Laboratorio 13 Cursos Ciberseguridad

Sesión #13 Escaneo de vulnerabilidades

Jesús Rodrigo Toro Navarro

Universidad Popular del Cesar

Facultad de Ingeniería y Tecnológica

Instrucciones para cada caso (lo que deben hacer los estudiantes):

1. Identificar activos críticos.
2. Describir amenazas y vulnerabilidades.
3. Estimar impacto y probabilidad.
4. Calcular el nivel de riesgo (puede ser cualitativo o con matriz).
5. Determinar si el riesgo es aceptable.
6. Proponer un plan de tratamiento.
7. Definir responsables y tiempo estimado.
8. Proponer mecanismos de monitoreo.
9. Redactar conclusiones y recomendaciones.

CASO 1: Robo de credenciales por phishing en una entidad educativa

Escenario:

Un estudiante recibe un correo aparentemente institucional con un enlace a una supuesta plataforma de calificaciones. Al ingresar sus credenciales, estas son capturadas por un tercero. Al día siguiente, se detecta que alguien accedió con esas credenciales a los registros de notas y los modificó.

Detalles clave:

• Plataforma afectada: sistema académico web.

• No existe segundo factor de autenticación (2FA).

• No hay filtros de spam o análisis de enlaces en los correos entrantes.

• Usuarios no han recibido capacitación en ciberseguridad.

1. Activos críticos
    - Sistema académico web.
    - Credenciales de usuarios.
    - Información académica (notas, registros de estudiantes).
    - Correos electrónicos institucionales.
2. Amenazas y vulnerabilidades
    - Amenaza: Phishing (engaño por correo).

- Vulnerabilidades:
    - Falta de segundo factor de autenticación (2FA).
    - Ausencia de filtros de spam y análisis de enlaces.
    - Usuarios sin formación en ciberseguridad.
    - Ausencia de validación de sesiones sospechosas.

3. Impacto y probabilidad

- Impacto: Alto. Modificación de notas afecta la integridad académica e institucional.
- Probabilidad: Alta. Usuarios no capacitados + correos sin filtros = alto riesgo de éxito del ataque.

4. Nivel de riesgo (matriz cualitativa)

Impacto / Probabilidad	Baja	Media	Alta
Alta	Medio	Alto	Crítico

Nivel de riesgo: Crítico

5. ¿Riesgo aceptable?

- No. Riesgo crítico que compromete la integridad institucional.

6. Plan de tratamiento

- Implementar 2FA en todos los sistemas críticos.
- Configurar filtros antiphishing y análisis de enlaces en el correo institucional.
- Capacitación periódica en ciberseguridad para todos los usuarios.
- Revisión y validación de accesos y modificaciones en el sistema académico.

7. Responsables y tiempo estimado

- Área de TI: Implementación de 2FA, filtros y monitoreo (4 semanas).
- Área de Talento Humano / Dirección académica: Capacitación a usuarios (2 semanas).
- Responsable de seguridad informática: Revisión de logs y procedimientos (2 semanas).

8. Mecanismos de monitoreo

- Monitoreo de accesos inusuales en el sistema.

- Registro de cambios en notas con alertas automáticas.
- Auditorías periódicas de seguridad en los sistemas.
- Revisión de estadísticas de correos bloqueados y ataques detectados.

9. Conclusiones y recomendaciones

- El incidente evidenció fallas importantes en los controles preventivos de la entidad educativa.
- La capacitación de los usuarios y el uso de tecnologías como 2FA pueden reducir drásticamente la probabilidad de este tipo de ataques.
- Es fundamental establecer políticas de seguridad y monitoreo proactivo en todos los sistemas críticos.
- Se recomienda realizar simulacros de phishing para concientizar a los usuarios de forma continua.

CASO 2: Ransomware en una clínica odontológica

Escenario:

Un empleado abre un archivo adjunto en un correo que aparenta ser una factura. Inmediatamente, el sistema muestra un mensaje de que todos los archivos han sido cifrados. Piden un rescate en criptomonedas. La clínica no cuenta con respaldos automáticos actualizados.

Detalles clave:

• Archivos clínicos, administrativos y financieros cifrados.

• Software antivirus caducado.

• Sin políticas de copia de seguridad.

• Sin segmentación de red.

• El ransomware se propaga a todas las estaciones de trabajo.

1. Activos críticos

- Archivos clínicos, administrativos y financieros.
- Equipos de cómputo y red.
- Aplicaciones de gestión médica.
- Confianza de los pacientes.

2. Amenazas y vulnerabilidades

- Amenaza: Infección por ransomware a través de archivo adjunto.
- Vulnerabilidades:
    - Antivirus caducado.
    - Ausencia de backups actualizados.
    - Red sin segmentación (propagación total).
    - Políticas débiles de uso del correo y apertura de archivos.

