

# Enum4linux

Enum4linux是一个从Windows和Samba系统中枚举信息的工具。他试图提供一个类似的功能。

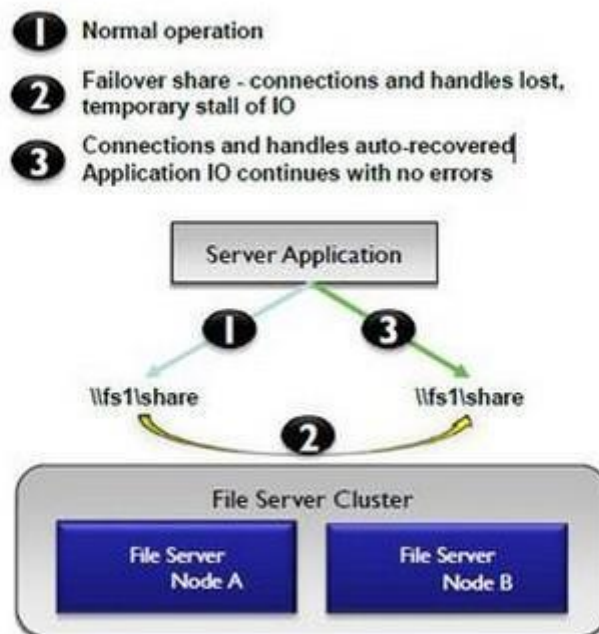
而Enum4linux是用Perl而编写的，基本上是一个围绕Samba工具smbclient,rpclient,net和nmblookup的包装器

—— Mark Lowe

---

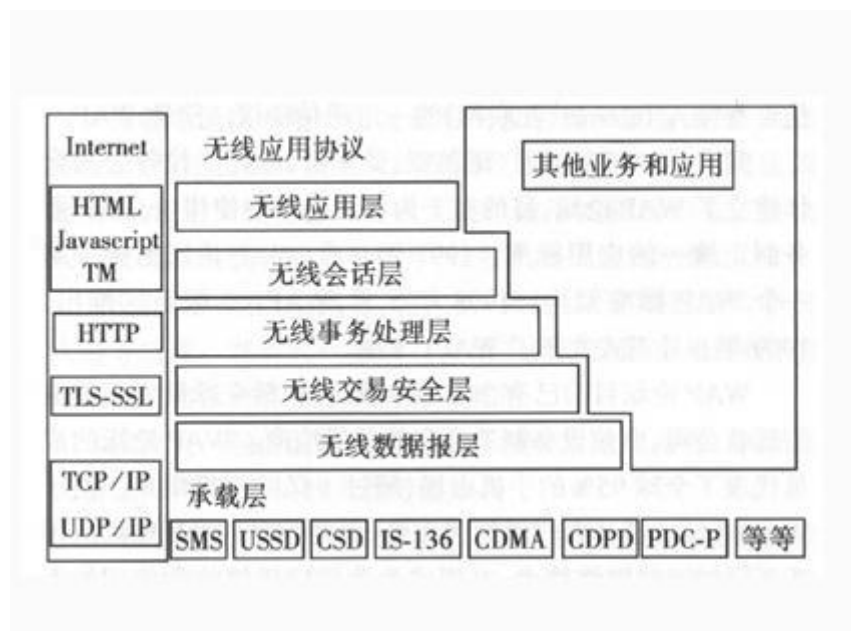
## 一，前期准备

### SMB



信息服务块（SMB，Server Message Block）是一种在局域网上共享文件和打印机的一种通信协议，它为不同局域网内 不同计算机提供文件及打印机等资源服务。

### WAP



无线应用协议（WAP，Wireless Application Protocol）主要在移动电话、个人数据主力（PDA）等移动设备与因特网或其他业务之间通信与开放性及全球性的标准，在1998年发布。

通过该协议，可以接收到各种信息，如浏览网页、收发电子邮件、

## Samba

Samba是SMB的一种实现方法，主要用于实现Linux系统的文件和打印服务，Linux用户通过配置使用Sambau可以实现与Windows用户的资源共享，守护进程smba和nmbd是samba的核心，全部时间内运行。Samba程序使得通过企图计算机可以浏览Linux服务器。

