Recon-ng Reference

Automate your Intelligence Collection

Recon-ng Reference

Automate your Intelligence Collection

A Guide by Striker Security
https://strikersecurity.com

Last updated 09/22/2016

Recon-ng is an incredible tool for automating OSINT collection, but its power comes with complexity. Modules offer their own capabilities and options, and knowing what they all do takes many long hours of practice. This reference book helps you navigate the power at your fingertips without endlessly guessing at what modules do and constantly typing "show info." The module descriptions below are all extracted directly from recon-ng's source code, so you know they're straight from the source.

If you don't know how to use Recon-ng, or want a refresher, check out Striker Security's tutorial at:
https://strikersecurity.com/blog/getting-started-recon-ng-tutorial/.

You can also take a look at recon-ng itself here:
https://bitbucket.org/LaNMaSteR53/recon-ng

As always, you can get in touch with me directly with an email to dakota@strikersecurity.com with any questions or comments. I always love hearing what you want to see next.

Happy hunting!

Dakota

Contents

Discovery

DNS Cache Snooper

Module name: cache_snoop
Categories: *discovery, info_disclosure*
Author(s): *thrapt (thrapt@gmail.com)*

Uses the DNS cache snooping technique to check for visited domains

Interesting File Finder

Module name: interesting_files
Categories: *discovery, info_disclosure*
Author(s): *Tim Tomes (@LaNMaSteR53), thrapt (thrapt@gmail.com), Jay Turla (@shipcod3), and Mark Jeffery*

Checks hosts for interesting files in predictable locations.

Exploitation

Xpath Injection Brute Forcer

Module name: xpath_bruter
Categories: *exploitation, injection*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Exploits XPath injection flaws to enumerate the contents of serverside XML documents.

Remote Command Injection Shell Interface

Module name: command_injector
Categories: *exploitation, injection*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Provides a shell interface for remote command injection flaws in web applications.

Recon

DNS Public Suffix Brute Forcer

Module name: brute_suffix
Categories: *recon, domains-domains*
Author(s): *Marcus Watson (@BranMacMuffin)*

Brute forces TLDs and SLDs using DNS. Updates the 'domains' table with the results.

Ports to Hosts Data Migrator

Module name: migrate_ports
Categories: *recon, ports-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Adds a new host for all the hostnames stored in the 'ports' table.

Hosts to Domains Data Migrator

Module name: migrate_hosts
Categories: *recon, hosts-domains*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Adds a new domain for all the hostnames stored in the 'hosts' table.

LinkedIn Authenticated Contact Enumerator

Module name: linkedin_auth
Categories: *recon, companies-contacts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Harvests contacts from the LinkedIn.com API using an authenticated connections network. Updates the 'contacts' table with the results.

Bing Cache Linkedin Profile and Contact Harvester

Module name: bing_linkedin_cache
Categories: *recon, companies-contacts*

Author(s): *Joe Black (@MyChickenNinja) and @fullmetalcache*

Harvests profiles from LinkedIn by querying the Bing API cache for LinkedIn pages related to the given companies, and adds them to the 'profiles' table. The module will then parse the resulting information to extract the user's full name and job title (title parsing is a bit spotty currently). The user's full name and title are then added to the 'contacts' table. This module does not access LinkedIn at any time.

Indeed Resume Crawl

Module name: indeed
Categories: *recon, companies-contacts*
Author(s): *Tyler Rosonke (tyler@zonksec.com)*

Crawls Indeed.com for contacts and resumes. Adds name, title, and location to the contacts table and a link to the resume in the profiles table. Can only harvest the first 1,000 results. Result set changes, so running the same crawl mutiple times can produce new contacts. If the PAST_EMPS option is set to true, the module will crawl both current and past employees. Given a keyword, the module will only harvest contacts whose resumes contain the keyword. (e.g. Linux Admin)

Jigsaw - Single Contact Retriever

Module name: purchase_contact
Categories: *recon, companies-contacts, jigsaw*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Retrieves a single complete contact from the Jigsaw.com API using points from the given account.

Jigsaw - Point Usage Statistics Fetcher

Module name: point_usage
Categories: *recon, companies-contacts, jigsaw*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Queries the Jigsaw API for the point usage statistics of the given account.

Jigsaw Contact Enumerator

Module name: search_contacts
Categories: *recon, companies-contacts, jigsaw*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Harvests contacts from the Jigsaw.com API. Updates the 'contacts' table with the results.

