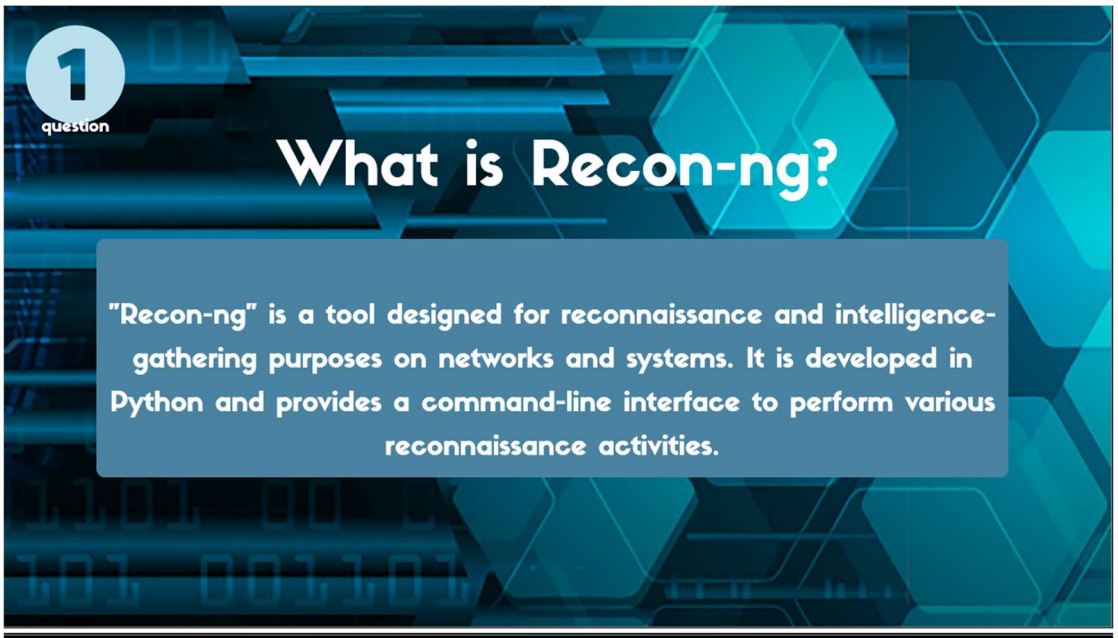
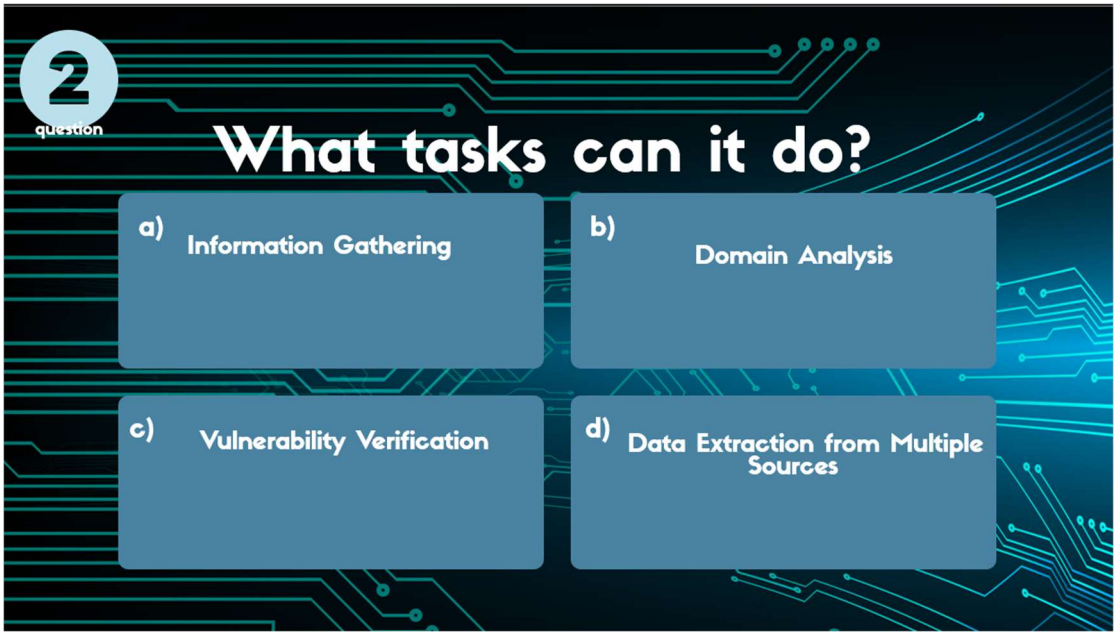
RECON - NG


1
question
What is Recon-ng?
"Recon-ng" is a tool designed for reconnaissance and intelligence-gathering purposes on networks and systems. It is developed in Python and provides a command-line interface to perform various reconnaissance activities.


