Asociación de Seguridad Ofensiva de Coruña

Índice de contenidos.

1. Descripción
2. Contenidos
    2.1. Arquitectura de computadoras
    2.2. Sistemas operativos
    2.3. Aplicaciones de nivel de usuario
    2.4. Redes de computadoras

Descripción:

La Asociación de Seguridad Ofensiva de Coruña (De aquí en adelante ASOC) pretende ser una asociación estudiantil de carácter formativo, sin ánimo de lucro e íntimamente ligada al grado en Ingeniería Informática.

La rama de conocimiento general de la ASOC es la seguridad informática, en su forma específica se basará en cuatro pilares:

1. Arquitectura de computadoras.
2. Sistemas operativos.
3. Aplicaciones de nivel usuario.
4. Redes de computadoras.

Contenidos: (provisional)

Como se introdujo al comienzo de este documento, los bloques fundamentales del contenido de las reuniones serán:

1. Arquitectura de computadoras.
2. Sistemas operativos.
3. Aplicaciones de nivel usuario.
4. Redes de computadoras.

La elección de estos y el orden en el que se imparten no es aleatorio, si no que sale de la filosofía: desplazarse de menor a mayor grado de abstracción.

1. Arquitectura de computadoras:

Sobre el **primer bloque** se tratará de mostrar la arquitectura de un computador, incluyendo:

Concepto de computadora
Historia de las computadoras
Sistemas de numeración (BIN/OCT/HEX)
Maquina de Turing
Arquitectura Von Neumann
Concepto de biestable
Algebra de Boole

Puertas lógicas
Flip Flops
Introducción al concepto de señal

La unidad de memoria
El direccionamiento de memoria
El registro
El bus de interconexión
La unidad aritmético lógica
Entrada salida

Paralelamente se ofertará un curso básico de las herramientas necesarias para el proyecto:

El sistema linux
- Instalación de linux y puesta a punto
- Manejo básico de la terminal bash

Introducción al lenguaje C
- Operaciones aritméticas y variables
- Control de flujo
- Sentencias repetitivas
- Funciones y parámetros
- Punteros
- Estructuras básicas
- Operaciones bit a bit

La suite gcc
- Uso básico de gcc

La suite gdb
- Uso básico de gdb

La finalidad de este bloque, de duración estimada 4 meses es la elaboración de un emulador de un sistema basado en arquitectura RISC muy simple. Tal vez el propio Simplez ó el archiconocido 8-CHIP.

Las correspondencias con asignaturas oficiales del grado son: FC, IB y EC.

2. Sistemas operativos:

Este segundo bloque será el primero en introducir conocimientos propios de la rama de seguridad. En concreto el concepto de **rootkit** y una introducción a los fundamentos que darán pie en el tercer bloque a la explicación de las técnicas basadas en el **overflow** y el **return oriented programming.**

Los contenidos, mucho menos extensos serán:

Introducción al kernel UNIX
Sistema de ficheros
Memoria
Procesos
Entrada/Salida

Secuencia de inicio de la arquitectura x86
Introducción a la programación concurrente

En paralelo se hará una breve introducción al lenguaje ensamblador para x86, siguiendo el manual oficial publicado por Intel. Y a las principales estructuras de datos necesarias para el correcto inicio de un sistema operativo moderno (GDT, IDT, A20 Gate, etc).

Se enseñarán también las siguientes herramientas:
qemu
gdb avanzado
docker

El objetivo es la elaboración de una ambiciosa práctica final, que se hará entre todos los alumnos y tiene una duración esperada de 4 meses:

Elaborar un kernel multiproceso UNIX-LIKE.

Para esto se seguirán los libros:
-BSD UNIX Operating System S.J. Leffler, M.K. McKusick.
-Design of the Unix Operating System M.J. Bach.

Las corespondencias con asignaturas son: EC, SO, AL y CP

Aplicaciones de nivel usuario:

Este bloque, será el primero íntegramente dedicado a la seguridad.
En el veremos como analizar y atacar un programa escrito para el entorno de usuario.

Los contenidos son:

Desensamblado de binarios.

Análisis de binarios e ingeniería inversa.

El concepto de overflow.
El concepto de return oriented programming.
Shellcode y payloads.

Identificación de vulnerabilidades.
Elaboración de exploits.

Análisis de malware.

Automatización de la explotación.
Introducción al proceso de un pentesting en entornos profesionales.

En paralelo se enseñará python a un nivel básico y el uso de las siguientes herramientas:

objdump, metasploit framework, tenable nesus, nmap, etc.

La prueba de fin de bloque de duración también 4 meses, consistirá en una pequeña olimpiada en la cual todos los alumnos competirán por un premio simbólico, el sistema de la olimpiada es el conocido como CTF (Capture the flag)

(Se valorará la posibilidad de abrir esta prueba a toda la comunidad universitaria, no solo a miembros de la asociación. Entendiendo la competición sana como uno de los medios mas efectivos para incentivar el ingenio y la iniciativa personal).

Las correspondencias con asignaturas son: SO, LSI, ISD y XP.

Redes de computadoras:

Esta parte final del curso, pretende finalizar las áreas de conocimiento básicas de todo aspirante a convertirse en profesional de la ciberseguridad.

En este bloque se verán conceptos de redes básicos tales como:

Modelo OSI
Concepto de protocolo
Fundamentos de redes LAN

Análisis de protocolos
Ataques sobre contraseñas y cifrados

Ataques en redes LAN
Técnicas de intrusión en servidores remotos
Seguridad en servicios web
Seguridad en IPv6

Seguridad en dispositivos móviles
Seguridad en IoT
Nuevas técnicas de intrusión.
Ataques basados en IA (Por petición popular)

Paralelamente se enseñarán: python avanzado, fundamentos de SQL, fundamentos de html, fundamentos de JS, la librería SCAPY y las herramientas: Wireshark, Aircrack, Zanti, Dsniff, hashcat. También se hará uso de portales como: haveibeenpwned.

Tanto la duración como la prueba que finaliza este bloque no están definidas todavía.