3. Impacto y probabilidad

- Impacto: Muy alto (pérdida de información crítica).
- Probabilidad: Alta (múltiples vulnerabilidades evidentes).

Nivel de riesgo: Crítico

4. Nivel de riesgo

- Impacto: Muy alto (pérdida total de archivos).
- Probabilidad: Alta (múltiples vulnerabilidades).

Nivel de riesgo según matriz: Crítico

5. ¿Riesgo aceptable?

- No. Riesgo crítico con consecuencias directas sobre la operatividad y reputación.

6. Plan de tratamiento

- Implementar y mantener un antivirus actualizado.
- Establecer políticas de copias de seguridad automáticas y fuera de línea.
- Segmentar la red para limitar propagación.
- Capacitaciones de seguridad para empleados sobre correos sospechosos.

7. Responsables y tiempo estimado

- Área de TI / Soporte: Instalación de antivirus y rediseño de red (2-4 semanas).
- Gerencia / Administración: Compra de servidores de respaldo y licencias (3 semanas).
- Todo el personal: Capacitación básica en ciberseguridad (1 semana).

8. Mecanismos de monitoreo

- Panel centralizado de monitoreo antivirus.
- Verificación automática diaria de copias de seguridad.
- Monitoreo de tráfico inusual en la red.
- Informes mensuales de seguridad y cumplimiento.

9. Conclusiones y recomendaciones

- La falta de prevención y mantenimiento de seguridad básica permitió un ataque devastador.
- Es crucial establecer una política integral de respaldo y respuesta a incidentes.
- La formación de empleados y la implementación de tecnologías básicas (antivirus, backups) reduce significativamente la probabilidad de ataques exitosos.

CASO 3: Acceso no autorizado a cámara IP de una empresa

Escenario:

Una empresa de seguridad privada instala cámaras IP para monitoreo remoto. Sin embargo, no cambian las contraseñas por defecto ni actualizan el firmware. Un atacante logra visualizar transmisiones en vivo desde una interfaz web abierta al público.

Detalles clave:

• Acceso remoto habilitado vía HTTP sin autenticación segura.

• Firmware desactualizado con vulnerabilidades conocidas.

• Contraseñas por defecto (“admin/admin”).

• El sistema no genera alertas ni logs de acceso.

1. Activos críticos

- Cámaras IP de seguridad.
- Imágenes en tiempo real.
- Información de vigilancia privada.
- Red de monitoreo.

2. Amenazas y vulnerabilidades

- Amenaza: Acceso no autorizado y espionaje.
- Vulnerabilidades:

    - Contraseñas por defecto (“admin/admin”).
    - Firmware desactualizado.
    - Acceso remoto sin autenticación segura.
    - Falta de alertas y registros de acceso.

3. Impacto y probabilidad

- Impacto: Alto. Riesgo de violación de privacidad, espionaje y pérdida de confianza.
- Probabilidad: Alta. Múltiples vulnerabilidades abiertas y sin mitigación.

Nivel de riesgo: Crítico

4. Nivel de riesgo (matriz cualitativa)

- Impacto: Alto (vulneración de privacidad y posible espionaje).
- Probabilidad: Alta (contraseñas por defecto, sin actualizaciones).

Nivel de riesgo según matriz: Crítico

5. ¿Riesgo aceptable?

- No. El sistema está totalmente expuesto.

6. Plan de tratamiento

- Cambiar contraseñas por defecto.
- Actualizar firmware de todos los dispositivos.
- Implementar autenticación segura (HTTPS, VPN).
- Activar logs y alertas de acceso no autorizado.

7. Responsables y tiempo estimado

- Área técnica de seguridad / TI: Reconfiguración y actualización del sistema (1 semana).
- Gerente de operaciones: Supervisar cumplimiento y normativas (1 semana).
- Proveedor externo: Validar configuración segura (1 semana).

8. Mecanismos de monitoreo

- Registro de logs de acceso a cámaras.
- Alertas automáticas por accesos remotos.
- Escaneos de vulnerabilidades periódicos.

- Informes mensuales de integridad del sistema.

9. Conclusiones y recomendaciones

- La falta de buenas prácticas básicas de seguridad expuso un sistema crítico a ataques externos.
- Es fundamental realizar configuraciones iniciales seguras y mantener el firmware actualizado.
- Las cámaras IP deben estar aisladas en redes segmentadas, con accesos controlados y auditables.

CASO 4: Uso indebido de información personal en una alcaldía

Escenario:

Un contratista accede a bases de datos con información personal de ciudadanos para “validar datos”. Después se descubre que vendía esta información a una empresa de marketing. La alcaldía no tenía controles para registrar el acceso a datos sensibles.

Detalles clave:

• No existen registros de logs ni auditoría.

• Acceso a bases de datos sin niveles de privilegio.

• Sin política de clasificación de la información.

