Curso de Ciberseguridad

Pautas del curso

- **El curso esta armado en 14 clases de 2 horas y 30 minutos de duración, de 17:30 a 20:00 horas, con un break de 15 minutos.**
- **Esta creado para ser interactivo con los asistentes, por lo que en caso de necesitar interrumpir por una duda o consulta, está permitido, lo mismo para interactuar.**
- **Hay un temario aceptado y validado, se debe respetar el orden del mismo.**
- **El instructor, antes de iniciar la primer clase, explicará todo lo que se necesita a nivel de configuración y laboratorios.**
- **Muchos ejercicios hay que enviarlos por mails o subirlos a la plataforma, donde los mismos serán evaluados y con un feedback en caso de ser necesario.**
- **Por clase, se realizarán varios prácticos o laboratorios.**

Telefónica

Temario

1. REDES Y APLICACIONES TÉCNICAS Y SEGURIDAD WIRELESS
2. INTRO LINUX & HACKING CON PYTHON
3. CRIPTOGRAFÍA Y ESTEGANOGRAFÍA
4. ANÁLISIS FORENSE DE SISTEMAS INFORMÁTICOS
5. HACKING ÉTICO
6. METASPLOIT
7. VULNERACIÓN DE MECANISMOS DE IDENTIFICACIÓN Y AUTENTICACIÓN

Telefónica

00

Introducción Ciberseguridad

Los principios teóricos a conocer

Telefónica

Hacking Ético y la Seguridad de la Información

El antes y el ahora

El antes:

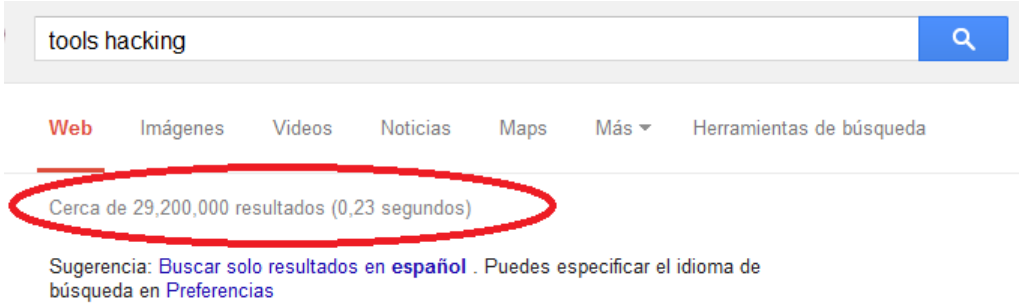
En los años 80, se tienen conocimientos de los primeros ataques, donde se realizaban sobre sistemas individuales o centralizados, inclusive hasta mediados de la década del 90, los cuales el método de traslado era a través de un acceso local o por línea telefónica.

Conexiones de redes a través de módems

Telefónica

Hacking Ético y la Seguridad de la Información

- Realizar un ataque informático hoy en día no requiere de gran conocimiento y es numerosa la cantidad de información que hay, tanto de tutoriales como de herramientas free



- Los ataques alcanzaron una madurez que sobrepasan el alcance de la legislatura, todavía hay países que no cuentan con leyes

www.cybercrimelaw.net

Telefónica

Hacking Ético y la Seguridad de la Información

Seguridad Informática VS Seguridad de la Información

- La seguridad informática es un área que se ocupa de la protección de toda la infraestructura relacionada con la informática (sean medios de contención de información, dispositivos, etc)

- Nos ocupamos de crear, diseñar, aplicar normas, técnicas para obtener una seguridad en el entorno que sea confiable, actualizable y que fomente esa protección

- Mientras que la seguridad de la información se ocupa de todo lo relacionado con la información en si, utilizando medidas como la prevención, protección y resguardo, y sobre todo mantener la disponibilidad, integridad y confidencialidad.

Telefónica

Hacking Ético y la Seguridad de la Información

- No existe una conciencia en materia de seguridad de la Información

SE NECESITAN MUCHAS MAS CHARLAS DE CONCIENTIZACION!!!

- Se observa que se convierte en un negocio (para quien?) quien es el principal beneficiado?

**En el año 2017,
Se reportaron entre
robos de cuentas
y perdidas operacionales,
por un valor aproximado de mas de
2000 millones de dólares, por ejemplo
Sony reporto 400 millones u$s en el
ultimo ataque**

Telefónica

Hacking Ético y la Seguridad de la Información

Que es la Ciberseguridad?

