FUNDACIÓN ADECCO

Temario Ciberseguridad y Hacking Ético

Curso de 230 horas

FUNDACIÓN ADECCO

Temario Ciberseguridad y Hacking Ético

1 REDES y SISTEMAS OPERATIVOS

- **Introducción a las Redes Informáticas**

1.1. Introducción 1.2. Tipos de redes 1.3. Sistemas operativos de red

- **Ethernet y Canales de Comunicación**

2.1. Canales de comunicación 2.2. Cableado 2.3. Instalaciones

- **Direccionamiento IP**

3.1. Fundamentos3.2. Subredes3.3. Redes privadas3.4. IPv6

- **Modelo OSI y TCP/IP**

4.1. Modelo OSI y sus capas4.2. Modelo TCP/IP y sus capas

- **Utilidades TCP/IP**

5.1. NET5.2. PING5.3. NETstat5.4. ARP5.5. Telnet

- **Windows Server**

6.1. Instalación de diferentes versiones (2003-2016)

- **Sistemas Linux**

7.1. Características 7.2. Sistemas de ficheros 7.3. Fundamentos 7.4. Usuarios y grupos 7.5. Configuración de red

- **Modos de Acceso a Internet**

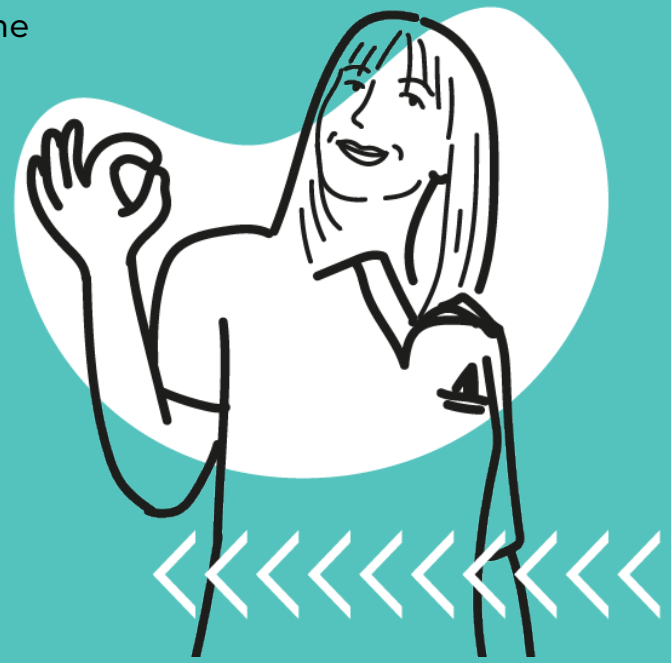
8.1. Modulación digital 8.2. Digital Subscriber Line (DSL)

- **Redes WAN**

9.1. Arquitectura 9.2. Dispositivos 9.3. Políticas 9.4. Servidores

- **Packet Tracer**

10.1. Instalación y uso



2 Introducción a la Ciberseguridad

- **Entorno Linux**

12.1. Distribuciones (Distros)12.2. Sistemas12.3. Sistemas de ficheros12.4. Rutas y formato de archivos

- **Tipos de Auditorías**

13.1. Por tipo13.2. Por ámbito

- **Pentesting**

14.1. Fases explicadas

- **Virtualización e Instalación de Laboratorios**

15.1. Tipos de hypervisores15.2. Tipos de archivos de instalación

- **Bash Scripting**

16.1. Completo básico

- **Herramientas Básicas**

17.1. Whois17.2. Ping17.3. Tracert17.4. Nslookup17.5. Dig17.6. Google

- **Metadatos**

18.1. Tipos18.2. FOCA18.3. ExifTool

- **OSINT (Open Source Intelligence)**

19.1. Maltego 19.2. TheHarvester 19.3. Dmitry 19.4. Dorks 19.5. CEWL 19.6. Redes sociales 19.7. Filtraciones 19.8. IoT

- **Descubrimiento de Máquinas**

- **Análisis de Puertos**

21.1. Herramientas21.2. Tipos de escaneo

- **Análisis de Vulnerabilidades**

22.1. Clasificación de vulnerabilidades22.2. Herramientas de escaneo

- **Metasploit**

23.1. Websploit23.2. Searchsploit

- **CMS (Content Management Systems)**

24.1. JoomScan24.2. WPScan

- **Ataques a Servicios**

25.1. SSH25.2. VNC25.3. SMB25.4. FTP

- **Autenticación**

26.1. LM26.2. NTLM26.3. Linux

- **Diccionarios Disponibles**

27.1. RockYou 27.2. Big WPA List 27.3. CrackStation 27.4. Diccionarios por idiomas

- **Generación de Diccionarios**

28.1. Crunch 28.2. CEWL 28.3. CUPP

- **Ataques por Fuerza Bruta**

29.1. Hydra 29.2. Medusa 29.3. Hashcat 29.4. John the Ripper

- **Ataques DoS y DDoS**

- **Red Tor**

31.1. Arquitectura 31.2. Tor 31.3. HexChat 31.4. ProxyChains 31.5. TorGhost

- **Red I2P**

- **Cuentas de Correo Temporales**

- **VPN**

- **Métodos de Evasión**

35.1. Shellter 35.2. MSFvenom 35.3. TheFatRat 35.4. Evasión manual

- **Ataques WiFi**

36.1. Conceptos básicos 36.2. Funcionamiento 36.3. Tipos de ataques 36.4. Automatización 36.5. Portales cautivos

- **Análisis de Tráfico**

37.1. Wireshark 37.2. Ettercap 37.3. Tshark

- **Envenenamiento de Tráfico**

38.1. MITM6 38.2. EvilFOCA

- **Ingeniería Social**

39.1. Psicología 39.2. Manipulación 39.3. Contacto humano real 39.4. Técnicas de ingeniería social 39.5. Contramedidas

- **Hacking Web**

40.1. Ejecución de código remoto 40.2. Inyección SQL40.3. XSS40.4. LFI/RFI40.5. Webshells

- **Pentesting en Dispositivos Móviles**

41.1. Técnicas 41.2. Pasos básicos 41.3. Creación de APK maliciosa 41.4. Análisis de APKs

- **Postexplotación**

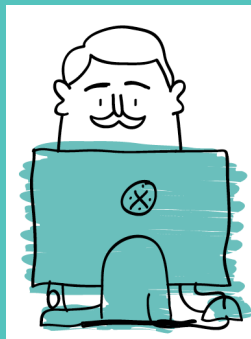
42.1. Métodos pasivos y activos 42.2. Escalada de privilegios 42.3. Persistencia 42.4. Pivoting

- **Ataques a Active Directory**

43.1. NetExec

- **Documentación en Auditorías**

44.1. Contrato 44.2. Tipos de informes



FUNDACIÓN ADECCO

Empleo para todas las personas