Actividad 02 - Análisis de servicios de seguridad

Jorge Alejandro Cabrera Meza – 181591

CNO V – Seguridad informática

Ing. Tecnologías de la información

Mt Servando López Contreras

Introducción

El propósito de este análisis es comprender cómo estos marcos definen los servicios, mecanismos y términos necesarios para proteger la información en redes modernas. Su relevancia actual radica en que proporcionan el lenguaje técnico y la estructura lógica para enfrentar amenazas globales de forma estandarizada, utilizándolo en caso practico con 10 escenarios donde se nos contextúa el como utilizar el ITU-T X.800 y el RFC 4949.

Contexto

La seguridad informática no se limita a instalar software; requiere un diseño arquitectónico y una terminología precisa para ser efectiva para poder llevar a cabo su buen uso:

- **ITU-T X.800:** Proporciona un marco sistemático para definir dónde y cómo aplicar la seguridad en las capas de red. Clasifica los servicios (como autenticación y confidencialidad) y los mecanismos (como cifrado y firmas digitales) para mitigar ataques.
- **RFC 4949:** Establece las definiciones oficiales y el vocabulario técnico para la comunidad de Internet. Su función es evitar ambigüedades, asegurando que conceptos como "vulnerabilidad" o "explotación" tengan el mismo significado para todos los actores.

Análisis de casos de uso

Escenario 01.

En múltiples incidentes atribuidos al grupo LockBit, organizaciones públicas y privadas han sufrido el cifrado masivo de servidores tras un acceso inicial no autorizado. Antes de ejecutar el ransomware, los atacantes exfiltraron información sensible y posteriormente amenazaron con su publicación, evidenciando un compromiso simultáneo de **la confidencialidad, la integridad y la disponibilidad.** Desde el enfoque del RFC 4949, el incidente se clasifica como un multi-stage attack con data breach y availability attack, donde la indisponibilidad del sistema es solo una fase final del daño. La ausencia de respaldos inmutables y de detección temprana permitió que el impacto fuera total.

Elemento	Respuesta
Servicios X.800 comprometidos	Control acceso; Integridad; Disponibilidad; Confidencialidad
Definición(es) aplicable(s) RFC 4949	multi-stage; data breach; availability attack
Tipo de amenaza	Ransomware / Extorsión
Vector de ataque	Acceso no autorizado; Exfiltración
Impacto técnico / operativo	Cifrado masivo; Pérdida datos; Indisponibilidad
Medida de control recomendada	Backups inmutables; EDR; Segmentación; Detección precoz

Escenario 02.

En diversos casos documentados, bases de datos completas quedaron accesibles públicamente debido a errores de configuración en servicios de almacenamiento en la nube. No existió una explotación técnica sofisticada, sino una falla en el **control de acceso**, lo que derivó directamente en la pérdida de **confidencialidad de los datos**. El RFC 4949 describe este tipo de incidentes como misconfiguration y exposure, subrayando que la amenaza no siempre implica malware o intrusión activa. El impacto suele ser legal y reputacional, aun cuando **no se pueda demostrar acceso malicioso.**

Elemento	Respuesta
Servicios X.800 comprometidos	Control acceso; Confidencialidad; No repudio
Definición(es) aplicable(s) RFC 4949	misconfiguration; exposure
Tipo de amenaza	Exposición por error
Vector de ataque	Configuración errónea (cloud)
Impacto técnico / operativo	Fuga datos; Riesgo legal; Daño reputacional
Medida de control recomendada	Revisiones IAM; Políticas S3/ACL; Auditoría

Escenario 03.

Un proveedor legítimo de software fue comprometido y distribuyó una actualización que incluía código malicioso, afectando a cientos de organizaciones que confiaban en él. Este escenario refleja una violación grave de la integridad de los sistemas y, en muchos casos, de la **confidencialidad**, al **permitir accesos no autorizados** posteriores. El RFC 4949 lo identifica como supply chain attack, destacando el abuso de relaciones de confianza. El daño es particularmente crítico porque rompe el supuesto de legitimidad del software firmado.

Elemento	Respuesta
Servicios X.800 comprometidos	Confidencialidad; Control acceso; Integridad; Disponibilidad
Definición(es) aplicable(s) RFC 4949	supply chain attack
Tipo de amenaza	Cadena de suministro comprometida
Vector de ataque	Actualización maliciosa (proveedor)
Impacto técnico / operativo	Compromiso masivo; Confianza rota
Medida de control recomendada	Verificación firma; SBOM; Aislamiento; Lista blanca

Escenario 04.

Mediante campañas de **phishing**, atacantes obtuvieron credenciales válidas y accedieron a sistemas corporativos durante meses sin levantar alertas. Aunque la autenticación funcionó técnicamente, el servicio de autenticación fue comprometido al basarse en credenciales robadas, afectando también el control de acceso. Según el RFC 4949, se trata de un credential compromise con authentication failure conceptual, no técnica. La falta de MFA y de monitoreo de comportamiento facilitó la persistencia del atacante.

Elemento	Respuesta
Servicios X.800 comprometidos	Autenticación; Control acceso
Definición(es) aplicable(s) RFC 4949	credential compromise; authentication failure
Tipo de amenaza	Robo de credenciales / Phishing
Vector de ataque	Emails phishing; Ingeniería social
Impacto técnico / operativo	Acceso persistente; Mov. lateral
Medida de control recomendada	MFA; Monitor UEBA; Rotación credenciales

Escenario 05.

