

# Protocols and Servers

## Task 1 Introduction (Görev 1 Giriş)

Bu oda, kullanıcıya yaygın olarak kullanılan birkaç protokolü tanıtır:

- HTTP
- FTP
- POP3
- SMTP
- IMAP

Her protokolle ilgili her görev, düşük seviyede neler olduğunu anlamamıza yardımcı olmak için tasarlanacak ve genellikle zarif bir GUI (Grafik Kullanıcı Arayüzü) tarafından gizlenecektir. GUI istemcinizin kaputun altında ne yaptığını tam olarak anlamak için basit bir Telnet istemcisi kullanarak yukarıdaki protokolleri kullanarak "konuşacağız". Amacımız protokol komutlarını ezberlemek değil, çalışırken protokole daha yakından bakmaktır.

Ayrıca bazı güvensizlikleri de tartışıyoruz. Özellikle, açık metin olarak gönderilen şifrelere odaklanıyoruz.

Soru ⇒ Aşağıdaki görevleri yerine getirmeye devam ederken AttackBox'ı ve sanal makineyi başlatmanızı öneririz. Daha iyi uygulama ve öğrenme deneyimi için Telnet üzerinden farklı hizmetlere bağlanabilirsiniz.

Cevap ⇒ **Cevap Gerekmemektedir.**

## Task 2 Telnet (Görev 2 Telnet)

Telnet protokolü, başka bir bilgisayarın sanal terminaline bağlanmak için kullanılan bir uygulama katmanı protokolüdür. Telnet kullanarak, bir kullanıcı başka bir bilgisayarda oturum açabilir ve programları çalıştırmak, toplu işlemleri başlatmak ve sistem yönetimi görevlerini uzaktan gerçekleştirmek için terminaline (konsol) erişebilir.

Telnet protokolü nispeten basittir. Bir kullanıcı bağlandığında, kendisinden bir kullanıcı adı ve parola istenecektir. Doğru kimlik doğrulamasının ardından, kullanıcı uzak sistemin terminaline erişecektir. Ne yazık ki, Telnet istemcisi ve Telnet sunucusu arasındaki tüm bu iletişim şifrelenmez ve bu da saldırganlar için kolay bir hedef haline getirir.

Bir Telnet sunucusu, 23 numaralı bağlantı noktasında gelen bağlantıları dinlemek için Telnet protokolünü kullanır. (Lütfen Telnet bağlantı noktasının hedef VM'de açık olmadığını unutmayın.) Aşağıda gösterilen örneği ele alalım. Bir kullanıcı Telnet sunucusu olan telnetd'ye bağlanıyor. Adımlar aşağıdaki gibidir:

