How to Use ENUM4LINUX-NG on a Security Test

The **enum4linux-ng** is the next generation version of **enum4linux**. It is available from https://github.com/cddmp/enum4linux-ng, and its usage is as follows:

```
$ ./enum4linux-ng.py
ENUM4LINUX - next generation

usage: enum4linux-ng.py [-h] [-A] [-As] [-U] [-G] [-Gm] [-S] [-C] [-P] [-O] [-L]
                        [-I] [-R] [-N] [-w DOMAIN] [-u USER] [-v] [--keep]
                        [-p PW | -K TICKET_FILE | -H NTHASH] [--local-auth] [-d]
                        [-k USERS] [-r RANGES] [-s SHARES_FILE] [-t TIMEOUT]
                        [-oJ OUT_JSON_FILE | -oY OUT_YAML_FILE | -oA OUT_FILE] host
enum4linux-ng.py: error: the following arguments are required: host
$
```

The options for **enum4linux-ng** are as follows

-U	Get users via RPC
-G	Get groups 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	Enumerate users via RID cycling
-Gm	Get groups with group members via RPC

We can use **enum4linux-ng** to identify the target's operating system

```
$ enum4linux-ng -O 172.16.2.100
. . . . . .
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[+] Found OS information via 'srvinfo'
[+] After merging OS information we have the following result:
OS: Windows Server 2003 3790
OS version: '5.2'
OS release: not supported
OS build: not supported
Native OS: Windows Server 2003 3790
Native LAN manager: Windows Server 2003 5.2
Platform id: '500'
Server type: '0x84102b'
Server type string: Wk Sv PDC Tim NT LMB
```

We can also use it to enumerate file shares exported by the target system.

```
$ enum4linux-ng -S 172.16.2.100
[*] Enumerating shares
[+] Found 7 share(s):
. . . . . .
Data:
  comment: The Data Folder
  type:    Disk
Presentations:
  comment: Corporate Presentations
  type:    Disk
```