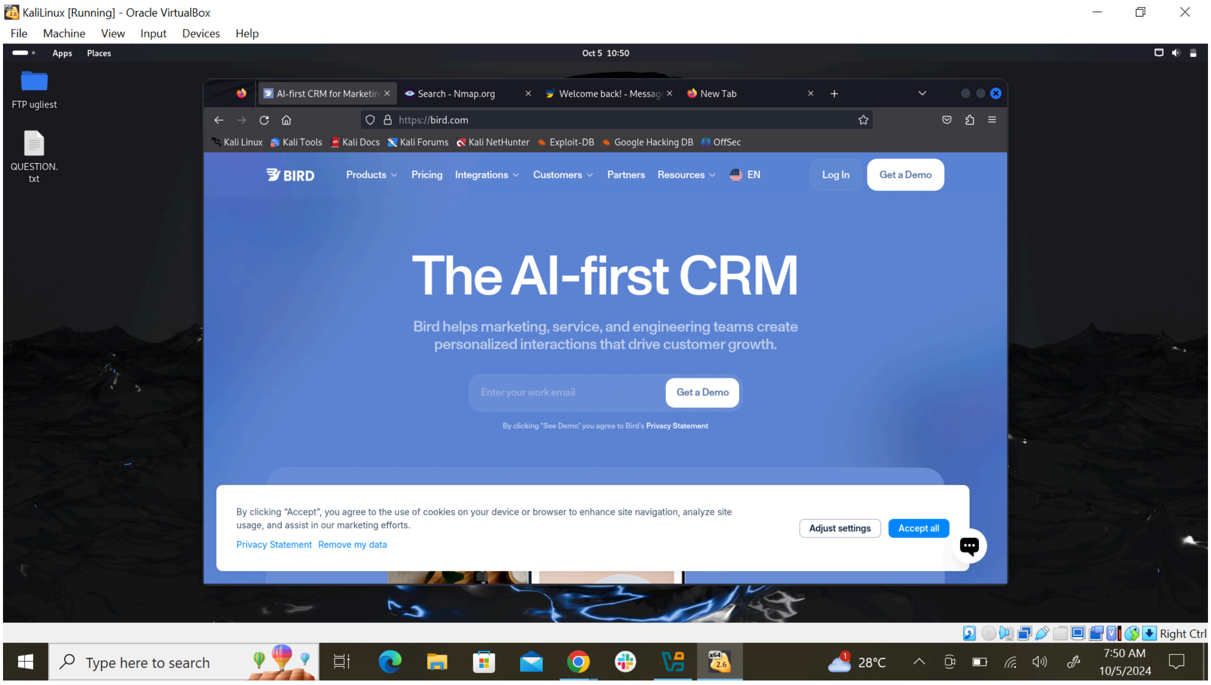
INFORMATION GATHERING

Tool: RECON-NG
Project-Site- www.messagebird.com

Recon-ng is an open-source web reconnaissance framework that helps security professionals gather and analyze information about target domains and organizations.


KaliLinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Oct 5 10:50
FTP ugliest
QUESTION.txt
AI-first CRM for Marketin
Search - Nmap.org
Welcome back! - Messag
New Tab
https://bird.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
BIRD
Products Pricing Integrations Customers Partners Resources EN
Log In
Get a Demo
Enter your work email
Get a Demo
Adjust settings
Accept all
Privacy Statement Remove my data
Right Ctrl
Type here to search
28°C
7:50 AM
10/5/2024

