

# Experto Universitario en Ethical Hacking

Módulo 4:

# Ethical Hacking

Unidad 4:

## Introducción sobre un Pentesting



## Presentación

En esta cuarta Unidad del módulo, se conocerán los distintos procesos iniciales para poder realizar un Pentesting.

Aprenderán lo que hay que tener en cuenta en cuanto al uso correcto de las tools y como realizar un modelo de reporte.

También conocerán la importancia de un convenio de confidencialidad.



## 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. El ABC de un Pentesting
2. Tools “auto mágicas”
3. Modelo de reporte y convenio de confidencialidad
4. Ejercicio Final del módulo

# El ABC de un Pentesting

## Mi consejo antes de continuar y empezar:

Ante todo, respirar y leer, entender y comprender, dado que una vez que estamos dentro de este procedimiento, no hay vuelta atrás, se empieza y se termina, no se puede dejar a medias, ni terminarlo en 10 segundos.

Estarán en juego muchas cosas, nuestra reputación o la de nuestro empleador o empresa, credibilidad, confiabilidad, y todo los “dad” posibles.

Saber que tareas vamos a realizar y llevar a cabo, en un orden preestablecido, cuidar lo que conseguimos y no dejarlo disponible a todo el mundo, respetar al pie de la letra el contrato, y no exagerar, ser lo más explícito posible en los informes.

Tener en cuenta que un informe de 3 páginas podría ser mejor que uno de 100 páginas, o al revés, así que hay que aceptar todas las posibilidades.

No caer en el juego de que porque no se encontró nada es un fracaso, al contrario, decirle al cliente las fortalezas que uno encuentra es parte de nuestro trabajo y se valorará.

El Pentesting, está dentro de los requerimientos que se necesita conocer y aprender para ingresar a los modelos que la Ciberseguridad necesita del mercado.



## Cuáles son las principales razones para realizar un Pentesting:

Es el método más efectivo para determinar el nivel real de seguridad de la información.

Un ataque simulado nos da la posibilidad de identificar las vulnerabilidades que plantean riesgos para la organización:

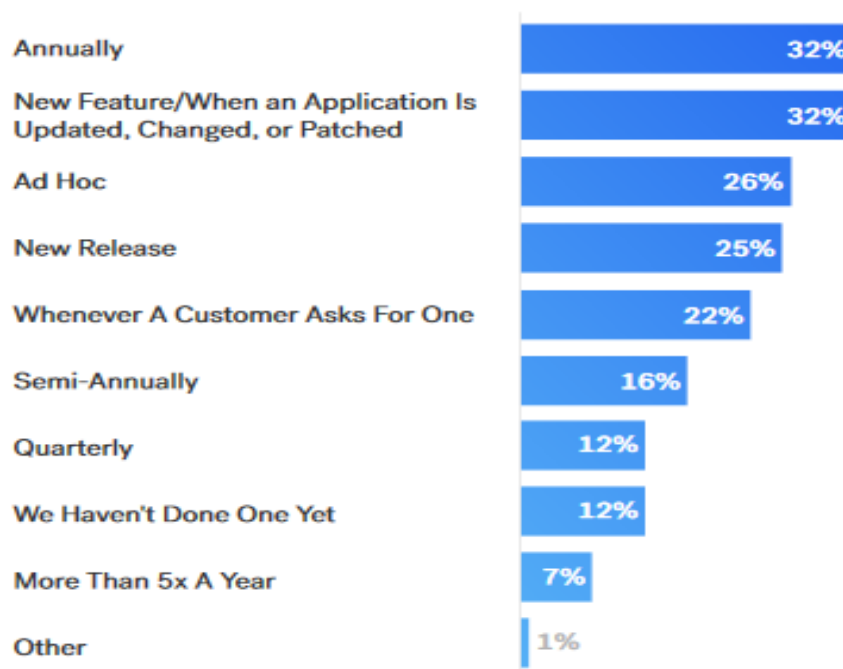
*Fraude (hackers, extorsión o empleados molestos)*

*Pérdida de confianza de los clientes u otra parte interesada*

*Crisis de relaciones públicas si trasciende a los medios masivos*

Otros de los temas más importantes, por lo cual es necesario realizarlo, es el tiempo, a continuación expongo estadísticas de Cobalt.io, una organización que se encarga de realizar distintos tipos de aportes en la comunidad, en esta caso métricas.

### HOW OFTEN DO YOU DO PEN TESTING?



Fuente:Cobalt.io



## ¿Quieren conocer los principales riesgos? Son pocos.....

Mails “anónimos” con información crítica o con agresiones

Robo de información

Spamming

Violación de e-mails

Destrucción de equipamiento

Violación de contraseñas

Intercepción y modificación de e-mails

Virus

Incumplimiento de leyes y regulaciones

Violación de la privacidad de los empleados

Ingeniería social

Fraudes informáticos

Programas “bomba”

Propiedad de la Información

Principales riesgos

Interrupción de los servicios

Destrucción de soportes documentales

Acceso clandestino a redes

Robo o extravío de notebooks

Acceso indebido a documentos impresos

Captura de PC desde el exterior

Indisponibilidad de información clave

Intercepción de comunicaciones

Falsificación de información para terceros

Agujeros de seguridad de redes conectadas



A continuación expondré una serie de pasos, donde el orden de aparición es el que a mi parecer es correcto, dada mi experiencia.

## **La primera “Reunión con el cliente”**



En la misma, se conocerá el alcance solicitado, que podría ser con 3 escenarios posibles: Pentest Interno o Externo o ambos.

Aquí se definirán los objetivos, que puede ser desde una IP específica, un rango de red, varios dispositivos, servidores internos o externos, servicios web u otros, etc.

