ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

Metodologías de Test de Intrusión

OSSTMM e ISSAF

Florencio Cano Gabarda

SEINHE

¿Qué es ISACA?

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Auditoría y Control de los Sistemas de Información
- Desarrolla estándares relacionados
- Administra las certificaciones CISA, CISM, CGEIT

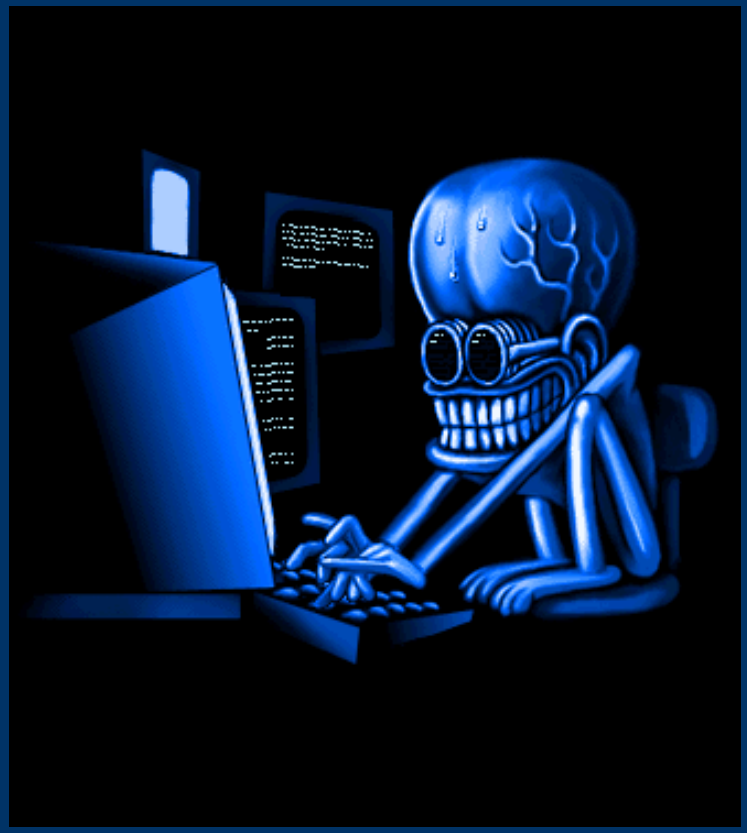
ISACA: Eventos

- Charlas Técnicas
- Cervezas con ISACA
- Jornadas Rafael Bernal

HISTORIA

- Origen de la palabra “hacker”
- Hacker vs Cracker

ISACA®
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter



ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

ISSAF – Penetration Testing Framework

ISSAF

- FASE 1: PLANIFICACIÓN Y PREPARACIÓN
- FASE 2: ANÁLISIS
- FASE 3: INFORMES Y LIMPIEZA

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

FASE 1: PLANIFICACIÓN Y PREPARACIÓN

FASE 1: PLANIFICACIÓN Y PREPARACIÓN

- Intercambio de información entre las partes
- Acuerdo

FASE 1: PLANIFICACIÓN Y PREPARACIÓN

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Identificación de contactos
- Definición del alcance, proceso y metodología
- Acuerdo sobre casos específicos y posibles escalados

