

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~
$ enum4linux -u
Could not find command-not-found database. Run 'sudo apt update' to populate it.
enum: command not found
kali@kali: ~
$ enum4linux -h
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
-U get userlist
-M get machine list*
-S get sharelist
-P get password policy information
-G get group and member list
-d be detailed, applies to -U and -S
-u user specify username to use (default "")
-p pass specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -W, -D, -f

Additional options:
-a Do all simple enumeration (-U -S -G -P -R -o -n -i).
  This option is enabled if you don't provide any other options.
-h Display this help message and exit
-r enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n Keep searching RIDs until n consecutive RIDs don't correspond to
  a username. Implies RID range ends at 999999. Useful
  against DCs.
-l Get some (limited) info via LDAP 389/TCP (for DCs only)
-s file brute force guessing for share names
-k user User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins,root,bin,none)
  Used to get sid with "lookupsid known_username"
  the commas to try several users: "-A admin,user1,user2"
-o Get OS information
-i Get printer information
-w workgroup Specify workgroup manually (usually found automatically)
-n Do an nmblookup (similar to nbtstat)
-v Verbose. Shows full commands being run (net, rpcclient, etc.)
-A Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

kali@kali: ~
$ enum4linux -u
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
```

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali ~
File Actions Edit View Help
-o Get OS information
-i Get printer information
-w wrkg Specify workgroup manually (usually found automatically)
-n Do an nmblookup (similar to nbtstat)
-v Verbose. Shows full commands being run (net, rpcclient, etc.)
-A Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.

Dependancy info: You will need to have the samba package installed as this
script is basically just a wrapper around rpcclient, net, nmblookup and
smbclient. Polenum from http://labs.portcullis.co.uk/application/polenum/
is required to get Password Policy info.

[kali@kali]~$
$ enum4linux 192.168.1.1 -a
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue May 9 08:26:23 2023

( Target Information )
Target ..... 192.168.1.1
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

( Enumerating Workgroup/Domain on 192.168.1.1 )

[E] Can't find workgroup/domain

( Nbtstat Information for 192.168.1.1 )
Looking up status of 192.168.1.1
No reply from 192.168.1.1

( Session Check on 192.168.1.1 )

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
```