Hackathon #CyberCamp19 AllIntelligence

Ammemgence



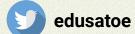
Hackathon.ini













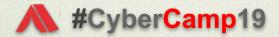




Índice



- Presentación
- Funcionalidad y Capacidades
- Ámbito y Beneficios
- Innovación y Originalidad
- Planteamiento General
- Resumen
- Agradecimientos



Funcionalidades y Capacidades



- Obtención de los Vectores de Ataque de una Organización:



Nivel Técnico



Nivel Identidad Digital

- Generación de Informes de resultados

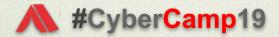




Funcionalidades y Capacidades







Funcionalidades y Capacidades









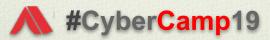
AllIntelligence











Ámbito y Beneficios



Aspectos de seguridad:

Analizaremos a partir de un **dominio** todos los posibles **vectores de ataque,** dependiendo de los **servicios expuestos** en el mismo.

No sólo en el ámbito técnico podemos encontrar vulnerabilidades, sino que precisamente el usuario al ser el eslabón más débil, debemos **auditar** también la parte de **Identidad Digital** de los **miembros de la organización**.

Al final el procesamiento del conjunto de unidades de información obtenidas en la parte técnica y en la parte de identidad digital nos generarán inteligencia.



Ámbito y Beneficios



Público Objetivo:

- Clientes con necesidad de conocer su nivel de exposición. Teniendo en cuenta que hay que cuidar ambas partes en todas las organizaciones.
- Empresas que se dediquen al ámbito de la Ciberseguridad para hacer un análisis de superficie de cuales pueden ser los problemas de sus clientes.
- La comunidad de Hacking en general, ya que este tipo de herramienta ahorra tiempo a la hora de realizar un análisis completo de una organización.
- Pentesters, Analistas de Inteligencia...



Innovación y originalidad



- Proyectos similares:
 - Maltego y Spiderfoot.
 - Mejoras de AllIntelligence: no hay tantos falsos positivos, muestra de fuentes de información para subsanar los leaks, informes finales con información técnica y de identidad digital, muestra de información fácil de inferir y mejoras en el acceso a la información.
- Este proyecto surge por la necesidad de obtener una visión general de los posibles vectores de ataque que pueden afectar a nuestros clientes. Dado que la mayoría de ellos se ven vulnerados por vectores de entrada dependientes del usuario.
- Uso de Python ya que es un lenguaje bastante globalizado, fácil de manejar y con mucho potencial.



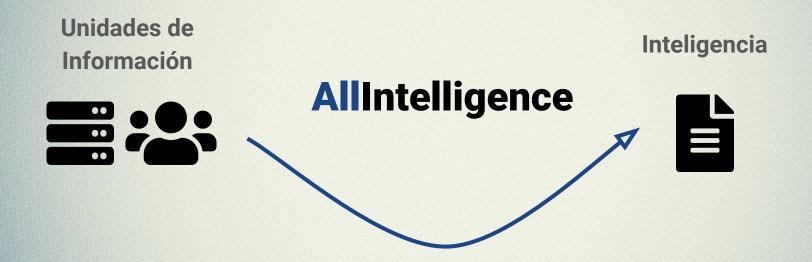
Planteamiento General



- Desarrollo inicial desde 0.
- Uso de diferentes APIs de terceros.
- Comprobación manual de diferentes vulnerabilidades.
- Relacionar las diferentes unidades de información para obtener Inteligencia.

Resumen





Agradecimientos



¡¡Muchas gracias!!

"El conocimiento que se comparte se multiplica"

Especial agradecimiento a Selva Orejón



