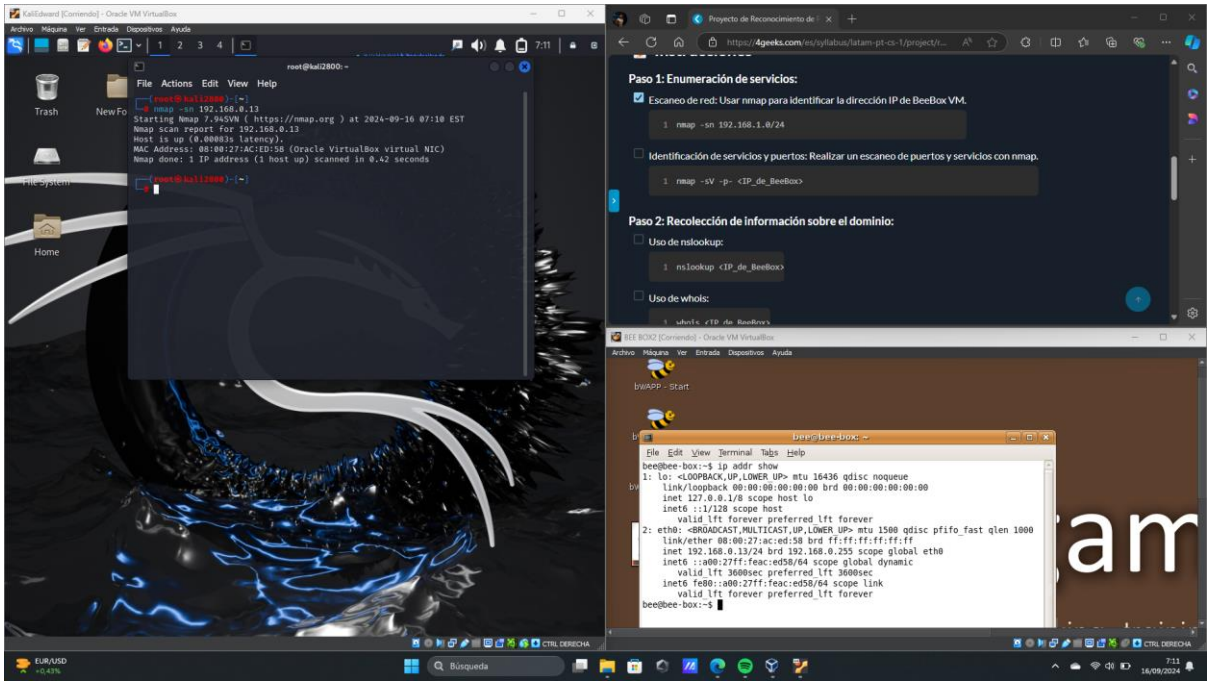
Reporte de Reconocimiento de Pentesting en sitio Web Vulnerable

Un proyecto de reconocimiento de **pentesting** en un **sitio web vulnerable** se centra en identificar y evaluar las debilidades de seguridad en un sitio web específico. Consiste en llevar una planificación, reconocimiento, mapeo, identificación de vulnerabilidades, explotación y reporte que es como en este caso que haremos.

