Horizon Tecnologies

“The future is now”

Informe Ejecutivo de Seguridad

Emulación Red Team – MITRE ATT&CK

Autor: Sebastián Useche – Profesional en formación en Ciberseguridad y Cloud Security.

Fecha: octubre 2025

Resumen Ejecutivo

Evaluamos la infraestructura del servidor web frente a técnicas adversarias alineadas con MITRE ATT&CK.

Principales hallazgos: Se logro comprometer mediante servicios expuestos que pueden desencadenar un escalda de privilegios desde un rol mal configurado, comprometiendo Datos críticos del servidor.

Impacto: Riesgo inminente de perdida de datos, interrupción de servicios, sanciones legales y reputación.

Recomendaciones:

- No exponer servicios sensibles
- Usar contraseñas robustas, rotación periódica y habilita MFA
- Implementar firewall
- Monitorear accesos y creación de cuentas

Metodología

Se Utilizo el framework MITRE ATT&CK para simular al atacante

Se ejecutaron fases como:

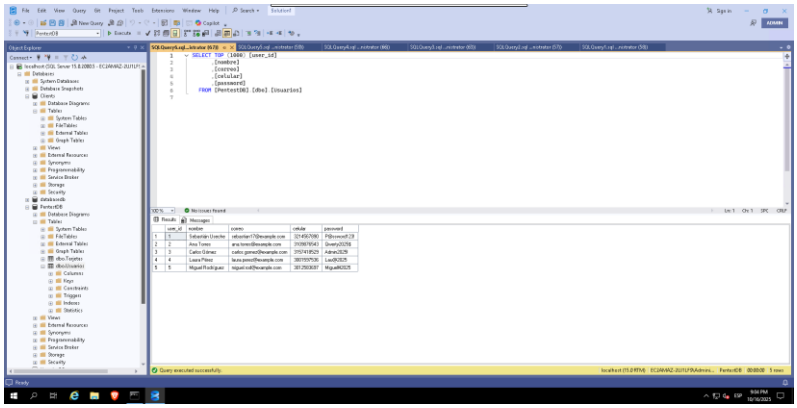
- Reconocimiento y Acceso inicial
- Descubrimiento
- Obtención de credenciales
- Escalada a administrador
- Acceso a base de datos
- Persistencia

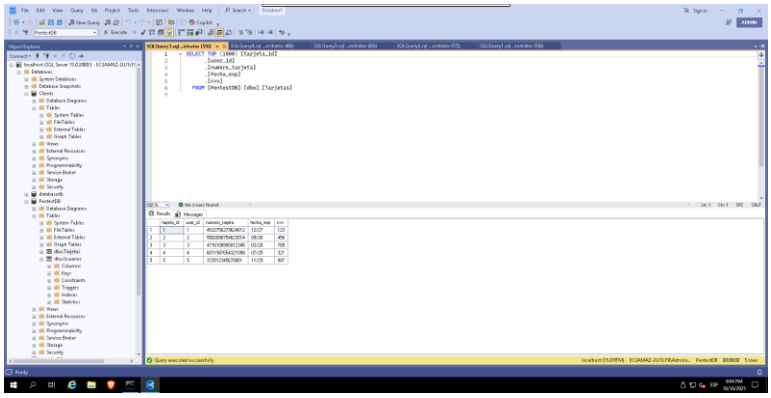
Hallazgos Detallados

Se detallan hallazgos técnicos identificados durante la emulación Red Team.

ID	Táctica	Técnica	Riesgo	Recomendación
H-01	Privilegie Escalación	Exploting misconfigured IAM roles	Alto	Revisar y aplicar principio least privilegie en todos los roles IAM
H-02	Credential Access	Password brute-forcé en servicio RPD	Medio	Implementar MFA y políticas de bloqueo tras intentos fallidos
H-03	Lateral Movement	SMB shares sin control de acceso	Medio	Restringir permisos de compartición y aplicar segmentación de red

Evidencias





Conclusiones

El ejercicio evidencia brechas críticas en el servidor, Si no se corrige podría permitir que un atacante escale privilegios y comprometer datos sensibles, Se recomienda implementar las medidas sugeridas en un plazo máximo de 30-60 días para reducir significativamente el riesgo, seguir las recomendaciones permitirá no solo mitigar amenazas, si no también elevar la madurez en ciberseguridad y alinear la estrategia con las mejores praticas de estándar internacional.