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

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 3:

Hardening (Windows Servers o Linux Servers)

Unidad 1:

Introducción a implementaciones de seguridad

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, se conocerán formas de proteger la información, priorizando los activos más importantes.

Aprender cómo empezar a seleccionar el proceso adecuado, pensando en distintas topologías y como un atacante podría aprovechar.

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…

- Conocer sobre el mundo de los servidores informáticos, existentes en toda infraestructura informática de mediana y alta gama.

- Conocer las herramientas esenciales y las buenas prácticas necesarias para obtener el máximo nivel de seguridad en una red de servidores de arquitectura Microsoft Windows Server o Linux Server, protegiéndola de potenciales amenazas.

- Comprender los conceptos básicos referentes a la implementación, configuración, mantenimiento y soporte de servidores de infraestructura en tecnologías Windows o Linux.

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

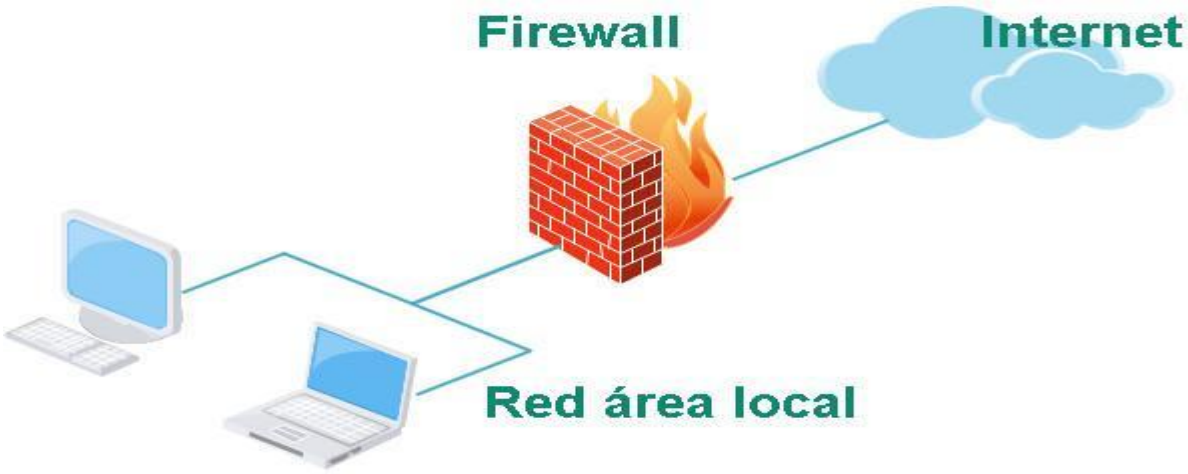
1. ¿En qué consiste?
2. ¿Por dónde empezar?
3. Tipos de ataques
4. Ejemplos

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

¿En qué consiste?

Consiste en establecer métodos y mecanismos diseñados para que el sistema de información sea el más apropiado y seguro, y que podamos aplicar reglas definidas a través de las políticas de seguridad.

Por intermedio del curso, se ha aprendido que existen dispositivos que se utilizan para asegurar una red, por ejemplo los **FIREWALL.**



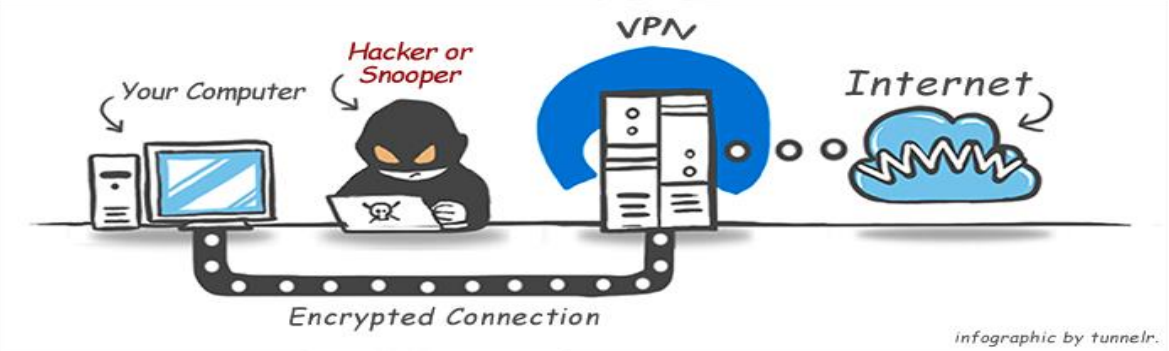
Utilizado para poder interactuar entre la red local (LAN) e Internet (más allá de que también se utiliza internamente entre distintos segmentos de red y DMZ).

