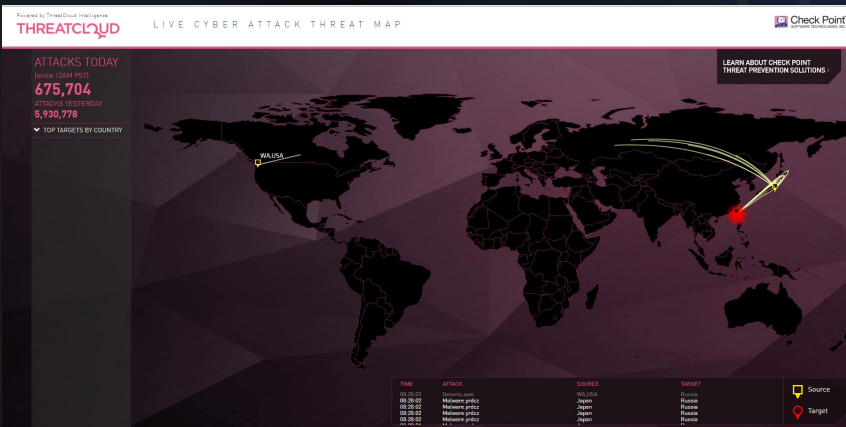




ETHICAL HACKING 2

Ataques Globales

• <http://www.digitalattackmap.com>



• <https://threatmap.checkpoint.com>

• <http://map.norsecorp.com>



UTNFra – Arquitectura y Sistemas Operativos

Fuente de información OSINT

- Se refiere Open Source Intelligence o Inteligencia de fuentes abiertas.
- Muy empleado entre militares, fuerza del orden y personal de inteligencia de las agencias gubernamentales.
- Tiene que ver con la búsqueda de información en Internet y la Internet Profunda.

Fuente de información OSINT



Fuente de información OSINT

- Algunas de las mas utilizadas son recursos como:
 - **SHODAN**: El cual es un buscador que localiza ordenadores, webcams, impresoras y distintos dispositivos electrónicos.
 - **NAMECHK**: Comprueba si un nombre de usuario está disponible en mas de 150 servicios online.
 - **TINEYE**: Es un buscador que parte de una fotografía y nos muestra en que sitios web se encuentra.

Fuente de información OSINT

- Algunas de las mas utilizadas son recursos como:
 - [PIPL](#): Buscador de personas y las relaciona con distintas redes sociales y vínculos en internet.
 - [DOMAINTOOLS](#): Es un servicio que permite identificar, monitorear, buscar y analizar un nombre de dominio
 - [TAGBOARD](#): Permite analizar distintos hashtag o etiquetas de Twitter.

Fuente de información OSINT

- Algunas de las mas utilizadas son recursos como:
 - [TWOPCHARTS](#): Es una herramienta que analiza todo lo que se publica en Twitter, permite conocer los likes, el cronograma e historial de publicaciones, listas, contenido relevante, etc.
 - [FOCA](#): Es un software el cual permite extraer y analizar los metadatos a distintos tipos de documentos. Al conocer los metadatos puedo conocer quien creó, modificó y la distinta información relacionada con un archivo.

Fuente de información OSINT

- Algunas de las mas utilizadas son recursos como:
 - [METAPICZ](#): Permite extraer los metadatos a fotografías y con esto conocer distinta información como qué cámara, software, fechas, teléfono fueron utilizados.

Fuente de información OSINT

- Algunas de las mas utilizadas son recursos como:
 - [Scans.io](https://www.scans.io): proporcionan los resultados de escaneos semanales a diferentes puertos en todo el espacio de direccionamiento **IPv4**, por lo que si conocemos vulnerabilidades de ciertas versiones de software, tenemos toda la información necesaria y cruzada.
 - [censys.io](https://www.censys.io): el motor de búsqueda para descubrir vulnerabilidades de seguridad en internet.

Fuente de información OSINT

- Algunas de las mas utilizadas son recursos como:
 - **XSSPOSED**: es una web que archiva y premia a los cazadores de bugs **XSS** (y **Open Redirects**) en **Internet**. En él se pueden acceder a los **bugs** que han sido encontrados y reportados en la web organizados por importancia de la web o por fecha de reporte, además de permitir ver quiénes son los mejores cazadores de **XSS** en **Internet**.

