THM-Protocols and Servers(协议和服务器)-学习

本文相关的TryHackMe实验房间链接： https://tryhackme.com/room/protocolsandservers

通过学习相关知识点：了解 HTTP、FTP、POP3、SMTP 和 IMAP 等常见协议以及相关的不安全因素。

H2 介绍

本文介绍了一些常用的协议，例如：

- HTTP
- FTP
- POP3
- SMTP
- IMAP

每个协议的相关问题都旨在帮助我们理解底层发生的事情，这些事情通常会被优雅的 GUI（图形用户界面）隐藏；我们将通过使用简单的 Telnet 客户端来与上述协议进行“交谈”，以充分了解你的 GUI 客户端在幕后所做的事情；我们的目的不是记住协议命令，而是在协议工作时仔细查看和协议相关的信息。

我们还讨论了和协议相关的不安全因素，特别是以明文形式发送的密码。

建议你在学习以下知识点时，启动TryHackMe房间界面的AttackBox 和虚拟机；你可以通过 Telnet 连接到不同的服务，以获得更好的练习和学习体验。

H2 Telnet协议

Telnet 协议是一种应用层协议，用于连接另一台计算机的虚拟终端。使用 Telnet，用户可以登录到另一台计算机并访问其终端（控制台）以远程运行程序、启动批处理和执行系统管理任务。

Telnet 协议比较简单，当用户连接时，他们将被要求输入用户名和密码，通过验证之后，用户将能够访问远程系统的终端。不幸的是，Telnet 客户端和 Telnet 服务器之间的所有这些通信都没有经过加密处理，因此这很容易成为攻击者的目标。

Telnet 服务器使用 Telnet 协议侦听端口23上的传入连接(请注意，目标 VM 上的Telnet端口未打开)，让我们考虑下面的示例：用户正在连接到 `telnetd` (一个 Telnet 服务器)，具体的步骤如下：

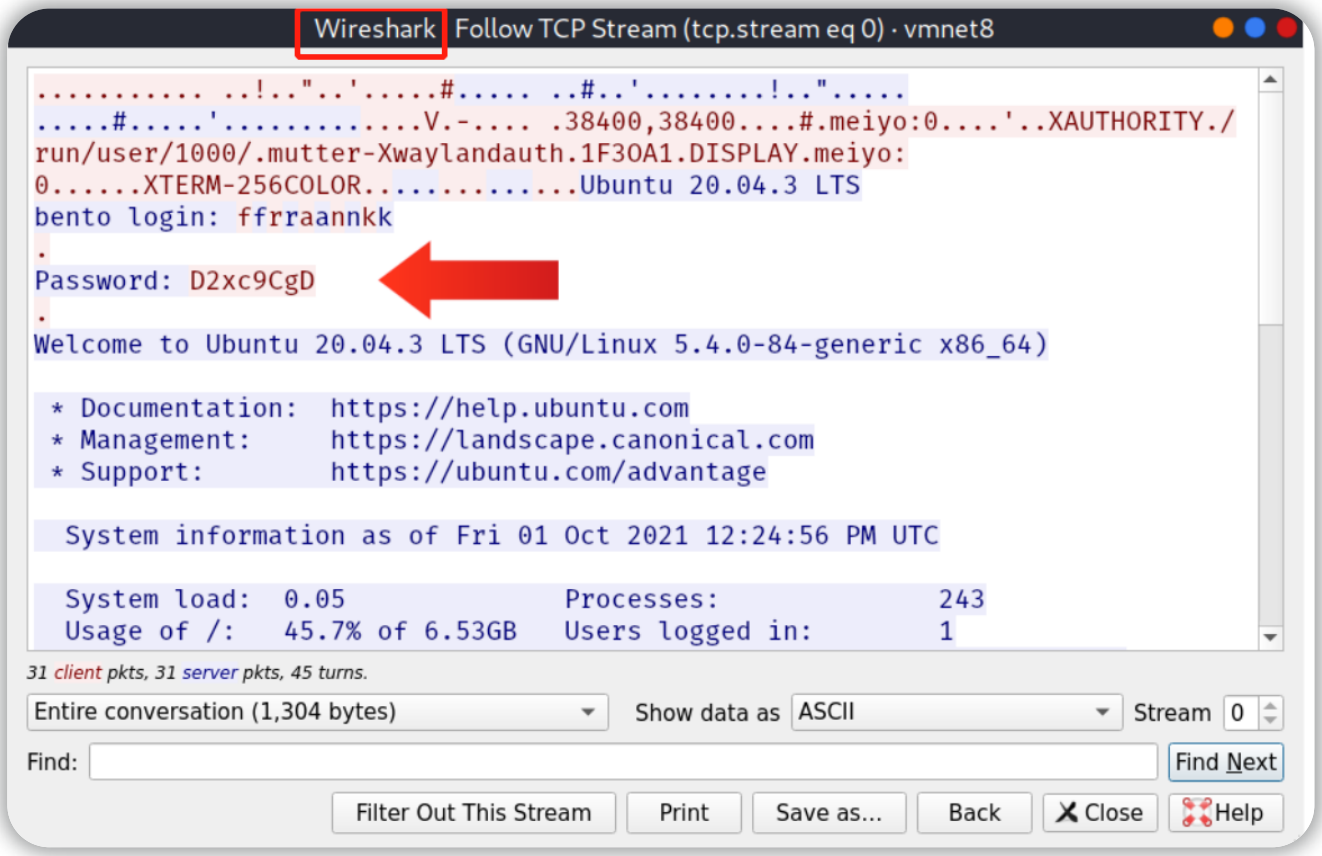
1. 首先，要求用户提供他的登录名（用户名），我们可以看到用户输入了 `frank` 。
2. 然后，用户被要求输入密码 `D2xc9CgD` ，密码明文并不会显示在屏幕上；但是，我们会将密码明文显示在下面的例子中以达到演示目的。
3. 一旦系统检查了用户的登录凭据，用户就会收到一条欢迎消息。
4. 远程服务器授予用户一个命令提示符 `frank@bento:~$` ， `$` 符号表示这不是root权限的终端。

```
pentester@TryHackMe$ telnet MACHINE_IP
Trying MACHINE_IP ...
Connected to MACHINE_IP.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
bento login: frank
Password: D2xc9CgD
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 01 Oct 2021 12:24:56 PM UTC

  System load:  0.05              Processes:              243
  Usage of /:   45.7% of 6.53GB   Users logged in:        1
  Memory usage: 15%               IPv4 address for ens33: MACHINE_IP
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.


*** System restart required ***
Last login: Fri Oct  1 12:17:25 UTC 2021 from meiyo on pts/3
You have mail.
frank@bento:~$
```