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

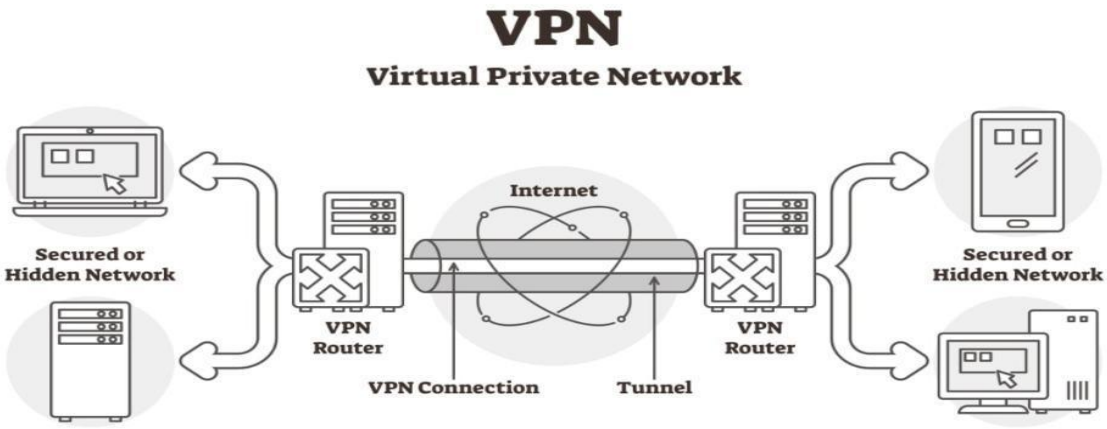
Pero hablamos de **asegurar**, no de **proteger** la confidencialidad de los datos que circulan a través de nuestro tráfico de red.

En este caso, también tendríamos que saber, que una de las maneras de proteger la confidencialidad de la información, es a través de algoritmos criptográficos.

Una de las maneras de que veamos y aseguremos que circule tráfico encriptado, es bajo la utilización de una red virtual privada, conocida con el nombre de "**VPN**" (**virtual private network).**



La misma es encontrada a través del uso de software o vía hardware, a través de routers, firewalls, etc.



Puede ser punto a punto desde un router a otro, o desde un firewall a otro, o desde un dispositivo VPN.

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

¿Se implementan políticas o procesos de seguridad informática?

¿Qué podemos encontrar en **Internet** que responda esa pregunta?:

"Las políticas de seguridad son documentos que constituyen la base del entorno de seguridad de una empresa y deben definir las responsabilidades, los requisitos de seguridad, las funciones, y las normas a seguir por los empleados de la empresa"

Cuál es la realidad:

"Más del 60% de las grandes empresas, no cuentan con un plan de contingencia ni normas, por ejemplo ante un ataque de **DOS** (**Denegación de servicio**)"

Más allá de esta realidad, existen ciertas normas que uno podría implementar, donde las mismas fueron creadas para mitigar, gestionar y hasta facilitar todo lo relacionado a los incidentes informáticos o Hardening de seguridad.

Las normas ISO

Las normas **ISO** son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (**ISO**) y la Comisión Electrotécnica Internacional (**IEC**) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

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

En concreto la familia de normas **ISO/IEC 27000** son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporciona un marco para la gestión de la seguridad.

Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (**SGSI**) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información, según la **ISO 27001**, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento.

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

Tenemos también la **ISO 17799** es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

El objetivo de la norma **ISO 17799** es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre las empresas.

¿Los atacantes o intrusos tienen en cuenta esto? Realmente no, la mayoría se aprovecha de las vulnerabilidades que se puedan encontrar, por lo tanto, en caso de no encontrar una, tienen dos posibilidades, la crean (Zero Day) o se dan por vencidos.

Algunas ISOS a tener en cuenta relacionadas con la gestión:

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

Norma	Descripción
ISO/IEC 27000	Vocabulario estándar para el SGSI para todas las normas de la familia.. Se encuentra en desarrollo actualmente.
ISO/IEC 27001	Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
ISO/IEC 27002	*Information technology - Security techniques - Code of practice for information security management.* Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un **código de buenas prácticas** para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
ISO/IEC 27003	Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
ISO/IEC 27004	Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
ISO/IEC 27005	Normativa dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standar BS 7799 parte 3. Publicada en junio de 2008.
ISO/IEC 27006	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
ISO/IEC 27007	Guía para auditar al SGSI. Se encuentra en preparación.
ISO/IEC 27799:2008	Guía para implementar ISO/IEC 27002 en la industria de la salud.

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 dónde empezar?

1- Que haya responsables en el área de desarrollo, implementación y gestión de la política a imponer

En este punto, tener un referente, un responsable, llámese “Director de Seguridad”, que note que se estén cumpliendo funciones de controlar accesos, asignar roles, proveer permisos, identificar el problema, etc.

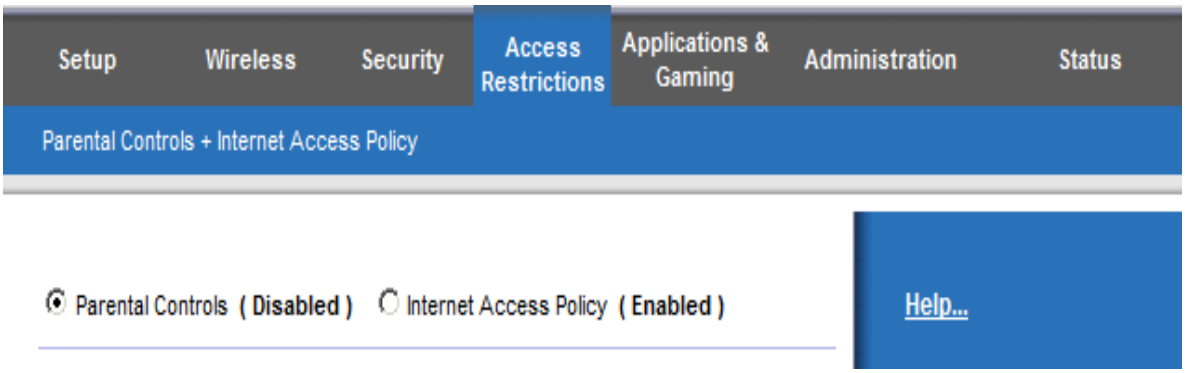
Hablar con los empleados, **CONCIENTIZARLOS**!!!!

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

2- Proteger equipos y dispositivos en uso

Usar las políticas más conocidas, por ejemplo, instalar antivirus, tener las últimas actualizaciones referentes a sistemas operativos y aplicaciones.

Controlar el acceso al exterior, llámese **INTERNET**.



Tener en cuenta, si es realmente necesario que los dispositivos cuentan con hardware que se pueda utilizar de forma potencialmente maliciosa para nuestra red, llámese puertos **USB.**

IMPORTANTE: una de las buenas prácticas es impedir o restringir el uso de los USB, aplicar una política de uso y hasta que los mismos sean utilizados a través de procesos de detección de malware.

