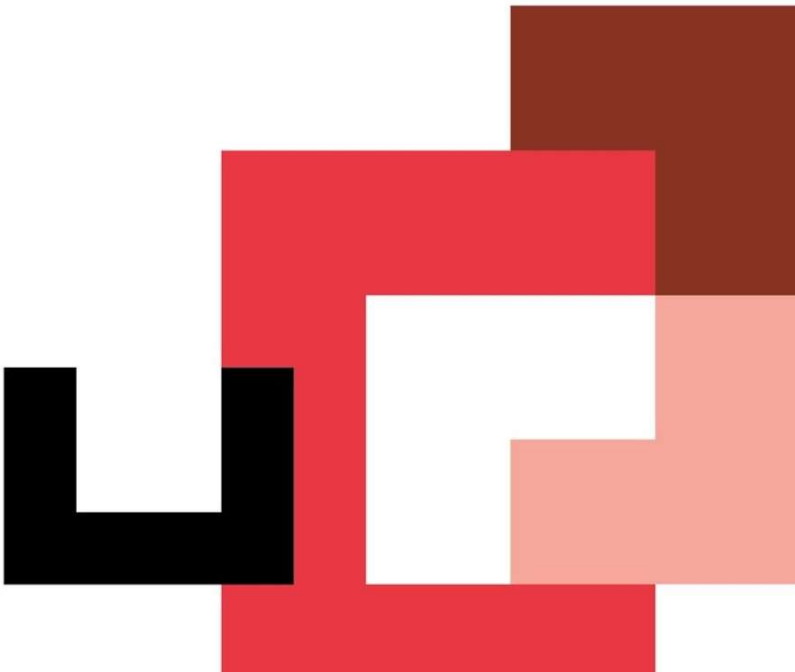
THE BRIDGE

BOOTCAMP Ciberseguridad en formato online



Ponte en situación. Trabajas para una consultora de Ciberseguridad y un cliente te ha pedido que realices un análisis de vulnerabilidades a dos equipos que creen que podrían tener fallos de seguridad; estos equipos son las dos máquinas virtuales que has estado utilizando durante este sprint, Metasploitable y Windowsplotaible. Como resultado final de este análisis de vulnerabilidades tienes que elaborar un informe en el que puedas explicar las vulnerabilidades que has encontrado y los riesgos a los que se puede exponer estaorganización.

Este informe debe constar de dos partes: un **informe ejecutivo** y un **informe técnico**.

A continuación, te explicamos que puntos debe contener cada parte del informe y como debes elaborarlo.

INTRODUCCIÓN

Añade una introducción al documento donde expliques el objetivo del mismo.

INFORME EJECUTIVO

Esta parte del informe tiene que ser muy visual y clara, puedes añadir gráficos que ayude a la comprensión del mismo ya que va dirigido a aquellos roles de una organización que no conocen la parte técnica, pero necesitan comprenderlo de forma rápida para poder tomar decisiones.

El informe ejecutivo debe constar de los siguientes puntos:

1. **Introducción**: breve resumen del objetivo que se plantea. Por ejemplo, en un escenario en el que nos encontramos con dos hosts se ha llevado a cabo un análisis de vulnerabilidades con Nessus y un reconocimiento de puertos y servicios con nmap. Puedes añadir un gráfico en el que expliques los resultados más importantes que has encontrado en estas fases.

2. **Alcance**: explica en qué medida las vulnerabilidades que has encontrado ponen en riesgo la seguridad de la organización.

3. **Vulnerabilidades encontradas**: explica los resultados que has obtenido en el análisis de las vulnerabilidades y a que riesgos se enfrenta la organización ante

estas vulnerabilidades. Por ejemplo, puedes explicar las principales vulnerabilidades que has encontrado y explicar los riesgos a los que se expone la organización. Puedes añadir un gráfico o tabla donde expliques de forma clara pero no muy detallada que vulnerabilidades has encontrado y que riesgos conlleva para la organización.

4. **Soluciones o recomendaciones**: en base a los resultados obtenidos debes explicar que soluciones o recomendaciones darías ante las vulnerabilidades que has encontrado. Para ello te ayudará analizar los resultados que has obtenido realizando el análisis de vulnerabilidades con Nessus. Puedes añadir una tabla o gráfico donde lo expliques de forma clara, aunque no muy detallada.

INFORME TÉCNICO

Esta parte del informe debe de ser más técnico ya que va dirigido a aquellos roles de una organización que deben de comprender en todo su alcance que vulnerabilidades has encontrado y a que riesgo se enfrentan. En esta parte del informe si debes de explicar de forma muy detallada las vulnerabilidades que has encontrado en los sistemas y que recomendaciones o soluciones que darías para poder evitar que un atacante pueda aprovechar dichas vulnerabilidades en beneficio propio.

El informe técnico debe constar de los siguientes puntos:

1. **Introducción**: puedes añadir una descripción que ponga en contexto el análisis que has realizado y que vas a exponer en el informe.

2. **Alcance**: explica en qué medida las vulnerabilidades que has encontrado pone en riesgo la seguridad de la organización.

3. **Vulnerabilidades encontradas**: explicar en detalle las vulnerabilidades que has encontrado y si pueden llegar a explotarse de forma activa, explicación de su criticidad, solución por cada una de las vulnerabilidades encontradas. Mientras que en el informe ejecutivo se explica lo más destacado de los resultados obtenidos presentándolo con gráficas y métricas en este punto del informe técnico hay que explicarlo de forma más detallada.

ANEXOS

En el anexo puedes explicar los niveles de criticidad de las vulnerabilidades, las metodologías que has utilizado como CVE, CVSS y las herramientas que has empleado para la realización del análisis de vulnerabilidades.

RECOMENDACIONES

Te damos una serie de recomendaciones para que puedas elaborar tú primer informe:

1. Añade una portada y pon la fecha en la portada.
2. Añade un control de cambios con una tabla parecida a esta

CONTROL DE CAMBIOS

HISTÓRICO DE VERSIONES/REVISIONES

VERSIÓN	1
TIPO DE DOCUMENTO	Informe de resultados
FECHA	02/04/2022
CAMBIOS REALIZADOS	Informe inicial
REALIZADO POR	Laura Sainz Torres
REVISADO POR	
APROBADO POR	

3. Añade un índice de contenidos.
4. Justifica los márgenes.
5. Si incluyes imágenes o gráficos céntralos en el documento y pon un pie de foto.
6. Utiliza negrita para los conceptos más importantes
7. Limita los colores que utilices, debe quedar un formato sobrio
8. Utiliza un interlineado no muy amplio ni apretado, 1 ó 1,5.
9. No realices preguntas retóricas
10. Escribe en tercera persona o impersonal. No escribas “he detectado”, sino “se ha detectado”
11. Utiliza un fondo blanco


THE
BRIDGE