Curso de Hacking Ético Escuela de Videojuegos MasterD

Ejercicio 16

Ingeniería Social

evilURL

Alumno: Julián Gordon

Índice

Introducción 3
Instalación y uso de evilURL 4
Acceso al enlace desde Windows 9
Conclusiones 10

Introducción

En este ejercicio vamos a generar un nombre de dominio malicioso con EvilURL para llevar a cabo la impersonificación de un dominio legítimo. Esta es una práctica fundamental en el ámbito del hacking ético.

La impersonificación de dominios, también conocida como typosquatting o URL hijacking, es una técnica utilizada por ciberdelincuentes para engañar a los usuarios y obtener información confidencial, como credenciales de inicio de sesión o datos financieros. Aprenderemos a utilizar EvilURL, una herramienta especializada en la generación de URLs maliciosas, para crear un nombre de dominio que se asemeje a uno legítimo.

Instalación y uso de evilURL

Empezaremos este ejercicio al igual que empezamos con casi todos los ejercicios de este módulo, instalando las herramientas necesarias para realizar este ataque. Haremos un git clone del repositorio de github, con el comando:
‘git clone https://github.com/UndeadSec/EvilURL.git’

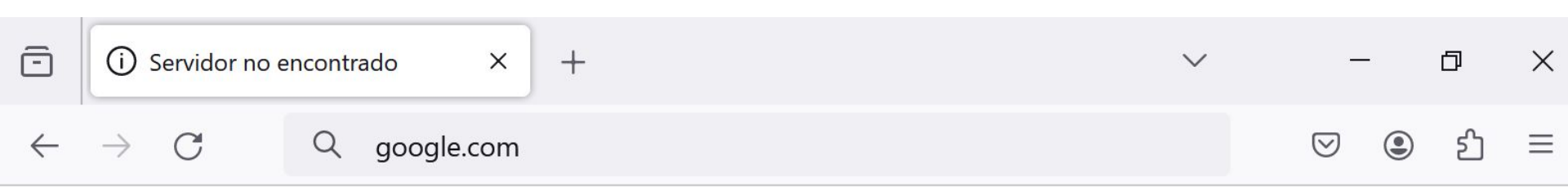
Ya que evilURL está escrito en python, debemos asegurarnos de tenerlo instalado. Una vez instalado, vamos a hacer una prueba para impersonificar el dominio google.com, para ello ejecutamos el siguiente comando:

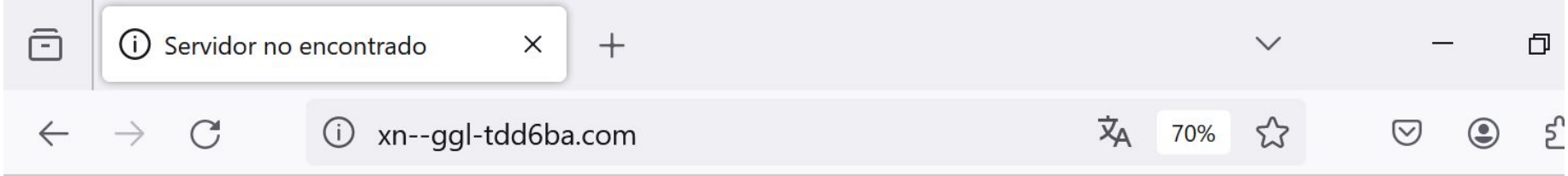
‘python3 evilurl.py -g -d google.com’

Esto nos va a generar una URL que a simple vista es igual a google.com, pero tiene un truco. La "o" es en realidad la letra cirílica "o" al igual que la “e”, que se parece mucho a la "o" y a la “e” latina pero son caracteres diferentes. La herramienta nos dará una url maliciosa ‘google.com’ .

Podemos observar este proceso en la siguiente imagen. Luego probaremos pegar este link generado en nuestro navegador para ver qué sucede.

```
88888888888          88  88  88        88  88888888ba   88
88                   ""  88  88        88  88      "8b  88
88                       88  88        88  88      ,8P  88
88aaaaa  8b      d8  88  88  88        88  88aaaaaa8P'  88
88"""""  `8b    d8'  88  88  88        88  88""""88'    88      v3.0
88        `8b  d8'   88  88  88        88  88    `8b    88
88         `8b,d8'   88  88  Y8a.    .a8P  88     `8b   88
88888888888  "8"     88  88   `"Y8888Y"'   88      `8b  88888888

[ by UNDEADSEC - Alisson Moretto @UndeadSec ]

[~] Original: google.com

[*] Domain name: google
[*] Char replaced: ['e']
[*] Using Unicode: ['e']
[*] Unicode number: ['Cyrillic Small Letter Ie']
[*] Evil URL: google.com

[*] Domain name: google
[*] Char replaced: ['o']
[*] Using Unicode: ['o']
[*] Unicode number: ['Cyrillic Small Letter O']
[*] Evil URL: google.com

[*] Domain name: google
[*] Char replaced: ['e', 'o']
[*] Using Unicode: ['e', 'o']
[*] Unicode number: ['Cyrillic Small Letter Ie', 'Cyrillic Small Letter O']
[*] Evil URL: google.com
```


Servidor no encontrado
google.com



Uf. Tenemos problemas para encontrar ese sitio.

No podemos conectar al servidor en xn--ggl-tdd6ba.com.

Si escribió la dirección correcta, puede:

- Probar de nuevo más tarde
- Verificar la conexión a internet
- Comprobar que Firefox tiene permiso para acceder a la web (puede ser que esté conectado pero detrás de un firewall)

Reintentar

Acceso al enlace desde una máquina Windows

Podemos observar que nos redirigió a ‘http://xn--ggl-tdd6ba.com/’ y no a google.com , cómo creíamos que nos llevaría.

Esto lo podríamos utilizar en un escenario de phishing, enviando correos electrónicos o mensajes que contengan enlaces a este nombre de dominio a posibles víctimas. Cuando las víctimas hiciesen clic en el enlace (que pone ‘google.com’), serían redirigidas al sitio web controlado por nosotros, en lugar del sitio web legítimo ‘google.com’ que están esperando.

Conclusiones

En este ejercicio, exploramos el proceso de generar un nombre de dominio malicioso utilizando la herramienta EvilURL con el objetivo de realizar la impersonificación de un nombre de dominio legítimo.

Utilizando EvilURL, pudimos generar un nombre de dominio que, a simple vista, se asemejaba al dominio legítimo que queríamos impersonar. Sin embargo, al examinar más de cerca la URL generada, pudimos identificar que se habían utilizado caracteres unicode para hacerla parecer legítima. Al intentar acceder a la URL maliciosa generada, observamos que fuimos redirigidos a un sitio web distinto al que esperábamos, lo cual ilustra cómo este tipo de técnicas pueden ser utilizadas en escenarios de phishing para engañar a los usuarios y dirigirlos a sitios controlados por el atacante.

Este ejercicio nos proporcionó una visión práctica de cómo los ciberdelincuentes pueden utilizar la impersonificación de dominios para llevar a cabo ataques de phishing y obtener información confidencial de los usuarios.