Unidad 0 – Precurso

Módulo 5
Metodologías de Ataque

THE BRIDGE DIGITAL TALENT ACCELERATOR

ÍNDICE

- ¿Qué es un APT?
- ¿Qué es un 0-day?
- Fases de un pentest
- MITRE ATT&CK Framework

APT

APT = Advanced Persistent Threat (Amenaza Persistente Avanzada)

Procesos informáticos organizados por un tercero (organización, grupo, estado…) con la intención y capacidad de atacar de forma avanzada y continuada en el tiempo, con un objetivo determinado.

- Organizadas por grupos con grandes recursos
- Quieren mantener el control de la infraestructura de forma contínua
- Usa varios vectores de ataque y persistencia para obtener y mantener el acceso.

0-Day

Tipo de vulnerabilidad que es o bien desconocida o bien no es posible gestionarla por aquellos interesados en mitigarla (usuarios, fabricantes, etc…)

Hasta que la vulnerabilidad pueda ser mitigada, los hackers pueden explotarla.

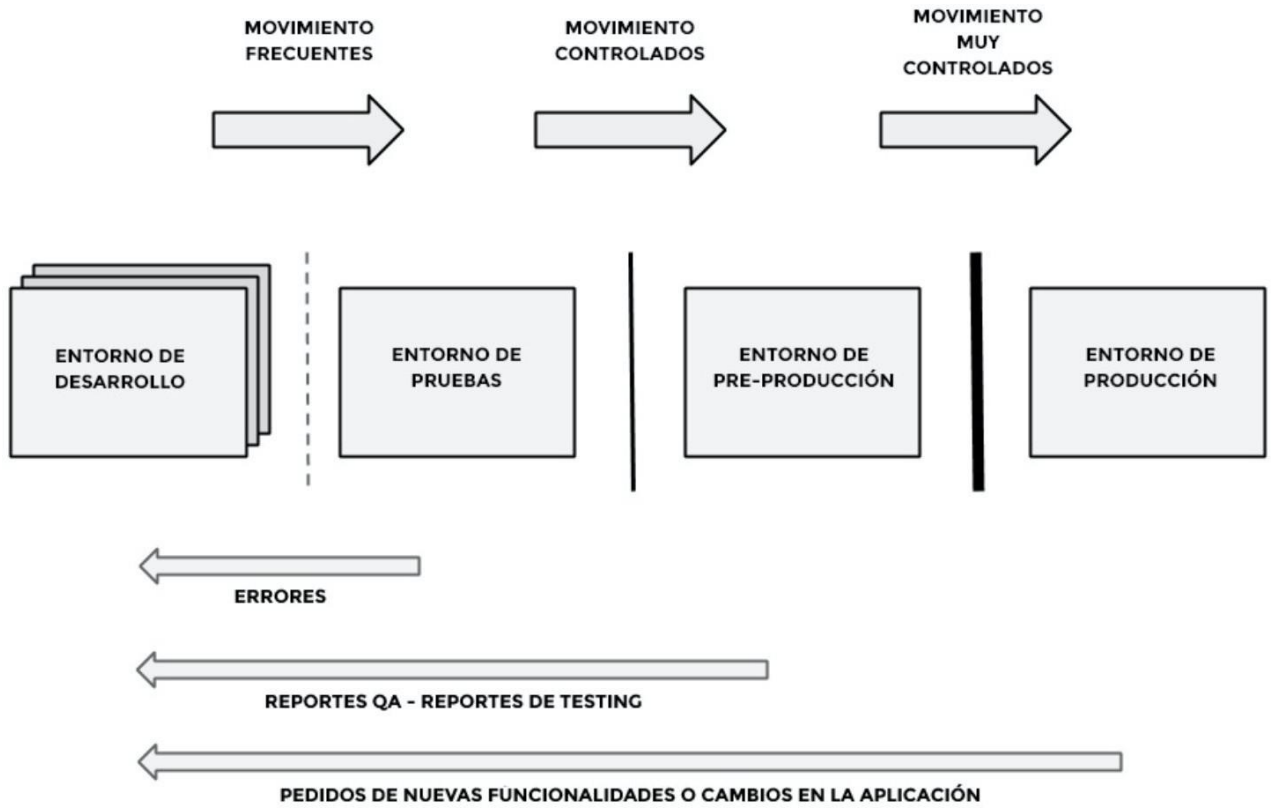
0-Day Exploit o 0-Day Attack es cuando existe un exploit que se aprovecha de una vulnerabilidad de tipo 0-Day.

