

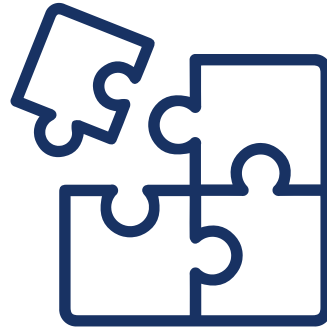
LAS 10 CLAVES PARA EMPEZAR TU CAMINO EN CIBERSEGURIDAD CON ÉXITO



TÚ

@SAULRUIZPLAZA





ENTIENDE LA ARQUITECTURA COMPLETA

- Mira el sistema como un mapa: qué dispositivos, servicios y aplicaciones existen y cómo se conectan entre sí. No es solo buscar fallos aislados, sino comprender relaciones y dependencias.
- Te permite anticipar dónde un fallo o vulnerabilidad puede propagarse, y priorizar esfuerzos de análisis y protección de manera efectiva.





APRENDE A ESCANEAR Y ENUMERAR SISTEMAS

- Es el proceso de identificar activos, servicios y puertos en una red o sistema. Esto implica mapear hosts, detectar servicios activos y recopilar información que pueda ser usada para auditorías o pruebas de penetración.
- Puedes detectar versiones de software, servicios expuestos y configuraciones débiles con nmap.





GESTIONA LAS CREDENCIALES CÓMO UN PRO

- **Cómo se crean, almacenan y usan las credenciales, además de cómo se podrían comprometer. Técnicamente, esto abarca hashing, políticas de acceso y mecanismos de autenticación.**
- **Comprender esto te permite evaluar la fuerza de contraseñas, probar sistemas en entornos controlados y aplicar controles que prevengan ataques de fuerza bruta, diccionario o reutilización de credenciales.**





AUTOMATIZA TAREAS BÁSICAS

- Aprender a automatizar análisis, escaneos y reportes ahorra tiempo y minimiza errores. Scripts simples o herramientas de automatización permiten replicar pruebas de forma consistente.
- Puedes usar Python, Bash o PowerShell para crear scripts. Te permitirá centrarte en interpretar resultados y practicar técnicas avanzadas sin perder tiempo en tareas repetitivas.





CENTRALIZA LOS LOGS

- **Aprender a centralizar logs te da visión completa de la actividad de sistemas y redes. No se trata solo de leer registros: se trata de detectar patrones, anomalías y amenazas persistentes.**
- **Practica con herramientas SIEM como Wazuh, creando dashboards, alertas, reportes y respuestas ante alertas**





SECURIZA EQUIPOS FINALES

- Son la puerta de entrada más común para ataques. Conocer cómo proteger laptops, móviles y servidores es esencial.
- Practica configurando antivirus, firewalls locales, políticas de acceso y cifrado.





PRACTICA > TEORÍA

- Entender la teoría es útil, pero aplicar lo aprendido en laboratorios, VMs y entornos controlados fija conocimientos y desarrolla habilidades reales.
- La clave es combinar teoría y práctica: estudia conceptos, pero ponlos a prueba en Hack The Box . 30-60 minutos de práctica diaria superan horas de solo lectura, y te preparan para escenarios del mundo real.





LA NECESIDAD DE UN BACKUP

- Las copias de seguridad garantizan continuidad ante fallos o ataques, no solo en teoría, sino en sistemas reales.
- Configura backups de servidores, bases de datos y VMs con herramientas como rsync, Acronis y practica restauraciones para asegurarte de que funcionan cuando más se necesitan.





DOCUMENTA TODO LO QUE HAGAS

- **Registra cómo identificas y explotas vulnerabilidades en entornos controlados, incluyendo pasos, resultados y mitigaciones.**
- **Para tu marca personal, comparte: contexto, prueba realizada y lecciones aprendidas, siempre indicando que son entornos con permiso y sin exponer exploits reales.**





APRENDE DE INCIDENTES REALES

- **Analizar brechas y vulnerabilidades reportadas te permite ver cómo los sistemas fallan en la práctica.**
- **Esto ayuda a identificar patrones repetitivos, reforzar configuraciones y anticipar posibles fallos en tus laboratorios, acercando la teoría al mundo real y mejorando tus capacidades técnicas desde el inicio.**





Saúl Ruiz

Ciberseguridad y Sistemas

PlaSysX

**¡Más consejos en
mis redes sociales!**

plasysx

saulruizplaza