CEH v10 NOTES

# Cyber Quotient

## Progressive Assessment

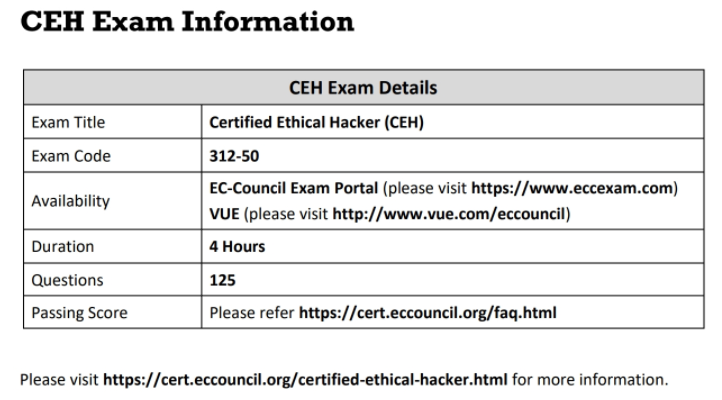
Total Topics 67

Topics Passed 6

Introduction to Ethical Hacking 5/5

Repasar Information Security Controls y Ethical Hacking Concepts and Scope

Footprinting and Reconnaissance 1/3



# Module 01: Introduction to Ethical Hacking

Hack Value 🡪 cómo de valiosa es la información que vamos a proteger

Payload 🡪 lo que queremos hacer con un exploit

Daisy Chaining 🡪 utilizar una información obtenida para acceder a otros recursos

Doxing 🡪 buscar toda la información posible en línea acerca de un obetivo (doxear)

Elementos de la seguridad de la información:

* Confidencialidad
* Integridad
* Disponibilidad
* Autenticidad
* No repudio

Ataques:

**Attacks = Motive (Goal) + Method + Vulnerability**

Command and Control 🡪 máquina que crea el hacker que manda instrucciones a la máquina víctima

**Pregunta examen: ¿Quién es el atacante más peligroso para una organización? Un Insider Attack (empleado descontento)**

Script Kiddies 🡪 Hacker que comienza utilizando las herramientas de otros, normalmente todos empiezan siendo script kiddies hasta que eres capaz de crear tus propias herramientas

Fases del hacking:

1. Reconocimiento
   1. Pasivo: busca toda la información posible en fuentes abiertas (OSINT) sin interacción directa con el objetivo (buscar noticias)
   2. Activo: busca toda la información posible interactuando con el objetivo (vamos al sitio web de la empresa)
2. Escaneo: fase de preataque
   1. Escaneo de puertos
   2. Extraer información: estado de las máquinas, de qué tipo son…
3. Ganar acceso: busca controlar la máquina
   1. Escalar privilegios
4. Mantener acceso
5. Borrar las huellas
   1. Alterar logs, borrar ciertos archivos

Pentesting: se sigue una metodología paso a paso y se realiza la explotación de una vulnerabilidad para recabar informaficón, de este modo podemos decir con certeza si una vulnerabilidad encontrada es explotable o no.

Security Testing Methodology (todas son libres):

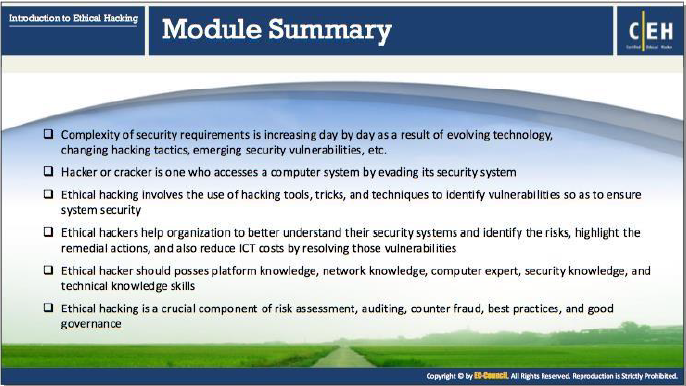
* OWASP
* OSSTMM
* ISSAF
* EC-Council LPT Methodology

PCI DSS: Estandar de seguridad para tarjetas de crédito.

ISO 27001

HIPAA: orientado a empresas relacionadas con la salud.

SOX: orientado a las compañías financieras, persigue normalmente crímenes de cuello blanco.



