Workshop Google Hacking

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Domingo 30 de Noviembre del 2016

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Digital Forensics.

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú y Conferencista en PERUHACK. Cuenta con más de trece años de experiencia en el área y desde hace nueve años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre.

@Alonso_ReYDeS www.facebook.com/alonsoreydes

pe.linkedin.com/in/alonsocaballeroquezada/

Sobre el Workshop

Objetivos:

El objetivo de este workshop es mostrar el poder Google para descubrir cosas verdaderamente sorprendentes. El termino “Google Hacking” implica utilizar los operadores avanzados del motor de búsquedas Google para ubicar cadenas de texto específicas dentro de los resultados de búsqueda. De esta manera es factible encontrar agujeros, fallas, vulnerabilidades o malas configuraciones dentro de todo aquello indexado por Google.

Temario:

- Fundamentos para la Búsqueda con Google
- Operadores Avanzados de Google
- Fundamentos del Hacking con Google
- Ejemplos Prácticos utilizando Google

Fundamentos para la Búsqueda en Google

“Google” es el motor de búsqueda más utilizado en Internet. El orden de los resultados de las búsquedas está definida por un rango de prioridad denominado “PageRank”.

- La página web para la búsqueda en Google
- La página web con los resultados de Google
- Grupos de Google
- Búsquedas de imágenes en Google
- Preferencia de Google
- Herramientas de lenguaje

* http:/www.google.com
* http://groups.google.com
* http://images.google.com
* http://translate.google.com

Reglas de Oro para la Búsqueda en Google

La construcción de consultas en Google en un proceso. Aunque no existe en realidad algo como una búsqueda incorrecta, es completamente posible crear una búsqueda inefectiva.

Aprender la sintaxis de Google es la parte fácil. A continuación se detallan las reglas de oro para realizar búsquedas en Google.

- Las consultas en Google no son sensibles a mayúsculas (Hackers, hAckErs, etc.).
- Utilización de comodines en Google (*).
- Google se reserva el derecho de ignorarlo. (where, how).
- Limite de hasta 32 palabras. (Incluyendo operadores avanzados).

* https://support.google.com/websearch/answer/134479

Búsquedas en Google

La búsqueda en Google es un proceso cuyo objetivo es encontrar información sobre un tópico.

- Búsqueda básica: hacker etico, “curso de hacking”
- Utilizar operadores booleanos y caracteres especiales: AND, OR, NOT, +, |, -.
- Reducción de búsquedas: Modificar la consulta de búsqueda.
- Trabajando con las URLs de Google: Cada consulta de Google puede ser representada por una URL.
- Sintaxis de las URLs: variable1=valor1&variable2=valor2
- Caracteres especiales: Codificación URL “%20”.
- Juntar todo las partes detalladas: Se puede iniciar con una URL, y modificarla conforme se necesite.

* https://www.google.com/advanced_search

Operadores Avanzados

El utilizar estos operadores adecuadamente puede ayudar a obtener exactamente la información buscada.

Sintaxis: operador:termino_de_busqueda

Se pueden aplicar operadores booleanos y caracteres especiales.

- intitle
- allintitle
- inurl
- allinurl
- filetype
- allintext
- site
- link
- cache
- info
- related

Fundamentos de Google Hacking

La información presentada ayuda a comprender las motivaciones de los atacantes, para protegerse a si mismo o a las organizaciones. Todos los conceptos exponen la manera como un Hacker utilizaría Google.

- Anonimato utilizando el “cache”.
- Localizando listados de directorios: intitle:index.of ”parent directory”
- Encontrando directorios específicos: intitle:index.of.admin, intitle:index.of inurl:admin
- Encontrando archivos específicos: filetype:log inurl:ws_ftp.log
- Versión del servidor: intitle:index.of “server at”
- Substituciones incrementales: filetype:xls inurl:1.xls, intitle:index.of inurl:0001
- Caminata de extensiones: .bak, .tmp

Excavando Documentos y Bases de Datos

Recordar Google únicamente excava en lo interpretado o visible de un documento, no en los metadatos.