尽管 Telnet 让我们可以立即访问远程系统的终端，但它不是远程管理的可靠协议，因为Telnet相关的所有数据都是以明文形式发送的。

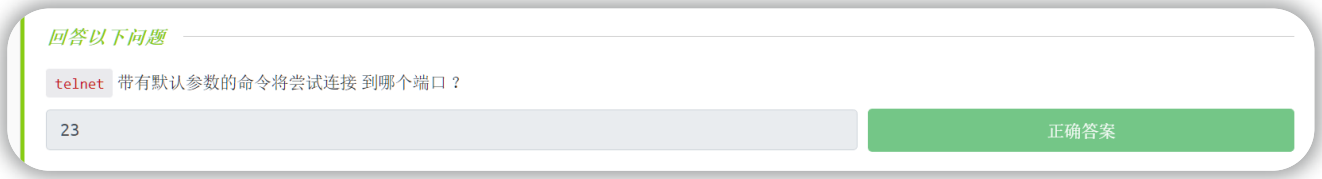
在下图中，我们使用Wireshark捕获了 Telnet 产生的流量，而且很容易就能找到密码。下图显示了我们的本地计算机和远程系统之间交换的 ASCII 数据。

红色文本是我们发送到远程系统的文本，而蓝色文本是远程系统正在发送的文本。注意用户名是如何被发回的（在我们的终端上会显示用户名），而密码并不会在终端中显示，换句话说，即使有人在看我们打字，他们也无法在屏幕上的终端界面上看到我们输入的明文密码。



Telnet 不再被认为是一种安全的协议选择，任何能够捕获你的网络流量的人都能够发现你使用的用户名和密码，这将授予他们访问远程系统的权限。 Telnet 的一个安全替代方案是 SSH协议，我们将在其他文章中介绍它。

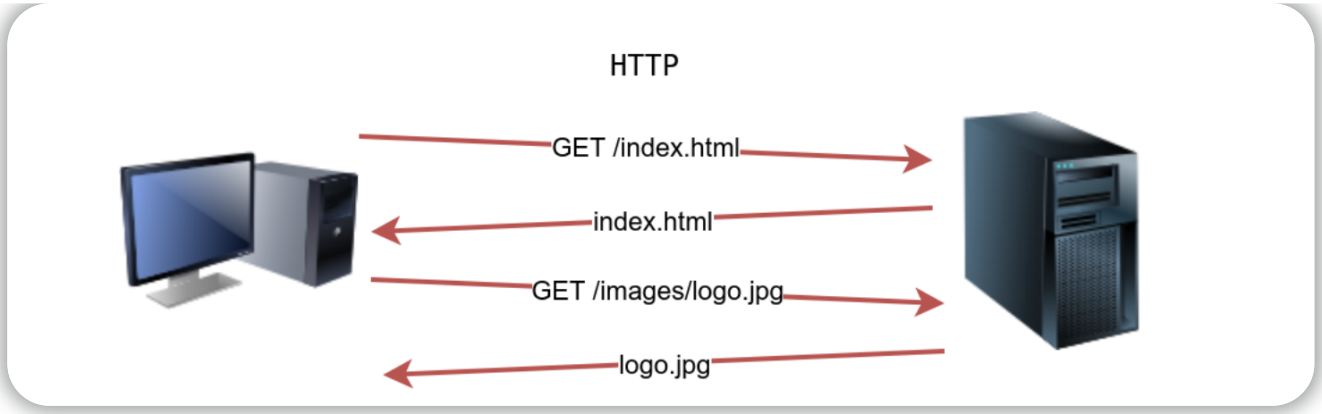
答题



H2 HTTP协议(Hypertext Transfer Protocol)

超文本传输协议 (HTTP) 是用于传输网页的协议，你的网络浏览器会连接到网络服务器并使用 HTTP 请求 HTML 页面和图像以及其他文件，并且提交表单并上传各种文件。每当你浏览万维网 (WWW) 时，你肯定使用的是 HTTP 协议。

下图显示了客户端首先请求 Web 服务器提供HTML页面 `index.html` ，客户端在得到页面之后，再接着请求一个图像资源 `logo.jpg` ，然后 Web 服务器会发送该图像资源到客户端。



HTTP 以明文形式发送和接收数据（未加密），因此，你可以使用 Telnet（或 Netcat）等简单工具与 Web 服务器通信并充当“Web 浏览器”。主要区别在于你需要手动输入与 HTTP 相关的命令，而不是 Web 浏览器为你输入这些命令。

在下面的示例中，我们将看到如何从 Web 服务器请求页面； 此外，我们还能看到目标web服务器的版本。 为此，我们将使用 Telnet 客户端请求页面，我们选择它是因为 Telnet 是一个简单的协议； 而且，它能够使用明文进行通信，方便我们查看 web服务器返回的页面信息。 我们将使用 telnet 而不是 Web 浏览器向Web 服务器请求文件，具体步骤如下：

1. 首先，我们使用 `telnet MACHINE_IP 80` 连接到端口 80。
2. 接下来，我们输入 `GET /index.html HTTP/1.1` 来检索 `index.html` 页面， 或者输入 `GET / HTTP/1.1` 来检索默认页面。
3. 最后，你需要为主机提供一些值，例如 `host: telnet` 并按两次 `Enter/Return` 键。

在下面的控制台输出中，我们可以查看我们所请求的页面以及 Web 浏览器通常不显示的大量信息，如果web服务器找不到我们所请求的页面，我们会收到一个404错误代码提示。

```
pentester@TryHackMe$ telnet MACHINE_IP 80
Trying MACHINE_IP ...
Connected to MACHINE_IP.
Escape character is '^]'.
GET /index.html HTTP/1.1
host: telnet

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 15 Sep 2021 08:56:20 GMT
Content-Type: text/html
Content-Length: 234
Last-Modified: Wed, 15 Sep 2021 08:53:59 GMT
Connection: keep-alive
ETag: "6141b4a7-ea"
Accept-Ranges: bytes
```

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Welcome to my Web Server</title>
  <meta charset="UTF-8" />
  <meta name="viewport" content="width=device-width,initial-scale=1" />
</head>
<body>
  <h1>Coming Soon<h1>
</body>
</html>
```

用户只需要键入几个命令就可以获取他们需要的页面：`GET /index.html HTTP/1.1`，还有`host: telnet`。

我们需要一个 HTTP 服务器（webserver）和一个 HTTP 客户端（web 浏览器）来使用 HTTP 协议。Web 服务器将向 发出请求的 Web 浏览器“提供”一组特定的文件。

HTTP 服务器的三种流行选择是：

- Apache
- Internet Information Services (IIS)
- nginx

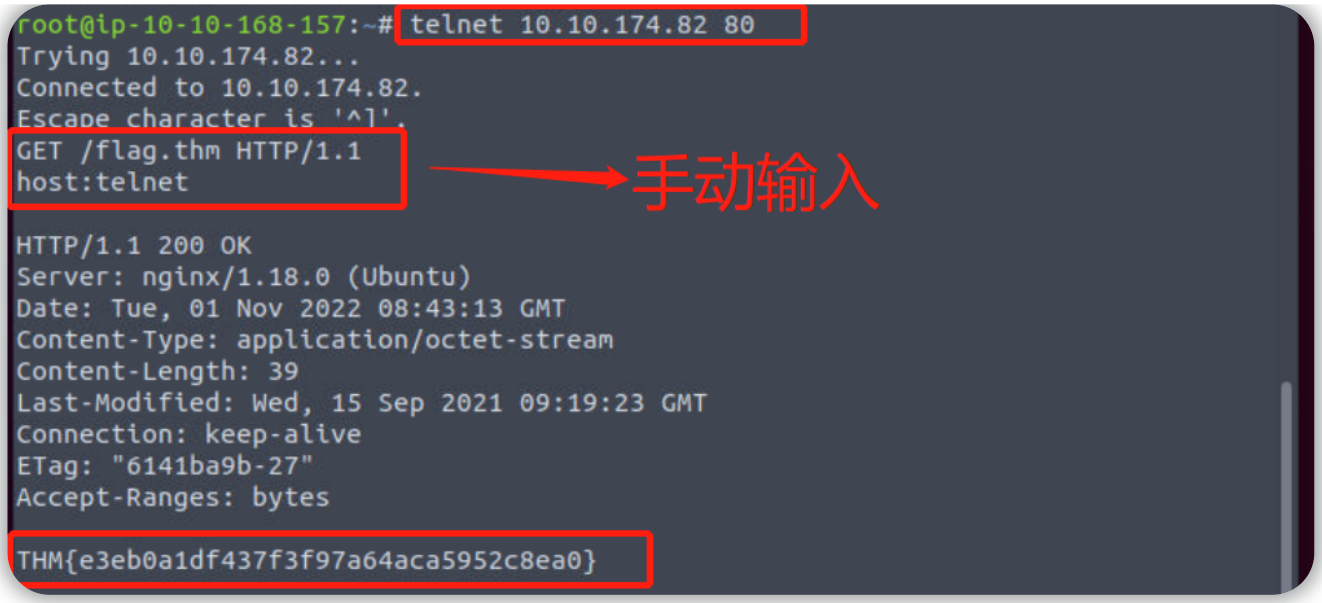
Apache 和 Nginx 是免费的开源软件，但是，IIS 是闭源软件，需要支付许可证费用。

有许多可用的网络浏览器，较流行的网络浏览器是：

- 谷歌浏览器
- 微软的Edge浏览器
- 火狐浏览器
- 苹果公司的 Safari浏览器

Web 浏览器通常可以免费安装和使用； 此外，科技巨头还在为他们的浏览器争取更高的市场份额。

答题



> THM{e3eb0a1df437f3f97a64aca5952c8ea0}

H2 FTP协议(File Transfer Protocol)

文件传输协议 (FTP-File Transfer Protocol) 的开发旨在使具有不同系统的不同计算机之间的文件传输变得高效。

FTP 也以明文形式发送和接收数据； 因此，我们可以使用 Telnet（或 Netcat）与 FTP 服务器通信并充当 FTP 客户端。 在下面的示例中，我们执行了以下步骤：

1. 我们使用 Telnet 客户端连接到 FTP 服务器。 由于 FTP 服务器默认侦听端口为21，因此我们必须指定 Telnet 客户端尝试连接到端口21而不是默认的 Telnet 端口。
2. 我们需要使用命令 `USER frank` 提供用户名。
3. 然后，我们使用命令 `PASS D2xc9CgD` 提供密码。
4. 因为我们提供了正确的用户名和密码，所以我们能够登录成功。

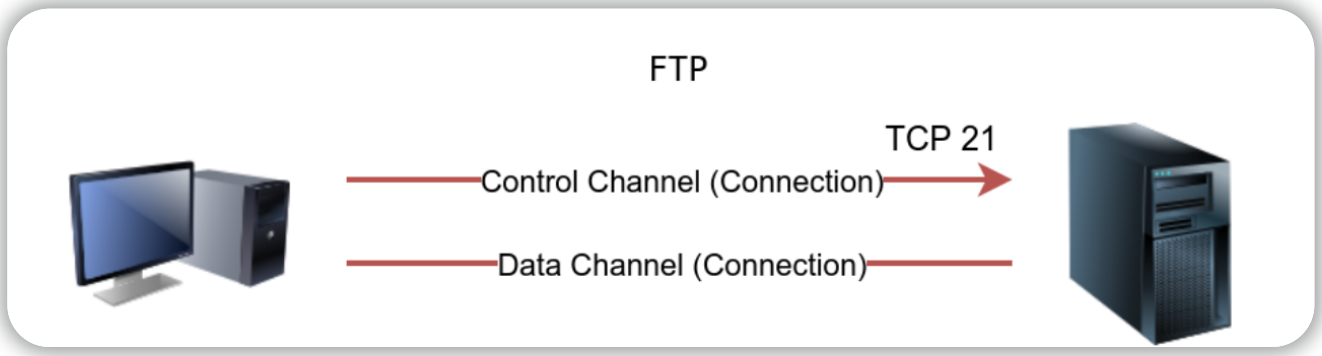
像 `STAT` 这样的命令可以提供一些附加信息， `SYST` 命令会显示目标的系统类型（本例中为 UNIX），`PASV` 命令会将模式切换为被动。值得注意的是，FTP有两种模式：

- 主动：在主动模式下，数据会通过来自 FTP 服务器端口 20 的单独通道发送。
- 被动：在被动模式下，数据会通过一个单独的通道发送，该通道源自 FTP 客户端的端口号 1023 以上。

`TYPE A` 命令会将文件传输模式切换为 `ASCII` ，而 `TYPE I` 命令会将文件传输模式切换为二进制；但是，我们无法使用Telnet等简单客户端传输文件，因为 FTP 为文件传输创建了单独的连接。