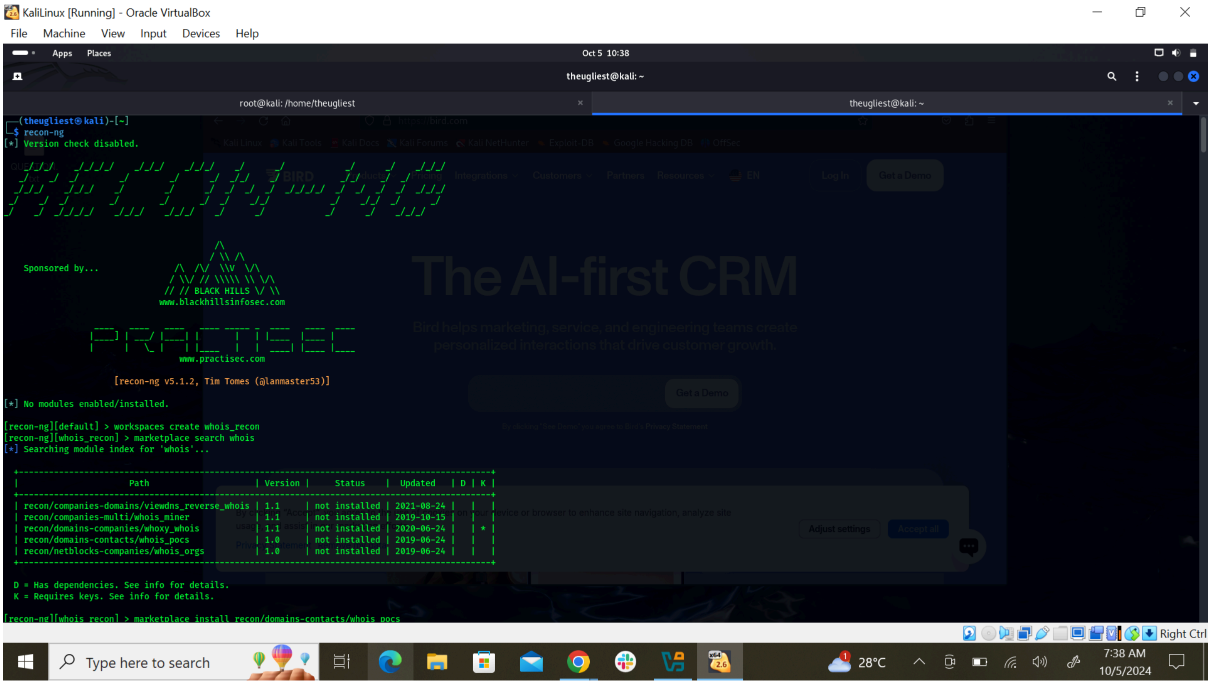
The AI-first CRM

Bird helps marketing, service, and engineering teams create personalized interactions that drive customer growth.

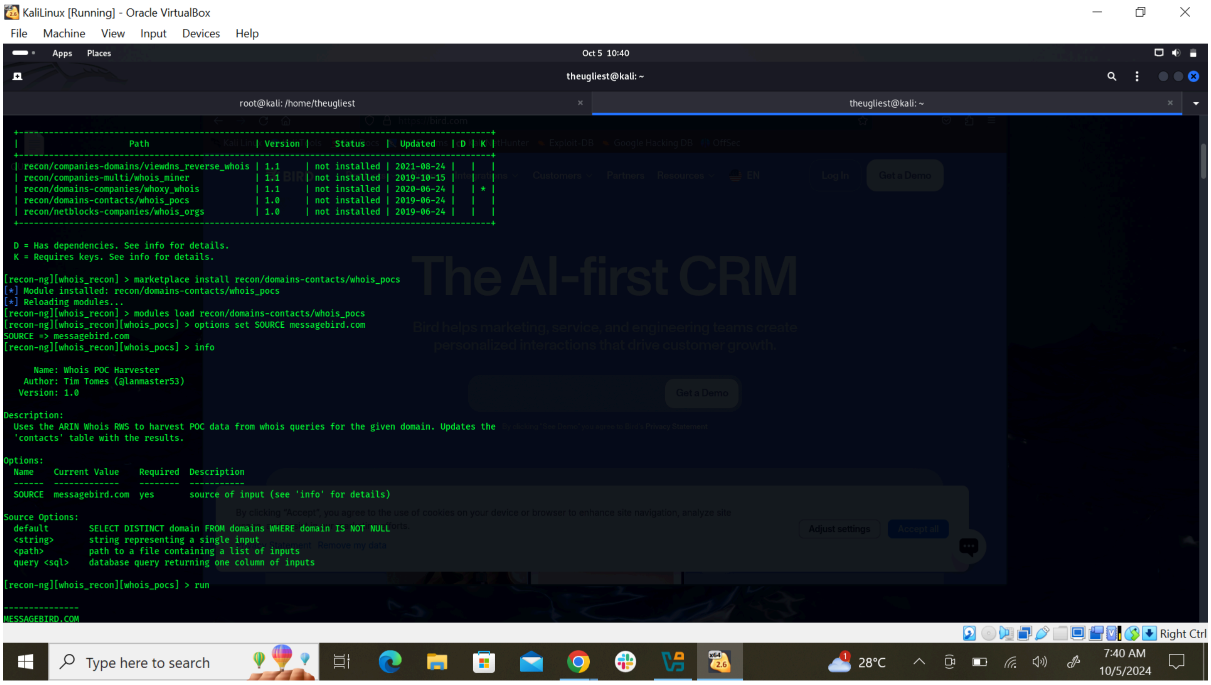
By clicking "See Demo" you agree to Bird's Privacy Statement

By clicking "Accept", you agree to the use of cookies on your device or browser to enhance site navigation, analyze site usage, and assist in our marketing efforts.

