Iván Arce | ivan.arce@corest.com

Prácticas y Tecnologías de Seguridad Informática

El estado del arte actual

CORE SECURITY TECHNOLOGIES

Agenda

- El estado actual: Prácticas
  - Penetration Tests
- El estado actual: Herramientas
  - Vulnerability Scanners
  - Intrusion Detection Systems (IDS)
  - Otras herramientas
- El futuro
- Conclusiones

Penetration Tests

PT

Definición

- Un intento localizado y limitado en el tiempo de vulnerar la arquitectura de seguridad utilizando las tecnicas del atacante

Objetivos

- Concientización interna
- Identificar el riesgo
- Mitigar el riesgo
- Mejorar los procesos de seguridad
- Ayudar a la toma de decisiones

Requerimientos

- Definir objetivos
- Definir alcance
- Definir modalidad de la prueba
- Consensuar tiempos
- Consensuar resultados esperados

Ejecución

- Etapas de ejecución:
  - Obtención de información
  - Analisis de información y planeamiento
  - Detección de vulnerabilidades
  - Intrusión
  - Escalada de privilegios y ataques
  - Análisis y reporte de resultados
  - Limpieza

Resultados: Informe Final

- Descripción clara del alcance y la metodología utilizada
- Ejecución reproducible y verificable
- Análisis de alto nivel y reporte para el management no técnico
- Recomendaciones generales y conclusiones
- Detalle de vulnerabilidades encontradas

El estado actual

- Ausencia de herramientas que contemplen todas las etapas del PenTest
- Ausencia de herramientas específicas para algunas etapas específicas
- Requiere un alto nivel de conocimientos y experiencia
- No es facil formalizar y definir una metodologia standard
- Práctica mas cercana a lo artesanal que a lo profesional
- Alto costo
- Baja confiabilidad

Vulnerability Scanners

Definición

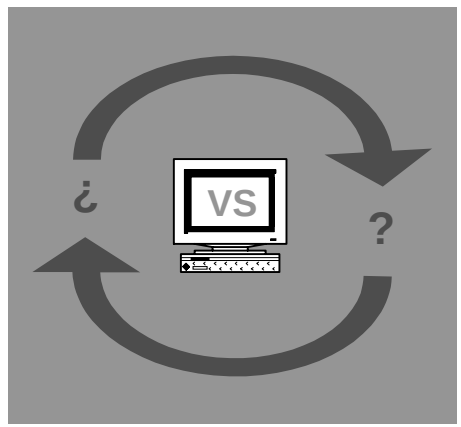
- Herramienta automatizada para la detección de vulnerabilidades conocidas en un entorno tecnológico determinado de antemano.

Características Generales

- Tipos de vulnerability scanners

  - Host vulnerability scanners

  Detección de vulnerabilidades conocidas en forma local basada en el análisis de la configuración y del ambiente de ejecución

