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 2:

Configuraciones y servicios (Parte 01)

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 segunda Unidad del módulo, se conocerán las configuraciones de seguridad principales,

También se aprenderá que tener en cuenta con respecto a un buen Hardening en los servidores.

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. Configuraciones de Seguridad (Práctica-Lab)
2. Servicios disponibles para instalar/aplicar
3. Checklist Hardening

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

Configuraciones de seguridad (Práctica-Lab)

En la unidad anterior, hemos visto parte de las políticas de seguridad que se pueden implementar dentro de un entorno al que "quisiéramos" considerarlo seguro.

Como hacer para que ese "quisiéramos" se transforme en una realidad, que podamos tener una seguridad ante nuestros servicios, sistemas, usuarios, etc.

Para ello, se llevarán a cabo, ejercicios prácticos para poder estar al tanto de todo lo que uno debe tener a mano y… ¿que no se dieron cuenta??

Muchas de las soluciones que un especialista de seguridad dispone, las tiene al alcance de la mano, el problema principal es que sepa cuales se deben aplicar, como implementarlas y el momento adecuado, por ejemplo, actualizar un SO en un servidor de producción, tiene que llevar una planificación adecuada, no se puede reiniciar porque sí.

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 2

Pregunta para pensar y responder en foro cual es la correcta

¿Qué es el Hardening?

• Configuración segura y robusta del sistema operativo

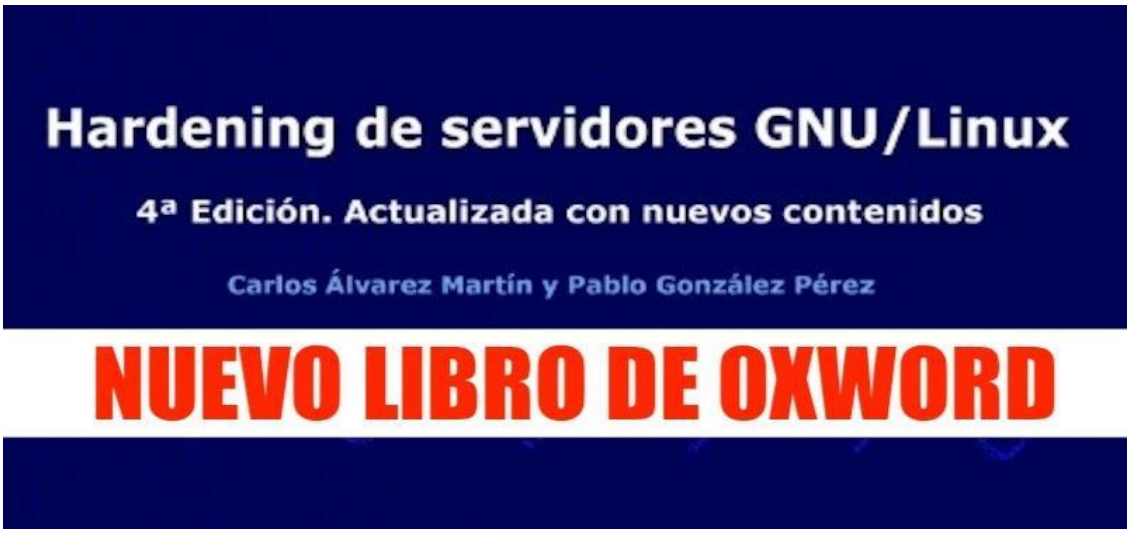
• Una manera de endurecer un dispositivo

• Hardware seguro solamente

• Es una técnica que usan los atacantes para ver nuestras debilidades

De acuerdo a su elección, justificar el porqué de la misma.

Recomendamos la siguiente bibliografía:



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 esta práctica, nos limitaremos a estos objetivos:

¿Qué queremos conseguir?

– Prevenir la pérdida de información y caídas del sistema

– Proteger el sistema contra ataques y accesos no autorizados

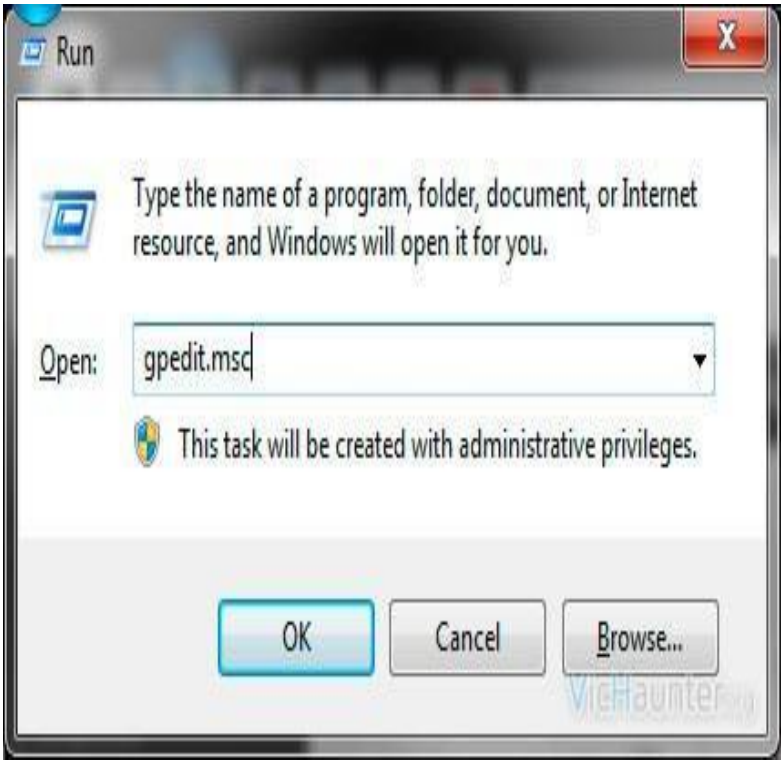
– Limitar el impacto de vulnerabilidades

