

Enum4Linux

Enum4linux is a tool for enumerating information from Windows and Samba systems and is capable of discovering the following:

- Password policies on target
- The operating system of a remote target
- Shares on a device (drives and folders)
- User listings
- Domain and group membership

Enum4linux is already installed on kali.

<https://tools.kali.org/information-gathering/enum4linux>

To run enum you need to execute the command like that:

```
sudo enum4linux -a <ip-address> | tee <outputfile>.log
```

With this command you export the results into the defined output file. Makes it easier to analyze. It takes some time to see all results ca. 5 minutes.

To see all possible actions you do: **enum4linux -h**

During the execution you will see everything what gets scanned:

```
root@kali:~# enum4linux -v 172.168.0.6
[V] Dependent program "nmblookup" found in /usr/bin/nmblookup
[V] Dependent program "net" found in /usr/bin/net
[V] Dependent program "rpcclient" found in /usr/bin/rpcclient
[V] Dependent program "smbclient" found in /usr/bin/smbclient
[V] Dependent program "polenum" found in /usr/bin/polenum
[V] Dependent program "ldapsearch" found in /usr/bin/ldapsearch
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application,
enum4linux/ ) on Thu Nov  1 18:37:11 2018

=====
|   Target Information   |
=====
Target ..... 172.168.0.6
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root,
```

Revision #2

Created 9 July 2022 13:28:05 by Togoboi

Updated 10 July 2022 08:23:32 by Togoboi