Seguridad ofensiva

Informe de prueba de penetración para el examen

email@address.com

OSID: OS-

Tabla de contenidos

[1.0 - Resumen de alto nivel 3](#_Toc40695114)

[1.1 – Recomendaciones 3](#_Toc40695115)

[2.0 – Metodologías 4](#_Toc40695116)

[OS-XXXXX utilizó un enfoque ampliamente adoptado para realizar pruebas de penetración que es efectivo en 4](#_Toc40695117)

[probar qué tan seguros son los laboratorios de seguridad ofensiva y los entornos de examen. A continuación se muestra un resumen de 4](#_Toc40695118)

[cómo OS-XXXXX fue capaz de identificar y explotar una serie de sistemas. 4](#_Toc40695119)

[2.1 - Recopilación de información 4](#_Toc40695120)

[2.2 - Enumeración de servicios 4](#_Toc40695121)

[2.3 – Penetración 4](#_Toc40695122)

[**Vulnerabilidad del sistema: 0.0.0.0**  **(<nombre de host>)** **6**](#_Toc40695123)

[2.4 – Informe – Limpieza de la casa 7](#_Toc40695124)

# 1.0 - Resumen de alto nivel

OS-XXXXX se encargó de realizar una prueba de penetración interna en los Laboratorios de Seguridad Ofensiva y

Red de exámenes. Una prueba de penetración interna es un ataque simulado contra sistemas conectados internamente.

El objetivo de esta prueba es realizar ataques, similares a los de una entidad maliciosa, e intentar

infiltrarse en los sistemas de laboratorio internos de Offensive Security: el dominio THINC.local y la red de exámenes. OSXXXX

El objetivo general era evaluar la red, identificar sistemas y explotar fallas mientras

reportando los hallazgos a Seguridad Ofensiva.

Al realizar la prueba de penetración interna, hubo varias vulnerabilidades alarmantes que fueron

identificados dentro de la red de Offensive Security. Por ejemplo, OS-XXXXX pudo obtener acceso a

Múltiples máquinas, principalmente debido a parches obsoletos y configuraciones de seguridad deficientes. Durante las pruebas,

OS-XXXXX tenía acceso de nivel administrativo a múltiples sistemas. Todos los sistemas fueron explotados con éxito

y acceso concedido. Estos sistemas, así como una breve descripción sobre cómo se obtuvo el acceso se enumeran

abajo:

|  |  |
| --- | --- |
| Blanco | Descripción del acceso |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |

## 1.1 – Recomendaciones

OS-XXXXX recomienda parchear las vulnerabilidades identificadas durante la prueba de penetración para garantizar que un atacante no puede aprovechar estos sistemas en el futuro. Una cosa para recordar es que estos sistemas requieren parches frecuentes y, una vez parcheados, deben permanecer en un programa de parches regular para mitigar vulnerabilidades adicionales que puedan descubrirse en una fecha posterior.

# 2.0 – Metodologías

## OS-XXXXX utilizó un enfoque ampliamente adoptado para realizar pruebas de penetración que es efectivo para probar qué tan seguros son los laboratorios de seguridad ofensiva y los entornos de examen. A continuación se muestra un resumen de cómo OS-XXXXX fue capaz de identificar y explotar una serie de sistemas.

## 2.1 - Recopilación de información

La parte de recopilación de información de una prueba de penetración se centra en identificar el alcance de la prueba de penetración. Durante esta prueba de penetración, OS-XXXXX se encargó de explotar el laboratorio y el examen.

red. Las direcciones IP específicas fueron:

**Red** de exámenes

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

## 2.2 - Enumeración de servicios

La parte de enumeración de servicios de una prueba de penetración se centra en recopilar información sobre qué los servicios están vivos en un sistema o sistemas. Esto es valioso para un atacante, ya que proporciona información sobre posibles vectores de ataque en un sistema. Descripción de las aplicaciones que se ejecutan en el sistema proporciona al atacante información vital antes de realizar la prueba de penetración real. En algunos casos, es posible que algunos puertos no aparezcan en la lista.

|  |  |
| --- | --- |
| Dirección IP del servidor | Puertos abiertos - Servicio |
| 0.0.0.0 | **TCP:**  80 |
|  |  |
|  |  |
|  |  |
|  |  |

## 2.3 – Penetración

La parte de pruebas de penetración de la evaluación se centra en gran medida en obtener acceso a una variedad de sistemas. Durante esta prueba de penetración, OS-XXXXX pudo obtener acceso con éxito a 10 de los 50 sistemas.

Leyenda del color del texto de la consola:

Texto estándar de la consola

Comandos introducidos por el probador de penetración

Salida que deseamos destacar

{...} Salida abreviada para la brevedad

Nota: Los eventos en esta prueba de penetración no ocurrieron necesariamente en el orden descrito en este informe. Además, parte de la salida mostrada en el formato de consola anterior se reconstruyó o modificó (por ejemplo, se reemplazaron los alias). Ambos cambios se han realizado para aumentar la legibilidad de este informe.

|  |
| --- |
| **Sistema vulnerable: 0.0.0.0** (<nombre de host>) **Vulnerabilidades explotadas:**  **Explicación de la vulnerabilidad:**  **Corrección de vulnerabilidad:**  **Gravedad: Crítica**  **Prueba de concepto:**  **Local.txt:**  **Escalada de privilegios:**  **Prueba.txt** |

## 2.4 – Informe – Limpieza de la casa

La limpieza se llevó a cabo después de la evaluación de cada objetivo para eliminar cualquier artefacto de la prueba de penetración. Las eliminaciones incluyeron cualquier cuenta de usuario creada y cualquier archivo cargado en los objetivos. Además, cualquier cambio de configuración realizado se revirtió a su estado original.