

Universidad Nacional Autónoma de México
Facultad de Ciencias
Criptografía y Seguridad

Tarea Moral 4

García Ponce José Camilo - 319210536

1. Investigación

Email Spoofing es el acto de enviar correos electrónicos con una dirección falsa de quien envía el correo, esto es usado debido a que algunos protocolos de correos no puede verificar la fuente de los correos y por lo tanto este tipo de acciones se usan para generar spam o otras actividades no éticas. Es una forma de robo de identidad.

Funciona debido a que al enviar los correos ponen algo en las secciones de **para quien** y **de para te quien** (como si fuera una carta donde pones que otra persona la envía), entonces cuando le llega el correo al destinatario, el programa de correos le estos parámetros y si fueron cambiados de manera exitosa, se mostrara como que otra persona envió el correo

Esta practica tiene varios riesgos

- Ocultar la identidad
Al ocultar la identidad de quien envía el correo se puede hacer pasar por empresas o gente de confianza para así poder hacer creer a las víctimas que les llega un correo legítimo
- Evitar llegar a la bandeja de spam
Como aparece que otra persona envió el correo entonces es una manera de evitar la bandeja de spam, ya que pueden usar diferentes nombres o direcciones que no estén registradas como spam
- Arruinar la imagen de personas Esto puede pasar al enviar contenido malicioso, desinformar, mentiras o otras formas de agresiones pero como se hace creer que lo envió otra persona, entonces creemos que la persona que se suplanta no es tan buena o nos quiere hacer daño y así causando desconfianza y una mala imagen
- Obtener información personal Si los correos enviados tienen ransomware, puede pasar que se robe la información que el destinatario tenga en su dispositivo
- Estafas También es posible que se realicen estafas como pedir dinero, información bancaria o información personal al hacerse pasar por personas de confianza, instituciones, entre otros.

Fuente

2. Anotaciones y proceso de resolver

Lo primero fue importar la clave del ayudante con el comando `gpg --import IvanGalindo_pub.asc`

```
camilo@wowi:~/Downloads$ gpg --import IvanGalindo_pub.asc
gpg: key DFC093385F70B46A: "Ivan Galindo <ivangalindo@ciencias.unam.mx>" not changed
gpg: Total number processed: 1
gpg:          unchanged: 1
camilo@wowi:~/Downloads$
```

Luego revisamos que se importo bien con `gpg --list-keys`

```
camilo@wowi:~$ gpg --list-keys
[keyboxd]
-----
pub   rsa3040 2024-01-20 [SC]
      53E7B7C4924631944330B906E672BF2C128DC854
uid           [ultimate] Camilo (llaveInt1) <jcg191224@gmail.com>
sub   rsa3040 2024-01-20 [E]

pub   rsa4096 2024-08-13 [SC]
      74F151A87ED481BACDA8A58C9A7DF21D7EEA4CA2
uid           [ unknown] Luis Sebastian Arrieta Mancera (Practica 1) <sebastian_
luis@ciencias.unam.mx>
sub   rsa4096 2024-08-13 [E]

pub   rsa4096 2023-08-29 [SC]
      A70E2A4E10915788A9ACFD5ADFC093385F70B46A
uid           [ unknown] Ivan Galindo <ivangalindo@ciencias.unam.mx>
sub   rsa4096 2023-08-29 [E]
```

Después creamos el mensaje a enviar

```
camilo@wowi:~$ echo "¡Hola! De parte de Camilo reclamo la tarea moral." > mensaj
e.tx
camilo@wowi:~$
```

Y encriptamos el mensaje con la clave publica del ayudante con el comando `gpg --encrypt --armor -r ivangalindo@ciencias.unam.mx mensaje.tx`