NIVELES DE UN ENTORNO DE DESARROLLO

1. Entorno o servidor de desarrollo

2. Entorno o servidor de pre-producción

3. Entorno o servidor de producción



FASES DE UN INFORME PENTEST

Fase 1 : Definición de alcance y requisitos del proyecto
Fase 2 : Recolección de información
Fase 3 : Modelado de amenaza y estrategias de penetración
Fase 4 : Análisis de vulnerabilidades

1. : Exploración
2. : Evaluación

Fase 5 : Explotación de vulnerabilidades
Fase 6 : Post-explotación
Fase 7 : Conclusiones, retrospectiva…

FASE 1 : DEFINICIÓN DE ALCANCE Y REQUISITOS

Habitualmente esta fase se realiza junto al cliente o responsable del cliente.

1. **Objetivos del análisis**
   - ¿Cuáles son los servicios críticos para la empresa?
   - ¿Cuáles supondrían un mayor problema en caso de ataque?

2. **Ámbito y alcance del análisis**
   - ¿Qué IPs, servicios o dispositivos se van a incluir en las pruebas? ¿Son internos o externos a la red de la empresa?
   - ¿Trabajaremos sobre el entorno de preproducción o sobre producción?
   - ¿Se pueden explotar las vulnerabilidades encontradas o únicamente identificarlas?
   - ¿Hay algún tiempo de ejecución que deba ser tenido en cuenta?

FASE 1 : DEFINICIÓN DE ALCANCE Y REQUISITOS

Habitualmente esta fase se realiza junto al cliente o responsable del cliente.

3. Disponibilidad

- ¿Se puede realizar el pentest en cualquier momento, o tiene que ser en algún horario concreto? (Sobre todo la fase de explotación)
- ¿Cuál sería la persona de contacto en caso que se encuentre alguna vulnerabilidad crítica para la empresa que deba ser notificada de inmediato?

FASE 2 : RECOLECCIÓN DE INFORMACIÓN

Obtención de información relacionada con el recurso disponible para identificar los programas y sistemas utilizados, actividades de empleados en redes sociales, correos electrónicos, credenciales... utilizando técnicas **pasivas** de extracción de información. De esta manera se permite empezar a delimitar las áreas sobre las que luego se focalizará el modelo de amenaza y las estrategias de penetración.

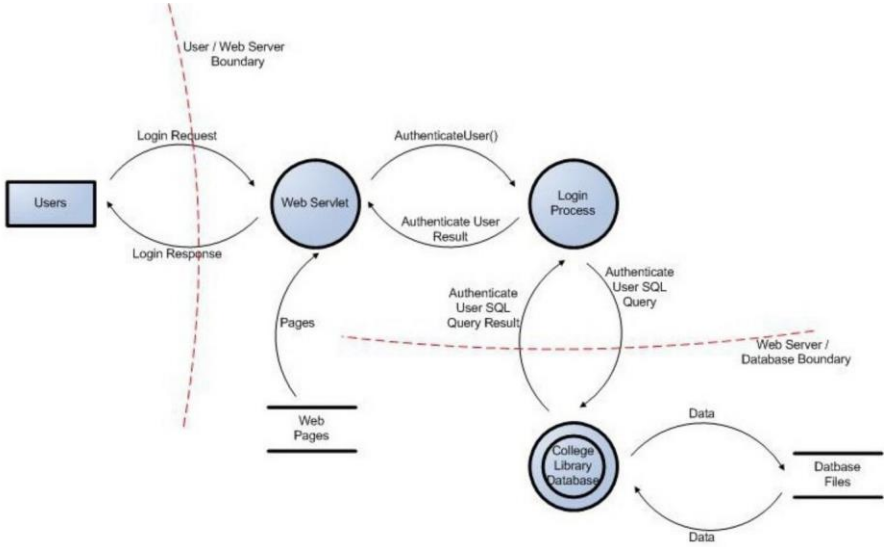
Ejemplos:

- Rangos de direcciones IP asignados
- Dirección física de la empresa
- Nombres de personal técnico
- Direcciones IP de servicios de terceros
- Números telefónicos
- Cuentas de correo electrónico y credenciales filtradas
- Instituciones, Organizaciones o Compañías vinculadas
- Análisis de la web principal : módulos que contiene, mapa de la web
- Incidentes de seguridad informática reportados

FASE 3 : MODELADO DE AMENAZA Y ESTRATEGIAS

A partir de la información recogida, se definen las estrategias de penetración, objetivos y maneras de conseguirlos.

¿Donde el sistema es más vulnerable? ¿De qué manera podemos atacarlo?



FASE 4 : ANALISIS DE VULNERABILIDADES

Valoración y validación de las estrategias de penetración definidas. Está dividida en dos fases:

1. - Fase de Exploración
2. - Fase de Evaluación

FASE 4.1 : EXPLORACIÓN

Se realiza una exploración utilizando técnicas **activas** de reconocimiento.

Ejemplos de exploración:
- Confirmación de rangos de direcciones IP
-Detección de equipos activos e identificación de Sistemas Operativos
-Detección de servicios activos e identificación de Software y versiones
- Detección de sistemas de protección

FASE 4.2 : EVALUACION

Se realiza una evaluación y análisis de todos los datos encontrados para determinar las vulnerabilidades que afectan a los sistemas.

Ejemplos de evaluación:

- Ejecución de herramientas de scanning de vulnerabilidades.
- Búsqueda y verificación manual de vulnerabilidades.
- Enumeración de usuarios y datos de configuración.

FASE 5 : EXPLOTACIÓN DE VULNERABILIDADES

Ejecución de exploits contra las vulnerabilidades identificadas o credenciales obtenidas en las fases anteriores para conseguir acceso a los sistemas y obtener el control de los mismos.

Ejemplos de explotación :

- Credenciales de usuario de equipos
- Exploits remotos
- Recursos compartidos
- Aplicaciones web vulnerables
- Ejecución de código remoto
- Búsqueda de información de accesos en recursos compartidos
- Fuerza bruta sobre sistemas de autenticación

FASE 6 : POST-EXPLOTACIÓN

Intento de conseguir el máximo nivel de privilegios, información de la red y acceso al mayor número posible de sistemas identificando qué tipo de datos y/o servicios tenemos a nuestro alcance.

Ejemplo de post-explotación :

- Elevación de privilegios
- Movimientos laterales a otras subredes/equipos

FASE 7 : CONCLUSIONES EN EL INFORME FINAL

Presentación de resultados al cliente marcando aquellos puntos en los que la seguridad se haya implementado de manera correcta y aquellos que deben de ser corregidos y de qué manera.

De manera habitual se realizan **dos** informes, uno **ejecutivo** con explicación general y otro **técnico** con descripciones más detalladas, aunque dependerá de los requisitos del proyecto.

FASE 7 : INFORME FINAL

Presentación de resultados al cliente marcando aquellos puntos en los que la seguridad se haya implementado de manera correcta y aquellos que deben de ser corregidos y de qué manera.

De manera habitual se realizan **dos** informes, uno **ejecutivo** con explicación general y otro **técnico** con descripciones más detalladas, aunque dependerá de los requisitos del proyecto.

MITRE ATT&CK FRAMEWORK

ATT&CK significa "*Adversarial Tactics, Techniques, and Common Knowledge.*" Es un repositorio de documentación sobre tácticas, técnicas y procedimientos que los APT utilizan contra infraestructuras.

Las técnicas ("el cómo") se agrupan en un conjunto de tácticas ("el por qué") para explicar el contexto en el que utilizan.

https://attack.mitre.org