Práctica 5. *PenTesting*

Capture The Flag

Temporalización

- Semana 11.

Motivación

En cualquier Congreso de Ciberseguridad que se preste (Navaja Negra, RootedCON, TizonaCON, Jornadas STIC CNI) se plantean una serie de retos relacionados con Ciberseguridad, que muchas veces ayudan a captar talento a las empresas que patrocinan este tipo de Congresos.

Además, es una buena oportunidad para completar tu CV poner la participación en este tipo de retos relacionados con Ciberseguridad: en la mayoría de las veces, son problemas reales con los que te encontrarás en una auditoría informática real, en un escenario real.

Material necesario

- Herramienta volatility para el análisis de las evidencias digitales extraídas de la máquina comprometida.
- Fichero "trojan.vmem" con la información volátil presente en la máquina atacada.

Enunciado

Dado el estado de alarma del Ciberespacio español vinculado con la guerra entre Rusia y Ucrania, uno de los analistas del Mando Conjunto del Ciberespacio Español (MCCE) ha detectado un ciberataque a una de las máquinas presentes en el Ministerio de Defensa

encargada del entrenamiento de la inteligencia artificial utilizada por los drones ucranianos a la hora del reconocimiento de civiles y su posterior descarte antes de cualquier tipo de acción bélica.

larazon.es/espana/20220502/fs5356ec6fav5pcqqzvnwe3wn4.html

LA RAZÓN

España

España aplica técnicas de Inteligencia Artificial para el entrenamiento de los drones ucranianos.

El Ministerio de Defensa en colaboración con el Departamento de Informática de la UVa prepara drones equipados con técnicas de Inteligencia Artificial.

▲ El equipo español desplegado en la madrileña base de Retamares, sede del Mando Conjunto del Ciberespacio FOTO: EMAD

Tras un reconocimiento previo se sospecha que se ha utilizado el troyano Zeus para el robo y la alteración de los datos de entrenamiento de los drones ucranianos.

Entregable

Se pide un informe que realmente determine la presencia del troyano Zeus en la evidencia digital proporcionada, así como la dirección IP y zona geográfica de la máquina a la que se ha conectado el troyano una vez que ha comprometido la máquina de entrenamiento de los drones militares.