Documentación Sala Cyber Kill Chain(Cadena de Asesinato Cibernético)

Tarea 1: Introducción

En esta tarea vemos un pequeño pantallazo de lo que sería en este caso la cadena de asesinato cibernético y las fases q vamos a ir viendo en toda la sala. No tenemos que responder preguntas, solo debemos hacer click en Complete.

Tarea 2: Reconnaissance(Reconocimiento)

En esta tarea vamos a ver el concepto de reconocimiento con el cual tenemos herramientas para adquirir información de la empresa y los empleados los que serán posibles objetivos.

Pregunta

What is the name of the Intel Gathering Tool that is a web-based interface to the common tools and resources for open-source intelligence?

Respuesta

OSINT Framework

Pregunta

What is the definition for the email gathering process during the stage of reconnaissance?

Respuesta

email harvesting

Tarea 3: Weaponization(Armatizacion)

En esta tarea vamos a aprender sobre cómo elegir un arma para atacar el objetivo, tenemos múltiples opciones como crearla nosotros mismo o adquirirlas en la Dark Web.

Pregunta

This term is referred to as a group of commands that perform a specific task. You can think of them as subroutines or functions that contain the code that most users use to automate routine tasks. But malicious actors tend to use them for malicious purposes and include them in Microsoft Office documents. Can you provide the term for it?

Respuesta

Macro

Tarea 4: Delivery(Entrega)

En esta tarea vamos a ver las opciones que tenemos para hacer entrega del arma que adquirimos.

Pregunta

What is the name of the attack when it is performed against a specific group of people, and the attacker seeks to infect the website that the mentioned group of people is constantly visiting.

Respuesta

Watering hole attack

Tarea 5: Exploitation(Explotación)

En esta tarea veremos lo que sería las formas de explotar las vulnerabilidades adquiridas con el acceso al sistema del objetivo.

Pregunta

Can you provide the name for a cyberattack targeting a software vulnerability that is unknown to the antivirus or software vendors?

Respuesta

Zero-day

Tarea 6: Installation(Instalación)

En esta tarea veremos las distintas formas que tenemos de instalarnos en la computadora del objetivo.

Pregunta

Can you provide the technique used to modify file time attributes to hide new or changes to existing files?

Respuesta

Timestomping

Pregunta

Can you name the malicious script planted by an attacker on the web server to maintain access to the compromised system and enables the webserver to be accessed remotely?

Respuesta

web shell

Tarea 7: Command & Control(Comando y Control)

En esta tarea veremos la herramienta o método que utilizaremos para mantener en control de la computadora objetivo.

Pregunta

What is the C2 communication where the victim makes regular DNS requests to a DNS server and domain which belong to an attacker.

Respuesta

DNS Tunneling

Tarea 8: Actions on Objectives (Exfiltration)(Acciones sobre Objetivos (Exfiltración))

En esta tarea vamos a ver qué cosas podemos hacer una vez q hayamos cumplido con los 6 pasos anteriores.

Pregunta

Can you provide a technology included in Microsoft Windows that can create backup copies or snapshots of files or volumes on the computer, even when they are in use?

Respuesta

Shadow Copy

Tarea 9: Practice Analysis(Análisis de Práctica)

En esta tarea vamos a tener un lab donde podremos poner en práctica lo aprendido previamente. Tenemos que hacer click en View Site

Orden
powershell
spear phishing attachment
exploit public-facing application
dynamic linker hijacking
fallback channels
data from local system

Pregunta

What is the flag after you complete the static site?

Respuesta

THM{7HR347_1N73L_12_4w35om3}

Tarea 10: Conclusión

Como lo dice el título esta tarea es la conclusión de lo que vimos en la totalidad de la sala. Debemos presionar Complete