```
pentester@TryHackMe$ telnet MACHINE_IP 21
Trying MACHINE_IP ...
Connected to MACHINE_IP.
Escape character is '^]'.
220 (vsFTPd 3.0.3)
USER frank
331 Please specify the password.
PASS D2xc9CgD
230 Login successful.
SYST
215 UNIX Type: L8
PASV
227 Entering Passive Mode (10,10,0,148,78,223).
TYPE A
200 Switching to ASCII mode.
STAT
211-FTP server status:
     Connected to ::ffff:10.10.0.1
     Logged in as frank
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     At session startup, client count was 1
     vsFTPd 3.0.3 - secure, fast, stable
211 End of status
QUIT
221 Goodbye.
Connection closed by foreign host.
```

下图显示了如何使用 FTP 进行实际文件传输。为了简单理解起见，我们只关注 FTP 客户端将启动与 FTP 服务器的连接这一事实，该服务器默认会侦听端口 21。所有命令都将通过控制通道发送，一旦FTP客户端向FTP服务器请求一个文件，它们之间就会建立另一个 TCP 连接------数据通道。（建立数据连接/通道的详细细节超出了本文的知识点范围，在此不做过多介绍）。



考虑到通过 FTP 传输数据的复杂性，让我们使用实际的 FTP 客户端下载文本文件，同时我们还需要使用少量命令来检索目标文件。 登录成功后，我们得到 FTP 提示符 `ftp>` ，接着我们就可以执行各种 FTP 命令。

我们可以使用 `ls` 命令列出文件并查看文件名； 然后，我们需要切换文件格式为 `ascii` ，因为它是一个文本文件（不是二进制文件）；最后，获取 `FILENAME` 使客户端和服务器建立另一个文件传输通道。