Lo ideal sería que participen de la reunión, gente con conocimientos del lado del cliente, donde podrán exponer a nivel técnico, datos importantes sobre los mismos, siempre y cuando se trabaje en escenarios declarados.

Colaborar y ayudar al cliente, a comprender que distintos resultados podremos ofrecerles, referido a que todo dependerá tanto del entorno a examinar hasta el punto máximo de vulnerabilidades encontradas.

Uno no es adivino, es imposible saber de antemano lo que se puede encontrar, requiere un análisis profundo, por eso el pentesting es la solución.

## **Hablemos del alcance**

En el momento de la reunión, habrá que explicarle al cliente, los distintos alcances que se puede ofrecer o que el cliente pueda requerir, hay que comprender que el cliente puede pedir un alcance que no sea válido (quizás pueda estar equivocado, confundido o mal asesorado) entonces hay que estar dispuesto a explicarle exactamente lo que es “un alcance”.

Dentro del alcance tiene que quedar bien asentado estos tipos de procesos:

**Pentest Interno:** procedimiento que se realiza dentro del cliente

**Pentest Externo:** procedimiento que se realiza remotamente fuera del cliente o que el escenario no sea a nivel LAN.

**Objetivo:** dispositivo lógico o físico a evaluar (IP, Router, aplicación, celular, etc)

Ejemplo:

**“El alcance comprende 1 (un) Pen Test y Análisis de Vulnerabilidades Externo para los siguientes objetivos y componentes a ser validado por la compañía”**

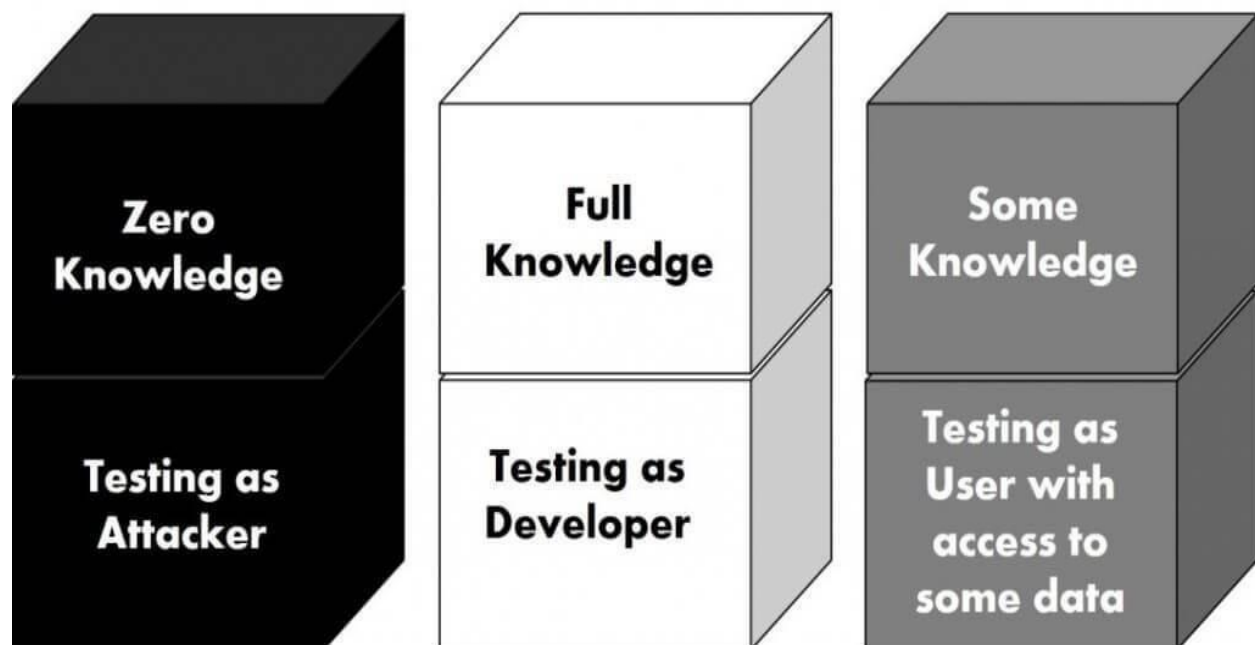
- **Muestreo de IP's EXTERNAS hasta un máximo de 5 en cada Sucursal**
- **Análisis de sistemas de acceso remoto.**
- **Situación de la seguridad en la conexión a Internet.**
- **Seguridad en la conexión con otras redes.**
- **Seguridad en aplicaciones Web.**
- **Seguridad en redes inalámbricas.**

Otro de los procesos de mayor importancia en el alcance, es el tipo de ambiente, lo cual hay varios también pero los más importantes y utilizados son:

**Ambiente WhiteBox:** el cliente nos ofrecerá información sobre el objetivo o nosotros podemos solicitarla

**Ambiente BlackBox:** el cliente nos comentara únicamente datos específicos sobre el objetivo, sin dar mucho detalle de los mismos.

### Differences between Types of Penetration Testing



Generalmente el cliente, siempre va a querer que el **Pentest** sea lo más parecido a un ataque real de un intruso, por ende, el ambiente **BlackBox** es el indicado, pero a nivel comercial es el mas costoso.

## **Preguntas que aconsejo realizar:**

- 1- ¿Que sucesos o incidentes impactarían más en su empresa/hogar?**
- 2- ¿Cuáles son los activos claves a proteger? (información de los mismos)**
- 3- ¿Cuáles son los procesos más importantes de la empresa/hogar?**
- 4-¿Cuáles son los dispositivos y equipos más importantes?**
- 5 y más importante: ¿qué dice el último informe de auditoría o alguna vez realizó un Pentest?**

### **Ejercicio Número 1 Unidad 4**



En un hipotético escenario, tomando como ejemplo el hogar del alumno o el trabajo del mismo como el objetivo, ¿qué responderían a las siguientes preguntas realizadas anteriormente?

