Guardia Civil

Mando de Apoyo

Jefatura de Servicios Técnicos

Seguridad en las Tecnologías de la Información y la comunicación

SEMINARIO DE AUDITORÍA DE SEGURIDAD

ACADEMIA DE INGENIEROS

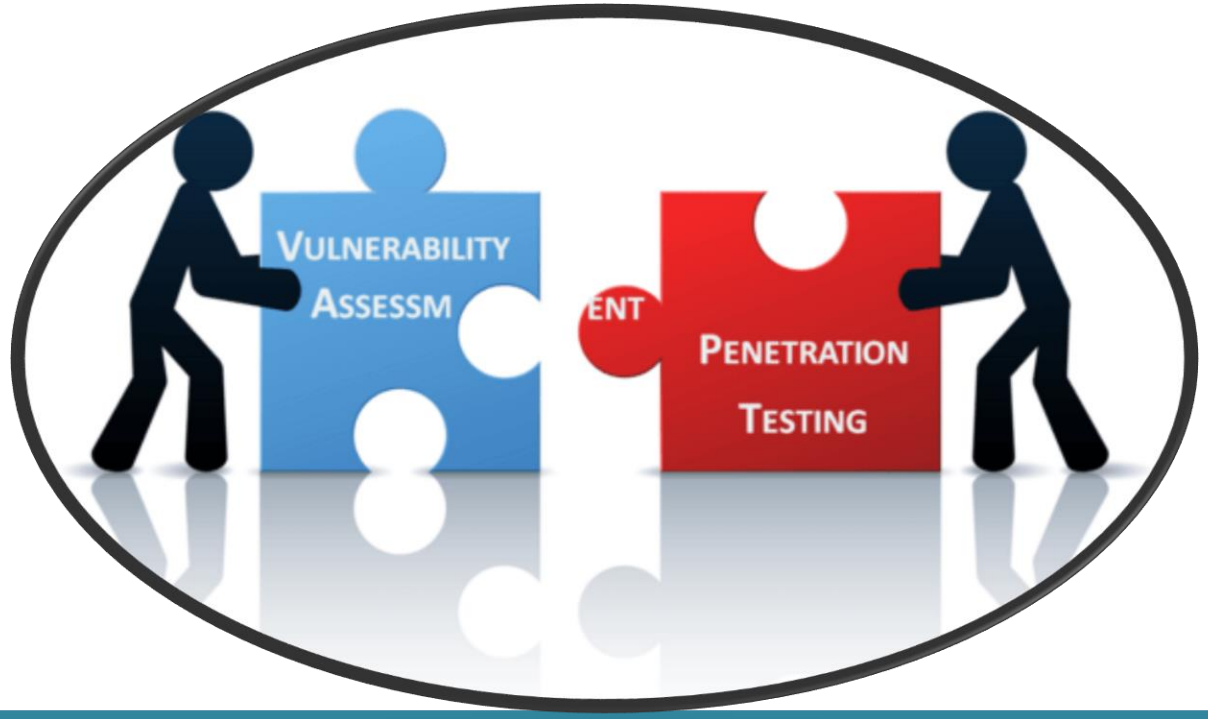
Capitán GC Jesús
S. Cano Carrillo

Estado de Alarma, 15 de junio de 2020


SI VEO QUE TARDAS CON LOS DE LA AUDITORIA, ¿LLAMO A TU OFICINA O PREGUNTO EN LA POLICIA?

Auditoría de seguridad

- Un estudio de seguridad de los sistemas de información, el estado de todos los activos y ver puntos débiles con el objeto de establecer medidas correctivas o preventivas.