Twitter Handles

Module name: twitter
Categories: *recon, profiles-profiles*
Author(s): *Robert Frost (@frosty_1313, frosty[at]unluckyfrosty.net)*

Searches Twitter for users that mentioned, or were mentioned by, the given handle.

OSINT HUMINT Profile Collector

Module name: profiler
Categories: *recon, profiles-profiles*
Author(s): *Micah Hoffman (@WebBreacher)*

Takes each username from the profiles table and searches a variety of web sites for those users. The list of valid sites comes from the parent project at https://github.com/WebBreacher/WhatsMyName

NameChk.com Username Validator

Module name: namechk
Categories: *recon, profiles-profiles*
Author(s): *Tim Tomes (@LaNMaSteR53) and thrapt (thrapt@gmail.com)*

Leverages NameChk.com to validate the existance of usernames on specific web sites and updates the 'profiles' table with the results.

Hashes.org Hash Lookup

Module name: hashes_org
Categories: *recon, credentials-credentials*

Author(s): *Tim Tomes (@LaNMaSteR53) and Mike Lisi (@MikeCodesThings)*

Uses the Hashes.org API to perform a reverse hash lookup. Updates the 'credentials' table with the positive results.

PyBozoCrack Hash Lookup

Module name: bozocrack
Categories: *recon, credentials-credentials*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Searches Google for the value of a hash and tests for a match by hashing every word in the resulting page using all hashing algorithms supported by the 'hashlib' library. Updates the 'credentials' table with the positive results.

Adobe Hash Cracker

Module name: adobe
Categories: *recon, credentials-credentials*
Author(s): *Ethan Robish (@EthanRobish) and Tim Tomes (@LaNMaSteR53)*

Decrypts hashes leaked from the 2013 Adobe breach. First, the module cross references the leak ID to identify Adobe hashes in the 'password' column of the 'creds' table, moves the Adobe hashes to the 'hash' column, and changes the 'type' to 'Adobe'. Second, the module attempts to crack the hashes by comparing the ciphertext's decoded cipher blocks to a local block lookup table (BLOCK_DB) of known cipher block values. Finally, the module updates the 'creds' table with the results based on the level of success.

Shodan IP Enumerator

Module name: shodan_ip
Categories: *recon, hosts-ports*
Author(s): *Tim Tomes (@LaNMaSteR53) and Matt Pluckett (@t3lc0)*

Harvests port information from the Shodan API by using the 'ip' search operator. Updates the 'ports' table with the results.

Contact Name Mangler

Module name: mangle
Categories: *recon, contacts-contacts*

Author(s): *Tim Tomes (@LaNMaSteR53)*

Applies a mangle pattern to all of the contacts stored in the database, creating email addresses or usernames for each harvested contact. Updates the 'contacts' table with the results.

Contact Name Unmangler

Module name: unmangle
Categories: *recon, contacts-contacts*
Author(s): *Ethan Robish (@EthanRobish)*

Applies a regex or unmangle pattern to all of the contacts stored in the database, pulling out the individual name components. Updates the 'contacts' table with the results.

MailTester Email Validator

Module name: mailtester
Categories: *recon, contacts-contacts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Leverages MailTester.com to validate email addresses.

Github Code Enumerator

Module name: github_repos
Categories: *recon, profiles-repositories*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Uses the Github API to enumerate repositories and gists owned by a Github user. Updates the 'repositories' table with the results.

Meta Data Extractor

Module name: metacrawler
Categories: *recon, domains-contacts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Searches for files associated with the provided domain(s) and extracts any contact related metadata.

Whois POC Harvester

Module name: whois_pocs
Categories: *recon, domains-contacts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the 'contacts' table with the results.

PGP Key Owner Lookup

Module name: pgp_search
Categories: *recon, domains-contacts*
Author(s): *Robert Frost (@frosty_1313, frosty[at]unluckyfrosty.net)*

Searches the MIT public PGP key server for email addresses of the given domain. Updates the 'contacts' table with the results.

Reverse Geocoder

Module name: reverse_geocode
Categories: *recon, locations-locations*
Author(s): *Quentin Kaiser (contact@quentinkaiser.be)*

Queries the Google Maps API to obtain an address from coordinates.

