

# **Seminario de Desarrollo de Software, Tendencias y Seguridad**

**07/11/2014**

**Tema: Pentesting con énfasis en  
herramientas prácticas**

**Universidad Autónoma de  
Encarnación**

**Juan Carlos Miranda**

## Índice de contenido

1.Derechos del autor y otras cosas.....	3
2.Resumen.....	4
3.Panorama. ¿Donde estamos parados ahora en cuanto a seguridad de la información?.....	5
3.1.Unas cifras.....	5
3.2.Otros casos... Gobiernos que buscan en redes.....	5
3.3.Hacktivistas que protestan y se defienden manteniendo sus puntos de vista en la red.....	6
3.4.Tendencias, lo que colocamos/ usamos en la red.....	6
4.Factores humanos y tecnológicos.....	8
4.1.¿Como generar ambientes inseguros?.....	8
4.2.¿Que hace un encargado de seguridad?.....	9
4.3.Características para dedicarse a la seguridad de la información.....	10
4.4.Las cosas no siempre serán fáciles.....	10
5.Conceptos aplicados a la práctica de un pentest.....	12
5.1.Herramientas para un laboratorio de pentest.....	12
5.2.Metodologías para pentest.....	12
5.3.Recolección de información (Information Gathering).....	14
5.3.1.Introducción a la recolección de información.....	14
5.3.2.Conceptos y tipos de pruebas.....	15
5.3.3.Utilización de páginas públicas para recabar información.....	15
5.3.4.Utilización de buscadores.....	15
5.3.5.Herramientas especializadas para recolección de datos.....	16
5.3.6.Resumen de herramientas según la información a buscar.....	18
5.4.Herramientas para conservar el anonimato.....	19
6.Punto final.....	20
7.Anexos.....	22
7.1.Ejercicio – Atacar un servidor mediante el servicio ssh utilizando fuerza bruta.....	22
7.2.Ejercicio – Atacar un hash y obtener una contraseña.....	23
7.3.Recursos útiles sobre seguridad de la información.....	24

## **1. Derechos del autor y otras cosas**

Puedes compartir el documento, deberás mencionar siempre al autor.

El autor no se responsabiliza por la mala utilización de los conocimientos expuestos aquí.

Si encuentras errores colabora para que este sea un documento mejor y que sirva a otras personas.

Si quieres mejorar el documento, colabora con el autor.

**Juan Carlos Miranda**

Algunos emails en: [juancarlosmiranda81@gmail.com](mailto:juancarlosmiranda81@gmail.com)

Algunos códigos en Git Hub: <https://github.com/freelanceparaguay>

Algunos artículos en :<http://otroblogdetecnologias.blogspot.com/>

## **2. Resumen**

El presente documento, tiene como objetivo introducir al lector en aspectos actuales de nivel general, para luego ir trabajando en otras cosas más puntuales y prácticas.

Se hace una introducción sobre el panorama actual de la seguridad de la información en la red.

Se citan factores humanos y tecnológicos, los cuales modifican el nivel de la seguridad de la información en instituciones.

Por último, se enfatiza en la parte práctica para llevar a cabo un pentest, haciendo uso de herramientas y distribuciones Linux.

Se concluye con una serie de puntos a llevar en cuenta al momento de utilizar los conocimientos sobre pentesting.

### 3. Panorama. ¿Donde estamos parados ahora en cuanto a seguridad de la información?

Actualmente, parte de nuestra vida, por no decir, casi la totalidad de nuestra vida está ligada a medios electrónicos.

Estamos parados, en una situación donde no pasamos un día sin estar conectados a un dispositivo con acceso a Internet, aunque sea por unos minutos.

Es una realidad, donde pocas personas y sus datos personales no aparecen registrados en medios electrónicos. Ni que decir si uno abraza una profesión relacionada a las tecnologías.

Es un escenario donde en nuestro día a día conviven el trabajo por Internet, el anonimato en Internet, los ciberataques / ciberguerra, el espionaje de gobiernos y otros grupos, gran cantidad de información libre, fuentes creíbles y no tan creíbles, botnets y malware en general, educación en la red, servicios del mundo real en la web.

#### 3.1. Unas cifras

Al momento de escribir este documento tenemos que Paraguay maneja unas cifras de 30%-40% de penetración de Internet en nuestro mercado.

26,6% 30 % 40%

- Accedida el día 08/10/2014, publicación 23/03/2014, Diario La Nación, Casi un 40% de paraguayos ya tiene acceso a internet, <http://www.lanacion.com.py/articulo/159963--casi-un-40-de-paraguayos-ya-tiene-acceso-a-internet.html>
- Accedida el día 08/10/2014, publicación 17/05/2014, Diario Ultima Hora, El acceso de Internet a los hogares, <http://www.ultimahora.com/el-acceso-internet-los-hogares-n795345.html>
- Accedida el día 08/10/2014, publicación 22/07/2014, Diario ABC Color, Paraguay, 30% de avance en internet, <http://www.abc.com.py/edicion-impresaeconomia/paraguay-30-de-avance-en-internet-1268444.html>

#### 3.2. Otros casos... Gobiernos que buscan en redes

Se puede ver el control por parte de gobiernos y corporaciones en el espacio virtual.

