

Hacking ético desde CERO

Guía para dominar las herramientas y desarrollar criterio experto

180 sesiones de una hora + especialización progresiva

Linux + redes + herramientas de hacking + defensa + IA

Una ruta desde los fundamentos hasta el uso avanzado de herramientas de hacking ético. Comprender, practicar, interpretar resultados y verificar hallazgos.

Alcance realista. Las 180 horas construyen fundamentos y una primera práctica avanzada. No equivalen a dominar todas las especialidades. La experiencia experta se desarrolla después mediante ciclos de especialización, proyectos nuevos, revisión y trabajo autorizado.

Desde cero. No se requieren conocimientos previos. Empieza por preparar Kali en VirtualBox, comprender la terminal y aprender redes. Avanza hacia análisis de tráfico, evaluación de servicios, seguridad web y automatización en laboratorios autorizados.

Entregables. Una bitácora, una red CCNA, scripts explicables, informes de laboratorio, una investigación defensiva y un proyecto integral.

Cómo estudiar cada hora

00-05 min: recuperar de memoria lo aprendido y definir el objetivo.

05-20 min: concepto, ejemplo y lectura de una fuente primaria.

20-45 min: práctica. Antes de cada acción, predice el resultado.

45-55 min: explicar la salida, comprobar evidencia y corregir errores.

55-60 min: registrar aprendizaje y responder tres preguntas sin ayuda.

Sesiones de proyecto o evaluación: 5 min de objetivo, 40 min de trabajo, 10 min de verificación y 5 min de bitácora. Si una práctica no cabe, continúa en otra sesión de una hora; no sacrifiques comprensión por cumplir el calendario.

Bitácora mínima: fecha, objetivo, concepto, hipótesis, comando y significado, resultado, evidencia, conclusión, dudas y siguiente prueba.

Uso de IA: pedir explicaciones y pistas antes de soluciones. Verificar comandos y fuentes. Repetir al final sin asistencia. Nunca incluir claves reales ni datos privados.

Prompt para iniciar una sesión

"Hoy hacemos la sesión [número y título]. Enséñame desde cero y relaciónala con los fundamentos de redes. Respeta una hora: 5 de repaso, 15 de teoría, 25 de práctica, 10 de explicación y 5 de bitácora. Explica cada comando antes de ejecutarlo. Pregunta mi predicción y da pistas antes de la solución. Usa mi laboratorio y termina evaluando lo que puedo explicar sin IA."

Laboratorio: Kali en NAT para actualizaciones. Para objetivos vulnerables, Kali y objetivo en una red interna compartida, sin puente ni puertos publicados. Desconecta adaptadores externos del objetivo. NAT no es un aislamiento total: puede permitir alcanzar redes accesibles desde el anfitrión. Guarda instantáneas y copias; usa datos ficticios.

Sin gasto obligatorio: prioriza herramientas locales y recursos abiertos. Cloud se estudia con diseños y simulaciones; AD puede estudiarse primero con registros y diagramas. No necesitas comprar hardware ni contratar nube. Ajusta VMs a la RAM disponible.

Mapa del programa

001-010 / Laboratorio y método

011-020 / Computación y Linux básico

021-030 / Redes I: fundamentos CCNA

031-040 / Redes II: servicios y diagnóstico

041-050 / Redes III: acceso y protección CCNA

051-060 / Linux: administración y protección

061-070 / Principios, riesgo y criptografía

071-080 / Python, Bash y Git

081-090 / Web: cómo funciona una aplicación

091-100 / Seguridad web: laboratorios guiados

101-110 / Evaluación de seguridad y reportes

111-120 / Defensa y respuesta a incidentes

121-130 / Windows y Active Directory

131-140 / Cloud, contenedores y desarrollo seguro

141-150 / Seguridad de IA y agentes

151-160 / Profundización técnica

161-170 / Proyecto integral

171-180 / Especialización: primer ciclo

001-120: fundamentos y práctica inicial. 121-160: identidad, cloud, IA y profundización. 161-180: integración y primer ciclo de especialización.

Ritmo orientativo

3 sesiones por semana: 60 semanas para el programa nominal.

5 sesiones por semana: 36 semanas.

7 sesiones por semana: unas 26 semanas.

Los tiempos excluyen descansos, descargas, repeticiones y trabajo adicional. Mantén CCNA como curso principal de redes: estas sesiones complementan su teoría con observación y seguridad, sin sustituir todo su temario ni su preparación de examen.

Repaso: al iniciar cada sesión, recupera un concepto reciente y uno antiguo. Cada diez sesiones, repite una tarea previa con una variante. Si necesitas recuperar contenido, añade una sesión y conserva la numeración del plan original.

Laboratorio y método

Competencia: Instalar, recuperar y describir tu entorno.

Entorno y fuentes: VirtualBox y documentación de Kali

Sesión	Concepto y evidencia de aprendizaje
001	Alcance y ética Redacta reglas: objetivos propios, permisos, límites y evidencias.
002	Anfitrión e invitado Dibuja Windows, VirtualBox, Kali y el disco virtual.
003	Arquitectura e imágenes Distingue ISO, VDI, VBOX, x86-64 y ARM64.
004	Recursos virtuales Revisa RAM, CPU y almacenamiento sin agotar Windows.
005	Red virtual Compara NAT, puente, interna y solo anfitrión; dibuja sus accesos.
006	Teclado y usuarios Configura distribución, cambia contraseña y prueba signos.
007	Paquetes y repositorios Explica apt update, full-upgrade y firmas; actualiza Kali.
008	Instantáneas y copias Crea un archivo, guarda un estado y ensaya recuperación.
009	Bitácora e IA Registra un error, hipótesis, prueba y conclusión sin datos sensibles.
010	Evaluación inicial Recupera el laboratorio y explica configuración sin ayuda.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Computación y Linux básico

Competencia: Usar archivos, terminal y procesos con criterio.

Entorno y fuentes: Kali, manuales man y Bandit

Sesión	Concepto y evidencia de aprendizaje
011	Bits y representación Convierte números pequeños entre binario, decimal y hexadecimal.
012	Sistema operativo Relaciona kernel, aplicación, proceso, memoria y disco.
013	Rutas y directorios Practica pwd, ls y cd; identifica rutas absolutas y relativas.
014	Operaciones de archivos Crea, copia y mueve archivos; elimina solo archivos de práctica.
015	Lectura y búsqueda Usa less, find y grep para localizar datos ficticios.
016	Entrada y salida Construye tuberías y redirecciones sin sobrescribir originales.
017	Permisos Compara lectura, escritura y ejecución en archivos y directorios.
018	Usuarios y sudo Crea un usuario de prueba y demuestra mínimo privilegio.
019	Procesos y recursos Identifica procesos con ps y top; interpreta consumo.
020	Evaluación Linux Completa tareas de archivos y permisos sin instrucciones copiadas.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Redes I: fundamentos CCNA

Competencia: Entender cómo viajan datos en una red local.

Entorno y fuentes: Curso CCNA, Packet Tracer y Wireshark

Sesión	Concepto y evidencia de aprendizaje
021	OSI y TCP/IP Ubica protocolos en capas y explica encapsulación.
022	Ethernet y MAC Identifica trama, interfaz, dirección MAC y dominio de broadcast.
023	Switch y router Construye dos segmentos y explica sus diferencias.
024	IPv4 Distingue direcciones privadas, públicas, loopback y link-local.
025	Máscara y CIDR Calcula red y broadcast de ejemplos /24, /26 y /28.
026	Subredes Divide una red para tres grupos con necesidades distintas.
027	ARP Observa resolución IP-MAC en una captura del laboratorio.
028	TCP y UDP Compara conexión, entrega, orden y aplicaciones típicas.
029	Puertos y sockets Relaciona IP, puerto, proceso y servicio con ss.
030	Evaluación redes I Explica un paquete y resuelve subredes con justificación.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Conexión CCNA: lleva dudas y capturas a tu lección de redes; confirma conceptos con el temario oficial y tu curso.

Redes II: servicios y diagnóstico

Competencia: Separar problemas de enlace, rutas y DNS.

Entorno y fuentes: CCNA, terminal y Wireshark

Sesión	Concepto y evidencia de aprendizaje
031	Gateway y rutas Interpreta ip route y decide la siguiente salida.
032	DHCP Observa asignación de IP, máscara, gateway y DNS.
033	DNS Consulta getent y dig; distingue A, AAAA, CNAME y caché.
034	El error de dedo Compara resultados de nombres sin visitar dominios desconocidos.
035	ICMP y ping Interpreta pérdida, latencia y límites de la prueba.
036	NAT y PAT Dibuja traducciones de direcciones y puertos.
037	IPv6 Identifica global, link-local, prefijos y descubrimiento de vecinos.
038	HTTP y HTTPS Observa petición, respuesta, puerto y protección TLS.
039	Diagnóstico por capas Resuelve tres fallos preparados: IP, ruta y DNS.
040	Evaluación redes II Documenta un diagnóstico con hipótesis y evidencia.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Conexión CCNA: lleva dudas y capturas a tu lección de redes; confirma conceptos con el temario oficial y tu curso.

Redes III: acceso y protección CCNA

Competencia: Configurar y comprobar segmentación y acceso.

Entorno y fuentes: Curso CCNA y Packet Tracer

Sesión	Concepto y evidencia de aprendizaje
041	VLAN Separa usuarios y administración en una topología simulada.
042	Troncales Explica etiquetas, VLAN nativa y tráfico entre switches.
043	STP Simula enlaces redundantes y observa prevención de bucles.
044	EtherChannel Agrupa enlaces y describe sus límites.
045	Rutas estáticas Conecta subredes y diagnostica una ruta errónea.
046	OSPF Configura un área sencilla y explica vecinos y rutas.
047	ACL Permite un servicio y verifica tráfico permitido y bloqueado.
048	SSH y AAA Compara administración segura, autenticación y autorización.
049	Wi-Fi y seguridad Explica radio, SSID, autenticación, WPA y segmentación.
050	Proyecto CCNA Entrega topología, direccionamiento y pruebas de aislamiento.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Conexión CCNA: lleva dudas y capturas a tu lección de redes; confirma conceptos con el temario oficial y tu curso.

Linux: administración y protección

Competencia: Administrar servicios y conservar evidencia.

Entorno y fuentes: Kali y una VM Linux de práctica

Sesión	Concepto y evidencia de aprendizaje
051	Servicios Usa systemctl y distingue proceso de servicio.
052	Registros Busca eventos con journalctl y registra tiempo y contexto.
053	Almacenamiento Interpreta df, du, sistemas de archivos y espacio libre.
054	Gestión de paquetes Comprueba procedencia y versiones; evita scripts desconocidos.
055	SSH y llaves Configura acceso en laboratorio y protege la clave privada.
056	Firewall Define reglas mínimas y comprueba acceso desde otra VM.
057	Tareas programadas Crea una tarea inocua y registra su resultado.
058	Copias y restauración Restaura un directorio de prueba y verifica integridad.
059	Configuración segura Reduce servicios y permisos; explica cada cambio.
060	Evaluación administración Recupera un servicio roto y documenta su causa.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Principios, riesgo y criptografía

Competencia: Relacionar controles con amenazas concretas.

Entorno y fuentes: Apuntes, documentación y archivos ficticios

Sesión	Concepto y evidencia de aprendizaje
061	CIA Da ejemplos de confidencialidad, integridad y disponibilidad.
062	Riesgo Distingue activo, amenaza, vulnerabilidad, probabilidad e impacto.
063	Modelo de amenazas Dibuja datos, límites de confianza y amenazas de una app.
064	Identidad Compara autenticación, autorización, MFA y mínimo privilegio.
065	Hash Calcula huellas de archivos y observa cambios de contenido.
066	Cifrado simétrico Explica clave, confidencialidad y autenticación de datos.
067	Criptografía asimétrica Distingue cifrado, firma y verificación.
068	TLS y certificados Inspecciona certificado y explica cadena de confianza.
069	Contraseñas y secretos Explica salt, derivación, gestores y rotación de claves.
070	Evaluación de riesgo Prioriza cinco riesgos y justifica controles y límites.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Python, Bash y Git

Competencia: Automatizar tareas pequeñas que puedas explicar.

Entorno y fuentes: Python, Bash y Git; datos sintéticos

Sesión	Concepto y evidencia de aprendizaje
071	Variables y tipos Escribe un programa que transforme datos sencillos.
072	Condiciones y bucles Clasifica eventos ficticios por severidad.
073	Funciones Separa lectura, análisis y salida en funciones.
074	Archivos y JSON Lee datos de prueba y genera un resumen.
075	Errores y validación Maneja archivo ausente, formato incorrecto y entradas inesperadas.
076	Expresiones regulares Extrae campos de logs; prueba coincidencias erróneas.
077	HTTP y APIs Consulta un servicio local con límites de tiempo.
078	Bash Automatiza inventario local sin cambios destructivos.
079	Git y secretos Versiona el proyecto; excluye claves y datos personales.
080	Proyecto automatización Entrega analizador de registros con ejemplos y pruebas útiles.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Web: cómo funciona una aplicación

Competencia: Comprender peticiones, sesiones y datos.

Entorno y fuentes: Navegador, curl y servidor local

Sesión	Concepto y evidencia de aprendizaje
081	Cliente y servidor Dibuja navegador, API, servidor y base de datos.
082	HTTP Interpreta métodos, estados, cabeceras y cuerpo.
083	HTML y JavaScript Crea una página mínima y observa su ejecución.
084	Cookies y sesiones Describe cómo se mantiene una sesión y su caducidad.
085	Autenticación web Distingue inicio de sesión de permisos sobre recursos.
086	SQL Consulta tablas ficticias y usa parámetros seguros.
087	APIs y JSON Construye y valida una petición a una API local.
088	Origen y CORS Explica origen, política del navegador y permisos CORS.
089	Proxy de pruebas Observa tráfico de tu app con Burp sin cuentas personales.
090	Evaluación web Explica una transacción completa y los límites de confianza.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Seguridad web: laboratorios guiados

Competencia: Explicar fallo, impacto y corrección.

Entorno y fuentes: PortSwigger Academy y app aislada

Sesión	Concepto y evidencia de aprendizaje
091	Control de acceso Resuelve un laboratorio básico de permisos sobre objetos.
092	Autenticación débil Analiza un laboratorio de sesión o recuperación de cuenta.
093	Inyección SQL Resuelve un reto introductorio y explica consultas parametrizadas.
094	XSS Distingue datos de código; practica en un laboratorio básico.
095	CSRF Explica acción no deseada y controles en un ejemplo guiado.
096	Traversal Estudia acceso indebido a rutas y validación de archivos.
097	SSRF Dibuja peticiones del servidor y límites de acceso a destinos.
098	Carga de archivos Analiza tipo, tamaño, almacenamiento y permisos de ejecución.
099	Configuración y errores Identifica información expuesta en una app de práctica.
100	Evaluación AppSec Reproduce un fallo, aplica corrección y repite la prueba.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Evaluación de seguridad y reportes

Competencia: Investigar con alcance y evidencias reproducibles.

Entorno y fuentes: Dos VMs aisladas y herramientas locales

Sesión	Concepto y evidencia de aprendizaje
101	Alcance Define objetivos, exclusiones, horarios y condiciones de parada.
102	Inventario Identifica activos propios y servicios esperados.
103	Puertos con Nmap Examina solo la VM objetivo; interpreta estados y límites.
104	Servicios y versiones Corroborar resultados sin asumir vulnerabilidad por versión.
105	CVE y CVSS Lee un aviso oficial y valora impacto en el contexto.
106	Análisis y falsos positivos Comprueba un hallazgo con evidencia independiente.
107	Validación controlada Reproduce un problema en el objetivo autorizado sin destruir datos.
108	Evidencias Guarda pasos, tiempos y capturas sin secretos.
109	Informe Escribe causa, impacto, alcance, corrección y prioridad.
110	Reevaluación Comprueba la corrección y explica riesgos residuales.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Defensa y respuesta a incidentes

Competencia: Investigar eventos y proponer acciones verificables.

Entorno y fuentes: Registros sintéticos y capturas de práctica

Sesión	Concepto y evidencia de aprendizaje
111	Eventos y alertas Distingue registro, sospecha, alerta e incidente.
112	Telemetría Relaciona logs de autenticación, proceso, red y aplicación.
113	SIEM y EDR Explica recolección, correlación y visibilidad del endpoint.
114	Detección Crea una regla sobre eventos ficticios de acceso.
115	Falsas alarmas Mide qué eventos normales dispara tu regla.
116	Línea de tiempo Ordena eventos y conserva zona horaria.
117	Contención Propón aislamiento y revocación minimizando pérdida de evidencia.
118	Recuperación Diseña restauración y criterios de retorno a operación.
119	Evidencia y comunicación Registra cadena de custodia y hechos frente a hipótesis.
120	Proyecto defensivo Entrega análisis de incidente simulado y lecciones aprendidas.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Windows y Active Directory

Competencia: Entender identidad y permisos empresariales.

Entorno y fuentes: Windows disponible; AD opcional en laboratorio

Sesión	Concepto y evidencia de aprendizaje
121	Windows por dentro Ubica servicios, procesos, usuarios y archivos del sistema.
122	Permisos NTFS Compara permisos y herencia en una carpeta de práctica.
123	Event Viewer Identifica registros de seguridad y sistema.
124	PowerShell Filtrar eventos locales y exportar datos ficticios.
125	Dominio y directorio Dibujar controlador, equipos, usuarios y grupos.
126	Kerberos y NTLM Explica flujos de autenticación y diferencias conceptuales.
127	Políticas de grupo Diseña políticas de cuentas y administración.
128	Privilegios Audita membresías en datos sintéticos o dominio aislado.
129	Protección de identidad Propón segmentación, cuentas separadas y registro de accesos.
130	Proyecto identidad Entrega matriz de permisos y corrección de un exceso.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Cloud, contenedores y desarrollo seguro

Competencia: Diseñar controles sin contratar servicios.

Entorno y fuentes: Diagramas, Docker opcional y código local

Sesión	Concepto y evidencia de aprendizaje
131	Responsabilidad compartida Reparte controles entre proveedor y cliente en tres escenarios.
132	IAM cloud Diseña permisos limitados y evita credenciales permanentes.
133	Almacenamiento Evalúa acceso público, cifrado y retención en configuraciones ficticias.
134	Red cloud Dibuja subredes, reglas y servicios expuestos.
135	Contenedores Distingue imagen, proceso, volumen y máquina virtual.
136	Docker seguro Inspecciona una imagen; limita permisos y exposición local.
137	Dependencias Revisa avisos oficiales y prioriza actualizaciones.
138	CI/CD Dibuja controles de cambios y protección de secretos.
139	Revisión de código Detecta un fallo sencillo y verifica la corrección.
140	Proyecto arquitectura Entrega diseño seguro y pruebas locales de sus controles.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Seguridad de IA y agentes

Competencia: Aplicar seguridad a proyectos con IA.

Entorno y fuentes: Modelo disponible, datos ficticios y OWASP GenAI

Sesión	Concepto y evidencia de aprendizaje
141	Arquitectura de IA Dibuja modelo, contexto, RAG, herramientas y usuarios.
142	Datos e instrucciones Distingue entrada no confiable de instrucciones autorizadas.
143	Prompt injection Prueba casos inocuos en un asistente de laboratorio.
144	Información sensible Evalúa filtración con secretos ficticios.
145	Permisos del agente Limita operaciones y separa lectura de escritura.
146	Herramientas y validación Valida argumentos, destinos y resultados antes de actuar.
147	RAG y procedencia Marca fuentes, permisos y contenido no confiable.
148	Costos y disponibilidad Diseña cuotas, tiempos límite y límites de llamadas.
149	Evaluación Crea casos de prueba y registra aciertos y fallos.
150	Proyecto de asistente seguro Diseña un asistente de práctica con controles y trazabilidad.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Profundización técnica

Competencia: Explorar sistemas y elegir una especialidad.

Entorno y fuentes: pwn.college y programas propios de práctica

Sesión	Concepto y evidencia de aprendizaje
151	Memoria y C Comprende pila, heap, punteros y límites con ejemplos pequeños.
152	Binarios y ensamblador Relaciona instrucciones con un programa propio.
153	Depuración Observa variables y ejecución de un ejemplo inocuo.
154	Errores de memoria Estudia un fallo didáctico y su corrección.
155	Ingeniería inversa Describe comportamiento de un binario propio sin código fuente.
156	Análisis de archivos Compara análisis estático y dinámico usando archivos benignos.
157	Wi-Fi e IoT Modela firmware, actualizaciones, radio y secretos de un dispositivo IoT de práctica.
158	Seguridad móvil Dibuja permisos, almacenamiento y comunicaciones de una app.
159	Especialidad Compara redes, AppSec, SOC, cloud, DFIR y seguridad de IA.
160	Evaluación avanzada Explica límites de tu análisis y redacta plan de especialización.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Proyecto integral

Competencia: Integrar evaluación, protección y detección.

Entorno y fuentes: App y red ficticias en laboratorio aislado

Sesión	Concepto y evidencia de aprendizaje
161	Diseño del escenario Define red, usuarios, servicio y datos ficticios.
162	Construcción Prepara el entorno y registra versiones y recursos.
163	Modelo de amenazas Identifica activos, flujos y prioridades.
164	Plan de pruebas Define evidencias y criterios de éxito antes de ejecutar.
165	Evaluación de red Comprueba segmentación y servicios dentro del alcance.
166	Evaluación de aplicación Valida permisos y entradas con pruebas controladas.
167	Correcciones Aplica controles y explica su efecto.
168	Detección Genera eventos de prueba y verifica una alerta.
169	Reevaluación y recuperación Repite pruebas y restaura el entorno.
170	Defensa del proyecto Presenta informe y responde preguntas sin consultar la IA.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Especialización: primer ciclo

Competencia: Construir experiencia verificable en un área.

Entorno y fuentes: Fuentes primarias del área elegida

Sesión	Concepto y evidencia de aprendizaje
171	Diagnóstico de habilidades Elige área y detecta tres lagunas concretas.
172	Lectura técnica Resume una documentación o investigación con sus límites.
173	Laboratorio nuevo I Resuelve un reto desconocido con pistas mínimas.
174	Laboratorio nuevo II Continúa investigación y registra intentos fallidos.
175	Corrección y detección Propón mitigación y una forma de observar el problema.
176	Reproducción Repite el resultado desde un entorno limpio.
177	Revisión externa Pide revisión de un informe sin compartir datos sensibles.
178	Portafolio Publica solo material propio o permitido y evidencia anonimizada.
179	Entrevista técnica Explica decisiones y resuelve preguntas de diagnóstico.
180	Plan siguiente Define otro ciclo de diez sesiones con mayor dificultad.

Para avanzar: realiza la última sesión sin una solución copiada, explica el resultado y conserva evidencia. Si no puedes hacerlo, dedica otra hora a la habilidad pendiente y vuelve a intentarlo con una variante.

Evaluación y camino a experiencia experta

Califica cada módulo de 0 a 2 en cinco dimensiones: conceptos, ejecución, interpretación, corrección y documentación. 0: no lo logro; 1: necesito pistas; 2: lo logro y lo explico por mi cuenta. Avanza con al menos 8/10 y ninguna dimensión en cero. Es una regla de estudio propuesta, no una certificación.

Hitos: 020: Linux básico; 050: red segmentada; 080: script propio; 100: fallo web y corrección; 120: incidente simulado; 150: asistente con permisos mínimos; 170: proyecto integral; 180: especialidad y siguiente ciclo.

Prueba final: alguien prepara una variante del laboratorio con un fallo nuevo. Debes diagnosticar, justificar herramientas, preservar evidencia, corregir y volver a comprobar. Una conclusión válida puede ser "no confirmado" si explicas la evidencia que falta.

Después de las 180 sesiones

Repite el ciclo 171-180 con problemas progresivamente menos guiados. Como planificación inicial, reserva 100-200 sesiones adicionales en UNA especialidad, revisando el alcance cada 20 horas. Esta cifra organiza la práctica; no garantiza un nivel experto.

Redes: segmentación, VPN, firewall, observabilidad y recuperación.

AppSec/pentesting: laboratorios desconocidos, revisión de código y reevaluación.

Defensa/DFIR: registros nuevos, detecciones, cronologías y conservación de evidencia.

Cloud/IA: IAM, modelos de amenazas, pruebas de permisos y límites de agentes.

Evidencia de madurez: resolver casos nuevos, reconocer incertidumbre, explicar decisiones, recibir revisión, demostrar correcciones y trabajar dentro de un alcance acordado. La experiencia real autorizada y la revisión de otras personas son parte del proceso.

Compartir el aprendizaje: puedes documentar aprendizajes, diagramas y laboratorios propios. Antes de publicar soluciones de una plataforma, revisa sus reglas; pwn.college pide no difundir walkthroughs ni soluciones de sus retos.

Fuentes y recursos

Kali: documentación e instalación

<https://www.kali.org/docs/>

Kali: descarga oficial

<https://www.kali.org/get-kali/>

VirtualBox: manual oficial

<https://docs.oracle.com/en/virtualization/virtualbox/7.2/user/working-with-vms.html>

Cisco: CCNA y áreas del examen

<https://www.cisco.com/site/us/en/learn/training-certifications/certifications/enterprise/ccna/index.html>

Cisco: Packet Tracer

<https://www.netacad.com/cisco-packet-tracer>

OverTheWire: Bandit para principiantes

<https://overthewire.org/wargames/bandit/>

PortSwigger: Web Security Academy

<https://portswigger.net/web-security>

OWASP: Juice Shop

<https://owasp.org/projects/juice-shop>

pwn.college: práctica de fundamentos

<https://pwn.college/>

OWASP: seguridad de IA generativa

<https://owasp.org/projects/top-10-for-large-language-model-applications>

Fuentes consultadas para orientar recursos y plataforma. La secuencia, horas, ejercicios y criterios de evaluación son un diseño propio para tu aprendizaje. Las versiones de herramientas y temarios cambian: revisa documentación vigente al comenzar cada módulo.

Cómo comenzar desde cero

Empieza por la 001 para fijar alcance y bitácora. Completa las 002-006 para comprender y configurar la máquina virtual. En la 007 comprueba los repositorios y actualizaciones. En la 008 crea una instantánea y ensaya recuperación con archivos de prueba. Continúa en orden y repite las habilidades que todavía no puedas explicar sin ayuda.