2
question
What tasks can it do?
a) Information Gathering
b) Domain Analysis
c) Vulnerability Verification
d) Data Extraction from Multiple Sources

4

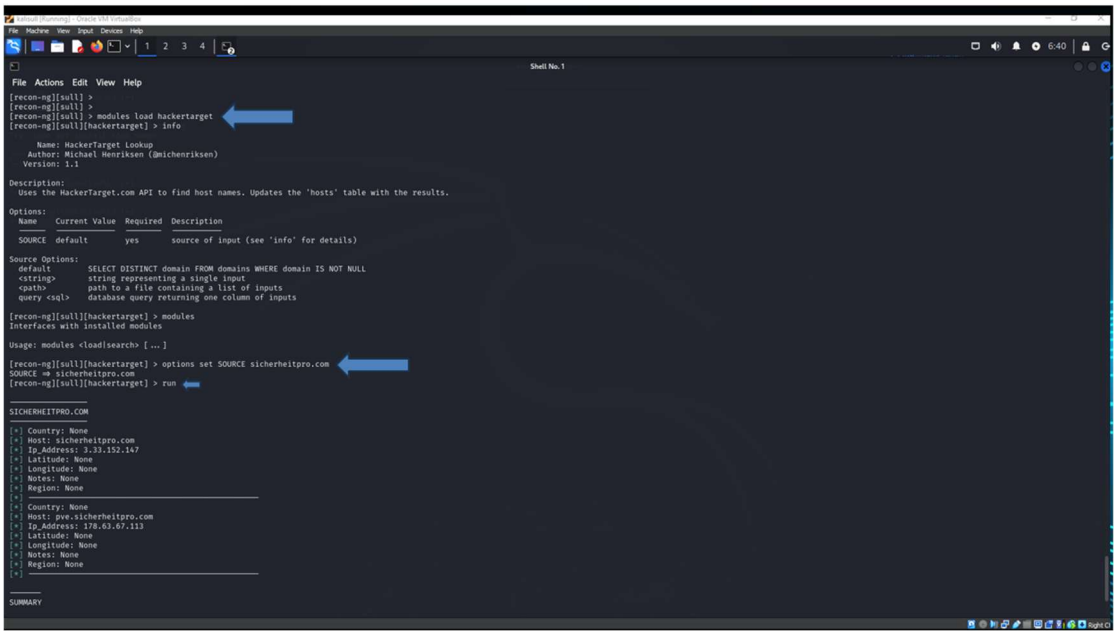
answer

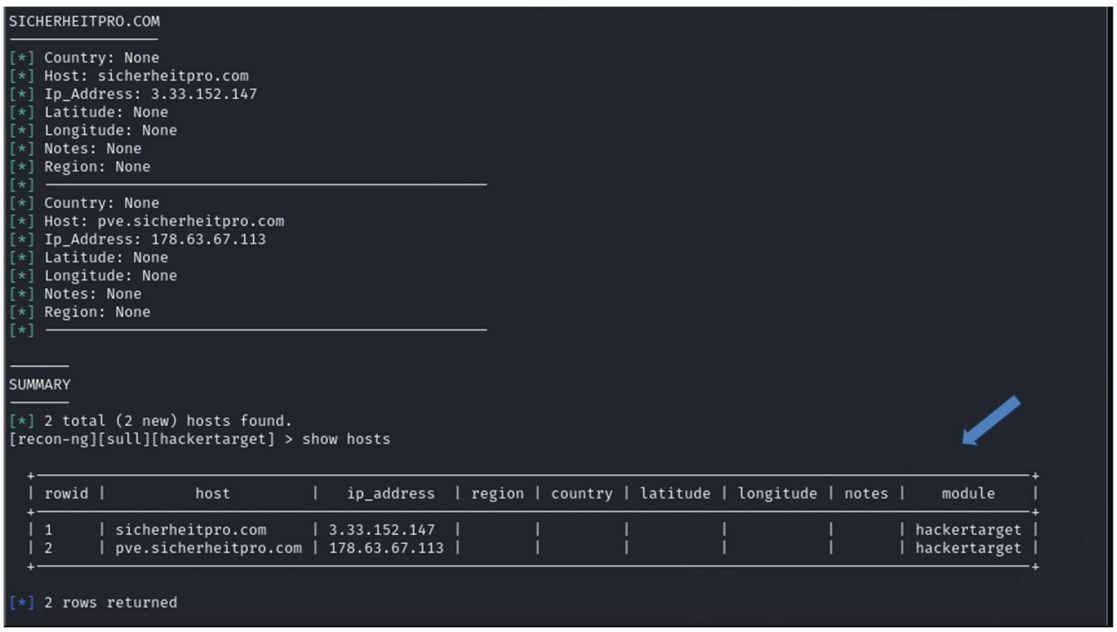
Recon-ng offers multiple modules and extensions that you can install and use to expand the tool's capabilities and achieve various reconnaissance goals.

