

Experto Universitario en Ethical Hacking

Módulo 4:

Ethical Hacking

Unidad 2:

Métodos de control de Vulnerabilidades



Presentación

En esta segunda Unidad del módulo, se conocerán los distintos métodos utilizados para el testeo y obtención de vulnerabilidades.

Conocerán los conceptos más importantes en las tareas de un Pentester, así como las recomendaciones de uso.



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.



Bloques temáticos

1. Vulnerability Assessment
2. Penetration Testing
3. Ejercicios (distribuidos en la unidad)

Vulnerability Assessment

vulnerabilidades en cámaras IP del fabricante chino Foscam

9 junio, 2017 admin_ Seguridad

Vulnerabilidades en cámaras IP del fabricante chino Foscam

Investigadores en seguridad de **F-Secure** estuvieron analizando cámaras conectadas a Internet de la marca **Foscam** de procedencia china y se dieron cuenta de **graves vulnerabilidades** quedarían expuestas en manos equivocadas, el acceso a estas cámaras daría al cibercriminal una ventaja para ver transmisiones de video, descargar archivos e infectar dispositivos en red.

Pierre Kim dio a conocer un 0 day de otro **fabricante chino con 200.000 cámaras vulnerables** en internet.



Para realizar una evaluación correcta, hay una serie de pasos a efectuar, donde se aprende a tener en cuenta desde lo más pequeño encontrado hasta algún acontecimiento mayor, donde impondremos nuestros conocimientos, para demostrar la vulnerabilidad encontrada.

"Se ha publicado una vulnerabilidad presente en determinados Chipset de la firma Broadcom, en especial los modelos BCM4325/29 integrados en multitud de dispositivos inalámbricos como smartphones, tablets e incluso vehículos (como el Ford Edge).

Las estadísticas nos demuestran que las principales vulnerabilidades, son las personas, por lo que nos demostrara que no existen políticas ni reglas que se respeten para evitar este tipo de problema.



Sería recomendable tener en cuenta estos conceptos utilizados en este campo, donde veremos:

- **ACTIVOS** = recursos de la empresa
- **AMENAZA** = es cualquier peligro potencial que afecte negativamente a los activos, involucrando la Confidencialidad, Integridad y Disponibilidad
- **RIESGO** = posibilidad de que una amenaza concrete una vulnerabilidad en un activo
- **VULNERABILIDAD** = una debilidad en un sistema

¿Pero que es una vulnerabilidad?

Es todo aquello que no ha sido considerado en la protección de los activos, es una debilidad que tiene un bien y que puede ser explotada por una amenaza.

Las vulnerabilidades son muy variadas y al igual que las amenazas poseen una clasificación de acuerdo a su origen:

Física: Se refiere a las debilidades que pueda tener el entorno físico en el que se encuentran los activos, por ejemplo el control de acceso al lugar en donde se encuentran los bienes.

Natural: Son las vulnerabilidades que tienen que ver con que el sistema pueda ser dañado en caso de que ocurra algún desastre natural o ambiental.

De hardware: Al igual que las amenazas, las vulnerabilidades de hardware tienen que ver son los dispositivos y equipos. En este caso son consideraciones no tomadas en cuenta para el buen funcionamiento de los mismos, por ejemplo no darle mantenimiento constante al hardware, no verificar que el equipo que se compra cuente con los requerimientos necesarios, entre otros.

De software: Las fallas en los sistemas o debilidades en los programas instalados son ejemplos de este tipo de vulnerabilidades. Como su nombre lo dice, se refiere a aquellas relacionadas con el software como errores de programación, o que los protocolos de comunicación carezcan de seguridad.

De red: Son todas aquellas vulnerabilidades existentes en la conexión de equipos, por ejemplo si no existe un control que permita limitar el acceso, se puede penetrar al sistema por medio de la red. También abarca las fallas en la estructura del cableado y el no seguir los estándares recomendados para realizarlo.

Humana: Del mismo modo que las amenazas humanas, las vulnerabilidades tienen que ver con las acciones de las personas, por ejemplo ser vulnerable a la ingeniería social, no capacitar al personal como se debe, colocar contraseñas en lugares visibles, entre otras.

