Tenemos grupo de estudio!!! Link del servidor de Discord

SOC CLASE 4

Emulación de adversarios

Metodología que simula las operaciones de un adversario para probar la seguridad de una organizacion.

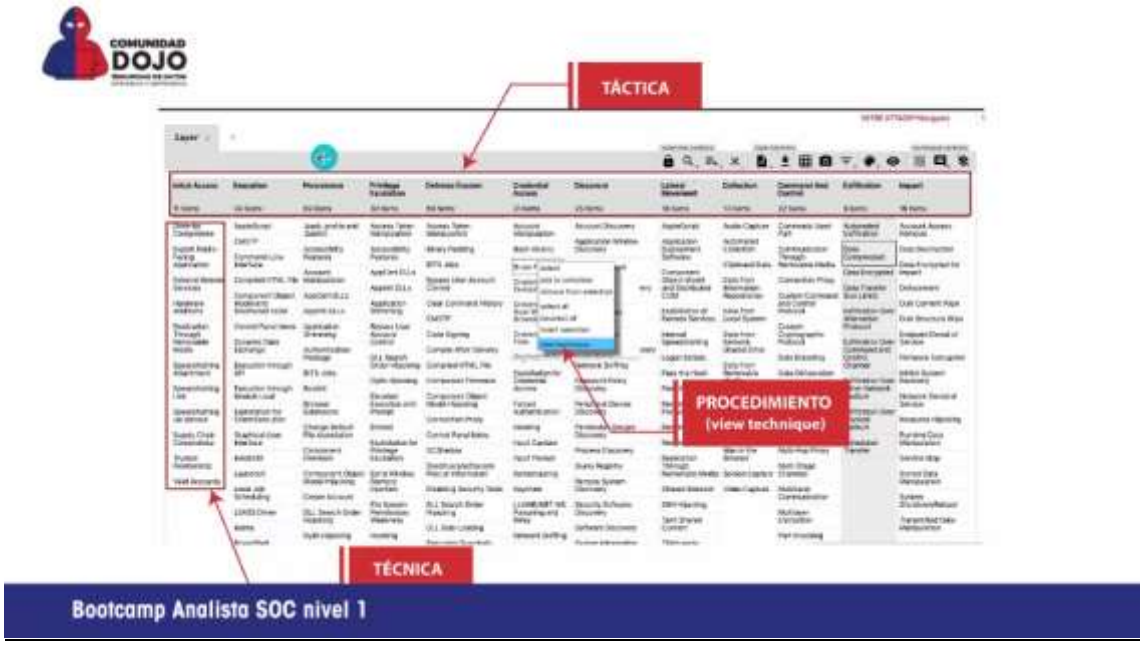
Bootcamp Analista SOC nivel 1

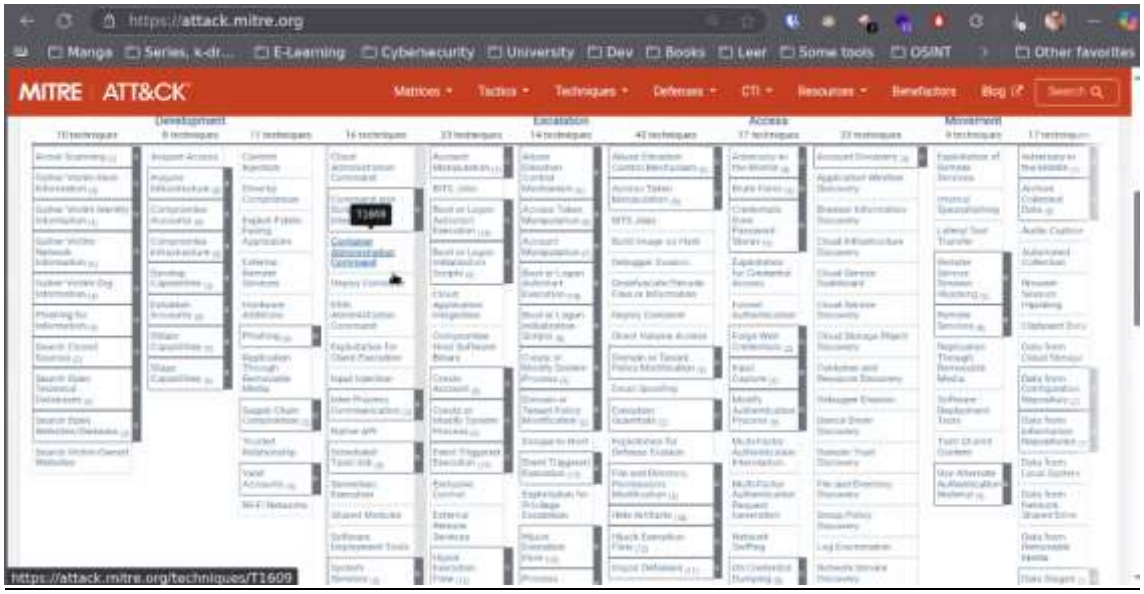
Objetivos

Medir la eficacia de las implementaciones de las herramientas
Reglas de correlación
Umbrales de detección
Disminucion de falsos positivos

Si te sirvió, conectemos en LinkedIn (¿

Tenemos grupo de estudio!!! Link del servidor de Discord





Pagina de Mitre – Link

Si te sirvió, conectemos en LinkedIn (¿

