Pruebas de penetración (cómo se ve los ataques)

↳ sirven para evaluar la seguridad que ya tenemos, ver alrance evaluar la seguridad de red, reportar para tomar acciones

- reportes buenos → que tienen que hacer
- Técnicas comúnes usadas por ciberdelincuentes en sistemas informáticos, para encontrar vulnerabilidades y bajo un esquema controlado, explotarlas
- Proceso de forma sistemática, de forma profesional y Segura
- Definir un alcance claro y específico
- Evaluar riesgo (con reporte)

M-Trends

- Vulnerabilidad tiene un ciclo
- Pruebas de penetración: En función del conocimiento previo de la información, por su ubicación en la ejecución, por su alcance
  - Caja negra → No se provee info del sistema o red
    ↳ Similar a un ataque externo
  - Caja blanca → acceso a Configuraciones de aplicaciones o código fuente
    Su objetivo es identificar posibles fallas en las configuraciones
  - Caja gris → Similar a la negra pero con un poco de info sobre el sistema arqui de red

Ubi:

- Externas: Fuera del perimetro de la organicación
  - Muestra vulnerabilidades que podrían ser explotadas por un atacante externo
- Internas: Dentro de la red de la organización,
  Permite identificar vulnerabilidades que puede explotar una persona dentro de la organización.

Alcance:

Pruebas de seguridad física, servicio de red, inalámbrica (seguridad), aplicaciones

web, ingeniería social

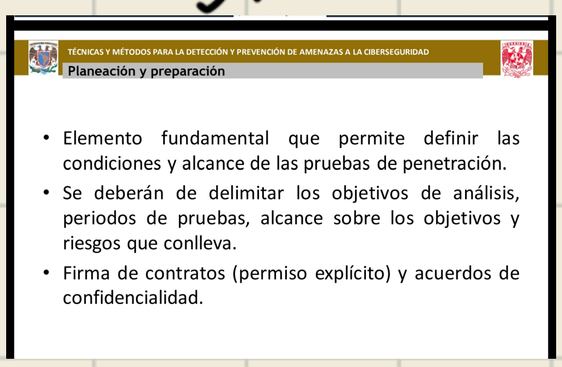
- PTES (Penetration Testing Execution Standard)
  - Consta de 7 fases
  - Cuenta con recomendaciones, técnicas practicas, así como también procedimientos y recomendaciones para el uso de herramientas para las pruebas de penetración

- OSSTMM → Metodología de acceso libre, que se basa en el tipo de alcance
- NIST 800-115
- Penetration Test Framework (PTF)

• Metodologías comerciales (EC Council, SANS Institute, Offensive Security)

Fases para la aplicación de pruebas de penetración

- Planeación y preparación (No forma como tal de la revisión)
  - P y P
- Reconocimiento
- Escaneo
- Explotación
- Documentación



- Reconocimiento: Proceso de investigación sobre la organización a evaluar, para reunir la mayor cantidad de info al respecto

Shodan escaneando internet público (buscamos unam.mx

Netcraft? Sobre páginas web https

built with : Ayuda identificar que bibliotecas tiene el sitio

↳unam prohibido

traceroute

Escaneo : encontrar entrada vulnerable del objeto de evaluación, punto de acceso inalámbrico

barrido de red nmap (ip tuya)

nmap 197.168.163.179/24

especificar puertos nmap -F

sistema operativo nmap -O

escaneo de versiones -SV

escaneo de vulnerabilidades