Mediante una serie de técnicas se pueden detectar las vulnerabilidades que afectan los activos:

- **Técnica de Seguridad Interna:** Análisis desde un sistema conectado a la red
- **Técnica de Seguridad Perimetral:** se evalúa la seguridad externa, chequeando fallos
- **Técnica de Seguridad Wireless:** Análisis a la red inalámbrica, desde un entorno externo e interno
- **Análisis WEB:** se chequean los servicios activos externos e internos (INTRANET)
- **Análisis de Aplicaciones y Código Fuente:** se conoce la aplicación, el software y el código fuente del mismo, para buscar fallos en la programación
- **Técnica de Análisis Forense:** una vez sucedido un problema, esta técnica puede guiarnos a ver que fue lo que aconteció, desde el posible inicio del incidente hasta el final del mismo, pasando también por datos relacionados con el atacante (IP ORIGEN, HORARIOS, TOOLS UTILIZADAS)

¿¿¿Que herramientas disponemos.....???

Dentro de los parámetros normales de software y hardware que podremos encontrar, veremos muchos dispositivos y aplicaciones preparadas para utilizarlas y que nos muestren resultados acorde a lo encontrado (te mostramos los nombres de las más conocidas)

- **Scanner de vulnerabilidades NESSUS**
 - **Scanner NIKTO**
 - **Scanner WPSCAN**
 - **Scanner SKIPFISH**
- **Dispositivos IPS / FIREWALL**

Ejercicio Número 1 Unidad 2



Buscar en Internet o en el uso habitual en nuestros trabajos, para realizar una lista de lo que podremos encontrar respecto a nombres de scanners de vulnerabilidades.

Ponerlo en el foro por favor, únicamente nombre de la aplicación, alguna captura y sitio web de descarga.

¿Cómo identificar esas vulnerabilidades?

Primero hay que encontrarlas y luego clasificarlas.

Chequear la relación de las mismas con el equipo evaluado (¿cómo se encontró?, ¿cómo llegó?, ¿cómo se ejecutó?, etc)

Por último, se identifica:

- ✓ **Por criticidad**
- ✓ **Por simplicidad de ejecución**
- ✓ **Vulnerabilidad de público conocimiento**
- ✓ **Por medida de riesgo**

¿Cómo se identifica una vulnerabilidad?

Cuando se trabaja con cualquier listado o categorización necesitamos utilizar identificadores únicos para poder trabajar de forma compartida.

Con la utilización de estos identificadores únicos se evitan confusiones y malos entendidos entre todas las personas que trabajan con estos sistemas.

En nuestro ámbito, la seguridad informática, el sistema de identificación de vulnerabilidades más conocido y utilizado a nivel mundial, si bien no es el único, es el **CVE** (*Common vulnerabilities and Exposures*) creado y mantenido por **MITRE**.



Common Vulnerabilities and Exposures
The Standard for Information Security

CVE-ID Syntax Changing on January 1, 2014 — [learn more](#)

TOTAL CVEs: 57577

About CVE
Terminology
Documents
FAQs

CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID

CVE In Use
CVE-Compatible Products
NVD for CVE Fix
Information
CVE Numbering
Authorities

News & Events
Calendar
Free Newsletter

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.
CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- ▲ [Vulnerability Management](#)
- ▲ [Patch Management](#)
- ▲ [Vulnerability Alerting](#)
- ▲ [Intrusion Detection](#)
- ▲ [Security Content Automation Protocol \(SCAP\)](#)

- ▲ [NVD \(National Vulnerability Database\)](#)
- ▲ [US-CERT Bulletins](#)
- ▲ [CVE Numbering Authorities \(CNAs\)](#)
- ▲ [Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures \(CVE\), ITU-T CYBEX Series](#)

Procedimiento etiquetado de vulnerabilidades

La numeración de las nuevas vulnerabilidades es responsabilidad de las **CVE Numbering Authority (CNA)**. Actualmente las CNA oficiales son la propia MITRE y 18 fabricantes de software (Adobe, Apple, Cisco, Google, HP, Microsoft, Mozilla, Symantec...) a los que se unen los tres principales coordinadores de equipos de seguridad: CERT/CC, ICS-CERT y JPCERT/CC. Cada uno de estos CNA dispone de bloques de numeración no coincidentes y que gestionan por sí mismos.