Explicación WIKIPEDIA:

La **ciberseguridad** es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

Es el área que se encarga de la privacidad y protección de datos de las empresas y las organizaciones para **hacer** frente a los ciberataques

Telefónica

Hacking Ético y la Seguridad de la Información

Que es un Ethical Hacking?

El objetivo de un Ethical Hacking (hacking ético) es explotar las vulnerabilidades existentes en un entorno a través de un test de intrusión (Penetration Test o Pentest) donde se verifica y se corrobora la seguridad tanto lógica como física en las redes, sistemas de información, aplicaciones, servidores, etc

La idea es ganar acceso y demostrar que un sistema es vulnerable, donde la información obtenida contribuirá para que la organización involucrada en el test, pueda tomar medidas preventivas y/o reactivas, y todo de manera AUTORIZADA

Lo que se realiza es una simulación de varios escenarios donde se intentara reproducir diversos ataques en entornos controlados

Telefónica

Hacking Ético y la Seguridad de la Información

Fundamentos basados en normas

A lo largo de toda la seguridad informática, se podrá contar con muchas certificaciones, tanto en lo técnico, en los procesos, en la información.

Telefónica

Hacking Ético y la Seguridad de la Información

Sitios como :

SecurityFocus.com

Antes se tardaba mucho en generar el exploit !!!!

Telefónica

Hacking Ético y la Seguridad de la Información

ES NECESARIO COMPRENDER EL FUNCIONAMIENTO DE UNA RED

Aplicaciones, Http, FTP, SSH, SMTP, POP3

Estandariza la forma en que se presentan los datos.

Establecer, administra y termina sesiones entre Host

TCP-UDP

Direccionamiento IP, Enrutamiento

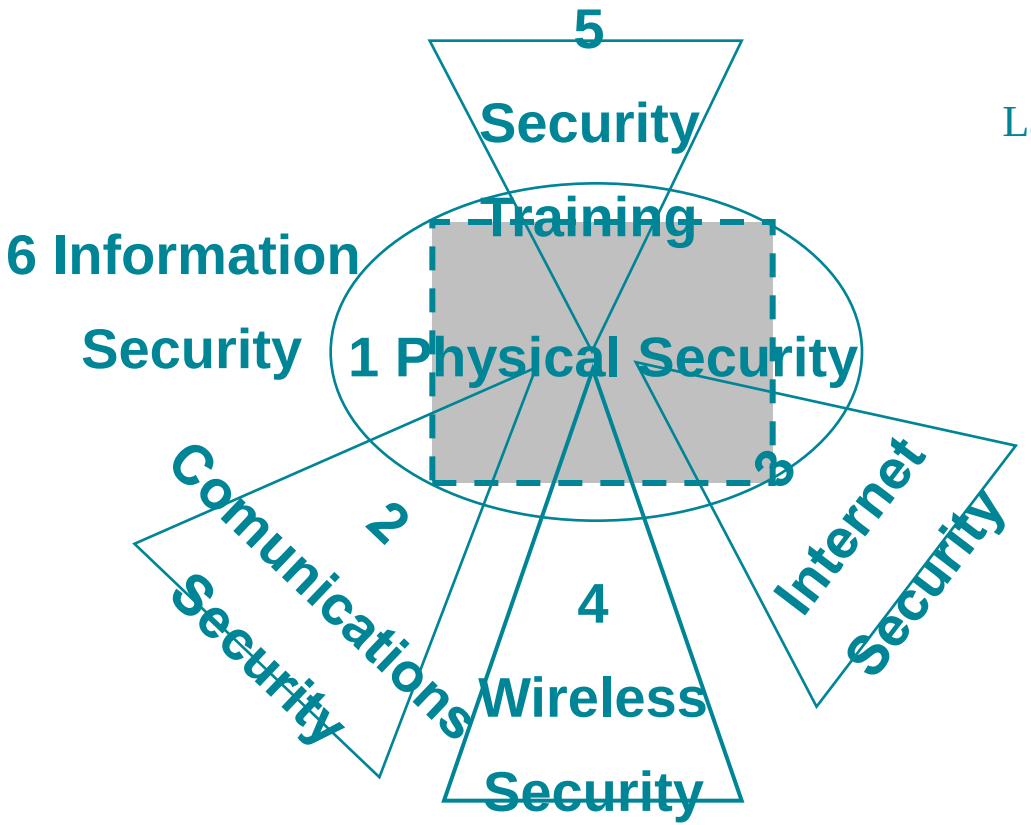
Switches, Bridge, MAC Address

Medios de trasmisión: Cables, Radiofrecuencias, F.O, AP, Hubs

Telefónica

Hacking Ético y la Seguridad de la Información

Que tener en cuenta para tener presencia de seguridad en la Organización?
Fuente OSSTMM, Open Source Security Testing Methodology Manual



¿Qué Testear?