1. İlk olarak, kullanıcı adını (username) girmesi istenir. Kullanıcının frank girdiğini görebiliriz.
2. Ardından, kendisinden D2xc9CgD şifresi istenir. Parola ekranda gösterilmez; ancak, gösterim amacıyla aşağıda gösteriyoruz.
3. Sistem giriş bilgilerini kontrol ettiğinde, bir karşılama mesajı ile karşılaşılır.
4. Ve uzak sunucu ona bir komut istemi verir, frank@bento:~\$. \$ işareti bunun bir kök terminal olmadığını gösterir.

```
pentester@TryHackMe$ telnet MACHINE_IPTrying 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.

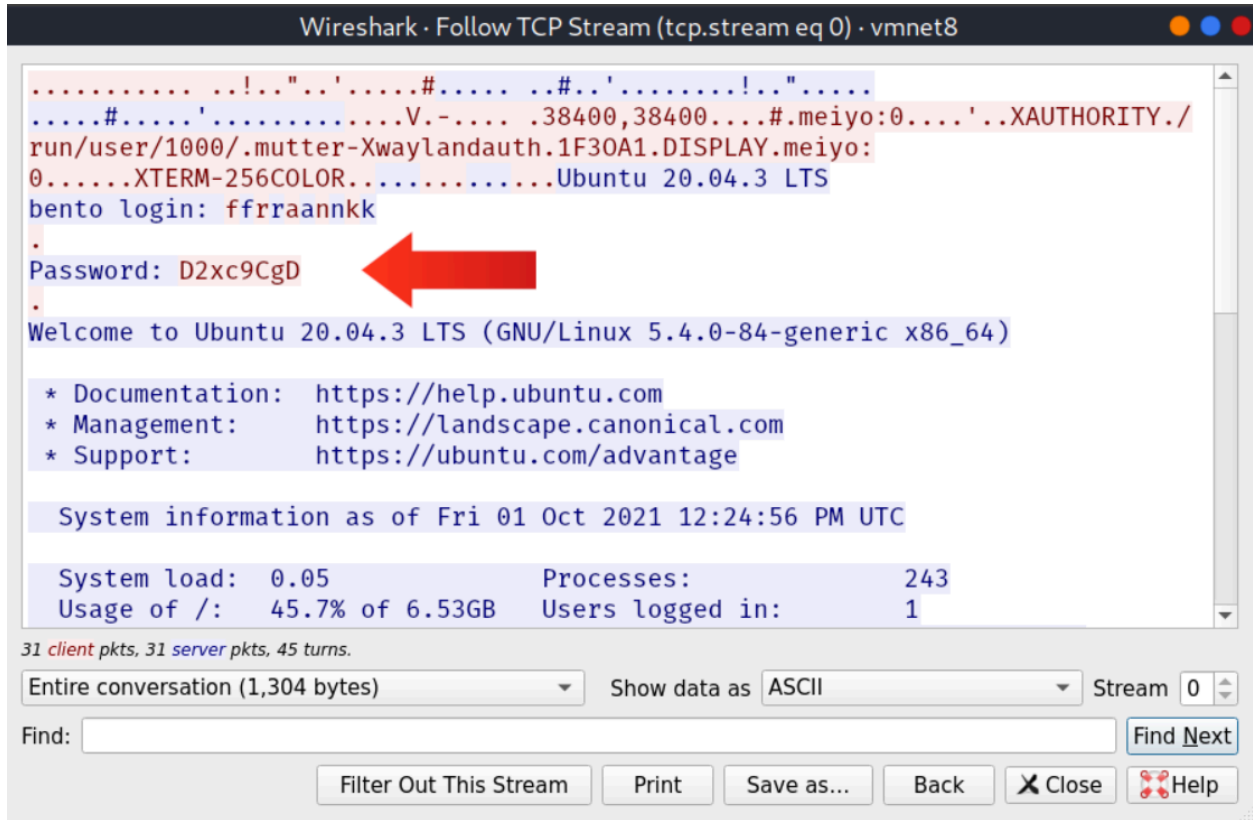
\*\*\* System restart required \*\*\*

Last login: Fri Oct 1 12:17:25 UTC 2021 from meiyo on pts/3

You have mail.

frank@bento:~\$

Telnet uzaktaki sistemin terminaline kısa sürede erişmemizi sağlasa da, tüm veriler açık metin olarak gönderildiği için uzaktan yönetim için güvenilir bir protokol değildir. Aşağıdaki şekilde, Telnet tarafından oluşturulan trafiği yakaladık ve şifreyi bulmak çok kolaydı. Aşağıdaki şekil bilgisayarımız ve uzaktaki sistem arasında değiş tokuş edilen ASCII verilerini göstermektedir. Kırmızı renkteki metin bizim uzak sisteme gönderdiğimiz metin, mavi renkteki metin ise uzak sistemin gönderdiği metindir. Kullanıcı adının nasıl geri gönderildiğine dikkat edin (terminalimizde görüntülemek için bize yankılandı); ancak şifre gönderilmedi. Başka bir deyişle, eğer birisi bizi yazarken izliyorsa, ekranda parola karakterlerini göremeyecektir.



Wireshark · Follow TCP Stream (tcp.stream eq 0) · vmnet8

