Metasploitable 2 系列教程：信息收集

Metasploitable 2 系统是一个基于 ubuntu 的系统。其设计的最初目的为安全工具测试和常见漏洞攻击演示。而在这篇关于 Metasploit 的教程中，我们将列举有关 Metasploitable 2 这个系统的相关漏洞，并利用漏洞，来收集和获取我们所需要的信息。

在数学或计算机科学中的枚举是指，在一组中一一列出其中的元素。但在黑客术语中，枚举通常是指将我们所要收集的信息枚举出来。例如：我们需要枚举出数据库的用户名甚至密码，枚举系统的文件共享，枚举服务器当前状态，枚举 web 目录，群组及当前网络主机存活量等信息。在枚举过程中，我们还将收集到其它可利用的网络相关信息，这对于我们后续的渗透具有重要意义。对于 Metasploitable 2 最重要的是端口扫描和指纹识别的枚举信息的收集。端口扫描是用来探测服务器或主机开放的 TPC 和 UDP 端口的。而指纹识别，则是用来确定这些服务版本等基本信息的过程。在本篇文章中，我们将使用鼎鼎大名的扫描神器 Nmap，来实现对 Metasploitable 2 的信息收集。除此之外，我们还将结合另一款枚举工具 enum4linux 来一起帮助我们完成信息的收集工作。enum4linux 是一款用于枚举 Windows 和 Samba 主机信息的工具。

从枚举过程中检索到的信息，例如，操作系统版本和正在运行的服务，我们将在这些服务中寻找到已知的漏洞。并通过开源的漏洞库（OSVDB）和已被公布出来的 CVE 来进行漏洞的利用！最后,我们还将使用 kali 下的 OpenVAS 来对目标主机进行一次全方位的漏洞扫描。

1、Metasploitable 2 的枚举与端口扫描

在这部分的 Metasploitable 2 枚举的教程中，我们将枚举正在运行的服务，帐户并同时执行端口的扫描动作。我们将使用 nmap 扫描及探测虚拟机的端口开放状态和开放服务的指纹信息。在本篇文章中，我们主要集中在网络信息的枚举收集上！

现在，让我们来打开已经安装好的 Metasploitable 2 虚拟机。并进行初始登陆，登录名及密码均为 msfadmin！登陆成功后，我们可以使用 ifconfig 命令来查看我们当前虚拟机的 IP 地址。同样，我们也可以在 kali 上使用 netdiscover 来扫描整个网段的 IP 地址，以此来锁定目标的 IP！使用命令如下：

```
Netdiscover -r 192.168.111.0/24
```

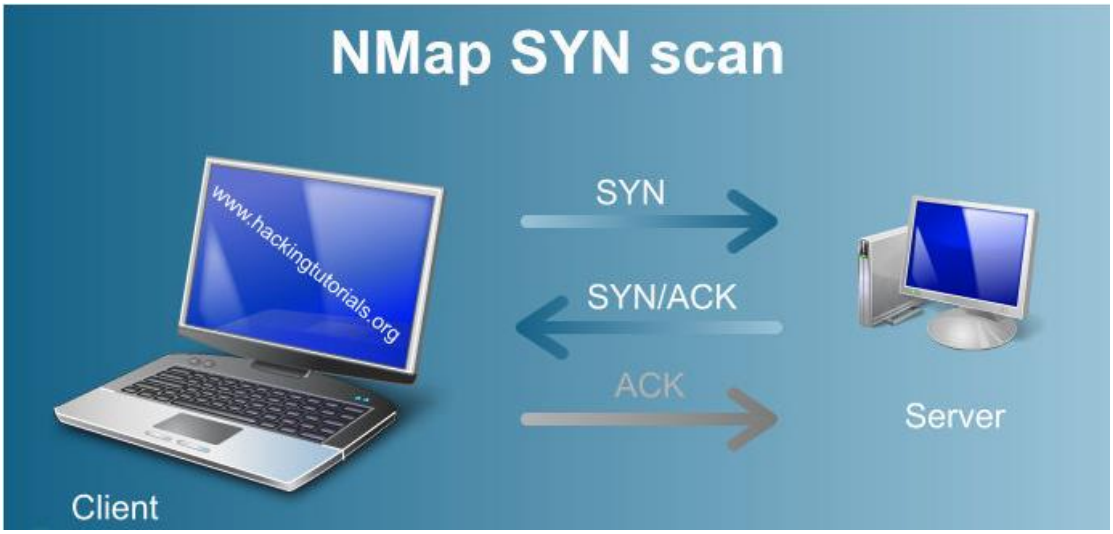
以上命令会列举出所有处在 192.168.111.0 ~192.168.111.255 范围内的存活主机。当然了，如果想取得 Metasploitable 2 的 IP，则必须保证你们同处一个地址段内！