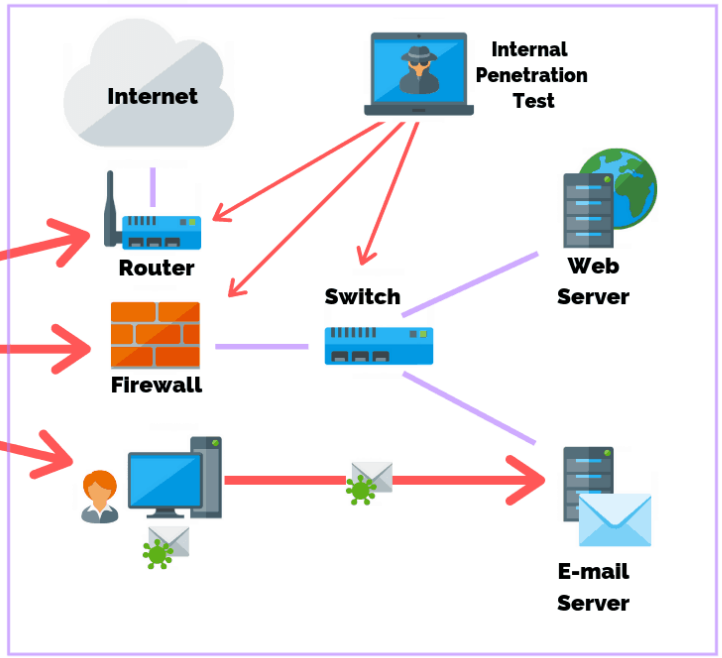


Actividades de una auditoría de seguridad

- Cumplimiento de estándares (ENS, ISO 27.000, LOPD-RDD/R(UE) 2016/679, Cobit, etc.)
- Redes
- Sistemas operativos
- Servicios y aplicaciones
- Vulnerabilidades
- Salvaguardas correctivas
- Recomendaciones

Tipos de auditorías

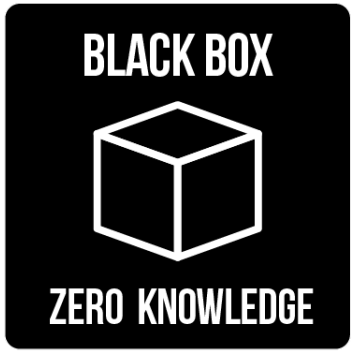
- Auditoría de Desarrollo (Código limpio)
- Auditoría interna
- Auditoría perimetral
- Auditoría web (i.e. OWASP)
- Auditoría especializada (wifi, cookies, exfiltraciones, malware, ramsonware…)
- Pentesting (complementario del anterior)
- Auditoría post-mortem
- Auditoría forense digital

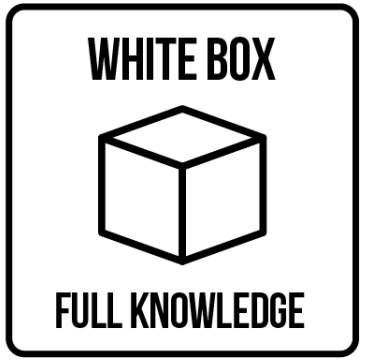


Img: purplesec.us

Pentesting

- Prueba de Penetración = proceso de evaluación/auditoría de seguridad de alto nivel
- Metodología = conjunto de reglas, prácticas, procedimientos y métodos
- Hoja de ruta → ideas útiles y prácticas
- Tipos:
  - De caja negra
  - De caja blanca
  - De caja gris





Img: mile2.com

Blackbox Pentesting

- Se da una URL o IP
- Intrusión web externa
- Ninguna otra información de la organización
- “Simula” o “se parece” a un hacker real
- Requiere autorización/acuerdo expreso
- Cuidado con aplicaciones reales propias o de terceros
- La auditoría es bastante autónoma → Bajo esfuerzo interno de la organización
- En coste, no es barato +$$$$ pero no requiere tanto esfuerzo interno -$$$$.
- Pero es una auditoría que necesita su tiempo y los resultados no son los mejores ni la profundidad (a veces falsos positivos, consideraciones genéricas no reales)

