

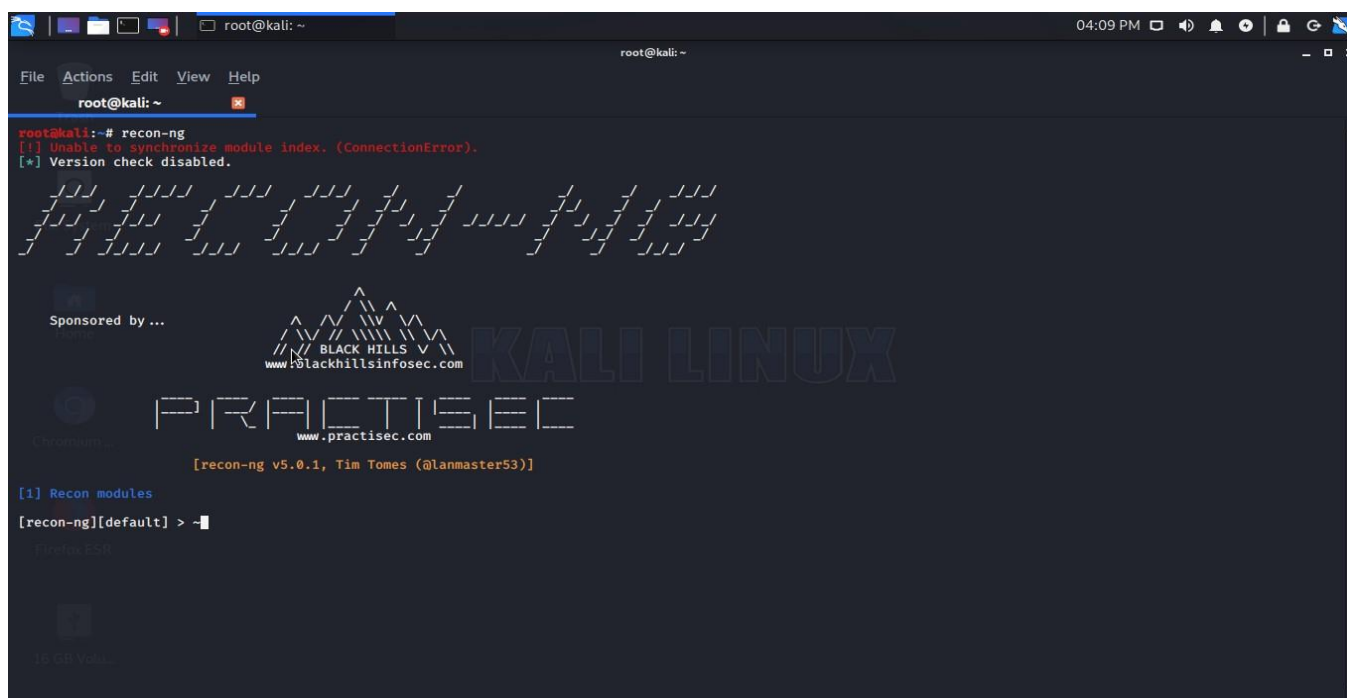
Soutech Cyber Security Lab Test on Recon-NG

Recon-ng

Recon-ng is a full feature Web Reconnaissance framework used for information gathering purpose as well as network detection. This tool is written in python, having independent modules, database interaction and other features. You can download the software from www.bitbucket.org. This Open Source Web Reconnaissance tool requires kali Linux Operating system.

Recon-ng Overview

Run the Application Recon-ng or open the terminal of Kali-Linux and type recon-ng and hit enter.



```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# recon-ng  
[!] Unable to synchronize module index. (ConnectionError).  
[*] Version check disabled.  
  
Recon-NG  
  
Sponsored by ...  
BLACK HILLS  
www.blackhillsinfosec.com  
KALI LINUX  
PRACTISEC  
www.practisec.com  
[recon-ng v5.0.1, Tim Tomes (@lanmaster53)]  
[1] Recon modules  
[recon-ng][default] > -
```

```

root@kali: ~
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default] > options list
-----
Name          Current Value  Required  Description
-----
NAMESERVER    8.8.8.8        yes       default nameserver for the resolver mixin
PROXY         no             no        proxy server (address:port)
THREADS       10            yes       number of threads (where applicable)
TIMEOUT       10            yes       socket timeout (seconds)
USER-AGENT    Recon-ng/v5    yes       user-agent string
VERBOSITY     1             yes       verbosity level (0 = minimal, 1 = verbose, 2 = debug)

[recon-ng][default] > marketplace refresh
[*] Marketplace index refreshed.
[recon-ng][default] > 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][default] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > info

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

```

root@kali: ~
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default] > options list
-----
Name          Current Value  Required  Description
-----
NAMESERVER    8.8.8.8        yes       default nameserver for the resolver mixin
PROXY         no             no        proxy server (address:port)
THREADS       10            yes       number of threads (where applicable)
TIMEOUT       10            yes       socket timeout (seconds)
USER-AGENT    Recon-ng/v5    yes       user-agent string
VERBOSITY     1             yes       verbosity level (0 = minimal, 1 = verbose, 2 = debug)

[recon-ng][default] > marketplace refresh
[*] Marketplace index refreshed.
[recon-ng][default] > 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][default] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > info

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
    
```