2、Nmap 的端口及服务扫描

在这部分我们将使用 NMap 来进行扫描任务。我们将会使用 TCP SYN 的扫描方式，众所周知 SYN 是一种相对隐蔽的扫描方式，原因在于它并不向目标主机建立完整的三次握手连接。这里简单概述下，TCP 扫描的过程。TCP 扫描首先会向目标服务器发送一个 SYN 包，当目标的服务端口处于开启时，则 nmap 收到一个 SYN-ACK 的响应包。如果我们发的 SYN 包在第一次发送时就没有获得响应，那么可以猜测目标防火墙可能对我们的探测进行了过滤或则并未开启服务。最后 Nmap 则会向目标再次返回一个 ACK 包从而完成一次完整的 TCP 连接！

当我们使用 Nmap 进行 SYN 或其它形式的扫描时，如果我们不指定端口，那么 Nmap 默认会从所有的 65535 个端口中，选出其中 1000 个最为常见的端口作为扫描目标来进行探测。如果你怕遗漏一些重要信息我们可以使用-p-这个参数来实现对 所有 65535 个端口进行扫描！例如：

```
nmap -sS -p-[目标 IP 地址]
```



Tip：值得一提的是虽说 SYN 扫描是一种相对隐蔽的扫描方式。但是它只对那些比较老的防火墙有效，而对于如今技术不断更新及趋于完善的防火墙，它并不隐蔽！

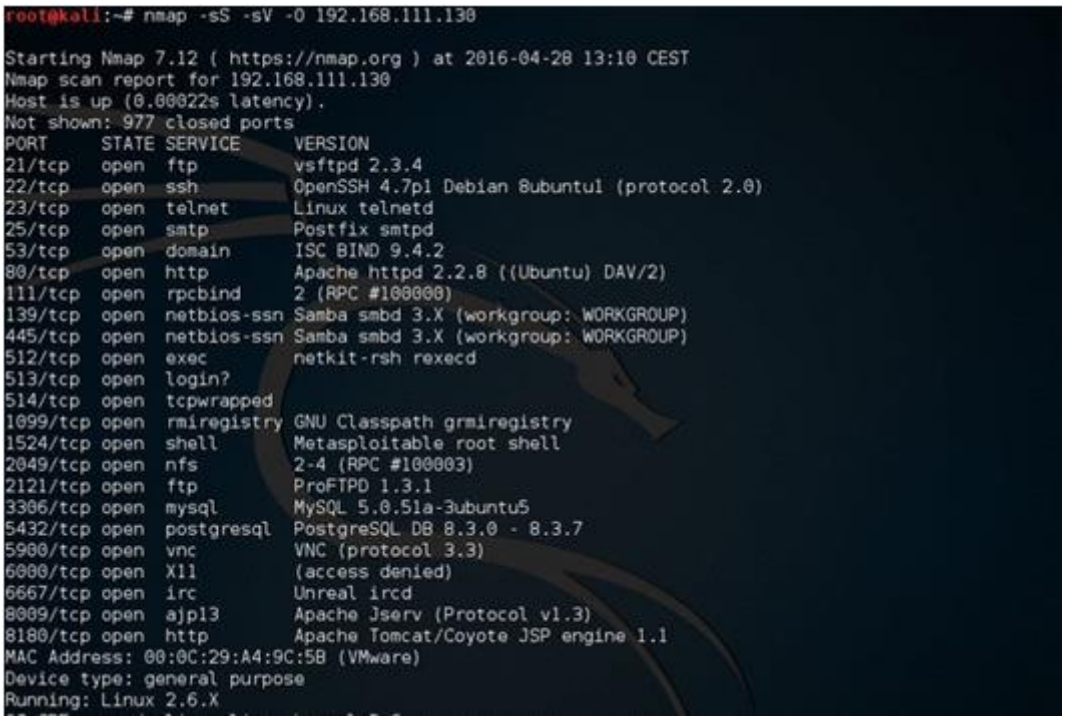
2.1 端口开放就意味着有漏洞可被利用吗？

以上的命题，显而易见是错误的。端口开放并不意味着其底层的软件就存在可利用漏洞，我们还需结合其操作系统及运行服务的当前版本号。因此收集版本信息，对我们后续渗透也至关重要！下面 Nmap 将很好的帮我们解决这些问题。在 Nmap 中，我们可以使用-sV 和-O 参数来分别获取到目标主机的版本及操作系统版本信息。除此之外其实我们还可以使用-A 参数来取代-O 参数，它同样可以

获取版本信息，但它是基于 TCP 的全连接扫描，因此并不安全！命令如下：

```
Nmap -sS -sV -O [目标 IP 地址]
```

当我们成功执行以上扫描后，我们可以看到一下返回结果：



从以上结果，我们可以很清晰的看到，目标系统开放了很多危险端口及应用服务。并且详细列举出了目标操作系统的版本为 Linux 2.6.9 – 2.6.33 我们可以看到主机正在跑的服务有 :SSH 其使用的是 OpenSSH 这款软件 ,还有 telnet 服务，Apache 2.2.8 web 服务，SQL server 和其它各类服务。下面让我们来做个简单的总结：