## RID

RID有多个意思，比如相对识别符，行标识符，要求标识符，记录标识，记录唯一标识符，资源标识符，远程标识符等。

## 安全标识符（SID，Security Identifiers）

在计算机中，通常使用SID来跟踪每个账户，这就使得在系统中。你不管如何更改帐号名称，系统都知道你使用的是管理帐号还是来宾帐号。

在通常的情况下，SID标识符是不会改变的。

例如：SID S-1-5-32 是我的帐号所在

## 二，主要特征

- 1.RID（资源识别符）循环（当Windows 2000上将限制模式设置为1时）
- 2.用户列表（在Windows 2000上将限制权限为0时）
- 3.组成员信息列表

- 4.共享枚举
- 5.检测主机是否在工作组或域中
- 6.识别远程操作系统
- 7.密码策略检索（使用Polenum）

### 三，帮助手册

选项有（例如：“枚举”）：

- U 获取用户列表
- M 获取共享列表
- P 获取密码策略信息
- G 获取组和成员列表

- d 详细输出
- u user 用户指定需要使用的用户名（默认为空）
- p pass 传递指定要使用的密码（默认为空）

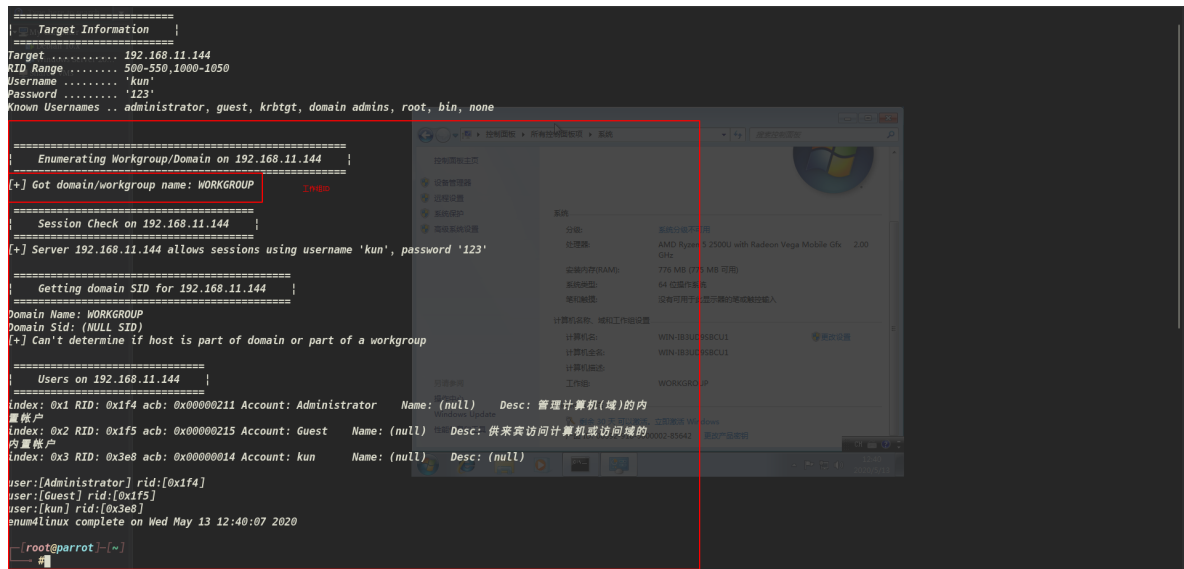
下列选项还未实现：-l\ -N\ -D\ -f

其他选项：

- a 做所有简单的枚举，如果不提供热和选项，此操作将会被启用
- h 显示帮助信息并推出
- R 范围 通过RID循环枚举用户
- K n 继续搜索RID，直到N个连续的RID不对应用户名，impies RID范围结束于9999999对跟单信用证有用。
- l 通过LDAP 389/TCP获取一些（有限）信息（仅仅适用于跟单信用证）
- s 文件 强力猜测共享名
- k 用户 远程系统上存在的用户（默认为管理员、来宾、Krbtgt、域管理员、根、bin、无）用于获取带有“查找已知用户名的sid使用逗号尝试多个用户如：“andmin,user1,user2”
- o 获取操作系统信息
- i 获取打印机信息
- w 工作组 手动指定工作组
- n 执行Nmblookup（类似与Nbtstat）
- v 冗长，显示正在运行的完整命令（Net,Rpcclient等）