Shrink Wrap code attack 🡪 es sólo el acto de explotar agujeros en software sin parches o mal configurado. Para utilizar el término de otra manera, una "vulnerabilidad de Shrink Wrap" sería aquella que sólo debería verse en un producto inmediatamente después de su instalación inicial. Por ejemplo, un error de software presente en la versión original de un producto, para el cual el vendedor ha publicado una actualización pero el administrador del sistema no la ha parcheado.

Piggybacking 🡪 es una técnica de transmisión de datos bidireccional en la capa de enlace de datos (Modelo OSI). Con esta técnica, en vez de enviar ACK en un paquete individual, éste es incluido dentro del próximo paquete a enviar. El receptor puede atascar el servicio si no tiene nada que enviar. Esto se puede solucionar si el receptor añade una contador regresivo (timer) que se activa cuando se recibe un paquete. Si el timer finaliza sin que se hayan enviado datos, el receptor enviará un paquete ACK. Por otra parte el emisor también crea su propio timer, si el timer finaliza antes de recibir un paquete ACK, el emisor volverá a enviar el paquete.

Hacktivists 🡪 Hackers que irrumpen en los ordenadores del gobierno o de las empresas como acto de protesta o para aumentar la conciencia.

Cyber terrorists 🡪 Individuos motivados por creencias religiosas o políticas para crear miedo a una interrupción a gran escala.

Script kiddies 🡪 Hackers no cualificados que comprometen los sistemas ejecutando scripts, herramientas y software desarrollados por otros hackers.

Suicide hackers 🡪 Hackers que tienen como objetivo derribar infraestructuras críticas y no se preocupan por ser atrapados y enfrentarse a penas de cárcel o cualquier otro tipo de castigo.

OWASP es el Proyecto de Seguridad de Aplicaciones Web Abiertas, que es un proyecto de seguridad de aplicaciones de código abierto que ayuda a las organizaciones a comprar, desarrollar y mantener herramientas de software, aplicaciones de software y documentación basada en el conocimiento para la seguridad de las aplicaciones Web. Proporciona un conjunto de herramientas y una base de conocimientos, que ayudan a proteger las aplicaciones y servicios de la Web. Es beneficioso para los arquitectos de sistemas, desarrolladores, vendedores, consumidores y profesionales de la seguridad que podrían trabajar en el diseño, desarrollo, despliegue y prueba de la seguridad de las aplicaciones y servicios Web.

OSSTMM es el Manual de Metodología de Pruebas de Seguridad de Código Abierto, compilado por Pete Herzog. Es una metodología revisada por pares para realizar pruebas de seguridad de alta calidad como pruebas de metodología: controles de datos, niveles de control de fraude e ingeniería social, redes de computadoras, dispositivos inalámbricos, dispositivos móviles, controles de acceso de seguridad física y varios procesos de seguridad. El OSSTMM es un conjunto estándar de pruebas de penetración para lograr métricas de seguridad. Se considera un estándar de facto para el nivel más alto de pruebas, y asegura una alta consistencia y una precisión notable.

Los controles de seguridad se clasifican de la siguiente manera:

? Controles preventivos - Evitan que ocurra un incidente. Por ejemplo, guardia de seguridad, autenticación de tarjetas inteligentes, etc.

? Controles de detección - Identificar y caracterizar un incidente en curso. Por ejemplo, pista de auditoría, supervisión del sistema, etc.

? Controles correctivos - Limitar el alcance de cualquier daño causado por el incidente. Por ejemplo, la política de seguridad, el plan de continuidad de las operaciones, etc.

# Module 2: Footprinting and Reconnaissance

Footprinting 🡪 recabar toda la información posible de un objetivo, normalmente hacemos búsquedas en fuentes abiertas (OSINT). Buscamos información sobre la organización, buscamos a nivel de red como dominios, registros de DNS, IPs, Whois…, buscaremos también información del sistema.