Vsftpd 2.3.4 on open port 21

OpenSSH 4.7p1 Debian 8ubuntu 1 (protocol 2.0) on open port 22

Linux telnetd service on open port 23

Postfix smtpd on port 25

ISC BIND 9.4.2 on open port 53

Apache httpd 2.2.8 Ubuntu DAV/2 on port 80

A RPCbind service on port 111

Samba smbd 3.X on port 139 and 445

3 r services on port 512, 513 and 514

GNU Classpath grmiregistry on port 1099

Metasploitable root shell on port 1524

A NFS service on port 2049

ProFTPD 1.3.1 on port 2121

MySQL 5.0.51a-3ubuntu5 on port 3306

PostgreSQL DB 8.3.0 – 8.3.7 on port 5432

VNC protocol v1.3 on port 5900

X11 service on port 6000

Unreal ircd on port 6667

Apache Jserv protocol 1.3 on port 8009

Apache Tomcat/Coyote JSP engine 1.1 on port 8180

2.2 Nmap UDP 扫描

到目前为止，我们一直在介绍关于 TCP 的扫描。下面让我们介绍关于 UDP 的扫描！我们可以使用以下命令：

```
nmap -sU 192.168.111.128
```

同样我们可以使用-p 参数，来指定我们要扫描的端口。相对于 TCP 扫描，UDP 扫描会慢于TCP。经过一小会儿的等待，Nmap 返回了以下 UDP 的扫描结果：