Address Geocoder

Module name: geocode
Categories: *recon, locations-locations*
Author(s): *Quentin Kaiser (contact@quentinkaiser.be)*

Queries the Google Maps API to obtain coordinates for an address. Updates the 'locations' table with the results.

Github Profile Harvester

Module name: github_users
Categories: *recon, profiles-contacts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Uses the Github API to gather user info from harvested profiles. Updates the 'contacts' table with the results.

Dev Diver Repository Activity Examiner

Module name: dev_diver
Categories: *recon, profiles-contacts*
Author(s): *Micah Hoffman (@WebBreacher)*

Searches public code repositories for information about a given username.

IPInfoDB GeoIP

Module name: ipinfodb
Categories: *recon, hosts-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Leverages the ipinfodb.com API to geolocate a host by IP address. Updates the 'hosts' table with the results.

Hostname Resolver

Module name: resolve
Categories: *recon, hosts-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Resolves the IP address for a host. Updates the 'hosts' table with the results.

Bing API IP Neighbor Enumerator

Module name: bing_ip
Categories: *recon, hosts-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Leverages the Bing API and "ip:" advanced search operator to enumerate other virtual hosts sharing the same IP address. Updates the 'hosts' table with the results.

Reverse Resolver

Module name: reverse_resolve
Categories: *recon, hosts-hosts*
Author(s): *John Babio (@3vi1john), @vulp1n3, and Tim Tomes (@LaNMaSteR53)*

Conducts a reverse lookup for each IP address to resolve the hostname. Updates the 'hosts' table with the results.

FreeGeoIP

Module name: freegeoip
Categories: *recon, hosts-hosts*
Author(s): *Gerrit Helm (G) and Tim Tomes (@LaNMaSteR53)*

Leverages the freegeoip.net API to geolocate a host by IP address. Updates the 'hosts' table with the results.

SSLTools.com Host Name Lookups

Module name: ssltools
Categories: *recon, hosts-hosts*
Author(s): *Tim Maletic (borrowing from the ssl_san module by Zach Graces)*

Uses the ssltools.com site to obtain host names from a site's SSL certificate metadata to update the 'hosts' table. Security issues with the certificate trust are pushed to the 'vulnerabilities' table.

Flickr Geolocation Search

Module name: flickr
Categories: *recon, locations-pushpins*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Searches Flickr for media in the specified proximity to a location.

Instagram Geolocation Search

Module name: instagram
Categories: *recon, locations-pushpins*

Author(s): *Nathan Malcolm (@SintheticLabs) and Tim Tomes (@LaNMaSteR53)*

Searches Instagram for media in the specified proximity to a location.

Twitter Geolocation Search

Module name: twitter
Categories: *recon, locations-pushpins*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Searches Twitter for media in the specified proximity to a location.

Shodan Geolocation Search

Module name: shodan
Categories: *recon, locations-pushpins*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Searches Shodan for media in the specified proximity to a location.

Picasa Geolocation Search

Module name: picasa
Categories: *recon, locations-pushpins*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Searches Picasa for media in the specified proximity to a location.

YouTube Geolocation Search

Module name: youtube
Categories: *recon, locations-pushpins*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Searches the YouTube API for media in the specified proximity to a location.

Reverse Resolver

Module name: reverse_resolve
Categories: *recon, netblocks-hosts*

Author(s): *John Babio (@3vi1john)*

Conducts a reverse lookup for each of a netblock's IP addresses to resolve the hostname. Updates the 'hosts' table with the results.

Shodan Network Enumerator

Module name: shodan_net
Categories: *recon, netblocks-hosts*
Author(s): *Mike Siegel and Tim Tomes (@LaNMaSteR53)*

Harvests hosts from the Shodan API by using the 'net' search operator. Updates the 'hosts' table with the results.

PwnedList - Account Credentials Fetcher

Module name: account_creds
Categories: *recon, domains-credentials, pwnedlist*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Queries the PwnedList API for credentials associated with the given usernames. Updates the 'credentials' table with the results.

PwnedList - Leak Details Fetcher

Module name: leak_lookup
Categories: *recon, domains-credentials, pwnedlist*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Queries the local database for information associated with a leak ID. The 'leaks_dump' module must be used to populate the local database before this module will execute successfully.

PwnedList - Pwned Domain Credentials Fetcher

Module name: domain_creds
Categories: *recon, domains-credentials, pwnedlist*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Queries the PwnedList API to fetch all credentials for a domain. Updates the 'credentials' table with the results.