```
pentester@TryHackMe$ ftp MACHINE_IP
Connected to MACHINE_IP.
220 (vsFTPd 3.0.3)
Name: frank
331 Please specify the password.
Password: D2xc9CgD
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (10,20,30,148,201,180).
150 Here comes the directory listing.
-rw-rw-r--    1 1001     1001         4006 Sep 15 10:27 README.txt
226 Directory send OK.
ftp> ascii
200 Switching to ASCII mode.
ftp> get README.txt
local: README.txt remote: README.txt
227 Entering Passive Mode (10,10,0,148,125,55).
150 Opening BINARY mode data connection for README.txt (4006 bytes).
WARNING! 9 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
4006 bytes received in 0.000269 secs (14892.19 Kbytes/sec)
ftp> exit
221 Goodbye.
```

FTP 服务器和 FTP 客户端使用 FTP 协议，如果要托管 FTP 文件服务器，可以选择各种 FTP 服务器软件。FTP 服务器软件的示例包括：

- vsftpd
- ProFTPD
- uFTP

对于 FTP 客户端，除了 Linux 系统中常见的控制台 FTP 客户端外，你还可以使用具有 GUI 的 FTP 客户端，例如 FileZilla；另外，一些网络浏览器也支持 FTP 协议。

由于FTP是以明文形式发送登录凭据、命令和文件，因此 FTP 流量很容易成为攻击者的目标。

答题

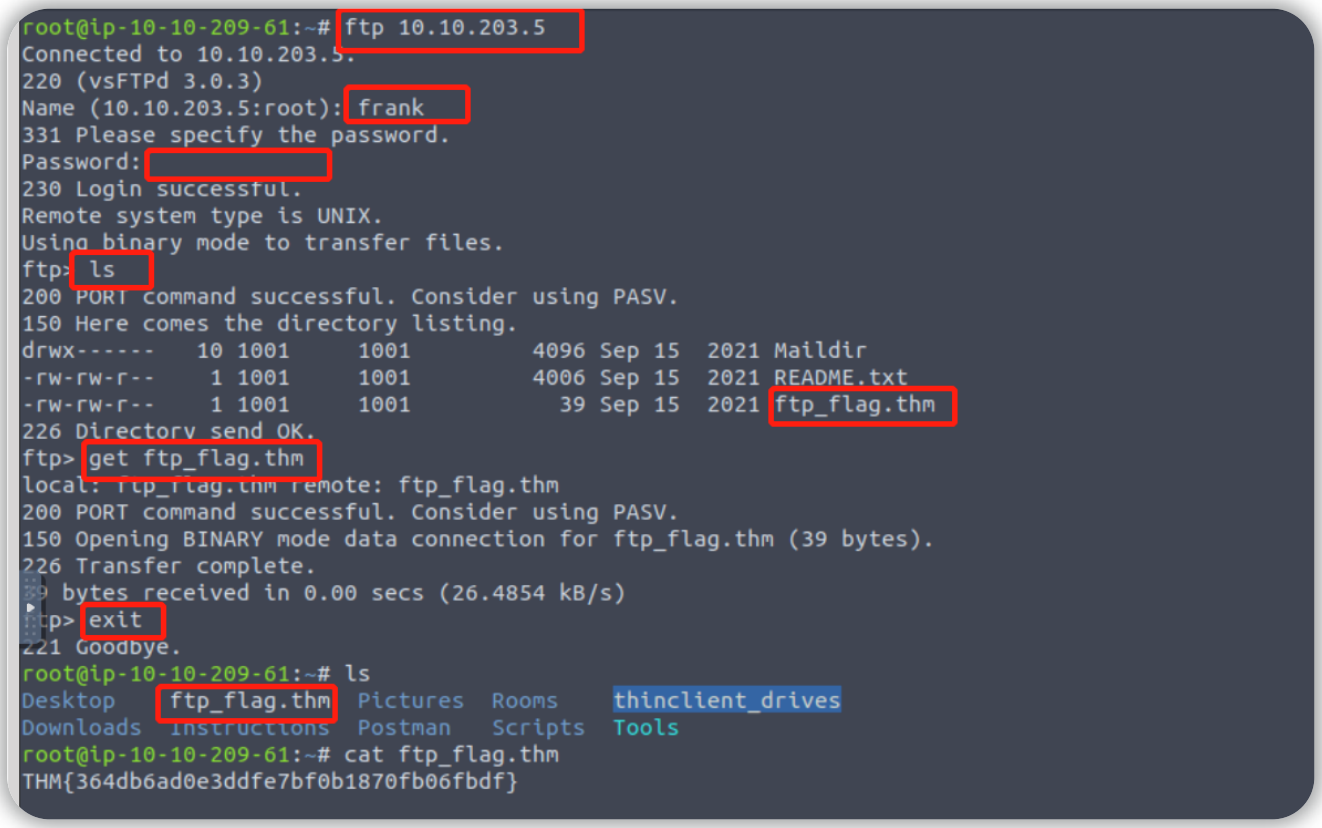
回答以下问题

使用FTP客户端，连接到 VM 并尝试恢复标志文件。什么是国旗？

- 用户名：frank
- 密码：D2xc9CgD

THM{364db6ad0e3ddfe7bf0b1870fb06fbdf}

正确答案



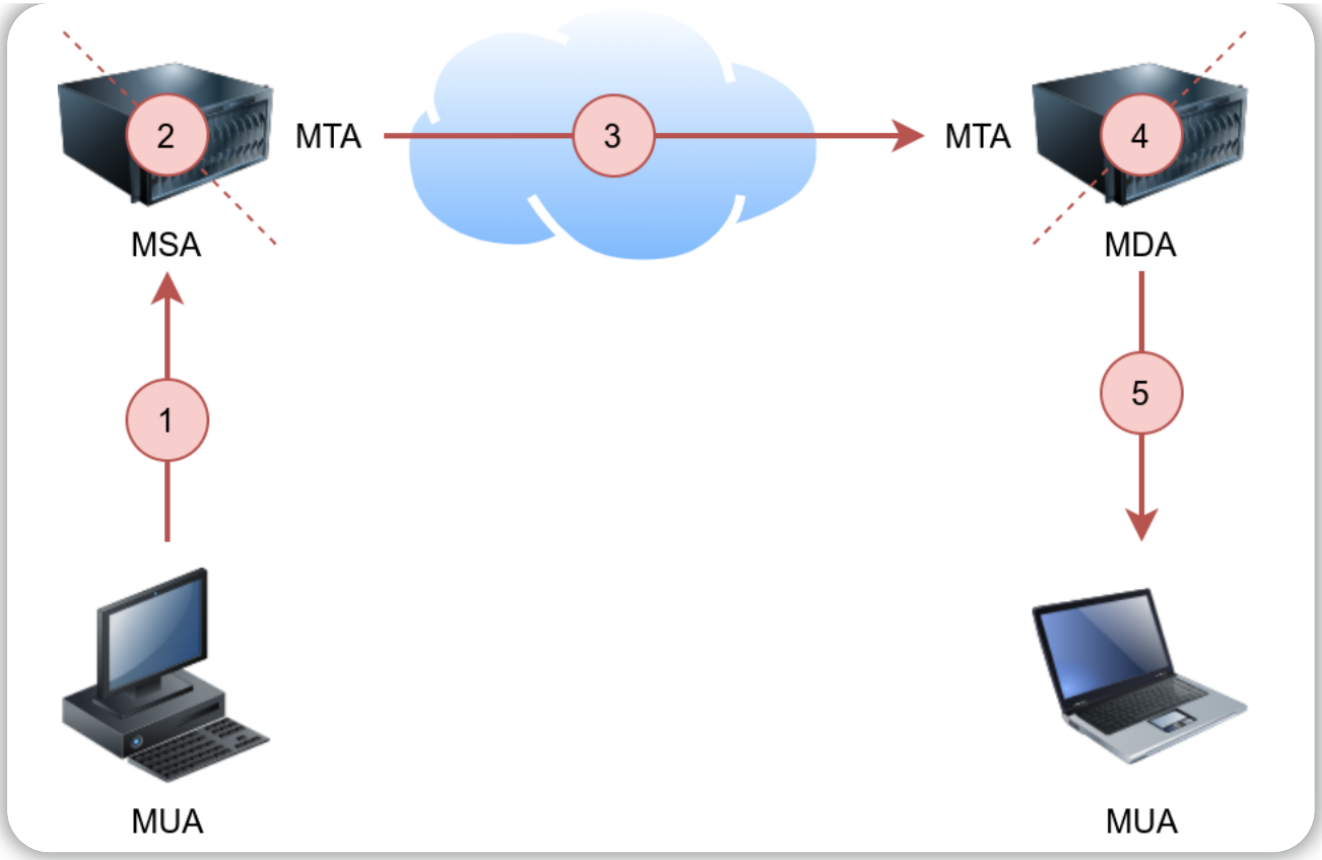
H2 SMTP协议(Simple Mail Transfer Protocol)