El procedimiento para crear un identificador único de vulnerabilidad CVE es relativamente simple:

- 1. Se descubre una nueva vulnerabilidad ya sea de forma interna (los propios fabricantes de software) o desde un tercero (que avisaría al CERT correspondiente).*
- 2. La CNA avisada asigna un identificador CVE, de la numeración que tiene asignada, en estado candidato. Se trata de la numeración que será asignada de forma oficial si la vulnerabilidad se confirma y se publica.*
- 3. Se revisa y confirma la vulnerabilidad y se estudia su alcance, afectación y criticidad.*
- 4. La vulnerabilidad se publica, con la numeración asignada inicialmente, en la web de CVE y se propone al consejo editor de CVE para su aprobación final. En caso positivo la numeración pasa al estado entry quedando fijada.*

Formato CVE

El formato de numeración CVE es sencillo pero efectivo. En la misma numeración se indica qué se está identificando y el año de aparición. Tras estos datos se muestra un identificador único para cada vulnerabilidad. Debido al sistema de reparto de la numeración entre CNA, por bloques, no es posible asegurar que el orden numérico de las vulnerabilidades correspondan con el cronológico de su publicación.

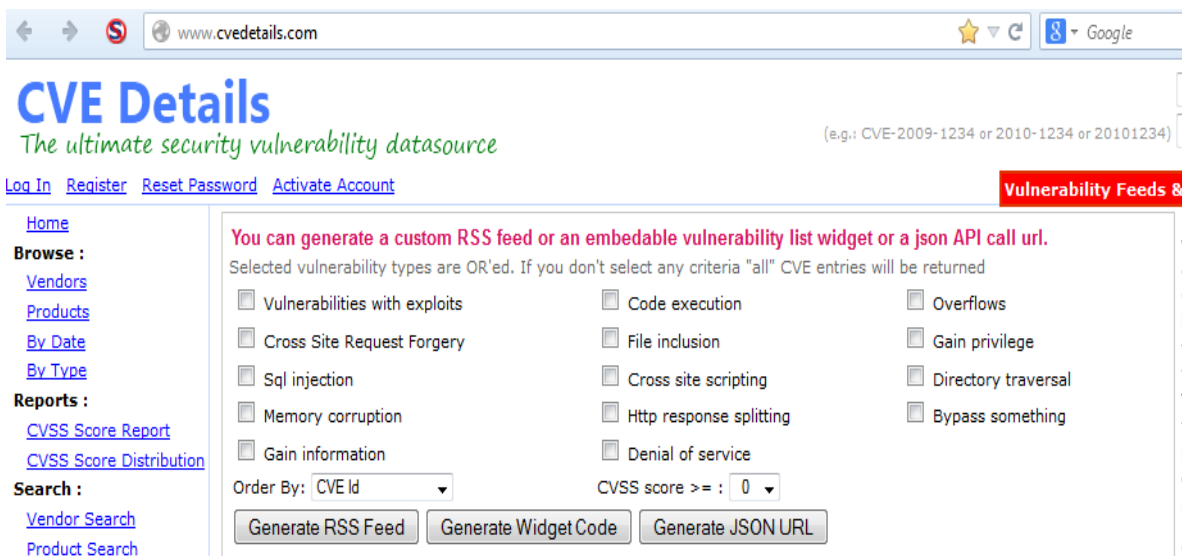
Ejemplo de código CVE:

Pondremos como ejemplo el identificador de una vulnerabilidad que afecta al sistema operativo Android y que se popularizó con el nombre de **Stagefright: CVE-2015-1538** donde podemos ver que está compuesto por tres partes:

CVE: Estas tres siglas identifican que la numeración siguiente corresponde a una vulnerabilidad CVE. Se introdujeron para evitar cualquier posible confusión con otros sistemas de identificación tanto públicos como privados (despieces de motores, etc.).

2015: El año de descubrimiento de la vulnerabilidad. Se trata del año en el que la primera CNA le asigna un código. Es posible que la publicación definitiva se realice durante el año siguiente, como pasaría con muchas vulnerabilidades descubiertas en diciembre.

1538: Identificador único dentro de CVE, del año en cuestión, que hace referencia a esta vulnerabilidad en concreto.



The screenshot shows the CVE Details website interface. At the top, there's a navigation bar with links like 'Log In', 'Register', 'Reset Password', and 'Activate Account'. Below this, the main heading 'CVE Details' is followed by the tagline 'The ultimate security vulnerability datasource'. A search bar is present with a placeholder '(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)'. On the left, there's a sidebar with 'Browse' and 'Reports' sections. The 'Browse' section includes links for 'Vendors', 'Products', 'By Date', and 'By Type'. The 'Reports' section includes links for 'CVSS Score Report' and 'CVSS Score Distribution'. Below the sidebar, there's a 'Search' section with 'Vendor Search' and 'Product Search' links. The main content area features a heading 'You can generate a custom RSS feed or an embedable vulnerability list widget or a json API call url.' followed by a note: 'Selected vulnerability types are OR'ed. If you don't select any criteria "all" CVE entries will be returned'. Below this, there's a grid of checkboxes for selecting vulnerability types: 'Vulnerabilities with exploits', 'Cross Site Request Forgery', 'Sql injection', 'Memory corruption', 'Gain information', 'Code execution', 'File inclusion', 'Cross site scripting', 'Http response splitting', 'Denial of service', 'Overflows', 'Gain privilege', 'Directory traversal', and 'Bypass something'. At the bottom, there's a 'Order By' dropdown set to 'CVE Id' and a 'CVSS score >= ' dropdown set to '0'. Three buttons are at the bottom: 'Generate RSS Feed', 'Generate Widget Code', and 'Generate JSON URL'.

Penetration Testing

A diferencia de la evaluación de vulnerabilidades, aquí podremos hacer uso de las técnicas mismas, que un atacante puede usar para crear un incidente.

Siempre se recomienda realizarlo en un ambiente controlado ya que al tener la posibilidad de usar herramientas y técnicas que se pueden considerar peligrosas, se podría ocasionar un inconveniente en el lugar donde se realice.

Esto se encuentra especificado en el contrato, donde estará aclarado las herramientas y técnicas que se usaran para realizar la tarea solicitada, así como también el alcance.

Un Pentest cuenta con una serie de tareas, donde la importancia de cada una es esencial.

- ✓ **RECONOCIMIENTO ACTIVO / PASIVO**
- ✓ **SCANNING / ESCANEEO**
- ✓ **ACCESO / ENUMERACION**
- ✓ **MANTENIMIENTO DE ACCESO / BORRADO HUELLAS**

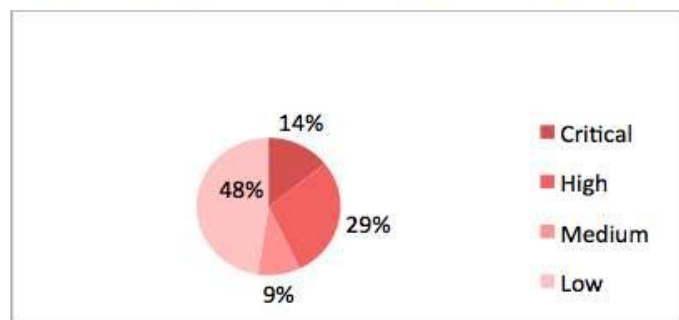
ATENCION: Se muestran estas 4 tareas, por ser las de mayor relevancia, pero igualmente a lo largo del curso, se verán todas

El objetivo de un pentest, es el de lograr reducir el riesgo mediante la prevención, detección y solución de las posibles vulnerabilidades encontradas, demostrando que tan fuerte puede ser la seguridad aplicada en el objetivo.

Vulnerability Summary

This chapter contains all identified vulnerabilities in the audited systems of the company <Client Name>

Severity	# of vulnerabilities
Critical	3
High	6
Medium	2
Low	10
Total	



2.6 Total Risk per Target

The following table contains a risk assessment for each system which contained security flaws.

System	Field of application	Risk
www.example.org	http/Web	High

2.7 Vulnerability Risk Rating

The following table contains a risk assessment for the discovered vulnerabilities.

Vulnerability	System	Risk
SQL Injection	Web 1	High
Cross-site Scripting	Web 1	High

Se habrá notado a lo largo del tiempo, las diferencias que hay entre un Análisis de Vulnerabilidades y un Pentest, a continuación, se expondrán las diferencias e igualdades consideradas de importancia:

ANALISIS DE VULNERABILIDAD

- ✓ Identificación de fallas de seguridad
- ✓ Análisis de vulnerabilidades
- ✓ Enumeración de los riesgos y amenazas
- ✓ La verificación escapa al análisis
- ✓ Se realiza al inicio del plan de seguridad

PENTEST

- ✓ Identificación de fallas de seguridad
- ✓ Búsqueda de vulnerabilidades
- ✓ Explotación de las mismas para comprobar falencias
- ✓ Se muestra y explica las evidencias del acceso logrado
- ✓ Se realiza al final del plan de seguridad

¿Qué no es un Pentest?

Conseguir todas las vulnerabilidades: en caso de ser un ataque de caja negra, los sistemas que no logren ser comprometidos pueden tener vulnerabilidades ocultas que solo son visibles desde una posición administrativa y como es un test rápido, la probabilidad de ocurrencia de falsos negativos y falsos positivos se incrementa.

Atacar todas las vulnerabilidades: hay vulnerabilidades que técnicamente no pueden ser atacadas en un período de tiempo acotado (por eso la importancia del alcance), dado que pueden existir varios caminos de ataque, un atacante puede elegir utilizar solo una y documentar el resto de las vulnerabilidades.

Corregir las vulnerabilidades: el pentester no debe solucionar las vulnerabilidades, ya que representa un conflicto de interés y se debe limitar a realizar recomendaciones para solucionarlas o mitigarlas, y luego realizar una auditoría de revisión (verificar lo realizado).

Ejercicio Número 2 Unidad 2



Buscar en Internet o en el uso habitual, y hacer una lista de lo que podremos encontrar respecto a pentesting (eventos, tools, etc)

Ponerlo en el foro, SER BREVE por favor, no más de 15 renglones.

Consejo del instructor de la unidad

Sabemos que una herramienta nos puede ayudar en nuestras tareas, pero en esta profesión, más importante que una tool es nuestra manera de actuar y pensar ante un incidente o eventualidad.

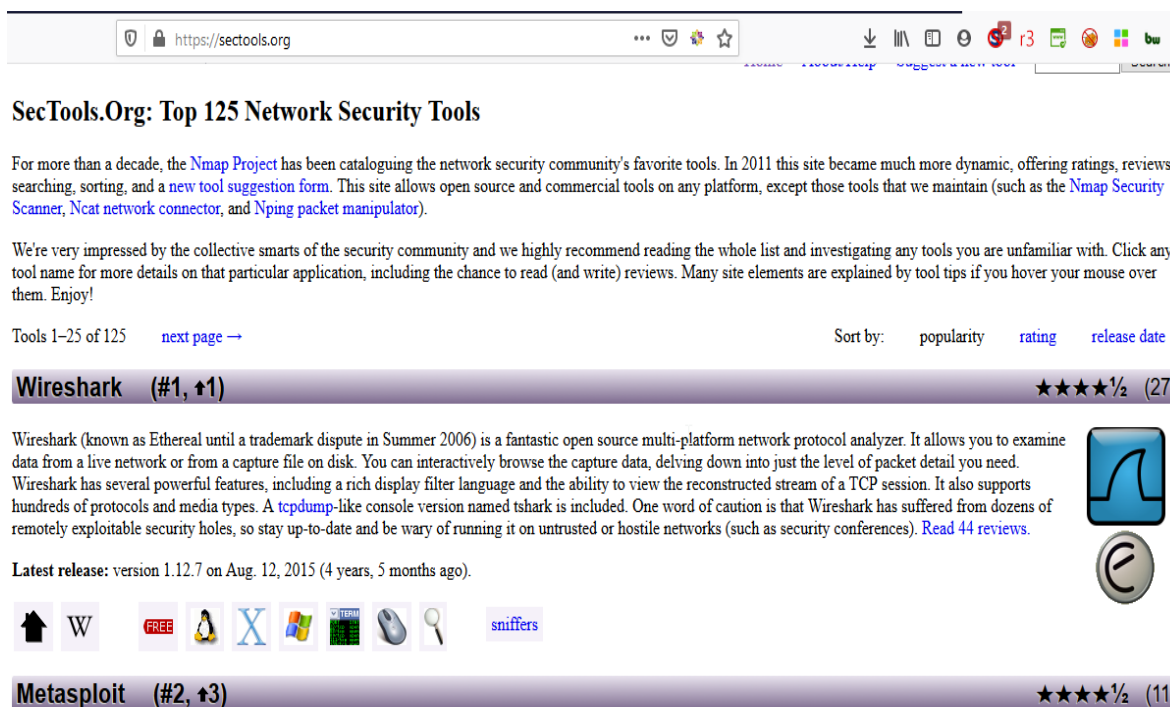
Existen miles de cientos de herramientas, y no existe en el mundo una persona que sepa el manejo y uso de todas las existentes, por eso es preferible saber para que utilizarla, como utilizarla y si es necesario hacer uso de la misma.

En un Pentest, el tiempo es oro, y sería una pérdida valiosa, el perder tiempo por una herramienta o el resultado que no sea el esperado.

Por eso recomiendo, analizar la situación, tener un listado de tools TOP, y saber en qué momentos utilizarlas.

Metasploit es muy bueno, pero no es la solución, porque en caso de utilizarlo para vulnerabilidades, se basa en una librería, nosotros nos basamos en nuestra mente, pensamos y podemos descartar un falso positivo, tengan en cuenta esto.

La herramienta o la tool, no es la única solución.



SecTools.Org: Top 125 Network Security Tools

For more than a decade, the [Nmap Project](#) has been cataloguing the network security community's favorite tools. In 2011 this site became much more dynamic, offering ratings, reviews, searching, sorting, and a [new tool suggestion form](#). This site allows open source and commercial tools on any platform, except those tools that we maintain (such as the [Nmap Security Scanner](#), [Ncat network connector](#), and [Nping packet manipulator](#)).

We're very impressed by the collective smarts of the security community and we highly recommend reading the whole list and investigating any tools you are unfamiliar with. Click any tool name for more details on that particular application, including the chance to read (and write) reviews. Many site elements are explained by tool tips if you hover your mouse over them. Enjoy!

Tools 1-25 of 125 [next page →](#) Sort by: [popularity](#) [rating](#) [release date](#)

Wireshark (#1, ↑1) ★★★★★½ (27)

Wireshark (known as Ethereal until a trademark dispute in Summer 2006) is a fantastic open source multi-platform network protocol analyzer. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, delving down into just the level of packet detail you need. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. It also supports hundreds of protocols and media types. A [tcpdump](#)-like console version named [tshark](#) is included. One word of caution is that Wireshark has suffered from dozens of remotely exploitable security holes, so stay up-to-date and be wary of running it on untrusted or hostile networks (such as security conferences). [Read 44 reviews](#).

Latest release: version 1.12.7 on Aug. 12, 2015 (4 years, 5 months ago).

Icons: Home, Wireshark, Free, Linux, Windows, Mac OS X, Sniffers

Metasploit (#2, ↑3) ★★★★★½ (11)

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 Learn the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU.

Link complementarios:

<http://www.cvedetails.com/>

<http://cve.mitre.org/>

<http://sectools.org>

<http://www.securityfocus.com/vulnerabilities>

<http://www.pengowin.com.ar>

<http://packetstormsecurity.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

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)