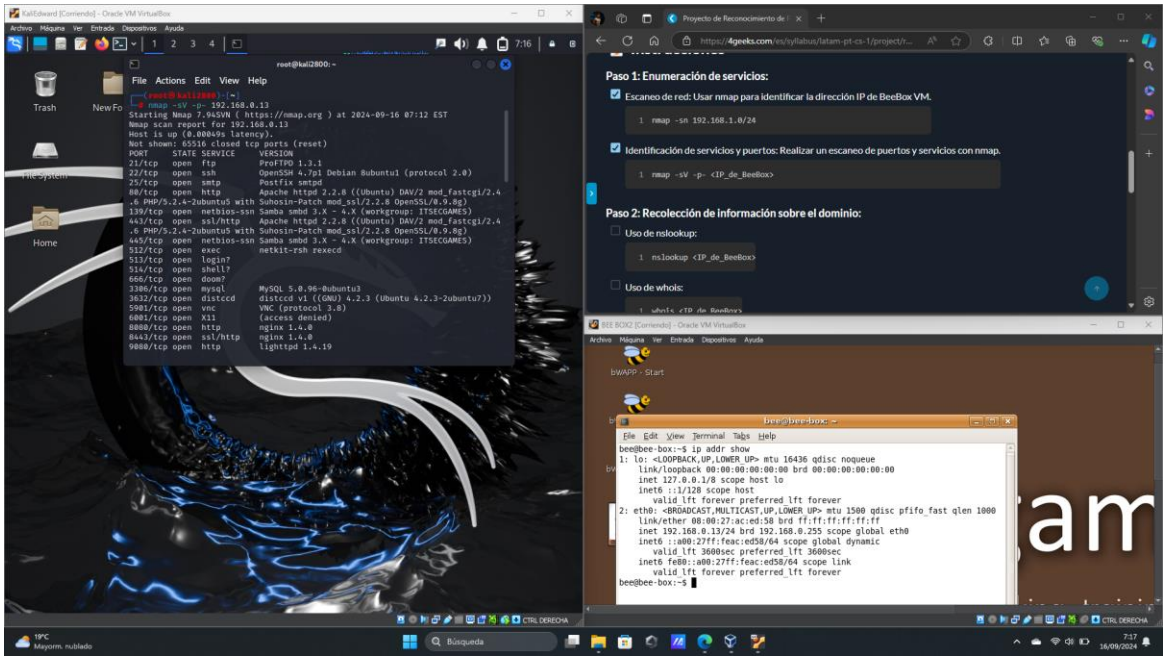
Resultado del escaneo de red.

- Para este caso usamos el comando nmap + la dirección ip de la maquina victima para identificar la dirección IP, nmap es una herramienta de código abierto ampliamente utilizada para la exploración de redes y la auditoría de seguridad.



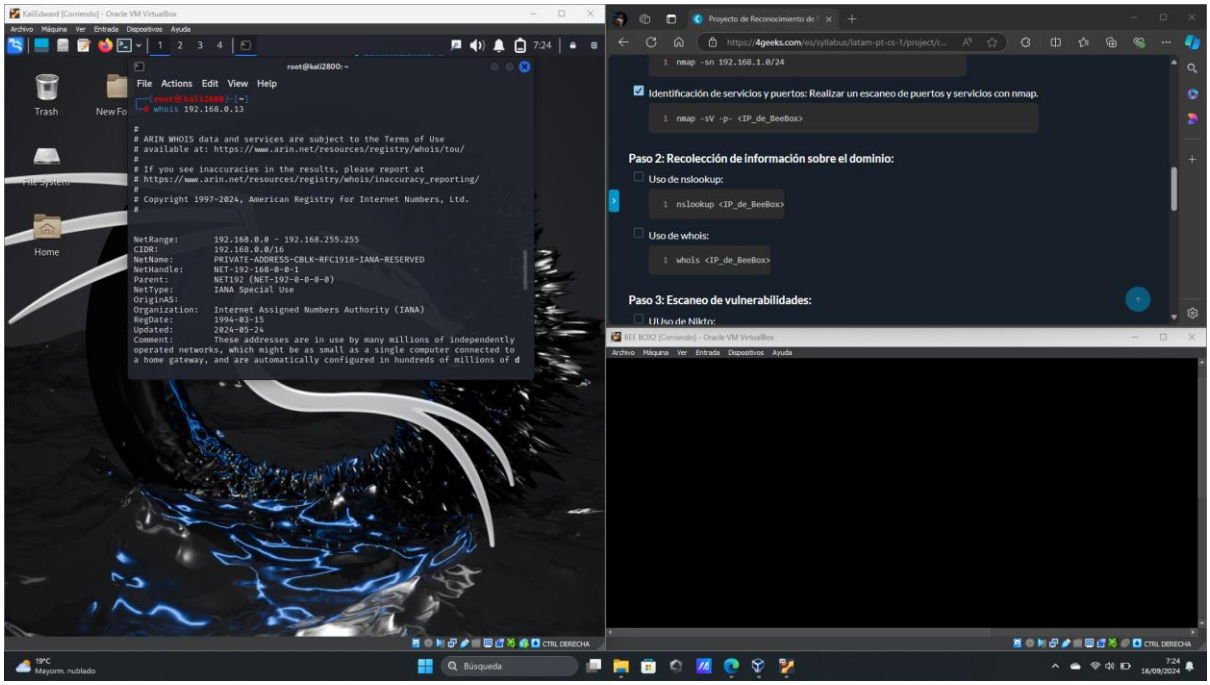
Resultados de enumeración de servicios.