注意：Samba服务通常在3000~3050之间

### 四，案例演示



enum4linux -u kun -p 123 -U 192.168.11.144

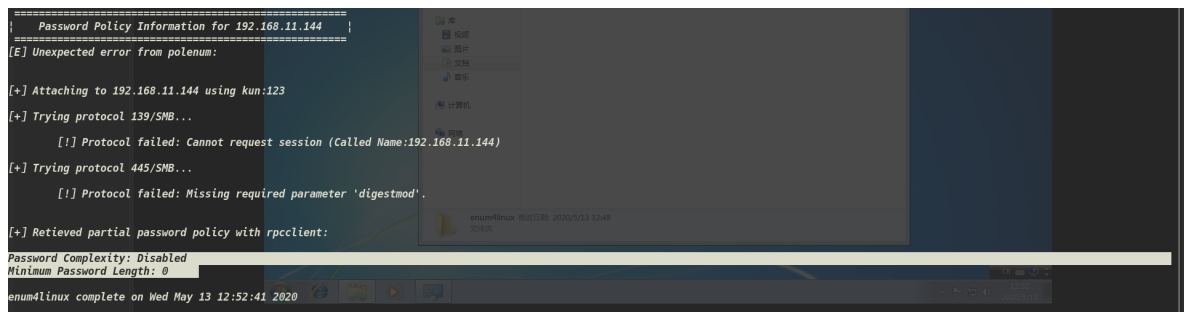
使用用户名为  密码为  对192.168.11.144进行枚举用户列表

-M参数未在此版本中所实现

具体例子为：enum4linux -u kun -p 123 -M 192.168.11.144

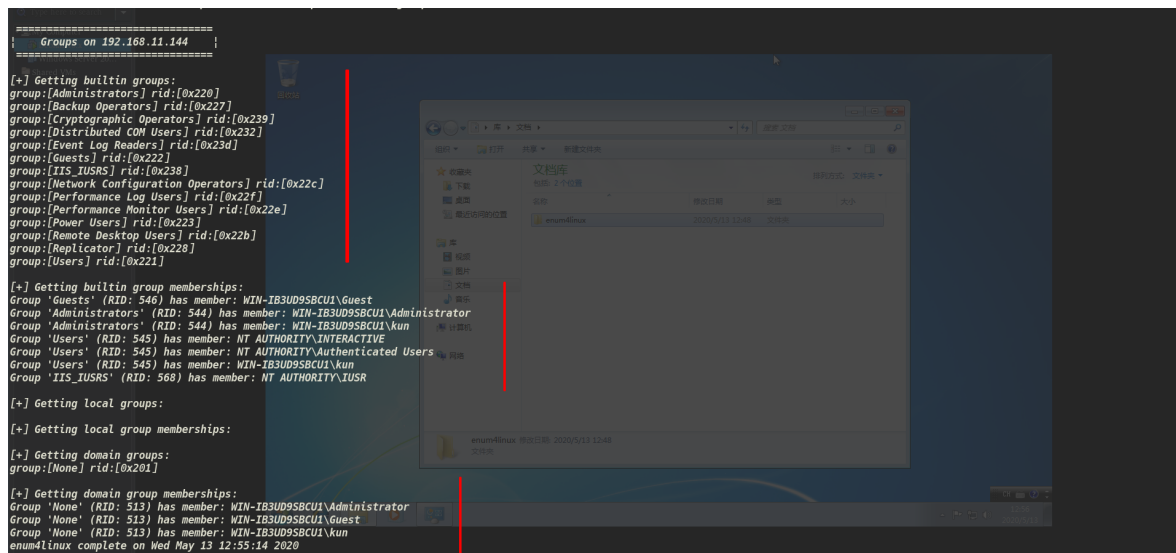
enum4linux -u kun -p 123 -P 192.168.11.144