```
.....!..".'.#.....#..'.!..".....  
.....#.....'.V.-.....38400,38400.....#.meiyo:0....'..XAUTHORITY./  
run/user/1000/.mutter-Xwaylandauth.1F30A1.DISPLAY.meiyo:  
0.....XTerm-256COLOR.....Ubuntu 20.04.3 LTS  
bento login: ffrannkk  
.  
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
```

31 client pkts, 31 server pkts, 45 turns.

Entire conversation (1,304 bytes) Show data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

Telnet artık güvenli bir seçenek olarak görülmemektedir, özellikle de ağ trafiğinizi yakalayan herhangi biri kullanıcı adlarınızı ve şifrelerinizi keşfedebilecek ve bu da onlara uzaktaki sisteme erişim sağlayacaktır. Güvenli alternatif, bir sonraki odada sunacağımız SSH'dir.

Soru ⇒ Varsayılan parametrelerle telnet komutu hangi porta bağlanmaya çalışacaktır?

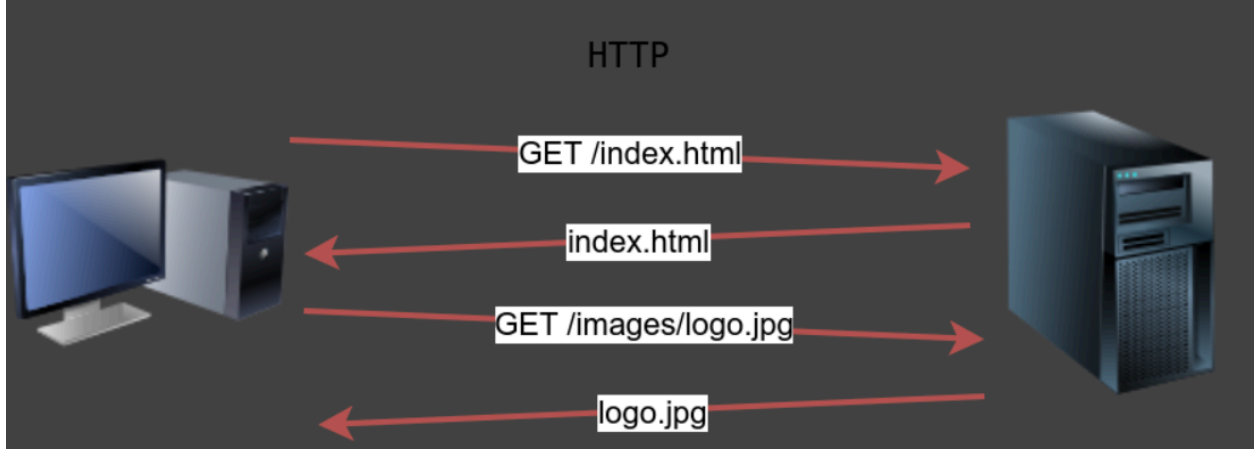
Cevap ⇒ 23

### Task 3 Hypertext Transfer Protocol (HTTP) (Görev 3 Köprü Metni Aktarım Protokolü (HTTP))

Köprü Metni Aktarım Protokolü (HTTP) web sayfalarını aktarmak için kullanılan protokoldür. Web tarayıcınız web sunucusuna bağlanır ve diğer dosyaların yanı sıra HTML sayfaları ve resimler istemek, form göndermek ve çeşitli dosyalar

yüklemek için HTTP kullanır. World Wide Web'e (WWW) her göz attığınızda, kesinlikle HTTP protokolünü kullanıyorsunuzdur.

Aşağıdaki resim, web sunucusunun sağladığı index.html HTML sayfasını talep eden bir istemciyi göstermektedir. Ardından istemci logo.jpg adlı bir resim talep eder ve web sunucusu bunu gönderir.



HTTP verileri açık metin (şifrelenmemiş) olarak gönderir ve alır; bu nedenle, bir web sunucusuyla iletişim kurmak ve bir "web tarayıcısı" olarak hareket etmek için Telnet (veya Netcat) gibi basit bir araç kullanabilirsiniz. Temel fark, HTTP ile ilgili komutları web tarayıcısının sizin için yapması yerine sizin girmeniz gerektiğidir.

Aşağıdaki örnekte, bir web sunucusundan bir sayfayı nasıl isteyebileceğimizi göreceğiz; dahası, web sunucusu sürümünü keşfedeceğiz. Bunu gerçekleştirmek için Telnet istemcisini kullanacağız. Bunu seçtik çünkü Telnet basit bir protokoldür; ayrıca iletişim için açık metin kullanır. Web sunucusundan bir dosya istemek için bir web tarayıcısı yerine telnet kullanacağız. Adımlar aşağıdaki gibi olacaktır:

1. İlk olarak, telnet MACHINE\_IP 80 kullanarak 80 numaralı bağlantı noktasına bağlanıyoruz.
2. Ardından, index.html sayfasını almak için GET /index.html HTTP/1.1 veya varsayılan sayfayı almak için GET / HTTP/1.1 yazmamız gerekir.
3. Son olarak, host için host: telnet gibi bir değer girmeniz ve Enter/Return tuşuna iki kez basmanız gerekir.

Aşağıdaki konsol çıktısında, istenen sayfayı genellikle web tarayıcısı tarafından görüntülenmeyen bir bilgi hazinesiyle birlikte kurtarabiliriz. İstedığımız sayfa

bulunamazsa 404 hatası alırız.

```
pentester@TryHackMe$ telnet MACHINE_IP 80Trying 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>
```

Yukarıdaki çıktıda özellikle ilgi çekici olan, kullanıcının ihtiyaç duyduğu sayfayı almak için yalnızca birkaç komut yazması gerektiğidir: GET /index.html HTTP/1.1 ve ardından host: telnet.

HTTP protokolünü kullanmak için bir HTTP sunucusuna (web sunucusu) ve bir HTTP istemcisine (web tarayıcısı) ihtiyacımız vardır. Web sunucusu, talep eden

web tarayıcısına belirli bir dosya kümesi "sunacaktır".

HTTP sunucuları için üç popüler seçenek vardır:

- Apache
- Internet Information Services (IIS)
- nginx

Apache ve Nginx ücretsiz ve açık kaynaklı yazılımlardır. Ancak IIS kapalı kaynak kodlu bir yazılımdır ve lisans için ödeme yapılmasını gerektirir.

Birçok web tarayıcısı mevcuttur. Bu yazının yazıldığı sırada en popüler web tarayıcıları şunlardır:

- Chrome by Google
- Edge by Microsoft
- Firefox by Mozilla
- Safari by Apple.

Web tarayıcılarının kurulumu ve kullanımı genellikle ücretsizdir; ayrıca, teknoloji devleri tarayıcıları için daha yüksek bir pazar payı için savaşırlar.

Soru ⇒ Ekli sanal makineyi başlatın. AttackBox terminalinden, Telnet kullanarak MACHINE\_IP 80'e bağlanın ve flag.thm dosyasını alın. Ne içeriyor?

Cevap ⇒ `THM{e3eb0a1df437f3f97a64aca5952c8ea0}`

## **Task 4 File Transfer Protocol (FTP) (Görev 4 Dosya Aktarım Protokolü (FTP))**

Dosya Aktarım Protokolü (FTP), farklı sistemlere sahip farklı bilgisayarlar arasında dosya aktarımını verimli hale getirmek için geliştirilmiştir.

FTP ayrıca verileri açık metin olarak gönderir ve alır; bu nedenle, bir FTP sunucusuyla iletişim kurmak ve bir FTP istemcisi olarak hareket etmek için Telnet (veya Netcat) kullanabiliriz. Aşağıdaki örnekte, aşağıdaki adımları gerçekleştirdik:

1. Bir Telnet istemcisi kullanarak bir FTP sunucusuna bağlandık. FTP sunucuları varsayılan olarak 21 numaralı bağlantı noktasını dinlediğinden, Telnet istemcimize varsayılan Telnet bağlantı noktası yerine 21 numaralı bağlantı noktasına bağlanmayı denemesini belirtmemiz gerekiyordu.
2. Kullanıcı adını USER frank komutu ile sağlamamız gerekiyordu.
3. Daha sonra PASS D2xc9CgD komutu ile şifreyi girdik.
4. Doğru kullanıcı adı ve şifreyi verdiğimiz için giriş yaptık.

STAT gibi bir komut bazı ek bilgiler sağlayabilir. SYST komutu hedefin Sistem Türünü gösterir (bu durumda UNIX). PASV modu pasif olarak değiştirir. FTP için iki mod olduğunu belirtmek gerekir:

- Aktif: Aktif modda, veriler FTP sunucusunun 20 numaralı portundan kaynaklanan ayrı bir kanal üzerinden gönderilir.
- Pasif: Pasif modda, veriler bir FTP istemcisinin 1023 numaralı portun üzerindeki portundan kaynaklanan ayrı bir kanal üzerinden gönderilir.

TYPE A komutu dosya aktarım modunu ASCII olarak değiştirirken, TYPE I dosya aktarım modunu binary olarak değiştirir. Ancak, Telnet gibi basit bir istemci kullanarak dosya aktaramayız çünkü FTP dosya aktarımı için ayrı bir bağlantı oluşturur.