• No se realizaron acuerdos de confidencialidad con el contratista.

1.Activos críticos

- Bases de datos de información personal de ciudadanos.
- Reputación institucional.
- Sistemas administrativos.

2. Amenazas y vulnerabilidades

- Amenaza: Uso no autorizado y venta de datos personales.
- Vulnerabilidades:
    - No hay logs de acceso ni auditorías.
    - Acceso sin niveles de privilegio.
    - Ausencia de clasificación de la información.
    - No existen acuerdos de confidencialidad firmados.

3. Impacto y probabilidad

- Impacto: Muy alto. Violación de datos personales puede acarrear sanciones legales.
- Probabilidad: Alta. Accesos abiertos y sin controles.

Nivel de riesgo: Crítico

4. Nivel de riesgo (matriz cualitativa)

- Impacto: Muy alto (filtración de datos personales con implicaciones legales).
- Probabilidad: Alta (no hay controles de acceso ni registros).

Nivel de riesgo según matriz: Crítico

5. ¿Riesgo aceptable?

- No. Riesgo crítico con implicaciones legales y reputacionales.

6. Plan de tratamiento

- Establecer políticas de acceso por roles (principio de menor privilegio).
- Implementar sistema de auditoría y registro de accesos.
- Clasificar la información según sensibilidad.
- Firmar acuerdos de confidencialidad con todos los contratistas.

7. Responsables y tiempo estimado

- Área jurídica: Redacción y firma de acuerdos de confidencialidad (1 semana).
- Área de TI: Implementación de control de accesos y logs (2 semanas).
- Gerencia administrativa: Clasificación y protección de la información (2 semanas).

8. Mecanismos de monitoreo

- Registro de logs de acceso a bases de datos.
- Alertas por acceso a datos sensibles.
- Auditorías mensuales.
- Informes periódicos de cumplimiento normativo.

9. Conclusiones y recomendaciones

- La falta de controles básicos de acceso y supervisión permitió un uso indebido de información sensible.

- Las entidades públicas deben cumplir con la legislación sobre protección de datos personales.
- Se recomienda implementar controles técnicos, legales y administrativos.

CASO 5: Corte de servicio por ataque DoS a sitio web institucional

Escenario:

El sitio web de una universidad sufre una caída durante el proceso de inscripciones. El análisis revela un ataque de denegación de servicio (DoS) lanzado desde múltiples IPs, provocando la caída del servidor durante 8 horas.

Detalles clave:

• No existían medidas de mitigación como WAF o protección DoS.

• El servidor web estaba sobrecargado y sin alta disponibilidad.

• No había monitoreo en tiempo real.

• No se informó al área de sistemas hasta pasadas 3 horas.

1. Activos críticos

- Sitio web institucional.
- Infraestructura de servidores.
- Servicios de inscripción en línea.
- Reputación de la universidad.

2. Amenazas y vulnerabilidades

- Amenaza: Ataque de denegación de servicio (DoS).
- Vulnerabilidades:
    - No existe protección DoS/WAF.
    - Infraestructura sin alta disponibilidad.
    - Ausencia de monitoreo en tiempo real.
    - Notificación tardía al área técnica.

3. Impacto y probabilidad

- Impacto: Alto. Afectación directa a procesos académicos.
- Probabilidad: Media-Alta. Sitios institucionales son blanco frecuente.

→ Nivel de riesgo: Alto

4. Nivel de riesgo (matriz cualitativa)

- Impacto: Alto (interrupción del proceso de inscripción por 8 horas).
- Probabilidad: Media (infraestructura débil pero no constantemente atacada).

Nivel de riesgo según matriz: Alto

5. ¿Riesgo aceptable?

- No. Aunque no es crítico, sigue siendo un riesgo inaceptable en eventos importantes.

6. Plan de tratamiento

- Implementar un firewall de aplicaciones web (WAF).
- Migrar a arquitectura con alta disponibilidad.
- Establecer un sistema de monitoreo en tiempo real.
- Procedimiento de respuesta rápida ante incidentes.

7. Responsables y tiempo estimado

- Área de TI / Infraestructura: Configuración de WAF y balanceadores (3 semanas).
- Área académica: Coordinar procedimientos alternativos en caso de caída (1 semana).
- Soporte técnico: Establecer canales de comunicación para notificación temprana (1 semana).

8. Mecanismos de monitoreo

- Dashboards en tiempo real de carga del servidor.
- Alertas automáticas por tráfico anómalo.
- Reportes semanales de rendimiento del sitio web.
- Simulacros de incidentes.

9. Conclusiones y recomendaciones

- El impacto de este incidente pudo reducirse si existieran mecanismos de mitigación temprana.
- Las instituciones deben prepararse ante ataques DoS, especialmente durante eventos críticos.
- Es recomendable utilizar proveedores con infraestructura escalable y herramientas anti-DDoS.