获取密码策略信息



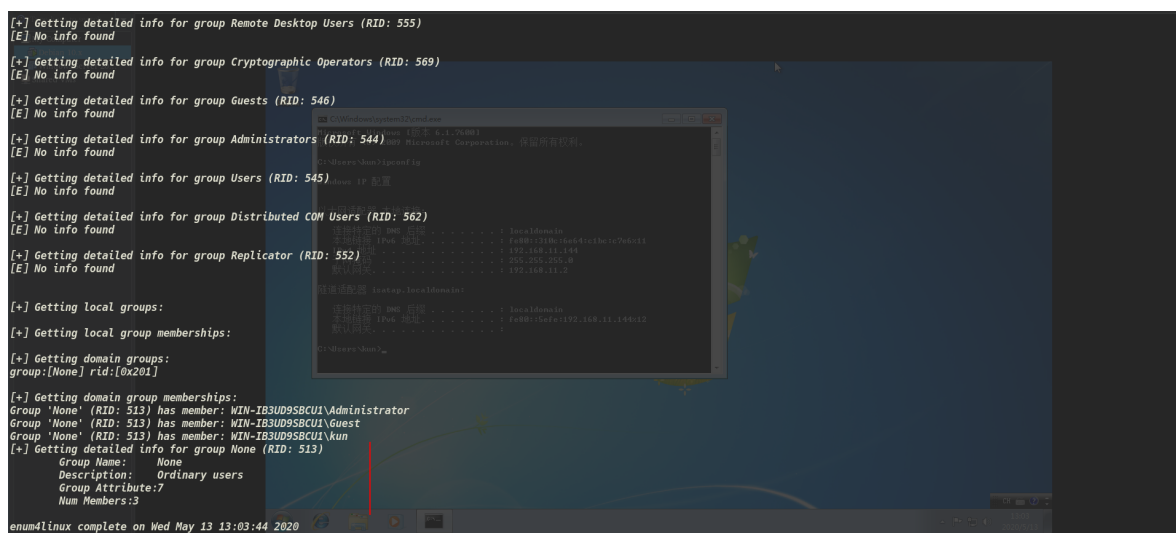
enum4linux -u kun -p 123 -G 192.168.11.144

获取对方服务器/主机用户组和成员列表



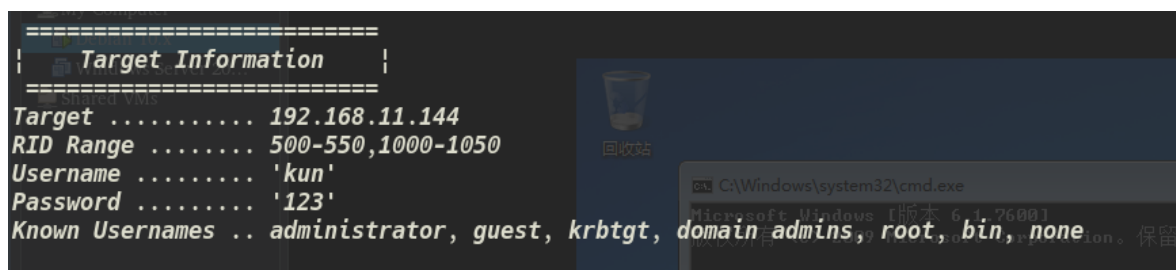
enum4linux -u kun -p 123 -G -d 192.168.11.144