– Prevenir el uso no autorizado del sistema a los usuarios

– Evitar vectores y técnicas de ataques conocidos

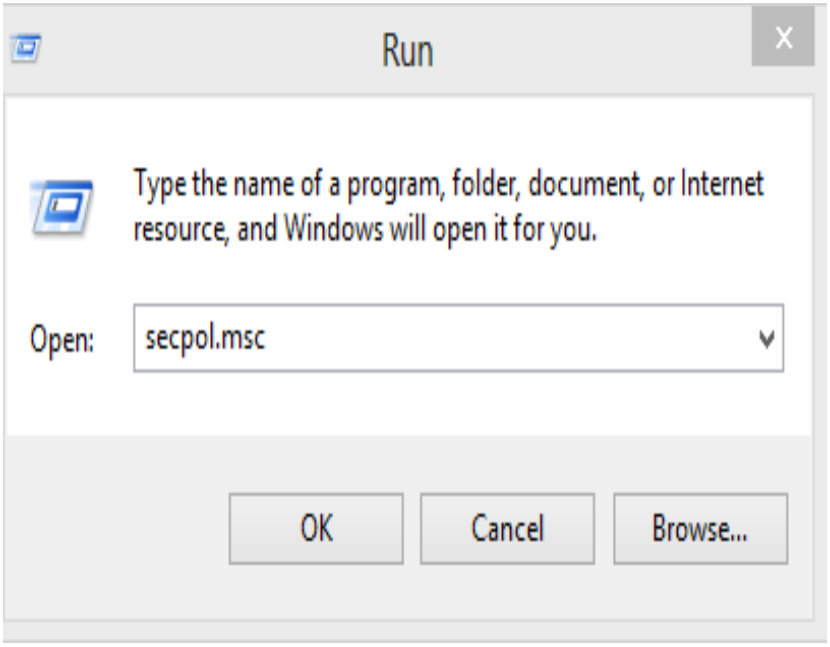
En una máquina virtual, que disponga de un SO basado en Windows 10, hacer uso de lo expuesto relacionado a seguridad y mejora del mismo.

A) Uso de **SECPOL.MSC** y de **GPEDIT.MSC** (desde boton inicio, ejecutar)



gpedit.msc: Permite modificar las políticas de grupo

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



secpol.msc: Configuración de la política de seguridad local

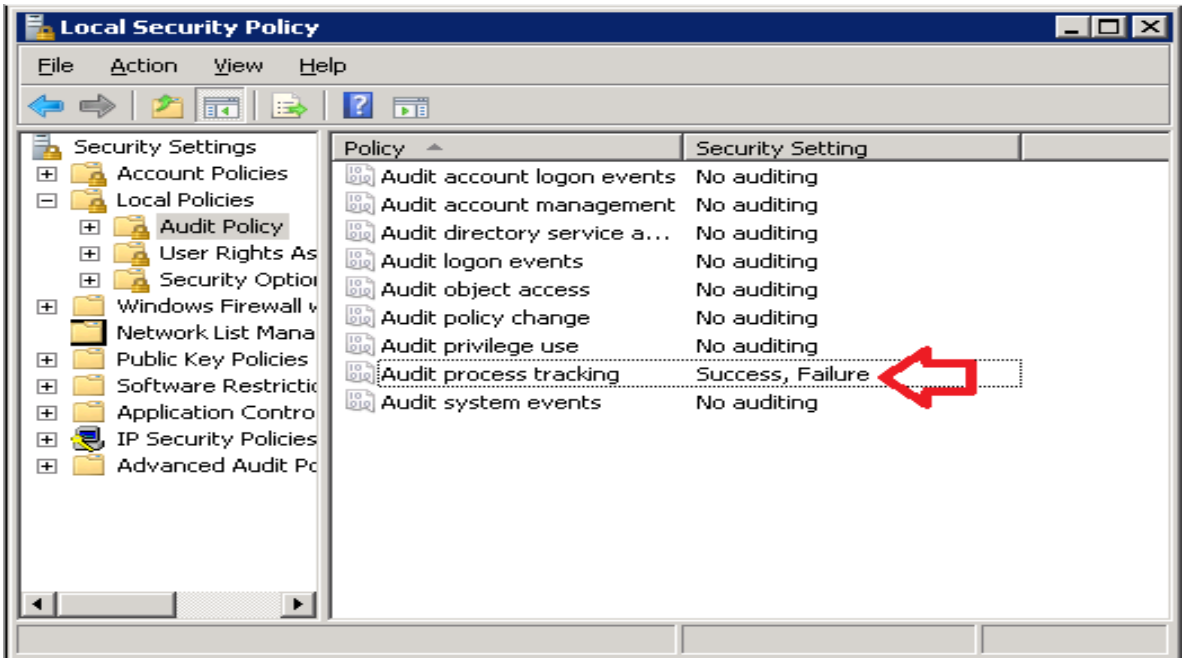
El uso de estos comandos, revelara todo lo relacionado a seguridad que disponemos para ser utilizado, ejemplo, auditar servicios, políticas de passwords, etc.

