RECON-NG USING WHOIS

TOOL: KALI LINUX

TEST SUBJECT: FACEBOOK.COM

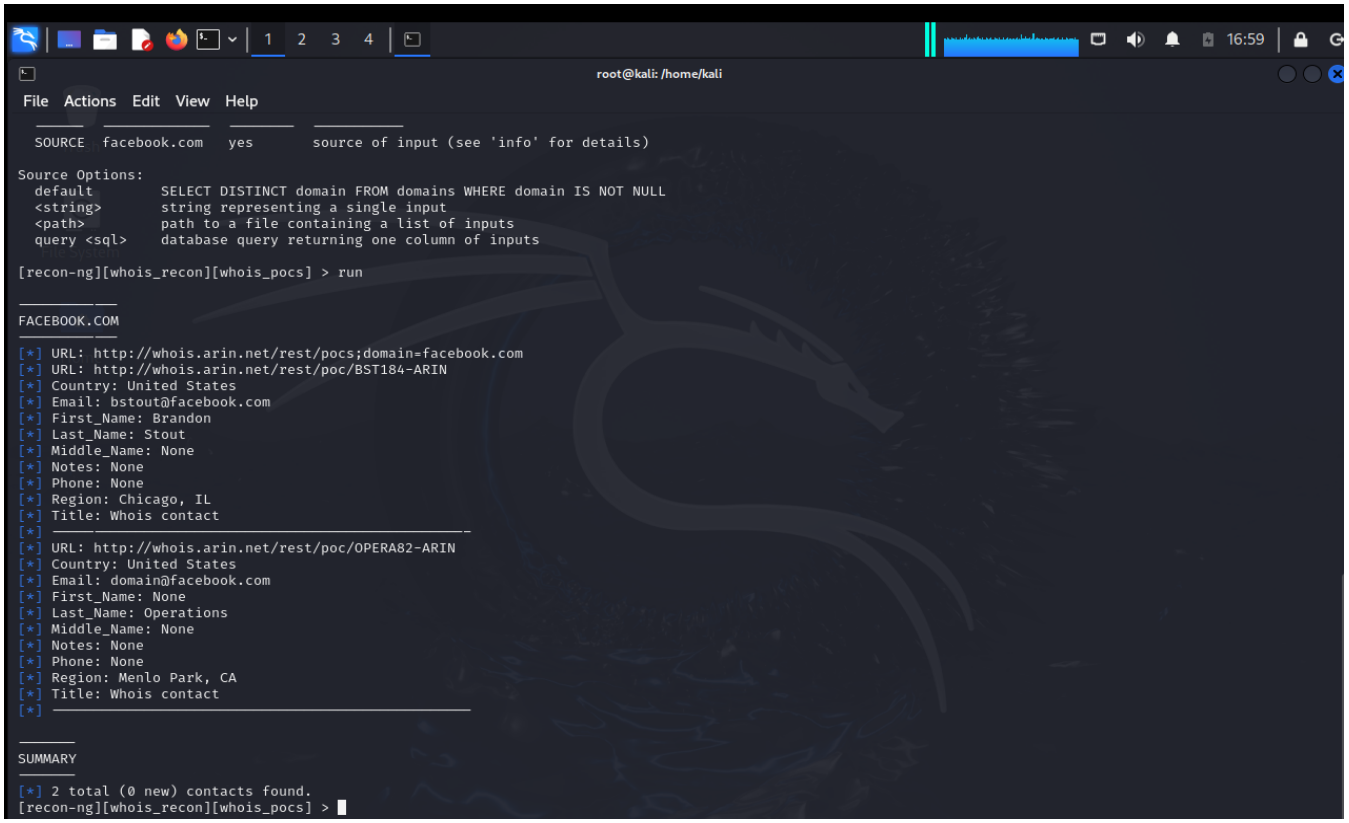
WHOIS is a protocol used to query databases that store registered users or assignees of a domain name or an IP address block. It provides information about the ownership and availability of domain names, including details such as:

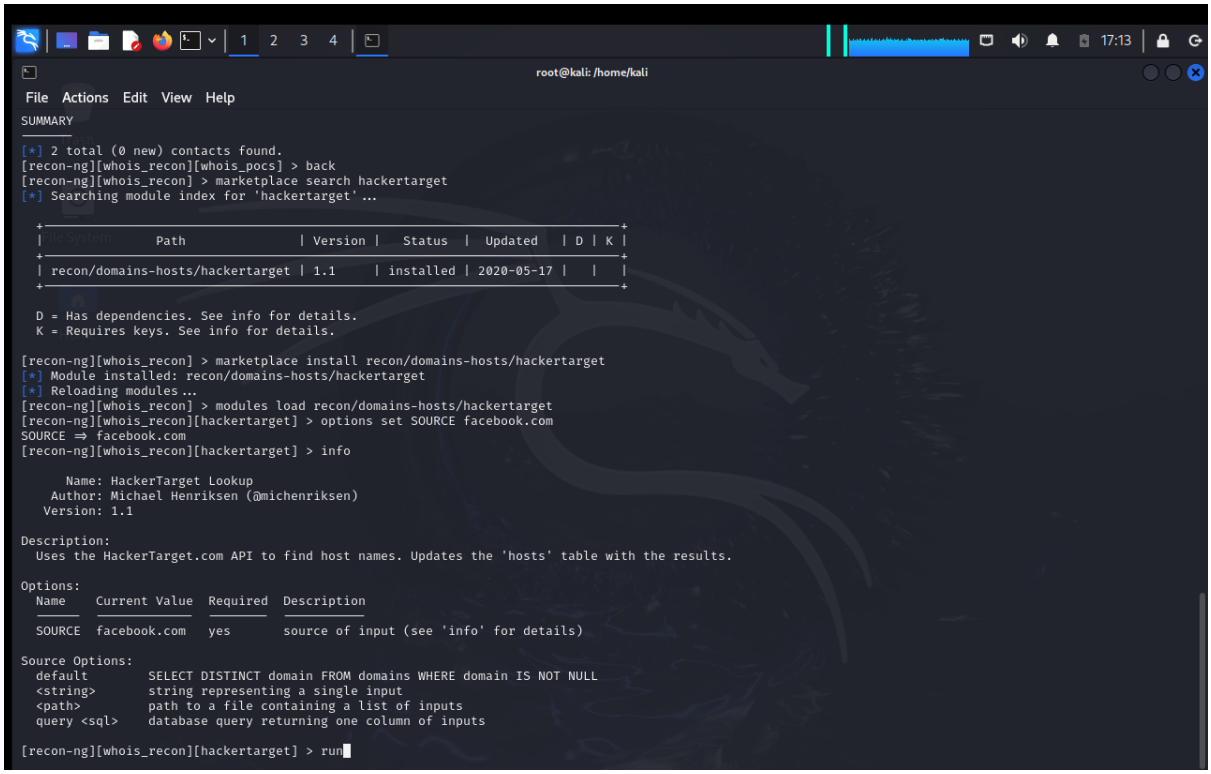
- **Registrant Name**: The person or organization that owns the domain.
- **Contact Information**: Email, phone number, and address of the registrant.
- **Domain Status**: Indicates if the domain is active, expired, or on hold.
- **Creation and Expiration Dates**: When the domain was registered and when it is set to expire.
- **Nameservers**: The DNS servers associated with the domain.

WHOIS is commonly used for:

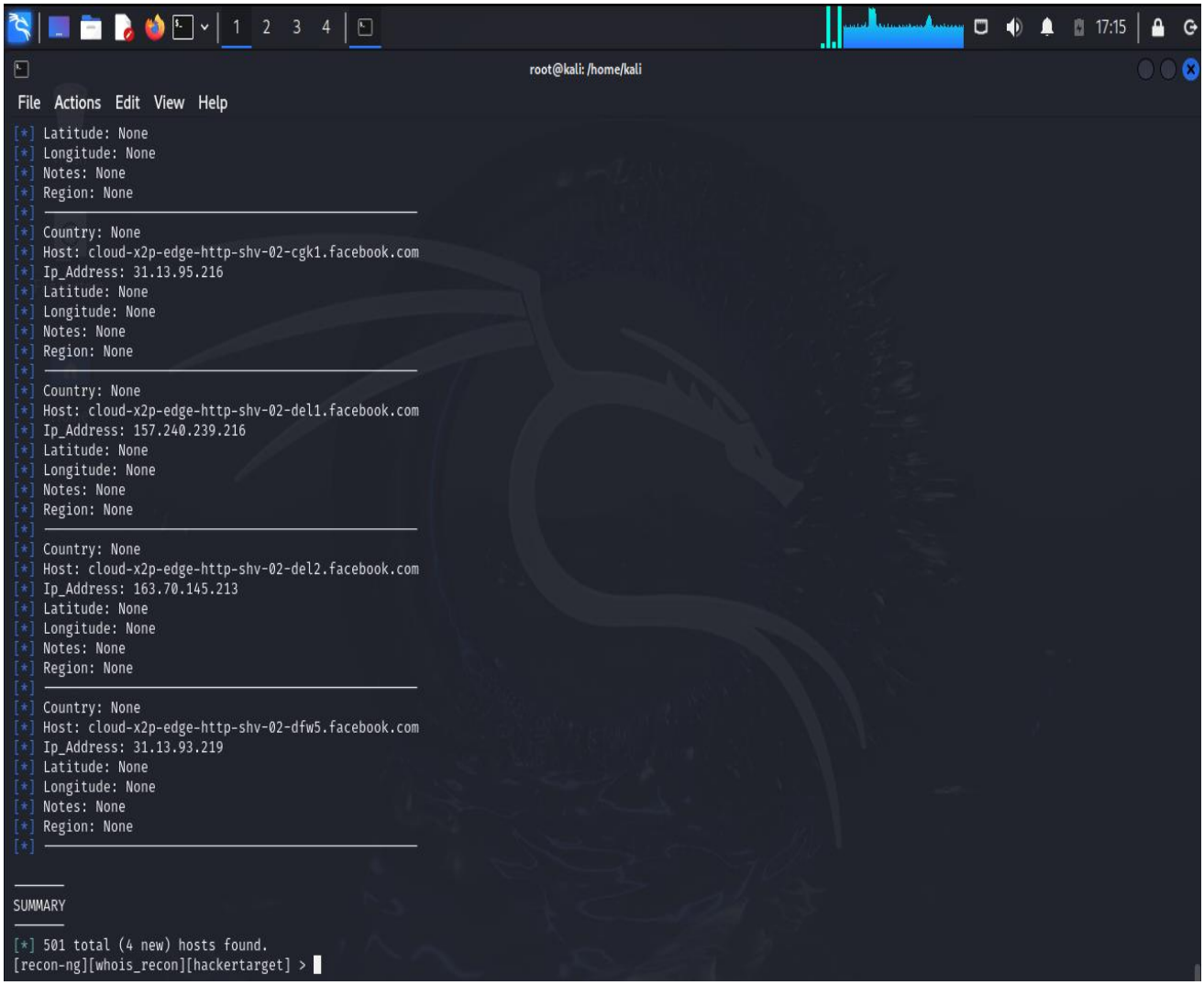
1. **Domain Research**: Finding out who owns a domain or its registration status.
2. **Contacting Domain Owners**: Reaching out to owners for inquiries or offers.
3. **Checking Domain Availability**: Seeing if a specific domain name is registered or available for purchase.
4. **Cybersecurity**: Identifying malicious domains or understanding potential threats.
5. **Trademark Protection**: Ensuring that domain registrations do not infringe on existing trademarks.


root@kali: /home/kali
File Actions Edit View Help
[2] Recon modules
[recon-ng][default] > workspaces 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	2019-10-15		
recon/domains-companies/whoxy_whois	1.1	not installed	2020-06-24		*
recon/domains-contacts/whois_pocs	1.0	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] > options set SOURCE facebook.com
[!] Invalid option name.
[recon-ng][whois_recon] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
[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:


root@kali: /home/kali
File Actions Edit View Help
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
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
[*] Title: Whois contact
SUMMARY
[*] 2 total (0 new) contacts found.
[recon-ng][whois_recon][whois_pocs] >


1 2 3 4
17:13
root@kali: /home/kali
File Actions Edit View Help
SUMMARY
[*] 2 total (0 new) contacts found.
[recon-ng][whois_recon][whois_pocs] > back
[recon-ng][whois_recon] > marketplace search hackertarget
[*] Searching module index for 'hackertarget' ...
| Path | Version | Status | Updated | D | K |
| recon/domains-hosts/hackertarget | 1.1 | 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] > run


1 2 3 4
17:16
root@kali: /home/kali
File Actions Edit View Help
query <sql> database query returning one column of inputs
[recon-ng][whois_recon][hackertarget] > run
FACEBOOK.COM
[*] Country: None
[*] Host: facebook.com
[*] Ip_Address: 157.240.254.35
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: alf.facebook.com
[*] Ip_Address: 192.168.16.27
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: anycast-control-ext-shv-01-akl1.facebook.com
[*] Ip_Address: 31.13.78.21
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: anycast-control-ext-shv-01-ams2.facebook.com
[*] Ip_Address: 157.240.247.16
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: anycast-control-ext-shv-01-ams4.facebook.com
[*] Ip_Address: 157.240.201.7
[*] Latitude: None


1 2 3 4
17:15
root@kali: /home/kali
File Actions Edit View Help
[*] 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
[*] 501 total (4 new) hosts found.
[recon-ng][whois_recon][hackertarget] >