Subir el ejercicio al foro de la unidad, dando su punto de vista, no es un ejercicio obligatorio, pero es para ver si se comprende la importancia de entender lo que es un alcance.

## ¿Qué enfoque utilizar?

Se utilizara un enfoque de trabajo que va de lo general al detalle, metodología de trabajo con bases de conocimiento y uso de herramientas automáticas, alineándose con estándares internacionalmente aceptados para la práctica de seguridad informática

(COBIT AUDIT GUIDELINES - COBIT: Control Objectives for Information and Related Technology, Normas ISO 27001 y sus relacionadas, Metodología OSSTMM Open Source Security Testing Methodology Manual, OWASP y GNU Public License).

## ¿Qué tareas básicas necesito saber y realizar sobre un Pentest externo?

Se compone de un elevado número de pruebas:

- **Ataques de Reconocimiento.**
- **Detección de conexiones externas.**
- **Obtención de rangos de direcciones en Internet.**
- **Detección de protocolos.**
- **Scanning de puertos TCP, UDP e ICMP.**
- **Análisis Dispositivos de comunicaciones**
- **Análisis de seguridad de conexiones remotas.**
- **Scanning de vulnerabilidades.**
- **Ingeniería Social.**
- **Prueba de ataques de denegación de servicio.**
- **Ejecución de código Exploit aplicable.**
- **Information Gathering**
- **DNS Stuff**

## **¿Qué tareas básicas necesito saber y realizar sobre un Pentest interno?**

Adicionalmente a las pruebas anteriores se pueden agregar:

- **Análisis de protocolos internos.**
- **Test a nivel de autenticación de usuarios.**
- **Análisis de la seguridad de los Servidores.**
- **Nivel de detección de la intrusión de los sistemas.**
- **Análisis de la seguridad de las estaciones de trabajo.**
- **Ejecución de código exploits**
- **Intento de DOS desde la red interna.**
- **Keylogging**
- **Lectura de tráfico de red para la obtención de usuario y password, lectura de correos, etc.**

## ¿Cuál será el trabajo de campo?

**Reconocimiento Superficial:** Network Footprinting (se intentará obtener la mayor cantidad de información posible del objetivo), rangos ip válidos, host vivos, ruteo hasta el objetivo, información de DNS (rangos IP Internos, servidores, transferencia de zona, subdominios), whois, presencia en internet, ingeniería social, Dumpster Diving, copia del sitio web, Information Gathering.

**Reconocimiento en Profundidad y Enumeración:** Fingerprint de Sistemas Operativos, Servidores, Dispositivos de Red, Dispositivos de protección (Detectores de Intrusos, Firewalls, filtros); escaneo de puertos, reconocimiento de servicios puestos en escucha, Banner Grabbing, sniffing de protocolos.

**Enumeración de vulnerabilidades** comunes a los servicios puestos en escucha, tests manuales de cada uno de los host vivos. Vulnerability Assessment de Dispositivos, Sistemas Operativos, Servidores, Aplicaciones mediante el uso de herramientas automáticas. Web Assessment, Wireless Assessment.

**Definición de las Herramientas a Utilizar:** Se analizan los resultados arrojados por las etapas anteriores y se preparan los ambientes para realizar las etapas posteriores.

**Ataque Puro o Penetración:** Se ejecutan los ataques predefinidos en ambiente controlado, dependiendo de los objetivos los ataques pueden ser sniffing pasivo, sniffing activo, recolección de credenciales de acceso, password cracking, ataques a los servidores, ejecución de código exploit, Inyección de código malicioso en aplicaciones (SQL Injection, Cross Site Scripting, Representación Canónica), ataques a los dispositivos, búsqueda de credenciales default, WEP Cracking, etc. Se obtienen evidencias del acceso o del ataque que puede ser captura de un trofeo, sembrado de un trofeo o reducción de la capacidad del servicio. Ataques de denegación de servicio en ambientes controlados a servidores y dispositivos de comunicación.

**Redefinición de pruebas** y herramientas a utilizar en base a resultados obtenidos

**Borrado de rastro y evidencias:** Se intentará borrar los rastros de accesos: logs, registro de eventos, huellas en dispositivos, aplicaciones y sistemas operativos.

**Consolidación:** Mediante el uso de técnicas no destructivas se intentará lograr un acceso a los sistemas para evidenciar el compromiso del sistema, pueden ser credenciales de usuario

obtenidas durante el test, dando de alta un nuevo usuario, levantando algún servicio cerrado. Posteriormente se volverá al estado anterior a la consolidación.

## Tools “auto mágicas”

En este trabajo, hay demasiados sitios web que ofrecen herramientas que “podrían” servir para darnos la posibilidad de hacerlo RAPIDO, ¿pero será PRECISO el resultado obtenido?

Cuando hablamos de herramientas “auto mágicas”, nos referimos a las tools que son muy fácil de usar (next, next, next, etc) y que lo único que se espera es cobrar el trabajo....

Dentro de este grupo, uno podría mostrar los scanners de vulnerabilidades conocidos y herramientas disponibles, pero hablemos de los más recomendados a mi parecer, sabiendo que hay muchas, mostrare unas cuantas.