- Ross Ulbricht por el caso 'Silk Road'. El portal de ventas de drogas dentro de la red Tor.  
Accedida el día 08/10/2014, publicación 08/10/2014, Actualidad RT , EE.UU.:El FBI puede

'hackear' servidores en el extranjero sin orden judicial previa  
<http://actualidad.rt.com/actualidad/view/142737-eeuu-fbi-hackear-servidores-extranjero-orden-judicial>

### **3.3. Hacktivistas que protestan y se defienden manteniendo sus puntos de vista en la red**

Otro punto, también existen organizaciones no gubernamentales de todo tipo que se defienden y buscan expresar sus opiniones en Internet.

- Accedida el día 08/10/2014, publicación 14/08/2014, Actualidad RT ,Anonymous dice haber identificado al policía que mató al joven afroamericano en Ferguson <http://actualidad.rt.com/actualidad/view/137145-anonymous-identificar-matar-ferguson-joven>
- Accedida el día 08/10/2014, publicación 5/09/2014, Actualidad RT ,Anonymous declara la ciberguerra al Estado Islámico, [http://actualidad.rt.com/ultima\\_hora/view/139354-anonymous-guerra-estado-islamico-internet](http://actualidad.rt.com/ultima_hora/view/139354-anonymous-guerra-estado-islamico-internet)

### **3.4. Tendencias, lo que colocamos/ usamos en la red**

La tendencia es asociar los datos a la nube, nunca sabemos en que ubicación geográficas están nuestros datos, pero si sabemos que están allí.

Las actividades cotidianas van teniendo una transición paulatina hacia el ciberespacio, tal cual como lo comenta la publicación de FRANCESC FONT COT “La Empresa Híbrida.”.

Gran parte de las transacciones en Internet se realizan con moneda electrónica y tarjetas de créditos. El Internet de las Cosas nos rodea constantemente.

Y... por si todo esto fuera poco, algunos de los servicios que se especifican a continuación:

- Tarjeta de crédito.
- Correos electrónicos personales, en algunos casos 2 o más.
- Correos electrónicos laborales.
- Acceso a redes sociales: Facebook, Twitter, Google Plus. (pueden agregar otras)
- Contraseña de bloqueo del celular.
- Contraseña de acceso del home banking.
- Pin de acceso de billetera del celular.
- Accesos a las páginas web de servicios.
- Acceso al sitio web de Hacienda.
- Universidad y plataformas de aprendizaje.
- Accesos a páginas de tele trabajos.

- Contraseña Wifi del hogar.
- Y ... otros. Juegos online, cursos y educación online, servicios de noticias, películas.

Muchos servicios se encuentran vinculados a una cuenta de correo personal y a un teléfono personal para la recuperación de las contraseñas.

Pregunta para el lector...

# **¿Cuanto vale mi cuenta de correo personal?**

## 4. Factores humanos y tecnológicos

Cuando se realizan labores relacionadas a la seguridad de la información, no encontraremos con factores humanos y con factores tecnológicos con los cuales se tendrá que trabajar en el día a día.

### 4.1. ¿Como generar ambientes inseguros?

Existen varios puntos que **“pueden hacer favorables los ataques a la redes”**.

- ✓ Exceso de confianza.
  - ✓ Falta cambios y pereza.
  - ✓ Software desactualizado.
  - ✓ Administradores con sobrecarga de trabajos y falta de tiempo.
  - ✓ Debilidades en conocimientos de seguridad.
  - ✓ Debilidades en datos que se publican.
  - ✓ Dispositivos con falta de mantenimiento, debilidades en políticas de contraseñas.
  - ✓ Usuarios finales con poco conocimiento.
- 
- **Exceso de confianza:** Se realizan auditorías pero estas son limitadas (por varios motivos), brindan resultados positivos dando una falsa sensación de seguridad. Muchas veces las auditorías externas no pueden poner de manifiesto todas las fallas de seguridad en una empresa. Esto se puede dar por ocultación de datos por parte del personal de TI, por desconocimiento de la propia empresa y su tecnología, por el alcance pactado en la auditoría de seguridad. Los administradores deberán seguir trabajando aunque no existen errores demostrables.
  - **Falta de cambios y pereza:** Muchas veces, los administradores de seguridad se encuentran bien acomodados en sus funciones y en sus labores diarias, no ven la necesidad de investigar sobre temas nuevos, solamente ejecutan tareas operativas repetitivas.
  - **Software desactualizado:** Sumado a la falta de cambios, se suman la falta de actualización que ocurren en los diferentes elementos de software. Es decir no renuevan ni parchan contra fallos de seguridad.
  - **Administradores con sobrecarga de trabajos y falta de tiempo:** Administradores sumidos en diversas tareas, que incluso, no hacen a la seguridad de la información. Tareas que les roba el tiempo y los distrae de aspectos importantes.
  - **Debilidades en conocimientos de seguridad:** Administradores que no buscan la superación y se estacan en las tecnologías que manejan en el día a día.
  - **Debilidades en datos que se publican:** Sin darse cuenta, personal de distintas instituciones, publican datos acerca de sus sistemas operativos, que luego de ser recolectados, ayudan a un atacante a ingresar a los distintos sistemas.
  - **Dispositivos con falta de mantenimiento, debilidades en políticas de contraseñas:** Además de contar con varios dispositivos que hacen a la red de comunicaciones, los mismos



## Seminario de Desarrollo de Software, Tendencias y Seguridad

no cuentan con revisiones periódicas y también no cumplen con la implementación de las políticas de contraseñas. Es decir, existen las políticas pero no están reflejadas en los dispositivos y accesos.

- **Usuarios finales con poco conocimiento:** El punto mas débil es el usuario que no conoce, aquel que hace clic en los links que se le envía. Que cree que las políticas de seguridad “**son para estorbarle en el trabajo**”, que se resiste a acatar las medidas de seguridad de la información. Como administrador, muchas veces se olvida este factor tan importante.

