UTN.BA UNIVERSIDAD TECNOLÓGICA NACIONAL FACULTAD REGIONAL BUENOS AIRES | Centro de e-Learning Secretaría de Cultura y Extensión Universitaria

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Experto Universitario en Ethical Hacking

UTN.BA | Centro de e-Learning
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES
Secretaría de Cultura y Extensión Universitaria

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Módulo 4:

Ethical Hacking

Unidad 1:

Introducción sobre Ethical Hacking

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Presentación

En esta primera Unidad del módulo, especialmente los participantes podrán comprender que es el Ethical Hacking y que tan importante es el peligro que un activo se encuentre expuesto y vulnerable.

Conocerán varias etapas y fases que hay que realizar para poder realizar un análisis completo y detallado.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Objetivos

Que los participantes logren…

- Aprender sobre los conceptos expuestos en el mundo del Hacking.

- Conocer las herramientas y metodologías necesarias para realizar tareas de análisis de vulnerabilidades y test de penetración (Pentesting), con una filosofía enfocada en la ética profesional.

- Comprender la importancia de usar cifrado seguro en aplicaciones, abordar vulnerabilidades y potenciales ataques y amenazas, así como la correcta concientización en los usuarios.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Bloques temáticos

1. Introducción sobre el Ethical Hacking
2. Conceptos y Metodología
3. Tareas del Ethical Hacker
4. Ejercicios (distribuidos en la unidad)

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Introducción sobre el Ethical Hacking

Situación hace años:

En la década del 80 se realizaban ataques sobre sistemas individuales o centralizados, inclusive hasta mediados de la década del 90 se materializaban a través de un acceso local o por línea telefónica.

Se acuerdan de los modem…

Modem Robotics 56K

Placa Interna de Modem

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Con la llegada de Internet los ataques crecieron por varios factores:

- Acceso global a bajo costo
- Las empresas necesitan exponer sus servicios e información en Internet
- Posibilidad de anonimato o rastros débiles

Efectivizar un ataque hoy no requiere un gran conocimiento y se disponen de herramientas libres para todo tipo de ataques.

- Los ataques pueden sobrepasar el alcance de la legislatura
- No se le da importancia a tener conciencia en materia de Seguridad de la Información.
- Se convierte en un negocio

Hoy le damos a través de un celular Internet a nuestros dispositivos

Entonces que se dispone con este avance tecnológico:

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

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

Keylogging, troyanos, Spoofing, Password cracking, Denegación de servicio (DOS), 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

Violación de la privacidad de los empleados / Violación de contraseñas

Ingeniería Social / Violación de e-mails / Port scanning / Intercepción de comunicaciones

Mails “anónimos” con información crítica o con agresiones / Destrucción de equipamiento / Fraudes informáticos

Propiedad de la Información / Virus & Gusanos / Backups inexistentes / Indisponibilidad de información clave

Destrucción de soportes documentales / Servicios de log inexistentes o que no son chequeados

Acceso indebido a documentos impresos / Redireccionamiento de Puertos

Escalamiento de privilegios / Interrupción de los servicios / Instalaciones default / Últimos parches no instalados

Acceso clandestino a redes / Robo de información / Programas “bomba”

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Código malicioso en móviles: por ejemplo SPIM todos los ataques Bluetooth (bluesnarf, blueoover, etc)

-Malware Cero day (0 Day)

-Secuestro de Archivos: llamado Ransomware: cifran el disco y piden rescate por la clave del cifrado

-Regionalización de la codificación: los ataques ahora no son a todo el mundo sino a ciertos segmentos por ejemplo, Phishing sólo a usuarios del dominio del banco que simulan, o Spam en castellano para países de Latinoamérica

-Ataques a nuevos dispositivos: RFId, dispositivos controlados por internet por ejemplo semáforos, cámaras IP, etc.

-Redes Zombies: conjunto de computadoras que se encuentran troyanizadas y las venden para campañas de Phishing o Spam o ataques distribuidos.

-Pharming: envenenamiento de las tablas de los DNS.

SORPRENDIDOS/AS por la cantidad y variantes????

Hay muchos más, los cuales la mayoría son derivaciones de los ya mostrados

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejercicio Número 1 Unidad 1

EJERCICIO: seleccionar 1 técnica de ataque y hacer una breve descripción de la misma, por ejemplo detallar de qué se trata la técnica de Phishing, no se pide realizar la técnica, únicamente explicar que entienden por la misma.