Tenemos grupo de estudio!!! Link del servidor de Discord

Es como una WIKI para saber el tipo de ataque y su método.

Si te sirvió, conectemos en LinkedIn (¿

Tenemos grupo de estudio!!! Link del servidor de Discord

Tenemos grupo de estudio!!! Link del servidor de Discord

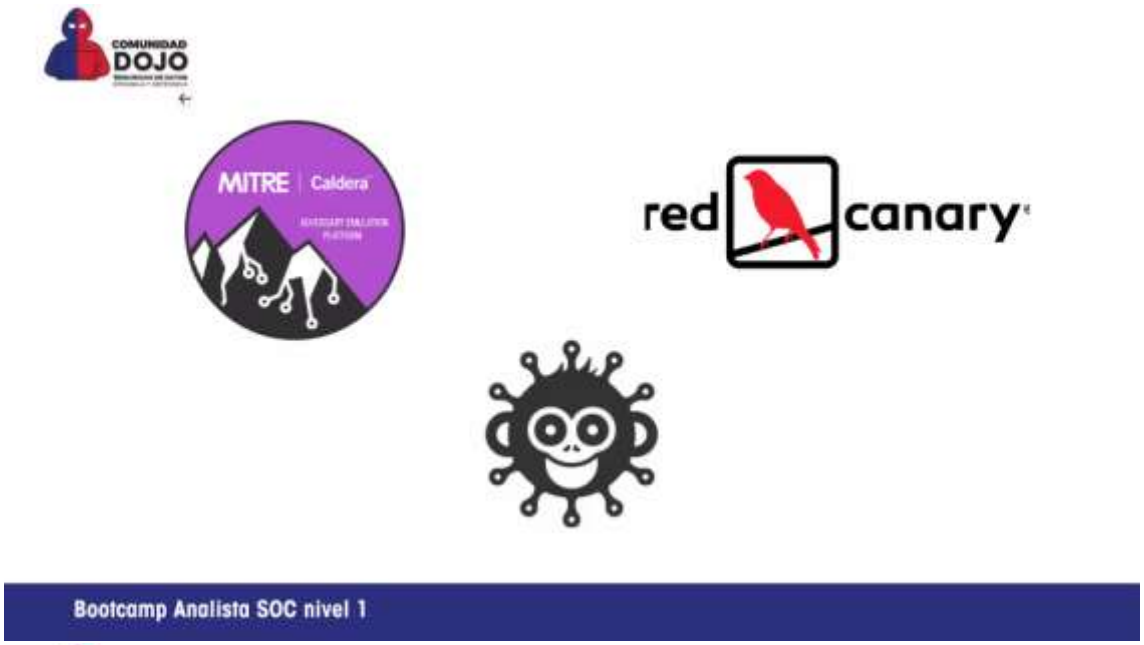
Adversarios

Diferencias

	Emulacion de adversarios	Pentest	Evaluacion de vulnerabilidad
Objetivo	Comportamiento de adversarios	Basado en un contexto, varia, no se rije tanto por TTPS, sino la habilidad del pentester	Unicamente busca evaluar vulnerabilidad, dada una clasificacion y su severidad

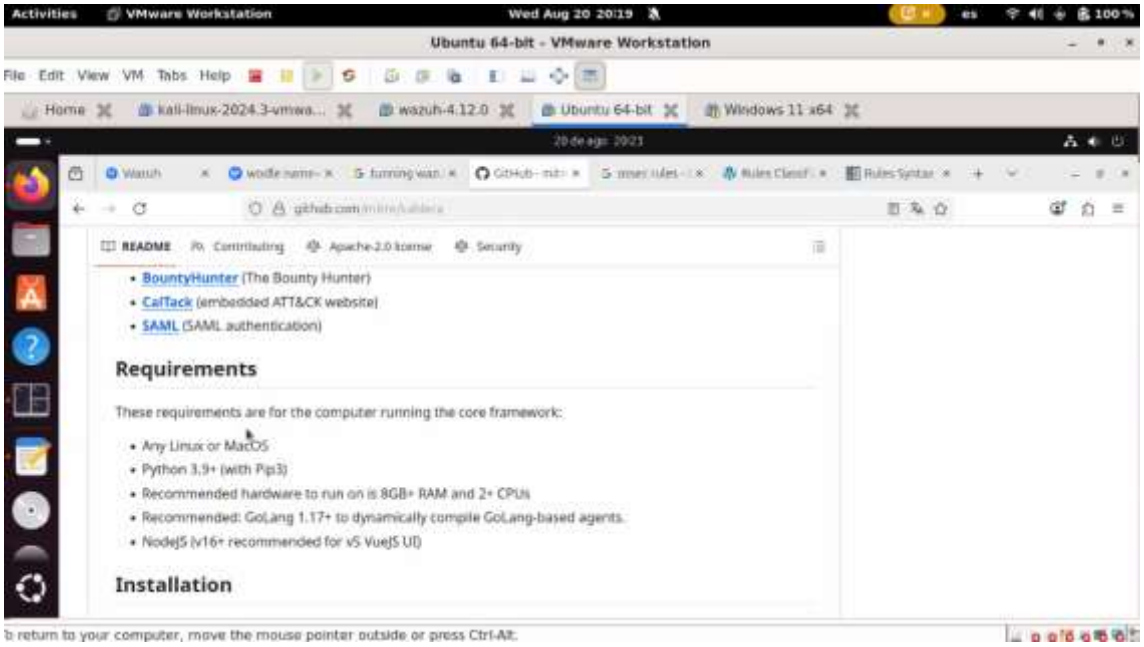
Si te sirvió, conectemos en LinkedIn (¿

Tenemos grupo de estudio!!! Link del servidor de Discord

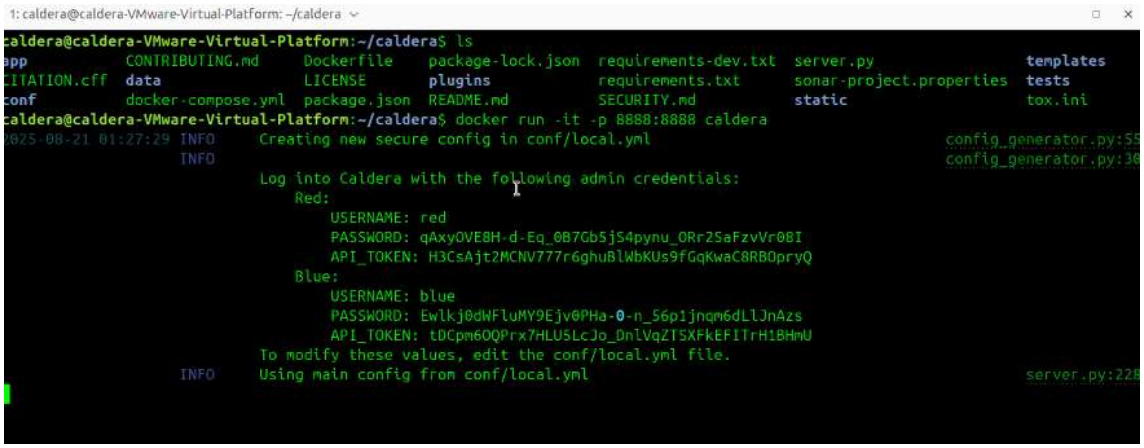


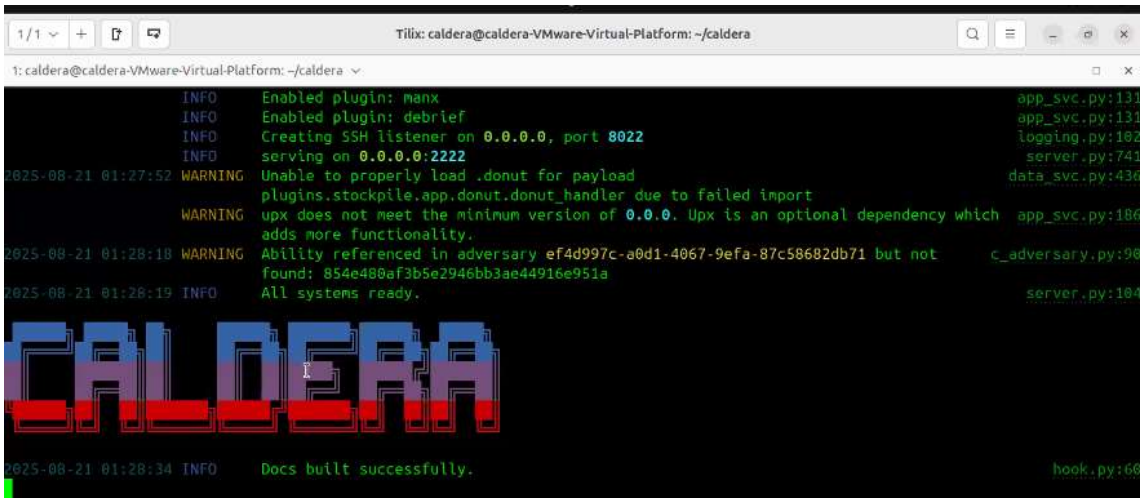
Si te sirvió, conectemos en LinkedIn (¿

Tenemos grupo de estudio!!! Link del servidor de Discord



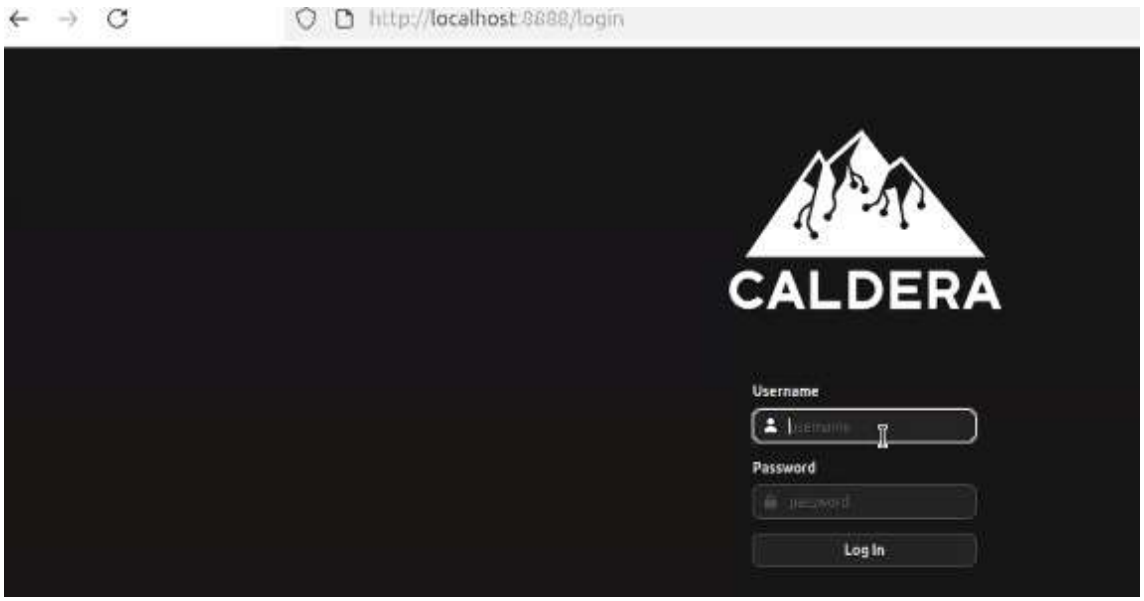
Virtual de Ubuntu 24.04 en VMWARE, el profe recomienda usar DOCKER, se habla bastante de DOCKER, no viene mal aprenderlo!! – Contenedores de Linux - LINK Tambien recomendaron Podman como alternativa a Docker





Si te sirvió, conectemos en LinkedIn (¿

Tenemos grupo de estudio!!! Link del servidor de Discord

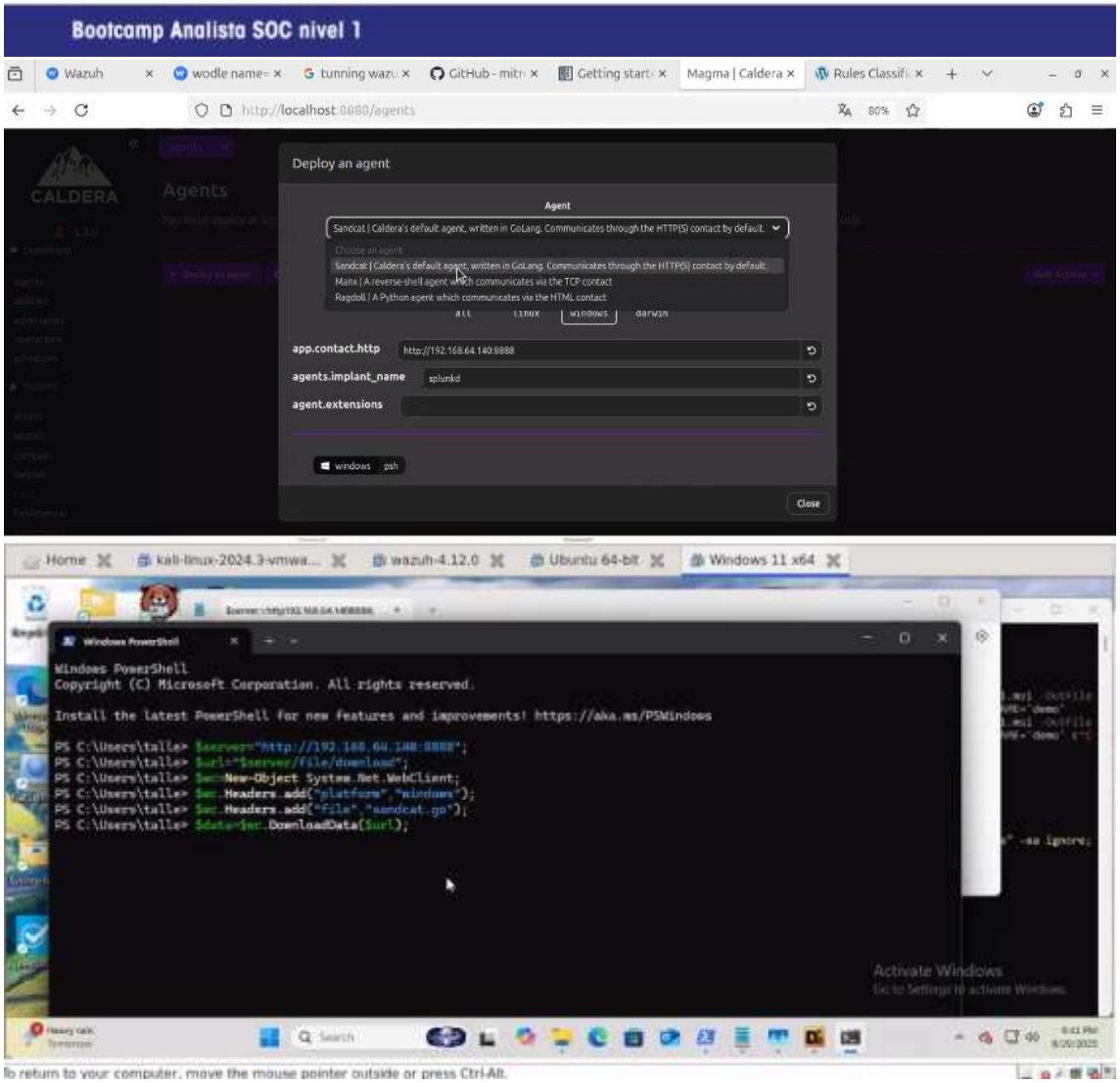


Configurando caldera! – Link de la documentación.