Ejercicio Número 2 Unidad 2

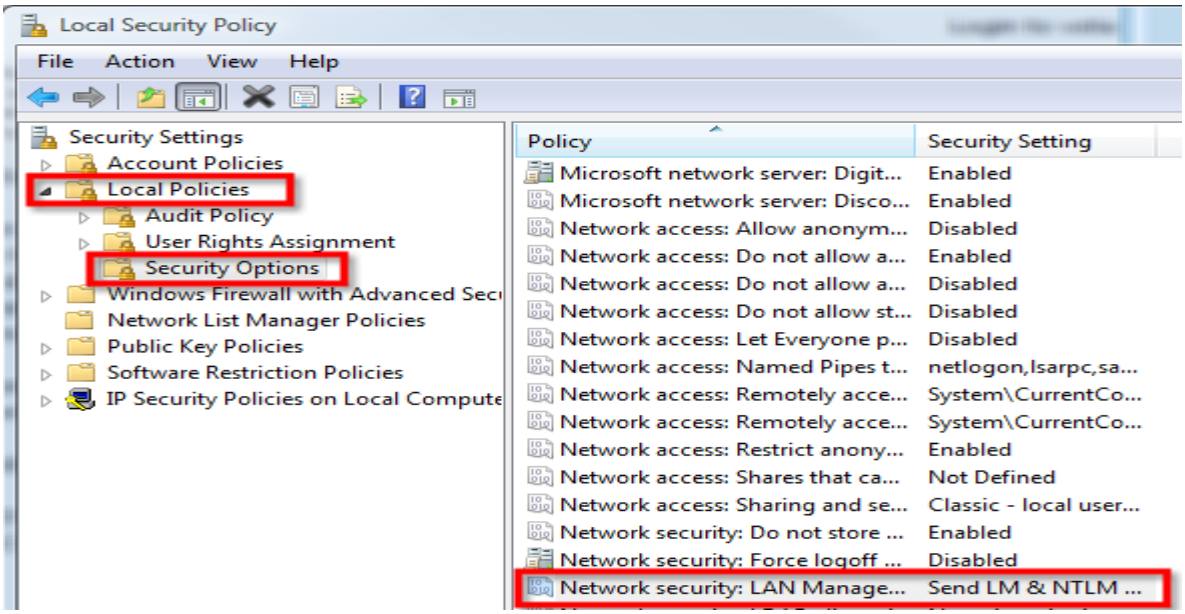
Probar las siguientes opciones e informar qué procesos se están llevando a cabo (siempre en el foro, para que todos vean).

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

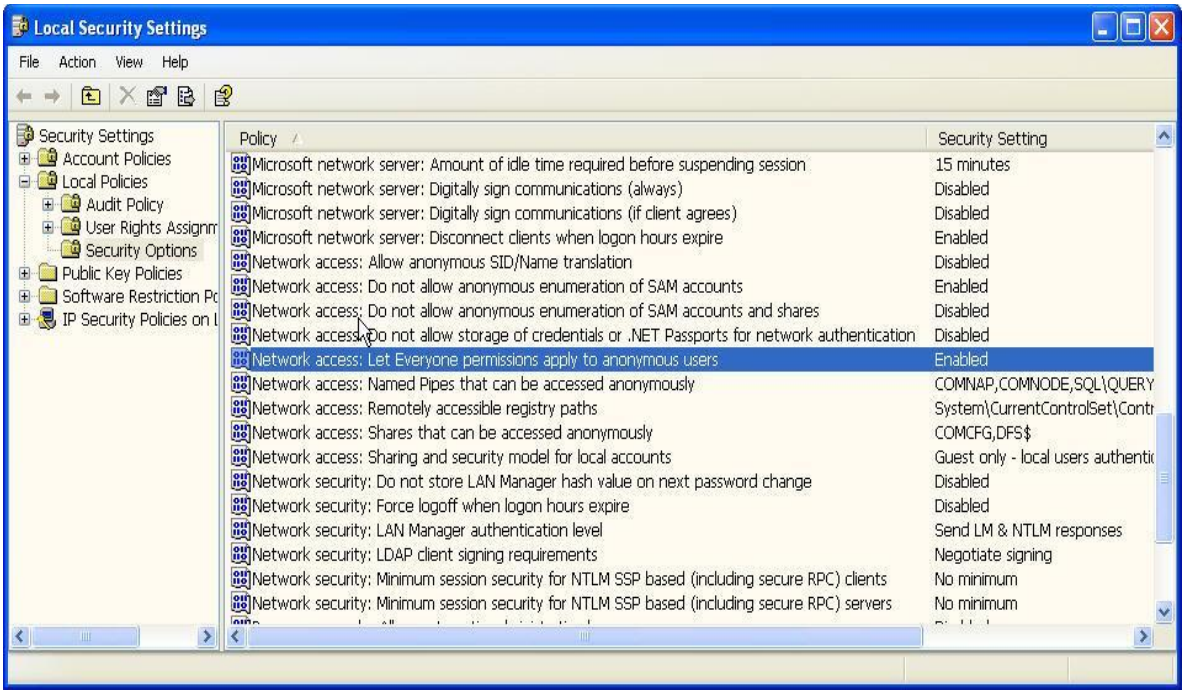
1-



2-



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- 

Lo que se pide en estas 3 capturas, es explicar con palabras lo que cada una de las opciones seleccionadas realiza.