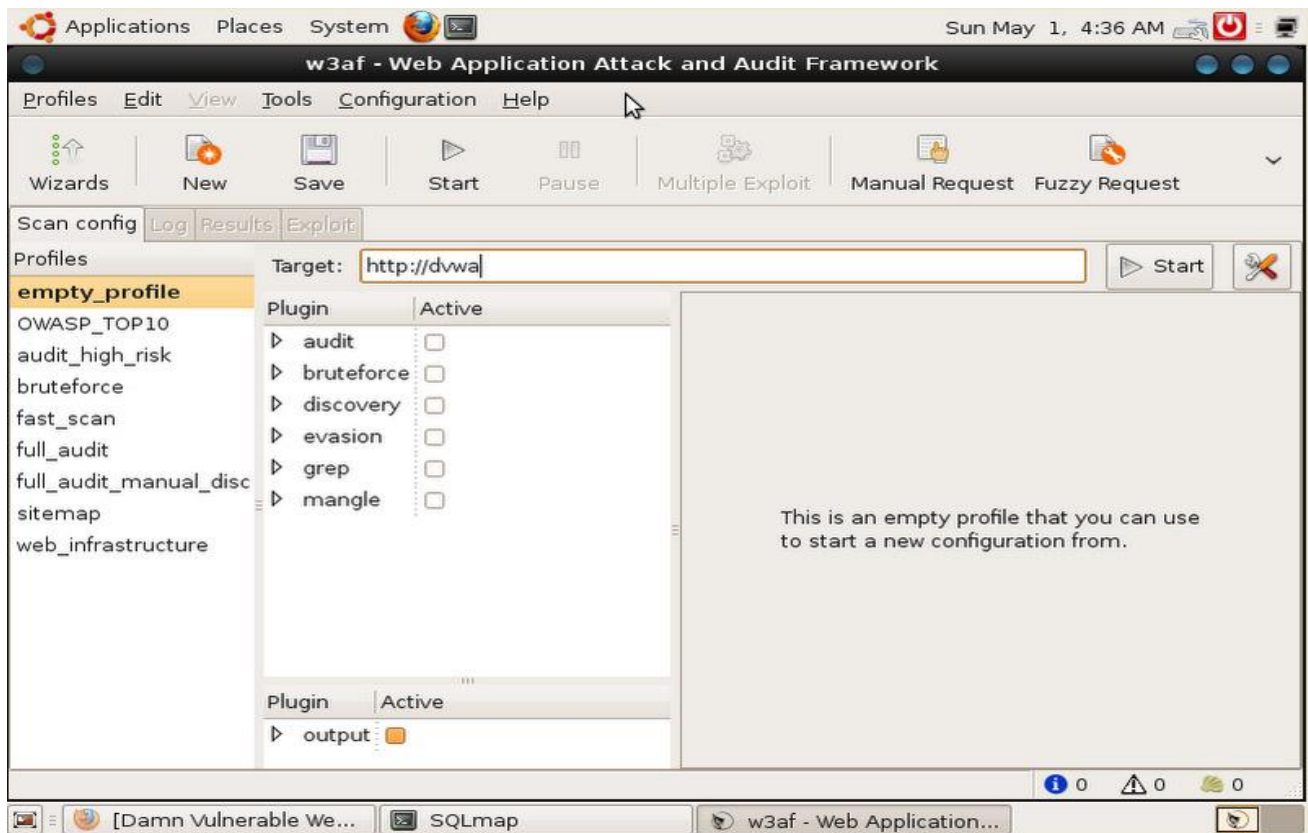
Arranquemos por uno que hizo historia, un framework de test de intrusión web, creado por un gran amigo: Andres Riancho en el 2007.

Esta desarrollado en Python, y tiene funcionalidad como scanner de vulnerabilidades.

Da la posibilidad de automatizar tareas repetitivas en un pentest.

Su arquitectura modular ofrece: bruteforce, grep, gathering, discovery, evasion, audit, attack



