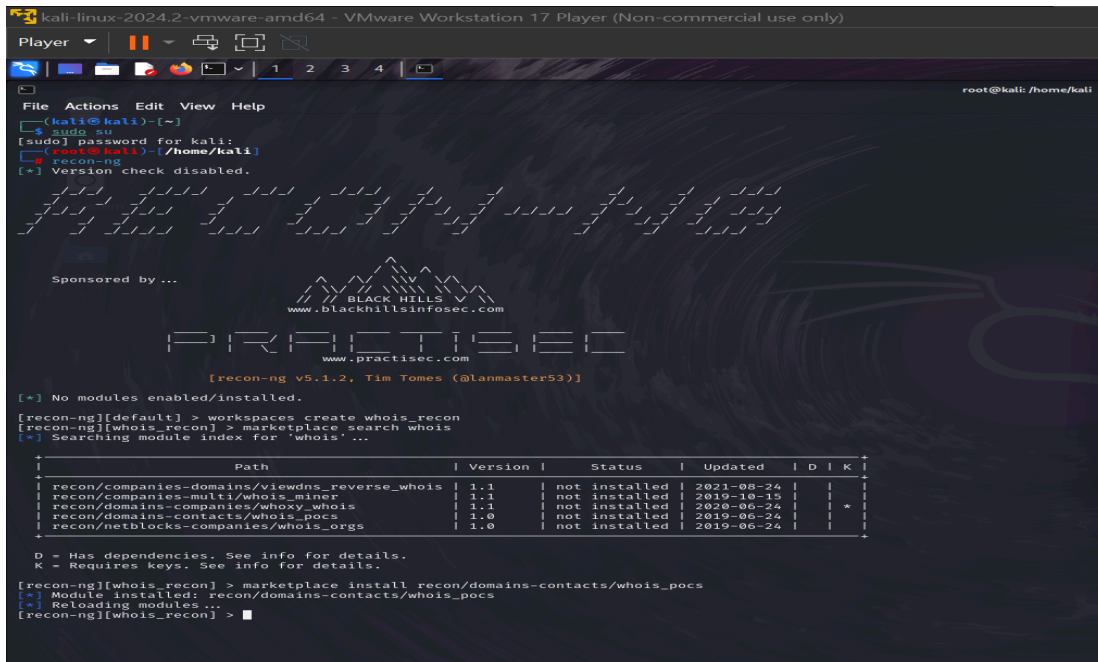
# FINDING INFORMATION ON A TARGET DOMAIN USING [WHOIS]

TOOLS :KALI LINUX [RECON-NG]

PROJECT-SITE : FACEBOOK.COM [FOR EDUCATIONAL PURPOSES ONLY]

RECON-ng is a powerful web reconnaissance framework designed for open-source intelligence (OSINT) gathering. It provides a modular environment with various built-in tools for tasks such as domain reconnaissance, social media investigations, and network enumeration. It uses features like: modularity, data management, APIs and Integration, User-friendly Interface and Reporting to carry out the given tasks. RECON-ng is a powerful web reconnaissance framework designed for open-source intelligence (OSINT) gathering. It provides a modular environment with various built-in tools for tasks such as domain reconnaissance, social media investigations, and network enumeration.

Input from kali : recon-ng



```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
root@kali: /home/kali
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~/home/kali$ recon-ng
[*] Version check disabled.

RECON-NG

Sponsored by ...
BLACK HILLS
www.blackhillsinfosec.com
PRACTISEC
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.
[recon-ng][default] > workspace create whois_recon
[recon-ng][whois_recon] > marketplace search whois
[*] Searching module index for 'whois' ...

+-----+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| recon/companies-domains/viewdns_reverse_whois | 1.1 | not installed | 2021-08-24 | | |
| recon/companies-multi/whois_miner | 1.1 | not installed | 2019-18-15 | | |
| recon/domains-companies/whoxy_whois | 1.1 | not installed | 2020-06-24 | | * |
| recon/domains-contacts/whois_pocs | 1.0 | not installed | 2019-06-24 | | |
| recon/netblocks-companies/whois_orgs | 1.0 | not installed | 2019-06-24 | | |
+-----+-----+-----+-----+-----+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.
[recon-ng][whois_recon] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
[recon-ng][whois_recon] > 
```

## Input from kali using : whois

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
root@kali: /home/kali

File Actions Edit View Help
+ recon/netblocks-companies/whois_orgs | 1.0 | not installed | 2019-06-24 | |
+
D - Has dependencies. See info for details.
K - Requires keys. See info for details.

[recon-ng][whois_recon] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules...
[recon-ng][whois_recon] > options set SOURCE facebook.com
[!] Invalid option name.
[recon-ng][whois_recon] > options set SOURCE facebook.com
[!] Invalid option name.
[recon-ng][whois_recon] > modules load recon/domains-contacts/whois_pocs
[recon-ng][whois_recon][whois_pocs] > options set SOURCE facebook.com
SOURCE ==> facebook.com
[recon-ng][whois_recon][whois_pocs] > info

Name: Whois POC Harvester
Author: Tim Tomes (@lanmaster53)
Version: 1.0

Description:
Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
'contacts' table with the results.