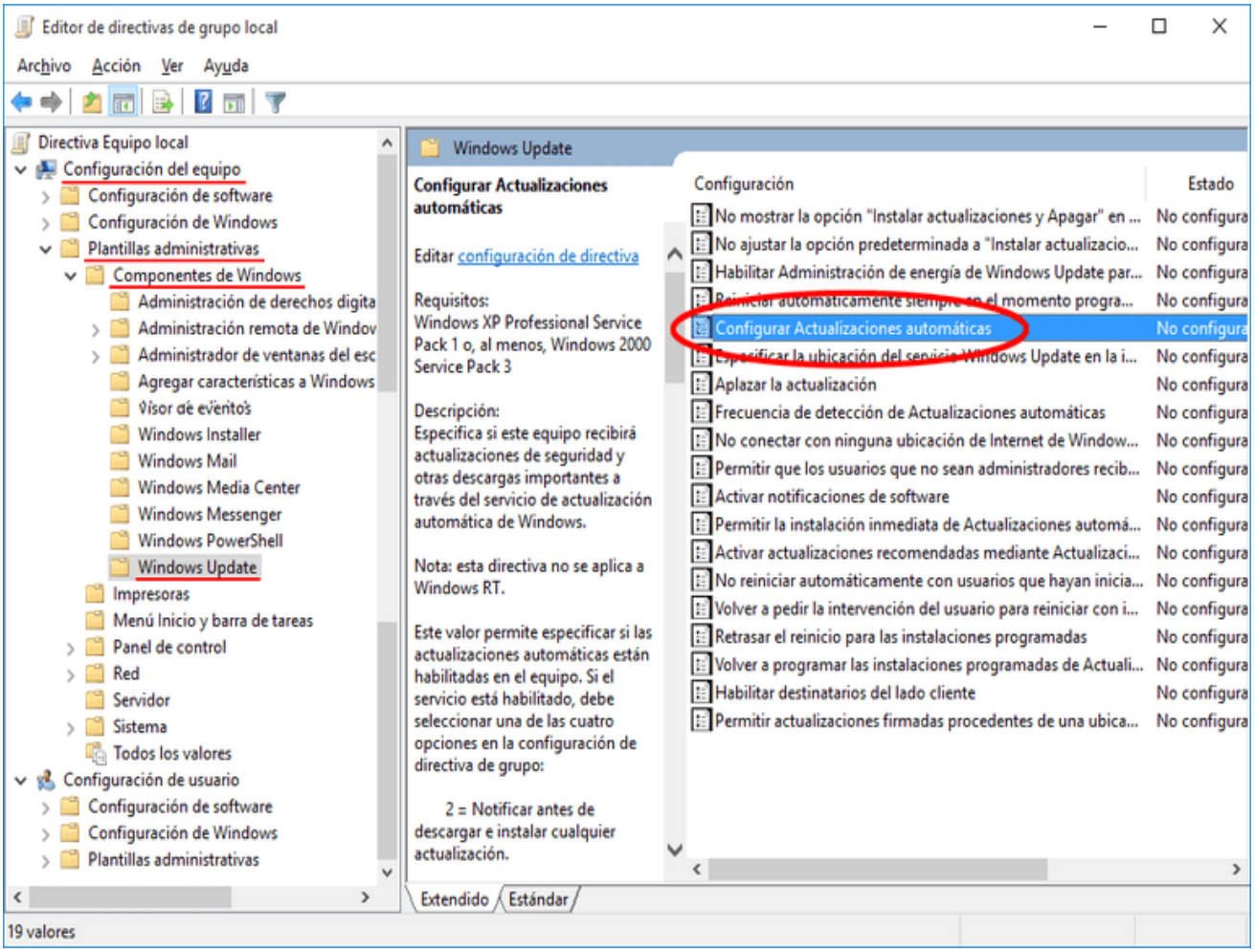
Se darán cuenta que las opciones son muy importantes, por eso, es bueno entender su función.

Recordar que hay muchos SO de Windows, puede ser que en otros que no sea el expuesto, se vea de forma diferente o con otros textos, las opciones solicitadas, en ese caso, recomendamos buscar la correcta.

Servicio WSUS (Windows Server Update Services)

Un problema que uno comúnmente puede encontrar, es ver configurado de forma incorrecta todo lo referente a las actualizaciones automáticas, el servicio WSUS es el que se encarga de ese proceso.