```
pentester@TryHackMe$ telnet MACHINE_IP 21Trying 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

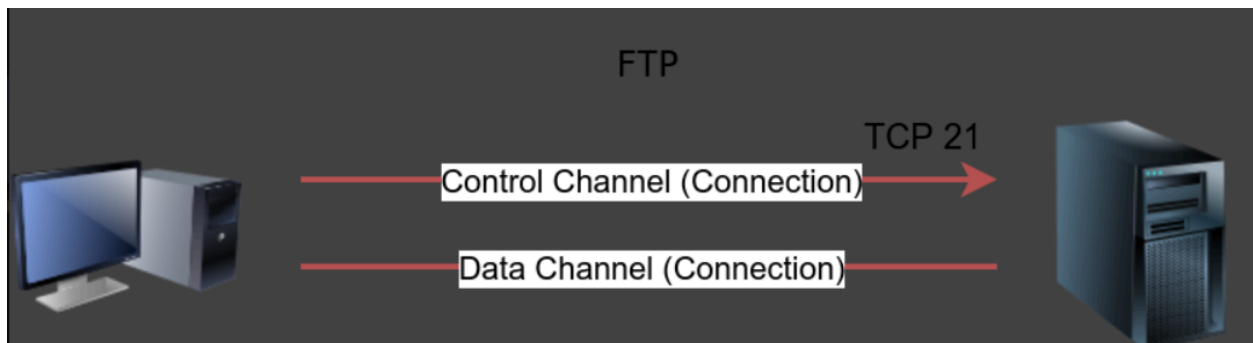
211 End of status

QUIT

221 Goodbye.

Connection closed by foreign host.

Aşağıdaki resim gerçek bir dosya transferinin FTP kullanılarak nasıl gerçekleştirileceğini göstermektedir. Bu şekilde işleri basit tutmak için, sadece FTP istemcisinin varsayılan olarak 21 numaralı bağlantı noktasını dinleyen bir FTP sunucusuna bağlantı başlatacağı gerçeğine odaklanalım. Tüm komutlar kontrol kanalı üzerinden gönderilecektir. İstemci bir dosya talep ettiğinde, aralarında başka bir TCP bağlantısı kurulacaktır. (Veri bağlantısı/kanalı kurmanın ayrıntıları bu odanın kapsamı dışındadır).



FTP üzerinden veri aktarımının karmaşıklığını göz önünde bulundurarak, bir metin dosyasını indirmek için gerçek bir FTP istemcisi kullanalım. Dosyayı almak için sadece az sayıda komuta ihtiyacımız var. Başarılı bir şekilde oturum açtıktan sonra,