### 4.2. ¿Que hace un encargado de seguridad?

Anteriormente, el hacker de los años 90 era una persona joven, generalmente entre 16 y 25 años, aficionado a la informática que utilizaba conexiones a redes mediante teléfonos de línea fija.

Hoy en día con la expansión de Internet, los hackers han cambiado el nivel de profesionalismo, muchos de ellos son expertos en seguridad certificados. Otros son contratados por empresas, gobiernos o por el crimen organizado.

En cuanto a la inspiración, no prima justamente el querer desafiar a otros, se superpone la ganancias que podrá otorgar un objetivo concreto.

Cada día que pasa, los ataques en Internet son más puntuales y con un alto nivel de profesionalismo. Un hacker dijo lo siguiente:

*“El hacking es una habilidad. Cualquiera puede adquirir esta habilidad de forma autodidacta. Desde mi punto de vista, el hacking es un arte creativo, es averiguar cómo se puede burlar la seguridad utilizando el ingenio, del mismo modo que los aficionados a abrir cerraduras intentan sortear los mecanismos de cierre por pura diversión. Se podría hacer hack sin incumplir la ley.”*  
(MITNICK, Kevin, “El Arte de la Intrusión”. p. 123).

Por otro lado, también es preciso tener en cuenta lo siguiente:

*“Moraleja: si está a cargo de la seguridad de la información en un colegio, grupo de trabajo, empresa o cualquier otra entidad, debe contar con que algunos adversarios malintencionados, incluidas personas de la misma organización, están buscando una pequeña grieta en la pared, el unto más débil de la cadena de seguridad para romper la red. No espere que todo el mundo vaya a respetar las reglas. Tome medidas rentables para evitar las potenciales intrusiones, pero no olvide seguir buscando algo que haya podido pasar por alto. Hay quien cuenta con sus descuidos”.*  
(MITNICK, Kevin, “El Arte de la Intrusión”. p. 92).

El encargado de seguridad, tiene como tarea crear, ejecutar y actualizar políticas de seguridad. Se encarga de verificar que todos los elementos que hacen a una infraestructura de sistemas informáticos se encuentren seguros.

El área de seguridad informática abarca cosas como:

- Pruebas de intrusión.
- Verificación de vulnerabilidades.

## **Seminario de Desarrollo de Software, Tendencias y Seguridad**

- Actualización de parches de seguridad en software y dispositivos.
- Emisión de informes sobre el estado de seguridad, sobre intrusiones internas y/o externas.
- Trabaja en conjunto con el área de TI.

**“Seguridad de la información es mucho mas que contraseñas. Es mucho mas que utilizar una herramienta en particular.”**

### **4.3. Características para dedicarse a la seguridad de la información**

Una pregunta que siempre llega a la mente en cada charla de seguridad de la información

## **¿Si quiero dedicarme a la seguridad que necesito?**

- Curiosidad.
- Autodidacta.
- Capacidad de aprendizaje rápido de conocimientos técnicos y del negocio.
- Prueba y puesta en ejecución.
- Búsqueda de desafíos.
- Curiosidad.
- Curiosidad.

Es necesario:

- Conocer de redes informáticas y protocolos de comunicaciones.
- Programación de computadoras.

### **4.4. Las cosas no siempre serán fáciles**

En ciertos lugares, el encargado de la seguridad de la información, no goza de suficiente autonomía, también en otros casos se encuentra bajo la supervisión directa de un jefe del área de informática.

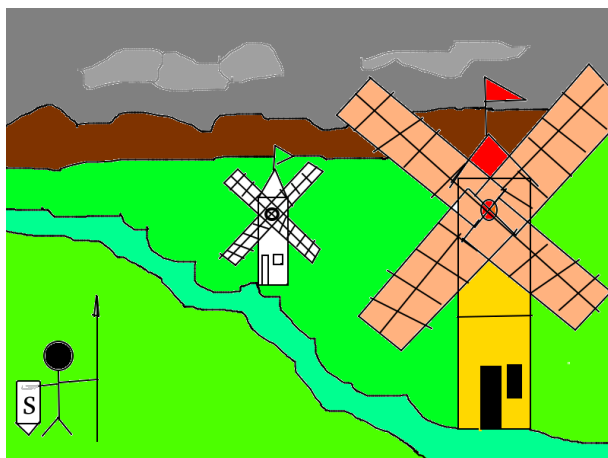
En algunos lugares, el mismo encargado de red, mezcla tareas de seguridad de la información, mantenimiento de redes y atención a usuarios finales.

Será necesario mucha paciencia y labor de concienciación para llevar a cabo la tarea evangelización sobre la seguridad de la información.

## Seminario de Desarrollo de Software, Tendencias y Seguridad



*Ilustración 1: Camino largo en el desierto*



*Ilustración 2: El encargado de seguridad de la información contra los problemas*

## 5. Conceptos aplicados a la práctica de un pentest

En este apartado se intenta dar respuesta a los siguientes interrogantes:

- ¿Cómo puedo comenzar a practicar?.
- ¿Qué debo llevar en cuenta?
- ¿Qué herramientas puedo utilizar para conservar el anonimato?

### 5.1. Herramientas para un laboratorio de pentest

Se citan herramientas, el lector no debe cerrarse a estas solamente, sino que puede hacer uso de software alternativo. Incluso puede contar con una red amplia para instalar y probar distintas distribuciones y montar servidores que simulen un entorno empresarial.