Las 6 Secciones del mapa son

1- Seguridad Física
2- Seguridad en comunicaciones
3- Seguridad en Internet
4- Seguridad Wireless
5- Capacitación en Seguridad
6- Seguridad de la Información

Telefónica

Metodologías de Penetration Testing

Conceptos y Definiciones

El **hacking** corresponde a todos los métodos de penetración utilizados por los distintos tipos de hackers

El **hacking ético** esta relacionado con el descubrimiento de los fallos de seguridad y vulnerabilidades para garantizar la seguridad del sistema.

Un **Pentest o prueba de penetración** es un término específico y que se centra sólo en el descubrimiento de las vulnerabilidades, riesgos, y el entorno de destino con el propósito de asegurar y tomar el control del sistema.

Telefónica

Metodologías de Penetration Testing

Conceptos y Definiciones

Los ataques, técnicas y errores más vistos durante estos últimos años

Keylogging, troyanos, spoofing, Password cracking, Denegación de servicio, arp poison

War dialing, voip sniffing, vishing, clonaciones.

Dumpster diving, Robo o extravío de notebooks, ingeniería social, destrucción de documentos

XSS, SQl Injection, pharming, phishing, ransonware, spam, spyware, snmp walk , information gathering, Exploits

War driving, man in the middle, war nibbling, wep cracking, sniffing

Telefónica

Metodologías de Penetration Testing

Conceptos y Definiciones

Violación de la privacidad de los empleados

Violación de e-mails

Port scanning

Mails “anónimos” con información crítica o con agresiones

Propiedad de la Información

Backups inexistentes

Destrucción de soportes documentales

REDIRECCIONAMIENTO DE PUERTOS

Acceso indebido a documentos impresos

Escalamiento de privilegios

Interrupción de los servicios

Acceso clandestino a redes

Violación de contraseñas

Intercepción de comunicaciones

Destrucción de equipamiento

Fraudes informáticos

Virus & Gusanos

Indisponibilidad de información clave

Servicios de log inexistentes o que no son chequeados

Instalaciones *default*

Últimos parches no instalados

Robo de información

Programas “bomba”

Telefónica

Metodologías de Penetration Testing

Conceptos y Definiciones

A lo largo del crecimiento tecnológico, hemos visto también el nacimiento de nuevos términos: analista de sistemas, programador, auditor, técnico informático, hasta habremos escuchado: "SER HACKER"

Una palabra mal utilizada por varios medios, donde se asocia a un delincuente informático o atacante malicioso como un "HACKER"

En esta unidad, hablaremos de un nuevo concepto: ETHICAL HACKING

Que es? Un procedimiento donde se toma medidas preventivas contra posibles ataques maliciosos, a través de utilizar los mismos métodos de un atacante, vulnerando su propia red en búsqueda de posibles fallas de seguridad y poder brindar un informe acorde a lo encontrado

Telefónica

Sobre Análisis Forense (el después del incidente)

Aprender los componentes en una FASE DE INVESTIGACIÓN

Prueba de los ilícitos informáticos/Evidencia digital

Aspectos procesales según la legislación internacional y local
Sentencia / Legislación y jurisprudencia nacional e internacional

Exposición de Obtención ilícita/lícita de pruebas
Valor probatorio de los documentos electrónicos / correo electrónico.
Falsificación de documentos electrónicos
Diseño de políticas para el resguardo de la evidencia digital en caso de incidentes
Pasos para la construcción de un caso forense
Software de apoyo a las pericias / Análisis de dispositivos Móviles

Telefónica

En que me beneficia este curso

Comprender las técnicas básicas y necesarias para poder meterse en el mundo de la Seguridad Informática

Tener la posibilidad de ofrecer los conocimientos aprendidos en escenarios comprometidos con incidentes

Aprender y conocer los distintos métodos de protección

Y por último, meterse en un mercado laboral de alto crecimiento, acorde a la tecnología

Telefónica

Telefónica