

ÍNDICE

INTRODUCCIÓN.....	11
¿PARA QUIÉN ES ESTE LIBRO?	11
¿QUIÉN SOY?	12
ESTRUCTURA DEL LIBRO	12
CÓMO OBTENER AYUDA	13
CAPÍTULO 1. FUNDAMENTOS	15
1.1 LINUX.....	15
1.1.1 Terminal de Linux	16
1.1.2 Instalando herramientas.....	18
1.1.3 Interfaz de red	20
1.2 REDES, PROTOCOLOS Y PUERTOS	20
1.2.1 Modelo OSI.....	21
1.2.2 TCP / IP	24
1.2.3 Puertos	27
1.2.4 Firewall	27
1.2.5 Cookies	28
1.3 SEGURIDAD INFORMÁTICA.....	29
1.3.1 Filosofías de hacking.....	29
1.3.2 Seguridad de la información y seguridad informática	31
1.3.3 Cualidades de la seguridad de la información	32
1.3.4 Metodología para mejorar la seguridad de la información	33
1.3.5 Retos en la seguridad de la información.....	35
1.3.6 Ingeniería Social.....	36
1.3.7 Prueba de penetración	41
1.4 FORMAS DE OCULTAR INFORMACIÓN.....	46
1.4.1 Criptografía	46
1.4.2 Cifrado en archivos	47

1.4.3	Esteganografía.....	48
1.4.4	Práctica.....	48
1.5	PREPARACIÓN DEL LABORATORIO	49
1.5.1	Virtualización.....	50
1.5.2	Windows & Macintosh.....	52
1.5.3	Sistemas Operativos	62
1.5.4	Instalando Linux Vulnerable de pruebas	69
1.5.5	Instalando emulador Android	71
1.5.6	Instalando servidor web vulnerable.....	72
CAPÍTULO 2. RECONOCIMIENTO		73
2.1	RECONOCIMIENTO PASIVO.....	73
2.1.1	Información de dominios	74
2.1.2	OSINT - Obtener correos, números, nombres y otras cosas.....	74
2.1.3	Maltego	80
2.1.4	El buscador de los hackers	84
2.1.5	¿Has sido hackeado?	88
2.1.6	Encontrar con que están hechas las páginas web.....	89
2.1.7	Encontrar versiones anteriores de páginas web.....	89
2.1.8	Encontrar ubicaciones por medio de una foto	90
2.1.9	Entrar a cámaras de seguridad.....	91
2.1.10	Rastreo de IP e información en email.....	92
2.1.11	Reconocimiento en red pasivo	94
2.1.12	WireShark - Análisis de paquetes	94
2.2	RECONOCIMIENTO ACTIVO.....	97
2.2.1	Nmap.....	98
2.2.2	OSINT + Reconocimiento Activo - Obtener información con una sola herramienta.....	104
CAPÍTULO 3. ANÁLISIS DE VULNERABILIDADES.....		107
3.1	CVES Y CWES	107
3.2	OWASP.....	111
3.2.1	OWASP top 10	111
3.3	ANALIZADORES DE VULNERABILIDADES	115
3.3.1	Nessus	115
3.3.2	Acunetix	121
3.3.3	Otros analizadores de vulnerabilidades.....	125
3.3.4	Análisis a páginas WordPress.....	127
3.3.5	Análisis OWASP a páginas web	129
CAPÍTULO 4. EXPLOTACIÓN.....		133
4.1	ATAQUES FUERA DE LA RED LOCAL DESDE LA NUBE.....	133
4.1.1	Amazon Web Services.....	134
4.2	PHISHING	154
4.2.1	Robo de credenciales de redes sociales.....	154