Fuente de información OSINT

<https://youtu.be/T8cLztvBCIM>

Fuente de información OSINT

- OSINT Framework: <http://osintframework.com/>

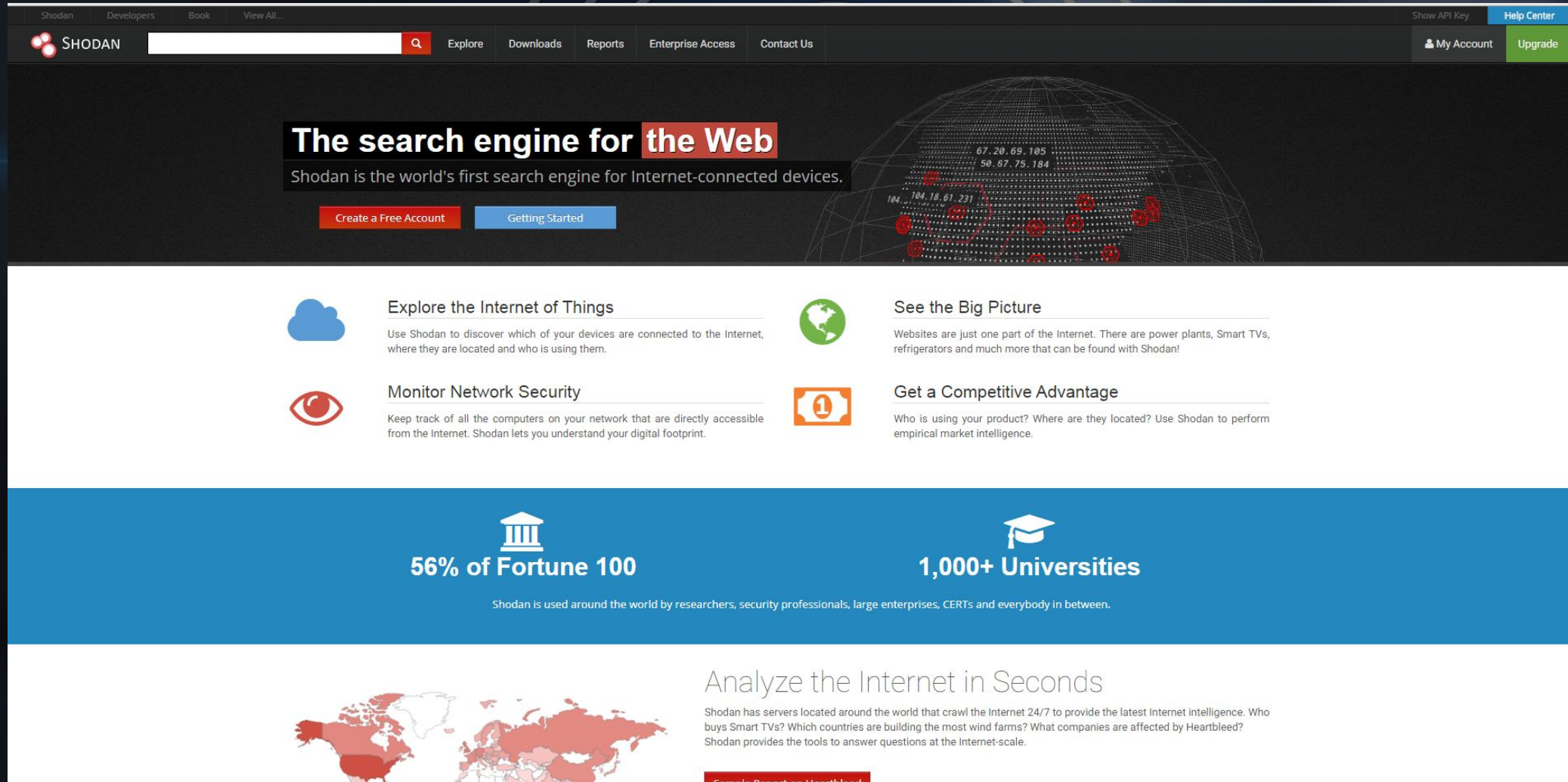


Fuente de información OSINT

Shodan.io

- **Es un motor de búsqueda** que le permite al usuario encontrar iguales o diferentes tipos específicos de equipos (routers, servidores, etc.) conectados a Internet a través de una variedad de filtros.
- Recoge datos sobre todo en los servidores web (HTTP **puerto 80, 8080**, HTTPS **puerto 443, 8443**), pero también hay algunos datos de FTP (**21**), SSH(**22**) Telnet (**23**), SNMP (**161**) y SIP (**5060**).