Subirlo en el foro de la unidad correspondiente por favor, exponer con capturas o pantallas.

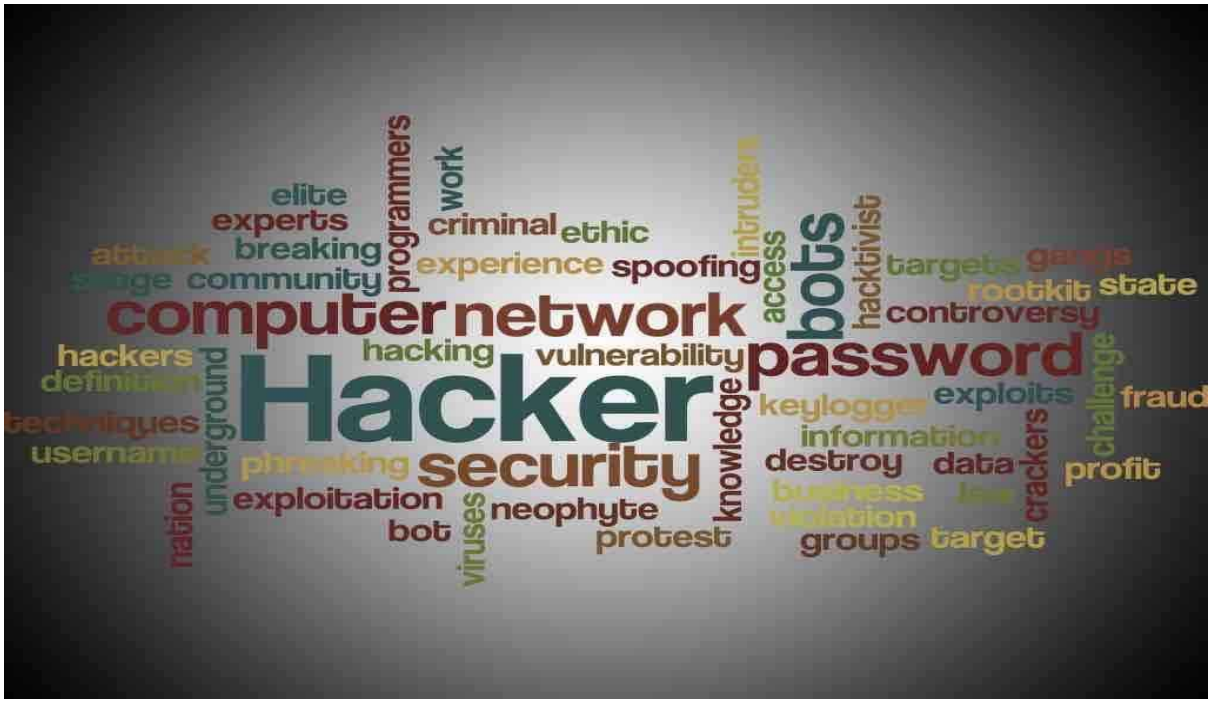
Recordar: el post es individual de cada alumno, no subir el ejercicio en post ajeno

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Conceptos y Metodologías

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 de comunicación, donde se asocia a un delincuente informático o atacante malicioso como un **"HACKER"**



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

¿Qué significa?

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

¿Qué es un Intruso informático?

