

# Enum4Linux

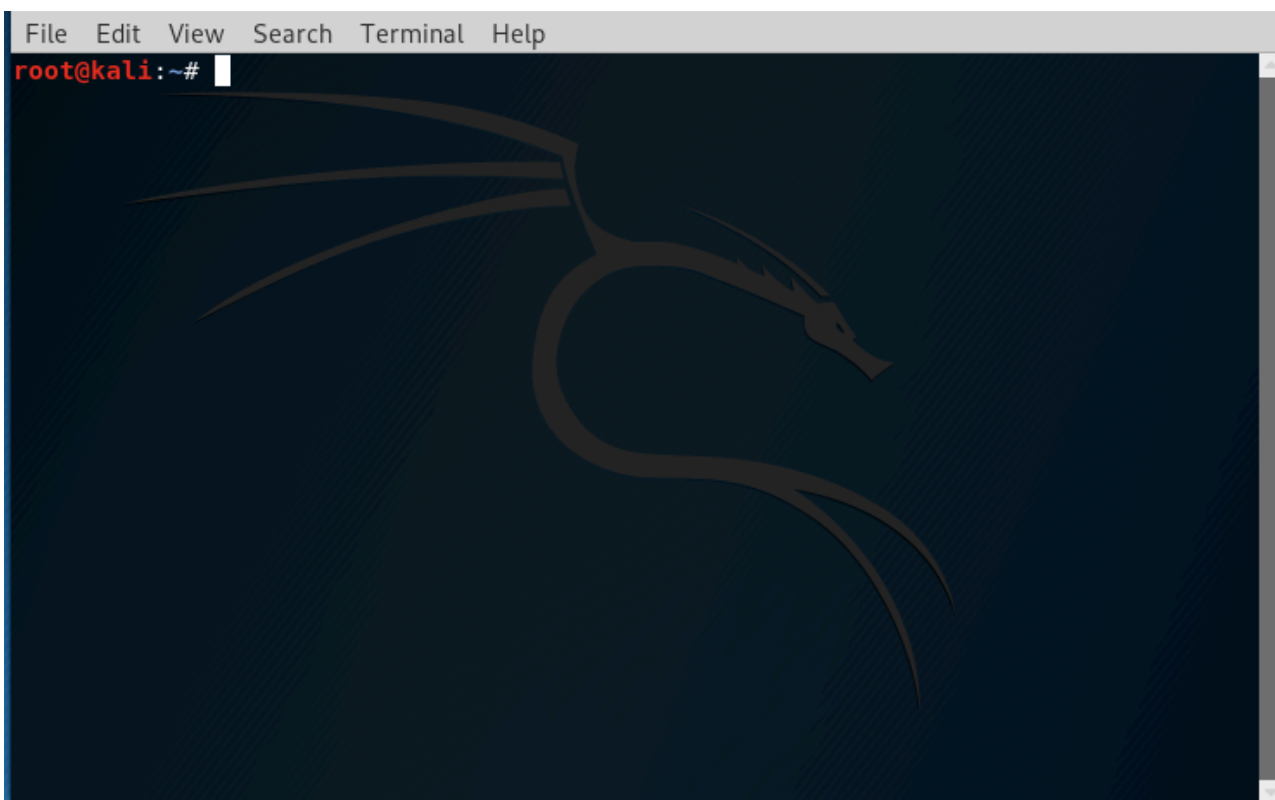
Monday, October 28, 2019

9:38 PM

## What is Enum4Linux?

Enum4Linux is a tool for enumerating information from Windows and Samba systems. It attempts to offer similar functionality to enum.exe formerly available from [www.bindview.com](http://www.bindview.com). It is written in Perl and is basically a wrapper around Samba tools smbclient, rpcclient, net and nmblookup.

1. Go to Kali Linux Terminal:



2. Type enum4linux:



```

root@kali:~# enum4linux
enum4linux v0.8.9 (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, -N, -D, -f

Additional options:
  -a      Do all simple enumeration (-U -S -G -P -r -o -n -i).

```

Read the list of options to decide what you would like to do.

3. Put in a command and see results:

```

root@kali:~# enum4linux -U -P -o -G 10.0.2.17

```

- U : means get userlist
- P : means get password policy information
- o : means get OS (operation system) information
- G : means get group & member list

Result:

```

root@kali:~# enum4linux -U -P -o -G 10.0.2.17
Starting enum4linux v0.8.9
( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Nov 2 16:27:55
2019

```



```
=====
```

```
| Target Information |
```

```
=====
```

```
Target ..... 10.0.2.17
```

```
RID Range ..... 500-550,1000-1050
```

```
Username ..... "
```

```
Password ..... "
```

```
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin,  
none
```

```
=====
```

```
| Enumerating Workgroup/Domain on 10.0.2.17 |
```

```
=====
```

```
[E] Can't find workgroup/domain
```

```
=====
```

```
| Session Check on 10.0.2.17 |
```

```
=====
```

```
Use of uninitialized value $global_workgroup in concatenation (.) or string  
at ./enum4linux.pl line 437.
```

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

```
root@kali:~#
```

## What is This Good For?

This is useful for building wordlists, checking possible credentials or even gaining a foothold on the system to sniff from.