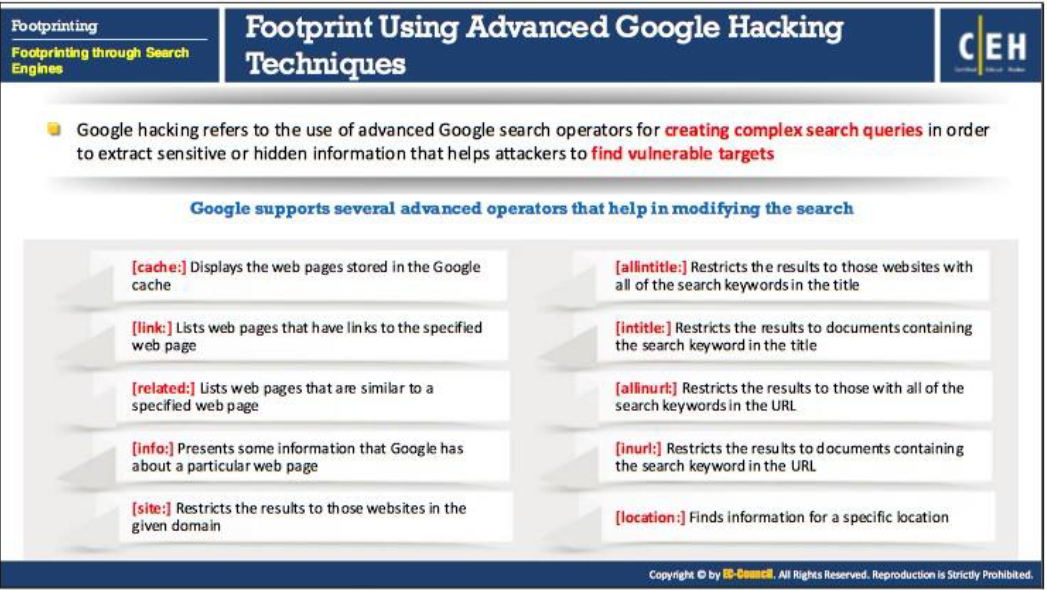
Normalmente utilizamos motores de búsquedas, Google, Bing, DuckduckGo…, tendrán información sobre la surface web.

Google Hacking:

cache:eltiempo.com 🡪 nos trae la versión en cache de esta página, no estamos llegando hasta el servidor de eltiempo.com. No deja huella en el servidor.

inurl:eccouncil 🡪 busco todos los sitios en los que su url tiene una palabra puntual.

site:https://www.eccouncil.org/ ext:pdf 🡪 busca todos los archivos pdf contenidos en la url indicada. Se pueden buscar archivos de configuración .conf o archivos .bak



Google Hacking Database (GHDB) 🡪 patrones de búsqueda muy útiles, se encuentra en la web de Exploit Database.

Herramienta Netcraft 🡪 netcraft.com, nos permite saber un poco sobre la tecnología de un sitio.

Google Maps 🡪 para buscar la posición geográfica del objetivo.

Búsqueda de personas en redes sociales. Podemos usar **intelius.com, beenverfied.com, spokeo.com.**

**knowem.com 🡪** me permite buscar por nombre de usuario

Para buscar información sobre el sistema operativo:

shodan.io 🡪 como un Google pero para servicios, ssoo…

Web Spiders 🡪 buscan información relevante dentro de un sitio web, por ejemplo busca direcciones de correo electrónico. Uno de los mejores es **Web Data Extractor**.

archive.org 🡪 puedes ver el contenido de una página en momentos pasados.

Herramienta Exiftool 🡪 para extraer metadatos de imágenes.

Whois 🡪 comando que nos permite recabar información



whatismyipaddress.com 🡪 buena herramienta para geolocalizar IPs, trackear emails…

tools.dnsstuff.com

dig 🡪 herramienta por cli nos entrega información de registros

dig mx certifiedhacker.com 🡪 nos da info sobre el registro de email

Cómo ubicar el rango de máquinas 🡪 buscar los registros de DNS y cruzarlo con shodan. Por ejemplo, si encuentro el registro A de DNS, con la dirección IP busco ese rango en shodan.

dnsmap 🡪 herramienta por cli para buscar subdominios, se le puede proporcionar un diccionario de palabras.

netcraft 🡪 herramienta par subdominios entre otras cosas

Footprinting a través de Ingenieria Social:

Eavesdropping 🡪 escucha no autorizada.

Shoulder Surfing 🡪 mirar por encima del hombro lo que la persona está introduciendo.

Dumpster Diving 🡪 buscar en la papelera algún papel interesante.

Maltego 🡪 herramienta muy buena para búsqueda de personas.

FOCA 🡪 entregas un dominio y busca los metadatos sobre todos los documentos que encuentre.

OSRFramework 🡪 herramienta que busca en OSINT (Open Source INTelligence).

theHarvester 🡪 herramienta que nos permite detectar información de dominios, emails, entre muchas más cosas. Es un script de Python.

github theharvester para descargar la herramienta

git clone <pongo la url>

./theHarvester.py -d certifiedhacker.com -b all