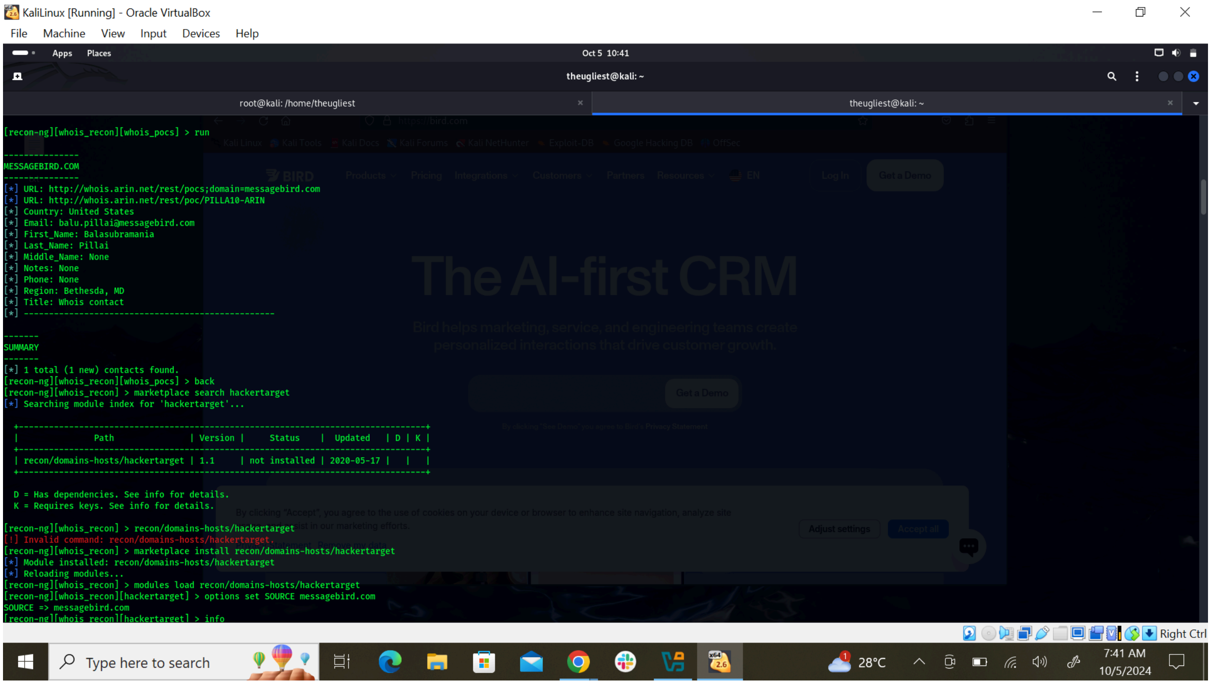
Scan method from kali: **recon-ng**
workspaces create whois_recon
marketplace search whois
marketplace install
recon/domains-contacts/whois_pocs
options set SOURCE facebook.com
modules load
recon/domains-contacts/whois_pocs
marketplace search hackertarget
marketplace install
recon/domains-hosts/hackertarget
modules load recon/domains-hosts/hackertarget
options set SOURCE facebook.com