Nombre	Función	URL
Virtual Box	Software para crear hosts virtuales. Podrá ser utilizado para pruebas con distintos sistemas operativos.	<a href="https://www.virtualbox.org/">https://www.virtualbox.org/</a>
Kali	Distribución Linux, orientada al pentesting. Cuenta con gran variedad de herramientas agrupadas.	<a href="http://www.kali.org/">http://www.kali.org/</a>
Exploit Excercises	Nebula es una distribución con fallos de seguridad a nivel sistema operativo Linux. Cubre fallos simples y a nivel intermedio, basándose en niveles los cuales representan retos a cumplir. Es ideal para las personas que desean iniciarse en la explotación de vulnerabilidades Linux. Pueden ser encontradas otras distribuciones: Protostar y Fusion.	<a href="https://exploit-exercises.com/">https://exploit-exercises.com/</a>
Game Over	Distribución orientada a la explotación de vulnerabilidades web y aplicaciones con fallos de seguridad colocados estratégicamente para aprendizaje.	<a href="http://sourceforge.net/projects/null-gameover/files">http://sourceforge.net/projects/null-gameover/files</a>
Perl, Python, C	Compiladores e intérpretes de lenguajes de programación. Editores de sintaxis para lenguajes.	
Conectividad a Internet.	Conectividad a Internet para verificación de información y documentos.	
Router Wi-Fi	Router Wi-Fi para armar una red de prueba.	

### 5.2. Metodologías para pentest

Actualmente, para llevar a cabo los pentest se han desarrollado metodologías, las cuales han documentado las diversas pruebas que se pueden realizar en los sistemas computacionales.

No todos los puntos citados en una metodología son utilizados, dado que las mismas cubren un amplio espectro de situaciones.

Si bien, las metodologías sirven como referencia para encontrar vulnerabilidades. Un atacante no necesita seguir una metodología, sino mas bien encontrar solamente una falla.

Las metodologías nos ayudan a tener un marco de referencia y no dejar pasar los detalles.

## Seminario de Desarrollo de Software, Tendencias y Seguridad

A modo de información se puede citar las siguientes metodologías:

Penetration Testing Execution Standard		<a href="http://www.pentest-standard.org">http://www.pentest-standard.org</a>
Open Source Security Testing Methodology Manual - OSSTMM		<a href="http://www.isecom.org/">http://www.isecom.org/</a>
Information Systems Security Assessment Framework		<a href="http://www.oissg.org/">http://www.oissg.org/</a>
The Open Web Application Security Project - OWASP		<a href="https://www.owasp.org">https://www.owasp.org</a>

Habitualmente un pentest contiene las siguientes fases:

- Recolección de información. (tratado en este documento)
- Análisis de vulnerabilidades. (\*)
- Explotación de vulnerabilidades. (\*)
- Generación de informes. (\*)

**(\* fuera del alcance del presente documento)**

Se deja como tarea para el lector profundizar e indagar si tiene interés en metodologías.

Particularmente, no se hace énfasis en una metodología principal, se deja al lector la posibilidad de poder estudiar e investigar por su cuenta. También, se deja la posibilidad de investigación sobre la generación de informes al lector.

## Seminario de Desarrollo de Software, Tendencias y Seguridad

Las fases de análisis de vulnerabilidades, explotación e informes quedan fuera del alcance de este documento.

### 5.3. Recolección de información (Information Gathering)

#### 5.3.1. Introducción a la recolección de información

En el presente apartado se desarrollan distintas maneras de recolección de información utilizando fuentes de uso público las cuales son:

- Utilización de páginas públicas para recabar información.
- Utilización de buscadores.
- Herramientas especializadas para recolección de datos.

A las fuentes de uso público se las denomina OSINT (Open Source Intelligence).

Dentro de OSINT se pueden encontrar distintos tipos de áreas para relevar información, las cuales pueden ser:

<b>Empresas/instituciones</b> <ul style="list-style-type: none"><li>• Instalaciones físicas, localización física.</li><li>• Números de teléfonos.</li><li>• Organigramas de cargos.</li><li>• Proveedores.</li><li>• Empleados.</li><li>• Sistemas informáticos.</li></ul>
<b>Sistemas informáticos</b> <ul style="list-style-type: none"><li>• Nombres de dominio.</li><li>• Rangos de Ips públicas.</li><li>• Servidores DNS.</li><li>• Servicios de máquinas.</li><li>• Sistemas operativos.</li><li>• Metadatos de documentos públicos</li><li>• Localización geográfica.</li></ul>
<b>Datos de personas</b> <ul style="list-style-type: none"><li>• Números de documentos.</li><li>• Dirección de correo.</li><li>• Nombres y apellidos.</li><li>• Datos en redes sociales (esto puede variar por zona geográfica)</li></ul>
<b>Búsqueda de documentos y metadatos</b> <p>De los metadatos se busca lo siguiente:</p> <ul style="list-style-type: none"><li>• Usuarios: autores de documentos</li><li>• Carpetas donde se crearon los documentos.</li><li>• Impresoras.</li><li>• Correos.</li><li>• Versión de software con el que fue creado.</li><li>• Sistemas operativos.</li><li>• Software de ofimática.</li></ul>

El éxito de un ingreso a los sistemas depende fuertemente de la información relevada durante la

## Seminario de Desarrollo de Software, Tendencias y Seguridad

etapa de recolección de datos o “**information gathering**”.

Si bien es necesario conocer las herramientas para realizar tests, lo más importante **es saber lo que se desea averiguar del objetivo**. Cuanto más información se recolecte mayor será la probabilidad de éxito.