电子邮件是 Internet 上最常用的服务之一。 电子邮件服务器有多种配置，例如，你可以设置一个电子邮件系统，允许本地用户在不访问 Internet 的情况下相互交换电子邮件；但是，我们将考虑更一般的设置，让不同的电子邮件服务器通过 Internet 连接。

通过 Internet 发送电子邮件需要以下组件：

1. 邮件提交代理 (MSA-Mail Submission Agent)
2. 邮件传输代理 (MTA-Mail Transfer Agent)
3. 邮件投递代理 (MDA-Mail Delivery Agent)
4. 邮件用户代理 (MUA-Mail User Agent)

以上四个术语可能看起来很神秘，但它们比看起来更简单。 我们将使用下图解释这些术语。



该图显示了电子邮件需要经过以下五个步骤才能到达收件人的收件箱：

1. MUA（邮件用户代理），或简称为电子邮件客户端，有要发送的电子邮件消息，所以MUA 将会连接到MSA（邮件提交代理）以发送其消息。
2. MSA（邮件提交代理）接收邮件，在将邮件传输到通常托管在同一服务器上的 MTA(邮件传输代理) 服务器之前检查是否有任何错误。
3. MTA（邮件传输代理）会将电子邮件消息发送给收件人的 MTA，另外，MTA 还可以用作MSA (邮件提交代理-Mail Submission Agent)。
4. 典型的设置会将 MTA 服务器也用作MDA (邮件投递代理)。
5. 收件人将使用其MUA（电子邮件客户端）从 MDA（邮件投递代理） 收取电子邮件。

如果上述步骤听起来令人困惑，可以考虑下面的类比:

1. 你 (MUA) 想要发送邮件。
2. 邮局员工 (MSA) 在你当地的邮局 (MTA) 接受邮件之前检查邮件是否有任何问题。
3. 当地邮局检查邮件目的地并将其发送到正确国家/地区的邮局 (MTA)。
4. 邮局 (MTA) 将邮件递送到收件人邮箱 (MDA)。
5. 收件人 (MUA) 定期检查邮箱是否有新邮件，如果他们注意到有新邮件，就会接收它。

我们需要依赖电子邮件协议来与 MTA 和 MDA 进行通信，具体的协议是：

1. SMTP协议（简单邮件传输协议-Simple Mail Transfer Protocol)

2. POP3协议（邮局协议版本3-Post Office Protocol version 3) 或IMAP协议（Internet 消息访问协议-Internet Message Access Protocol)

简单邮件传输协议 (SMTP) 用于与 MTA 服务器进行通信。 因为 SMTP 使用明文，所有命令都是在没有加密的情况下发送的，所以我们可以使用基本的 Telnet 客户端连接到 SMTP 服务器并充当电子邮件客户端 (MUA) 发送消息。

SMTP 服务器默认侦听的端口为 25，为了查看与 SMTP 服务器的基本通信，我们使用 Telnet 连接到它，连接后，我们发出 `helo hostname` ，然后开始输入我们要发送的电子邮件。