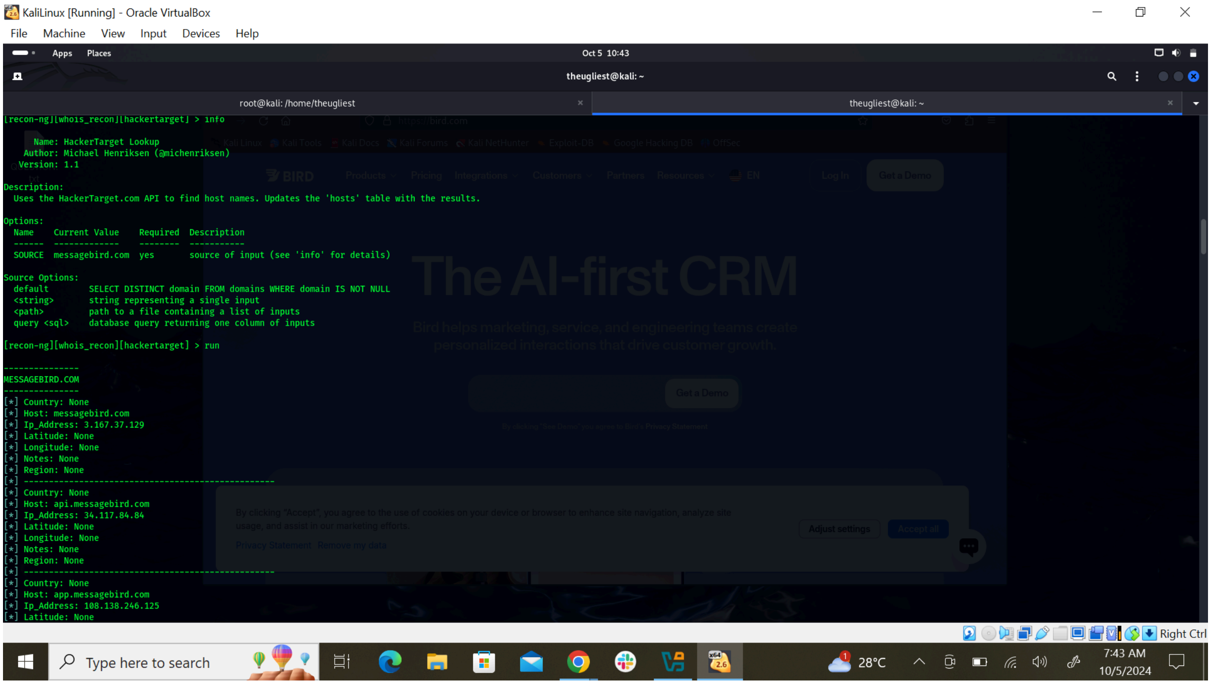
```
┌──(theugliest㉿kali)-[~]
└─$ recon-ng
[*] Version check disabled.

    _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/
   _/    _/  _/        _/        _/      _/  _/_/    _/            _/_/    _/  _/
  _/_/_/    _/_/_/    _/        _/      _/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
 _/    _/  _/        _/        _/      _/  _/    _/_/            _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/


                                          /\
                                         / \\ /\
    Sponsored by...               /\  /\/  \\V  \/\
                                 / \\/ // \\\\\ \\ \/\
                                // // BLACK HILLS \/ \\
                               www.blackhillsinfosec.com

                  ____   ____   ____   ____ _____ _ ____   ____   ____
                 |____] | ___/ |____| |       |   | |____  |____ |
                 |      |    \_|    | |____   |   |  ____| |____ |____
                                   www.practisec.com

                      [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[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     | 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
```