En ataques de ransomware avanzados, los atacantes eliminaron o cifraron los respaldos antes de afectar los sistemas productivos. Este hecho compromete directamente la disponibilidad y la integridad de la información, al impedir la recuperación. El RFC 4949 clasifica este comportamiento como data destruction y availability attack, evidenciando intención deliberada de maximizar el daño. La inexistencia de respaldos offline o inmutables convierte el incidente en catastrófico.

Elemento	Respuesta
Servicios X.800 comprometidos	Disponibilidad; Integridad
Definición(es) aplicable(s) RFC 4949	data destruction; availability attack
Tipo de amenaza	Ransomware avanzado (backup wipe)
Vector de ataque	Eliminación cifrado de backups
Impacto técnico / operativo	Imposible recuperación; Paralización
Medida de control recomendada	Backups offline/inmutables; Seg. de backups; Pruebas

Escenario 06.

Un empleado con acceso legítimo extrajo bases de datos completas y las vendió a terceros, sin explotar vulnerabilidades técnicas. El servicio afectado fue principalmente la confidencialidad, junto con fallas en el control de acceso por exceso de privilegios. El RFC 4949 define este escenario como insider threat, destacando que el riesgo interno puede ser tan grave como el externo. La carencia de monitoreo y de políticas de mínimo privilegio fue determinante.

Elemento	Respuesta
Servicios X.800 comprometidos	Confidencialidad; Control acceso
Definición(es) aplicable(s) RFC 4949	insider threat
Tipo de amenaza	Amenaza interna (malicioso)
Vector de ataque	Abuso de privilegios
Impacto técnico / operativo	Fuga datos; Pérdida confianza
Medida de control recomendada	Principio mínimo privilegio; DLP; Auditoría

Escenario 07.

Tras un ataque, los registros del sistema quedaron cifrados o alterados, impidiendo reconstruir la secuencia de eventos. Esto compromete la integridad de los datos y el no repudio, ya que no es posible demostrar qué ocurrió ni quién fue responsable. Desde el RFC 4949, se trata de una violación de evidentiary integrity y del audit trail. El impacto no solo es técnico, sino también probatorio y legal.

Elemento	Respuesta
Servicios X.800 comprometidos	Integridad; No repudio; Auditoría
Definición(es) aplicable(s) RFC 4949	evidentiary integrity; audit trail compromise
Tipo de amenaza	Manipulación de logs
Vector de ataque	Cifrado/alteración de registros
Impacto técnico / operativo	Imposible reconstruir eventos; Riesgo legal
Medida de control recomendada	Logs remotos/inmutables; SIEM; Backup logs

Escenario 08.

Una actualización mal ejecutada provocó la caída simultánea de múltiples servicios críticos a nivel global. Aunque no existió un atacante, el servicio de disponibilidad fue gravemente afectado. El RFC 4949 contempla estos eventos como operational failure, recordando que la seguridad también se ve afectada por errores internos. La falta de pruebas previas y planes de reversión amplificó el impacto.

Elemento	Respuesta
Servicios X.800 comprometidos	Disponibilidad
Definición(es) aplicable(s) RFC 4949	operational failure
Tipo de amenaza	Fallo operativo / Cambio erróneo
Vector de ataque	Actualización mal ejecutada
Impacto técnico / operativo	Caída servicios; Interrupción masiva
Medida de control recomendada	Pruebas preprod; Rollback; Automatización segura

Escenario 09.

Atacantes replicaron sitios y correos oficiales para engañar a ciudadanos y obtener información sensible. Este escenario afecta la autenticación, al suplantar identidades legítimas, y la confidencialidad de los datos recolectados. El RFC 4949 lo clasifica como masquerade y phishing, subrayando el componente de ingeniería social. La ausencia de mecanismos de autenticación del dominio y de concientización facilitó el éxito del ataque.

Elemento	Respuesta
Servicios X.800 comprometidos	Autenticación; Confidencialidad
Definición(es) aplicable(s) RFC 4949	masquerade; phishing
Tipo de amenaza	Suplantación / Phishing
Vector de ataque	Sites y emails falsos
Impacto técnico / operativo	Robo datos; Engaño usuarios
Medida de control recomendada	DMARC/DKIM/SPF; Concientización; MFA

Escenario 10.

En algunos incidentes, tras exfiltrar información, los atacantes ejecutaron acciones destructivas para borrar sistemas completos y eliminar rastros. Se produce un compromiso total de la confidencialidad, la integridad y la disponibilidad, configurando uno de los peores escenarios posibles. El RFC 4949 describe este patrón como destructive attack, donde el objetivo no es solo el lucro, sino el daño irreversible. La detección tardía impidió cualquier contención efectiva.

Elemento	Respuesta
Servicios X.800 comprometidos	Confidencialidad; Integridad; Disponibilidad
Definición(es) aplicable(s) RFC 4949	destructive attack
Tipo de amenaza	Ataque destructivo
Vector de ataque	Exfil + destrucción
Impacto técnico / operativo	Pérdida irreversible; Caída total
Medida de control recomendada	Seg. multicapa; Backups; Respuesta IR; Contención

Conclusión

Los casos analizados muestran que muchos incidentes ocurren por errores humanos, malas configuraciones o falta de controles básicos de seguridad. Estos problemas pueden afectar datos, sistemas y operaciones de las organizaciones. Sin embargo, con buenas prácticas, capacitación y medidas preventivas simples, es posible reducir riesgos y proteger mejor la información.

Referencias

- RFC 4949 - Internet Security Glossary, Version 2
- ITU: Connecting the world and beyond
- X.800 : Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT