Plantilla de informe de prueba de penetración de Satiex

Informe de prueba de penetración de laboratorio

y

Ejercicios del módulo del curso

Versión 1.0 xx  
/xx/xxxx

Nombre

XX-XXXXX

[satiex@satiex.net](mailto:satiex@satiex.net)

# Tabla de contenidos

[Tabla de contenidos 2](#_Toc15575237)

[Introducción 3](#_Toc15575238)

[Objetivo 3](#_Toc15575239)

[Requisitos 3](#_Toc15575240)

[Resumen de alto nivel 4](#_Toc15575241)

[Recomendaciones 4](#_Toc15575242)

[Metodología 4](#_Toc15575243)

[Informes 4](#_Toc15575244)

[Recopilación de información 6](#_Toc15575245)

[Prueba de penetración 7](#_Toc15575246)

[Nombre de host - x.x.x.x 7](#_Toc15575247)

[Resumen 7](#_Toc15575248)

[Exploits/Vulnerabilidades y Recomendaciones 8](#_Toc15575249)

[Referencias 8](#_Toc15575250)

[Mantenimiento del acceso 9](#_Toc15575251)

[Limpieza de la casa 9](#_Toc15575252)

[Apéndices 10](#_Toc15575253)

[Apéndice A – Ejercicios del curso 10](#_Toc15575254)

[Introducción a ... 10](#_Toc15575255)

[1.1.1.1 10](#_Toc15575256)

[Apéndice B – Código PoC 11](#_Toc15575257)

[Nombre de host (nombre de la vulnerabilidad) 11](#_Toc15575258)

# Introducción

# Objetivo

# Requisitos

# Resumen de alto nivel

## Recomendaciones



# Methodology

La metodología utilizada en este compromiso siguió una sólida metodología de pruebas de penetración basada en la Cyber Kill Chain para enumerar y explotar cada host. Este informe detalla cada paso ...

La metodología es la siguiente:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **011-lupa-lupa** | Ilustración de una flecha derecha negra : Free Stock Photo | **022-bomba** | Ilustración de una flecha derecha negra : Free Stock Photo | **020-virus-3** | Ilustración de una flecha derecha negra : Free Stock Photo | **028-navegador** | Ilustración de una flecha derecha negra : Free Stock Photo | **047-usuario** | Ilustración de una flecha derecha negra : Free Stock Photo | **033-archivo-1** |
| **Reconocimiento** | **Militarización** | **Entrega** | **Explotar** | **Escalada de privilegios** | **Acción sobre los objetivos** |

**Reconocimiento**

El inicio de cada enfrentamiento comienza con la realización de un reconocimiento en cada objetivo. El objetivo es...

Las herramientas y técnicas utilizadas en esta etapa incluyen ...

**Militarización**

Esta etapa de la Kill Chain se realiza una vez que se conoce lo suficiente sobre el objetivo desde la etapa de reconocimiento hasta ...

Las herramientas y técnicas utilizadas en esta etapa incluyen

**Entrega**Esta etapa del ataque implica la entrega ...

Las herramientas y técnicas utilizadas en esta etapa del ataque incluyen...

**Exploit**Esta etapa del ataque es donde una vulnerabilidad en una aplicación ...

Las herramientas y técnicas utilizadas en esta etapa del ataque incluyen ...

**Escalada de privilegios**Esta etapa del ataque implica un privilegio de escalada a un ...

Las herramientas y técnicas utilizadas en esta etapa del ataque incluyen ...

**Acción on Objetivos**Esta etapa del ataque generalmente ocurre solo después de comprometer completamente un ...

Las herramientas y técnicas utilizadas en esta etapa del ataque incluyen...

## Informes

En la sección Prueba de penetración del informe, cada host se ha separado en su propia sección, con un resumen, un informe de Kill Chain que detalla cada paso y algunas recomendaciones. Esta forma de organizar el informe permitirá a los administradores de sistemas ...

# Recopilación de información

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dirección IP del host | Nombre de host | Puertos abiertos | Sistema operativo | Servicios y aplicaciones |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Prueba de penetración

## Nombre de host - x.x.x.x

|  |  |
| --- | --- |
| **Nombre de host** |  |
| **Dirección IP** |  |
| **Sistema operativo** |  |
| **Puertos abiertos** |  |
| **Servicios y aplicaciones** |  |
| **Credenciales** |  |
| **Prueba** |  |

### Resumen

|  |  |
| --- | --- |
| **¿Qué funcionó?** | **¿Qué no funcionó?** |
|  |  |

|  |  |
| --- | --- |
| **Kill Chain – Fase 1** | |
| 011-magnifying-glass Reconocimiento |  |
|  |
| 022-bomb Militarización |  |
|  |
| 028-navegador  Explotar |  |
|  |
| **Kill Chain – Fase 2** | |
| 011-magnifying-glass Reconocimiento | A veces, una vez que obtenga acceso a un host, querrá comenzar desde la etapa de reconocimiento nuevamente. En estos casos, puede dividir el informe en Fase 1 y Fase 2. |
|  |
| 022-bomb Militarización |  |
|  |
| 020-virus-3 Entrega |  |
|  |
| **047-usuario**  Escalada de privilegios |  |
|  |
| 033-archivo-1  Acción sobre los objetivos |  |
|  |

### Exploits/Vulnerabilidades y recomendaciones

|  |  |  |  |
| --- | --- | --- | --- |
| **Severidad** | **Exploit/Vulnerabilidad** | **Descripción** | **Recomendación** |
|  |  |  |  |
|  |  |  |  |

### Referencias

# Mantenimiento del acceso

En cada host que se vio comprometido, ...

# Limpieza de la casa

Una vez que habíamos comprometido completamente a un anfitrión, ...

# Apéndices

## Apéndice A – Ejercicios del curso

### Introducción a ...

1.1.1.1  **Investigación ...**

## Apéndice B – Código PoC

### Nombre de host (nombre de la vulnerabilidad)

#!/usr/bin/python

#

#

Fuente - https://www.exploit-db.com/...