

Introducción:

El alumno utilizara las herramientas Nikto y Spiderfoot, con el objetivo de cumplir con la segunda y tercera fase del ciclo del hacking, además de completar el reto número #2 del SANS Holiday Hack Challenge y agregar sus conclusiones en el reporte final.

Herramientas necesarias:

- VirtualBox 6.0.4.

<https://www.virtualbox.org/wiki/Downloads>

- Kali Linux 2019.1a.

<https://www.kali.org/downloads/>

- Ubuntu 18.10

<https://www.ubuntu.com/download/server>

- Mutillidae 2.7.9.

<https://github.com/webpwnized/mutillidae>

- Metasploitable 2.

<https://sourceforge.net/projects/metasploitable/>

A. Obtener información de un objetivo con NIKTO.

Nikto es un escáner Open Source de vulnerabilidades escrito en lenguaje PERL que se utiliza por medio de la línea de comandos. Es muy ligero y sencillo de utilizar.

1. Se debe iniciar una máquina virtual con Kali Linux 2019.1.a y escribir en la terminal el siguiente comando:

Nikto -h "dirección ip"

```
root@kali:~# nikto -h http://192.168.2.4/mutillidae/
- Nikto v2.1.6
-----
+ Target IP:          192.168.2.4
+ Target Hostname:    192.168.2.4
+ Target Port:        80
+ Start Time:         2019-03-25 20:35:03 (GMT0)
-----
+ Server: Apache/2.4.34 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ Cookie showhints created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'logged-in-user' found, with contents:
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /mutillidae/robots.txt,
```

2. Si se desea obtener un archivo en formato HTML se agrega la opción -o.

```
root@kali:~# nikto -h http://192.168.2.4/mutillidae/ -o html
- Nikto v2.1.6
-----
+ Target IP:      192.168.2.4
+ Target Hostname: 192.168.2.4
+ Target Port:    80
+ Start Time:     2019-03-25 20:43:09 (GMT0)
-----
+ Server: Apache/2.4.34 (Ubuntu)
```

3. También se cuenta con la opción “evasion” donde se muestran varios tipos de técnicas para intentar evadir cualquier tipo de IDS que pudiera alertar o bloquearnos el escaneo, como las que nos indican en la documentación:

1. Random URI encoding (non-UTF8)
2. Directory self-reference (./.)
3. Premature URL ending
4. Prepend long random string
5. Fake parameter
6. TAB as request spacer
7. Change the case of the URL
8. Use Windows directory separator (\)
9. Use a carriage return (0x0d) as a request spacer
10. Use binary value 0x0b as a request spacer

Para utilizarlos solamente se añade la opción y el mode de la siguiente manera:

- Nikto -h “URL o IP” -evasion 1

```
root@kali:~# nikto -h http://192.168.2.4/mutillidae -evasion 1
- Nikto v2.1.6
-----
+ Target IP:      192.168.2.4
+ Target Hostname: 192.168.2.4
+ Target Port:    80
+ Using Encoding: Random URI encoding (non-UTF8)
+ Start Time:     2019-03-25 20:58:31 (GMT0)
-----
```

4. Ahora que conocemos como utilizar Nikto, lo siguiente será tratar de resolver el reto número 2 del SANS Holiday Hack Challenge.

Question 2:

Who submitted (First Last) the rejected talk titled **Data Loss for Rainbow Teams: A Path in the Darkness?** Please analyze the CFP site to find out. For hints on achieving this objective, please visit Minty Candycane and help her with the **The Name Game** Cranberry Pi terminal challenge.

