Webinar Gratuito

Fundamentos de Ciberseguridad

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Miércoles 29 Julio 2026

Alonso Eduardo Caballero Quezada

Cuento con más de diecinueve años de experiencia en el área y desde hace quince años me especializo en la áreas de Hacking, Forense, OSINT, Ciberseguridad y temas relacionados.

https://www.linkedin.com/in/alonsocaballeroquezada/

https://x.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

https://wa.me/51949304030

https://t.me/ReYDeS

El Panorama Actual de Amenazas

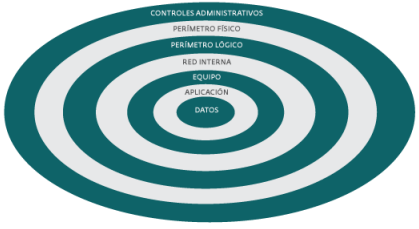
La Inevitabilidad del Compromiso: Entendiendo al Adversario

- **Automatización del cibercrimen:** Escaneos masivos y ciberataques no dirigidos buscando vulnerabilidades conocidas
- **El factor tiempo:** Importancia crítica del tiempo para detección, respuesta, y remediación (Dwell Time)
- **Modelo “Assume Breach”:** Diseñar la seguridad asumiendo algún control perimetral eventualmente fallará

El Principio de Defensa en Profundidad

Estrategia Multicapa para la Protección Organizacional

- **Superposición de capas:** Ninguna solución técnica es infalible por sí sola
- **Tecnología:** Herramientas de red, endpoint, y encriptación
- **Procesos:** Políticas, gestión de parches, y respuesta ante incidentes
- **Personas:** Capacitación y concientización contra ingeniería social



Arquitectura y Segmentación de Red

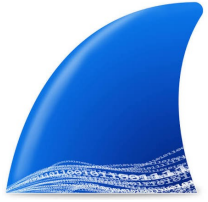
Diseñando una Red Defendible

- **Aislamiento de activos:** Uso estratégico de VLANs y micro-segmentación
- **Control de movimiento lateral:** Bloqueo de comunicaciones no autorizadas entre zonas internas
- **Control de accesos:** Implementación de listas para control de acceso (ACLs) y filosofía Zero Trust

Visibilidad y Vigilancia del Tráfico

Inspección y Análisis de Protocolos

- **Inspección de tráfico:** Roles complementarios de Firewalls, IDS, e IPS
- **Protocolos críticos:** Inspección de tráfico DNS y HTTP/HTTPS para detectar túneles maliciosos
- **Captura de paquetes:** Análisis táctico mediante herramientas como Wireshark o tcpdump



Encriptación y Comunicaciones Seguras

Protección de Datos en Tránsito

- **Cifrado de canales:** Eliminación definitiva de protocolos en texto plano (HTTP, Telnet, FTP)
- **TLS 1.3:** Protección robusta de aplicaciones web y APIs
- **SSH / IPsec:** Administración remota segura e interconexión mediante VPNs

Fortalecimiento de Sistemas (Hardening)

Asegurando Sistemas Operativos (Windows & GNU/Linux)

- **Reducción de la superficie de ataque:** Deshabilitar servicios, componentes, y puertos innecesarios
- **Configuraciones base (Baselines):** Aplicación de Directivas de Grupo (GPO) y CIS Benchmarks
- **Ajustes predeterminados:** Eliminación de credenciales de fábrica e interfaces administrativas expuestas

Evolución de la Protección del Endpoint

De la Protección Convencional a EDR/XDR

- **Antivirus tradicional:** Limitaciones operativas de la detección basada puramente en firmas
- **EDR (Endpoint Detection & Response):** Análisis de comportamiento e indicadores de compromiso en tiempo real
- **Aislamiento automatizado:** Capacidad para contener un equipo infectado directamente desde la red

Gestión de Vulnerabilidades

Programa Práctico de Evaluación y Parcheo

- **Ciclo de vida:** Descubrimiento, evaluación, priorización, y remediación sistemática
- **Priorización basada en riesgo:** Enfocarse en vulnerabilidades explotadas activamente
- **Gestión de parches:** Procesos automatizados de actualización para el Sistema Operativo y software de terceros.

Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

La Identidad como Nuevo Perímetro

Gestión de Identidades y Accesos (IAM)

- **Principio del Menor Privilegio:** Restricción de permisos administrativos al estricto mínimo necesario
- **Control de acceso basado en roles (RBAC):** Estructuración y auditoría periódica de accesos
- **Autenticación Multifactor (MFA):** Despliegue obligatorio para VPN, correo electrónico, y entornos en la nube.

Seguridad en Entornos Nube e Híbridos

Fundamentos de Protección en AWS, Azure y GCP

- **Modelo de Responsabilidad Compartida:** Delimitando los alcances entre el proveedor y el cliente
- **Visibilidad en la nube:** Vigilancia continua de configuraciones, identidades, y almacenamiento.
- **Postura de seguridad (CSPM):** Auditorías automatizadas para prevenir buckets o servicios expuestos.

Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Respuesta a Incidentes: Las 6 Fases

Ciclo Operativo ante un Compromiso de Seguridad

1. Preparación & 2. Identificación: Detección de indicadores de compromiso (IoC)

3. Contención: Detener la propagación del ciberataque en la infraestructura

4. Erradicación & 5. Recuperación: Restablecimiento seguro de las operaciones

6. Lecciones Aprendidas: Retroalimentación para mejorar los controles defensivos

Resiliencia y Copias de Seguridad

Estrategia Antiransomware y Recuperación de Datos

- **Regla de oro 3-2-1:** 3 copias de datos, en 2 medios distintos, y 1 copia fuera de sitio (off-site)
- **Respaldos inmutables (Air-Gapped):** Protección de copias contra borrado malicioso o encriptación por ransomware
- **Pruebas de restauración:** Validar frecuentemente los tiempos de recuperación reales (RTO y RPO)

Gobierno, Métricas y Monitoreo Continuo

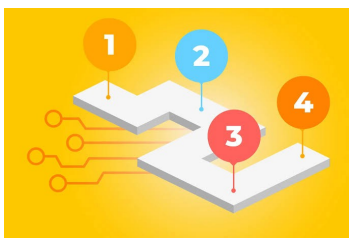
Evaluando la Postura Defensiva

- **Gestión de Logs y SIEM:** Centralización de eventos para análisis, auditoría, y correlación
- **Métricas defensivas:** Tasa de parches aplicados, adopción de MFA, y tiempo medio para detección (MTTD)
- **Alineación con el negocio:** Traducir eventos técnicos a niveles de riesgo operacional para la dirección

Hoja de Ruta Práctica para la Organización

Plan de Acción Inmediato

- **Paso 1:** Obtener visibilidad total de los activos de red y aplicar hardening inicial en los endpoints
- **Paso 2:** Exigir MFA de manera global, y restringir cuentas con privilegios administrativos
- **Paso 3:** Probar la restauración de copias de seguridad aisladas y definir el plan básico ante incidentes

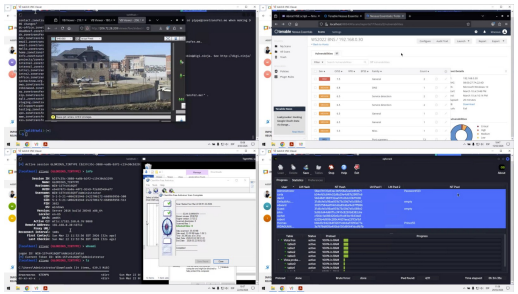


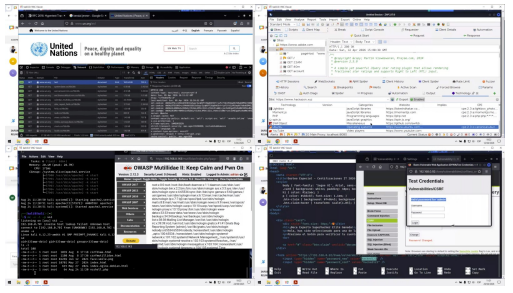
Resumen Operativo y Próximos Pasos

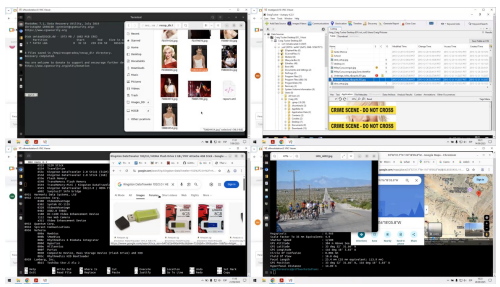
- **Estrategia ganadora:** Equilibrio constante entre Prevención, Detección y Respuesta
- **Higiene operacional:** La ciberseguridad no es un proyecto único, es un hábito operacional continuo

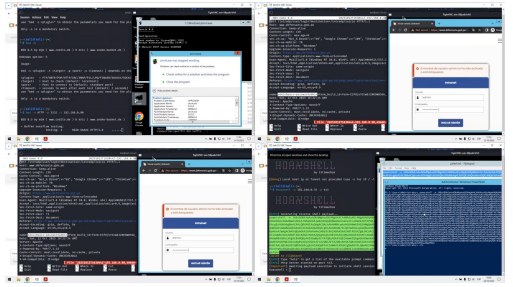
Cursos (Aula Virtual)

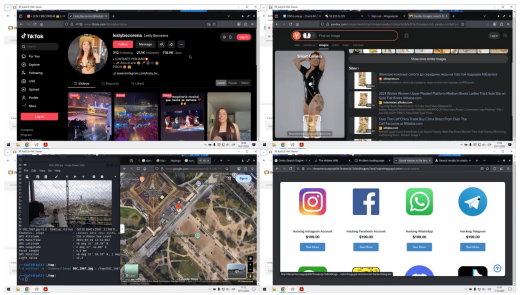
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Ciberseguridad Windows y Linux
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego Graph CE
- Y más...

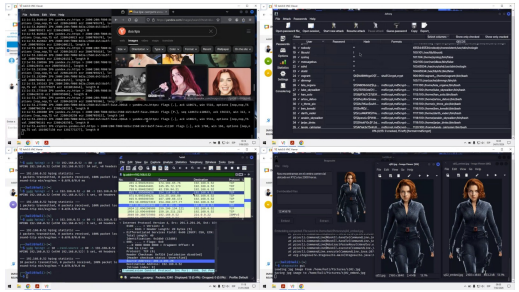












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Webinar Gratuito

Fundamentos de Ciberseguridad

Alonso Eduardo Caballero Quezada

:|: Hacking :|: Forense :|: Linux :|: OSINT :|: Ciberseguridad :|:

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Miércoles 29 Julio 2026