Fuente de información OSINT



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with links for Shodan, Developers, Book, View All..., Show API Key, and Help Center. Below this is a search bar with the Shodan logo and a search icon. The main header area features the text "The search engine for the Web" and "Shodan is the world's first search engine for Internet-connected devices." Below this are two buttons: "Create a Free Account" and "Getting Started".

The main content area is divided into four sections:

- Explore the Internet of Things**: Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them. (Icon: Cloud)
- Monitor Network Security**: Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint. (Icon: Eye)
- See the Big Picture**: Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan! (Icon: Globe)
- Get a Competitive Advantage**: Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence. (Icon: Coin)

Below these sections is a blue banner with two statistics:

- 56% of Fortune 100**: Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between. (Icon: Building)
- 1,000+ Universities**: (Icon: Graduation cap)

At the bottom, there is a section titled "Analyze the Internet in Seconds" with a world map showing server locations. The text states: "Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale." Below this is a button labeled "Sample Report on Heartbleed".

UTNFra – Arquitectura y Sistemas Operativos

Shodan.io

- Filtros que nos permite shodan cuando tenemos cuenta gratis:
 - **Country:** Nos permite encapsular la búsqueda solamente a un país específico, ejemplo:
 - `country:ar ftp`

Shodan.io

- Filtros que nos permite shodan cuando tenemos cuenta gratis:
 - **City:** Filtro por ciudad, Ejemplo para buscar Servidores Apache en Buenos Aires:
 - `city:Buenos Aires Apache`

Shodan.io

- Filtros que nos permite shodan cuando tenemos cuenta gratis:
 - **port:** Permite hacer búsqueda dependiendo del puerto que tenga abierto o el servicio que se este ejecutando, ejemplo:
 - port:21 city:Buenos Aires
 - **net:** Para buscar una ip especifica o rangos de ip, ejemplo:
 - net:186.65.127.0/24

Shodan.io

- Filtros que nos permite shodan cuando tenemos cuenta gratis:
 - **hostname:** Busca el texto que le indiquemos en la parte de hostname, veamos el resultado de este ejemplo:
 - hostname:Prensa

Shodan.io

- Búsquedas interesantes:

- Anonymous access allowed
- Webcamxp
- Sony: admin/admin



DEEP WEB

Deep WEB

- *El lado oscuro de la internet que no conocemos.*
- *Navegamos apenas el 20% de la realidad virtual.*
- *El 80% se esconde una realidad sumergida donde se pueden contratar un asesino, comprar droga o ver la pornografía infantil la mas dura.*
- *En la Deep Web, las URL se componen de secuencias alfanuméricas con la extensión “.onion” y algunas cambian cada cierto tiempo.*

Deep WEB



Deep WEB

- **Nivel 1** : continúa siendo superficie, pero allí hay sitios menos conocidos, pero de fácil acceso, relacionados con contenidos no aptos para menores.
- **Nivel 2** : todavía no es deep web, pero hay dominios que se encuentran por buscadores independientes
- **Nivel 3** : los dominios están compuestos por caracteres aleatorios. En ellas no hay publicidades, ni colores. Se puede encontrar desde películas y libros que ya no están en la superficie.

Deep WEB

A person wearing a dark hoodie is shown from the chest up, holding a tablet computer. The background is a dark, blue-toned digital space filled with glowing particles and a pixelated, glitch-like effect. The overall aesthetic is futuristic and tech-oriented.

- **Nivel 4** : está “plagado de hackers, verdaderos piratas informáticos relacionados con el robo y malversación de datos”
- **Nivel 5** : se habla de secretos militares y se dice que al 6 sólo pueden acceder los navegantes con conocimientos suficientes