53/udp open domain

111/udp open rpcbind

137/udp open netbios-ns

2049/udp open nfs

Tip：UDP 扫描相对于 TCP，可能会造成大量的误报。原因在于，当目标主机

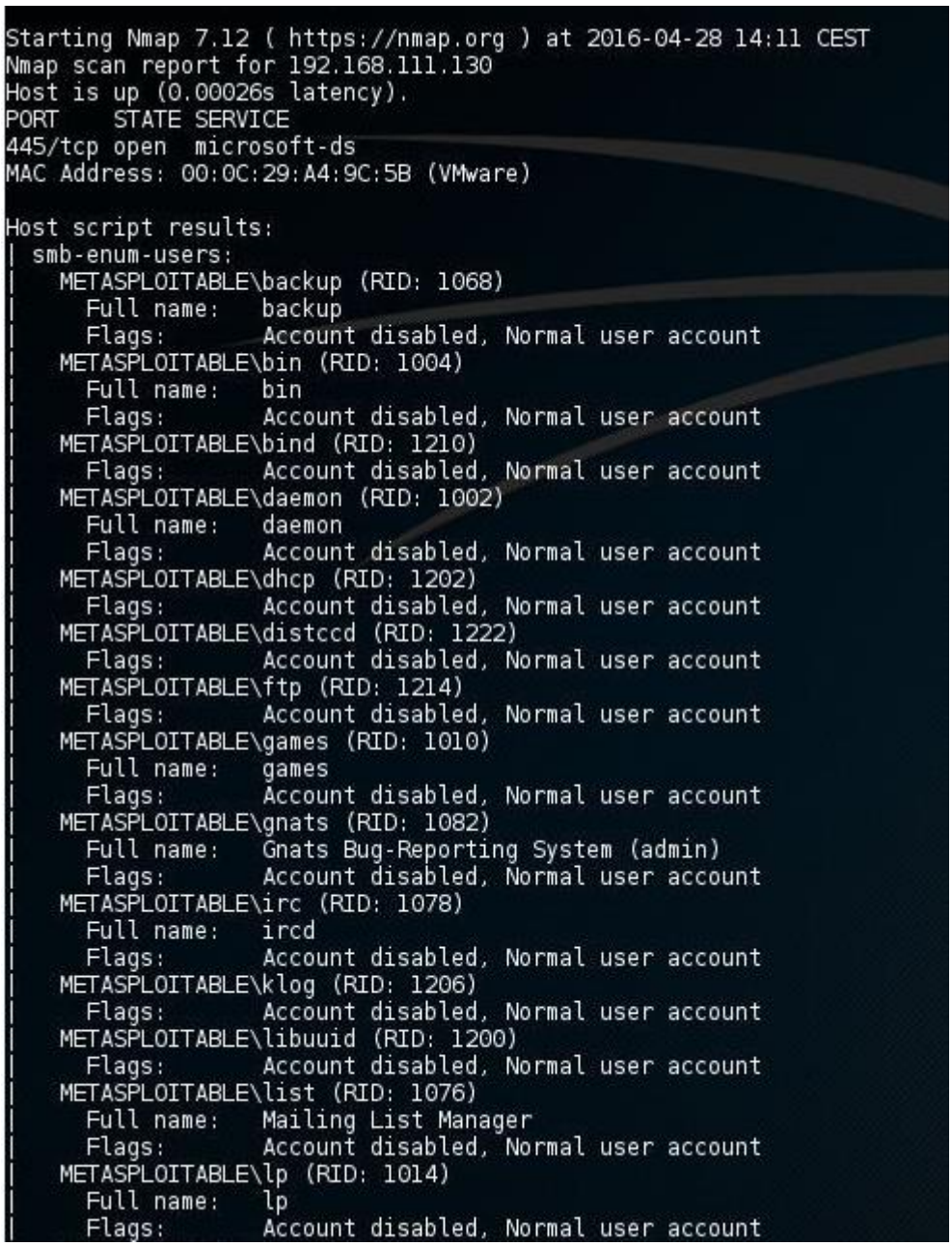
的端口处于关闭状态时，它只会返回一个 ICMP 端口不可达的信息。这种扫描类似与 TCP 的 SYN 扫描方式！由于包的丢失，在很多扫描器中对于 UDP 的扫描默认都认为其端口是开放的。当我们没有获取到 ICMP 不可达的提示时，则说明目标系统的 UDP 端口是出于开放状态的。

3、Metasploitable 2 用户枚举

为了获取目标虚拟机上的用户信息，接下来我们将使用到 Nmap 的一个脚本 smb-enum-users。使用命令如下：

```
nmap -script smb-enum-users.nse -p 445 [目标主机]
```