```
pentester@TryHackMe$ telnet MACHINE_IP 25
Trying MACHINE_IP ...
Connected to MACHINE_IP.
Escape character is '^]'.
220 bento.localdomain ESMTP Postfix (Ubuntu)
helo telnet  #####
250 bento.localdomain
mail from:
250 2.1.0 Ok
rcpt to:
250 2.1.5 Ok
data
354 End data with .
subject: Sending email with Telnet
Hello Frank,
I am just writing to say hi!
.
250 2.0.0 Ok: queued as C3E7F45F06
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

输入helo telnet 之后，我们会使用 `mail from:` 以及 `rcpt to:` 表示发件人和收件人。 当我们开始发送电子邮件时，我们会使用命令 `data` 并输入我们要发送的具体的邮件消息，之后我们输入 `<CR><LF>.<CR><LF>` （或更简单地说是 `Enter . Enter` ），SMTP 服务器就会开始对邮件消息进行排队处理。

一般来说，我们不需要记住 SMTP 命令，上面的控制台输出旨在帮助更好地解释典型的邮件客户端在使用 SMTP 时所做的事情。

答题

回答以下问题

使用 AttackBox 终端，连接到目标 VM 的 SMTP 端口。你能得到的旗帜是什么？

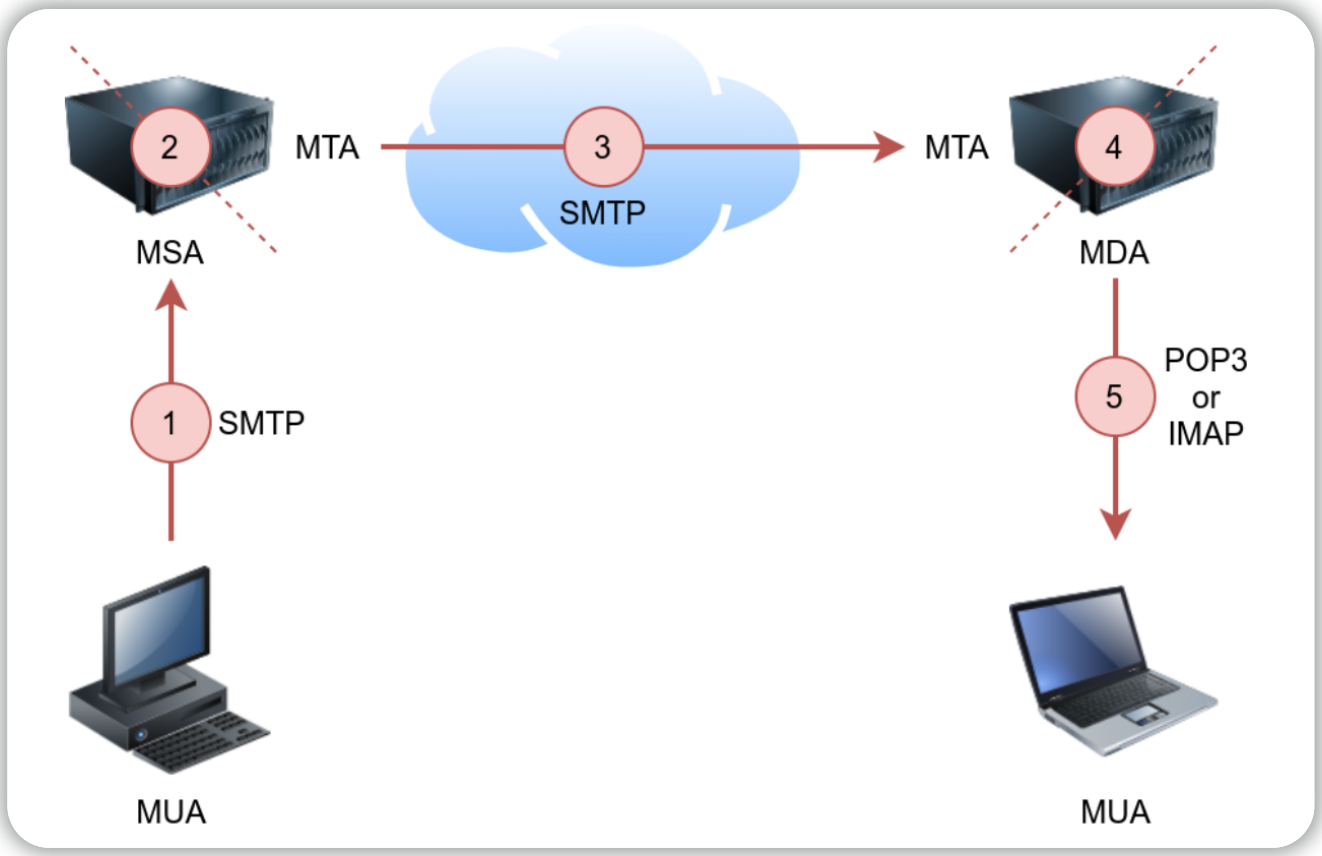
THM{5b31ddfc0c11d81eba776e983c35e9b5}

正确答案

```
root@ip-10-10-122-26:~# telnet 10.10.194.229 25
Trying 10.10.194.229...
Connected to 10.10.194.229.
Escape character is '^]'.
220 bento.localdomain ESMTP Postfix THM{5b31ddfc0c11d81eba776e983c35e9b5}
```

H2 POP3协议(Post Office Protocol 3)

POP3(邮局协议版本 3) 是用于从MDA (邮件投递代理) 服务器下载电子邮件的协议，如下图所示。邮件客户端可以连接到 POP3 服务器、验证、下载新的电子邮件，然后（可选地）删除它们。



下面的示例显示了通过 Telnet 客户端进行的 POP3 会话的过程。

首先，用户会使用 POP3 默认端口 110 连接到 POP3 服务器；

访问电子邮件消息需要身份验证，用户通过提供用户名 `USER frank` 和密码 `PASS D2xc9CgD` 来进行身份验证；

完成验证之后，使用命令 `STAT` ，我们能得到回复 `+OK 1 179` ;

根据 RFC 1939 ，对 `STAT` 的肯定响应的格式为 `+OK nn mm` ，其中 `nn` 是收件箱中的电子邮件数量， `mm` 是收件箱的大小，以八位字节（byte）为单位;

使用命令 `LIST` 会获得服务器上的新消息列表，使用命令 `RETR 1` 可以检索新消息列表中的第一条消息。

我们不需要特别记住这些命令，但是这些命令有助于加强我们对此类协议的理解。

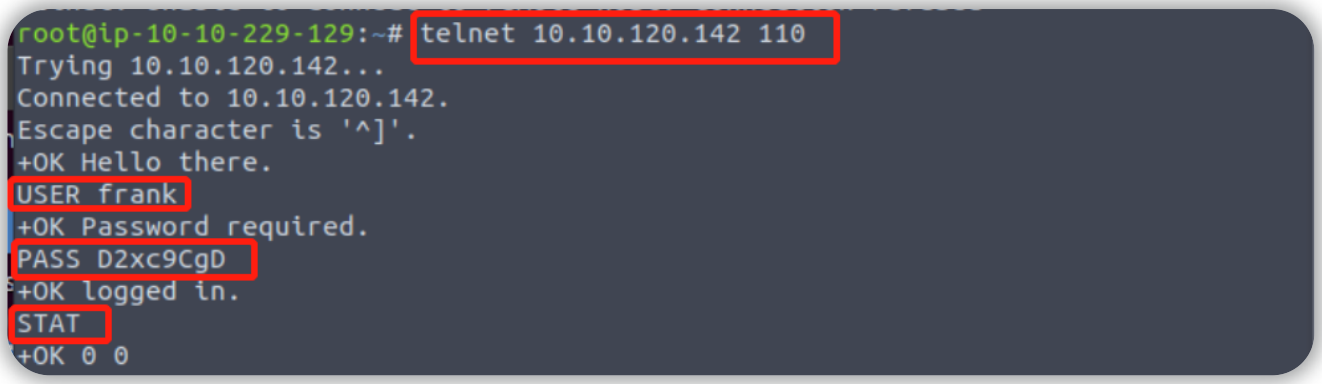
```
pentester@TryHackMe$ telnet MACHINE_IP 110
Trying 10.10.194.229 ...
Connected to MACHINE_IP.
Escape character is '^]'.
+OK MACHINE_IP Mail Server POP3 Wed, 15 Sep 2021 11:05:34 +0300
USER frank#####
+OK frank
PASS D2xc9CgD#####
+OK 1 messages (179) octets
STAT#####
+OK 1 179
LIST#####
+OK 1 messages (179) octets
1 179
.
RETR 1#####
+OK
From: Mail Server
To: Frank
subject: Sending email with Telnet
Hello Frank,
I am just writing to say hi!
.
QUIT
+OK MACHINE_IP closing connection
Connection closed by foreign host.
```

