

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TCP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。

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：

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.128.1	00:50:56:c0:00:08	1	60	VMware, Inc.
192.168.128.2	00:50:56:f3:e0:19	1	60	VMware, Inc.
192.168.128.130	00:0c:29:8f:6c:e9	1	60	VMware, Inc.
192.168.128.254	00:50:56:e4:ec:ac	1	60	VMware, Inc.

```
root@kali:~# netdiscover -r 192.168.128.0/24
```

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！

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：

```
root@kali:~# nmap -sS -p- 192.168.128.130
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-02 04:08 CST
Nmap scan report for 192.168.128.130
Host is up (0.00017s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
```

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：

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-02 04:17 CST
Nmap scan report for 192.168.128.130
Host is up (0.00027s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:8F:6C:E9 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

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

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：

```

root@kali:~# nmap --script smb-enum-users.nse -p 445 192.168.128.130
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-02 04:14 CST
Failed to resolve "-p".
setup_target: failed to determine route to 445 (0.0.1.189)
Nmap scan report for 192.168.128.130
Host is up (0.00085s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11

```

```

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name: backup
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name: bin
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name: daemon
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name: games
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name: Gnats Bug-Reporting System (admin)
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name: ircd
|     Flags: Account disabled, Normal user account
|   METASPLOITABLE\ircd
|     Full name: ircd
|     Flags: Account disabled, Normal user account

```


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。

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：

-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！

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：

```
root@kali:~# rpcclient -U "" 192.168.128.130
Enter WORKGROUP\'s password:
rpcclient $> querydominfo
Domain:          WORKGROUP
Server:          METASPLOITABLE
Comment:         metasploitable server (Samba 3.0.20-Debian)
Total Users:     35
Total Groups:    0
Total Aliases:   0
Sequence No:     1527886465
Force Logoff:    -1
Domain Server State: 0x1
Server Role:     ROLE_DOMAIN_PDC
Unknown 3:       0x1
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
```

```

rpcclient $> queryuser msfadmin
    密码 User Name      : msfadmin
        Full Name      : msfadmin,,,
        Home Drive     : \\metasploitable\msfadmin
        Dir Drive      : 
        Profile Path   : \\metasploitable\msfadmin\profile
wpa专 Logon Script:
        Description    :
        Workstations   :
        Comment        : (null)
        Remote Dial    :
        Logon Time      :      四, 01 1月 1970 08:00:00 CST
        Logoff Time     :      四, 14 9月 30828 10:48:05 CST
        Kickoff Time    :      四, 14 9月 30828 10:48:05 CST
        Password last set Time :      三, 28 4月 2010 14:56:18 CST
        Password can change Time :      三, 28 4月 2010 14:56:18 CST
666 Password must change Time:      四, 14 9月 30828 10:48:05 CST
        unknown_2[0..31]...
        user_rid       : 0xbb8
        group_rid      : 0xbb9
        acb_info       : 0x00000010
nesuss fields_present: 0x00ffffff
        方法 logon_divs: 168
        bad_password_count: 0x00000000
        logon_count     : 0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>

```

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。

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

```

root@kali:~# enum4linux 192.168.128.130
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jun  2 11:35:29 2018

=====
| Target Information |
=====
Target ..... 192.168.128.130
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.128.130 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 192.168.128.130 |
=====

```

```

=====
| Enumerating Workgroup/Domain on 192.168.128.130 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 192.168.128.130 |
=====
Looking up status of 192.168.128.130
  METASPLOITABLE <00> - B <ACTIVE> Workstation Service
  METASPLOITABLE <03> - B <ACTIVE> Messenger Service
  METASPLOITABLE <20> - B <ACTIVE> File Server Service
  .._MSBROWSE_.. <01> - <GROUP> B <ACTIVE> Master Browser
  WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
  WORKGROUP <1d> - B <ACTIVE> Master Browser
  WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
  nesuss使用
  方法: MAC Address = 00-00-00-00-00-00

=====
| Session Check on 192.168.128.130 |
=====
[+] Server 192.168.128.130 allows sessions using username '', password ''

```

来源: <http://www.freebuf.com/articles/network/117269.html>