Answer SUBMIT



5. Para tratar de obtener información de la página se utiliza el comando:

Nikto -h <https://cfp.kringlecastle.com>

```
root@kali:~# nikto -h https://cfp.kringlecastle.com
- Nikto v2.1.6
-----
+ Target IP:      35.196.29.176
+ Target Hostname: cfp.kringlecastle.com
+ Target Port:    443
-----
+ SSL Info:      Subject:  /CN=cfp.kringlecastle.com
                  Ciphers:  ECDHE-RSA-CHACHA20-POLY1305
                  Issuer:   /C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
+ Start Time:    2019-03-25 19:39:20 (GMT0)
-----
+ Server: nginx/1.10.3
+ Server leaks inodes via ETags, header found with file /, fields: 0x5c0bc4e0 0x18a3
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

Nota: Para soporte SSL en Nikto es necesario la librería OpenSSL y el módulo Net::SSLeay de Perl.

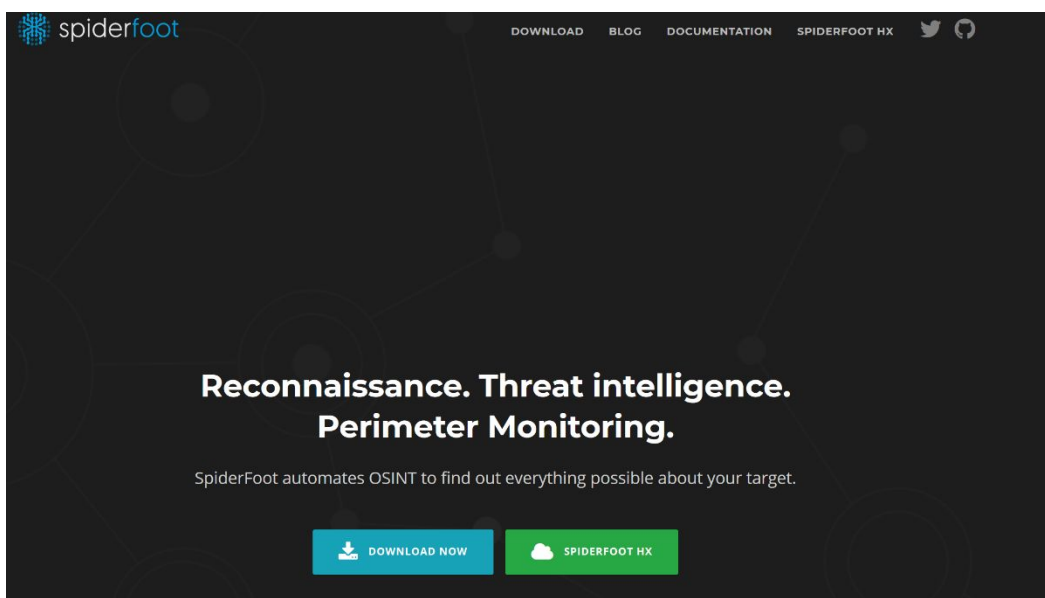
- `apt-get install openssl libcrypt-ssleay-perl`

Spiderfoot al rescate:

SpiderFoot es una herramienta de reconocimiento que consulta automáticamente más de 100 fuentes de datos públicas (OSINT) para recopilar información sobre direcciones IP, nombres de dominio, direcciones de correo electrónico, nombres y más.

1. Ingresar a la página de la herramienta en el siguiente enlace:

- <https://www.spiderfoot.net/>



2. En el apartado descargar seleccionar el paquete de Linux.

- <https://www.spiderfoot.net/download/>

3. Instalar las dependencias necesarias ejecutando los siguientes comandos en la terminal:

- `pip install lxml netaddr M2Crypto cherrypy mako requests bs4`
- `apt-get install python-m2crypto`

4. Ingresar a la carpeta donde se descargo Spiderfoot y extraer con el comando:

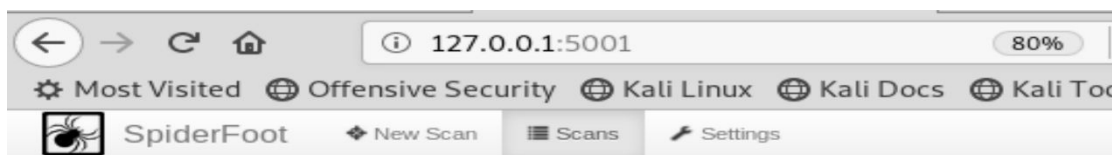
- \$ tar zxvf spiderfoot-X.X.X-src.tar.gz
5. Con el comando cd se accede a la nueva carpeta creada
- Cd spiderfoot-X.X.X
6. Una vez dentro de la carpeta se escribe los siguiente para iniciar la herramienta:
- Python ./sf.py

```
root@kali:~/Downloads/spiderfoot-2.12# python ./sf.py
Starting web server at http://127.0.0.1:5001 ...