Please note that the use of these tools should be done with the consent of the system owner or the administrator of the target network, and should only be used for legitimate purposes such as security testing and threat assessment.


File Machine View Input Devices Help
Shell No. 1
File Actions Edit View Help
Sponsored by ...
www.blackhillsinfosec.com
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[1] Recon modules
[recon-ng][default] > help
Commands (type [help|?] <topic>):
back Exits the current context
dashboard Displays a summary of activity
db Interfaces with the workspace's database
exit Exits the framework
help Displays this menu
index Creates a module index (dev only)
keys Manages third party resource credentials
marketplace Interfaces with the module marketplace
modules Interfaces with installed modules
options Manages the current context options
pdb Starts a Python Debugger session (dev only)
script Records and executes command scripts
shell Executes shell commands
show Shows various framework items
snapshots Manages workspace snapshots
spool Spools output to a file
workspaces Manages workspaces
[recon-ng][default] > workspaces
Manages workspaces
Usage: workspaces <create|list|load|remove> [...]
[recon-ng][default] > workspaces create sull
[recon-ng][sull] >
[recon-ng][sull] > workspaces list
Workspaces | Modified
default | 2024-05-04 16:36:49
sull | 2024-05-07 06:08:59
sultan wep | 2024-05-04 16:39:31
[recon-ng][sull] >
Right Ctrl


Shell No. 1
File Actions Edit View Help
[recon-ng][sull] > marketplace
Interfaces with the module marketplace
Usage: marketplace <info|install|refresh|remove|search> [...]
[recon-ng][sull] > marketplace info
Shows detailed information about available modules
Usage: marketplace info <<path>|<prefix>|all>
[recon-ng][sull] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-multi/censys_org
[*] Module installed: recon/companies-multi/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
[*] Module installed: recon/contacts-contacts/mailtester
[*] Module installed: recon/contacts-contacts/mangle
[*] Module installed: recon/contacts-contacts/unmangle
[*] Module installed: recon/contacts-credentials/hibp_breach
[*] Module installed: recon/contacts-credentials/hibp_paste
[*] Module installed: recon/contacts-domains/migrate_contacts
[*] Module installed: recon/contacts-domains/censys_email_to_domains
[*] Module installed: recon/contacts-profiles/fullcontact
[*] Module installed: recon/credentials-credentials/adobe
[*] Module installed: recon/credentials-credentials/bozocrack
[*] Module installed: recon/credentials-credentials/hashes_org
[*] Module installed: recon/domains-companies/censys_companies
[*] Module installed: recon/domains-companies/pen
[*] Module installed: recon/domains-companies/whoxy_whois
[*] Module installed: recon/domains-contacts/hunter_io
[*] Module installed: recon/domains-contacts/metacrawler
[*] Module installed: recon/domains-contacts/pen
[*] Module installed: recon/domains-contacts/pgp_search
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/wikileaker
[*] Module installed: recon/domains-domains/brute_suffix


Shell No. 1
File Actions Edit View Help
[recon-ng][sull] >
[recon-ng][sull] >
[recon-ng][sull] > modules load hackertarget
[recon-ng][sull][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 default 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][sull][hackertarget] > modules
Interfaces with installed modules
Usage: modules <load|search> [...]
[recon-ng][sull][hackertarget] > options set SOURCE sicherheitpro.com
SOURCE => sicherheitpro.com
[recon-ng][sull][hackertarget] > run
SICHERHEITPRO.COM
[*] Country: None
[*] Host: sicherheitpro.com
[*] Ip_Address: 3.33.152.147
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: pve.sicherheitpro.com
[*] Ip_Address: 178.63.67.113
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
SUMMARY


SICHERHEITPRO.COM
[*] Country: None
[*] Host: sicherheitpro.com
[*] Ip_Address: 3.33.152.147
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: pve.sicherheitpro.com
[*] Ip_Address: 178.63.67.113
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
SUMMARY
[*] 2 total (2 new) hosts found.
[recon-ng][sull][hackertarget] > show hosts
rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	sicherheitpro.com	3.33.152.147						hackertarget
2	pve.sicherheitpro.com	178.63.67.113						hackertarget
[*] 2 rows returned