Incluso el lector podrá crear su propio software si así lo desea.

### 5.3.2. Conceptos y tipos de pruebas

Se denomina “footprinting” a las técnicas de recolección de información acerca de sistemas computacionales.

El footprinting puede hacerse en forma pasiva o activa.

- **Footprinting activo:** Es cuando se utilizan herramientas que envían paquetes directamente a los host de la red que se está analizando.
- **Footprinting pasivo:** Es cuando se recolectan datos del objetivo a analizar en forma indirecta.

Según los conocimientos previos sobre los sistemas a analizar se tienen los siguientes tipos de pruebas:

- **Pruebas de caja negra:** ningún conocimiento sobre el sistema a evaluar, es lo más cercano a la visión de un atacante externo.
- **Pruebas de caja blanca:** para saltar la etapa de recolección de información, se proporcionan todos los datos necesarios para que el atacante realice las pruebas directamente en los sistemas.
- **Pruebas de caja gris:** representa un punto intermedio en cuanto a los conocimientos de los sistemas, se provee información al pentester a modo de orientación.

### 5.3.3. Utilización de páginas públicas para recabar información

Se pueden utilizar páginas públicas para la recolección de los primeros datos.

Consultas de dominio utilizando herramientas web	<a href="http://nic.com">http://nic.com</a> <a href="http://nic.py">http://nic.py</a> <a href="http://whois.domaintools.com/">http://whois.domaintools.com/</a> <a href="http://www.robtex.com">http://www.robtex.com</a> <a href="http://mxtoolbox.com">http://mxtoolbox.com</a> <a href="http://www.netcraft.com">http://www.netcraft.com</a>	Búsqueda de informaciones tales como: DNS, Blacklists, dominios de correo.
	<a href="http://www.cuwhois.com">http://www.cuwhois.com</a>	Análisis de enlaces de la página. Análisis de cabeceras. Análisis de metatags. Información sobre servidores activos.

### 5.3.4. Utilización de buscadores

Se puede utilizar los buscadores para encontrar información acerca de un objetivo específico.

Entre los datos que podemos recabar en los buscadores se tiene:

- Teléfonos.

## Seminario de Desarrollo de Software, Tendencias y Seguridad

- Cuentas de correos.
- Dominios relacionados a los sitios.
- Archivos de distintos tipos (.doc, .xls, .pdf, .pps, jpeg, .png, etc..) para obtención de metadatos.
- Dominios relacionados con sitios.

Para el caso de los buscadores Bing y Google, se permiten opciones avanzadas, las cuales pueden incluir operadores lógicos del tipo: AND, OR.

Utilizando los buscadores es posible conocer datos de un sitio web, los cuales no se encuentran accesibles desde la página principal.

Comandos Google	
Ayuda sobre el buscador Google <a href="http://www.elhacker.net/trucos_google.html">http://www.elhacker.net/trucos_google.html</a> . También se pueden buscar los verbos bajo la frase “Google Dorks”.	
Verbos	Función
<b>site:</b>	Búsqueda dentro de un dominio específico.
<b>filetype:, ext:</b>	Búsqueda de archivos en un formato determinado.
<b>intitle:</b>	Buscar páginas con palabras en el campo title de las páginas.
<b>inurl:</b>	Buscar páginas con palabras específicas en la URL.
Ejemplos	
Búsqueda de documentos .DOC	filetype:doc site: midominio.com
Búsqueda de cuentas de correos	@midominio.com site: midominio.com.py
Búsqueda de teléfonos en páginas en español	Tel. site:midominio.com.py
Buscar índices en sitios web	intitle:index of site: midominio.edu.py

Comandos Bing	
Ayuda del buscador Bing <a href="http://onlinehelp.microsoft.com/es-es/bing/ff808421.aspx">http://onlinehelp.microsoft.com/es-es/bing/ff808421.aspx</a>	
Verbos	Función
<b>filetype:</b>	Búsqueda de archivos según la extensión.
<b>inanchor:, inbody:, intitle:</b>	Devuelve resultados con las palabras que se encuentran en el enlace, cuerpo del documento, el título.
<b>site:</b>	Devuelve las páginas web pertenecientes al sitio que se especifica.
<b>IP:</b>	Busca datos relacionados con un número de IP específica.
Ejemplos	
Búsqueda de documentos .PDF	filetype:pdf site: midominio.com
Búsqueda de cuentas de correos	@midominio.com site:midominio.com
Búsqueda de teléfonos en páginas en español	Tel. site:midominio.com.py

### 5.3.5.Herramientas especializadas para recolección de datos

En la fase de “Recolección de datos” se utilizan varias herramientas, las mismas se presentan a



## Seminario de Desarrollo de Software, Tendencias y Seguridad

continuación:

Nombre	Función	Autor/es	URL	Disponibilidad (pago/gratuito)	S.O recomendado para ejecutarlo
dnsenum	Enumerar datos relacionados al DNS de un dominio dado. Permite conocer los servidores de correo relacionados al dominio. Script Perl	Filip Waeytens <a href="mailto:filip.waeytens@gmail.com">filip.waeytens@gmail.com</a> tix tixxDZ tixxdz@gmail.com		Gratuito, disponible en Kali Linux	Linux
theHarvester	Recolección de correos electrónicos en buscadores. Script Python.	Christian Martorella <a href="mailto:cmartorella@edge-security.com">cmartorella@edge-security.com</a>	<a href="http://code.google.com/p/theharvester">Http://code.google.com/p/theharvester</a>	Gratuito, disponible en Kali Linux	Linux
goofile	Búsqueda de documentos utilizando google. Script Python.	Tomas Richards <a href="http://www.g13net.com">www.g13net.com</a>	<a href="http://code.google.com/p/goofile">Http://code.google.com/p/goofile</a>	Gratuito, disponible en Kali Linux	Linux
list-urls	Permite listar urls de una página web. Script Python.	Mark Pilgrim <a href="mailto:mark@diveintopython.org">mark@diveintopython.org</a>	<a href="http://diveintopython.org">Http://diveintopython.org</a>	Gratuito, disponible en Kali Linux	Linux
whatweb	Reconocimiento de las tecnologías utilizadas en un sitio web, correos electrónicos y otros datos. Desarrollado en Ruby	Andrew Horton	<a href="http://www.morningstarsecurity.com/research/whatweb">Http://www.morningstarsecurity.com/research/whatweb</a>	Gratuito, disponible en Kali Linux	Linux
joomscan	Identificación de vulnerabilidades para Joomla. Script python.	Aung Khant	<a href="http://yehg.net/lab">Http://yehg.net/lab</a>	Gratuito, disponible en Kali Linux	Linux
plesco	Identificación de vulnerabilidades para Wordpress	Francisco J. Gomez. Daniel Garcia Garcia	<a href="http://iniqua.com/1abs">Http://iniqua.com/1abs</a>	Gratuito, disponible en Kali Linux	Linux
Anubis	Herramienta que permite distintos tipos de test para la realización de recolección de información.	Juan Antonio Calles García	<a href="http://elblogdecalls.blogspot.com">Http://elblogdecalls.blogspot.com</a> <a href="http://flu-project.com">http://flu-project.com</a>	Gratuito	Windows
FOCA	Combina muchas funcionalidades en una sola herramienta, desde reconocimiento de hosts hasta metadatos de documentos. Es una de las herramientas más	Informática 64	<a href="http://www.informatica64.com">Http://www.informatica64.com</a>	Versiones free y paga.	Windows

## Seminario de Desarrollo de Software, Tendencias y Seguridad

	completas. Se encuentra disponible para entornos Windows.				
Maltego	Recolecta datos basados en fuentes públicas, dibuja las relaciones entre los objetos encontrados.	Paterva	<a href="http://www.paterva.com">Http://www.paterva.com</a>	Versión comercial. Versión no comercial (descarga gratuita). Kali Linux	Linux/Windows

### 5.3.6. Resumen de herramientas según la información a buscar

Es difícil realizar una clasificación clara para las herramientas presentadas, debido a las funciones que tienen. También es necesario hacer notar que un mismo dato puede ser obtenido por varias herramientas.

Siempre se deberá contrastar la información obtenida contra otras herramientas.

La siguiente tabla resume las herramientas que pueden utilizarse según los datos expuestos al comienzo del documento.

Datos a recolectar	Fuentes y herramientas
<b>Empresas/instituciones</b> Instalaciones físicas, localización física. Números de teléfonos. Organigramas de cargos. Proveedores. Empleados. Sistemas informáticos.	Buscadores Google, Bing. Folletería de marketing. Cartelería. Trashing (recolección de residuos) Consultas telefónicas. Anubis. Foca. Maltego.
<b>Sistemas informáticos</b> <ul style="list-style-type: none"> <li>Nombres de dominio.</li> <li>Rangos de Ips públicas.</li> <li>Servidores DNS.</li> <li>Servicios de máquinas.</li> <li>Sistemas operativos.</li> <li>Metadatos de documentos públicos</li> <li>Localización geográfica.</li> </ul>	Buscadores Google, Bing Dnsenum theHarvester goofile. Anubis.
<b>Datos de personas</b> <ul style="list-style-type: none"> <li>Números de documentos.</li> <li>Dirección de correo.</li> <li>Nombres y apellidos.</li> <li>Datos en redes sociales (esto puede variar por zona geográfica)</li> </ul>	Redes sociales. Buscadores Google, Bing. Redes sociales. theHarvester list-urls whatweb joomscan plesco
<b>Búsqueda de documentos y metadatos</b> <ul style="list-style-type: none"> <li>De los metadatos se busca lo siguiente:</li> <li>Usuarios: autores de documentos</li> <li>Carpetas donde se crearon los documentos.</li> <li>Impresoras.</li> </ul>	FOCA



- Correos.
- Versión de software con el que fue creado.
- Sistemas operativos.
- Software de ofimática.

“Cuanto más datos se tenga, mayor será el nivel de éxito que se podrá lograr”.

#### 5.4. Herramientas para conservar el anonimato

Si bien, las herramientas anteriores nos permiten conocer información pública, es probable que dichas herramientas NO oculten nuestra identidad, dado que tanto las consultas como nuestra dirección IP quedarían grabadas en los registros de los servidores.

Otro problema al que se enfrenta un auditor de seguridad, es que algunas herramientas dejan sus firmas cuando son utilizadas, lo cual hace posible que en una lectura de registros se puedan seguir pistas acerca del origen de las pruebas.