çeşitli FTP komutlarını çalıştırmak için ftp> FTP komut istemini alırız. Dosyaları listelemek ve dosya adını öğrenmek için ls kullandık; daha sonra, bir metin dosyası olduğu için (ikili değil) ascii'ye geçtik. Son olarak get FILENAME, istemci ve sunucunun dosya aktarımı için başka bir kanal kurmasını sağladı.

```
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 sunucuları ve FTP istemcileri FTP protokolünü kullanır. FTP dosya sunucunuzu barındırmak istiyorsanız, aralarından seçim yapabileceğiniz çeşitli FTP sunucu yazılımları vardır. FTP sunucu yazılımı örnekleri şunları içerir:

- vsftpd

- ProFTPD
- uFTP

FTP istemcileri için, Linux sistemlerinde yaygın olarak bulunan konsol FTP istemcisine ek olarak, FileZilla gibi GUI'li bir FTP istemcisi kullanabilirsiniz. Bazı web tarayıcıları da FTP protokolünü destekler.

FTP, oturum açma kimlik bilgilerini komutlar ve dosyalarla birlikte açık metin olarak gönderdiğinden, FTP trafiği saldırganlar için kolay bir hedef olabilir.

Soru ⇒ Bir FTP istemcisi kullanarak VM'ye bağlanın ve bayrak dosyasını kurtarmayı deneyin. Bayrak nedir?

- Username: frank
- Password: D2xc9CgD

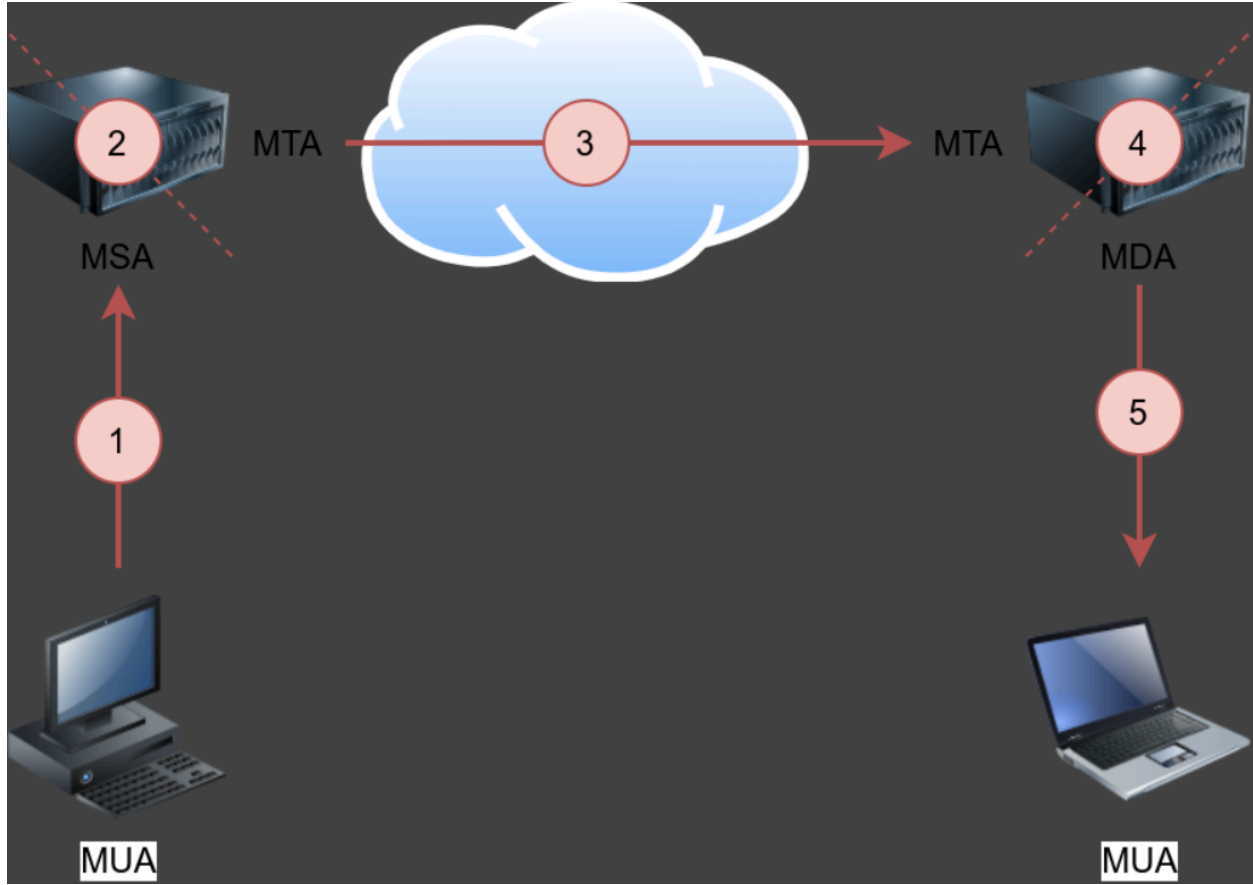
Cevap ⇒ `THM{364db6ad0e3ddfe7bf0b1870fb06fbdf}`

## **Task 5 Simple Mail Transfer Protocol (SMTP) (Görev 5 Basit Posta Aktarım Protokolü (SMTP))**

E-posta, İnternet üzerinde en çok kullanılan hizmetlerden biridir. E-posta sunucuları için çeşitli yapılandırmalar vardır; örneğin, yerel kullanıcıların internete erişimi olmadan birbirleriyle e-posta alışverişi yapmalarına izin vermek için bir e-posta sistemi kurabilirsiniz. Ancak, farklı e-posta sunucularının İnternet üzerinden bağlandığı daha genel bir kurulumu ele alacağız.

İnternet üzerinden e-posta iletimi aşağıdaki bileşenleri gerektirir:

1. Mail Submission Agent (MSA) (Posta Gönderme Aracısı (MSA))
2. Mail Transfer Agent (MTA) (Posta Aktarma Aracısı (MTA) )
3. Mail Delivery Agent (MDA) (Posta Teslim Aracısı (MDA))
4. Mail User Agent (MUA) (Posta Kullanıcı Aracısı (MUA))



Yukarıdaki dört terim şifreli görünebilir, ancak göründüklerinden daha basittirler. Bu terimleri aşağıdaki şekli kullanarak açıklayacağız.

1. Bir Posta Kullanıcı Aracısı (MUA) veya basitçe bir e-posta istemcisi, gönderilecek bir e-posta iletilisine sahiptir. MUA, mesajını göndermek için bir Posta Gönderme Aracısına (MSA) bağlanır.
2. MSA mesajı alır, genellikle aynı sunucuda barındırılan Posta Aktarım Aracısı (MTA) sunucusuna aktarmadan önce herhangi bir hata olup olmadığını kontrol eder.
3. MTA e-posta mesajını alıcının MTA'sına gönderir. MTA ayrıca Posta Gönderme Aracısı (MSA) olarak da işlev görebilir.
4. Tipik bir kurulumda MTA sunucusu aynı zamanda Posta Dağıtım Aracısı (MDA) olarak da işlev görür.
5. Alıcı, e-posta istemcisini kullanarak e-postasını MDA'dan alacaktır.

Yukarıdaki adımlar kafa karıştırıcı geliyorsa, aşağıdaki benzetmeyi düşünün:

1. Siz (MUA) posta göndermek istiyorsunuz.
2. Postane çalışanı (MSA), yerel postaneniz (MTA) postayı kabul etmeden önce herhangi bir sorun olup olmadığını kontrol eder.
3. Yerel postane posta hedefini kontrol eder ve doğru ülkedeki postaneye (MTA) gönderir.
4. Postane (MTA) postayı alıcı posta kutusuna (MDA) teslim eder.
5. Alıcı (MUA) düzenli olarak posta kutusunda yeni posta olup olmadığını kontrol eder. Yeni postayı fark ederler ve alırlar.

Aynı şekilde, bir HTTP sunucusuyla iletişim kurmak için bir protokol izlememiz ve bir MTA ve bir MDA ile konuşmak için e-posta protokollerine güvenmemiz gerekir. Protokoller şunlardır:

1. Basit Posta Aktarım Protokolü (SMTP)
2. Postane Protokolü sürüm 3 (POP3) veya İnternet İleti Erişim Protokolü (IMAP)

Bu görevde SMTP'yi açıklıyoruz ve sonraki iki görevde POP3 ve IMAP'i detaylandırıyoruz.

Basit Posta Aktarım Protokolü (SMTP) bir MTA sunucusuyla iletişim kurmak için kullanılır. SMTP, tüm komutların şifrelenmeden gönderildiği açık metin kullandığından, bir SMTP sunucusuna bağlanmak ve bir mesaj gönderen bir e-posta istemcisi (MUA) gibi davranmak için temel bir Telnet istemcisi kullanabiliriz.

SMTP sunucusu varsayılan olarak 25 numaralı bağlantı noktasını dinler. Bir SMTP sunucusuyla temel iletişimi görmek için, ona bağlanmak üzere Telnet kullandık. Bağlandıktan sonra, helo ana bilgisayar adını veriyoruz ve ardından e-postamızı yazmaya başlıyoruz.

