autorecon

AutoRecon is a multi-threaded network reconnaissance tool which performs automated enumeration of services. It is intended as a time-saving tool for use in CTFs and other penetration testing environments (e.g. OSCP). It may also be useful in real-world engagements.

Installed size: 1.24 MB

How to install: sudo apt install autorecon

Dependencies:

- curl
- dirb
- dirsearch
- dnsrecon
- enum4linux
- enum4linux-ng
- ffuf
- gobuster
- impacket-scripts
- nbtscan
- nikto
- nmap
- onesixtyone
- oscanner
- python3
- python3-colorama
- python3-impacket
- python3-platformdirs
- python3-psutil
- python3-requests
- python3-toml
- python3-unidecode

- redis-tools
- seclists
- sipvicious
- smbclient
- smbmap
- snmp
- sslscan
- tnscmd10g
- whatweb

```
root@kali:~# autorecon -h
usage: autorecon [-t TARGET_FILE] [-p PORTS] [-m MAX_SCANS]
                 [-mp MAX_PORT_SCANS] [-c CONFIG_FILE] [-g GLOBAL_FILE]
                 [--tags TAGS] [--exclude-tags TAGS] [--port-scans PLUGINS]
                 [--service-scans PLUGINS] [--reports PLUGINS]
                 [--plugins-dir PLUGINS_DIR] [--add-plugins-dir PLUGINS_DIR]
                 [-l [TYPE]] [-o OUTPUT] [--single-target] [--only-scans-dir]
                 [--no-port-dirs] [--heartbeat HEARTBEAT] [--timeout TIMEOUT]
                 [--target-timeout TARGET_TIMEOUT] [--nmap NMAP |
                 --nmap-append NMAP_APPEND] [--proxychains]
                 [--disable-sanity-checks] [--disable-keyboard-control]
                 [--ignore-plugin-checks]
                 [--force-services SERVICE [SERVICE ...]]
                 [-mpti PLUGIN:NUMBER [PLUGIN:NUMBER ...]]
                 [-mpgi PLUGIN:NUMBER [PLUGIN:NUMBER ...]] [--accessible] [-v]
                 [--version] [--curl.path VALUE]
                 [--dirbuster.tool {feroxbuster,gobuster,dirsearch,ffuf,dirb}]
                 [--dirbuster.wordlist VALUE [VALUE ...]]
```

[--dirbuster.threads VALUE] [--dirbuster.ext VALUE]
[--dirbuster.recursive] [--dirbuster.extras VALUE]
[--enum4linux.tool {enum4linux-ng,enum4linux}]
[--onesixtyone.community-strings VALUE]
[--subdomain-enum.domain VALUE]
[--subdomain-enum.wordlist VALUE [VALUE ...]]
[--subdomain-enum.threads VALUE]
[--vhost-enum.hostname VALUE]
[--vhost-enum.wordlist VALUE [VALUE ...]]
[--vhost-enum.threads VALUE] [--wpscan.api-token VALUE]
[--global.username-wordlist VALUE]
[--global.password-wordlist VALUE] [--global.domain VALUE]
[-h]
[targets ...]

Network reconnaissance tool to port scan and automatically enumerate services found on multiple targets.

positional arguments:
targets IP addresses (e.g. 10.0.0.1), CIDR notation (e.g. 10.0.0.1/24), or resolvable hostnames (e.g. foo.bar) to scan.

options:
-t, --target-file TARGET_FILE
Read targets from file.

-p, --ports PORTS Comma separated list of ports / port ranges to scan.
Specify TCP/UDP ports by prepending list with T:/U: To
scan both TCP/UDP, put port(s) at start or specify B:
e.g. 53,T:21-25,80,U:123,B:123. Default: None

-m, --max-scans MAX_SCANS
The maximum number of concurrent scans to run.
Default: 50

-mp, --max-port-scans MAX_PORT_SCANS
The maximum number of concurrent port scans to run.
Default: 10 (approx 20% of max-scans unless specified)

-c, --config CONFIG_FILE
Location of AutoRecon's config file. Default:
/root/.config/AutoRecon/config.toml

-g, --global-file GLOBAL_FILE
Location of AutoRecon's global file. Default:
/root/.config/AutoRecon/global.toml

--tags TAGS Tags to determine which plugins should be included.
Separate tags by a plus symbol (+) to group tags
together. Separate groups with a comma (,) to create
multiple groups. For a plugin to be included, it must
have all the tags specified in at least one group.
Default: default

--exclude-tags TAGS Tags to determine which plugins should be excluded.
Separate tags by a plus symbol (+) to group tags
together. Separate groups with a comma (,) to create
multiple groups. For a plugin to be excluded, it must

```
                have all the tags specified in at least one group.
                Default: None
--port-scans PLUGINS  Override --tags / --exclude-tags for the listed
                PortScan plugins (comma separated). Default: None
--service-scans PLUGINS
                Override --tags / --exclude-tags for the listed
                ServiceScan plugins (comma separated). Default: None
--reports PLUGINS    Override --tags / --exclude-tags for the listed Report
                plugins (comma separated). Default: None
--plugins-dir PLUGINS_DIR
                The location of the plugins directory. Default:
                /root/.local/share/AutoRecon/plugins
--add-plugins-dir PLUGINS_DIR
                The location of an additional plugins directory to add
                to the main one. Default: None
-l, --list [TYPE]    List all plugins or plugins of a specific type. e.g.
                --list, --list port, --list service
-o, --output OUTPUT   The output directory for results. Default: results
--single-target      Only scan a single target. A directory named after the
                target will not be created. Instead, the directory
                structure will be created within the output directory.
                Default: False
--only-scans-dir     Only create the "scans" directory for results. Other
                directories (e.g. exploit, loot, report) will not be
                created. Default: False
--no-port-dirs       Don't create directories for ports (e.g. scans/tcp80,
```

scans/udp53). Instead store all results in the "scans"
directory itself. Default: False