查询结果如下：



从扫描结果我们可以看到 Metasploitable 2 上大量的用户信息。其中很多服务账号和 admin 账号，都叫 msfadmin 这个用户名。下面让我们看看使用第二种方法 ,检索列表中的用户帐户 ,就是使用 Samba 服务器上的一个空会话的方式。

3.1 利用 rpcclient 空会话枚举用户账户

rpcclient 是用于执行客户端 MS-RPC 功能的 Linux 工具。空会话是指，连接一个 samba 或 SMB server 不需要用户名及密码验证，因此叫做空会话！支持空

会话，是由系统默认的。但是从 Windows XP SP2 和 Windows Server 2003 开始系统就不支持空会话的连接了！连接使用的是 445 端口，因此目标主机也开放着 445 端口。当我们成功进行空会话连接后，我们就可以输入相应的命令，来查询当前主机的端口开放状态了！

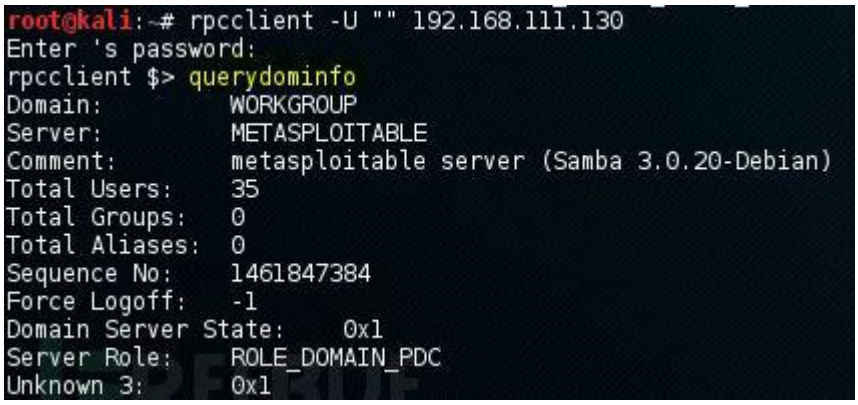
现在让我们打开一个新的 terminal 窗口，使用 Metasploitable 2 samba server 来建立一个空会话连接。命令如下：

```
rpcclient -U "" [目标 IP 地址]
```

-U 参数用来指定一个空用户，后面跟上 Metasploitable 2 VM 的 IP 地址。当我们按 enter 后，会要求你输入密码我们继续回车即可！

接着我们执行以下命令：

```
rcpclient $> querydominfo
```



通过 querydominfo 命令，我们获取到了 domain，server 和目标系统的用户总数还有一些其他的信息。从返回结果我们得知，目标系统有 35 个用户下面让我们来枚举出他们！命令如下：

```
rcpclient $> enumdomusers
```

可以看到，此时已经列举出了所有可用用户账户。现在让我们使用 rpcclient，利用已获取的用户账户信息，来查询用户更加详细的信息！命令如下：

```
rcpclient $> queryuser [用户名]
```