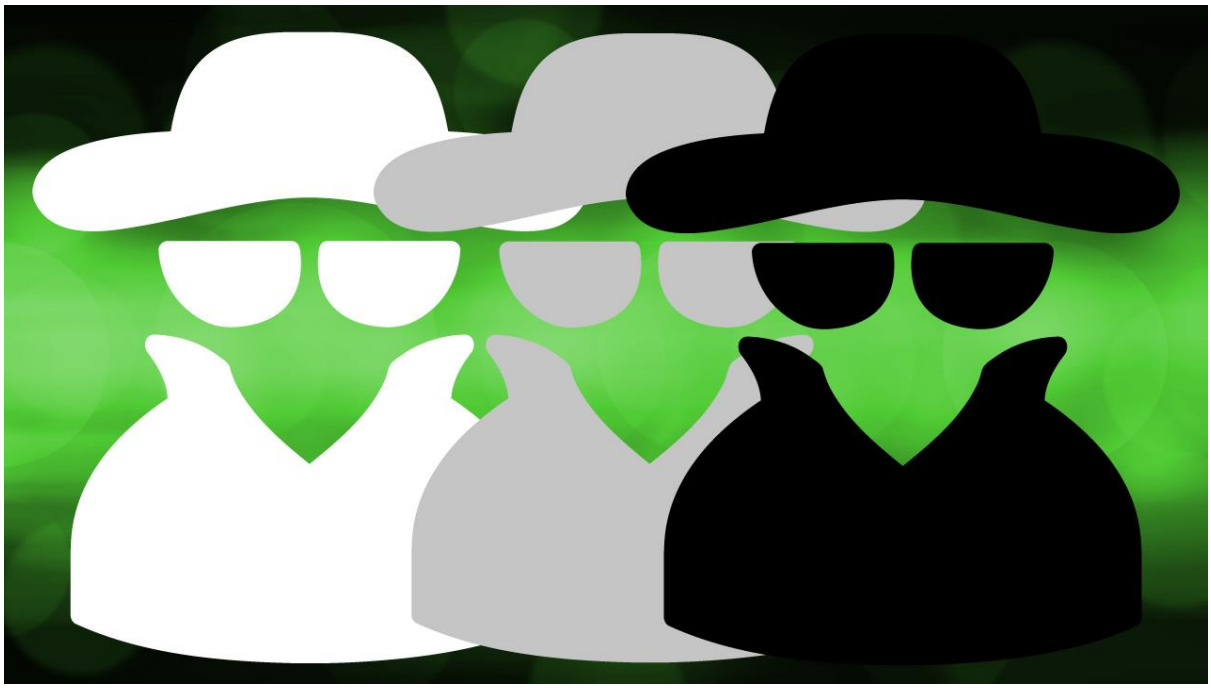
"Alguien que quiere acceder a los sistemas con o sin autorización pero con fines que pueden perjudicar a la organización".

Y en este mundo Underground existen términos como "El Mundo de los Sombreros"

- **White Hat**: "Los chicos buenos" también llamados "Samurai´s" a los que trabajan para las fuerzas de seguridad o agencias de inteligencia.

- **Grey Hat**: "Mercenarios" trabajan con el que más paga, por ende carecen de ética.

- **Black Hat:** " Los chicos malos" crackers, virusers y otros



Tomar estas categorías como significativas a lo que cada "Hacker" tiene como tarea, función u objetivo.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

A las pruebas de penetración o intrusión que se utilizan, llevan el nombre de:

PENTEST o TEST DE INTRUSION

Primero veamos los distintos tipos de test:

- ✓ **Intrusión con objetivo:** se busca las vulnerabilidades en componentes específicos de los sistemas informáticos de mayor importancia

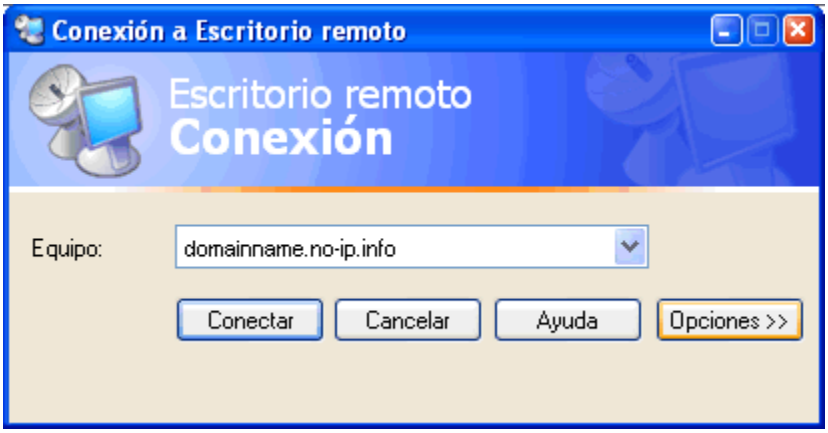
- ✓ **Intrusión sin objetivo:** examina la totalidad de los componentes en los sistemas informáticos presentes

También hay que tener en cuenta el lugar físico donde se realizará el Pentest.

Lleva el nombre de **PENTEST EXTERNO**, si el mismo se realiza desde fuera del área a chequear, por ejemplo, hacer un **PENTEST** a una empresa desde la casa de uno, en forma remota.