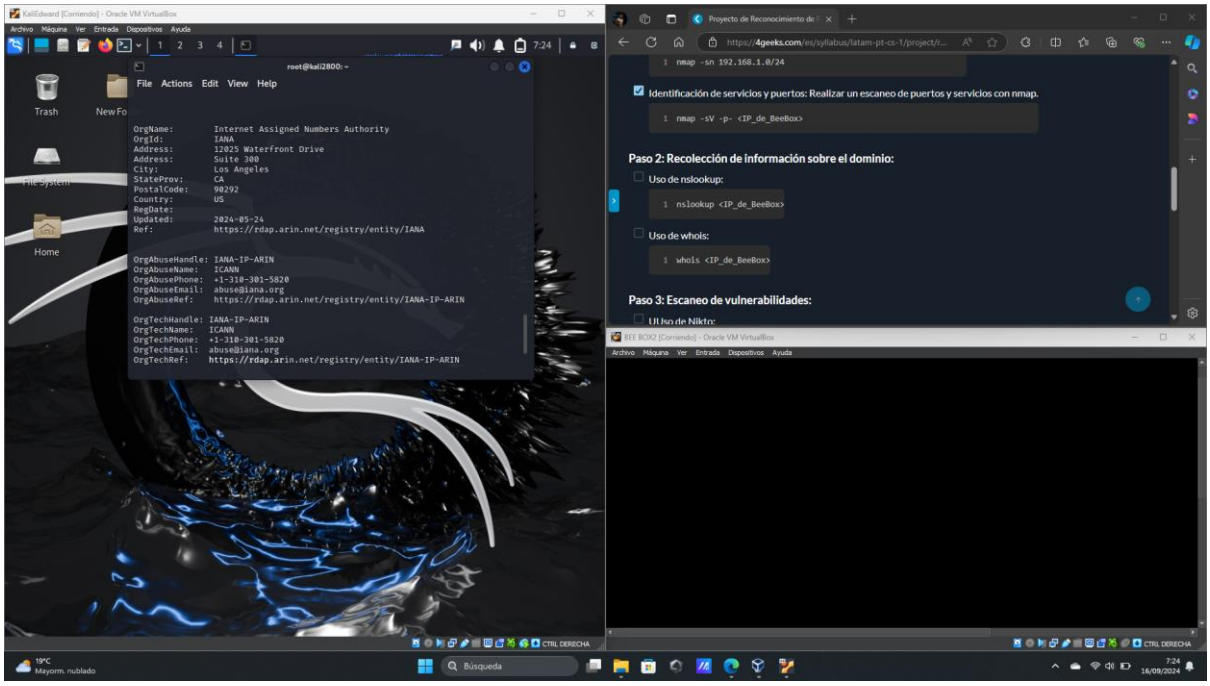
- Para identificar servicios y puertos utilizamos nmap, como mencionamos esta herramienta nos es de utilidad para ejecutar dicho escaneo. Utilizamos el comando nmap –sV –p- + la dirección ip de la maquina víctima.



Información del dominio.

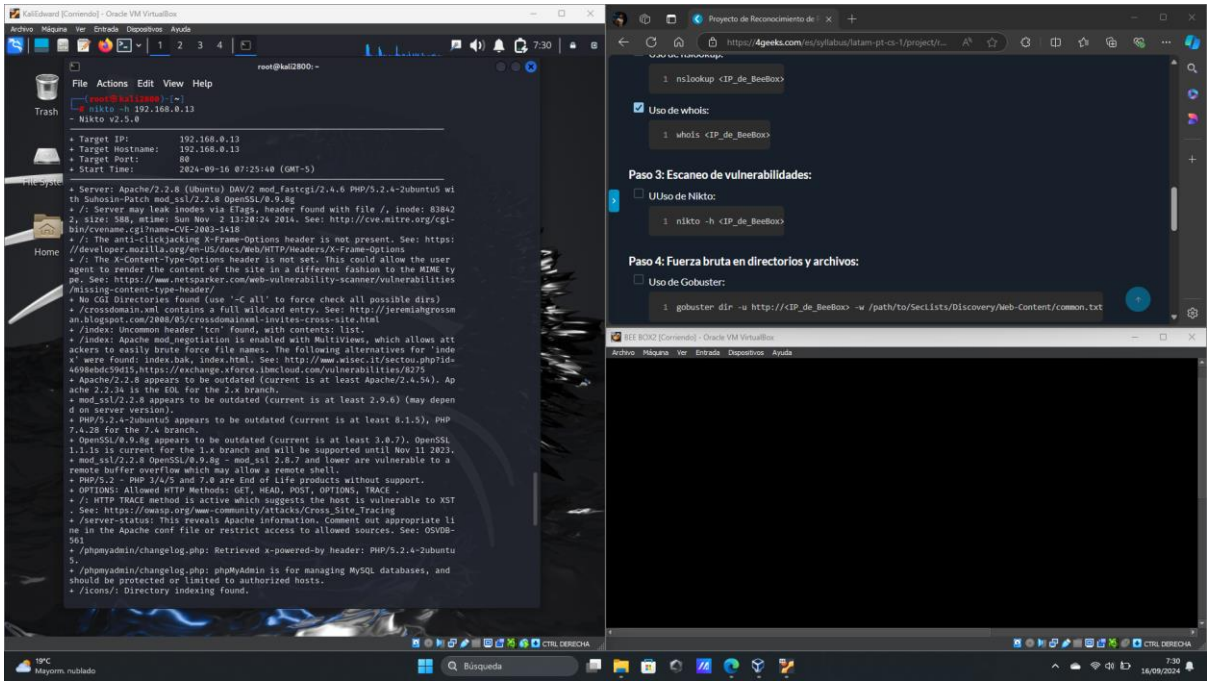
- En esta parte usamos comandos para hacer recolección de información sobre el dominio con herramientas como nslookup y whois. **nslookup** es una herramienta de red utilizada para consultar servidores DNS (Domain Name System) y obtener información sobre la resolución de nombres de dominio; **whois** permite obtener detalles sobre el registro de un nombre de dominio, como la fecha de creación, la fecha de vencimiento, los datos del registrador, y los datos de contacto del propietario del dominio.




Kali[Edward] [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali2800: ~
File Actions Edit View Help
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate:
Updated: 2024-05-24
Ref: https://rdap.arin.net/registry/entity/IANA
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN
Trash
New Fo
File System
Home
CTRL DERECHA
19°C
Mayorm. nublado
Búsqueda
Proyecto de Reconocimiento de
https://4geeks.com/es/syllabus/latam-pt-cs-1/project/r...
nmap -sn 192.168.1.0/24
Identificación de servicios y puertos: Realizar un escaneo de puertos y servicios con nmap.
nmap -sV -p- <IP_de_BeeBox>
Paso 2: Recolección de información sobre el dominio:
Uso de nslookup:
nslookup <IP_de_BeeBox>
Uso de whois:
whois <IP_de_BeeBox>
Paso 3: Escaneo de vulnerabilidades:
BEE BOX2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
CTRL DERECHA
7:24
16/09/2024

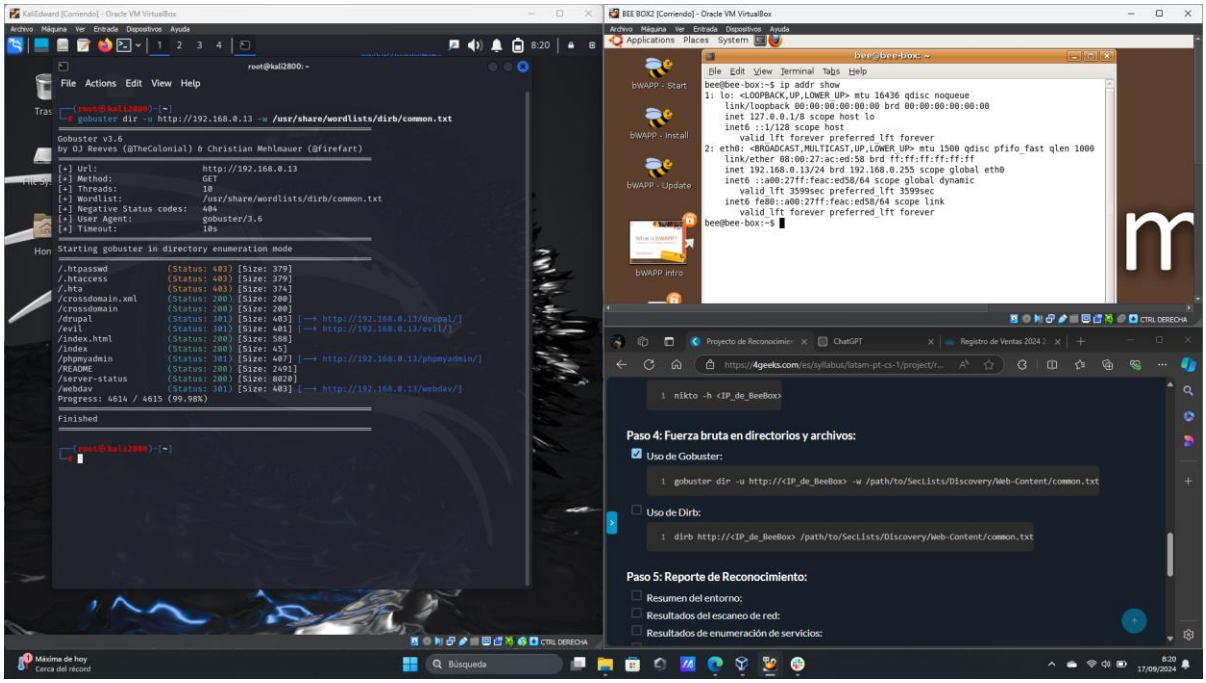
Vulnerabilidades encontradas.

- En este paso hacemos un escaneo de vulnerabilidades para encontrar fallas y posibles amenazas, pare esto usaremos **nikto** es una herramienta de escaneo de seguridad de aplicaciones web de código abierto que se utiliza para identificar vulnerabilidades y problemas de seguridad en servidores web. Usamos el comando Nikto –h + la dirección ip para escanear las posibles vulnerabilidades.

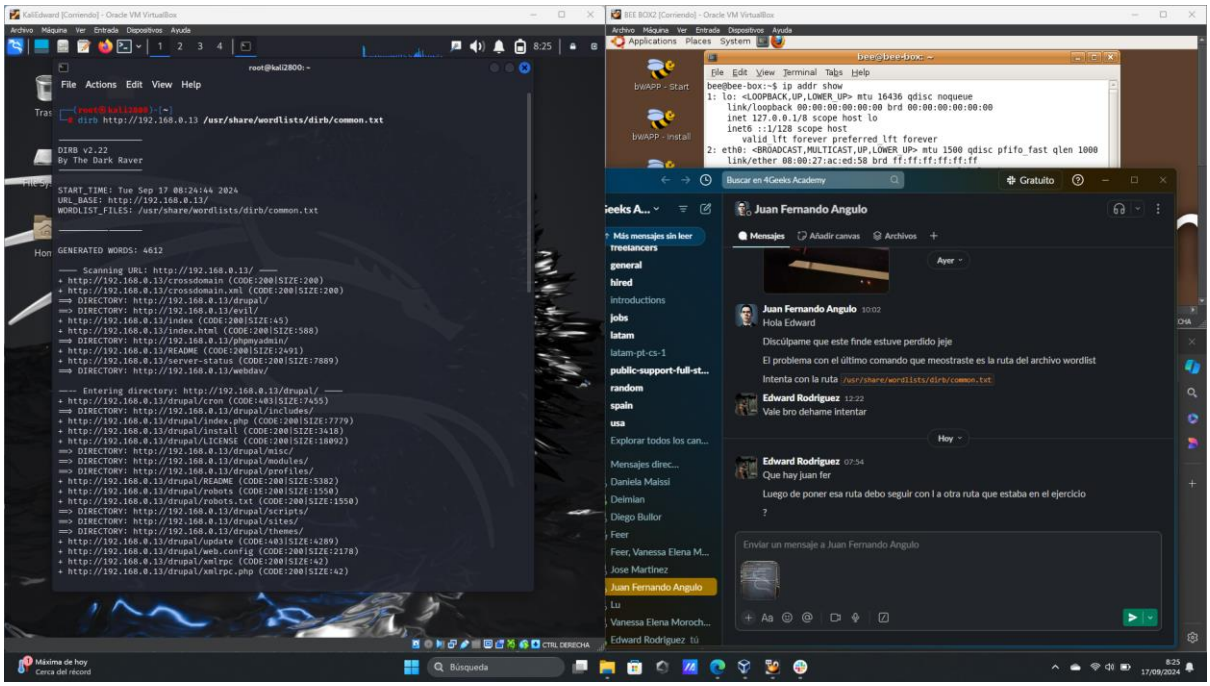


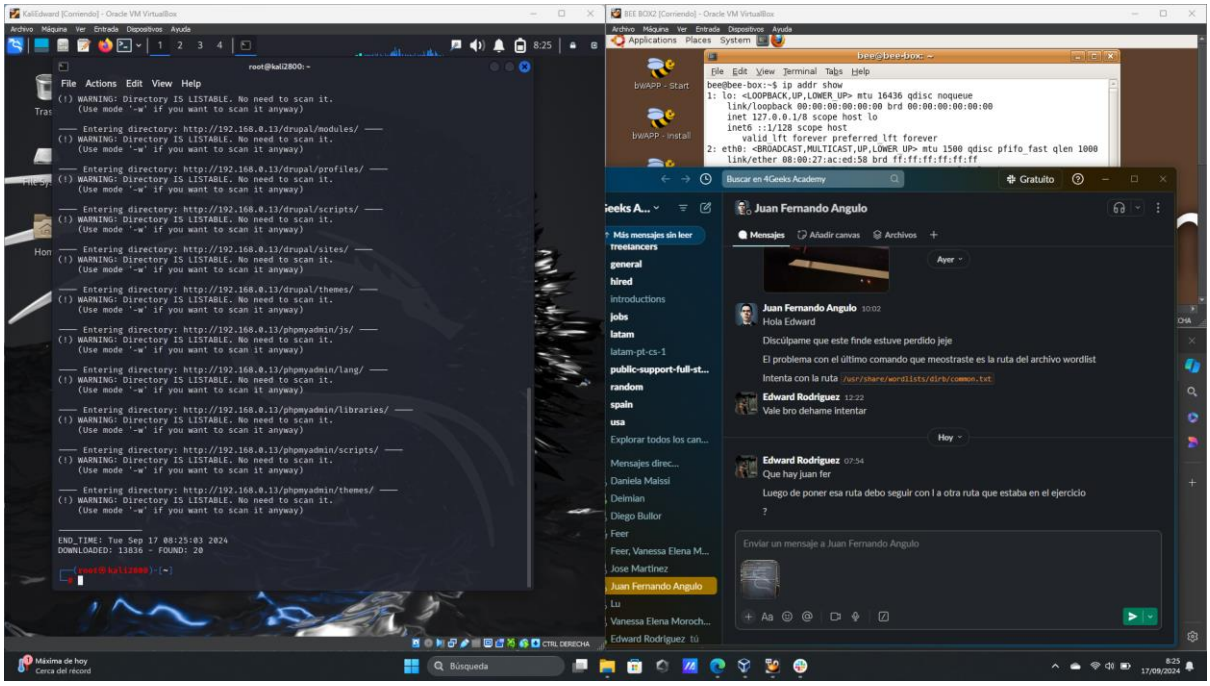
Directorios y archivos encontrados.

- Fuerza bruta en directorios y archivos utilizamos Gobuster que es una herramienta de enumeración de directorios y archivos utilizada principalmente en pruebas de penetración y auditorías de seguridad. Funciona enviando solicitudes HTTP a un servidor web y buscando directorios o archivos que puedan estar ocultos o no indexados.



- **DIRB** es una herramienta de enumeración de directorios y archivos utilizada en pruebas de penetración. Su función principal es descubrir rutas ocultas en un servidor web, enviando solicitudes HTTP a diferentes URLs basadas en una lista de palabras (wordlist).





Análisis y conclusiones.

- En el análisis de este proyecto fue identificar y evaluar las vulnerabilidades en un sitio web específico mediante un proceso de reconocimiento y escaneo. Esto incluye la recopilación de información sobre el objetivo, el mapeo de su estructura y la identificación de posibles vectores de ataque; en conclusión, El proyecto de reconocimiento de pentesting en el sitio web vulnerable logró identificar múltiples áreas de riesgo que podrían ser explotadas por un atacante. La metodología empleada permitió un enfoque sistemático y organizado, garantizando una cobertura amplia de posibles vectores de ataque.

  El reconocimiento es una fase vital en el proceso de pentesting y su adecuada ejecución puede prevenir ataques potencialmente devastadores. Implementar las recomendaciones surgidas de este análisis ayudará a mejorar la seguridad del sitio web y a proteger mejor la información de los usuarios.