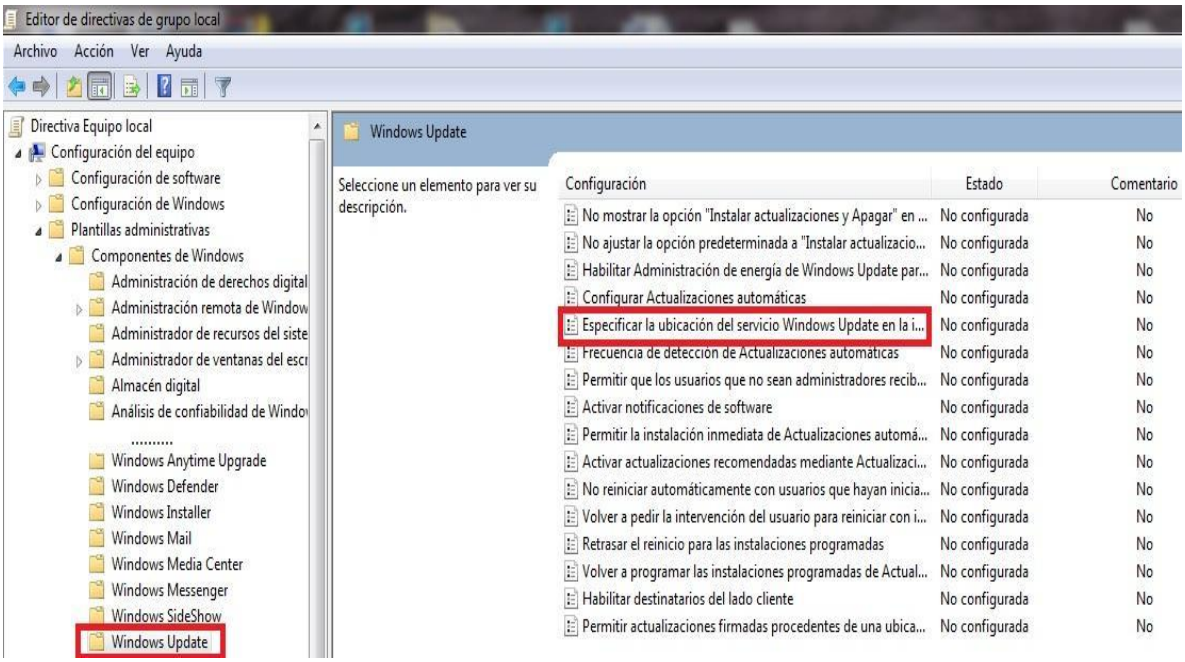
Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



Este ejemplo expuesto es una forma de configurar WSUS en nuestros dispositivos.

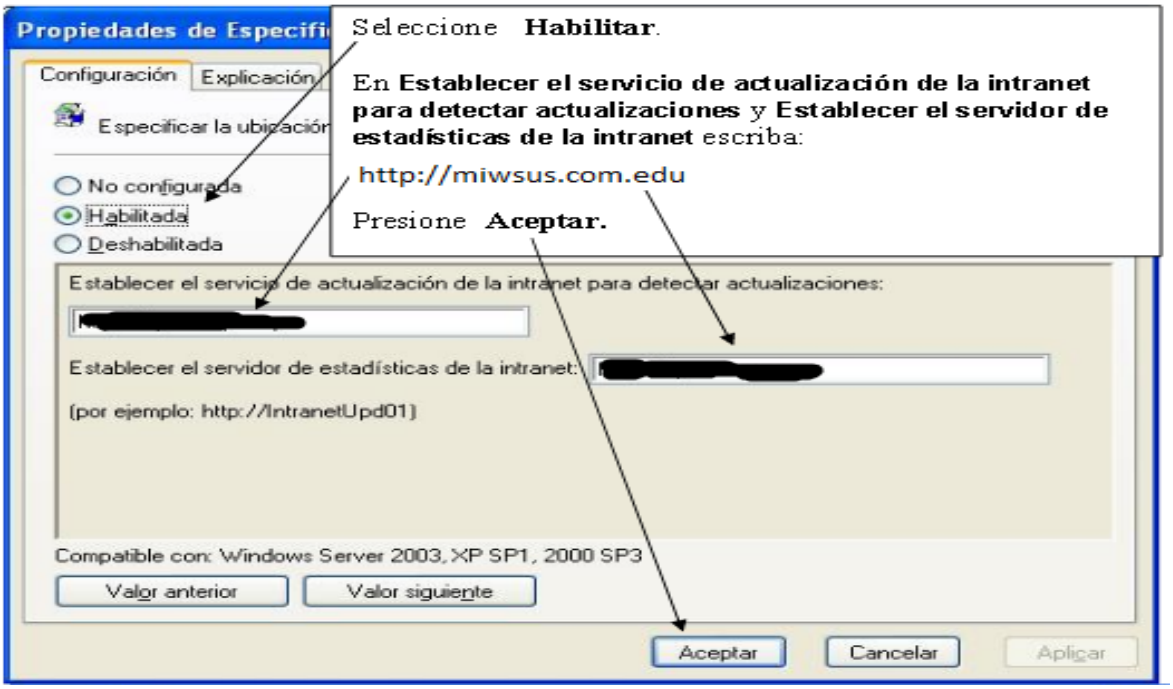
Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Se puede seleccionar horario y día, para que cumpla con la función.



Y en caso de tener un servidor WSUS, especificar su direccionamiento para que lo encuentre y aplique la correcta actualización, pero……

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 pesar de que podemos configurar las actualizaciones apuntando a donde queremos que las encuentre, quien se anima a explicar lo bueno y lo malo de esta opción de uso de WSUS.

Ejercicio Número 3 Unidad 2

Desarrollar en el foro, a través de las pregunta (no es por calificación, sino para debatir y ver distintos puntos de vista)

Si en vez de poner esa dirección, hubiésemos puesto otra pero de forma maliciosa, ¿qué se puede lograr u obtener?

