How to Use ENUM4LINUX on a Security Test

The **enum4linux** tool is a Linux/Kali tool designed to enumerate a Microsoft Windows computer gathering as much information as possible. The command line for **enum4linux** is as follows:

```
$ enum4linux
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
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 "")
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    -r        enumerate users via RID cycling
    -o        get operating systems information
```

By **enum4linux** HH will scan using no username and password. But if the username and password and know that we can make use of them with the -u and -p options. For Example, we can use **enum4linux** to enumerate users via RID cycling and enumerate users via the following command:

```
$ enum4linux -r -U 172.16.2.100
```

We can enumerate shares on a target machine via the following:

```
$ enum4linux -S 172.16.2.100
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
=======================(Share Enumeration on 172.16.2.100)=======================


        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        Data            Disk      The Data Folder
        Presentations   Disk      Corporate Presentations
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

[+] Attempting to map shares on 172.16.2.100

//172.16.2.100/IPC$       Mapping: OK Listing: DENIED Writing: N/A
//172.16.2.100/Data       Mapping: DENIED Listing: N/A Writing: N/A
//172.16.2.100/Presentations    Mapping: DENIED Listing: N/A Writing: N/A
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
enum4linux complete on Tue Jul 12 11:26:44 2022
```

We can enumerate the operating system of the target machine via the following:

```
$ enum4linux -o 172.16.2.100
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
[+] Got OS info for 172.16.2.100 from srvinfo:
        172.16.2.100   Wk Sv PDC Tim NT LMB
        platform_id     :       500
        os version      :       5.2
        server type     :       0x84102b
```