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

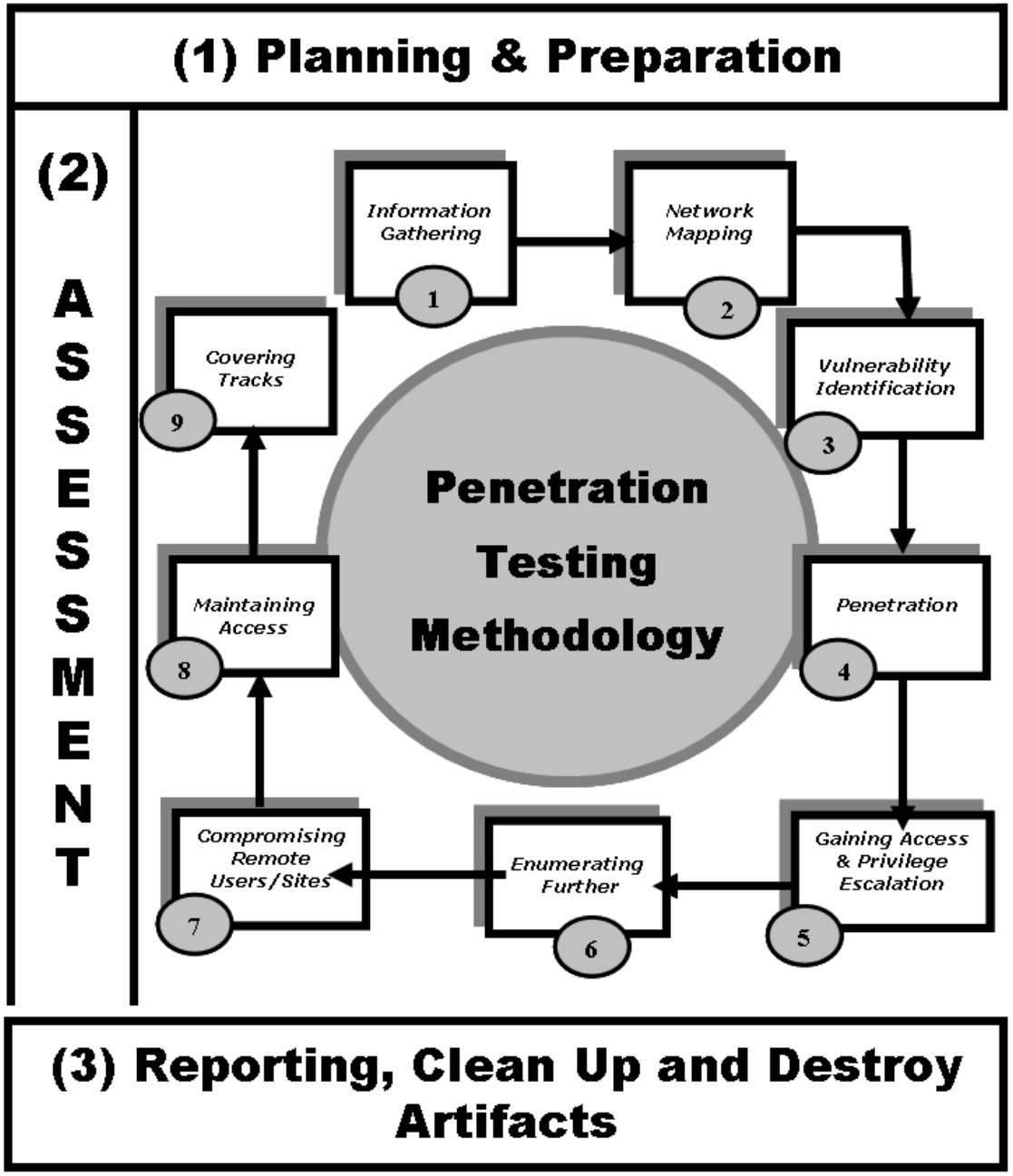
FASE 2: ANÁLISIS

FASE 2: ANÁLISIS

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Recopilación de información
- Mapeo de la red
- Identificación de vulnerabilidades
- Intrusión
- Obtención de acceso y escalada de privilegios
- Obtención de información adicional
- Compromiso de usuarios/sistemas remotos
- Mantenimiento del acceso
- Borrado del rastro

Approach & Methodology



FASE 2: ANÁLISIS – Recopilación de Información

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Buscadores (Google, Yahoo, Curl, Dogpile, Copernic, eInforma, etc.)
- WHOIS, DNS

FASE 2: ANÁLISIS – Mapeo de la Red

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Encontrar sistemas activos
- Escaneo de puertos y servicios
- Mapeo del perímetro de la red (routers, firewalls, etc.)
- Identificación de servicios críticos
- Identificación de los sistemas operativos y versiones
- Identificación de servicios y versiones

FASE 2: ANÁLISIS – Identificación de Vulnerabilidades

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Identificar servicios vulnerables a través de sus banners
- Realizar un escaneo automatizado de vulnerabilidades
- Realizar una verificación para evitar falsos positivos y negativos
- Listar vulnerabilidades encontradas
- Estimar el impacto potencial
- Identificar posibles ataques y escenarios para llevarlos a cabo