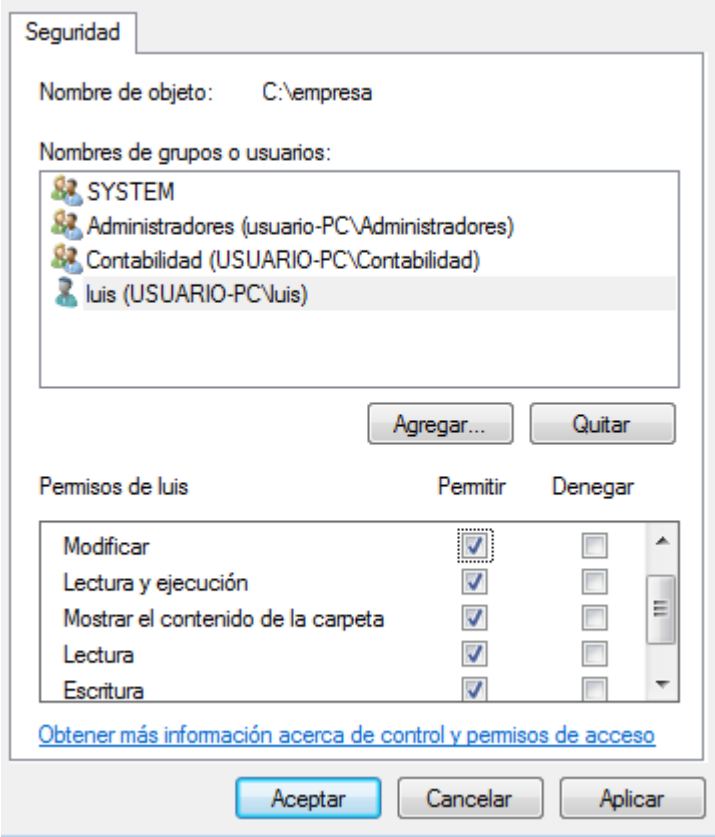
Detallar en lo posible, lo que un atacante quiere disponer o realizar.

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

Formas de mitigar este ataque

Las formas de evitar que se cambie la dirección a la que se buscan las actualizaciones son:

- Establecer usuarios que puedan cambiar esa configuración. Es decir, no darle los permisos suficientes al usuario "normal" de la PC para que realice esos cambios y sólo sean posibles por un administrador.



- Poseer un servidor de actualizaciones centralizado y que sea él quien provee las actualizaciones, de esta forma aseguramos que todas deberían apuntar a dicho servidor que descarga las actualizaciones únicamente de los servicios de Windows.

- Permitir actualizaciones firmadas sólo por Microsoft.

- Bloquear el servicio de actualización sólo para que se comunique con el servidor de Actualizaciones de Windows o por nuestro servidor centralizado.

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

- Si se conecta a un servidor centralizado, debemos permitir que **WSUS** se conecte a través de los puertos 8530 para **HTTP** y 8531 para **HTTPS** únicamente que a la dirección del servidor centralizado.

  Mientras que si se conecta con el servidor de Microsoft, solamente permitir que el servicio de **WSUS** se conecte a través de los puertos definidos para utilizar por **WSUS** (Por default son 80 para **HTTP** y 443 para **HTTPS**):

- ***http://windowsupdate.microsoft.com***
- ***http://*.windowsupdate.microsoft.com***
- ***https://*.windowsupdate.microsoft.com***
- ***http://*.update.microsoft.com***
- ***https://*.update.microsoft.com***
- ***http://*.windowsupdate.com***
- ***http://download.windowsupdate.com***
- ***http://download.microsoft.com***
- ***http://*.download.windowsupdate.com***
- ***http://test.stats.update.microsoft.com***
- ***http://ntservicepack.microsoft.com***

Éstas son las direcciones informadas por Microsoft para las actualizaciones.

Muchas pueden ser que dejen de funcionar o cambien el formato de la URL, por eso, siempre se recomienda chequear esta información en el sitio oficial de Microsoft.

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

Servicios disponibles para instalar / aplicar

Siguiendo con el **Hardening**, veamos lo que se debe saber:

Fortificación de cuentas de usuario

• Definición de roles restringidos
• Políticas de acceso restrictivas en base a grupos
• Política de contraseñas eficientes y no predecibles

Fortificación del sistema operativo

• Gestión periódica de parches
– Instalación: WSUS,SMS,BMC, CA PatchManagement
– Verificación: Microsoft Baseline

• Política de auditoría eficaz
– Auditar inicios de sesión
– Auditar cambios de políticas

• Auditar el acceso a cuentas falsas de usuario
– Administrador / Administrator

• Desinstalación de componentes no necesarios
– Software del sistema operativo
– Productos de terceros
– Servicios innecesarios

• Deshabilitar servicios del sistema no necesarios
– Evaluar la funcionalidad del sistema.

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

• Limitación de acceso al sistema de ficheros
– Lectura: robo de credenciales
– Escritura/Ejecución: Uso de exploits y backdoors.

• Comunicaciones seguras
– NTLM2/SSL
– IP estática

• Hosts restringido

Dispositivos y prevención de acceso físico

• Protector de pantalla

• Limitar uso de dispositivos USB

• Limitar acceso remoto a cdrom/floppy

• Deshabilitar dispositivos de Hardware
–Pantalla
–Teclado

• Ejecución automática.
– Chequear todo lo referente a Autorun

• Instalación de drivers no firmados

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

Anexo de Dispositivos

Instalación y afinación de Firewalls, Kits de Seguridad (Antivirus, antispyware, antimalware, anti hackers, anti banners) Sistemas de Detección de Intrusos y Sensores como **IDS,IPS,HIDS, NIDS.**

Uso de Herramientas para Penetration Testing y Monitoreo .