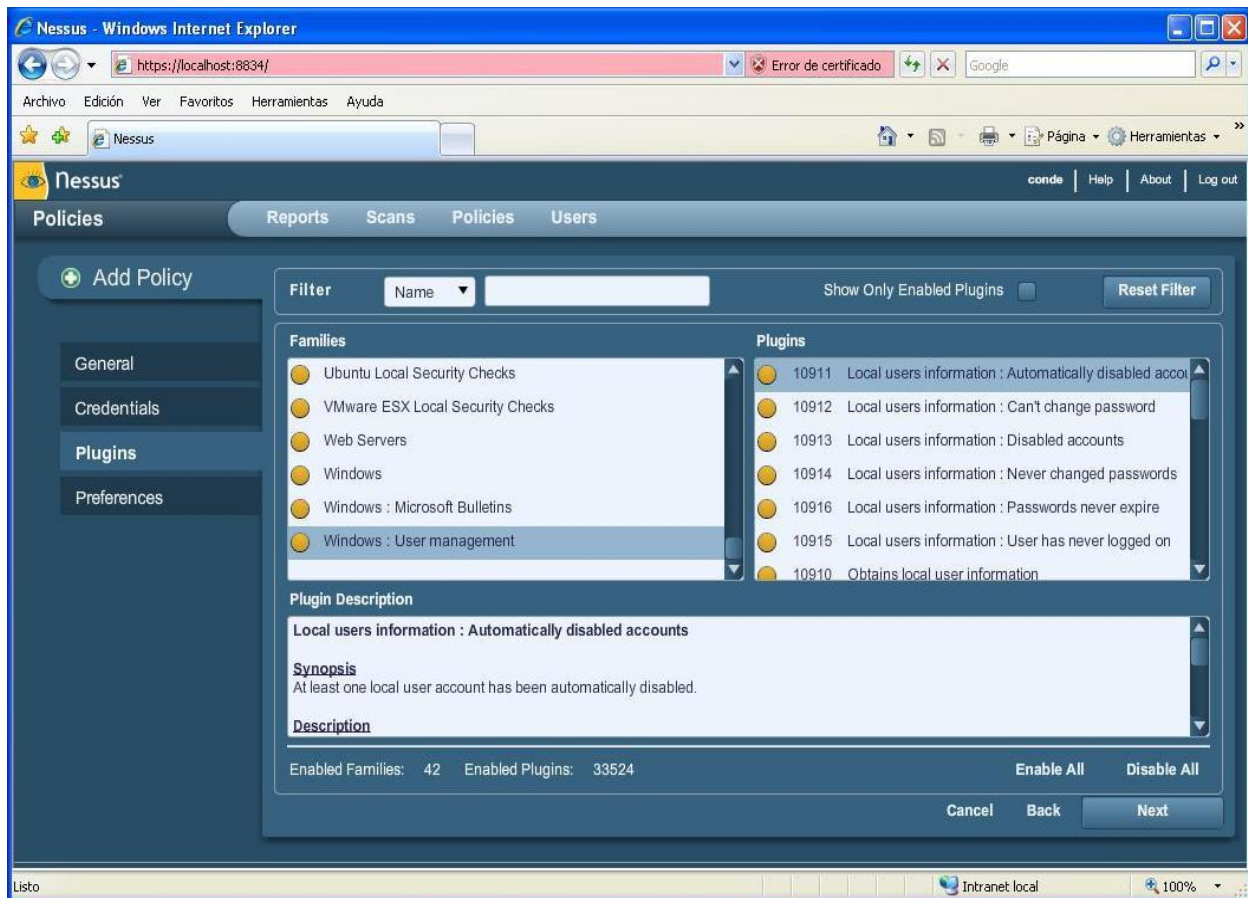


En el target se pone el objetivo, se seleccionan los parámetros necesarios, y luego START.



Nessus es un programa de scaneo de vulnerabilidades.

Nos da la posibilidad de realizar scaneos en los sistemas objetivos, aplicando en los mismos una enorme biblioteca de exploits y procesos automatizados, ofreciéndonos al final un reporte con cada vulnerabilidad encontrada y las manera de mitigar el riesgo.



Al igual que el W3AF, se inserta el objetivo, y los plugins a utilizar en el proceso de scaneo de vulnerabilidades.



Un scanner múltiple servicios por excelencia, dando la posibilidad de detectar: puertos, servicios, banners y hasta vulnerabilidades a través de scripts que podemos hacerlos manualmente o bajarlos de internet

Algunas Características:

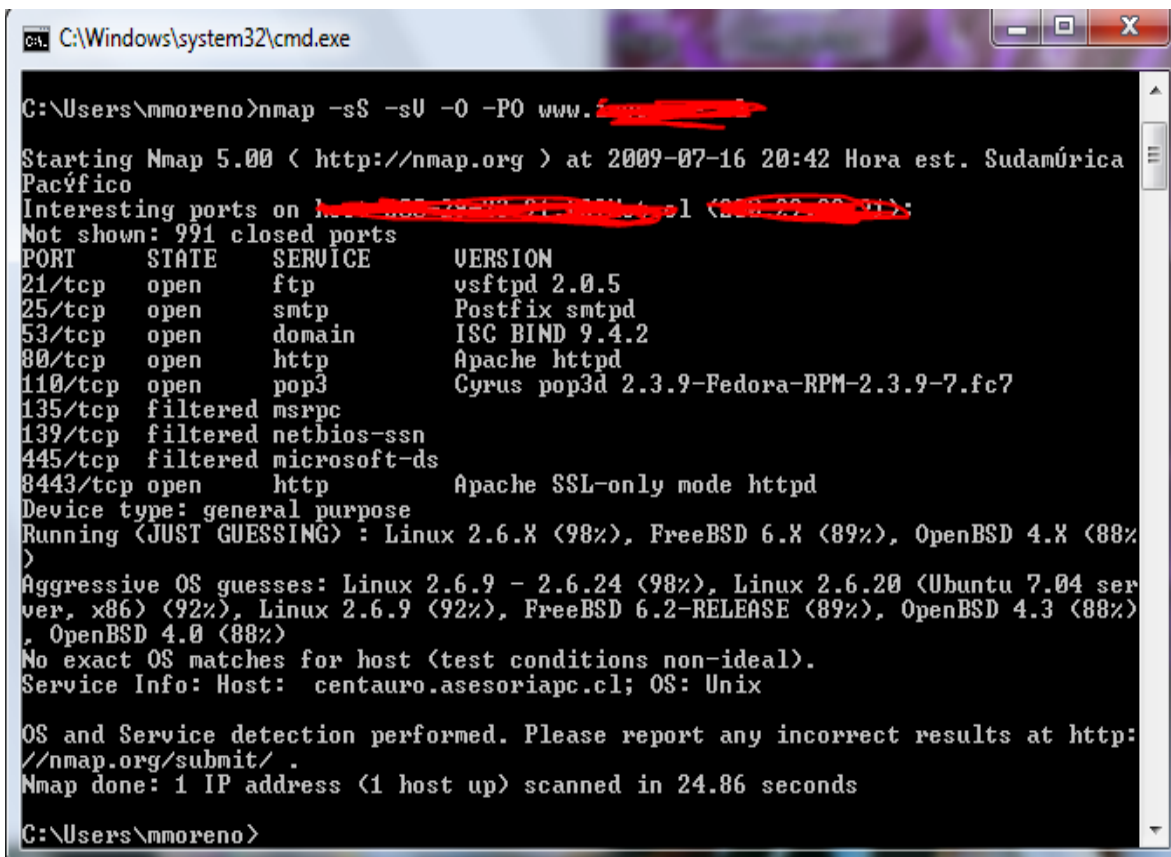
Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden ping.

Identifica puertos abiertos en una computadora objetivo.

Determina qué servicios está ejecutando la misma.

Determinar qué sistema operativo y versión utiliza el objetivo.

