CPHE 2020

DESCRIPCIÓN

Objetivos

Curso completo de Hacking Ético en el que aprenderás a detectar vulnerabilidades en sistemas informáticos, apoyándote en el uso de herramientas diseñadas para el ataque, así como el despliegue de defensas frente a ataques de forma eminentemente práctica.

PROGRAMA

1. Introducción al Hacking Ético

En este módulo se presenta el curso, se habla del hacking ético y de las auditorías de ciberseguridad; se introduce la arquitectura de redes, las distribuciones Linux y los comandos más utilizados y se instala la herramienta fundamental de este curso: Kali Linux.

Vídeos:

- Introducción al CPHE
- Introducción al Hacking Ético I
- Introducción al Hacking Ético II
- Redes y Linux I
- Redes y Linux II

2. Recolección de Información

Módulo dedicado a la recolección de información de manera activa y pasiva, el uso de las principales herramientas; el anonimato, el escaneo de puertos y servicios con Nmap, la ocasión de firewalls y las principales herramientas de análisis de vulnerabilidades como Acunetix, Nessus, Nikto, Cmsmap, Wpscan, Joomscan, Zap o Burpsuite-pro.

Vídeos:

- Recolección de Información I
- Recolección de Información II
- Recolección de Información III
- Anonimato
- Escaneo de vulnerabilidades I
- Escaneo de vulnerabilidades II
- Escaneo de vulnerabilidades III
- Escaneo de vulnerabilidades IV
- Escaneo de vulnerabilidades V
- Escaneo de vulnerabilidades VI

3. Explotación y Postexplotación

Módulo dedicado a la búsqueda de exploits, realización de ataques manuales y automatizados, uso de metasploit, ataques directos e inversos, pivoting, escalada de privilegios, backdoors y extracción de información.

Vídeos:

- Explotación I
- Explotación II
- Explotación III
- Explotación IV
- Explotación V

4. Password Cracking y Auditorías WiFi

Módulo que analiza los diferentes métodos de password guessing y password cracking (ataques online y offline, hashcat, hydra, ophcrack, metasploit auxiliares, john, cracking online, etc) así como ataques a redes wifi (aircrack, airgeddong, denegación de servicios DoS, desautenticación, gemelo malvado, puntos falsos de acceso y MitM).

Vídeos:

- Password Guessing
- Password Cracking I
- Password Cracking II
- Password Cracking III
- Password Cracking IV
- Wifi I
- Wifi II
- Wifi III

5. Malware

En este módulo aprenderás a configurar un troyano, el uso de crypters, herramientas online para obtener crypters, modding, evaluar el malware o diferentes métodos de infección.

Vídeos:

- Malware I
- Malware II
- Malware III

6. Forensia y Auditorías a Móviles

Módulo dedicado a la informática forense y a las auditorías de dispositivos móviles. En la parte de forensia veremos una introducción a las evidencias digitales, análisis de datos, correo electrónico, forensia en redes y geo, móviles y la elaboración de informes de forensia.
En la parte de móviles veremos la recolección de información, escaneo de puertos y servicios, rooteo y pruebas de pentesting para móviles.

Vídeos:

- Introducción a la forensia en móviles
- Volatility
- Móviles I
- Móviles II
- Móviles III

7. Auditorías Web

Módulo dedicado al hacking web, en el que aprenderás qué tipo de pruebas se realizan sobre las webs y aplicaciones web, qué tipo de vulnerabilidades podemos encontrar, las herramientas más utilizadas y las fases de un ataque web.

Vídeos:

- Hacking Web I
- Hacking Web II
- Hacking Web III