详细枚举出对方主机/服务器之中的用户组或成员列表。



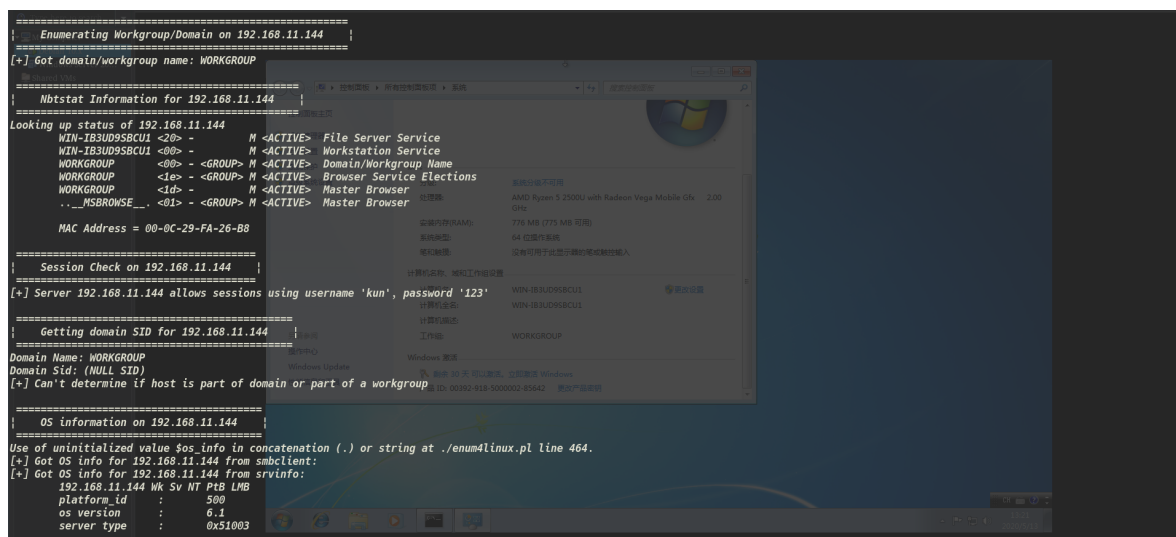
enum4linux -u kun -p 123 -d 192.168.11.144

指定用户名为 kun 密码为 123



enum4linux -u kun -p 123 -a 192.168.11.144

当你不想指定某一个参数的时候， -a 将会枚举出所有支持的选项。



安全标识符（SID，Security Identifiers）

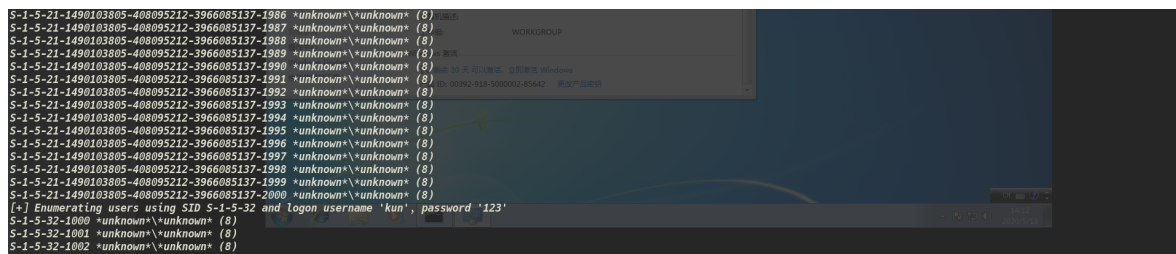
在计算机中，通常使用SID来跟踪每个账户，这就使得在系统中。你不管如何更改帐号名称，系统都知道你使用的是管理帐号还是来宾帐号。