PwnedList - Leak Details Retriever

Module name: leaks_dump
Categories: *recon, domains-credentials, pwnedlist*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Queries the PwnedList API for information associated with all known leaks. Updates the 'leaks' table with the results.

PwnedList - Pwned Domain Statistics Fetcher

Module name: domain_ispwned
Categories: *recon, domains-credentials, pwnedlist*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Queries the PwnedList API for a domain to determine if any associated credentials have been compromised. This module does NOT return any credentials, only a total number of compromised credentials.

PwnedList - API Usage Statistics Fetcher

Module name: api_usage
Categories: *recon, domains-credentials, pwnedlist*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Queries the PwnedList API for account usage statistics.

Whois Company Harvester

Module name: whois_orgs
Categories: *recon, netblocks-companies*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Uses the ARIN Whois RWS to harvest Companies data from whois queries for the given netblock. Updates the 'companies' table with the results.

FullContact Contact Enumerator

Module name: fullcontact
Categories: *recon, contacts-profiles*
Author(s): *Quentin Kaiser (@qkaiser, contact[at]quentinkaiser.be) and Tim*

Tomes (@LaNMaSteR53)

Harvests contact information and profiles from the fullcontact.com API using email addresses as input. Updates the 'contacts' and 'profiles' tables with the results.

Bing Hostname Enumerator

Module name: bing_domain_web
Categories: *recon, domains-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Harvests hosts from Bing.com by using the 'site' search operator. Updates the 'hosts' table with the results.

Shodan Hostname Enumerator

Module name: shodan_hostname
Categories: *recon, domains-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Harvests hosts from the Shodan API by using the 'hostname' search operator. Updates the 'hosts' table with the results.

BuiltWith Enumerator

Module name: builtwith
Categories: *recon, domains-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Leverages the BuiltWith API to identify hosts, technologies, and contacts associated with a domain.

HackerTarget Lookup

Module name: hackertarget
Categories: *recon, domains-hosts*
Author(s): *Michael Henriksen (@michenriksen)*

Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Bing API Hostname Enumerator

Module name: bing_domain_api
Categories: *recon, domains-hosts*
Author(s): *Marcus Watson (@BranMacMuffin)*

Leverages the Bing API and "domain:" advanced search operator to harvest hosts. Updates the 'hosts' table with the results.

Netcraft Hostname Enumerator

Module name: netcraft
Categories: *recon, domains-hosts*
Author(s): *thrapt (thrapt@gmail.com)*

Harvests hosts from Netcraft.com. Updates the 'hosts' table with the results.

DNS Hostname Brute Forcer

Module name: brute_hosts
Categories: *recon, domains-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Brute forces host names using DNS. Updates the 'hosts' table with the results.

ThreatCrowd DNS lookup

Module name: threatcrowd
Categories: *recon, domains-hosts*
Author(s): *mike2dot0*

Leverages the ThreatCrowd passive DNS API to discover hosts/subdomains.

VPNHunter Lookup

Module name: vpnhunter
Categories: *recon, domains-hosts*
Author(s): *Quentin Kaiser (contact[at]quentinkaiser.be)*

Checks vpnhunter.com for SSL VPNs, remote accesses, email portals and generic login sites. Updates the 'hosts' table with the results.

Google CSE Hostname Enumerator

Module name: google_site_api
Categories: *recon, domains-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Leverages the Google Custom Search Engine API to harvest hosts using the 'site' search operator. Updates the 'hosts' table with the results.

Google Hostname Enumerator

Module name: google_site_web
Categories: *recon, domains-hosts*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.

SSL SAN Lookup

Module name: ssl_san
Categories: *recon, domains-hosts*
Author(s): *Zach Grace (@ztgrace) zgrace@403labs.com*

Uses the ssltools.com site to obtain the Subject Alternative Names for a domain. Updates the 'hosts' table with the results.

PunkSPIDER Vulnerabilty Finder

Module name: punkspider
Categories: *recon, domains-vulnerabilities*
Author(s): *Tim Tomes (@LaNMaSteR53) and thrapt (thrapt@gmail.com)*

Leverages the PunkSPIDER API to search for previosuly discovered vulnerabltiies on hosts within a domain.

Google Hacking Database

Module name: ghdb
Categories: *recon, domains-vulnerabilities*

Author(s): *Tim Tomes (@LaNMaSteR53)*

Searches for possible vulnerabilites in a domain by leveraging the Google Hacking Database (GHDB) and the 'site' search operator. Updates the 'vulnerabilities' table with the results.