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

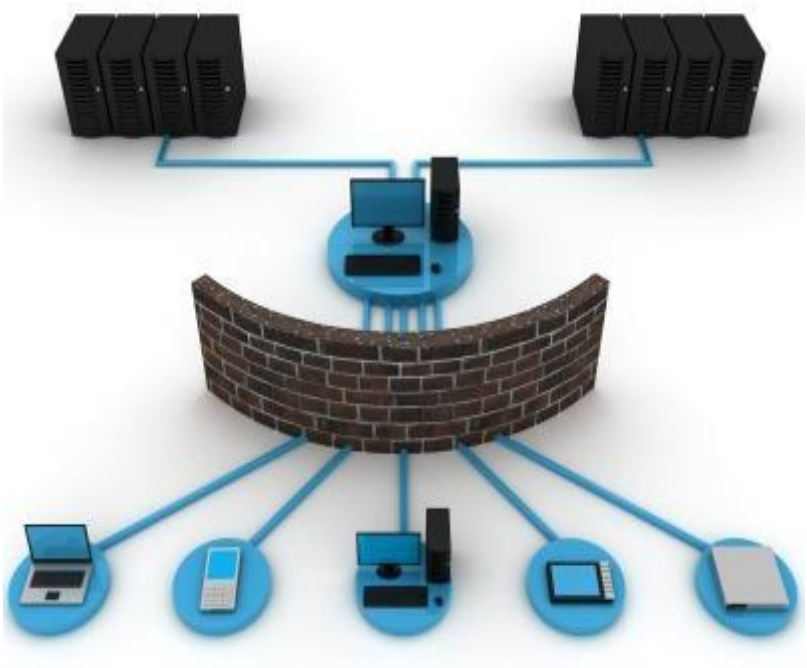
El uso de software ilegal o de procedencia dudosa, sería también una de las maneras de no poder evitar la intrusión, por ejemplo a través **de troyanos o keyloggers**.

En caso de que un dispositivo, se utilice para repositorio de archivos, que el mismo tenga un control (**LOG**) de quienes ingresan, y no dejarlo libre para todo el mundo.

Y cuando hablamos de navegación, utilizar medidas de control de páginas, por ejemplo (**NOSCRIPT**), plugin de **FIREFOX**, bloquea la ejecución de **Javascript**.

3- Proteger la red

Ya lo habíamos hablado en otras unidades, el uso de dispositivos, protocolos, técnicas, para la protección de la red.



En caso de tener acceso a los dispositivos de seguridad, evitar el uso de contraseñas en texto plano (uso de telnet), el cual sería muy sencillo a través de un **SNIFFER (analizador de tráfico)** la captura de la misma, sin necesidad de utilizar otras técnicas.

Para evitar esto, utilizar acceso a través de **SSH** (**secure shell**) u otro protocolo que use cifrado de datos.

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

4- Proteger los servidores

Uso de certificados digitales, a través del uso de protocolo **SSL**, cifrando la navegación, para establecer una comunicación segura y confiable.

Chequear los accesos al mismo, evitar políticas que nos digan que sea “tierra de todos” o “todos somos admin”.

Contar con un plan de recuperación ante desastres y no pensar en “tengo un backup, está solucionado seguramente”.

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

5- Proteger los datos

Copias de seguridad, tanto en forma local como remota.

Reflexionar con este ejemplo:

Tenemos un incidente, se incendia el edificio donde tenemos la base de datos, y el backup está en el mismo lugar donde se produjo el incendio, ¿qué posibilidades tenemos de recuperación de los datos?

Uso de cifrado de datos.

Limitación al uso de permisos de acceso a los mismos, aquí se recomienda el uso de perfiles adecuados, un usuario tiene que tener permisos asignados a sus funciones.

En caso de tener programadores propios, implementar políticas de testeo en las aplicaciones, para evitar posibles agujeros de seguridad.

Tener todo lo relacionado a la electricidad en perfecta “sintonía”, uso de UPS con control de voltaje.