在通常的情况下，SID标识符是不会改变的。

例如：SID S-1-5-32 是我的帐号所在

enum4linux -u kun -p 123 -R 100-200 192.168.11.144

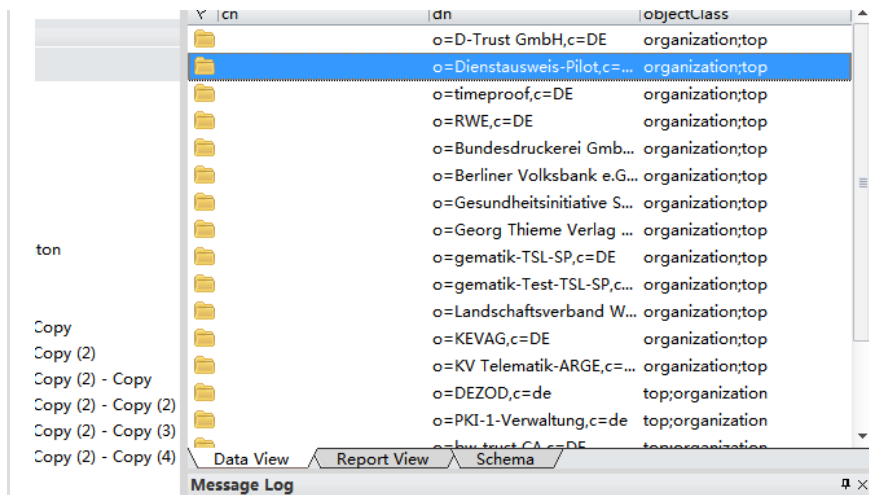
通过RID（资源标识符）来查找用户输出，如：用户名等。



轻量目录访问协议（LDAP，Lightweight Directory Access Protocol）

简单的来说LDAP是一的到关于人或者资源的集中，静态数据的快速方式。

LDAP用于发布目录中的不同资源的协议，通常他被作为一个集中地址本使用。



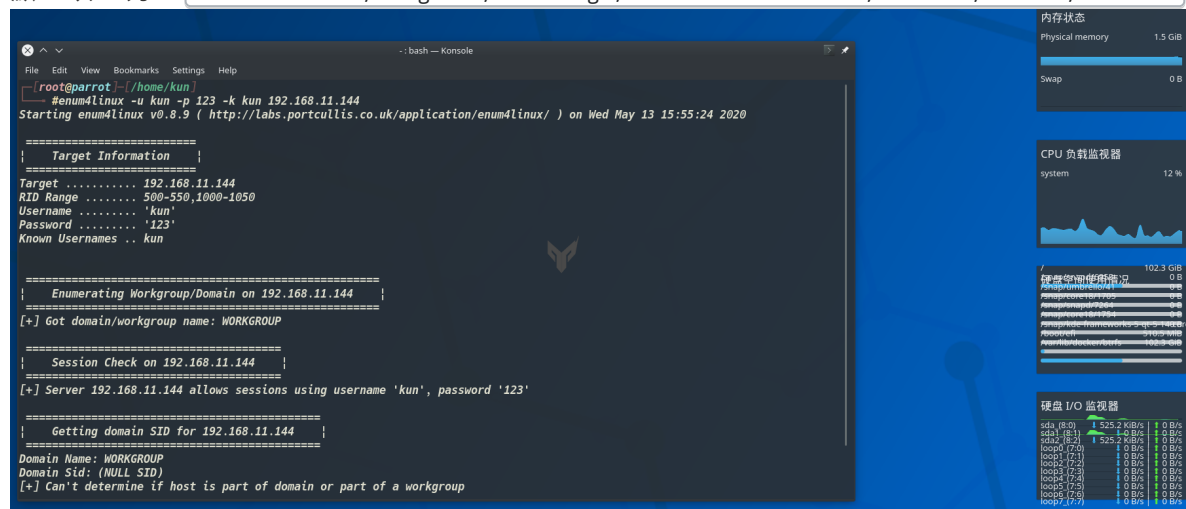
enum4linux -u kun -p 123 -l 192.168.11.144

查看对方LDAP信息

enum4linux -u kun -p 123 -k kun 192.168.11.144

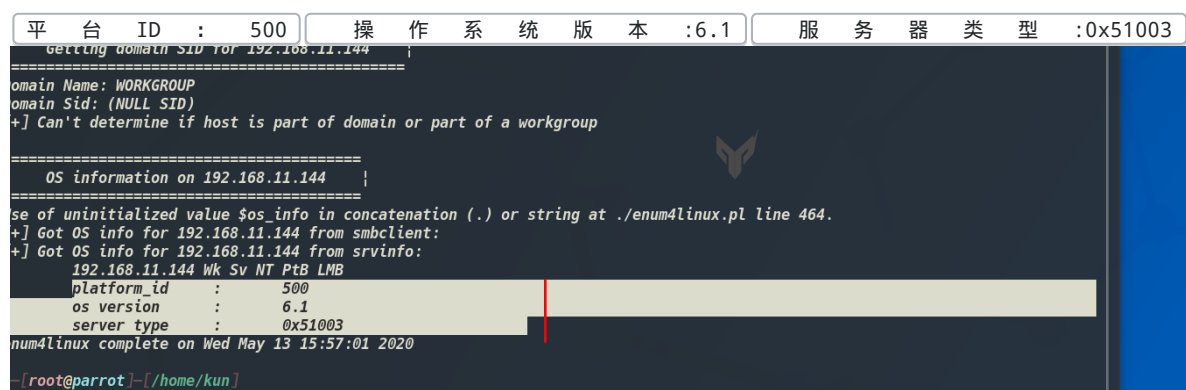
将远程系统上存在的用户指定为

默认为



enum4linux -u kun -p 123 -o 192.168.11.144

获取对方版本及系统信息



```
enum4linux -u kun -p 123 -i 192.168.11.144
```

## 获取打印机信息

```
enum4linux -u kun -p 123 -w WORKGROUP 192.168.11.144
```

## 手动指定工作组

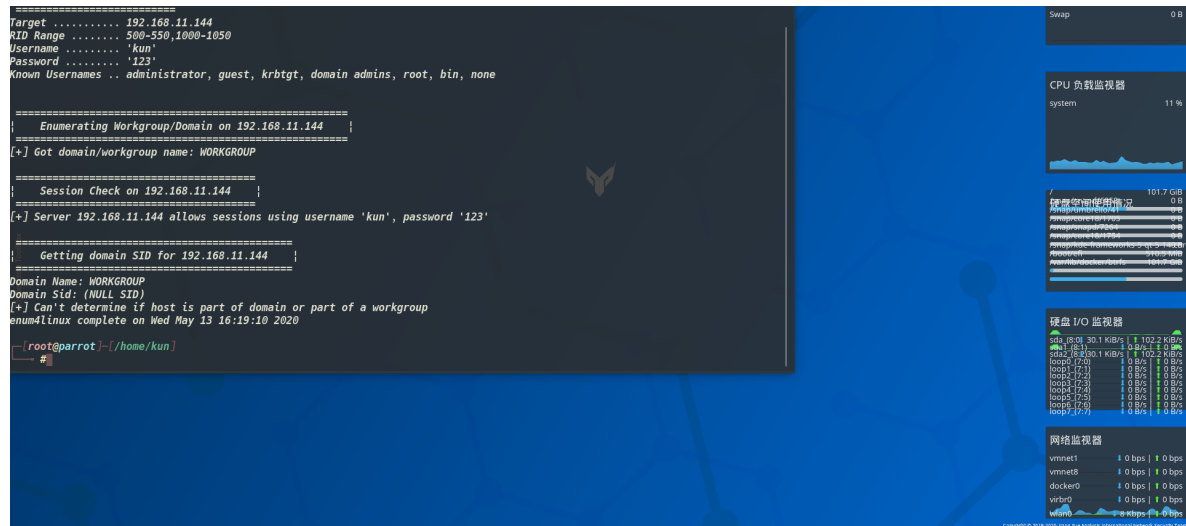
```
=====
Target ..... 192.168.11.144
RID Range ..... 500-550,1000-1050
Username ..... 'kun'
Password ..... '123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.11.144 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Session Check on 192.168.11.144 |
=====
[+] Server 192.168.11.144 allows sessions using username 'kun', password '123'

=====
| Getting domain SID for 192.168.11.144 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
enum4linux complete on Wed May 13 16:19:10 2020

[root@parrot:~/home/kun] #
```

The image shows a terminal window with the output of the enum4linux command. The output indicates that the user 'kun' with password '123' successfully authenticated on the target 192.168.11.144, and the domain/workgroup name is WORKGROUP. To the right of the terminal is a system monitoring dashboard with various charts and metrics, including CPU usage (11%), memory usage (101.7 GB), disk I/O, and network statistics.

## Nmblookup

在Enum4linux中是一个类似于Nbtstat，而Nbtstat早期主要用于早期WINDOWS的名称解析系统。

```
enum4linux -u kun -p 123 -n 192.168.11.144
```

## 执行Nmblookup

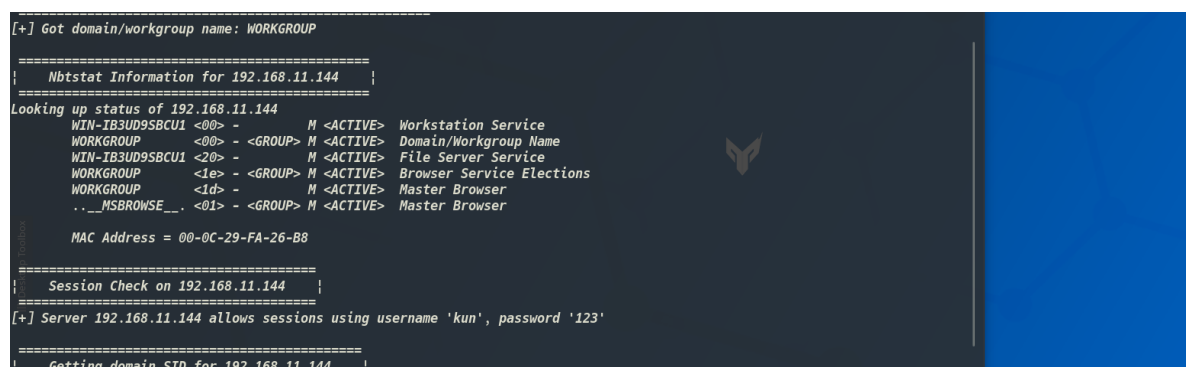
```
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 192.168.11.144 |
=====
Looking up status of 192.168.11.144
  WIN-1B3UD9SBCU1 <00> - M <ACTIVE> Workstation Service
  WORKGROUP <00> - <GROUP> M <ACTIVE> Domain/Workgroup Name
  WIN-1B3UD9SBCU1 <20> - M <ACTIVE> File Server Service
  WORKGROUP <1e> - <GROUP> M <ACTIVE> Browser Service Elections
  WORKGROUP <1d> - M <ACTIVE> Master Browser
  .._MSBROWSE_.. <01> - <GROUP> M <ACTIVE> Master Browser

  MAC Address = 00-0C-29-FA-26-B8

=====
| Session Check on 192.168.11.144 |
=====
[+] Server 192.168.11.144 allows sessions using username 'kun', password '123'

=====
| Getting domain SID for 192.168.11.144 |
=====
```

The image shows a terminal window with the output of the Nmblookup command. The output displays the status of various services on the target 192.168.11.144, including Workstation Service, Domain/Workgroup Name, File Server Service, Browser Service Elections, and Master Browser. To the right of the terminal is a system monitoring dashboard with various charts and metrics, including CPU usage (11%), memory usage (101.7 GB), disk I/O, and network statistics.

```
enum4linux -u kun -p 123 -v 192.168.11.144
```

## 显示正在运行的完整命令



```
V] Attempting to get domain name with command: nmblookup -A '192.168.11.144'
+ ] Got domain/workgroup name: WORKGROUP

=====
      Session Check on 192.168.11.144      |
=====
V] Attempting to make null session using command: smbclient -W 'WORKGROUP' //192.168.11.144/IPC$ -U'kun'%123' -c 'help' 2
&1
+ ] Server 192.168.11.144 allows sessions using username 'kun', password '123'

=====
      Getting domain SID for 192.168.11.144      |
=====
V] Attempting to get domain SID with command: rpcclient -W 'WORKGROUP' -U'kun'%123' 192.168.11.144 -c 'lsaquery' 2>&1
omain Name: WORKGROUP
omain Sid: (NULL SID)
+ ] Can't determine if host is part of domain or part of a workgroup
num4linux complete on Wed May 13 16:41:02 2020

-[root@parrot]-[/home/kun]
#
```