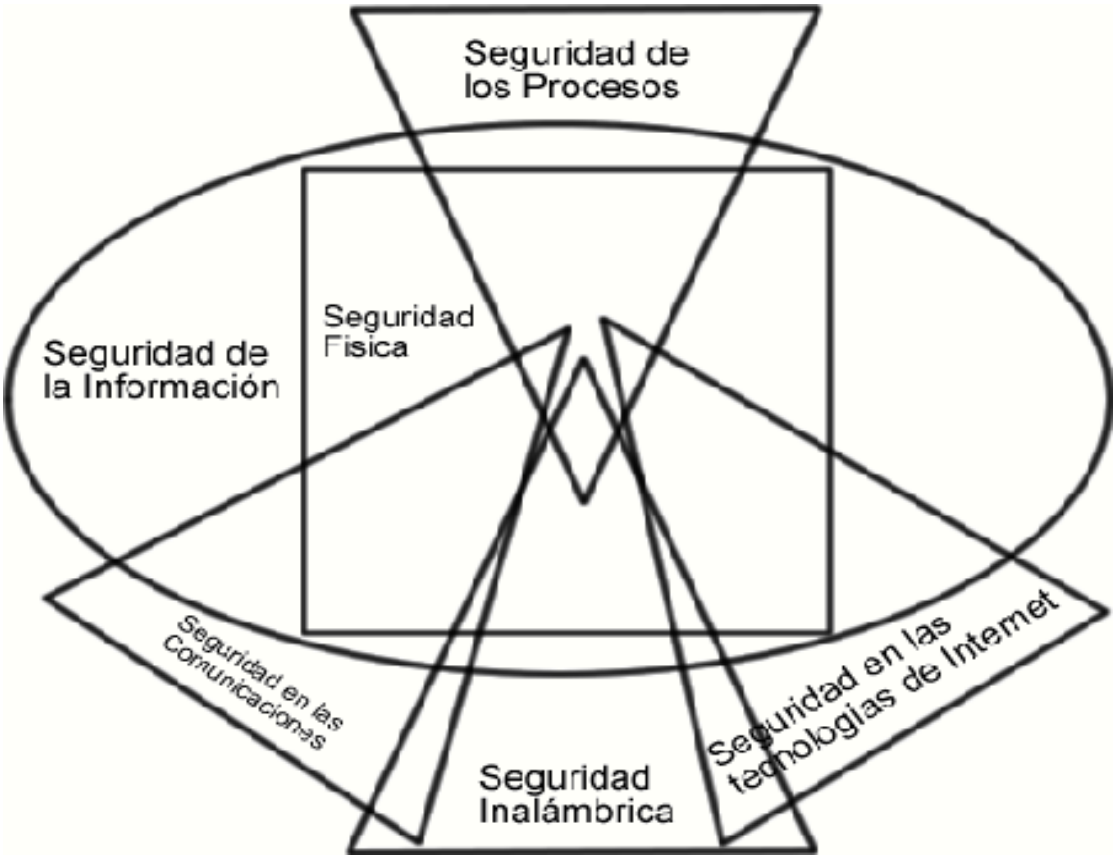
El nombre de **PENTEST INTERNO**, es el que define que el chequeo se realizara dentro del objetivo, por ejemplo, el cliente nos da una oficina con conexión a su **LAN** y desde ahí realizamos el test correspondiente

Puede ser el caso, de que el PENTEST INTERNO, se realice desde fuera, por ejemplo, a través del uso de una VPN o del uso de un escritorio remoto.



Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Una vez seleccionado el tipo de Pentest, uno tiene que dirigirse al uso de alguna metodología, por ejemplo, le exponemos OSSTMM.



Fuente OSSTMM, Open Source Security Testing Methodology Manual

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

¿Qué Testear?

Las 6 Secciones del mapa de seguridad son:

1- Seguridad Física

2- Seguridad en comunicaciones

3- Seguridad en las tecnologías de Internet

4- Seguridad Wireless

5- Seguridad de los procesos

6- Seguridad de la Información

La gráfica anterior quiere explicar que lo que un pentester debe evaluar no sólo es dentro de la empresa que están delimitados en la sección 1 sino que también hay conceptos a evaluar fuera de los límites, por ejemplo, seguridad inalámbrica ya que pueden ser interceptados desde afuera de los límites de la empresa.

Estos puntos son importantes, no significan el paso a paso ni un orden a seguir, significa todo lo que hay que tener en cuenta, cuando se habla de analizar la seguridad en un **TODO**

Un Pentester desarrolla sus tareas a través de ambientes más detallados:

- **Blind/Blackbox:** no cuenta con ninguna información del objetivo, pero el cliente tiene conocimientos de qué tipo de test se realizaran y cuando.