FASE 2: ANÁLISIS – Intrusión

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Encontrar código/herramientas de prueba de concepto (poc)
- Desarrollar scripts/herramientas propios
- Adaptar código existente a nuestro objetivo
- Usar el código de demostración contra el objetivo
- Documentar elementos encontrados

FASE 2: ANÁLISIS – Obtención de Acceso y Escalada de Privilegios

- Obtención de acceso
  - Obtención de acceso con mínimos privilegios
    - Descubrimiento de usuario/contraseña
    - Contraseñas en blanco o contraseñas por defecto
    - Aprovechar vulnerabilidades en parámetros estandar
    - Recursos públicos que admiten ejecutar ciertos comandos en el sistema
  - Intrusión en sistemas intermedios
  - Intrusión del sistema objetivo

FASE 2: ANÁLISIS – Obtención de Acceso y Escalada de Privilegios

- Escalada de privilegios

FASE 2: ANÁLISIS – Obtención de Información Adicional

- Obtener contraseñas encriptadas para crackearlas offline
- Obtener contraseñas por sniffing
- Sniffing y análisis de tráfico
- Recopilación de cookies para realización de ataques
- Recopilación de direcciones de correo
- Identificación de redes y rutas
- Mapeo de la red interna

FASE 2: ANÁLISIS – Compromiso de usuarios/sistemas remotos

- La intrusión en máquinas de usuarios remotos o en sistemas remotos de confianza puede equivaler a la intrusión en la red interna

FASE 2: ANÁLISIS – Mantenimiento del acceso

- Instalación y despliegue:
  - Canales secretos
    - ICMP Tunnel
  - Puertas traseras
  - Rootkits
- No suele hacerse en un test de intrusión habitual
  - Un usuario malicioso podría encontrarlas y aprovecharlas

FASE 2: ANÁLISIS – Borrado rastro

- Ocultación de ficheros
- Modificación o borrado de logs

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

FASE 3: INFORMES Y LIMPIEZA

FASE 3: INFORMES Y LIMPIEZA

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Informe final
  - Resumen ejecutivo
  - Alcance del proyecto
  - Herramientas y exploits
  - Fechas y horas
  - Todas las salidas devueltas por las herramientas probadas
  - Listado de vulnerabilidades encontradas junto con posibles soluciones para cada una de ellas

FASE 3: INFORMES Y LIMPIEZA

- Eliminación de todo el código y herramientas empleadas

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

OSSTMM: OPEN-SOURCE SECURITY TESTING METHODOLOGY MANUAL

OSSTMM

- Cuando testear es tan importante como qué y por qué testear
- Hay que sacar todo el jugo a cualquier pequeño detalle
- Hay que hacer más con menos
- No subestimar cualquier tipo de Política de Seguridad
- Lo que ellos obtengan depende de cómo tú se lo proporciones

OSSTMM

- Objetivo principal:
  - Proveer una metodología científica para la correcta caracterización de la seguridad mediante examinación y correlación de un modo consistente y fiable
- Objetivo secundario
  - Proveer guías que de ser seguidas por un auditor propocionen una auditoría certificada OSSTMM