上面的示例显示命令将以明文形式发送，所以使用Telnet足以验证和检索电子邮件；由于用户名和密码都以明文形式发送，所以任何观察网络流量的第三方都可以窃取登录凭据。

通常，你的邮件客户端 (MUA) 将连接到 POP3 服务器 (MDA)，进行身份验证并下载邮件。尽管使用 POP3 协议的通信将隐藏在简洁的GUI界面后面，但仍会发出类似的命令，如上面的 Telnet 会话所示。

根据默认设置，邮件客户端在下载邮件后会将其删除，如果你希望从另一个邮件客户端再次下载该电子邮件，则可以在邮件客户端设置处更改默认行为；使用 POP3 通过多个客户端访问同一个邮件帐户通常不是很方便，因为可能会丢失已读和未读邮件的跟踪；所以为了使所有邮箱保持同步，我们需要考虑使用其他协议，例如 IMAP协议。

答题



H2 IMAP协议(Internet Message Access Protocol)

Internet 消息访问协议 (IMAP) 比 POP3 协议更复杂。 IMAP 能够使你的电子邮件在多个设备（和邮件客户端）之间保持同步，换句话说，如果你在智能手机上检查电子邮件时将电子邮件标记为已读，则该更改将保存在 IMAP 服务器 (MDA) 上，并会在你同步收件箱时复制该更改到你的笔记本电脑设备上。

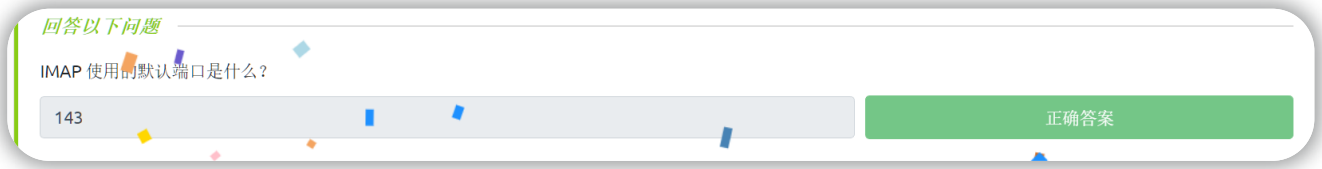
让我们看一下IMAP命令的示例：

在下面的控制台输出中，我们使用 Telnet 连接到 IMAP 服务器的默认端口143，然后使用 `LOGIN username password` 进行身份验证；IMAP 要求每个命令前面都有一个随机字符串，以便能够跟踪回复，所以我们可以在每个命令开头添加c1，然后添加c2，以此类推；我们可以使用 `LIST "" "*"` 列出我们的邮件文件夹，接着使用 `EXAMINE INBOX` 检查收件箱中是否有任何新邮件。

我们不需要记住这些命令，我们只是提供下面的示例，以生动地说明邮件客户端与 IMAP 服务器进行通信时发生的情况。

```
pentester@TryHackMe$ telnet MACHINE_IP 143
Trying MACHINE_IP ...
Connected to MACHINE_IP.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS ENABLE UTF8=ACCEPT]
Courier-IMAP ready. Copyright 1998-2018 Double Precision, Inc.  See COPYING for
distribution information.
c1 LOGIN frank D2xc9CgD
* OK [ALERT] Filesystem notification initialization error -- contact your mail
administrator (check for configuration errors with the FAM/Gamin library)
c1 OK LOGIN Ok.
c2 LIST "" "*"
* LIST (\HasNoChildren) "." "INBOX.Trash"
* LIST (\HasNoChildren) "." "INBOX.Drafts"
* LIST (\HasNoChildren) "." "INBOX.Templates"
* LIST (\HasNoChildren) "." "INBOX.Sent"
* LIST (\Unmarked \HasChildren) "." "INBOX"
c2 OK LIST completed
c3 EXAMINE INBOX
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS ()] No permanent flags permitted
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 631694851] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
c3 OK [READ-ONLY] Ok
c4 LOGOUT
* BYE Courier-IMAP server shutting down
c4 OK LOGOUT completed
Connection closed by foreign host.
```

很明显，IMAP协议是以明文形式发送登录凭据，正如我们在命令 `LOGIN frank D2xc9CgD` 中看到的那样，任何能够观察到网络流量的人都可以知道frank的用户名和密码。



H2 小结

本文涵盖了各种协议、它们的用法以及它们如何在幕后工作，在现实世界中攻击者对许多其他标准协议也会感兴趣，例如服务器消息块协议 (SMB)，它能够提供对网络之间文件和打印机的共享访问。 但是，本文仅旨在让你深入了解一些常见的协议以及它们是如何在幕后工作的；一篇文章甚至一个完整的知识模块都无法覆盖所有的网络协议。

最好能记住常用协议的默认端口号，下面是本文所涵盖的协议的摘要以及它们的默认端口号，按字母顺序排序。

Protocol	TCP Port	Application(s)	Data Security
FTP	21	File Transfer	Cleartext
HTTP	80	Worldwide Web	Cleartext
IMAP	143	Email (MDA)	Cleartext
POP3	110	Email (MDA)	Cleartext
SMTP	25	Email (MTA)	Cleartext
Telnet	23	Remote Access	Cleartext