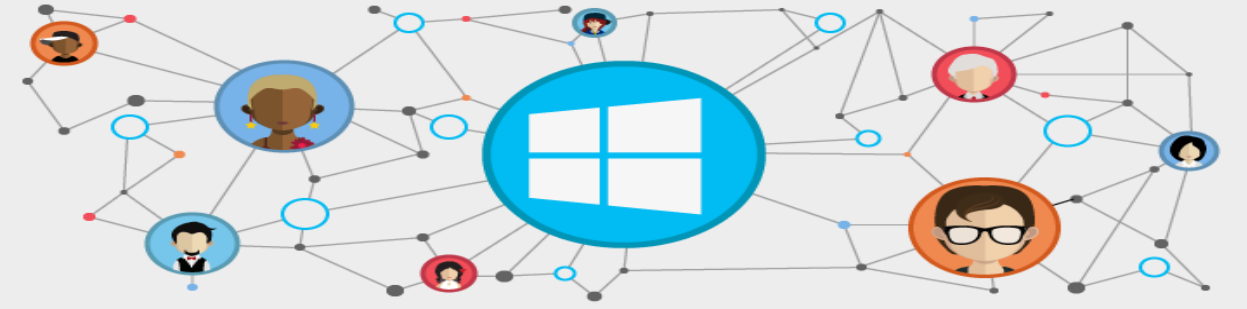
Utilizar normas de seguridad e higiene.

6- Protección de las aplicaciones y recursos

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

Implementar políticas de control de aplicaciones (no uso y no ejecución de software no autorizado).

Limitación al uso de recursos compartidos, implementando perfiles en los usuarios que sí puedan.



En caso de uso de software propietario, contar con las últimas actualizaciones o parches de seguridad.

En caso de contar con software libre, chequear el código fuente, testear y verificar su origen.

Un recurso compartido libremente (**SHARE ALL**) no es muy seguro, sobre todo, si el sistema operativo tiene agujeros de seguridad por intermedio del servicio compartir.

Contar con personal especializado, para el control de las aplicaciones, y no pensar en "mi programador nunca se equivoca".

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

Tipos de Ataques

Hay varias formas en que un atacante puede obtener acceso a un sistema.

El atacante debe ser capaz de explotar una debilidad o vulnerabilidad del mismo.

Expondremos los más utilizados, debido a que son cientos de técnicas que existen.