```
pentester@TryHackMe$ telnet MACHINE_IP 25Trying 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.
```

Helo'dan sonra, göndereni ve alıcıyı belirtmek için mail from:, rcpt to: komutlarını veriyoruz. E-posta mesajımızı gönderirken, data komutunu veririz ve mesajımızı yazarız. <CR><LF>.<CR><LF> (ya da daha basit bir ifadeyle Enter . Enter) komutunu veririz. SMTP sunucusu şimdi mesajı kuyruğa alır.

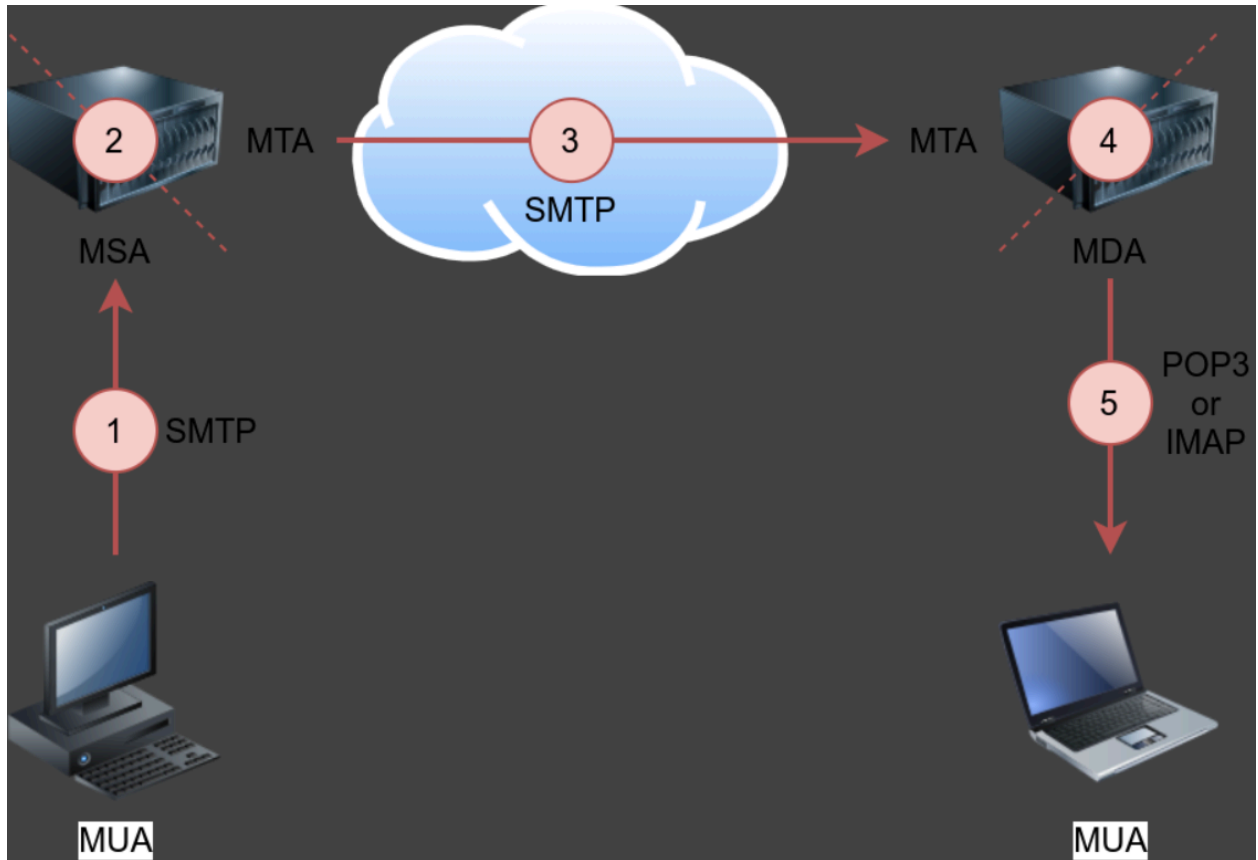
Genel olarak, SMTP komutlarını ezberlememize gerek yoktur. Yukarıdaki konsol çıktısı, tipik bir posta istemcisinin SMTP kullandığında ne yaptığını daha iyi açıklamaya yardımcı olmayı amaçlamaktadır.

Soru ⇒ AttackBox terminalini kullanarak hedef VM'nin SMTP portuna bağlanın. Alabileceğiniz bayrak nedir?

Cevap ⇒ **THM{5b31ddfc0c11d81eba776e983c35e9b5}**

## **Task 6 Post Office Protocol 3 (POP3) (Görev 6 Postane Protokolü 3 (POP3))**

Postane Protokolü sürüm 3 (POP3), aşağıdaki şekilde gösterildiği gibi, e-posta iletilerini bir Posta Dağıtım Aracısı (MDA) sunucusundan indirmek için kullanılan bir protokoldür. Posta istemcisi POP3 sunucusuna bağlanır, kimlik doğrulaması yapar, (isteğe bağlı olarak) silmeden önce yeni e-posta iletilerini indirir.



Aşağıdaki örnek, bir POP3 oturumunun Telnet istemcisi aracılığıyla gerçekleştirilmesi durumunda nasıl görüneceğini göstermektedir. İlk olarak, kullanıcı POP3 sunucusuna POP3 varsayılan bağlantı noktası 110'dan bağlanır. E-posta mesajlarına erişmek için kimlik doğrulama gereklidir; kullanıcı USER frank kullanıcı adını ve PASS D2xc9CgD şifresini girerek kimlik doğrulaması yapar. STAT komutunu kullanarak +OK 1 179 yanıtını alırız; RFC 1939'a göre, STAT'a olumlu bir yanıt +OK nn mm biçimindedir; burada nn gelen kutusundaki e-posta iletilerinin sayısıdır ve mm gelen kutusunun sekizli (bayt) cinsinden boyutudur. LIST komutu sunucudaki yeni mesajların bir listesini sağlar ve RETR 1 listedeki ilk mesajı alır. Bu komutları ezberlemekle ilgilenmemize gerek yok; ancak, bu tür protokol anlayışımızı güçlendirmek yararlı olacaktır.