Nombre	Función	URL	S.O recomendado para ejecutarlo
Tails	Distribución Linux, basada en Ubuntu. Es la distribución por excelencia dedicada al anonimato en Internet. Es una distribución amnésica, no guarda registros.	<a href="https://tails.boum.org/">https://tails.boum.org/</a>	
Tor	Es una red abierta basada en software libre, que permite mantener el anonimato en Internet. Diseñada en principio por U.S. Navy.	<a href="https://www.torproject.org">https://www.torproject.org</a>	

## Seminario de Desarrollo de Software, Tendencias y Seguridad


Privoxy	Es un proxy web, con capacidades avanzadas de privacidad y para remover publicidad y otros elementos no deseados.	<a href="http://www.privoxy.org/">http://www.privoxy.org/</a>	<p><b>Privoxy - Home Page</b></p> <p>Privoxy is a non-caching web proxy with advanced filtering capabilities for enhancing privacy, removing Internet junk, and removing other obnoxious Internet junk. Privoxy has a flexible configuration and can be customized for multi-user networks.</p> <p>Privoxy is Free Software and licensed under the GNU GPLV2.</p> <p>Privoxy is an associated project of Software in the Public Interest (SPI).</p> <p>Helping hands and donations are welcome:</p> <ul style="list-style-type: none"> <li>• <a href="http://www.privoxy.org/faq/general.html#PARTICIPATE">http://www.privoxy.org/faq/general.html#PARTICIPATE</a></li> <li>• <a href="http://www.privoxy.org/faq/general.html#DONATE">http://www.privoxy.org/faq/general.html#DONATE</a></li> </ul> <p>The most recent release is <a href="#">3.0.21 (stable)</a>.</p> <p><b>Download</b></p> <ul style="list-style-type: none"> <li>• <a href="#">Download recent releases</a></li> <li>• <a href="#">Quickstart after installation</a></li> </ul>
Proxychains	Es un proxy para aplicaciones. Permite hacer túneles TCP y DNS. Se puede correr cualquier programa. Esconde el IP. Se puede utilizar SSH, telnet, wget, ftp, nmap y otros. Es un proyecto Open Source	<a href="http://proxychains.sourceforge.net/">http://proxychains.sourceforge.net/</a>	

En cuanto a otros proyectos relacionados con el anonimato se pueden ver:


### Our Projects



**Tails**  
Live CD/USB operating system preconfigured to use Tor safely.




**Orbot**  
Tor for Google Android devices.




**Tor Browser**  
Tor Browser contains everything you need to safely browse the Internet.




**Arm**  
Terminal (command line) application for monitoring and configuring Tor.



**Atlas**  
Site providing an overview of the Tor network.



**Pluggable Transports**  
Pluggable transports help you circumvent censorship.



**Stem**  
Library for writing scripts and applications that interact with Tor.



**Tor cloud**  
A user-friendly way of deploying bridges to help users access the uncensored Internet.

Ilustración 3: Proyectos <https://www.torproject.org>

## 6. Punto final...

Luego de haber leído el documento, hay algunas cosas a tener en cuenta:

- La fase de recolección es de suma importancia, dado que nos abre las puertas para el análisis y la explotación de vulnerabilidades. Etapas donde utilizaremos herramientas o las

## **Seminario de Desarrollo de Software, Tendencias y Seguridad**

crearemos.

- En el caso de realizar un pentest, es necesario asegurarse de contar con la autorización correspondiente de la empresa que será auditada, “siempre”.
- Durante el tiempo que se realice un pentest, es probable que existan otros intentando hacer lo mismo, pero con resultados diferentes, tal vez para otros fines.
- Como profesionales de las tecnologías, en algún momento va a aparecer un sentimiento de querer saber más. Ese sentimiento es bueno, nos lleva a aprender muchísimo.
- Si no existe una herramienta que se adecue, siempre podremos crear una según nuestras necesidades, o inclusive adaptar una existente.
- El placer del aprendizaje deberá estar por sobre todas las cosas.
- Queda a criterio de cada uno probar y poner en práctica los conocimientos.

## 7. Anexos

### 7.1. Ejercicio – Atacar un servidor mediante el servicio ssh utilizando fuerza bruta

<b>Objetivos del ejercicio</b>	:	<ul style="list-style-type: none"> <li>Utilizar una herramienta de fuerza bruta contra un servicio ssh.</li> <li>Rastrear el incidente desde la máquina víctima en forma básica.</li> <li>Mitigación de riesgos.</li> </ul>
<b>Conocimientos necesarios</b>	:	Arrancar y parar servicios en sistemas Linux. Configuración de redes para montar el laboratorio de prueba.
<b>Materiales necesarios</b>	:	<ul style="list-style-type: none"> <li>Host víctima. Distribución GameOver o estación con sistema Unix/Linux que tenga instalado.</li> <li>Host atacante. Distribución Kali. U otro sistema operativo con las herramientas instaladas.</li> <li>Servicio sshd en escucha para peticiones.</li> <li>Comandos tail, fgrep, lastlog, lastb, medusa, hydra.</li> </ul>
<b>Escenario</b>	:	<ul style="list-style-type: none"> <li>El host A denominado “víctima” IP 192.168.1.34</li> <li>El host B denominado “atacante” IP 192.168.1.35</li> <li>Host B encuentra el servicio abierto en host A.</li> <li>Host B, intenta acceder al host B mediante pruebas y fuerza bruta.</li> </ul>
<b>Comandos en Host víctima</b>		<b>Comandos en host atacante</b>
<p>Verificar en GameOver si el servicio sshd se encuentra corriendo. service ssh restart.</p> <p>#tail -f /var/log/auth.log para ver el ataque.</p> <p>#tail -f \$HOME/.bash_history para ver los comandos ejecutados. Esto funciona solamente cuando cierra la consola.</p> <p>#fgrep Accepted /var/log/auth.log para ver los ingresos.</p> <p>#fgrep Failed /var/log/auth.log para ver los fallos.</p> <p>#lastb .Para ver los intentos fallidos.</p> <p>#lastlog -u usuario específico para ver los accesos.</p>		<p>Probar primero un intento acertado con la contraseña correcta.</p> <p>Probar un intento fallido.</p> <p>ssh <a href="#">root@maquinavictima</a></p> <p>Prueba con la herramienta medusa</p> <p>#medusa -h 192.168.1.34 -u root -P diccionario.txt -M ssh</p> <p>Otra herramienta a probar es hydra</p> <p>hydra -l root -P diccionario.txt ssh://192.168.1.34</p>
<b>Observaciones</b>	:	<p>El uso de estas herramientas deja una gran cantidad de trazas que hacen referencia a la estación que hizo las pruebas, pudiendose determinar la IP desde la cual han sido enviados los ataques.</p> <p>Para GameOver, se debe habilitar el servicio ssh. Ejecutar #ssh-keygen, colocar el nombre del archivo de clave /etc/ssh/ssh_host_rsa_key</p> <p>Comentar la línea HostKey /etc/ssh/ssh_host_dsa_key, en el archivo /etc/sshd_config.</p> <p>#service ssh restart</p>