•ATAQUES AL SISTEMA OPERATIVO

• ATAQUES A NIVEL DE APLICACIÓN

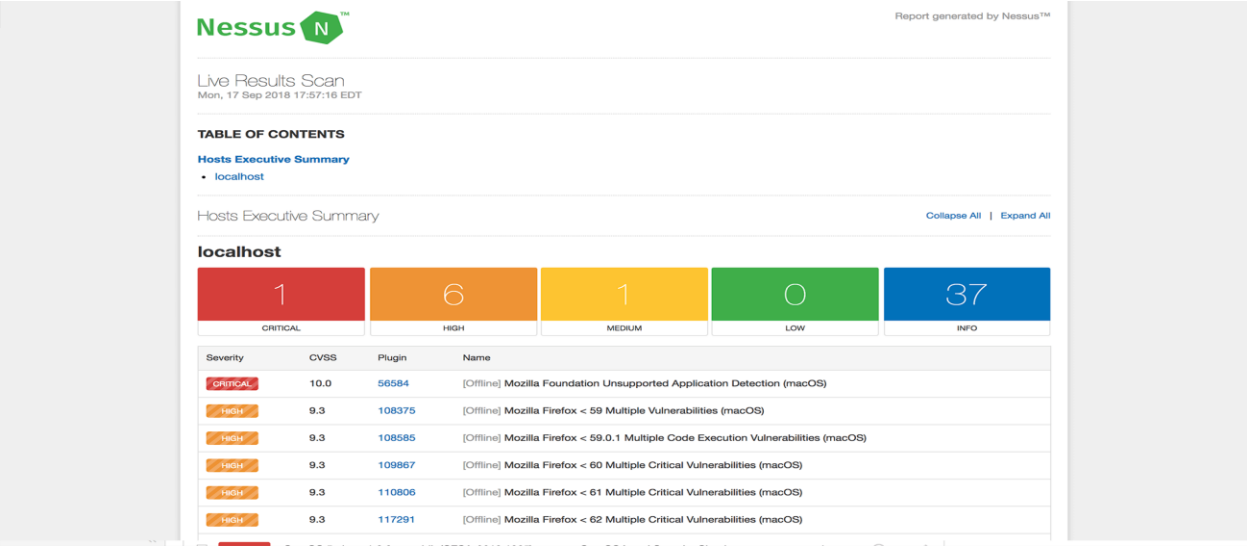
• ATAQUES APROVECHANDO MALAS CONFIGURACIONES

• ATAQUES A TRAVES DEL CODIGO DE LAS APLICACIONES

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

1-Los atacantes están a la búsqueda de vulnerabilidades del sistema operativo y de explotación de los mismos para obtener acceso a un sistema de red.

Utilizan muchos servicios de scanners de vulnerabilidades, por ejemplo Nessus, Acunetix, WPScan, Owasp ZAP, Openvas, Nexpose.



Solicitar al instructor un listado de los scanners de vulnerabilidades.

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

En este punto no interesa que sistema operativo es el mejor, si no que tan cuidadosos fuimos para que no se aprovechen de una vulnerabilidad que se pasó por alto.

Top 20 Products With the Most Technical Vulnerabilities Over Time

1999–2019	
Debian Linux	3,067
Android	2,563
Linux kernel	2,357
Mac OS X	2,212
Ubuntu	2,007
Mozilla Firefox	1,873
Google Chrome	1,858
iPhone iOS	1,655
Windows Server 2008	1,421
Windows 7	1,283
Adobe Acrobat Reader DC	1,182
Adobe Acrobat DC	1,182
Windows 10	1,111
Adobe Flash Player	1,078
Windows Server 2012	1,050

2019	
Android	414
Debian Linux	360
Windows Server 2016	357
Windows 10	357
Windows Server 2019	351
Adobe Acrobat Reader DC	342
Adobe Acrobat DC	342
cPanel	321
Windows 7	250
Windows Server 2008	248
Windows Server 2012	246
Windows 8.1	242
Windows RT 8.1	235
Ubuntu	190
Fedora	184

SOURCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S NATIONAL VULNERABILITY DATABASE

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

2-Las aplicaciones de software vienen con multitud de funcionalidades y características. Hay una escasez de tiempo para efectuar una prueba completa antes de lanzar productos. Esas aplicaciones tienen diferentes vulnerabilidades y se convierten en una fuente de ataque.

Appendix 1 – Vulnerable applications in Google Play

Package Name	Name	Version	Download Count
com.viber.voip	*Viber	*14.1.0.16	500,000,000
com.booking	*Booking.com	*24.8.2	100,000,000
com.aloha.browser	Aloha	2.23.0	1,000,000
com.walla.wallasports	Walla! Sports	1.8.3.1	100,000
videoeditor.videorecorder.screenrecorder	XRecorder	1.4.0.3	100,000,000
com.tranzmate	Moovit	5.56.0.459	50,000,000
com.walla.wallahamal	Hamal	2.2.2.1	1,000,000
com.indiamart.m	IndiaMART	12.7.4	10,000,000
com.microsoft.emmx	Edge	45.09.4.5083	10,000,000
com.grindrapp.android	Grindr	6.32.0	10,000,000
ru.yandex.taximeter	Yango Pro (Taximeter)	9.56	5,000,000
com.cyberlink.powerdirector	PowerDirector	7.5.0	50,000,000
com.okcupid.okcupid	OkCupid	47.0.0	10,000,000
com.cisco.wx2.android	Teams	40.10.1.274	1,000,000
com.bumble.app	Bumble	5.195.1	10,000,000

Listado de aplicaciones de Android que salieron al mercado y que tienen vulnerabilidades, nótese la cantidad de descargas que tuvo cada una.