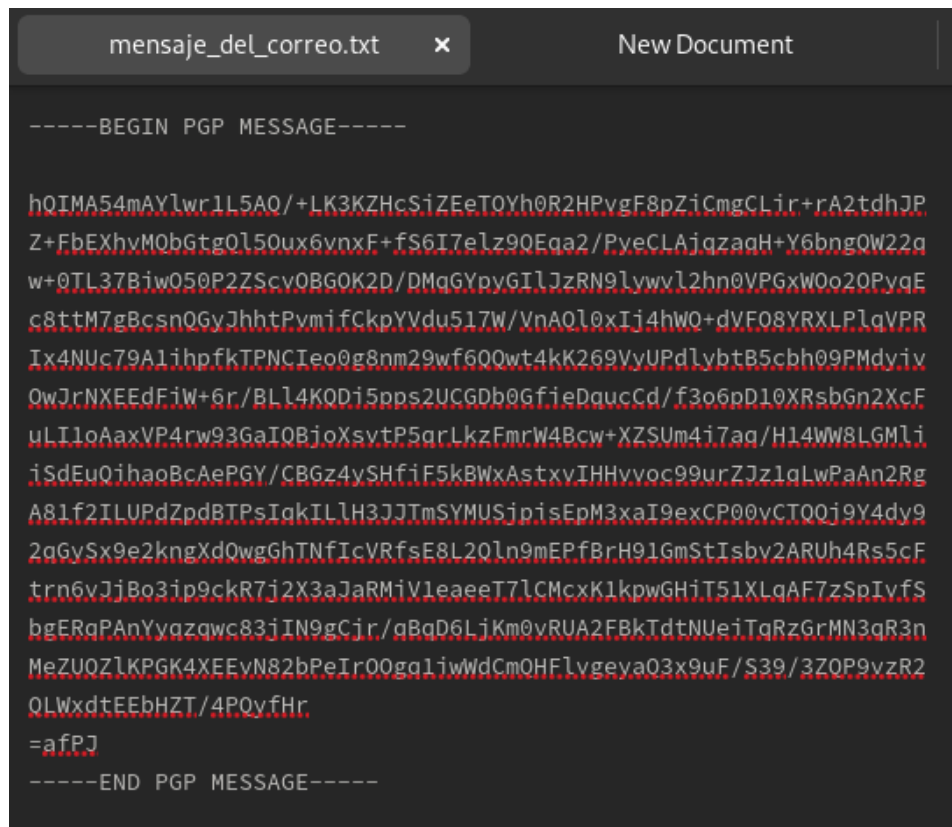
```
camilo@wowi:~$ gpg --encrypt --armor -r ivangalindo@ciencias.unam.mx mensaje.tx
gpg: 9E26018970AF52F9: There is no assurance this key belongs to the named user

sub   rsa4096/9E26018970AF52F9 2023-08-29 Ivan Galindo <ivangalindo@ciencias.unam
.mx>
Primary key fingerprint: A70E 2A4E 1091 5788 A9AC  FD5A DFC0 9338 5F70 B46A
Subkey fingerprint: B818 A984 15AA DC00 5F3B  5674 9E26 0189 70AF 52F9

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
camilo@wowi:~$
```

Copie el contenido y lo puse en un archivo de texto



```

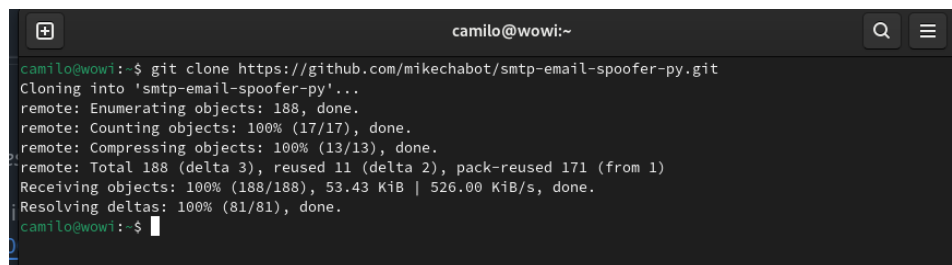
-----BEGIN PGP MESSAGE-----

h0IMA54mAYlwr1L5A0/+LK3KZHcSiZEeTOYh0R2HPvgF8pZiCmgCLir+rA2tdhJP
Z+FbEXhVMOBgGtg0L50ux6vnxF+fS6I7eLz90Eqa2/PyeCLAJqzaqH+Y6bng0W22a
w+0TL37Biw050P2ZScv0BGOK2D/DMqGYpyGILJzRN9lywv12hn0VPGxW0o20PyqE
c8ttM7gBcsn0GyJhhtPvmifCkpYVdu517W/VnA010xIj4hW0+dVF08YRXLP1qVPR
Ix4NUc79A1ihpfkTPNCIeo0g8nm29wf600wt4kK269VyUPdlybtB5cbh09PMdyiv
OwJrNXEEdFiW+6r/BLl4KQDi5pps2UCGDb0GfjeDaucCd/f3o6pD10XRsbGn2XcF
uLIloAaxVP4rw93GaIOBjoxsvtP5qrLkzFmrW4Bcw+XZSU4i7aq/H14WW8LGMli
iSdEuQihaoBcAePGY/CBGz4ySHfiF5kBWxAstxvIHHvvoc99urZJz1qLwPaAn2Rg
A81f2ILUPdZpdBTPsIakILH3JJTmSYMUSjipisEpM3xaI9exCP00vCT00j9Y4dy9
2qGySx9e2kngXdQwgGhTNfIcVRfsE8L20ln9mEPfBrH91GmStIsby2ARUh4Rs5cF
trn6vJiBo3ip9ckR7i2X3aJaRMiV1eaeT7lCMcxK1kpwGHiT51XLqAF7zSpIvfS
bgERqPAnYvazqwc83jIN9gCjr/aBqD6LiKm0vRUA2FBkTdtNUeiTqRzGrMN3qR3n
MeZUOZlKPGK4XEEvN82bPeIr00ga1iwWdCmQHFlvgeya03x9uF/S39/3Z0P9vzR2
QLWxdtEEbHZZ/4PQyfHr
=afPJ
-----END PGP MESSAGE-----