Options:
+-----+-----+-----+-----+
| Name | Current Value | Required | Description |
+-----+-----+-----+-----+
| SOURCE | facebook.com | yes | source of input (see 'info' for details) |
+-----+-----+-----+-----+

Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs

[recon-ng][whois_recon][whois_pocs] > run

FACEBOOK.COM

[*] URL: http://whois.arin.net/rest/pocs/domain-facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First_Name: Brandon
[*] Last_Name: Stout
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
root@kali: /home/kali

File Actions Edit View Help
+ recon/netblocks-companies/whois_orgs | 1.0 | not installed | 2019-06-24 | |
+ recon/domains-contacts/whois_pocs | 1.0 | not installed | 2019-06-24 | |
+ recon/domains-hosts/hackertarget | 1.1 | not installed | 2020-05-17 | |
+
D - Has dependencies. See info for details.
K - Requires keys. See info for details.

[recon-ng][whois_recon] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][whois_recon] > modules load recon/domains-hosts/hackertarget
[recon-ng][whois_recon][hackertarget] > options set SOURCE facebook.com
SOURCE ==> facebook.com
[recon-ng][whois_recon][hackertarget] > info

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
Version: 1.1

Description:
Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
+-----+-----+-----+-----+
| Name | Current Value | Required | Description |
+-----+-----+-----+-----+
| SOURCE | facebook.com | yes | source of input (see 'info' for details) |
+-----+-----+-----+-----+

Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs

[recon-ng][whois_recon][hackertarget] > s5s5
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-ccu1.facebook.com
[+] Ip_Address: 31.13.64.212
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-cdg4.facebook.com
[+] Ip_Address: 157.240.202.202
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-cgk1.facebook.com
[+] Ip_Address: 31.13.95.216
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-del1.facebook.com
[+] Ip_Address: 157.240.239.216
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-del2.facebook.com
[+] Ip_Address: 163.70.145.213
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-dfw5.facebook.com
[+] Ip_Address: 31.13.93.219
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
SUMMARY
[+] 500 total (500 new) hosts found.
[recon-ng][whois_recon][hackertarget] > ss
```

```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-ccu1.facebook.com
[+] Ip_Address: 31.13.64.212
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-cdg4.facebook.com
[+] Ip_Address: 157.240.202.202
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-cgk1.facebook.com
[+] Ip_Address: 31.13.95.216
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-del1.facebook.com
[+] Ip_Address: 157.240.239.216
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-del2.facebook.com
[+] Ip_Address: 163.70.145.213
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+] Country: None
[+] Host: cloud-x2p-edge-http-shv-02-dfw5.facebook.com
[+] Ip_Address: 31.13.93.219
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
SUMMARY
[+] 500 total (500 new) hosts found.
[recon-ng][whois_recon][hackertarget] >
```

# FACEBOOKRESULT FOR RECON-NG USING WHOIS ON THE SITE

How to find WHOIS information on a target domain-name with Recon-ng. Here we used RECON-NG to find the IP ADDRESS of a site using WHOIS.

After creating a new lab, we then begin by gathering WHOIS information about the target domain for FACEBOOK, we then installed modules from the marketplace to search **whois** information after that we set the SOURCE facebook.com, now we are ready to search WHOIS for information regarding "facebook.com" then we RUN.

Here we can see various contacts and locations in the second and third slide for facebook.com. Now we will attempt to discover as many subdomains as possible, with their IPV4 address for facebook.com by using HACKERTARGET.com API. We would first need to import the HACKERTARGET module. After doing that, we then want to load the module. Then we began searching HACKERTARGET for subdomain information in regards to FACEBOOK.COM. **After that we set SOURCE for FACEBOOK.COM then info to to see some information around what this module is used for and how its being used. Then we continued by typing RUN and enter to execute. Here in the fourth and fifth slide we noticed a list of various subdomains associated with facebook.com appearing.**

This information is useful for an attacker who may be targeting FACEBOOK. They can use this information to attack the various subdomains and their IP addresses associated with Facebook, as they may not all be equally secure, to find a way through their security.

Protecting against reconnaissance tools like RECON-ng, especially when it comes to WHOIS queries, involves several strategies to limit the amount of information publicly available about your domain. Here are some steps you can take:

1. **WHOIS Privacy Protection:** Use a domain registrar that offers WHOIS privacy services. This masks your personal information (like your name, email, and address) and replaces it with the registrar's information.
2. **Domain Registration:** Register domains under a company name or legal entity instead of personal names when possible. This adds a layer of anonymity.
3. **Limit WHOIS Data:** Some registrars allow you to customize the information that is publicly available. Check if you can limit the data disclosed.
4. **Use a Secure DNS Provider:** Some DNS providers offer features that can help obscure your domain information and provide additional security.
5. **Monitor WHOIS Data:** Regularly check your domain's WHOIS information to ensure it's accurate and not revealing more than you intend.

6. **Avoid Public Listings:** Be cautious about where you list your domain information (e.g., business directories). The more places your information appears, the easier it is for tools like RECON-ng to gather data.
7. **Educate Your Team:** Ensure that everyone involved with the domain understands the importance of maintaining privacy and security regarding sensitive information.

**By implementing these measures, you can significantly reduce the risk of exposing your domain to reconnaissance tools.**