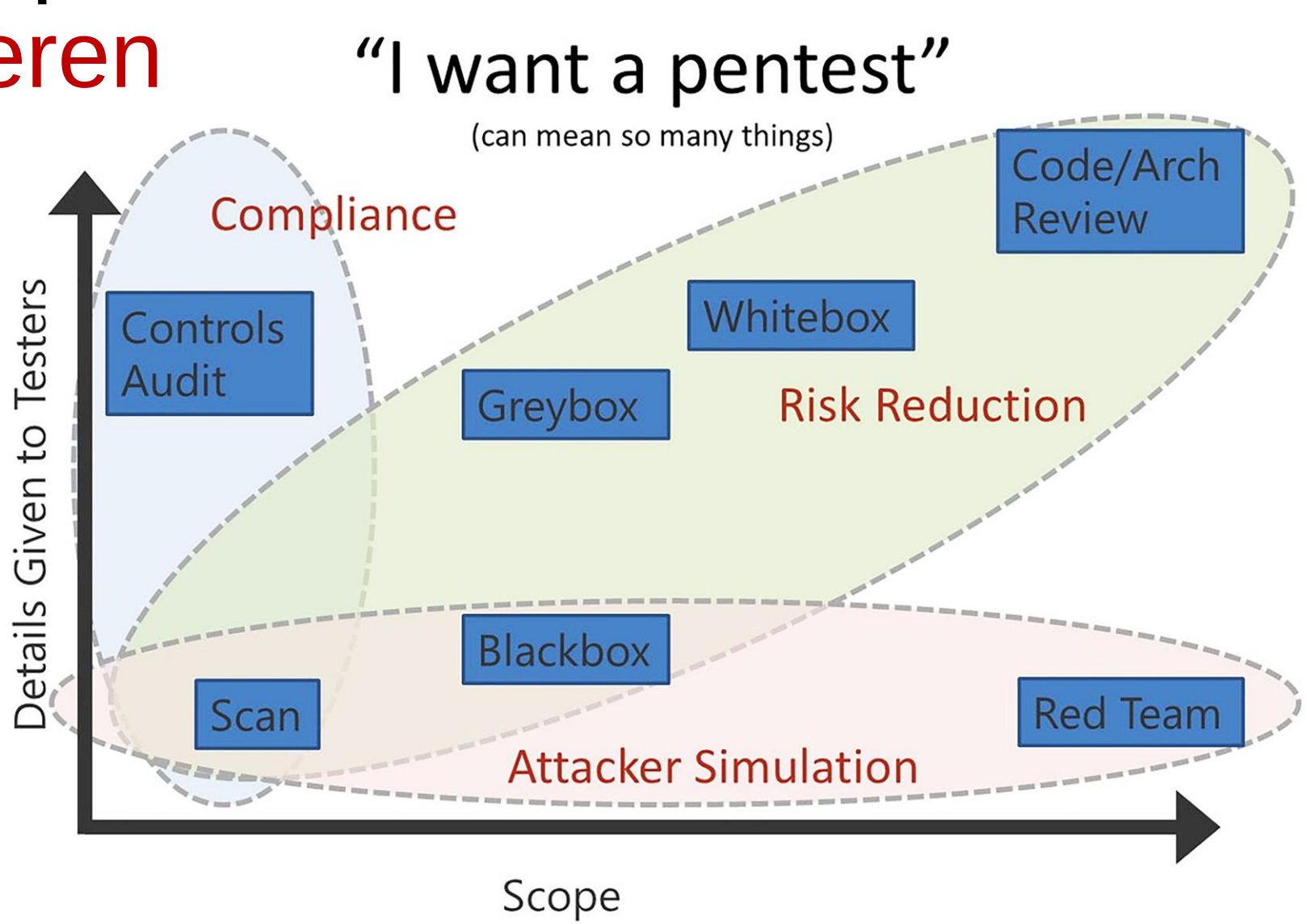
Whitebox Pentesting

- Con conocimientos de redes, sistemas, hardware u otros detalles
- Ahorra tiempo de la fase de “reconocimiento”
- Pentester puede hablar con desarrolladores/técnicos
- Depende del nivel de detalle/criticidad → Equipos internos → --$$$$
- Obligatoriamente en Crystal Pentesting
- Puede integrarse en el proceso/ciclo de desarrollo software institucional
- Requiere una alta implicación de la organización: el auditor va muy tutorizado → Es una auditoría relativamente rápida si fluye
- Resultados y profundidad de la auditoría de gran calidad (lo mejor)

Grey Pentesting

- Con conocimientos parciales
- Comunicación básica para aclaras algunas dudas
- Alcance definido previamente → p.ej. Aplicaciones web
- Por ello, alcance + conocimiento ➔ Testing rápido
- Puede “parecerse” a un ataque insider (depende de)
- Coste/Resultado: normalmente el que más interesa
- Calidad del resultado normalmente satisfactoria (alcance)
- Requiere cierta implicación de nuestra organización (dirección seguridad tic)

Bueno sí, pero ¿qué quieren ustedes?



Img: underdefense.com

Kali

- Plataforma Linux de Auditoría de Seguridad
- Creada en 2013, con sabor a Debian, con multitud de herramientas (https://tools.kali.org)
- Evolución de Backtrack
- Requiere conocimientos previos: fundamentos de seguridad y de sistema operativo

Bibliografía de interés

#	Material	pp	tipo
01			web
02	Metasploitable2 https://sourceforge.net/projects/metasploitable/files/Metasploitable2/		web
03	Metasploitable 3. https://github.com/rapid7/metasploitable3		web
04	Metasploitable https://www.vulnhub.com/entry/metasploitable-1,28/		web
05	Sitio Web: https://www.vulnhub.com/		web
06	Centro de evaluación de Microsoft. Sitio Web: https://www.microsoft.com/en-us/evalcenter/		web
07			web
08			web

ACADEMIA DE INGENIEROS

Seminario sobre auditoría de ciberseguridad

Capitán GC Jesús S. Cano Carrillo