Configuración de Protocolos, Puertos y Servicios (Solo los necesarios).

Implementación de esquemas de seguridad, **DMZ**, Front End / Back End, Router, proxys, Firewalls.

Protección a ataques físicos o de Hardware (Seguridad Física).

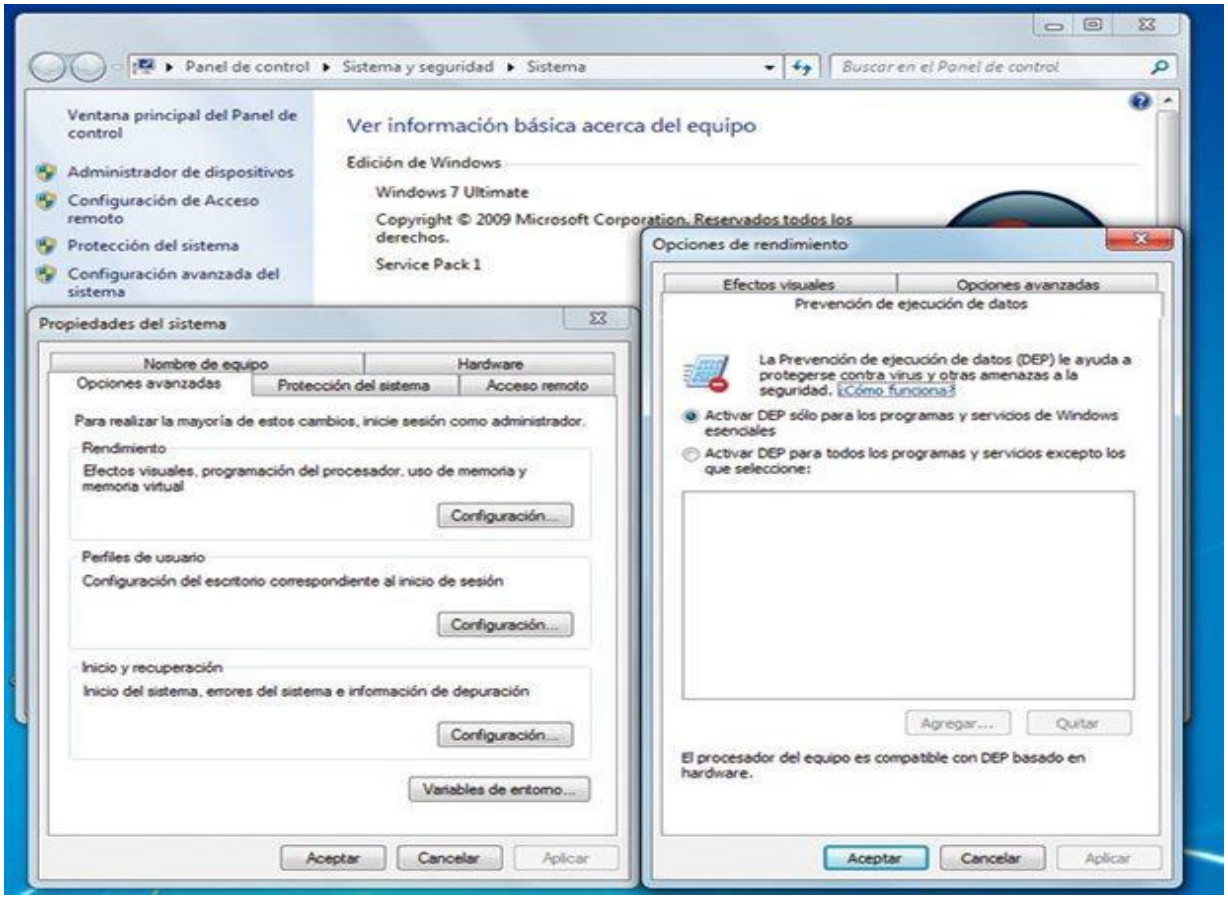
La prevención de ejecución de datos

La **Prevención de Ejecución de Datos** (**DEP**, en sus siglas en inglés) es una herramienta que limita la exposición de nuestro equipo a programas que ejecutan **código malicioso** desde la memoria del sistema.

Podemos supervisar los programas que indiquemos para asegurar que utilizan siempre la memoria sin riesgo, cerrando automáticamente los que estén haciendo un mal uso de ella y enviándonos al instante una notificación.

Así podremos evitar que el malware pueda ejecutar datos potencialmente peligrosos camuflados como instrucciones en tales programas legítimos.

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



***Panel de control/Sistema y seguridad/Sistema* y seleccionar *Configuración avanzada del sistema*.**

En *Opciones Avanzadas* pulsamos sobre el botón *Configuración*, en el apartado *Rendimiento*.

Accesos remotos

–Túneles SSH

• Filtrar todo el tráfico de entrada

• Instalar servidor SSHD

– Acceso mediante certificado y contraseña.

– Servicio como LocalService / usuario

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

• Redirección de puertos de acceso

– Terminal server.