```

Lo siguiente fue enviar el correo, esto lo realice usando la herramienta `smtp-email-spoofers-py` (fue una de las herramientas que encontré al buscar en Google como realizar esta actividad), la herramienta se encuentra en <https://github.com/mikechabot/smtp-email-spoofers-py>

Seguí los pasos del repositorio, lo primero fue clonarlo con `git clone https://github.com/mikechabot/smtp-email-spoofers-py`

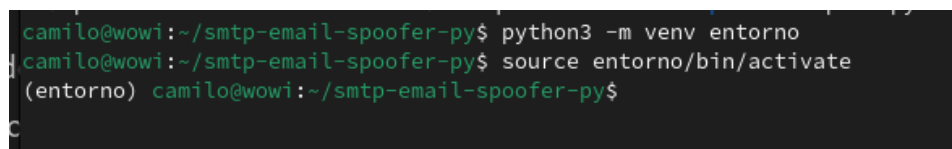


```

camilo@wowi:~$ git clone https://github.com/mikechabot/smtp-email-spoofers-py.git
Cloning into 'smtp-email-spoofers-py'...
remote: Enumerating objects: 188, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 188 (delta 3), reused 11 (delta 2), pack-reused 171 (from 1)
Receiving objects: 100% (188/188), 53.43 KiB | 526.00 KiB/s, done.
Resolving deltas: 100% (81/81), done.
camilo@wowi:~$

```

Después cree y active un ambiente virtual con `python3 -m venv entorno` y `source entorno/bin/activate`



```

camilo@wowi:~/smtp-email-spoofers-py$ python3 -m venv entorno
camilo@wowi:~/smtp-email-spoofers-py$ source entorno/bin/activate
(entorno) camilo@wowi:~/smtp-email-spoofers-py$

```

Posteriormente instale los requerimientos con `pip install -r requirements.txt`

```
(entorno) camilo@wowi:~/smtp-email-spoofers-py$ pip install -r requirements.txt
Collecting colorama==0.3.9 (from -r requirements.txt (line 1))
  Using cached colorama-0.3.9-py2.py3-none-any.whl.metadata (13 kB)
  Using cached colorama-0.3.9-py2.py3-none-any.whl (20 kB)
Installing collected packages: colorama
Successfully installed colorama-0.3.9

[notice] A new release of pip is available: 23.3.2 -> 24.2
[notice] To update, run: pip install --upgrade pip
(entorno) camilo@wowi:~/smtp-email-spoofers-py$
```

Y por ultimo ejecute el comando `python spoof.py wizard` y seguí los pasos que decía la terminal

```
(entorno) camilo@wowi:~/smtp-email-spoofers-py$ python spoof.py wizard

=====
email-spoofers-py v0.0.3 (CLI wizard)
Python 3.x based email spoofer
https://github.com/mikechabot/email-spoofers-py
=====

SMTP host: smtp.gmail.com
SMTP port: 587
Connecting to SMTP socket (smtp.gmail.com:587)...
Starting TLS session...
Disable authentication (Y/N)? n
Username: jcamilo@ciencias.unam.mx
Password:
Authentication successful
Sender address: ivangalindo@ciencias.unam.mx
Sender name: Ivan Galindo <ivangalindo@ciencias.unam.mx>
Recipient address: ivangalindo@ciencias.unam.mx
Enter additional recipients (Y/N)? n
Subject line: Tarea Moral
Load message body from file (Y/N)? y
Filename: mensaje_del_correo.txt
Send message (Y/N)? y
Sending spoofed message...
Message sent!
(entorno) camilo@wowi:~/smtp-email-spoofers-py$
```

Lo de SMTP host y puerto lo copie de un código que hice en Ingeniería de Software para enviar correos (posiblemente pude usar ese código para enviar el correo pero no estaba muy seguro), use `smtp.gmail.com` ya que envié el correo con mi cuenta de `ciencias.unam.mx` y el puerto 587 es puerto generalmente usado para enviar correos. En sender name puse tanto el nombre y correo del ayudante, debido a que en pruebas que realice no aparecía bien sender address (aparecía mi correo y no lo que ponía). Se intento realizar la tarea moral.



3. Complicaciones

La principal complicación fue que al enviar el correo no fui capaz de lograr cambiar el correo de quien envía

el correo, solo el nombre de quien lo envía. Supongo debido a que use como host SMTP a gmail no se puedo cambiar lo del correo del que lo envió, ya que en el ejemplo de GitHub usaba otro, además otras paginas decían usar sendinblue pero al parecer ese servicio ya no funciona de la igual manera.