CODAEP

CIBERSEGURIDAD OFENSIVA Y DEFENSIVA: AMENAZAS, EXPLOTACIÓN Y PROTECCIÓN

PRESENTADO POR
Jhoan y Daniel

1

INTRODUCCIÓN

- ***Contexto y Motivaciones***

La principal motivación que tuvimos fue nuestro interés por la ciberseguridad y por entender cómo funcionan realmente los ataques informáticos.

- ***Justificación CODAEP***

Este proyecto cumple perfectamente las bases de un proyecto informático porque integra diferentes áreas técnicas que hemos aprendido durante ASIX

- ***Estrategia y metodología***

Utilizamos herramientas de planificación como diagramas de Gantt y Kanban para organizar tiempos y hacer seguimiento de las tareas pendientes

OBJETIVOS

- *En cuanto a los objetivos del proyecto, nuestro propósito principal fue desarrollar un entorno práctico de investigación y simulación de ciberseguridad, donde pudiéramos analizar amenazas actuales y estudiar diferentes mecanismos de defensa*

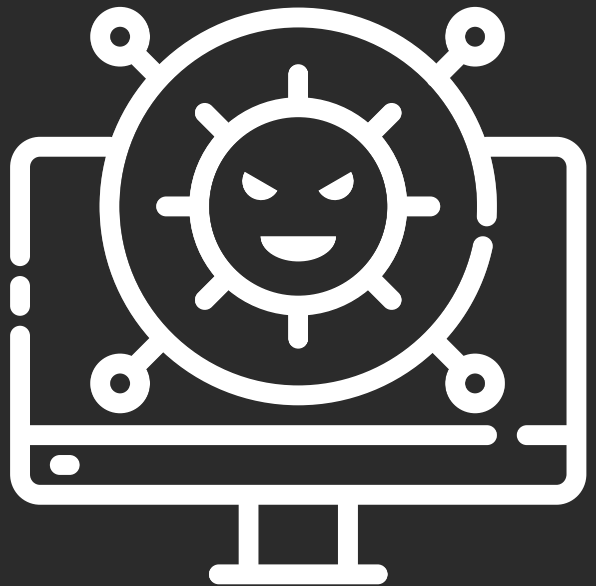
- *Y finalmente, también queríamos desarrollar nuestras capacidades de investigación, análisis técnico y resolución de problemas, además de aprender a documentar correctamente evidencias, resultados y medidas de protección para poder realizar una exposición clara y práctica del proyecto*

ATAQUES Y DEFENSAS

El phishing consiste en engañar al usuario mediante páginas o mensajes falsos para robar información o credenciales.

Simulamos un entorno de phishing utilizando un servidor Apache y páginas HTML falsas

1



El malware es software malicioso diseñado para dañar, espiar o comprometer sistemas.

Investigamos diferentes tipos como virus,escogimos Malware para mediante ingeniería social colar un virus a un sistema.

2

Los ataques de red buscan interceptar, manipular o interrumpir comunicaciones. Practicamos la famosa técnica Man-in-the-Middle

Aprendimos que proteger la comunicación entre sistemas es fundamental para evitar robo de información

3

ATAQUES Y DEFENSAS

Los ataques web explotan vulnerabilidades en aplicaciones y páginas web.

Quisimos explotar el ataque SQL Injection, La investigación y el entendimiento sobre su funcionamiento lo completamos satisfactoriamente

1

Los ataques de fuerza bruta intentan adivinar contraseñas mediante pruebas automatizadas. Utilizamos la herramienta nxc para realizar simulaciones controladas.

Estudiamos contraseñas robustas, límites de intentos y configuración del sistema

2

Los ataques a infraestructura buscan aprovechar configuraciones inseguras, vulnerabilidades o errores dentro de sistemas, servicios y entornos virtualizados.

Investigamos la explotación de vulnerabilidades a APIs.

3

Las insider threats son amenazas provocadas por personas internas de una organización, como empleados o usuarios con acceso autorizado.

Analizamos casos donde un trabajador puede filtrar información, abusar de privilegios o comprometer sistemas, ya sea de forma maliciosa o por negligencia.

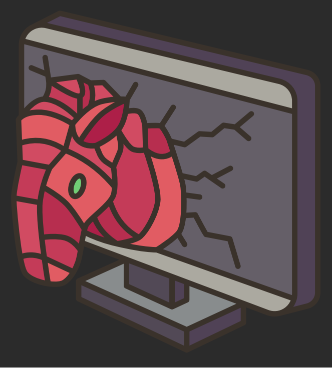
4

3 ROLES DEL PROYECTO

ROL ATACANTE

El objetivo era comprender cómo piensa un atacante y qué técnicas utiliza para comprometer sistemas.

- *Esto nos ayudó a entender que muchos ataques aprovechan errores humanos o malas configuraciones más que vulnerabilidades extremadamente complejas.*
- *Un atacante no es solo ser un experto en sistemas, si no saber como aprovecharse de las comodidades y fallas en los demas.*



ROL DEFENSOR

El objetivo era detectar actividades sospechosas, analizar tráfico y eventos de seguridad, aplicar medidas de protección y comprobar si las defensas eran efectivas frente a los ataques realizados.

- *Aprendimos la importancia de la monitorización, los logs, el hardening y la prevención*
- *Un defensor tambien es un atacante*
- *Por mas experto que seas en sistemas, al final podras defender todo al 100%*

EXPLICACIÓN LABORATORIO

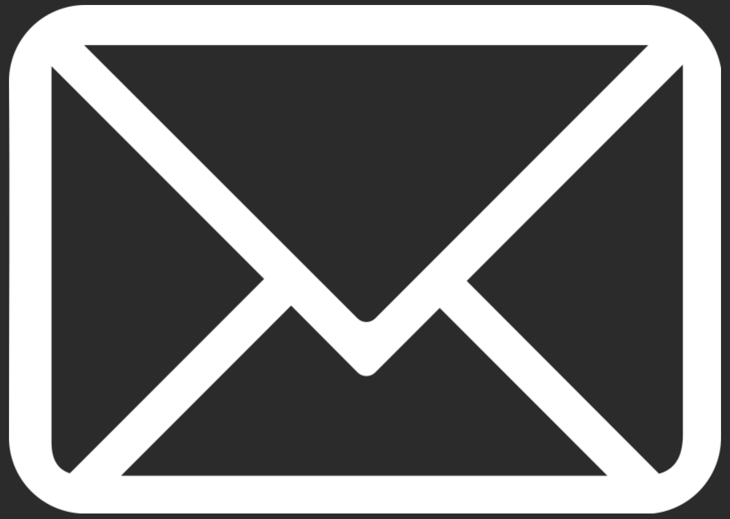
#1
¿Como lo preparamos?

#2
Elección de Herramientas

#3
Tecnologías

#4
Justificación

4 CONCLUSIONES Y DEMO



Preparamos 2 Demostraciones

Malware e infraestructuras

Conclusiones FInales

PRESENTADO POR

Jhoan Obando

Daniel Triaz

GRACIAS POR SU ATENCION.