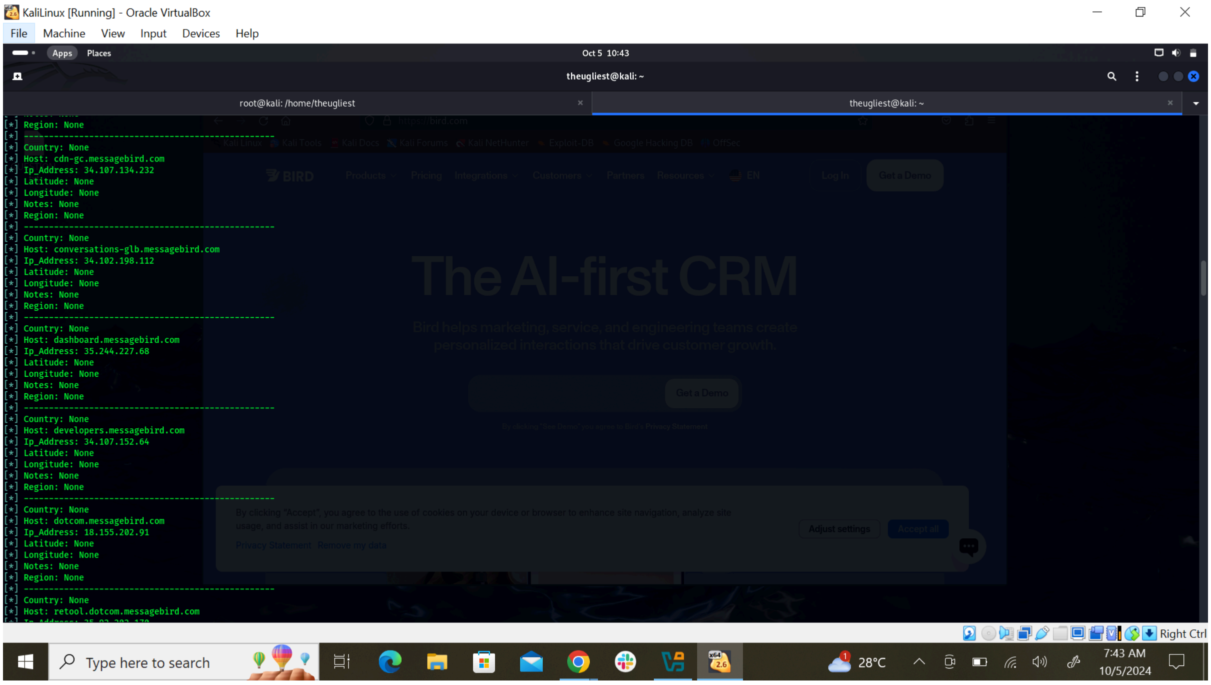
```
  +---------------------------------------------------------------------------------------+
  |                      Path                      | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------------+
  | recon/companies-domains/viewdns_reverse_whois | 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     | 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] > modules load recon/domains-contacts/whois_pocs
[recon-ng][whois_recon][whois_pocs] > options set SOURCE messagebird.com
SOURCE => messagebird.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  messagebird.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

---------------
MESSAGEBIRD.COM
```



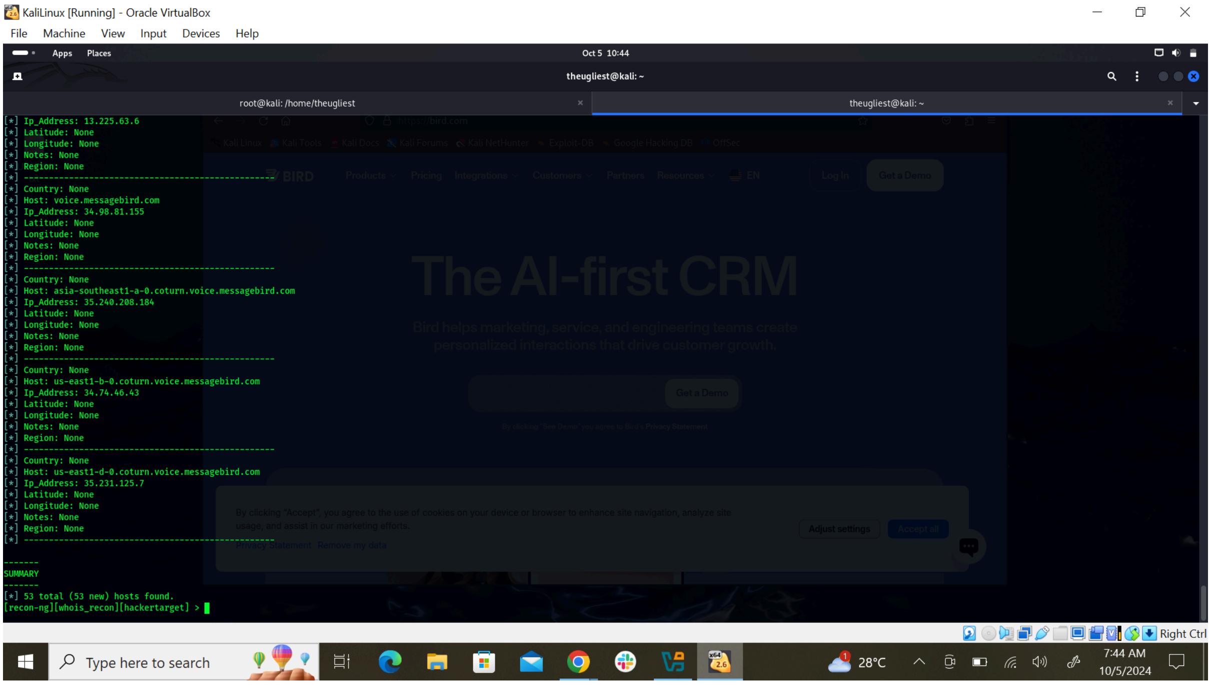
```
[recon-ng][whois_recon][whois_pocs] > run

---------------
MESSAGEBIRD.COM
---------------
[*] URL: http://whois.arin.net/rest/pocs;domain=messagebird.com
[*] URL: http://whois.arin.net/rest/poc/PILLA10-ARIN
[*] Country: United States
[*] Email: balu.pillai@messagebird.com
[*] First_Name: Balasubramania
[*] Last_Name: Pillai
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Bethesda, MD
[*] Title: Whois contact
[*] --------------------------------------------------

-------
SUMMARY
-------
[*] 1 total (1 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     | not installed | 2020-05-17 |   |   |
  +--------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][whois_recon] > recon/domains-hosts/hackertarget
[!] Invalid command: recon/domains-hosts/hackertarget.
[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 messagebird.com
SOURCE => messagebird.com
[recon-ng][whois_recon][hackertarget] > info
```



```
[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  messagebird.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

---------------
MESSAGEBIRD.COM
---------------
[*] Country: None
[*] Host: messagebird.com
[*] Ip_Address: 3.167.37.129
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: api.messagebird.com
[*] Ip_Address: 34.117.84.84
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: app.messagebird.com
[*] Ip_Address: 108.138.246.125
[*] Latitude: None
```


KaliLinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Oct 5 10:43
theugliest@kali: ~
root@kali: /home/theugliest
theugliest@kali: ~
Type here to search
28°C
7:43 AM
10/5/2024

```
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: cdn-gc.messagebird.com
[*] Ip_Address: 34.107.134.232
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: conversations-glb.messagebird.com
[*] Ip_Address: 34.102.198.112
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: dashboard.messagebird.com
[*] Ip_Address: 35.244.227.68
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: developers.messagebird.com
[*] Ip_Address: 34.107.152.64
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: dotcom.messagebird.com
[*] Ip_Address: 18.155.202.91
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: retool.dotcom.messagebird.com
```


KaliLinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Oct 5 10:44
theugliest@kali: ~
root@kali: /home/theugliest
theugliest@kali: ~
Type here to search
28°C
7:44 AM
10/5/2024

```
[*] Ip_Address: 13.225.63.6
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: voice.messagebird.com
[*] Ip_Address: 34.98.81.155
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: asia-southeast1-a-0.coturn.voice.messagebird.com
[*] Ip_Address: 35.240.208.184
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: us-east1-b-0.coturn.voice.messagebird.com
[*] Ip_Address: 34.74.46.43
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: us-east1-d-0.coturn.voice.messagebird.com
[*] Ip_Address: 35.231.125.7
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------

-------
SUMMARY
-------
[*] 53 total (53 new) hosts found.
[recon-ng][whois_recon][hackertarget] >
```

RESULTS

Vulnerabilities

When you obtain an IP address using Recon-ng on Kali Linux, there are several steps you can take to gather more information and assess the target. Here are some actions you can consider:

1. WHOIS Lookup: Use a WHOIS service to find information about the IP address, such as the organization that owns it, contact information, and registration details.
2. Geolocation: Use geolocation services to find out where the IP address is located. This can provide insights into the physical location of the server or device.
3. Ping and Traceroute: Use tools like `ping` and `traceroute` to test the connectivity and path to the IP address. This can help identify network latency and hops along the route.
4. Port Scanning: Utilize tools like Nmap to scan the IP for open ports. This can help identify services running on the target and potential vulnerabilities.
5. Service Enumeration: If you identify open ports, you can perform service enumeration to gather more details about the services running (e.g., web servers, FTP servers).
6. Reverse DNS Lookup: Find the domain name associated with the IP address, if any, using reverse DNS lookup.
7. Vulnerability Scanning: Use tools like Nikto or OpenVAS to check for vulnerabilities in web applications or servers associated with the IP.
8. Social Engineering: If the IP address is linked to a specific organization, you could gather information about the organization and its employees for potential social engineering tactics.
9. Malware and Threat Intelligence: Check the IP against threat intelligence databases to see if it's known for malicious activity.
10. OSINT Techniques: Use other open-source intelligence techniques to gather more context about the IP address or its associated entities.