Recon-ng è un software di ricognizione web scritto in Python.
Completo di moduli indipendenti come l'interazione del database, l'aiuto interattivo e il completamento automatico dei comandi.
Recon-ng fornisce un ambiente potente open source di ricognizione web, dove quest'ultima può essere condotta rapidamente e maniera accurata.

A cosa serve?

Dove si colloca la fase di recon? La fase di recon si colloca al primo posto nel primo segmento

di azioni di un attacco o pentest. La prima fase infatti e' la raccolta informazioni e la catalogazione, quindi avremo:

- reconnaissance
- info gathering

La raccolta delle informazioni puo' essere inserita in uno storage arcaico (testo semplice) o in maniera piu avanzata su un DB o gestita tramite **Maltego**.

Recon-NG

Recon-ng ha un look and feel simile a Metasploit Framework, quindi riduce la curva di apprendimento per sfruttarlo appieno.
Naturalmente è molto diverso, però Recon-ng è stato progettato esclusivamente per la ricognizione open source basato sul web.

E' uno strumento complementare a **Metasploit Framework** e **Social-Engineer Toolkit** perche' conduce una ricognizione passiva.

Un esempio di ricognizione attiva sarebbe **Skipfish** del Security Team di Google.

Recon-ng è un framework completamente modulare e rende facile contribuire scrivendo moduli. Ogni modulo è una sottoclasse della classe "module".
La classe "module" è un interprete personalizzato "cmd" dotato di funzionalità incorporate che fornisce interfacce semplici per le operazioni più comuni come la standardizzazione dell'output, l'interazione con il database, richieste web e la gestione delle API. Pertanto, tutto il lavoro piu' complesso e noioso è stato fatto.

Moduli

Recon-ng è dotato di circa 80 moduli di recon, 2 moduli di discovery, 2 moduli di exploitation, 7 moduli di reporting e 2 moduli di import.

- cache_snoop – DNS Cache Snooper
- interesting_files – Interesting File Finder
- command_injector – Remote Command Injection Shell Interface
- xpath_bruter – Xpath Injection Brute Forcer
- csv_file – Advanced CSV File Importer
- list – List File Importer
- point_usage – Jigsaw – Point Usage Statistics Fetcher
- purchase_contact – Jigsaw – Single Contact Retriever
- search_contacts – Jigsaw Contact Enumerator
- jigsaw_auth – Jigsaw Authenticated Contact Enumerator
- linkedin_auth – LinkedIn Authenticated Contact Enumerator
- github_miner – Github Resource Miner
- whois_miner – Whois Data Miner
- bing_linkedin – Bing Linkedin Profile Harvester
- email_validator – SalesMaple Email Validator
- mailtester – MailTester Email Validator
- mangle – Contact Name Mangler
- unmangle – Contact Name Unmangler
- hibp_breach – Have I been pwned? Breach Search
- hibp_paste – Have I been pwned? Paste Search
- pwnedlist – PwnedList Validator
- migrate_contacts – Contacts to Domains Data Migrator
- facebook_directory – Facebook Directory Crawler
- fullcontact – FullContact Contact Enumerator
- adobe – Adobe Hash Cracker
- bozocrack – PyBozoCrack Hash Lookup
- hashes_org – Hashes.org Hash Lookup
- leakdb – leakdb Hash Lookup
- metacrawler – Meta Data Extractor
- pgp_search – PGP Key Owner Lookup
- salesmaple – SalesMaple Contact Harvester
- whois_pocs – Whois POC Harvester
- account_creds – PwnedList – Account Credentials Fetcher
- api_usage – PwnedList – API Usage Statistics Fetcher
- domain_creds – PwnedList – Pwned Domain Credentials Fetcher
- domain_ispwned – PwnedList – Pwned Domain Statistics Fetcher
- leak_lookup – PwnedList – Leak Details Fetcher
- leaks_dump – PwnedList – Leak Details Fetcher
- brute_suffix – DNS Public Suffix Brute Forcer
- baidu_site – Baidu Hostname Enumerator
- bing_domain_api – Bing API Hostname Enumerator
- bing_domain_web – Bing Hostname Enumerator

- brute_hosts – DNS Hostname Brute Forcer
- builtwith – BuiltWith Enumerator
- google_site_api – Google CSE Hostname Enumerator
- google_site_web – Google Hostname Enumerator
- netcraft – Netcraft Hostname Enumerator
- shodan_hostname – Shodan Hostname Enumerator
- ssl_san – SSL SAN Lookup
- vpnhunter – VPNHunter Lookup
- yahoo_domain – Yahoo Hostname Enumerator
- zone_transfer – DNS Zone File Harvester
- ghdb – Google Hacking Database
- punkspider – PunkSPIDER Vulnerabilty Finder
- xssed – XSSed Domain Lookup
- xssposed – XSSposed Domain Lookup
- migrate_hosts – Hosts to Domains Data Migrator
- bing_ip – Bing API IP Neighbor Enumerator
- freegeoip – FreeGeoIP
- ip_neighbor – My-IP-Neighbors.com Lookup
- ipinfodb – IPInfoDB GeoIP
- resolve – Hostname Resolver
- reverse_resolve – Reverse Resolver
- ssltools – SSLTools.com Host Name Lookups
- geocode – Address Geocoder
- reverse_geocode – Reverse Geocoder
- flickr – Flickr Geolocation Search
- instagram – Instagram Geolocation Search
- picasa – Picasa Geolocation Search
- shodan – Shodan Geolocation Search
- twitter – Twitter Geolocation Search
- whois_orgs – Whois Company Harvester
- reverse_resolve – Reverse Resolver
- shodan_net – Shodan Network Enumerator
- census_2012 – Internet Census 2012 Lookup
- sonar_cio – Project Sonar Lookup
- migrate_ports – Ports to Hosts Data Migrator
- dev_diver – Dev Diver Repository Activity Examiner
- linkedin – Linkedin Contact Crawler
- linkedin_crawl – Linkedin Profile Crawler
- namechk – NameChk.com Username Validator
- profiler – OSINT HUMINT Profile Collector
- twitter – Twitter Handles
- github_repos – Github Code Enumerator
- gists_search – Github Gist Searcher
- github_dorks – Github Dork Analyzer
- csv – CSV File Creator
- html – HTML Report Generator

- json – JSON Report Generator
- list – List Creator
- pushpin – PushPin Report Generator
- xlsx – XLSX File Creator
- xml – XML Report Generator

dipendenze

Tutte le librerie di terze parti devono essere installate prima dell'uso.

- dnspython – http://www.dnspython.org/
- dicttoxml – https://github.com/quandyfactory/dicttoxml/
- jsonrpclib – https://github.com/joshmarshall/jsonrpclib/
- lxml – http://lxml.de/
- mechanize – http://wwwsearch.sourceforge.net/mechanize/
- slowaes – https://code.google.com/p/slowaes/
- XlsxWriter – https://github.com/jmcnamara/XlsxWriter/

È possibile scaricare Recon-ng clonando il repo git:

```
git clone https: [email protected] /LaNMaSteR53/recon-ng.git
```

E entrando nella directory eseguendo il comando di installazione tramite pip

```
pip install -r REQUIREMENTS
```

[fonte]