```
pentester@TryHackMe$ telnet MACHINE_IP 110Trying MACHINE_IP...
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.
```

Yukarıdaki örnek, komutların açık metin olarak gönderildiğini göstermektedir. Telnet kullanmak kimlik doğrulaması yapmak ve bir e-posta mesajı almak için yeterliydi. Kullanıcı adı ve parola açık metin olarak gönderildiğinden, ağ trafiğini izleyen herhangi bir üçüncü taraf oturum açma kimlik bilgilerini çalabilir.

Genel olarak, posta istemciniz (MUA) POP3 sunucusuna (MDA) bağlanacak, kimlik doğrulaması yapacak ve mesajları indirecektir. POP3 protokolünü kullanan iletişim şık bir arayüzün arkasına gizlenecek olsa da, yukarıdaki Telnet oturumunda gösterildiği gibi benzer komutlar verilecektir.

Varsayılan ayarlara göre, posta istemcisi posta iletisini indirdikten sonra siler. E-postaları başka bir posta istemcisinden tekrar indirmek isterseniz, varsayılan davranış posta istemcisi ayarlarından değiştirilebilir. POP3 kullanarak aynı posta hesabına birden fazla istemci üzerinden erişmek, okunan ve okunmayan iletilerin izini kaybedeceğinden genellikle çok uygun değildir. Tüm posta kutularını



senkronize tutmak için IMAP gibi diğer protokolleri göz önünde bulundurmamız gerekir.

Sorular

Soru ⇒ POP3 bağlantı noktasından VM'ye (MACHINE\_IP) bağlanın. Kullanıcı adı frank ve şifre D2xc9CgD kullanarak kimlik doğrulaması yapın. STAT'a aldığınız yanıt nedir?

Cevap ⇒ +OK 0 0

Soru ⇒ MACHINE\_IP üzerinde POP3 aracılığıyla indirilebilecek kaç e-posta iletisi var?

Cevap ⇒ 0

## **Task 7 Internet Message Access Protocol (IMAP) (Görev 7 İnternet İleti Erişim Protokolü (IMAP))**

İnternet İleti Erişim Protokolü (IMAP) POP3'ten daha karmaşıktır. IMAP, e-postanızın birden fazla cihaz (ve posta istemcisi) arasında senkronize edilmesini mümkün kılar. Başka bir deyişle, akıllı telefonunuzda e-postanızı kontrol ederken bir e-posta iletisini okundu olarak işaretlerseniz, bu değişiklik IMAP sunucusuna (MDA) kaydedilir ve gelen kutunuzu senkronize ettiğinizde dizüstü bilgisayarınıza kopyalanır.

Şimdi örnek IMAP komutlarına bir göz atalım. Aşağıdaki konsol çıktısında, IMAP sunucusunun varsayılan bağlantı noktasına bağlanmak için Telnet kullanıyoruz ve ardından LOGIN kullanıcı adı parolasını kullanarak kimlik doğrulaması yapıyoruz. IMAP, yanıtı izleyebilmek için her komuttan önce rastgele bir dize gelmesini gerektirir. Bu yüzden c1'i ekledik, sonra c2'yi ve bu şekilde devam ettik. Daha sonra LIST "" "\*" kullanarak posta klasörlerimizi listeledik ve EXAMINE INBOX kullanarak gelen kutusunda yeni mesaj olup olmadığını kontrol ettik. Bu komutları ezberlememize gerek yok; ancak, posta istemcisi bir IMAP sunucusuyla iletişim kurduğunda neler olduğuna dair canlı bir görüntü vermek için aşağıdaki örneği veriyoruz.