## 7.2. Ejercicio – Atacar un hash y obtener una contraseña

<b>Objetivos del ejercicio</b>	:	<ul style="list-style-type: none"> <li>Atacar un hash obtenido en un ataque.</li> <li>Dilucidar una contraseña a partir de un hash.</li> </ul>
<b>Conocimientos necesarios</b>	:	
<b>Materiales necesarios</b>	:	<ul style="list-style-type: none"> <li>Host víctima. Distribución GameOver o estación con sistema Unix/Linux que tenga instalado.</li> <li>Host atacante. Distribución Kali. U otro sistema operativo con las herramientas instaladas.</li> <li>Archivos con hashes de contraseñas. Esencial ganar muchísima información para poder llevar a cabo con éxito esta técnica.</li> </ul>
<b>Escenario</b>	:	<ul style="list-style-type: none"> <li>Se ha obtenido un hash del archivo shadow.</li> <li>Se han obtenido hashes desde bases de datos mysql.</li> </ul>

Comandos en Host víctima	Comandos en host atacante
Se recuperan los archivos	<pre>#john --wordlist=diccionario.txt --users=usuario shadow</pre> <pre>#john --show shadow</pre> <ul style="list-style-type: none"> <li>Los archivos de contraseñas encontradas se almacenan en un directorio oculto dentro del directorio del usuario que lo ejecuta. .john/ el cual contiene archivos de la ejecución de John The Ripper.</li> <li>Este es el archivo diccionario de la herramienta by default /usr/share/john/password.lst.</li> </ul>
Observaciones	: Existen veces donde para poder obtener un password pueden pasar años, o incluso miles de años. Esto varía según el ordenador en el cual se procesen los hashes. Esta clase de ataques no siempre es satisfactorio.

Comandos en Host víctima	Comandos en host atacante
<p>Se recuperan cadenas hash de distintos tipos. Pueden ser base de datos Mysql, CMS.</p> <p>Ejemplo de generación de hash.</p> <pre>#echo "unaclave" md5sum. Para generar una suma md5.</pre> <pre>#echo "unaclave" sha256sum. Para generar una suma Sha256.</pre> <p>Copiar el resultado y colocarlo para identificar con las herramientas.</p>	<pre>#hashid</pre> <pre>#hash-identifier</pre>
Observaciones	: Si no se encuentran indicios sobre el algoritmo utilizado. Se puede pensar en conseguir códigos fuentes de la aplicación para verificar el algoritmo.

## 7.3. Recursos útiles sobre seguridad de la información

Organismo/ institución	Descripción	Url
CERT Paraguay	Equipo de respuesta ante incidentes informáticos en Paraguay. Brinda asistencia sobre casos de delitos informáticos y ofrecen guías relacionadas a diversos temas.	<a href="http://www.cert.gov.py/">http://www.cert.gov.py/</a>
CVE MITRE	Base de datos sobre vulnerabilidades	<a href="https://cve.mitre.org/">https://cve.mitre.org/</a>
INCIBE	Organismo gubernamental del gobierno español. Se dedica a tratar temas relacionados a la seguridad de la información. En su página publican artículos y guías específicas.	<a href="https://www.incibe.es/">https://www.incibe.es/</a>
EXPLOIT DATABASE	Base de datos de exploits mantenida por la empresa Offensive Security. Información pública.	<a href="http://www.exploit-db.com/">http://www.exploit-db.com/</a>
SANS	Varios recursos relacionados a la información sobre vulnerabilidades.	<a href="http://www.sans.org/">http://www.sans.org/</a>
SEGU INFO	Blog sobre seguridad de la información con boletines sobre temas específicos.	<a href="http://seguinfo.com.ar/">http://seguinfo.com.ar/</a>
Agencia de la Unión Europea para la Red y Seguridad de la Información	Dentro de esta agencia funciona el CERT (Computer Emergency Response Team), el cual proporciona informaciones sobre ataques informáticos, provee materiales y recomendaciones.	<a href="http://www.enisa.europa.eu/activities/cert">http://www.enisa.europa.eu/activities/cert</a>
CERT	Materiales de lectura útiles, investigaciones sobre incidentes informáticos.	<a href="http://www.cert.org/">http://www.cert.org/</a>
Guías	Guía técnica sobre herramientas que pueden ser utilizadas para pentest	<a href="http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines">http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines</a>