4.2.2	Robo de credenciales de redes sociales 2	157
4.2.3	Dominios maliciosos	160
4.2.4	Email Spoofing.....	161
43	METASPLOIT.....	165
4.3.1	Estructura de la herramienta.....	166
4.3.2	Palabras reservadas	167
4.3.3	Armitage.....	168
44	TROYANOS PARA ACCESO REMOTO	169
4.4.1	Metasploit.....	170
4.4.2	Hacking Windows.....	171
4.4.3	Hacking Android.....	174
4.4.4	Obteniendo info (cámara, archivos, micrófonos, GPS, etc)	180
4.4.5	Archivos Office infectados.....	188
45	ATAQUES POR MEDIO DEL NAVEGADOR	206
4.5.1	Malware en página web por medio de JS	207
46	ATAQUES WIFI.....	215
4.6.1	Ataques de interceptación de información en la red (MITM)	215
4.6.2	Protocolo ARP.....	216
4.6.3	Envenenamiento ARP	217
4.6.4	Interpretando paquetes en WireShark.....	222
4.6.5	Interceptando Imágenes.....	222
4.6.6	Interceptando URLs	223
4.6.7	Interceptando credenciales no encriptadas	224
47	EXPLOITS	224
4.7.1	Base de datos de Exploits.....	224
4.7.2	Inyección SQL	227
4.7.3	Cross Site Scripting (XSS).....	240
4.7.4	Exploits de Metasploit.....	246
4.7.5	Hacking Windows con Exploits	246

CAPÍTULO 5. POST- EXPLOTACIÓN 253

5.1	POST-RECONOCIMIENTO LOCAL	253
5.1.1	¿Qué sistema es?	254
5.1.2	¿Qué usuario es?	254
5.1.3	Procesos.....	254
5.1.4	Dirección IP	255
5.2	ATAQUES AL OBJETIVO.....	256
5.2.1	Descarga de archivos.....	256
5.2.2	Sniffer.....	258
5.2.3	Robo de credenciales de navegadores y otros programas remotamente 260	
5.3	DESACTIVAR ANTIVIRUS.....	262
5.4	ELEVACIÓN DE PRIVILEGIOS	262
5.4.1	Getsystem.....	262

5.4.2	Elevación privilegios Android.....	263
5.5	PERSISTENCIA	263
5.5.1	Windows.....	263
5.6	PIVOTEO - ATACANDO DESDE SISTEMA COMPROMETIDO	266
5.6.1	Reconocimiento.....	266
5.6.2	Interceptando paquetes en redes externas.....	267
5.6.3	Atacando a otro sistema	268
5.7	HACKEANDO WHATSAPP.....	269
CAPÍTULO 6. FORENSE		277
6.1	METODOLOGÍA.....	277
6.2	PRÁCTICA - WINDOWS.....	278
CAPÍTULO 7. REPORTAJE		281
7.1	METODOLOGÍA.....	281
7.1.1	Reporte Ejecutivo.....	282
7.1.2	Reporte Técnico	284
CAPÍTULO 8. ANONIMATO, DARK WEB Y DEEP WEB		287
8.1	ANONIMATO.....	287
8.2	DEEP WEB & DARK WEB.....	290
8.2.1	Deep Web.....	290
8.2.2	Dark Web.....	291
CAPÍTULO 9. CASOS.....		293
9.1	ROBO BANCARIO	293
9.1.1	Mitigación.....	295
9.2	ROBO A LABORATORIO FARMACÉUTICO (ESPIONAJE INDUSTRIAL)....	296
9.2.1	Mitigación	297
9.3	FILTRACIÓN DE CADENA DE COMIDA RÁPIDA (ESPIONAJE INDUSTRIAL)	297
9.3.1	Mitigación	298
CAPÍTULO 10. CONCLUSIÓN		299

INTRODUCCIÓN

Este libro está diseñado para ser una guía e introducirte al área de seguridad informática, trabajando no solo desde el punto de vista técnico, si no también, usando las metodologías adecuadas para realizar pruebas de penetración o auditorías de seguridad en distintos casos. Lo más importante de este libro, será como entendiendo la metodología y su uso de manera y avanzaremos sin límites.

Este libro basado en la certificación **G.H.O.S.T** (*Grey Hat Offensive Security Technician*), tiene todo lo que necesita una persona para adentrarse al mundo del hacking por medio de técnicas utilizadas por un **sombrero gris**, para cuando termines el libro dominarás el tema, lo que significa que aprenderás cómo atacan los cibercriminales, para poder proteger a una empresa adecuadamente de ellos.