```
pentester@TryHackMe$ telnet MACHINE_IP 143Trying MACHINE_IP...
Connected to MACHINE_IP.
Escape character is '^'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=OR
DEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNIO
N STARTTLS ENABLE UTF8=ACCEPT] Courier-IMAP ready. Copyright 1998-2
018 Double Precision, Inc. See COPYING for distribution information.
c1 LOGIN frank D2xc9CgD
* OK [ALERT] Filesystem notification initialization error -- contact your mail ad
ministrator (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.
```

LOGIN frank D2xc9CgD komutunda görebileceğimiz gibi, IMAP'in oturum açma kimlik bilgilerini açık metin olarak gönderdiği açıktır. Ağ trafiğini izleyen herhangi biri Frank'in kullanıcı adını ve şifresini öğrenebilir.

Soru ⇒ IMAP tarafından kullanılan varsayılan bağlantı noktası nedir?

Cevap ⇒ 143

## Task 8 Summary (Görev 8 Özet)

Bu oda, çeşitli protokolleri, kullanımlarını ve kaputun altında nasıl çalıştıklarını ele aldı. Diğer birçok standart protokol saldırganların ilgisini çekmektedir. Örneğin, Sunucu Mesaj Bloğu (SMB) ağlar arasında dosya ve yazıcılara paylaşılan erişim sağlar ve heyecan verici bir hedef olabilir. Ancak, bu oda size sadece birkaç yaygın protokol ve bunların nasıl çalıştığı hakkında iyi bir bilgi vermeyi amaçlamaktadır. Tek bir oda ya da tam bir modül bile tüm ağ protokollerini kapsayamaz.

Yaygın protokoller için varsayılan bağlantı noktası numarasını hatırlamak iyidir. Aşağıda, ele aldığımız protokollerin varsayılan bağlantı noktası numaralarıyla birlikte alfabetik olarak sıralanmış bir özeti bulunmaktadır.

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

Bu modülün bir sonraki bölümünde, bu protokollere ve sunuculara yönelik çeşitli saldırıları ve bunları hafifletme adımlarını öğreneceğiz.

Soru ⇒ Böylece Ağ Güvenliği modülünün yedinci odasını tamamlamış oldunuz. İlgili saldırılar ve hafifletmeler hakkında bilgi edinmek için lütfen Protokoller ve Sunucular 2 odasına geçin.

Cevap ⇒ Cevap Gerekmemektedir.