XSSed Domain Lookup

Module name: xssed
Categories: *recon, domains-vulnerabilities*
Author(s): *Micah Hoffman (@WebBreacher)*

Checks XSSed.com for XSS records associated with a domain and displays the first 20 results.

XSSposed Domain Lookup

Module name: xssposed
Categories: *recon, domains-vulnerabilities*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Checks XSSposed.com for XSS records associated with a domain.

Have I been pwned? Breach Search

Module name: hibp_breach
Categories: *recon, contacts-credentials*
Author(s): *Tim Tomes (@LaNMaSteR53) & Tyler Halfpop (@tylerhalfpop)*

Leverages the haveibeenpwned.com API to determine if email addresses are associated with breached credentials. Adds compromised email addresses to the 'credentials' table.

Have I been pwned? Paste Search

Module name: hibp_paste
Categories: *recon, contacts-credentials*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Leverages the haveibeenpwned.com API to determine if email addresses have been published to various paste sites. Adds compromised email addresses to the 'credentials' table.

Whois Data Miner

Module name: whois_miner
Categories: *recon, companies-multi*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Uses the ARIN Whois RWS to harvest companies, locations, netblocks, and contacts associated with the given company search string. Updates the respective tables with the results.

Github Resource Miner

Module name: github_miner
Categories: *recon, companies-multi*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Uses the Github API to enumerate repositories and member profiles associated with a company search string. Updates the respective tables with the results.

Internet Census 2012 Lookup

Module name: census_2012
Categories: *recon, netblocks-ports*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Queries the Internet Census 2012 data through Exfiltrated.com to enumerate open ports for a netblock.

censys.io port lookup by netblock

Module name: censysio
Categories: *recon, netblocks-ports*
Author(s): *John Askew (https://bitbucket.org/skew)*

Queries censys.io to enumerate open ports for a netblock.

Hosts to Locations Data Migrator

Module name: migrate_hosts
Categories: *recon, hosts-locations*

Author(s): *Tim Tomes (@LaNMaSteR53)*

Adds a new location for all the locations stored in the 'hosts' table.

Github Gist Searcher

Module name: gists_search
Categories: *recon, repositories-vulnerabilities*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Uses the Github API to download and search Gists for possible information disclosures. Updates the 'vulnerabilities' table with the results.

Github Dork Analyzer

Module name: github_dorks
Categories: *recon, repositories-vulnerabilities*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Uses the Github API to search for possible vulnerabilites in source code by leveraging Github Dorks and the 'repo' search operator. Updates the 'vulnerabilities' table with the results.

Github Commit Searcher

Module name: github_commits
Categories: *recon, repositories-profiles*
Author(s): *Michael Henriksen (@michenriksen)*

Uses the Github API to gather user profiles from repository commits. Updates the 'profiles' table with the results.

Contacts to Domains Data Migrator

Module name: migrate_contacts
Categories: *recon, contacts-domains*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Adds a new domain for all the hostnames associated with email addresses stored in the 'contacts' table.

Reporting

XML Report Generator

Module name: xml
Categories: *reporting*
Author(s): *Eric Humphries (@e2fsck) and Tim Tomes (@LaNMaSteR53)*

Creates a XML report.

HTML Report Generator

Module name: html
Categories: *reporting*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Creates a HTML report.

PushPin Report Generator

Module name: pushpin
Categories: *reporting*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Creates HTML media and map reports for all of the PushPins stored in the database.

List Creator

Module name: list
Categories: *reporting*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Creates a file containing a list of records from the database.

JSON Report Generator

Module name: json
Categories: *reporting*
Author(s): *Paul (@PaulWebSec)*

Creates a JSON report.

CSV File Creator

Module name: csv
Categories: *reporting*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Creates a CSV file containing the specified harvested data.

XLSX File Creator

Module name: xlsx
Categories: *reporting*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Creates an Excel compatible XLSX file containing the entire data set.

Import

Advanced CSV File Importer

Module name: csv_file
Categories: *import*
Author(s): *Ethan Robish (@EthanRobish)*

Imports values from a CSV file into a database table.

List File Importer

Module name: list
Categories: *import*
Author(s): *Tim Tomes (@LaNMaSteR53)*

Imports values from a list file into a database table and column.