- **Double blind/ Blackbox:** no cuenta con ninguna información del objetivo y el cliente no cuenta con información sobre las tareas a realizar como así tampoco sobre el cuándo se harán.

- **Graybox:** solo conoce información parcial sobre los objetivos, dicha información será seleccionada por el cliente, el cliente tiene conocimientos de qué tipo de test se realizaran y cuando.

- **Double Graybox:** solo conoce información parcial sobre los objetivos, dicha información será seleccionada por el cliente, el cliente conoce las técnicas a utilizar pero no conoce el cómo y el cuándo estas serán utilizadas.

- **Whitebox:** tiene pleno conocimiento del objetivo, dicha información será entregada por el cliente, antes de iniciado el test, el cliente tiene pleno conocimiento de las tareas a realizar, del cómo y el cuándo.

- **Reversal:** tiene pleno conocimiento del objetivo, dicha información será entregada por el cliente, antes de iniciado el test, el cliente no cuenta con información sobre las tareas a realizar, como así tampoco sobre el cuándo.

Estos son las modalidades de tareas, con las cuales además de la forma, se hace **HINCAPIE** sobre la confidencialidad de las mismas.

Mediante un contrato, se especifica que no habrá ninguna fuga de los datos obtenidos, como así también un trato directo y único con el empleador.

Más adelante veremos en detalle, un modelo de convenio de confidencialidad.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Las etapas para contratar y realizar el **PENTEST** son:

- Entrevista con el cliente para definir el alcance de la intrusión
- Convenio del acuerdo de confidencialidad
- Briefing de los objetivos
- Definición de herramientas y tareas a utilizar
- Trabajo de campo
- Entrega del informe

Con o sin el Acuerdo de No Divulgación, el analista de seguridad esta éticamente obligado a mantener la confidencialidad y garantizar la no divulgación de la información del cliente ni los resultados del análisis.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Hablamos de la metodología de OSSTMM, agreguemos algunos datos más:

OSSTMM es un conjunto de Reglas y Guidelines para **cómo testear, qué testear y por qué testear los eventos**, por eso para que un test deba ser considerado dentro del OSSTMM debe:

- Ser cuantificable
- Consistente
- Válido en el tiempo más allá del "Ahora"
- Cumplir con las leyes individuales y locales y el derecho a la privacidad

El OSSTMM es un manual de seguridad, en el que participan abiertamente profesionales de todo el mundo, y que cumple con los estándares ISO 27001 y las normas dictadas por organismos internacionales. (Orange Book, ICM3)

OSSTM – Alineación con Estándares Internacionales y Leyes Vigentes

Estados Unidos: USA Government Information Security Reform Act of 2000, section 3534(a)(1)(A);

Alemania: Deutsche Bundesdatenschutzgesetz (BDSG);

España: la Agencia de Protección de Datos Personales (APD y su Ley LOPD);

Canadá: Canada Act Respecting the Protection of Personal Information in the Private Sector (1993).

OSSTM Open Source Security Test Metodology www.isecom.org

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Otra de las metodologías más conocidas es ***OWASP*** (**www.owasp.org**)

Objetivo: principalmente esta metodología está orientada al desarrollo seguro de aplicaciones Web.

Tools: Adicionalmente al manual, se han desarrollado varias herramientas prácticas para verificación de seguridad y para el entrenamiento:

Webgoat / Webscarab

Esta metodología define chequeos:

Autenticación – Diferentes tipos de autenticación y sus problemas más comunes.

Autorización – Conceptos de control de accesos.

Administración de Sesiones – Describe la manera adecuada de administrar sesiones.

Auditoría y Logging.

Validación de Datos – Describe estrategias para lidiar con entradas no esperadas por la aplicación.

Injecciones - SQL, XML, LDAP, code, user agent (includes XSS) y otras.

Privacidad – Aspectos de privacidad relacionados con la aplicación.

Criptografía – Cómo y dónde utilizarla, cuales son los errores más comunes.

Representación Canónica.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Tareas del Ethical Hacker

A continuación se detallan todas las tareas que se pueden realizar:

- **Búsqueda de Vulnerabilidades:** comprobaciones automáticas de un sistema.

- **Escaneo de la Seguridad:** búsquedas de vulnerabilidades (falsos positivos) y análisis profesional individualizado.