¿PARA QUIÉN ES ESTE LIBRO?

Este libro está hecho para el que quiera convertirse en un hacker profesional, te llevará de la mano para que te conviertas en un experto en el área de seguridad informática *sin importar si tienes conocimientos avanzados de informática, o si eres principiante*.

También, si tienes interés en hacer alguna certificación de ciberseguridad como **G.H.O.S.T** u otra como el **CEH**, este libro te dará las bases necesarias en conocimientos prácticos y técnicos para poder aprobar estas certificaciones, siempre y cuando realices todas las prácticas en el libro y estudies adecuadamente las técnicas y fundamentos mencionados aquí.

¿QUIÉN SOY?

Mi nombre es Pablo Gutiérrez, soy consultor en seguridad informática, hacker profesional en el área del pentesting, *CEO* de **WSH**, *CSO* de la empresa de seguridad anti-espionaje **Privasee**, conferencista, instructor y creador de la certificación **G.H.O.S.T**, actualmente la más completa y actualizada certificación de hacking con enfoque práctico, y del **Hacking Day**, el mejor curso de introducción al hacking, y estoy certificado en **CEH** por la empresa EC-Council.



Adicionalmente, si deseas tomar alguna **certificación** o **curso**, actualizarte con noticias y nuevas cosas en nuestro **blog**, o requieres algún **servicio profesional de ciberseguridad**, puedes encontrarnos/contactarnos en **whitesuithacking.com**, **fb.com/whitesuithacking**, o **fb.com/pablogtz.ciberseguridad**.

ESTRUCTURA DEL LIBRO

El libro está estructurado de manera muy similar a nuestro curso **G.H.O.S.T**, en base a la metodología internacional de prueba de penetración.

Esta metodología la llevaremos por pasos, y aunque para muchos que han visto y creen que el hacking es como en muchas películas (rápidamente teclear el código para entrar por la puerta trasera del sistema) en la realidad hacerlo toma tiempo y paciencia.

La metodología que usamos es muy similar al “método científico”. Esencialmente obtenemos la información, se analiza y luego atacamos, y en base al alcance del ataque, reportará, dependiendo de tu objetivo, adicionalmente, se verá un poco de análisis forense de forma superficial.

El libro consta de 9 **partes**:

1. **Teoría/fundamentos:** Fundamentos que necesitas para el resto del libro
2. **Reconocimiento:** Metodologías para obtener información del objetivo
3. **Análisis de vulnerabilidades:** Como analizar la información para encontrar un punto débil
4. **Explotación:** Formas de ataque
5. **Post-explotación** Que hacer luego que se obtiene el acceso
6. **Reportaje:** Cómo se debe reportar la información obtenida a un cliente y cómo debe ser estructurado un reporte final
7. **Análisis forense:** Los principios del análisis forense, pero debe considerarse que esto se verá superficialmente
8. **Anonimato:** Como mantener tu identidad y presencia oculta en la red.
9. **Casos:** Casos reales de ataques de cibercriminales y pruebas de penetración.

En cada una de estas secciones se expondrá cómo funciona cada uno de los pasos de la metodología y las distintas herramientas para obtener los resultados que se quieren. Se explica cómo se utiliza la herramienta, su funcionamiento, y en qué casos usar y en cuáles no, y se menciona un caso real para que se entienda la importancia de esa parte de la metodología.

Adicionalmente, subí una página donde están todas las herramientas y sistemas que utilizamos en el libro, además de algunos videotutoriales en

<https://whitesuithacking.com/ligaenlibro>

Recomiendo AMPLIAMENTE descargar el material ahí ANTES de empezar con las practicas, ya que el Kali normal no tiene muchas de las herramientas mencionadas en este libro.

CÓMO OBTENER AYUDA

Tenemos una comunidad en **Telegram** en la que puedes entrar y preguntar cualquier duda o problema de este libro, la liga para entrar es **ligaenlibro**, debes tener Telegram instalado para que la liga funcione.