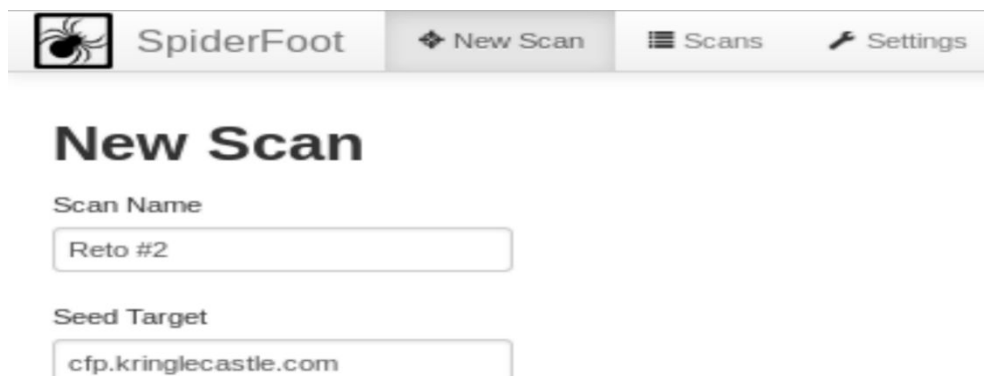
*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001
*****