--heartbeat HEARTBEAT
Specifies the heartbeat interval (in seconds) for scan
status messages. Default: 60

--timeout TIMEOUT Specifies the maximum amount of time in minutes that
AutoRecon should run for. Default: None

--target-timeout TARGET_TIMEOUT
Specifies the maximum amount of time in minutes that a
target should be scanned for before abandoning it and
moving on. Default: None

--nmap NMAP Override the {nmap_extra} variable in scans. Default:
-vv --reason -Pn -T4

--nmap-append NMAP_APPEND
Append to the default {nmap_extra} variable in scans.
Default:

--proxychains Use if you are running AutoRecon via proxychains.
Default: False

--disable-sanity-checks
Disable sanity checks that would otherwise prevent the
scans from running. Default: False

--disable-keyboard-control
Disables keyboard control ([s]tatus, Up, Down) if you
are in SSH or Docker.

--ignore-plugin-checks
Ignores errors from plugin check functions that would

```
                        otherwise prevent AutoRecon from running. Default:
                        False
  --force-services SERVICE [SERVICE ...]
                        A space separated list of services in the following
                        style: tcp/80/http tcp/443/https/secure
  -mpti, --max-plugin-target-instances PLUGIN:NUMBER [PLUGIN:NUMBER ...]
                        A space separated list of plugin slugs with the max
                        number of instances (per target) in the following
                        style: nmap-http:2 dirbuster:1. Default: None
  -mpgi, --max-plugin-global-instances PLUGIN:NUMBER [PLUGIN:NUMBER ...]
                        A space separated list of plugin slugs with the max
                        number of global instances in the following style:
                        nmap-http:2 dirbuster:1. Default: None
  --accessible          Attempts to make AutoRecon output more accessible to
                        screenreaders. Default: False
  -v, --verbose         Enable verbose output. Repeat for more verbosity.
  --version             Prints the AutoRecon version and exits.
  -h, --help            Show this help message and exit.

plugin arguments:
  These are optional arguments for certain plugins.

  --curl.path VALUE     The path on the web server to curl. Default: /
  --dirbuster.tool {feroxbuster,gobuster,dirsearch,ffuf,dirb}
                        The tool to use for directory busting. Default:
                        feroxbuster
```

--dirbuster.wordlist VALUE [VALUE ...]

The wordlist(s) to use when directory busting. Separate multiple wordlists with spaces. Default: ['/root/.local/share/AutoRecon/wordlists/dirbuster.txt']

--dirbuster.threads VALUE

The number of threads to use when directory busting. Default: 10

--dirbuster.ext VALUE

The extensions you wish to fuzz (no dot, comma separated). Default: txt,html,php,asp,aspx,jsp

--dirbuster.recursive

Enables recursive searching (where available). Warning: This may cause significant increases to scan times. Default: False

--dirbuster.extras VALUE

Any extra options you wish to pass to the tool when it runs. e.g. --dirbuster.extras='-s 200,301 --discover-backup'

--enum4linux.tool {enum4linux-ng,enum4linux}

The tool to use for doing Windows and Samba enumeration. Default: enum4linux-ng

--onesixtyone.community-strings VALUE

The file containing a list of community strings to try. Default: /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings-onesixtyone.txt

--subdomain-enum.domain VALUE

The domain to use as the base domain (e.g. example.com) for subdomain enumeration. Default: None

--subdomain-enum.wordlist VALUE [VALUE ...]

The wordlist(s) to use when enumerating subdomains. Separate multiple wordlists with spaces. Default: ['/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt']

--subdomain-enum.threads VALUE

The number of threads to use when enumerating subdomains. Default: 10

--vhost-enum.hostname VALUE

The hostname to use as the base host (e.g. example.com) for virtual host enumeration. Default: None

--vhost-enum.wordlist VALUE [VALUE ...]

The wordlist(s) to use when enumerating virtual hosts. Separate multiple wordlists with spaces. Default: ['/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt']

--vhost-enum.threads VALUE

The number of threads to use when enumerating virtual hosts. Default: 10

--wpscan.api-token VALUE

An API Token from wpvulndb.com to help search for more vulnerabilities.

global plugin arguments:

These are optional arguments that can be used by all plugins.

--global.username-wordlist VALUE

A wordlist of usernames, useful for bruteforcing.

Default: /usr/share/seclists/Usernames/top-usernames-shortlist.txt

--global.password-wordlist VALUE

A wordlist of passwords, useful for bruteforcing.

Default: /usr/share/seclists/Passwords/darkweb2017-top100.txt

--global.domain VALUE

The domain to use (if known). Used for DNS and/or Active Directory. Default: None