- **Penetration Test:** se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pre-condicionales.

- **Evaluación de Riesgo:** se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

- **Auditoría de Seguridad:** hace referencia a la inspección manual con privilegios administrativos del sistema

- **Hacking Ético:** se refiere generalmente a los test de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto

- **Test de Seguridad y su equivalente militar, Evaluación de Postura,** es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Consejos para pensar y deducir

- **Cuando testear es tan importante como qué testear y porqué testear.**
- **Esperar para hacer el test, esperar para reportar los problemas y esperar para solucionarlos, es un error.**
- **Haga las cosas pequeñas, porque en definitiva, todas son cosas pequeñas.**
- **Testear se refiere a los detalles, y muy a menudo los pequeños detalles llevan a las más importantes fallas de seguridad.**
- **Las soluciones deben ser prácticas y realistas.**
- **El nivel de riesgo que se determine debe poder ser medido y cuantificado según la realidad del Cliente.**
- **Deberán conocer las herramientas que utilizarán durante el test como así también su procedencia, también se requiere que sean probadas en ambientes controlados antes de su utilización.**
- **Si durante el test se descubre una vulnerabilidad de alto riesgo ésta deberá ser comunicada de inmediato al cliente junto con la posible recomendación/solución a la misma**

Y por último algo muy importante: no solucionamos el problema nosotros de raíz, lo que hacemos es darle nuestro análisis o punto de vista para que el cliente lo solucione, en caso de que el cliente nos solicite que lo solucionemos, no es parte de un pentest, sino de una consultoría.

Por ejemplo, si encuentran puertos abiertos, el pentester no debería configurar un Firewall y cerrar los puertos, tiene que informarle al cliente la recomendación del porque no dejarlos abiertos, y en caso de que el cliente no sepa como cerrarlos y solicite que lo haga el pentester, eso es parte de una consultoría o servicio aparte.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Parte de ser un pentester es conocer las motivaciones de un atacante, sería un buen punto a tener en cuenta cuando se estudia "el ¿por qué?"

Estos son algunos de los motivos por lo que los "atacantes" realizan:

- **Curiosidad y desafío**
- **Entretenimiento**
- **Creencias políticas**
- **Deseo de información**
- **Emoción de obtener privilegios de acceso**
- **Instalar troyanos y puertas traseras**
- **Intento de comprometer otros sistemas**
- **Usarlo como trofeo para obtener "status" en el ambiente**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Los atacantes tienen tiempo ilimitado

- Se deben proteger todos los sistemas del ataque
- Los atacantes sólo deben encontrar un agujero, mientras nosotros debemos cubrir todos.

Otra de las tareas es conocer los tipos de perfiles del Atacante

- **Old School:** Lentos, cuidadosos, precisos, invasivos
- **Profesionales:** Rápidos, cuidadosos, precisos, algunas veces invasivos
- **Scripts Kiddies:** Lentos, imprecisos, invasivos
- **Defacers:** Rápidos, precisos, medianamente invasivos
- **Wannabe:** Principiantes en el tema, o llegan a su objetivo o quedan en la categoría de Scripts Kiddies

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Este es un sitio web histórico, en donde se exponía, de acuerdo al ataque realizado la posibilidad de ganar puntos y estar en una tabla de posiciones.

¿Por qué los hackers necesitan investigar las vulnerabilidades?

- **Para identificar y corregir las vulnerabilidades de la red**
- **Para proteger la red de ser atacado por intrusos**
- **Para obtener información que ayuda a prevenir problemas de seguridad**
- **Para obtener información acerca de los virus**
- **Para encontrar puntos débiles en la red y alertar al administrador de red antes de un ataque a la red**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

❖ Para saber cómo recuperarse de un ataque de red

Estos sitios que se expondrán a continuación, son los recomendados para tener en cuenta en la búsqueda de vulnerabilidades.

http://www.kb.cert.org/vuls
nvd.nist.gov
www.securitytracker.com
www.microsoft.com/security
www.securiteam.com
www.packetstormsecurity.com
www.hackerstorm.com
www.hackerwatch.org
www.securityfocus.com
www.securitymagazine.com
www.scmagazine.com

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

¿Y los atacantes que necesitan?

Constantemente están a la búsqueda de errores, problemas o vulnerabilidades no declaradas (0DAY), lo cual son el punto de partida para empezar la intrusión o ataque.