[25/Mar/2019:20:00:27] ENGINE Listening for SIGHUP.
[25/Mar/2019:20:00:27] ENGINE Listening for SIGTERM.
[25/Mar/2019:20:00:27] ENGINE Listening for SIGUSR1.
[25/Mar/2019:20:00:27] ENGINE Bus STARTING
[25/Mar/2019:20:00:27] ENGINE Serving on http://127.0.0.1:5001
[25/Mar/2019:20:00:27] ENGINE Bus STARTED
```

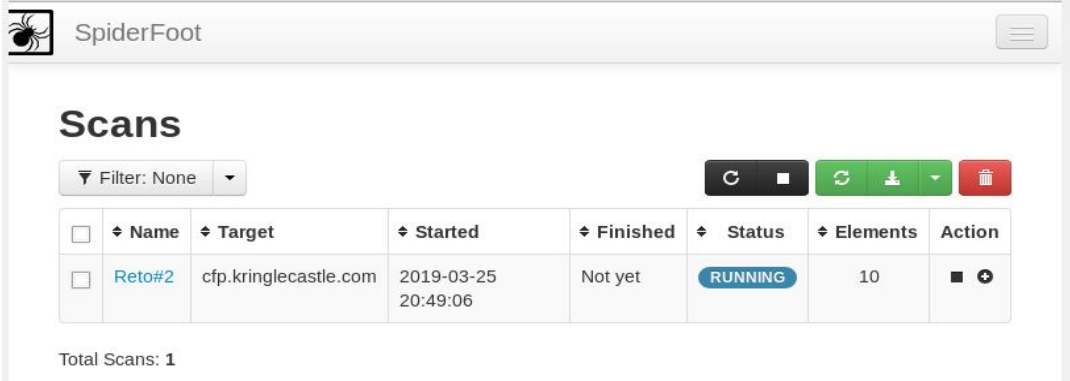
7. Una vez corriendo correctamente es necesario abrir el navegador y escribir la dirección 127.0.0.1:5001



8. Para iniciar un escaneo clic en el botón “New Scan”.



9. Mientras corre el escaneo podemos ver su avance de la siguiente forma:

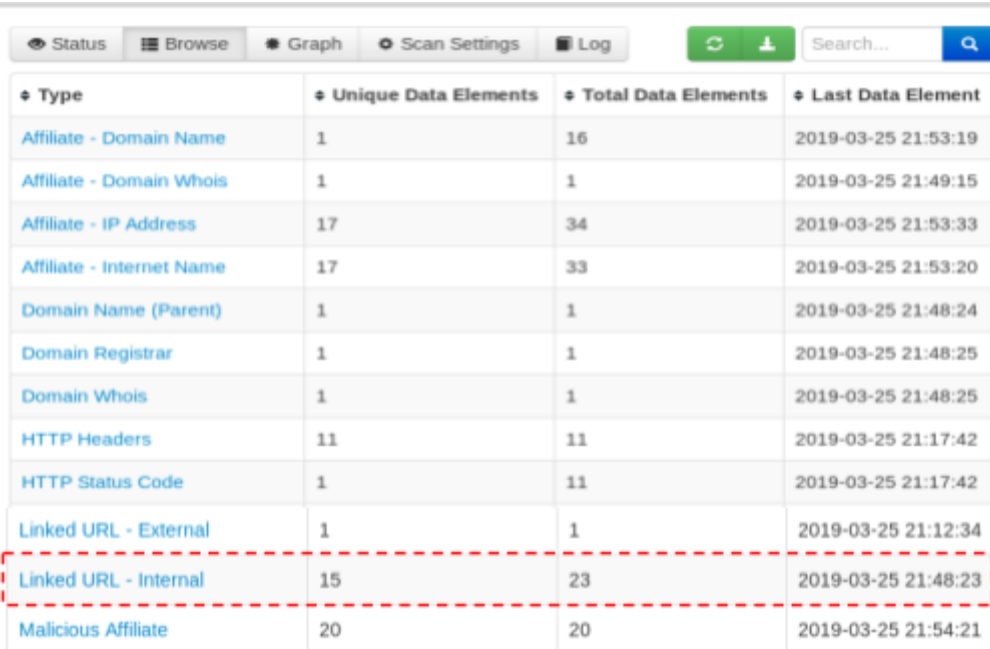


The screenshot shows the SpiderFoot web interface. At the top, there's a header with the SpiderFoot logo and a hamburger menu. Below the header, the title "Scans" is displayed. A filter dropdown is set to "None". To the right of the filter are several action buttons: a refresh button, a stop button, a scan button, a download button, and a delete button. Below these buttons is a table with the following columns: Name, Target, Started, Finished, Status, Elements, and Action. There is one row in the table with the following data: Name: "Reto#2", Target: "cfp.kringlecastle.com", Started: "2019-03-25 20:49:06", Finished: "Not yet", Status: "RUNNING" (in a blue pill), Elements: "10", and Action: a square icon with a plus sign. Below the table, it says "Total Scans: 1".

<input type="checkbox"/>	Name	Target	Started	Finished	Status	Elements	Action
<input type="checkbox"/>	Reto#2	cfp.kringlecastle.com	2019-03-25 20:49:06	Not yet	RUNNING	10	■ +

Total Scans: 1

10. Seleccionar la opción Linked URL - Internal.



The screenshot shows the SpiderFoot web interface with the "Scan Settings" tab selected. At the top, there are tabs for Status, Browse, Graph, Scan Settings, and Log. To the right of the tabs are a refresh button, a scan button, and a search bar. Below the tabs is a table with the following columns: Type, Unique Data Elements, Total Data Elements, and Last Data Element. The table contains the following rows:

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Domain Name	1	16	2019-03-25 21:53:19
Affiliate - Domain Whois	1	1	2019-03-25 21:49:15
Affiliate - IP Address	17	34	2019-03-25 21:53:33
Affiliate - Internet Name	17	33	2019-03-25 21:53:20
Domain Name (Parent)	1	1	2019-03-25 21:48:24
Domain Registrar	1	1	2019-03-25 21:48:25
Domain Whois	1	1	2019-03-25 21:48:25
HTTP Headers	11	11	2019-03-25 21:17:42
HTTP Status Code	1	11	2019-03-25 21:17:42
Linked URL - External	1	1	2019-03-25 21:12:34
Linked URL - Internal	15	23	2019-03-25 21:48:23
Malicious Affiliate	20	20	2019-03-25 21:54:21

11. Una vez en la sección, se puede encontrar un csv con platicas rechazadas.

<input type="checkbox"/>	https://cfp.kringlecastle.com/cfp/cfp.html	cfp.kringlecastle.com	sfp_yahoosearch	2019-03-25 21:48:23
<input type="checkbox"/>	https://cfp.kringlecastle.com/cfp/rejected-talks.csv	cfp.kringlecastle.com	sfp_bingsearch	2019-03-25 21:06:59
<input type="checkbox"/>	https://cfp.kringlecastle.com/cfp/rejected-talks.csv	cfp.kringlecastle.com	sfp_yahoosearch	2019-03-25 21:48:23

12. Se ingresa la respuesta en el reto. Felicitades resolviste el segundo reto.

qmt3,2,8040424,200,FALSE,FALSE,John,McClane,Director of Security,**Data Loss for Rainbow Teams: A Path in the Darkness**,1,11
qmt4,3,8040425,200,FALSE,FALSE,Davidde,Yellop,Analyst,Industrial Control Systems Content Filtering: Distributed,5,7
qmt5,4,8040426,200,FALSE,FALSE,Berton,Tupie,Meeting Planner,Rootkits Emailed Malware: Extensible Models,5,7
qmt6,5,8040427,200,FALSE,FALSE,Kelbee,McBean,Marketing Director,Web Application Filters and DNS: Anomaly Analysis,6,6

13. Se ingresa la respuesta en el reto. Felicitades resolviste el segundo reto.

Question 2:

Who submitted (First Last) the rejected talk titled **Data Loss for Rainbow Teams: A Path in the Darkness**? Please analyze the CFP site to find out. For hints on achieving this objective, please visit Minty Candycane and help her with the **The Name Game** Cranberry Pi terminal challenge.

Answer: John McClane



Ho Ho Ho!