Ethical Hacking

Introducción sobre un Pentesting

Ejercicio Número 1 Unidad 4:

En un hipotético escenario, tomando como ejemplo el hogar del alumno o el trabajo del mismo como el objetivo, ¿qué responderían a las siguientes preguntas?

1- ¿Que sucesos o incidentes impactarían más en su empresa/hogar?

2- ¿Cuáles son los activos claves a proteger? (información de los mismos)

3- ¿Cuáles son los procesos más importantes de la empresa/hogar?

4-¿Cuáles son los dispositivos y equipos más importantes?

5 y más importante: ¿qué dice el último informe de auditoría o alguna vez realizó un Pentest?

Voy a tratar de responder sobre mi lugar de trabajo, aunque no puedo dar demasiados detalles porque la información es confidencial, voy a simular alguna de ésta información, porque aún así es mucho más interesante que la red de mi casa. Se trata de una empresa que brinda servicios en la Nube a sus clientes.

Respuesta resumida:

1- ¿Que sucesos o incidentes impactarían más en su empresa/hogar?

Seria devastador el ataque de un ramsonware, la interrupción de los servicios que ofrecen los servidores, la vigilancia de la actividad de los empleados o la filtración de información.

2- ¿Cuáles son los activos claves a proteger? (información de los mismos)
   - Almacenamiento de software en desarrollo.
   - Toda información de la red interna detrás de la VPN. (base de datos de empleados, registros de visitas, reuniones, proyectos, etc).

3- ¿Cuáles son los procesos más importantes de la empresa/hogar?

- Servicio de almacenamiento en la nube para clientes externos.

4- ¿Cuáles son los dispositivos y equipos más importantes?

- Los servidores que se encuentran en la sala MDF.
- El sistema de refrigeración.
- Los UPS.

5 - ¿Qué dice el último informe de auditoría o alguna vez realizó un Pentest?

Unknown

Respuesta extendida:

1. ¿Qué sucesos o incidentes impactarían más en su empresa/hogar?

- **Filtración de credenciales**: Compromiso de claves de acceso y credenciales de API que puedan dar acceso no autorizado a los servicios de AWS.
- **Exposición de datos confidenciales**: Por ejemplo, filtración de datos almacenados en buckets de S3 que contengan información sensible, como datos de clientes.
- **Accesos no autorizados a recursos críticos**: Como bases de datos RDS, instancias de EC2 o almacenamiento S3 con datos sensibles o aplicaciones críticas.
- **Ataques DDoS (Denegación de Servicio Distribuido)**: Ataques que saturen los recursos y limiten el acceso a los servicios para los usuarios legítimos.
- **Configuración incorrecta de la seguridad**: Errores en la configuración de permisos de seguridad o redes, como políticas de IAM mal aplicadas o

grupos de seguridad de red que permitan acceso público a servicios internos.

- **Malware o Ransomware**: Instalación de software malicioso en instancias de EC2 o en redes privadas virtuales (VPC – Virtual Private Cloud), lo cual podría afectar tanto la integridad como la disponibilidad de los datos y servicios.

2. ¿Cuáles son los activos claves a proteger? (información de los mismos)

- **Buckets de S3**: Lugares donde se almacena información crítica de la empresa y de clientes.
- **Instancias de EC2**: Máquinas virtuales donde se ejecutan aplicaciones sensibles o que contienen datos importantes.
- **Base de datos RDS y DynamoDB**: Almacenan información confidencial y datos sensibles de usuarios, transacciones y aplicaciones internas.
- **Credenciales y políticas de IAM (Identity and Access Management)**: Administran los permisos y accesos a todos los recursos fundamentales para la seguridad de la plataforma.
- **Registros y Logs (CloudTrail, CloudWatch)**: Usados para monitorear actividades y auditar eventos, son cruciales para detectar y responder a posibles incidentes.
- **Funciones de Lambda**: Aplicaciones serverless que pueden contener código y lógica empresarial, su compromiso podría resultar en fuga de información o mal uso de los servicios.

3. ¿Cuáles son los procesos más importantes de la empresa/hogar?

- **Gestión de identidad y accesos (IAM)**: Controla quién puede acceder y qué pueden hacer en el entorno.
- **Monitoreo y respuesta a incidentes**: Monitoreo activo de logs con herramientas como CloudWatch y análisis de logs en CloudTrail para detectar actividades sospechosas.
- **Respaldo y recuperación de datos**: Procedimientos de backup de bases de datos y otros activos importantes en servicios como S3 o Glacier, para recuperación ante incidentes.
- **Pruebas de seguridad y auditorías periódicas**: Ejecución de pentests y auditorías de seguridad para evaluar vulnerabilidades en la configuración y servicios en la nube.

- **Gestión de la red y seguridad perimetral**: Configuración de VPC, subredes, y grupos de seguridad, estableciendo redes privadas y controlando el tráfico a nivel de firewall.

4. ¿Cuáles son los dispositivos y equipos más importantes?

- **Servidores locales**: Si existen, son los primeros puntos de conexión con la nube.
- **Dispositivos de red (routers, firewalls)**: Usados para conectar y proteger el acceso entre la red interna y los servicios.
- **Estaciones de trabajo de administradores**: Equipos desde los cuales los administradores y técnicos de seguridad configuran y monitorean los servicios.
- **Dispositivos de almacenamiento externo**: Para backups fuera del entorno de la nube, si se usa alguna infraestructura híbrida.

5. ¿Qué dice el último informe de auditoría o alguna vez se realizó un Pentest?

- **Configuración de permisos**: Se detectaron permisos excesivos asignados a algunas políticas de IAM, lo cual representa un riesgo de acceso indebido.
- **Contenedores de datos S3 mal configurados**: Algunos buckets tenían acceso público activado, exponiendo datos potencialmente confidenciales.
- **Instancias de EC2 sin cifrado**: No se utilizó el cifrado en instancias con datos críticos, lo que podría poner en riesgo la confidencialidad en caso de un ataque.
- **Múltiples cuentas con accesos privilegiados**: La auditoría recomienda reducir el número de usuarios con permisos de administración para minimizar los riesgos de escalación de privilegios.
- **Prácticas de hardening no aplicadas**: Algunos dispositivos y servicios, especialmente en entornos de desarrollo y pruebas, no tenían configuradas buenas prácticas de hardening (bloqueo de puertos innecesarios, autenticación multifactor, etc.).

Históricamente, la empresa ha realizado pentests anuales para evaluar sus niveles de seguridad en los servicios más críticos. El pentest más reciente incluyó evaluaciones en IAM, S3, EC2 y bases de datos, y recomendó algunas mejoras de configuración para reducir vulnerabilidades y fortalecer la protección de activos clave.

Rodrigo Vila,-