–Administrative shares

• Problemática con servicios de backup remoto

• Definición de nuevos shares

– XC$, XD$, Xadmin$

• Limitación efectiva de ataques locales y remotos

– Pwdump, dameware,…

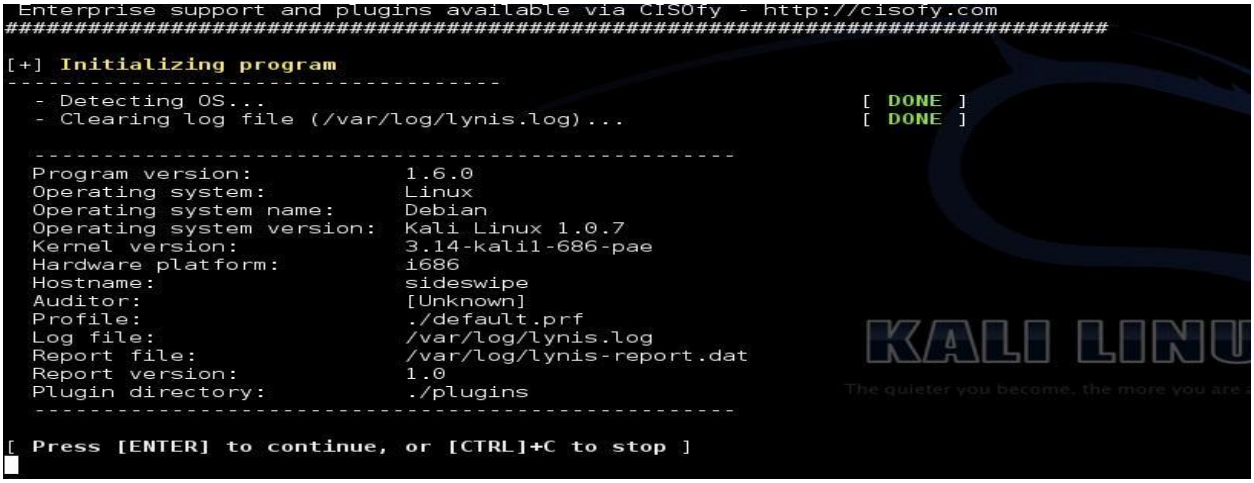
No se olviden que es recomendado tener preparada una máquina virtual, con cualquier sistema operativo Linux, ya que hablaremos de lo mismo pero con ese sistema.

Aquel que no tenga conocimientos de LINUX, por favor enviar un mail, que les paso manuales y tutoriales muy buenos para ponerse al tanto y no llenar de preguntas en el foro.

Tengan en cuenta que este curso está relacionado con la seguridad, por lo tanto, este no es un curso para aprender LINUX, únicamente expondremos los servicios dedicados a mantener áreas seguras.

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 de las mejores tools que se utilizan para ver qué tan robusta es la configuración de nuestro entorno en Linux, es **Lynis**.



Se recomienda que la prueben, cualquier consulta con el instructor.

Checklist Hardening

- Los procesos de arranque (del bootstrapping del sistema)
- Los servicios(en Windows) o demonios (en Linux) que se ejecuten en el inicio y apagado del sistema
- Aseguramiento de Sistemas de archivos (comúnmente denominados File System en *NIX y volúmenes en Netware - Novell)
- Uso de opciones de límites y forzar cuentas de usuario
- Políticas del sistema, filtrados y Acls
- Protección a ataques físicos o de Hardware (Seguridad Física)
- Actualización de Firmware, BIOS, Softpaq, contraseñas de arranque de los equipos, desactivación de unidades externas en servidores como pendrive o memorias USB, disqueteras, unidades de Cd/DvD, ópticas.

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

- Protección y renombre de cuentas de Administración y deshabilitar o invalidar cuentas estándares, invitado, uso de cuentas limitadas.

- Restricción de Instalación de Software y Hardware de acuerdo a las políticas de seguridad.

- Habilitar los sistemas de Auditorias y Monitoreo de logs.

- Asegurar consolas de administración, pantallas de logeo, terminales virtuales y accesos remotos.

- Políticas y procedimientos de administración de cuentas de usuario, grupos, TCBS (Truste Base Computing), módulos de autenticación agregables y relaciones de confianza.
- Administración de paquetes de instalacion, parches (Patchs), upgrades, updates, módulos instalables, integridad de archivos y permisos en el sistema.

- Aseguramiento de las Herramientas de Desarrollo y compiladores.

- Aseguramiento de Núcleos (Kernel) del sistema.

- Instalación y afinación de Firewalls, Kits de Seguridad (Antivirus, antispyware, antimalware, anti hackers, anti banners) Sistemas de Detección de Intrusos y Sensores como **IDS, IPS, HIDS, NIDS.**

- Uso de Herramientas para Pentesting y Monitoreo.

- Configuración de Protocolos, Puertos y Servicios (Solo los necesarios).

- Implementación de esquemas de seguridad, **DMZ**, Front End / Back End, Router apantallados, proxys, Firewalls.

- Políticas de Procedimientos de Respaldo y de Disaster Recovery.

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

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

Sitios excelentes, dado que nos exponen todas las medidas de Hardening posible en ambos versiones del sistema operativo Windows.

http://hardenwindows8forsecurity.com/index.html

http://hardenwindows10forsecurity.com/

http://www.networkedmediatank.com/wiki/index.php/Networking_with_Windows7

https://www.geeknetic.es/Guia/122/Menus-ocultos-del-sistema-operativo-Windows-XP.html

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

Guía paso a paso de Control de cuentas de usuario de Windows

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc709691(v=ws.10)?redirectedfrom=MSDN

30 cambios ideales para el uso de GPEDIT:

http://gpeditparamiscompanerosdehardware.blogspot.com.ar/

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).