Si te sirvió, conectemos en LinkedIn (¿

Tenemos grupo de estudio!!! Link del servidor de Discord

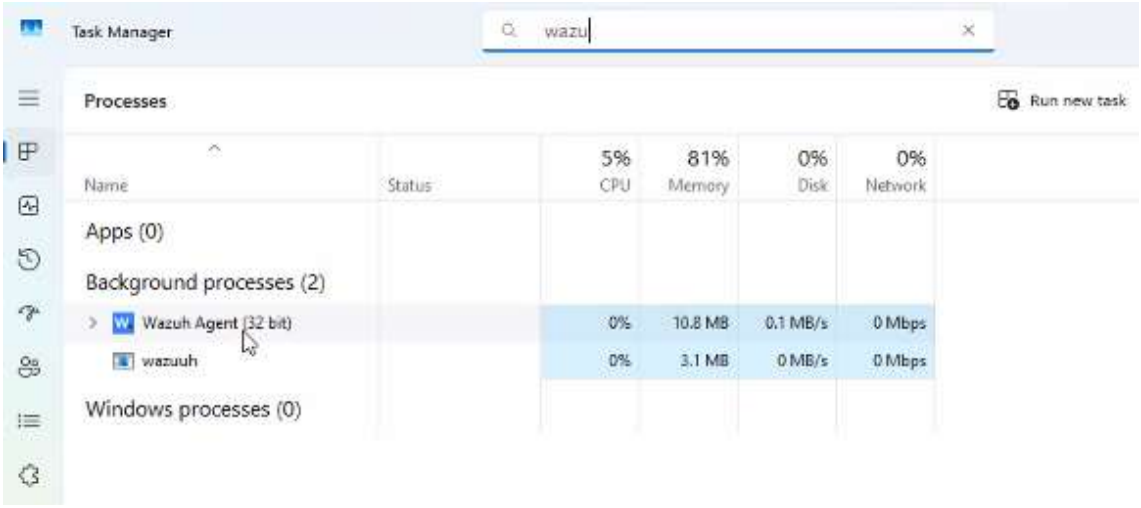
Agentes	Habilidades	Adversarios
GO		



Maquina de victima infectada.

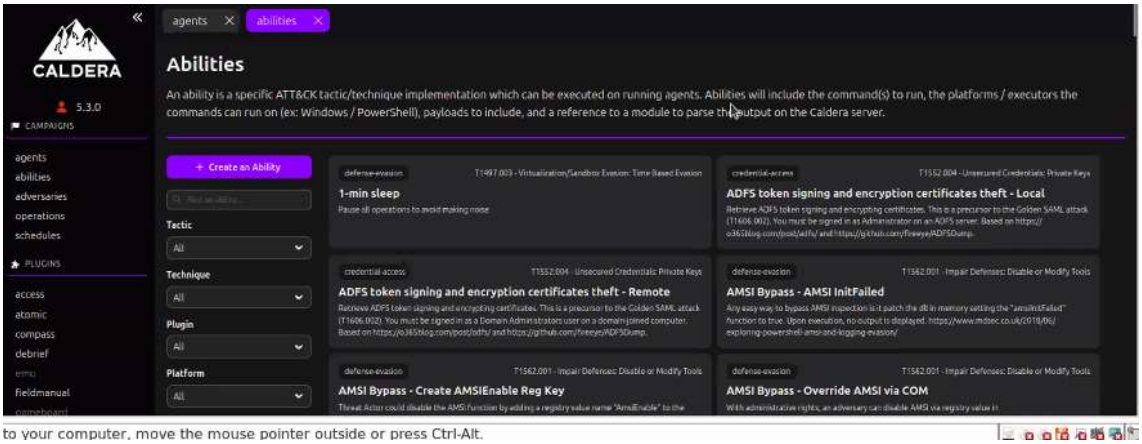
Si te sirvió, conectemos en LinkedIn (¿

Tenemos grupo de estudio!!! Link del servidor de Discord



Ejemplo de maquina infectada con "Wazu'nt" <- Victima de ataque.

Si estas leyendo esto y tu PC/Laptop es una tostadora, podes probar Alpine Linux para las pruebas!! - LINK



Habilidades de Caldera para realizar ataques en la maquina infectada.