enum4linux-ng

Next generation version of enum4linux (a Windows/Samba enumeration tool) with additional features like JSON/YAML export. Aimed for security professionals and CTF players.

Installed size: 173 KB

How to install: sudo apt install enum4linux-ng

Dependencies:

- python3
- python3-impacket
- python3-ldap3
- python3-yaml
- samba-common-bin
- smbclient

```
root@kali:~# enum4linux-ng -h

ENUM4LINUX - next generation (v1.3.5)


usage: enum4linux-ng [-h] [-A] [-As] [-U] [-G] [-Gm] [-S] [-C] [-P] [-O] [-L]

            [-I] [-R [BULK_SIZE]] [-N] [-w DOMAIN] [-u USER] [-p PW |

            -K TICKET_FILE | -H NTHASH] [--local-auth] [-d]

            [-k USERS] [-r RANGES] [-s SHARES_FILE] [-t TIMEOUT] [-v]

            [--keep] [-oJ OUT_JSON_FILE | -oY OUT_YAML_FILE |

            -oA OUT_FILE]

            host
```

```
This tool is a rewrite of Mark Lowe's enum4linux.pl, a tool for enumerating
information from Windows and Samba systems. It is mainly a wrapper around the
Samba tools nmblookup, net, rpcclient and smbclient. Other than the original
tool it allows to export enumeration results as YAML or JSON file, so that it
can be further processed with other tools. The tool tries to do a 'smart'
enumeration. It first checks whether SMB or LDAP is accessible on the target.
Depending on the result of this check, it will dynamically skip checks (e.g.
LDAP checks if LDAP is not running). If SMB is accessible, it will always
check whether a session can be set up or not. If no session can be set up, the
tool will stop enumeration. The enumeration process can be interupted with
CTRL+C. If the options -oJ or -oY are provided, the tool will write out the
current enumeration state to the JSON or YAML file, once it receives SIGINT
triggered by CTRL+C. The tool was made for security professionals and CTF
players. Illegal use is prohibited.

positional arguments:
  host

options:
  -h, --help       show this help message and exit
  -A               Do all simple enumeration including nmblookup (-U -G -S
                   -P -O -N -I -L). This option is enabled if you don't
                   provide any other option.
  -As              Do all simple short enumeration without NetBIOS names
                   lookup (-U -G -S -P -O -I -L)
```

```
-U            Get users via RPC

-G            Get groups via RPC

-Gm           Get groups with group members via RPC

-S            Get shares via RPC

-C            Get services via RPC

-P            Get password policy information via RPC

-O            Get OS information via RPC

-L            Get additional domain info via LDAP/LDAPS (for DCs only)

-I            Get printer information via RPC

-R [BULK_SIZE]    Enumerate users via RID cycling. Optionally, specifies

            lookup request size.

-N            Do an NetBIOS names lookup (similar to nbtstat) and try

            to retrieve workgroup from output

-w DOMAIN       Specify workgroup/domain manually (usually found

            automatically)

-u USER         Specify username to use (default "")

-p PW           Specify password to use (default "")

-K TICKET_FILE    Try to authenticate with Kerberos, only useful in Active

            Directory environment (Note: DNS must be setup correctly

            for this option to work

-H NTHASH       Try to authenticate with hash

--local-auth     Authenticate locally to target

-d            Get detailed information for users and groups, applies to

            -U, -G and -R

-k USERS        User(s) that exists on remote system (default:

            administrator,guest,krbtgt,domain admins,root,bin,none).
            Used to get sid with "lookupsids"
-r RANGES       RID ranges to enumerate (default: 500-550,1000-1050)
-s SHARES_FILE    Brute force guessing for shares
-t TIMEOUT      Sets connection timeout in seconds (default: 5s)
-v              Verbose, show full samba tools commands being run (net,
            rpcclient, etc.)
--keep          Don't delete the Samba configuration file created during
            tool run after enumeration (useful with -v)
-oJ OUT_JSON_FILE  Writes output to JSON file (extension is added
            automatically)
-oY OUT_YAML_FILE  Writes output to YAML file (extension is added
            automatically)
-oA OUT_FILE      Writes output to YAML and JSON file (extensions are added
            automatically)
```