# 100 PROYECTOS EN PYTHON
*(PRINCIPIANTE / INTERMEDIO / EXPERTO)*

---

## NIVEL PRINCIPIANTE (30 PROYECTOS)

1. **Escáner de puertos simple**
   - **Descripción:** Crear un script que escanee puertos comunes en un objetivo para determinar si están abiertos.
   - **Funciones:** Escaneo de puertos TCP y UDP.

2. **Generador de contraseñas aleatorias**
   - **Descripción:** Generar contraseñas seguras de una longitud definida.
   - **Funciones:** Incluir caracteres especiales, mayúsculas y minúsculas.

3. **Monitor de puertos abiertos**
   - **Descripción:** Crear un script para monitorear si un puerto específico está abierto en un servidor.
   - **Funciones:** Alerta cuando un puerto cambia su estado.

4. **Descargador de archivos desde URLs**
   - **Descripción:** Descargar archivos desde una URL dada, con manejo de errores.
   - **Funciones:** Descarga de imágenes, documentos y archivos comprimidos.

5. **Detector de direcciones IP**
   - **Descripción:** Crear una herramienta que detecte si una IP está dentro de un rango específico.
   - **Funciones:** Validación de IP y determinación de si está en el rango.

6. **Encriptador y desencriptador de archivos**
   - **Descripción:** Crear un sistema simple para encriptar y desencriptar archivos usando una clave secreta.
   - **Funciones:** Encriptación y desencriptación con AES o DES.

7. **Escáner de vulnerabilidades simples**
   - **Descripción:** Crear un escáner básico para detectar vulnerabilidades comunes como CVE en sistemas.
   - **Funciones:** Verificación de cabeceras HTTP y encabezados comunes.

8. **Generador de hashes**
   - **Descripción:** Crear un generador de hashes para contraseñas utilizando algoritmos como SHA256 y MD5.
   - **Funciones:** Calcular y mostrar el hash de un texto.

9. **Análisis de seguridad de contraseñas**
   - **Descripción:** Crear una herramienta que verifique la fuerza de una contraseña.
   - **Funciones:** Evaluar la complejidad de las contraseñas basándose en reglas comunes.

10. **Monitor de logs de acceso**
    - **Descripción:** Analizar logs de acceso en busca de patrones inusuales.

    - **Funciones:** Alerta cuando se detecta un número inusualmente alto de intentos fallidos.

11. **Comprobador de URLs seguras**
    - **Descripción:** Verificar si una URL está usando HTTPS.
    - **Funciones:** Hacer solicitudes HTTP y verificar los encabezados.

12. **Calculadora de cifrado Base64**
    - **Descripción:** Crear un script para codificar y decodificar texto en Base64.
    - **Funciones:** Codificación y decodificación de texto.

13. **Buscador de direcciones IP en una red**
    - **Descripción:** Encontrar todas las direcciones IP activas dentro de una red local.
    - **Funciones:** Realizar un escaneo de red para detectar dispositivos.

14. **Gestor de contraseñas básico**
    - **Descripción:** Crear un script para guardar y recuperar contraseñas de manera segura.
    - **Funciones:** Encriptación local de contraseñas.

15. **Enviador de correos con Python**
    - **Descripción:** Crear un script que envíe correos electrónicos de forma automática.
    - **Funciones:** Enviar emails utilizando SMTP y autenticación.

16. **Detector de proxies**
    - **Descripción:** Detectar si un sitio web está detrás de un servidor proxy.
    - **Funciones:** Verificación de cabeceras HTTP.

17. **Herramienta de análisis de red básica**
    - **Descripción:** Escanear una red en busca de hosts activos.
    - **Funciones:** Ping y detección de dispositivos en la red.

18. **Generador de claves públicas/privadas**
    - **Descripción:** Crear pares de claves públicas y privadas para cifrado asimétrico.
    - **Funciones:** Generación de claves RSA.

19. **Alerta de cambios en archivos**
    - **Descripción:** Monitorear un archivo y alertar cuando sea modificado.
    - **Funciones:** Uso de `os` y `watchdog` para monitorear archivos.

20. **Comprobador de certificados SSL**
    - **Descripción:** Verificar la validez de los certificados SSL de un dominio.
    - **Funciones:** Conexión SSL y comprobación de fechas de validez.

21. **Análisis de tráfico de red básico**
    - **Descripción:** Analizar paquetes de red en busca de patrones de tráfico sospechosos.
    - **Funciones:** Usar `scapy` para capturar y analizar paquetes.

22. **Generador de diccionario para ataque de diccionario**
    - **Descripción:** Crear un generador de diccionarios para pruebas de penetración.
    - **Funciones:** Combinar palabras para crear un diccionario.

23. **Buscador de servicios en red**
    - **Descripción:** Escanear una red para encontrar servicios activos.
    - **Funciones:** Realizar un escaneo de puertos.

24. **Verificador de vulnerabilidad XSS en sitios web**
    - **Descripción:** Crear un script que pruebe si un sitio es vulnerable a ataques XSS.
    - **Funciones:** Inyección de scripts simples en campos de entrada.

25. **Obfuscador de código Python**
    - **Descripción:** Crear un script que obfusque código Python para hacerlo menos legible.
    - **Funciones:** Ofuscar funciones y clases.

26. **Lector de archivos `.pcap`**
    - **Descripción:** Crear una herramienta que lea y analice archivos `.pcap` de tráfico de red.
    - **Funciones:** Decodificación y análisis básico de paquetes.

27. **Calculadora de fuerza de contraseña**
    - **Descripción:** Crear un script que calcule la fuerza de una contraseña.
    - **Funciones:** Evaluar longitud, complejidad y caracteres.

28. **Alarma de intentos fallidos de inicio de sesión**
    - **Descripción:** Crear un sistema que monitoree intentos fallidos de inicio de sesión.
    - **Funciones:** Monitorear logs y generar alertas.

29. **Escáner de vulnerabilidades CVE**
    - **Descripción:** Usar una API para verificar si un sistema está afectado por vulnerabilidades CVE.
    - **Funciones:** Consultar una base de datos de CVE.

30. **Verificador de archivos corruptos**
    - **Descripción:** Crear un script que verifique si un archivo está corrupto comparando su hash.
    - **Funciones:** Comparación de hashes y verificación de integridad.

---

## NIVEL INTERMEDIO (35 PROYECTOS)

### 31. Escáner de Vulnerabilidades para SSH
**Descripción:** Esta herramienta realiza un escaneo para identificar configuraciones inseguras en el servicio SSH, como la autenticación sin clave, la falta de cifrado adecuado o contraseñas débiles.

### 32. Monitor de Tráfico de Red con Scapy

**Descripción:** Usando Scapy, este proyecto captura y analiza el tráfico de red en tiempo real, permitiendo detectar patrones de tráfico anómalos que pueden indicar posibles intentos de intrusión o ataques.

### 33. Generador de Contraseñas Seguras
**Descripción:** Genera contraseñas aleatorias y seguras de una longitud especificada, combinando caracteres alfanuméricos y símbolos especiales para mejorar la seguridad de las cuentas.

### 34. Scraper para Detectar Vulnerabilidades en Sitios Web
**Descripción:** Scrapea sitios web y busca patrones de vulnerabilidad, como parámetros de URL inseguros que podrían ser explotados para inyecciones SQL, Cross-Site Scripting (XSS), entre otros.

### 35. Detector de Phishing con RegEx
**Descripción:** Utiliza expresiones regulares para detectar posibles URLs de phishing mediante la búsqueda de patrones comunes como "login", "secure" o "phish", lo que puede ayudar a identificar intentos de engaño en sitios web.

### 36. Script para Automatizar el Pentesting con nmap
**Descripción:** Automatiza el proceso de escaneo de red utilizando nmap, escaneando puertos abiertos y posibles vulnerabilidades en hosts o subredes, generando un reporte completo de los resultados.

### 37. Encriptador y Desencriptador de Archivos con `cryptography`
**Descripción:** Este script permite encriptar y desencriptar archivos de forma sencilla utilizando la librería `cryptography`, proporcionando una capa de seguridad para los datos sensibles almacenados.

### 38. Analizador de Logs para Eventos de Seguridad
**Descripción:** Analiza los logs del sistema, buscando eventos que puedan indicar intentos de acceso no autorizado o actividades maliciosas, como múltiples intentos fallidos de login.

### 39. Capturador de Paquetes con Scapy
**Descripción:** Captura y analiza paquetes de red utilizando Scapy, permitiendo inspeccionar en tiempo real las comunicaciones entre dispositivos y detectar cualquier anomalía que pueda indicar un ataque.

### 40. Monitor de Puertos Abiertos en la Red Local
**Descripción:** Realiza un escaneo de puertos en dispositivos dentro de la red local para identificar puertos abiertos y posibles servicios vulnerables que puedan ser explotados por un atacante.

### 41. Escáner de SSL/TLS para Certificados Caducados
**Descripción:** Analiza los certificados SSL/TLS en los servidores web para detectar certificados caducados o mal configurados que puedan poner en riesgo la seguridad de las conexiones cifradas.

### 42. Generador de Payloads Personalizados
**Descripción:** Esta herramienta genera payloads personalizados para pruebas de penetración, lo que permite simular ataques de manera controlada, como inyecciones de

código o ejecución remota de comandos.

### 43. Verificador de Seguridad de Archivos Descargados
**Descripción:** Analiza archivos descargados desde Internet en busca de malware o scripts maliciosos, utilizando firmas de virus y análisis heurísticos para verificar su seguridad antes de abrirlos.

### 44. Sistema de Detección de Intrusiones (IDS) Básico
**Descripción:** Crea un sistema simple que monitorea el tráfico de red y los logs del sistema en busca de actividades sospechosas, como intentos de acceso no autorizado o escaneos de puertos masivos.

### 45. Generador de Inyecciones SQL Aleatorias
**Descripción:** Este generador crea inyecciones SQL aleatorias, lo que permite probar la resistencia de las aplicaciones web contra este tipo de vulnerabilidades, como una prueba de seguridad.

### 46. Herramienta de Reconocimiento de Subdominios
**Descripción:** Realiza un escaneo de subdominios asociados a un dominio principal, identificando posibles puntos débiles en la infraestructura de la web y ayudando en las pruebas de penetración.

### 47. Escáner de Vulnerabilidades en Servidores Web
**Descripción:** Un escáner que analiza servidores web en busca de vulnerabilidades comunes, como fallos de configuración, puertos abiertos o problemas con la autenticación en los servicios.

### 48. Monitor de Actividad de Usuario en la Red Local
**Descripción:** Monitorea la actividad de los usuarios en la red local, detectando comportamientos inusuales, como intentos de acceso no autorizados o tráfico sospechoso entre dispositivos.

### 49. Script de Automación de Pruebas de Penetración de Aplicaciones Web
**Descripción:** Automatiza las pruebas de penetración en aplicaciones web, como escanear formularios para inyecciones SQL, XSS o la exposición de información sensible a través de los headers HTTP.

### 50. Análisis de Tráfico SSL/TLS con mitmproxy
**Descripción:** Utiliza mitmproxy para interceptar y analizar el tráfico SSL/TLS entre un cliente y un servidor, lo que permite observar comunicaciones cifradas y buscar posibles vulnerabilidades.

### 51. Descripción de Servicios Web en Puertos Abiertos
**Descripción:** Detecta y describe los servicios que se están ejecutando en puertos abiertos de un servidor, identificando versiones y configuraciones que podrían ser vulnerables.

### 52. Generador de Contraseñas para Fuerza Bruta
**Descripción:** Genera listas de contraseñas para ser utilizadas en ataques de fuerza bruta, mediante combinaciones alfanuméricas o utilizando diccionarios de palabras comunes.

### 53. Reporte de Actividad en un Sistema Linux
**Descripción:** Este script genera un reporte detallado de la actividad de un sistema Linux, como procesos activos, accesos al sistema, cambios en archivos importantes, etc.

### 54. Sistema de Protección contra Ataques DDoS Simulados
**Descripción:** Simula un ataque DDoS y luego implementa medidas de protección como limitación de conexiones simultáneas o la utilización de una red de distribución de contenido (CDN).

### 55. Herramienta de Fingerprinting de Sistemas Operativos
**Descripción:** Analiza la información de los paquetes de red para identificar el sistema operativo de los dispositivos conectados, utilizando técnicas de fingerprinting.

### 56. Herramienta para Probar Contraseñas de FTP
**Descripción:** Prueba contraseñas comúnmente utilizadas en servidores FTP en un esfuerzo por realizar un ataque de fuerza bruta o diccionario sobre servidores FTP vulnerables.

### 57. Análisis de Seguridad de Archivos en la Nube
**Descripción:** Analiza archivos almacenados en servicios de nube como Google Drive o Dropbox, verificando su integridad, seguridad de acceso y posibles vulnerabilidades asociadas.

### 58. Rastreo de Correo Electrónico para Detección de Phishing
**Descripción:** Realiza un análisis de correos electrónicos sospechosos para detectar características típicas de ataques de phishing, como enlaces maliciosos o dominios falsificados.

### 59. Análisis de Seguridad en una Red WiFi
**Descripción:** Analiza las redes WiFi cercanas, buscando posibles debilidades en la configuración, como contraseñas débiles, cifrado inseguro o puntos de acceso no autorizados.

### 60. Script para Automatizar el Uso de metasploit
**Descripción:** Automatiza la ejecución de metasploit para realizar pruebas de penetración, como la explotación de vulnerabilidades conocidas en sistemas remotos.

### 61. Herramienta para Detectar y Reportar HTTP Response Headers Mal Configurados
**Descripción:** Analiza los headers de respuesta HTTP de servidores web y detecta configuraciones inseguras que podrían exponer información sensible o permitir ataques como XSS.

### 62. Monitor de Seguridad en Tiempo Real para Redes Inalámbricas
**Descripción:** Monitorea el tráfico de redes WiFi en tiempo real, buscando patrones que puedan indicar posibles intentos de intrusión o ataques, como sniffing o spoofing de red.

### 63. Descubrimiento de Dispositivos IoT en la Red
**Descripción:** Detecta dispositivos IoT (Internet of Things) conectados a la red, como cámaras de seguridad o termostatos, y evalúa su seguridad para identificar

posibles vulnerabilidades.

### 64. Sistema de Backup y Recuperación Automática de Archivos Críticos
**Descripción:** Realiza copias de seguridad de archivos importantes en intervalos regulares y permite una recuperación rápida en caso de pérdida de datos o ataque de ransomware.

### 65. Generador de Exploits para Pruebas de Penetración
**Descripción:** Genera exploits personalizados que pueden ser utilizados para simular ataques en sistemas durante pruebas de penetración, ayudando a identificar vulnerabilidades en el software y la infraestructura.

---

# NIVEL AVANZADO (35 PROYECTOS)

## 66. Framework de Pentesting Personalizado
**Descripción:** Crea un marco modular para pruebas de penetración que integre herramientas comunes como nmap, metasploit y burpsuite, permitiendo la automatización de múltiples tareas de pentesting.

## 67. Ataque de Fuerza Bruta Distribuido con Python
**Descripción:** Desarrolla un sistema que permita ejecutar ataques de fuerza bruta distribuidos, utilizando múltiples máquinas en la red para probar contraseñas en servidores remotos.

## 68. Herramienta de Sniffing y Spoofing de Red con Scapy
**Descripción:** Utiliza Scapy para capturar paquetes en una red, modificar paquetes y realizar ataques de spoofing, como el envenenamiento ARP, para redirigir el tráfico hacia una máquina atacante.

## 69. Detección de Ataques DDoS con Machine Learning
**Descripción:** Implementa un sistema que utiliza machine learning para detectar patrones de tráfico sospechosos, identificando intentos de ataques DDoS a partir de la recopilación de datos en tiempo real.

## 70. Escáner de Vulnerabilidades de Aplicaciones Web con Wapiti
**Descripción:** Desarrolla un escáner que utiliza Wapiti para realizar un análisis exhaustivo de aplicaciones web en busca de vulnerabilidades como XSS, inyecciones SQL, CSRF, etc.

## 71. Monitor de Seguridad para Dispositivos IoT
**Descripción:** Crea un sistema de monitoreo en tiempo real para dispositivos IoT, detectando vulnerabilidades conocidas y patrones anómalos de comportamiento que puedan indicar un compromiso.

## 72. Script para Explotar Vulnerabilidades de Inyección SQL
**Descripción:** Desarrolla un script que utilice diversas técnicas de inyección SQL para explotar vulnerabilidades en aplicaciones web y obtener acceso a bases de datos sensibles.

## 73. Herramienta de Escalamiento de Privilegios en Linux

**Descripción:** Implementa una herramienta que explora un sistema Linux en busca de posibles vectores de escalamiento de privilegios, como vulnerabilidades en configuraciones de SUDO o en permisos de archivos.

## 74. Implementación de Técnicas de Escucha Silenciosa con tcpdump
**Descripción:** Crea un script que permita escuchar de manera pasiva las comunicaciones en una red utilizando tcpdump y realizar análisis de tráfico sin generar alertas en la red.

## 75. Análisis de Vulnerabilidades en Contenedores Docker
**Descripción:** Desarrolla una herramienta para analizar la seguridad de los contenedores Docker, buscando configuraciones incorrectas y vulnerabilidades conocidas en imágenes y contenedores en ejecución.

## 76. Sistema de Detección de Malware en Archivos
**Descripción:** Crea una herramienta de análisis de malware en archivos que utiliza firmas y heurísticas para detectar posibles infecciones en archivos comprimidos y ejecutables.

## 77. Herramienta de Bypass de Antivirus con Técnicas de Ofuscación
**Descripción:** Implementa un sistema que utiliza técnicas avanzadas de ofuscación de código para evadir los antivirus, permitiendo que los payloads maliciosos pasen desapercibidos en entornos de pruebas.

## 78. Generador de Payloads para Explotación Remota
**Descripción:** Desarrolla una herramienta que crea payloads personalizados para la explotación remota de sistemas, utilizando diferentes técnicas de evasión y canales de comunicación.

## 79. Ataques de Fuerza Bruta en Servicios Web con hydra
**Descripción:** Crea un script que automatice los ataques de fuerza bruta a través de servicios web utilizando hydra, incluyendo la validación de contraseñas mediante diccionarios personalizables.

## 80. Análisis de Seguridad para Redes Mesh
**Descripción:** Realiza un análisis profundo de las redes Mesh, identificando vulnerabilidades específicas que pueden ser explotadas en la capa de enlace de datos o en la comunicación entre nodos.

## 81. Escáner de Seguridad para Infraestructura de Nube
**Descripción:** Desarrolla una herramienta que escanea infraestructuras basadas en la nube, como AWS o Azure, en busca de configuraciones inseguras o vulnerabilidades que puedan ser explotadas.

## 82. Explotación de Vulnerabilidades de Buffer Overflow en C
**Descripción:** Crea un exploit que aproveche vulnerabilidades de desbordamiento de búfer en aplicaciones escritas en C, permitiendo la ejecución remota de código en sistemas vulnerables.

## 83. Creador de Rootkits en Python
**Descripción:** Desarrolla un rootkit en Python que permita a un atacante obtener privilegios elevados en un sistema comprometido y ocultar su presencia en los logs y

procesos del sistema.

## 84. Implementación de Tácticas de Evasión en Metasploit
**Descripción:** Crea módulos personalizados en metasploit que implementen técnicas avanzadas de evasión, como el uso de cifrado, enmascaramiento o explotación de puertos no comunes.

## 85. Sistema de Captura y Análisis de Tráfico HTTPS
**Descripción:** Desarrolla un sistema que intercepte y analice el tráfico HTTPS utilizando técnicas de Man-in-the-Middle, desencriptando el tráfico para observar los datos transmitidos.

## 86. Análisis de Seguridad en Redes 5G
**Descripción:** Desarrolla una herramienta que realice pruebas de seguridad en redes 5G, buscando vulnerabilidades en la infraestructura de la red y en los protocolos utilizados en las comunicaciones.

## 87. Realización de un Ataque Man-in-the-Middle con ARP Spoofing
**Descripción:** Implementa un ataque de ARP Spoofing para interceptar y modificar el tráfico entre dos dispositivos en una red local, permitiendo la observación o manipulación de las comunicaciones.

## 88. Análisis de Tráfico DNS para Detección de C2
**Descripción:** Desarrolla una herramienta que monitorice y analice el tráfico DNS para detectar patrones sospechosos de tráfico de comando y control (C2) en comunicaciones de malware.

## 89. Generación de Escenarios de Phishing Avanzados
**Descripción:** Crea un generador de escenarios de phishing avanzado, que simula ataques realistas utilizando páginas web falsas, correos electrónicos fraudulentos y redirecciones de tráfico.

## 90. Sistema de Automatización para Explotación de Web Shells
**Descripción:** Desarrolla un sistema automatizado que permite ejecutar comandos remotos en un servidor comprometido a través de una shell web, facilitando la escalada de privilegios y el control del servidor.

## 91. Detectores de Anomalías en Redes con Algoritmos de Machine Learning
**Descripción:** Implementa un sistema que utiliza técnicas de machine learning para detectar comportamientos anómalos en una red, como tráfico inusual o intentos de intrusión.

## 92. Automator de Explotación de Puertos RDP
**Descripción:** Crea una herramienta que automatiza la explotación de vulnerabilidades en puertos RDP (Remote Desktop Protocol), aprovechando configuraciones inseguras para obtener acceso remoto a los sistemas.

## 93. Automación de la Creación de Malware con pyinstaller
**Descripción:** Implementa un sistema que utiliza pyinstaller para empaquetar scripts maliciosos en ejecutables, dificultando la detección por herramientas antivirus.

## 94. Sistema de Monitoreo de Seguridad para IoT en Redes de Alta Velocidad

**Descripción:** Crea una herramienta que monitorea el tráfico de dispositivos IoT en redes de alta velocidad, analizando la seguridad de las comunicaciones y alertando sobre posibles vulnerabilidades.

## 95. Implementación de Técnicas de Evasión en Firewalls
**Descripción:** Desarrolla un sistema que implementa técnicas de evasión avanzadas para eludir firewalls y sistemas de detección de intrusiones (IDS) durante un ataque cibernético.

## 96. Fuzzer de Aplicaciones Web para Pruebas de Seguridad
**Descripción:** Crea un fuzzer que automatiza las pruebas de seguridad en aplicaciones web, enviando entradas aleatorias a formularios y parámetros de URL para detectar vulnerabilidades como XSS o inyecciones SQL.

## 97. Generador de Ransomware con Cifrado de Archivos
**Descripción:** Desarrolla un ransomware básico que cifra los archivos del sistema utilizando algoritmos de cifrado fuertes, con el fin de aprender sobre las técnicas utilizadas por el malware.

## 98. Sistema de Explotación de Vulnerabilidades en API RESTful
**Descripción:** Crea un script que explota vulnerabilidades comunes en APIs RESTful, como inyecciones de comandos, falta de autenticación adecuada o exposición de datos sensibles.

## 99. Creador de Payloads con Explotación de Vulnerabilidades Zero-Day
**Descripción:** Desarrolla un generador de payloads que explota vulnerabilidades zero-day (desconocidas) en software, permitiendo la ejecución de código arbitrario en sistemas desprotegidos.

## 100. Herramienta de Escaneo de Vulnerabilidades en Redes 5G
**Descripción:** Realiza escaneos avanzados en redes 5G, identificando fallos de seguridad en la infraestructura y servicios, ayudando a mejorar la protección de las redes móviles de próxima generación.