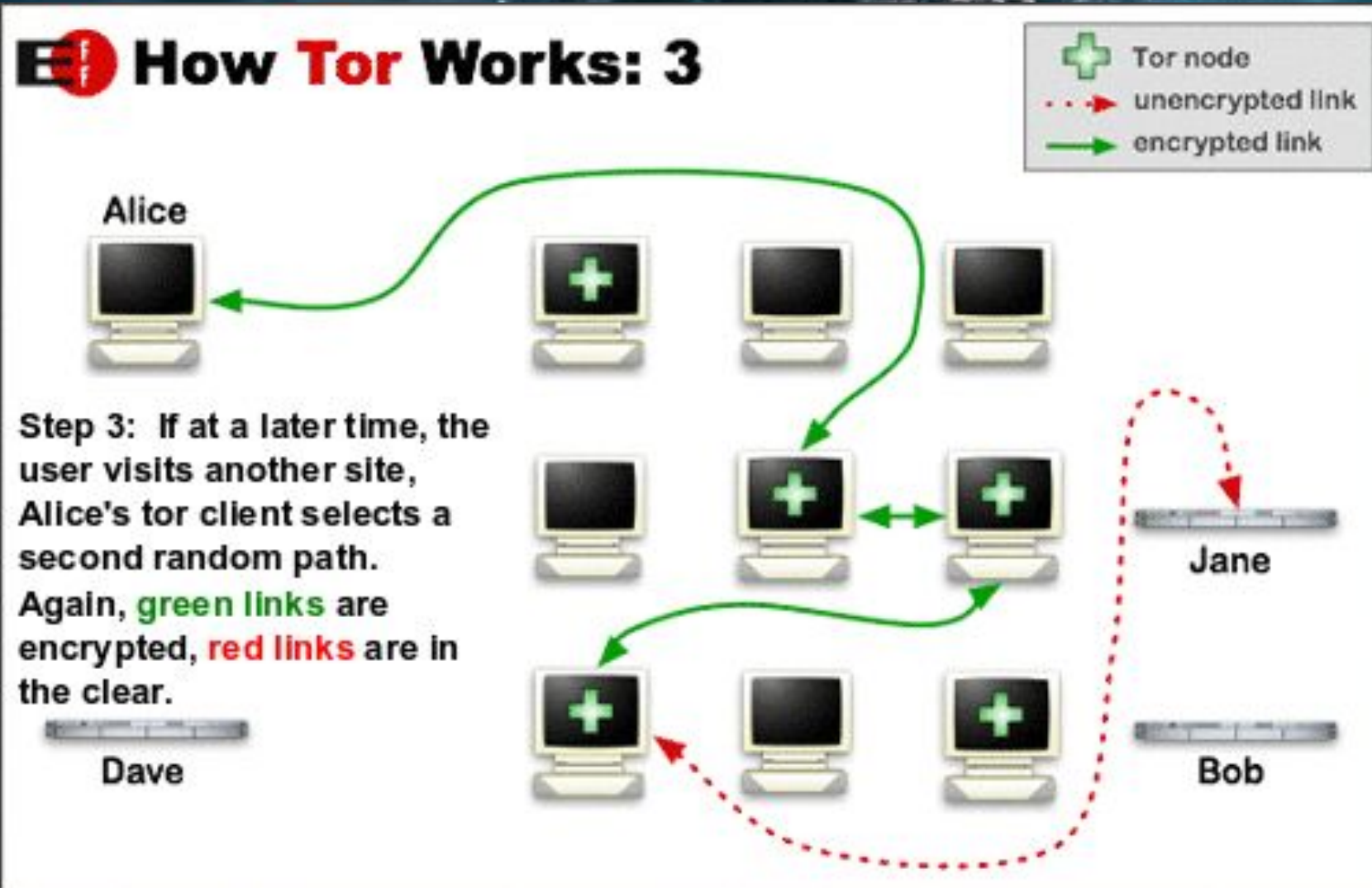
http://www.eset-la.com/pdf/prensa/concurso/677_AgustinaGrasso_DeepWeb_Perfil-AR.pdf

Deep WEB



UTNFra – Arquitectura y Sistemas Operativos

Deep WEB



Deep WEB

A person wearing a dark hoodie is holding a tablet computer. The background is a dark, blue-toned digital space filled with glowing particles and a faint grid pattern, suggesting a cyber or deep web theme.

- Buscadores

- <http://www.carontevaha5x626.onion/>
- <http://thebeast6pwekhvs.onion/> Beast Seach
- <http://qrjy2nhjdbzdprbq.onion/> Dark Seach
- <http://msydqstlz2kzerdg.onion/> AHMIA
- <http://xmh57jrznw6insl.onion/> Torch
- <http://hss3uro2hsxfogfq.onion/> Not Evil
- <http://papyrefb2tdk6czd.onion/> Libros para leer

GRACIAS !!!!!



UTNFra – Arquitectura y Sistemas Operativos