Aprovecharse de errores en las aplicaciones

- **Validación de entrada de datos**
- **Administración de Sesiones**
- **Administración de Cookies**
- **Variables de usuario**
- **Funcionalidad**

Aprovecharse de errores humanos

- **Ataques de diccionario**
- **Dumpster diving**
- **Ingeniería Social**

Aprovecharse de vulnerabilidades en los sistemas

- **SQL Injection**
- **Unicode**
- **HTR Chunked Encoding**
- **Apache Chunked Encoding**
- **Buffer overflows, overrun**
- **Cross Site Scripting**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Conozcamos los distintos tipos de entornos de ataques:

Pasivo

- No altera la funcionalidad, sólo escucha y transmite, o simplemente escucha. Análisis de tráfico, monitoreo de comunicaciones, captura de credenciales de acceso. Divulga información sin intentar romperlas por ejemplo obtiene medidas de protección, usuarios y contraseñas.

Activo

- Modificación del flujo de datos transmitido o generando uno falso, intenta romper las medidas de protección. Pueden ser: Interrupción, Intercepción, Modificación, Fabricación, Destrucción.

Ataque de cercanía

- Son los ataques relacionados con la aproximación de personas a redes, sistemas o dispositivos con el propósito de modificar, obtener o denegar acceso a la información. Ejemplo Wardriving, Warnibling, intercepción de emanaciones electromagnéticas.

Insider Factor

- Son personas que ya tienen acceso a la información y pertenecen a la compañía, generalmente provocan disclosure, robo o daño de la información.

- Usa esa información de una forma fraudulenta o suele bypasear controles para ingresar a sectores restringidos de los sistemas o para obtener beneficios laborales

Ataques de distribución

- Distribution attacks se enfocan en la modificación del software o hardware de un producto o durante el proceso de fabricación o durante la distribución se introduce código malicioso como backdoors, loggers para obtener información o acceder a sistemas cuando los dispositivos o los software sean instalados.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Por último “Grandes preguntas - Buenas Respuestas”

Muchos ante estos casos, se preguntan:

Que es el Hacking?

Es el uso de herramientas para explotar las vulnerabilidades de una red o sistema, y una vez dentro del mismo poder llevar a cabo la actividad dentro del sistema.

Que es un Penetration Test?

Es la evaluación de las normas de seguridad de una organización, utilizando herramientas de hacking para poder, recolecta, evaluar e informar, cual es el estado del objeto informático evaluado.

Y por último, que es el Ethical Hacking?

Esta definición engloba a las dos anteriores, pero excluyendo de la primera que solo se utiliza para fines benéficos, o mejor dichos éticos, cumpliendo todas las normas legales de no divulgación, modificación o destrucción de información.

Porque hablamos de estos puntos?

Por motivos variados que hacen a la flexibilidad en la comunicación o instrucción de la materia Seguridad Informática, no son pocas las veces en las que estos términos pueden confundirse y darse por sinónimos, cuando en realidad existe una diferencia entre ellos, además de una leve asociación jerárquica definida en términos de cual incluye o antecede al otro.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejercicio Número 2 Unidad 1

VERACRYPT: https://veracrypt.codeplex.com/

VeraCrypt es una aplicación para cifrar y ocultar datos en el ordenador que el usuario considere reservados, empleando para ello diferentes algoritmos de cifrado como ***AES*** ***Serpent*** y ***Twofish*** o una combinación de los mismos.

También permite crear volúmenes virtuales cifrados en un archivo de forma rápida y transparente, se usa en reemplazo de TrueCrypt

GPG4WIN: **www.**gpg4win**.org**

Gpg4win (GNU Privacy Guard for Windows) es un software para cifrar ficheros y correos electrónicos

Mediante una máquina virtual, hacer uso de estas 2 herramientas, cifrando un directorio personal y realizando un cifrado de un archivo (ambos resultados, subirlos al foro exponiendo la captura imagen)

ATENCIÓN: **el uso de estas herramientas requiere mucho cuidado al trabajar fuera de una máquina virtual, por ende se recomienda tomar los recaudos necesarios.**

Aquel que requiera manuales de estas herramientas, puede solicitarlo por mensajería.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy IMPORTANTE que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.

Bibliografía utilizada y sugerida

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU.

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México.

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España.

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU.

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learni the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU.

Link complementarios:

https://www.isecom.org/

https://www.owasp.org

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado)