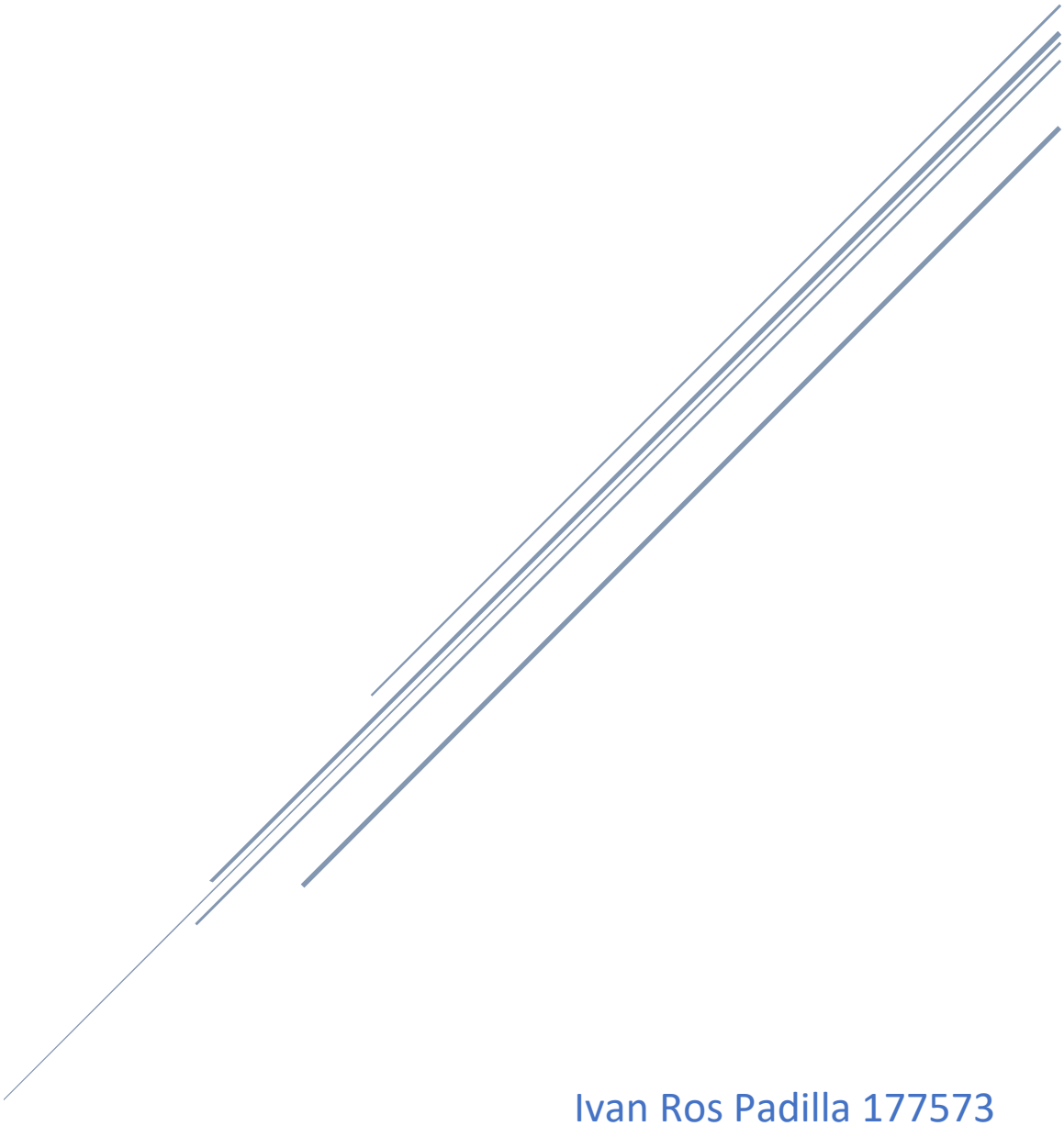
ESCENARIOS DE COMPROMISO DE SEGURIDAD INFORMATICA



Ivan Ros Padilla 177573

Escenario	Servicio X.800 comprometido	Definiciones RFC 4949	Amenaza	Vector de ataque	Impacto tecnico	Medida de control
1	Confidencialidad, integridad y disponibilidad	Multi-stage attack, data breach, availability attack	Externa	Compromiso de credenciales y filtración de datos	Perdida de informacion, acceso no autorizado	Respaldos inmutables/offline, EDR, detección temprana, segmentación de red
2	Confidencialidad	Misconfiguration, Exposure	Interna (error)	Configuración incorrecta en nube	Pérdida de confidencialidad, impacto legal/reputacional	Revisiones de configuración, controles de acceso estrictos, auditorías periódicas
3	Integridad, Confidencialidad	Supply chain attack	Externa	Actualización de software maliciosa	Violación de integridad, accesos no autorizados	Validación de firmas, SBOM, monitoreo de proveedores, Zero Trust
4	Autenticación, Control de acceso	Credential compromise, Authentication failure	Externa	Phishing + uso de credenciales válidas	Persistencia del atacante, acceso prolongado	MFA, monitoreo de comportamiento, detección de anomalías
5	Disponibilidad, Integridad	Data destruction, Availability attack	Externa	Eliminación/cifrado de respaldos	Imposibilidad de recuperación, impacto catastrófico	Respaldos offline/inmutables, segregación de copias, monitoreo de backup
6	Confidencialidad, Control de acceso	Insider threat	Interna	Extracción de datos con privilegios legítimos	Venta de datos, fuga de información	Políticas de mínimo privilegio, monitoreo de insiders, DLP
7	Integridad, No repudio	Evidentiary integrity, Audit trail violation	Externa	Alteración/cifrado de logs	Pérdida de trazabilidad, impacto legal/probatorio	Logs inmutables, SIEM, almacenamiento seguro de evidencias
8	Disponibilidad	Operational failure	Interna (error)	Ejecución incorrecta de actualización	Caída global de servicios críticos	Pruebas previas, planes de reversión, gestión de cambios
9	Autenticación, Confidencialidad	Masquerade, Phishing	Externa	Sitios y correos falsos	Robo de datos ciudadanos, suplantación	SPF/DKIM/DMARC, concientización, autenticación de dominios
10	Confidencialidad, Integridad, Disponibilidad	Destructive attack	Externa	Exfiltración + destrucción de sistemas	Daño irreversible, pérdida total	Detección temprana, planes de contingencia, redundancia geográfica

Referencias:

ITU-X 800: X.800 : Security architecture for Open Systems Interconnection for CCITT applications

RFC 4949: RFC 4949 - Internet Security Glossary, Version 2