PR0GR4M4C10N H4CK

Semana 4: Recolección de información

PARTE 1

- Recolección de información. PARTE 1
  - Motores de búsqueda
    - Google Hacking
    - Shodan Hacking

Semana 4: 2º parte

- Recolección de información. PARTE 1
  - Motores de búsqueda
    - Google Hacking
    - Shodan Hacking

Semana 4: 2º parte

- Es uno de los motores de búsqueda más utilizado en todo el mundo y una herramienta muy útil para encontrar información sobre sitios web.
- Johnny Long fue quien introdujo el término “Google Hacking”.
- Es posible que en un sitio web determinado existan fugas de información importante y que es capturada y almacenada por Google.
- Esto puede ser utilizado por los “buenos” y también por los usuarios maliciosos.

GOOGLE HACKING
RECOLECCIÓN DE INFORMACIÓN

- Algunas de las palabras reservadas para establecer filtros:
  - site → Indica el sitio web sobre el que se realiza la búsqueda.
  - intitle → Buscar un texto en un título de una determinada página.
  - inurl → Filtrar los resultados con aquellas coincidencias que contengan en la URL el texto indicado.
  - ext → Búsqueda de archivos con una extensión determinada.

GOOGLE DORKS
RECOLECCIÓN DE INFORMACIÓN

- EJEMPLOS:

```
site:thesecuritysentinel.es contacto
```

GOOGLE DORKS
RECOLECCIÓN DE INFORMACIÓN

- EJEMPLOS:

```
site:thesecuritysentinel.es contacto
```

```
intitle:Python 3.0
```

GOOGLE DORKS
RECOLECCIÓN DE INFORMACIÓN

- EJEMPLOS:

```
site:thesecuritysentinel.es contacto
```

```
intitle:Python 3.0
```

```
site:thesecuritysentinel.es inurl:curso
```

GOOGLE DORKS
RECOLECCIÓN DE INFORMACIÓN

- EJEMPLOS:

```
site:thesecuritysentinel.es contacto
```

```
intitle:Python 3.0
```

```
site:thesecuritysentinel.es inurl:curso
```

```
site:www.elmundo.es ext:pdf
```

GOOGLE DORKS
RECOLECCIÓN DE INFORMACIÓN

- EJEMPLOS:

site:thesecuritysentinel.es contacto

intitle:Python 3.0

site:thesecuritysentinel.es inurl:curso

site:www.elmundo.es ext:pdf

GOOGLE DORKS
RECOLECCIÓN DE INFORMACIÓN

- Recolección de información. PARTE 1
  - Motores de búsqueda
    - Google Hacking
    - Shodan Hacking

Semana 4: 2º parte

SHODAN HACKING
RECOLECCIÓN DE INFORMACIÓN

- Motor de búsquedas que permite encontrar servidores y dispositivos de internet que ejecutan servicios muy concretos.

SHODAN HACKING
RECOLECCIÓN DE INFORMACIÓN

- Motor de búsquedas que permite encontrar servidores y dispositivos de internet que ejecutan servicios muy concretos.
- Shodan indexa en su base de datos interna, las cabeceras y banners correspondientes a servidores que se encuentran en ejecución en internet.

SHODAN HACKING
RECOLECCIÓN DE INFORMACIÓN

- Motor de búsquedas que permite encontrar servidores y dispositivos de internet que ejecutan servicios muy concretos.
- Shodan indexa en su base de datos interna, las cabeceras y banners correspondientes a servidores que se encuentran en ejecución en internet.
- Cuenta con una serie de filtros que permiten restringir los resultados de las consultas.

SHODAN HACKING
RECOLECCIÓN DE INFORMACIÓN

- Motor de búsquedas que permite encontrar servidores y dispositivos de internet que ejecutan servicios muy concretos.
- Shodan indexa en su base de datos interna, las cabeceras y banners correspondientes a servidores que se encuentran en ejecución en internet.
- Cuenta con una serie de filtros que permiten restringir los resultados de las consultas.

city, country, geo, hostname, net, os, port

SHODAN HACKING
RECOLECCIÓN DE INFORMACIÓN

city:”Granada” proftpd

country:”ES” apache

hostname:.piramid apache

os:”Linux” ubuntu

port:21 proftpd

SHODAN HACKING
RECOLECCIÓN DE INFORMACIÓN

- Shodan cuenta con un apartado de búsquedas de exploits, que también podemos consultar.

mysql

php

proftpd

SHODAN HACKING - EXPLOITS
RECOLECCIÓN DE INFORMACIÓN

- Para instalar shodan en python:

```
sudo pip install shodan
```

- Haremos una serie de ejemplos de búsquedas sencillas a través de la página web de Shodan y usando la API con python.

SHODAN HACKING
RECOLECCIÓN DE INFORMACIÓN