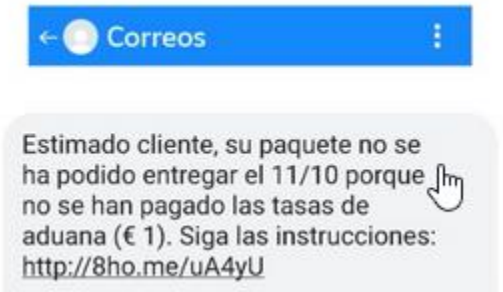
Esto siempre fue así, uno confía en un proveedor, fabricante, vendor, pero al no estar a cargo del testeo de la aplicación, uno queda expuesto, por ende se recomienda cuando se instala un proceso nuevo en nuestra red, al menos, verificar con un Hardening, si es vulnerable o no.

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

3-La mayoría de los administradores no tienen las habilidades necesarias para mantener o corregir los problemas, que pueden conducir a errores de configuración. Tales errores de configuración pueden llegar a ser las fuentes para un atacante para entrar en la red o el sistema del objetivo

La solución no es tener gente con cientos de certificaciones de seguridad (de hecho no hay muchas), sino disponer de personal que pueda obtener los conocimientos necesarios para poder solucionar el incidente.

4- Hay aplicaciones del sistema operativo que vienen con numerosos scripts de ejemplo para hacer el trabajo del administrador fácil, pero los mismos scripts pueden tener varias vulnerabilidades, que pueden conducir a disminuir los ataques de códigos.



Mensajes automáticos que uno piensa que los manda la aplicación, pero que realmente es un proceso de una de las técnicas más conocidas: Phishing.

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

Ejemplos beneficiados por los tipos de ataques

MALAS CONFIGURACIONES

Las vulnerabilidades afectan una mala configuración de servidores web, plataformas de aplicaciones, bases de datos, redes, hasta en Routers pueden resultar en el acceso ilegal o posible intrusión propietaria al sistema (en este ejemplo, password texto plano).

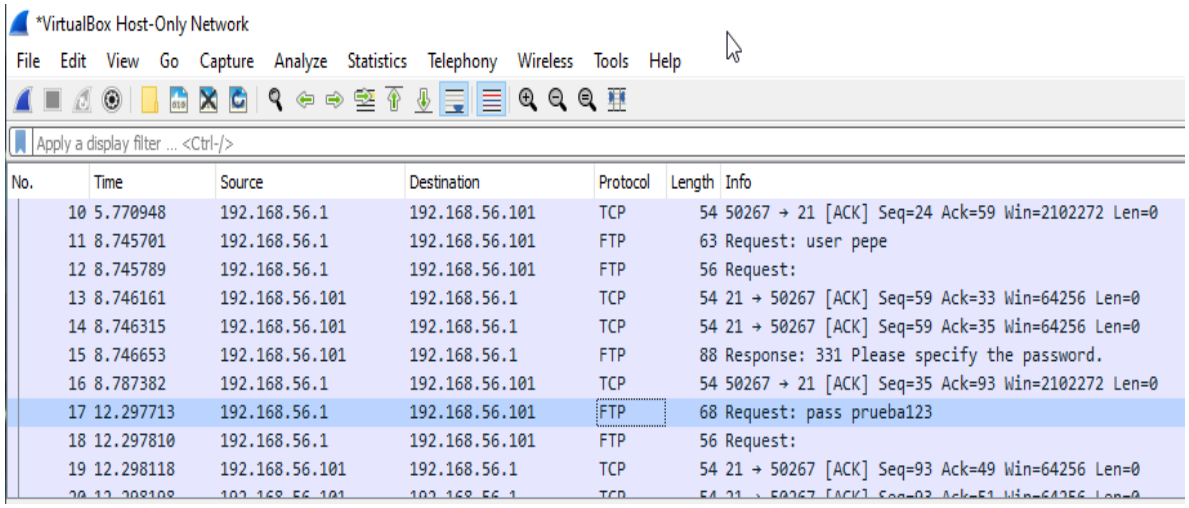
```
ISP(config)# show running-config
<output omitted>

username BORDER password 0 Cisco
!
interface Serial0/0/0
 ip address 209.165.200.225 255.255.255.252
 encapsulation ppp
 ppp authentication chap
```

```
BORDER(config)# show running-config
<output omitted>

username ISP password 0 cisco
!
interface Serial0/0/0
 ip address 209.165.200.226 255.255.255.252
 encapsulation ppp
 ppp authentication chap
```