我们来查询 msfadmin 这个账户：

```
rcpclient $> queryuser msfadmin
```

这将返回关于服务器上的配置文件路径信息，主驱动器信息及密码相关的设置等。如果想了解更多的关于 rcpclient 的使用方法，可以使用 help 来查看。

3.2 枚举工具之 enum4linux

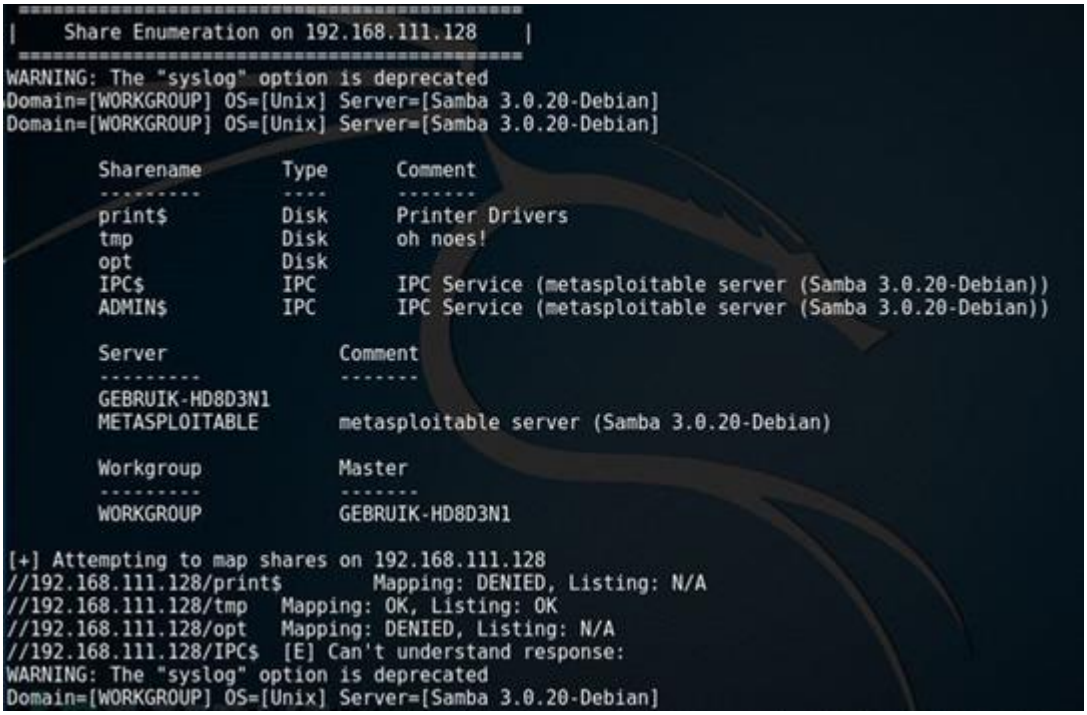
Enum4linux 是一款用 Perl 语言开发的工具，它主要用来枚举 Windows 和 Samba 主机。下面让我们来看看如何在 Metasploitable 2 下使用它。

```
Usage: ./enum4linux.pl [options]ip

-U get userlist 获取用户列表

-M get machine list* 获取机器列表

-S get sharelist 获取分享列表

-P get password policy information 获取密码策略信息

-G get group and member list 获取组成员信息

-d be detailed, applies to -U and -S 更加详细信息，结合 -U 和 -S 使用

-u user specify username to use (default “”) 指定用户名

-p pass specify password to use (default “”) 指定密码

-a Do all simple enumeration (-U -S -G -P -r -o -n -i) 执行所有枚举操作

-o Get OS information 获取系统信息

-i Get printer information 获取打印机信息
```

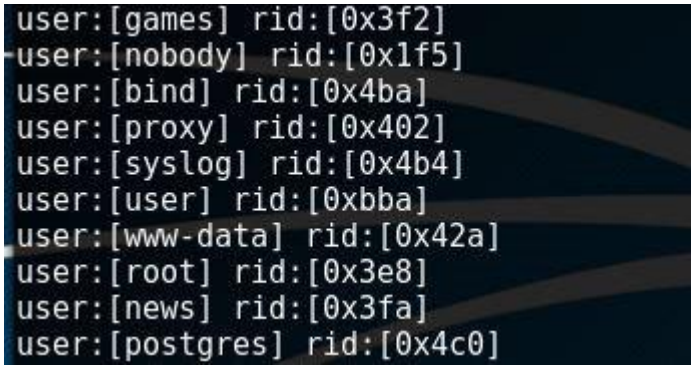
在基本了解后，现在我们在 Metasploitable 2 上执行如下命令：

```
enum4linux 192.168.111.128
```

可以看到 enum4linux 为我们获取了许多有用的信息，我们得到了一个可用的共享：



并且还列出了可用的账户信息：



还有有关操作系统的信息：

到此为止，我们已经收集到了目标操作系统 Metasploitable 2 的用户账户，开放端口及运行服务的版本等信息 !同时我们还获取到了比较机密的密码策略信

息。接下来我们就可以，对这些获取的信息进行评估分析，为我们下一步的渗透打下良好的基础。