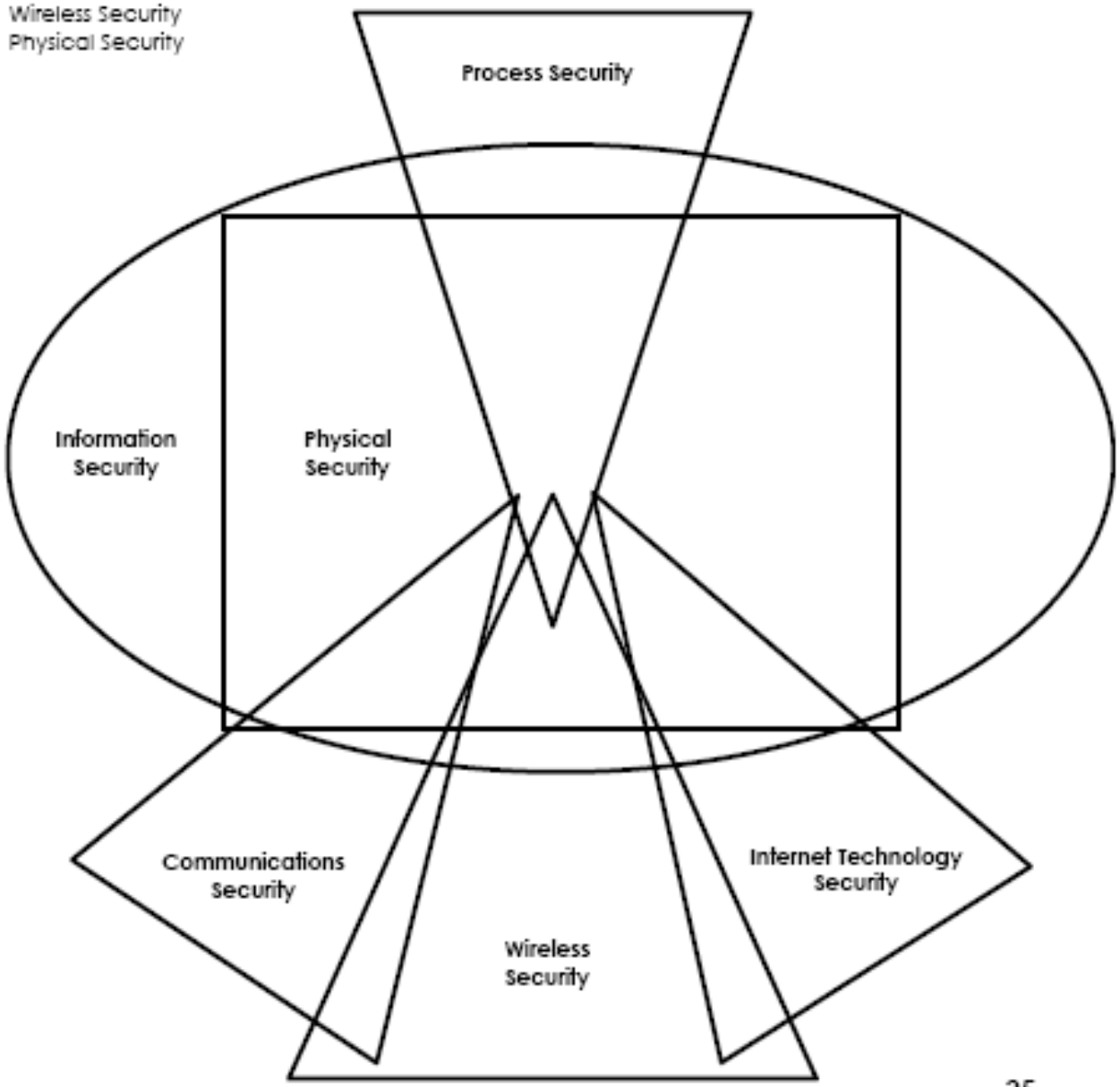
OSSTMM: Tipos de Tests de Seguridad

- Ciego
- Doble Ciego (Caja Negra)
- Caja Gris
- Doble Caja Gris (Caja Blanca)
- Tandem
- Inverso

OSSTMM: Conformidad

- Legislación
  - LOPD
  - LSSICE
- Regulación
- Políticas
  - ISO/IEC 27001

4. Communications Security
5. Wireless Security
6. Physical Security



OSSTMM: Secciones

- Testeo de la Seguridad de la Información
- Testeo de la Seguridad de los Procesos
- Testeo de la Seguridad de la Tecnología de Internet
- Testeo de la Seguridad en las Comunicaciones
- Testeo de la Seguridad Inalámbrica
- Testeo de la Seguridad Física

Module Example

Module Name
Description of the module.

Expected Results:	Item Idea Concept Map

Group task description.
- Task 1
- Task 2

Ejemplo: Inicio de un Test de Intrusión

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

- Recopilación de Información: eInforma
- Escaneo de puertos: PullThePlug