- Archivos de configuración:
  filetye:ini inurl:ws_ftp, filetype:conf inurl:firewall, inurl:conf OR inurl:config OR inurl:cfg, filetype:cfg mrtg “target[*]” -sample -cvs -example

- Localizar archivos:
  intitle:index.of ws_ftp.ini, filetype:ini inurl:ws_ftp.ini

- Archivos “Logs”:
  filetype:log inurl:log, ext:log log

- Documentos office:
  filetype:xls inurl:passwords.xls, filetype:xls username password email

* http://filext.com/
* www.exploit-db.com/google-dorks/

Excavando Documentos y Bases de Datos

Recientemente se enfoca más la atención en las aplicaciones de bases de datos basadas en web. Especialmente en software front-end con interfaz hacia una base de datos.

- Portales de login:
  login, welcome

- Archivos de apoyo:
  mysql_connect

- Mensajes de error:
  “SQL command not properly ended”

- Volcados de bases de datos:
  “#Dumping data for table”, username, password, “#Dumping data for table” (user | username | pass | password)

* https://www.exploit-db.com/google-hacking-database/

Google para Recolección de Información

Utilizando Google se puede recopilar una gran cantidad de información desde fuentes públicas.

- Direcciones de correo electrónico:
  (reydes at gmail.com, reydes at gmail dot com, reydes@gmail dot com, reydes_at_gmail.com, etc.)

- Personas:
  “Eva Ayllon”, Pedro Suarez Vertiz.

- Usar operadores “Especiales”:
  filetype:doc site:www.******.gob.pe, filetype:pdf site:www.******.edu.pe, password site:pe

- Dominios y subdominios:
  www.routers.com, routers.com -www

- Números de teléfono:
  987654321, +51 987654321.

10 Búsquedas Útiles sobre Seguridad

- site:cnn.com -site:www.cnn.com
- intitle:index.of
- (“for more information” | “not found”) (error | warning), “access denied for user” “using password”
- login | logon
- username | userid | “your username is ”
- password | passcode | “your password is”
- admin | administrator, “administrative login”
- -ext:html -ext:htm -ext:shtml -ext:asp -ext:php
- inurl:temp | inurl:tmp | inurl:backup | inurl:bak
- intranet | help.desk

Servidores Web, Portales de Login, Hardware de Red

- Listado de directorio: server.at “Apache/2,4,12”, “Microsoft-II/7.0 server at”

- Mensajes de error: “Internet Information Services”, intitle:”The page cannot be found”, “The Web site cannot be found”, intitle:”Under construction”, “Apache/2.4.12 Server at” “-intitle:index.of intitle:inf”, “Apache/2.14.12 Server at” -intitle:index.of intitle:error

- Mensajes de error en software de aplicación: “Fatal error: Call to undefined function” -reply -the -next, “ASP.NET_SessionId” “data source =”, intext:”Warning:Failed opening” include_path.

- Portales de Login: “microsoft outlook“ “web access” version,

- Dispositivos de red: “Version Info” “BootVersion” “Internet Settings”, intitle:”switch home page” “cisco systems” “Telnet -to”, intitle:”axis storpoint CD” intitle:”ip address”.

- Reportes de red: intitle:”Welcome to ntop!”

Nombres de Usuario y Contraseñas

- Nombres de Usuario:
  “your username is”, +intext:webalizer +intext:”Total Usernames” +intext:”Usage Statistics for”, filetype:reg HKEY_CURRENT_USER username, intitle:index.of install.log, filetype:log inurl:install.log.

- Contraseñas:
  ext:pwd inurl:_vti_pvt inurl:(Service | authors | administrators). “Your password”, intext:(password | passcode | pass) intext:(username | userid | user).

- Otras cosas a encontrar utilizando Google:
  filetype:ctt messenger, filetype:blt blt +intext:screenname. “This file was generated by Nessus”.

Más Contenidos

Videos de 30 Webinars Gratuitos

http://www.reydes.com/d/?q=videos

Diapositivas utilizadas en los Webinars Gratuitos.

http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1

¡Muchas Gracias!

Workshop Google Hacking

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Domingo 30 de Noviembre del 2016