En este ejemplo, podemos notar que la contraseña se encuentra en texto plano.



En este ejemplo, se ve por intermedio de un analizador de tráfico, una conexión realizada a un FTP, junto a sus credenciales en texto plano.

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

PROGRAMACIÓN O CÓDIGO INCORRECTO

Al instalar un sistema operativo / aplicación, el mismo viene con muchos scripts/librerías para hacer la vida del administrador más sencilla.

```
<form action="login_form.php">
  <input id="username" name="username"/>
  <input id="password" name="password"/>
  <input id="rememberMe" name="rememberMe"/>
  <input id="login" name="login"/>
  <input type="submit"/>
</form>
```

Este ejemplo, demuestra una forma sencilla de crear un formulario de ingreso.

Ejercicio Número 1 Unidad 1

En caso de tener conocimientos de programación WEB, te animas a exponer qué errores se pueden encontrar en esa configuración.

De no disponer de conocimientos de programación WEB, recomendamos estudiar:

- **Python**
- **HTML / CSS / JavaScript**
- **.NET**
- **Ruby**
- **Perl**

Ejercicio Número 2 Unidad 1

EJERCICIO: ¿ES SUFICIENTE?

Crear un documento (DOC/PDF), en el cual este explicado con sus propias palabras, de acuerdo a lo leído en esta unidad, si las medidas son ¿suficientes o no?

Desarrollar: si son suficientes las políticas, justificar el porqué de cada una (no más de 1 página).

Si son insuficientes: explicar que agregaría y justificar el porqué de cada una (no más de 2 páginas).

También se pueden aportar nuevas ideas de medidas.

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 tener en cuenta:

A esta altura, seguramente muchos pensarán que dentro de la Seguridad Informática, tanto en la rama de Hacking como en la de Seguridad de la Información, son muchos y variados los temas a aprender, conocer y entender.

En los primeros módulos, se realiza una introducción, para luego al acceder a este tercer módulo, comprender que existen cientos de técnicas diferentes, tanto a nivel defensa como ataque.

Las medidas de seguridad que puedan aportar como nuevas ideas, pueden ser muchas también, siendo realistas, sabemos que existen infinidad de escenarios y todo dependerá del relevamiento o conocimiento que tenga el especialista de seguridad para poder llevar a cabo esa tarea.

Por ende, toda medida que aporten, siempre SUMA!!!!!.

Les comparto este checklist

1- No se trata del mejor Antivirus, mejor es disponer de uno

2- Elemental utilizar un Firewall

3- Actualizar aplicaciones con parches de seguridad

4- Utilizar software legal

5- Analizar y tener precaución en todos los correos electrónicos

6- Ser cuidadoso con los archivos que se bajan de Internet

7- Uso y configuración adecuada de los usuarios locales (admin)

8- Utilizar contraseñas seguras

9- Utilizar navegadores actualizados

10- Realizar siempre copias de seguridad

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.

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

Bibliografía utilizada y sugerida

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

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

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

Links complementarios

NOSCRIPT: http://es.wikipedia.org/wiki/NoScript

WEB OFICIAL: http://noscript.net/

SSH: http://es.wikipedia.org/wiki/Secure_Shell

VERSION LIBRE: http://www.openssh.com/es/index.html

SSL: http://es.wikipedia.org/wiki/Transport_Layer_Security

USB WRITE PROTECTOR: https://www.gaijin.at/dlusbwp.php

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).