Obtiene algunas características del hardware de red del objetivo.



```

C:\Windows\system32\cmd.exe

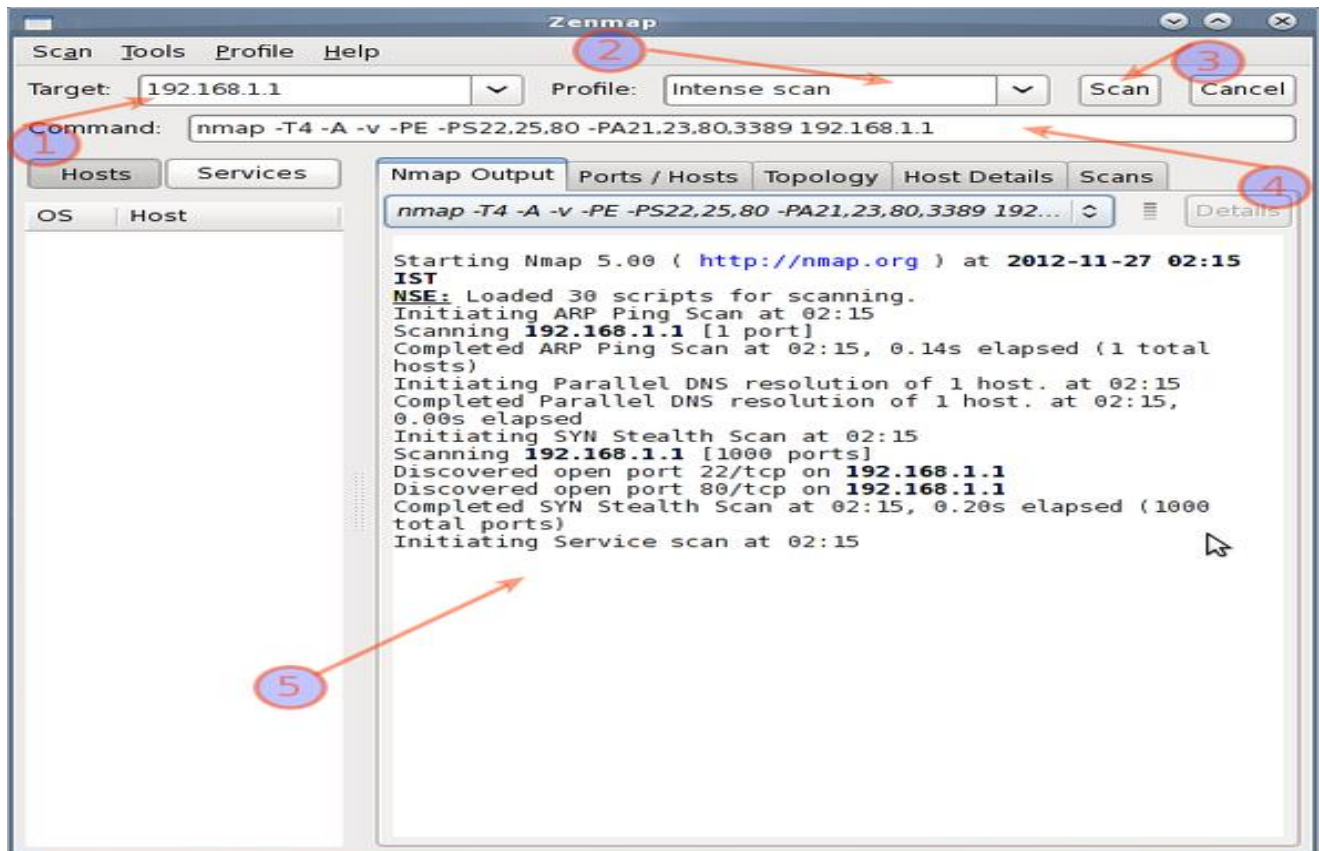
C:\Users\mmoreno>nmap -sS -sU -O -PO www.██████████
Starting Nmap 5.00 ( http://nmap.org ) at 2009-07-16 20:42 Hora est. Sudamérica
Pacífico
Interesting ports on ██████████ (██████████):
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.5
25/tcp    open  smtp         postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd
110/tcp   open  pop3         Cyrus pop3d 2.3.9-Fedora-RPM-2.3.9-7.fc7
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
8443/tcp  open  http         Apache SSL-only mode httpd
Device type: general purpose
Running (JUST GUESSING) : Linux 2.6.X (98%), FreeBSD 6.X (89%), OpenBSD 4.X (88%)
Aggressive OS guesses: Linux 2.6.9 - 2.6.24 (98%), Linux 2.6.20 (Ubuntu 7.04 server, x86) (92%), Linux 2.6.9 (92%), FreeBSD 6.2-RELEASE (89%), OpenBSD 4.3 (88%), OpenBSD 4.0 (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: centauro.asesoriapc.cl; OS: Unix

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 24.86 seconds

C:\Users\mmoreno>
  
```

Posibilidad de usarlo desde la línea de comandos, en este ejemplo, con opciones que nos mostrara sistema operativo, versión de servicios utilizados, y puertos abiertos, entre otros.

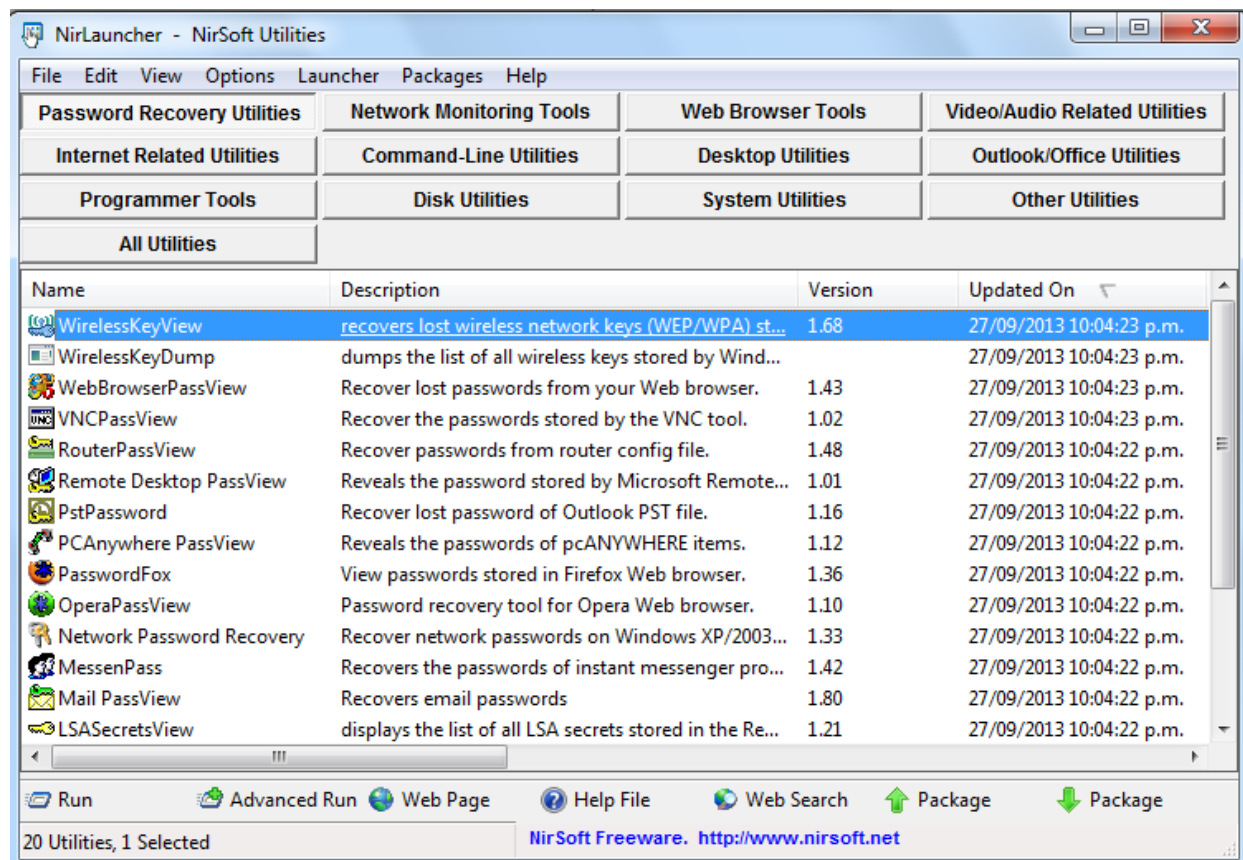
No solamente se puede manejar por consola, tiene un entorno GUI, para los que son fanáticos de las pantallas gráficas.



- 1- Insertar Target
- 2- Seleccionar tipo de acción/profile predefinido
- 3- Botón de scan
- 4- Opciones que podemos definir manualmente
- 5- Visual de procesos



Dos excelentes packages de tools, que se puede llegar a encontrar desde un visor de procesos hasta tools que mostrarán manejos de recursos o contraseñas ocultas.





Otras funciones:

- ✓ Utilizado para limpieza de valores del Registro.
- ✓ Listado de todos los controladores instalados.
- ✓ Comprobación de las asociaciones de archivos.
- ✓ Recuperación de contraseña.
- ✓ Programación.
- ✓ Monitoreo de red y muchas otras funciones que le permitirán ajustar, manejar y aprender más acerca del objetivo.
- ✓ Posibilidad de auditorías inalámbricas



No podemos dejar de nombrar la distribución de seguridad por excelencia, la cual está siendo utilizada tanto por profesionales y principiantes.

Podemos dar un curso de esta distribución debido a todo lo que tiene, por lo que recomendamos que busquen en internet o solicitar por mail, que les mando tutoriales.



Contiene más de 100 herramientas relacionadas con todo el mundo del Hacking, incluye Análisis Forense, OSINT, entre otros.

Por último las herramientas utilizadas por los consultores son de distribución libre y de fácil descarga de Internet, en algunos casos se utilizan formato LIVE que reúnen la mayoría de las herramientas necesarias para los testeos.

Estos listados son un resumen de las más conocidas, hay cientos más de herramientas.

**Reconocimiento Superficial:** IPSCAN, NMAP, HTTPFINGERPRINT, OSFPFINGER, UMIT, SAM SPADE, WEB SERVER FINGERPRINT, MENGSWEEPER, NETRANGER, MPTRACEROUTE, SUPER SCAN, SPIDERFOOTPRINTING, ITRACE, NSLOOKUP, TRACERT, DNS STUFF, GOOGLE, WIKTO, SITE DIGER, SERVICIOS NIC, WHOIS.

**Reconocimiento en Profundidad y Enumeración:** AMAP, QUESO, WOT WEB FINGER, TELNET, WIRESHARK, NETBIOS SECURITY KIT, RETINA WIFI SCANNER, NESSUS, MSBASELINE, NIKTO, PAROS, SPYKE PROXIE, WSKNIGHT, WSPAWN, PROMQRYUI, OPENRELAY CHECK, KISMET, NETWORK STUMBLER, HTTPTRACK, SNSCAN, SQLSCAN.

**Ataque Puro o Penetración:** META EXPLOIT FRAMEWORK, CAIN, R3X, HYDRA, BRUTUS, PWDUMP, NETCAT, FTP FUZZER, SQL INJECTOR, PUSH VNC, EXPLOITS

VARIOS PROGRAMADOS EN LENGUAJE C, PHYTON Y PERL, AIR CRACK, WLAN EXPERT, AIRODUMP.

**Borrado de rastro y evidencias:** COMANDOS PROPIOS DE LOS SISTEMAS OPERATIVOS COMPROMETIDOS.

**Consolidación:** ABEL, NETCAT, COMANDOS PROPIOS DEL SISTEMA OPERATIVO COMPROMETIDO.

En algunos casos se utilizan formato Live de distribución libre con un compendio de la mayoría de las herramientas descriptas anteriormente.

## Reporte e informe final

**Reporting y Quality Assessment:** es la documentación formal y el desarrollo de Informes Finales (Técnico y Ejecutivo).

El informe técnico, es para que los especialistas del lado del cliente con conocimientos de la infraestructura puedan chequear y asentar lo realizado.

Mientras que en el informe ejecutivo, estará un resumen de lo encontrado, haciendo hincapié en los riesgos, fortalezas y debilidades encontradas junto a un plan de acción.

Por último, se encontrara el valor de nuestro trabajo, lo cual en nuestro país no hay una lista estándar de precios, lo que sí la metodología está basada en cobrar por horas de trabajo.

Ejemplo:

“Un pentest externo sobre un servidor WEB, tendrá un período de Pentesting, de 20 horas de trabajo”

Involucra el testeo y el armado del informe.



# Convenio de confidencialidad

## CLÁUSULA DE CONFIDENCIALIDAD

“El siguiente informe contiene información confidencial, no debe ser enviada vía email, fax o cualquier otro medio electrónico a menos que este se encuentre específicamente aprobado por las políticas de seguridad de las copias electrónicas o en papel del presente documento deben ser guardadas en un sitio protegido. No comparta la información contenida en este documento, a menos que la otra persona este autorizada para ello.”

Es tan importante esta parte, dado que la información que obtendremos es muy delicada, un intruso podría tranquilamente utilizar la misma o peor aún, a partir de las encontradas usarlas como camuflaje, y hacer mas complicada la vida del administrador de la red.....

### De regalo un ejemplo de convenio

#### MODELO DE CONVENIO DE CONFIDENCIALIDAD SUGERIDO

##### Acuerdo de Confidencialidad

La “Parte Informante” (XXXXXXXXX) y la “Parte Receptora” (Empresa responsable Pentest) se ponen de acuerdo en:

1. La Parte Informante entrega a la Parte Receptora información de su propiedad relativa a las configuraciones de seguridad de sus equipos informáticos sujetos al relevamiento que la Parte Receptora recibe oportunamente.
2. La información entregada por la Parte Informante a la Parte Receptora, el hecho de esa entrega y todos los actos que sean su consecuencia, constituyen Información Confidencial.
3. La Parte Receptora se obliga a:
  - a) Mantener el carácter secreto de la Información Confidencial y no darla a conocer sin el consentimiento escrito de la Parte Informante.

b) Utilizar la Información Confidencial exclusivamente para las tareas definidas en el alcance específico de este proyecto.

c) Restituir toda la Información Confidencial al solo requerimiento de la Parte Informante. Alternativamente, podrá destruir la Información Confidencial con el consentimiento de la Parte Informante, en cuyo caso deberá probar a ésta tal destrucción.

d) Revelar la Información Confidencial sólo a aquéllas personas cuyo conocimiento sea indispensable para el fin para el cual fue provista. Estas personas tendrán las obligaciones aquí previstas, y la Parte Receptora responderá por ellas.

e) Eliminar toda copia electrónica y/o impresa de la Información Confidencial de cualquiera de los equipos informáticos u otros soportes, salvo autorización de la Parte Informante, una vez finalizado el trabajo.

4. La Parte Receptora estará liberada de su obligación de guardar secreto respecto de la Información Confidencial que:

a) Pruebe a satisfacción de la Parte Informante que era conocida por la Parte Receptora con anterioridad a este trabajo.

b) Sea públicamente conocida sin que ello resulte de un incumplimiento de la Parte Receptora o de un tercero sujeto a una obligación de confidencialidad.

c) Exista una obligación jurídica de dar a conocer la información. En este caso, la Parte Receptora podrá revelar solamente la mínima Información Confidencial necesaria para cumplir con la exigencia que se le impone, siempre que inmediatamente de conocido el requerimiento haya notificado a la Parte Informante tal circunstancia. Este derecho podrá ser ejercido por la Parte Receptora no antes del día inmediato anterior al vencimiento del plazo para proveer esa información, y sólo si subsiste el requerimiento.

5. La Parte Receptora consiente que:

a) La Parte Informante no otorga ninguna garantía respecto de la Información Confidencial, salvo que es de su propiedad y tiene el derecho de revelarla.

b) La Información Confidencial puede contener errores o ser inaplicable al destino para el cual fue elaborada.

c) La Parte Receptora es responsable exclusiva por la evaluación de la Información Confidencial, el uso que a ella otorgue, y los efectos que de esa evaluación o uso resulten.

d) La Información Confidencial tiene un valor estratégico para la Parte Informante.

6. La Parte Informante consiente que:

a) Los documentos entregables y papeles de trabajo serán de acceso exclusivo para los responsables de la Entidad.

b) La Entidad podrá disponer para su uso de todos los entregables, que no incluyen metodología ni softwares utilizados.

## **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.



## 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:

[https://www.owasp.org/index.php/OWASP\\_Mantra\\_-\\_Security\\_Framework](https://www.owasp.org/index.php/OWASP_Mantra_-_Security_Framework)

<http://www.kali.org/>

<http://nmap.org/>

<http://www.nirsoft.net/>

<http://www.tenable.com/products/nessus>

<http://w3af.org/>

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso

(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148

[www.sceu.frba.utn.edu.ar/e-learning](http://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)