

Actividad 02

CNOV SEGURIDAD INFORMATICA

Brian Salvador Espinoza Aguilar
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Contenido

Introducción	2
Contexto del X.800 y RFC 4949	2
Contenido.....	2
Conclusiones	5
Referencias.....	6

Introducción

En este documento se verán escenarios en los que se presentan vulnerabilidades o situaciones, en las cuales se podrán identificar los puntos importantes de dichos escenarios, como cuales servicios de x.800 fueron comprometidos y también con la ayuda del RFC 4949 identificar el tipo de vulneración que paso, de estos archivos también importante mencionarlos porque nos ayudarán a obtener definiciones que nos serán útiles para saber que está pasando.

Contexto del X.800 y RFC 4949

Para comenzar es importante saber de para que nos sirven y de que tratan estos dos conceptos el primero, la x.800 define seis servicios de seguridad fundamentales, aplicables a cualquier sistema de comunicación los cuales se definen como:

1. Autenticación: Verifica la identidad de las entidades que se comunican.
2. Control de acceso: Garantiza que solo usuarios autorizados puedan acceder a recursos.
3. Confidencialidad de los datos: Protege la información de accesos no autorizados durante la transmisión.
4. Integridad de los datos: Asegura que los datos no sean alterados durante la transmisión.
5. No repudio: Evita que una entidad niegue haber participado en una transacción.
6. Disponibilidad: Garantiza que los sistemas y servicios estén operativos cuando se necesiten.

Por otro lado, el RFC 4949 es uno de los documentos más importantes en materia de criminología y fundamentos conceptuales de seguridad informática. Es emitido por la IEFT y sirve como un glosario oficial de los términos utilizados en el ámbito de la seguridad en las redes, criptografía y protocolos de internet.

El nombre completo es “RFC 4949: Internet Security Glossary, Version 2”, se le atribuye a Russell L. (Russ) Shirey, del U.S. Department of Defense (DoD) y fue publicaso en Agosto de 2007, finalmente fue emitido por IETF (Internet Engineering Task Force) — organismo responsable de los estándares técnicos de Internet.

Contenido

Escenarios para analizar

Escenario 1

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.	
Servicio X.800 Comprometidos	Integridad de los datos, Disponibilidad, control de acceso
Definiciones aplicables RFC 4949.	Multi-stage attack: ataque compuesto por fases. Data breach: divulgacion de datos no autorizada
Tipo de amenaza	Externa
Vector de ataque	Compromiso de credenciales y pérdida del control del sistema al poder ejecutar un ransomware
Impacto técnico / operativo	Filtración de datos sensibles
Medida de control / recomendada	Copias de seguridad aisladas y verificacion doble al entrar al sistema
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.	
Servicio X.800 Comprometidos	Autenticación, Control de acceso Integridad de los datos
Definiciones aplicables RFC 4949.	Misconfiguration: Estado de un sistema accesible que crea vulnerabilidades Unauthorized Disclosure: Divulgacion no autorizada.
Tipo de amenaza	Externa
Vector de ataque	Los atacantes buscan activamente estos errores con escáneres automatizados.
Impacto técnico / operativo	Perdida completa de confidencialidad
Medida de control / recomendada	Configuración de privilegios de privilegios de la nube y herramientas de seguridad en la nube.
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.	
Servicio X.800 Comprometidos	Integridad de los datos, autenticación
Definiciones aplicables RFC 4949.	Supply Chain Attack: ataque que explota una relación de confianza
Tipo de amenaza	Externa
Vector de ataque	Actualización de software comprometido, abuso de la cadena de suministro.
Impacto técnico / operativo	Violación masiva de integridad del sistema
Medida de control / recomendada	Verificar firmas digitales, retraso controlado de actualizaciones críticas.
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.	
Servicio X.800 Comprometidos	Autenticación, control de acceso
Definiciones aplicables RFC 4949.	Control compromise: credencial ha sido obtenida por una entidad no autorizada
Tipo de amenaza	Externa
Vector de ataque	Phishing, los atacantes evitaron controles de autenticación.
Impacto técnico / operativo	Acceso no autorizado a sistema de datos
Medida de control / recomendada	Múltiple factor de autenticación, monitoreo de comportamiento de usuarios.
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.	
Servicio X.800 Comprometidos	Disponibilidad, Integridad de los datos
Definiciones aplicables RFC 4949.	Data destruction: datos inaccesibles, availability attack: ataque de denegación de servicios.
Tipo de amenaza	Externa
Vector de ataque	Credenciales robadas, uso de ransomware para localizar y destruir.
Impacto técnico / operativo	Eliminación total del plan de recuperación
Medida de control / recomendada	Backups inmutables
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.	
Servicio X.800 Comprometidos	Confidencialidad de datos, control de acceso
Definiciones aplicables RFC 4949.	Insider threat: Amenaza proveniente de personas dentro de la organización
Tipo de amenaza	Interna
Vector de ataque	Uso indebido de credenciales y permisos legítimos
Impacto técnico / operativo	Perdida masiva de confidencialidad
Medida de control / recomendada	Revisar y ajustar permisos regularmente
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.	
Servicio X.800 Comprometidos	Integridad de los datos, no repudio
Definiciones aplicables RFC 4949.	Audit Trail: Registro cronológico de actividades, evidentiary Integrity: Propiedad que asegura que la evidencia digital no ha sido alterada.
Tipo de amenaza	Externa

Vector de ataque	Usan acceso administrativo para modificar/eliminar logs
Impacto técnico / operativo	Imposibilidad de realizar un analisis forense efectivo
Medida de control / recomendada	Almacenamiento inmutable de 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	
Servicio X.800 Comprometidos	Disponibilidad, Integridad de los datos
Definiciones aplicables RFC 4949.	Operational Failure: fallo que resulta de errores de procedimientos operativos
Tipo de amenaza	Interna
Vector de ataque	Implementación de cambios sin pruebas adecuadas
Impacto técnico / operativo	Perdidas financieras masivas, Interrupción global de servicios
Medida de control / recomendada	Monitoreo proactivo
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.	
Servicio X.800 Comprometidos	Autenticación, confidencialidad de los datos
Definiciones aplicables RFC 4949.	masquerade: Ataque donde una entidad finge ser una entidad diferente
Tipo de amenaza	Externa
Vector de ataque	Creación de sitios y correos falsos que imitan entidades legítimas
Impacto técnico / operativo	Robo de credenciales
Medida de control / recomendada	Atentificaion del dominio
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	
Servicio X.800 Comprometidos	Confidencialidad de datos, integridad de datos, disponibilidad
Definiciones aplicables RFC 4949.	destructive Attack: "Ataque diseñado para causar daño físico o lógico permanente
Tipo de amenaza	Externa
Vector de ataque	Código malicioso específico para borra/sobrescribir datos
Impacto técnico / operativo	Pérdida total de datos

Medida de control / recomendada	Deteccion temprana y respuesta inmediata
--	--

Conclusiones

Como conclusión puedo obtener que existen muchas variables y vulnerabilidades que se pueden explotar y con esto puedo identificar muchas de ellas para poder tener más conocimiento al respecto e intentar evitar esos fallos en la seguridad en el futuro.

Referencias

- 1) [RFC 4949 - Glosario de Seguridad en Internet, Versión 2](#)