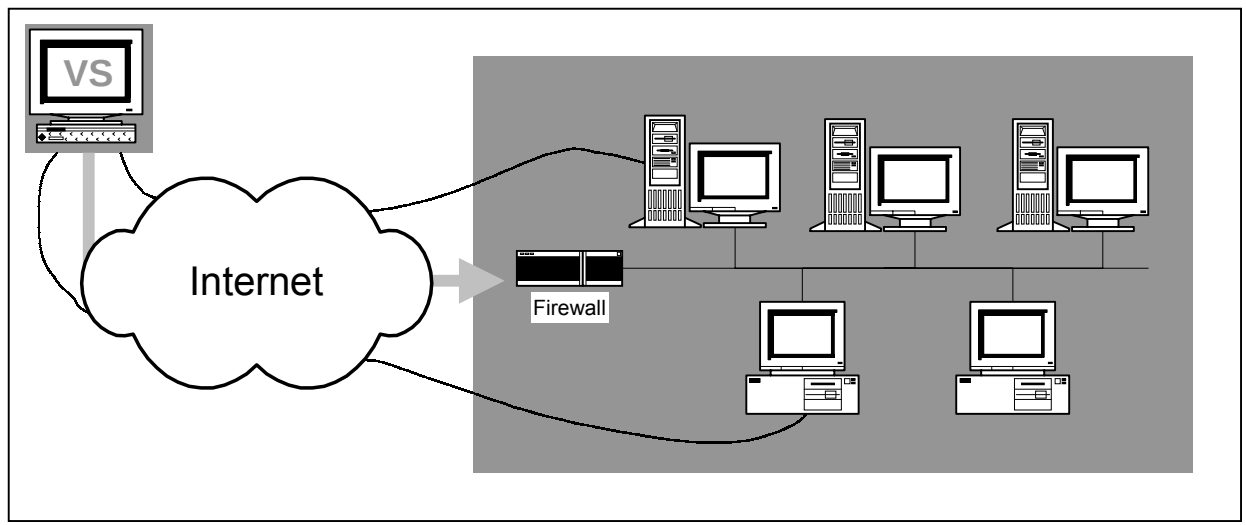


Características Generales

- Tipos de vulnerability scanners*:*

  - Network vulnerability scanners

  Detección de vulnerabilidades en forma remota, para un grupo de maquinas preestablecido, utilizando las técnicas de un hipotético atacante sin conocimiento previo.



Clasificación funcional

- De proposito general
  - Nessus www.nessus.org
  - CyberCop Scanner www.nai.com
  - Internet Scanner www.iss.com
  - HackerShield www.bindview.com
  - NetRecon www.axent.com
- Específicos por plataforma/aplicación
  - Whisker www.wiretrip.net/rfp/2/index.asp
  - Database scanner www.iss.com
  - Pandora www.nmrc.org/pandora/index.html
  - CGI scanners, SMB scanners, NT scanners
- De ejecución masiva
  - ScanSSH www.monkey.org/~provos/scanssh
  - BASS www.securityfocus.com/tools/394

Características Técnicas

- Solo detectan vulnerabilidades conocidas
- Falsos positivos
- Falsos negativos
- NO explotan las vulnerabilidades
- Generan reportes con información para la solucion de la vulnerabilidades detectadas
- Requieren de una actualización periódica

El estado actual

- Poca confiabilidad
- No son comprensivos
- Necesidad de adaptación a topologías y configuraciones particulares
- No contemplan vulnerabilidades específicas en aplicaciones de uso común en un entorno corporativo
- La calificación de riesgo es arbitraria y fuera de contexto
- No extraen conclusiones de alto nivel

Intrusion Detection Systems

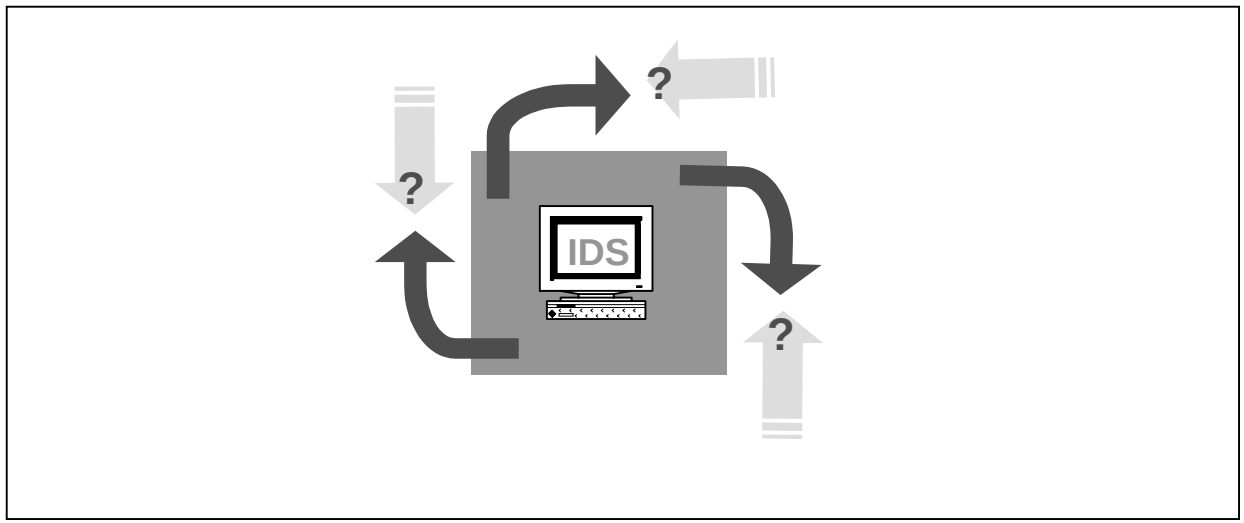
IDS

Definición

- Sistema automático para detectar intentos exitosos o fallidos de vulnerar la arquitectura de seguridad de un entorno tecnológico definido de antemano

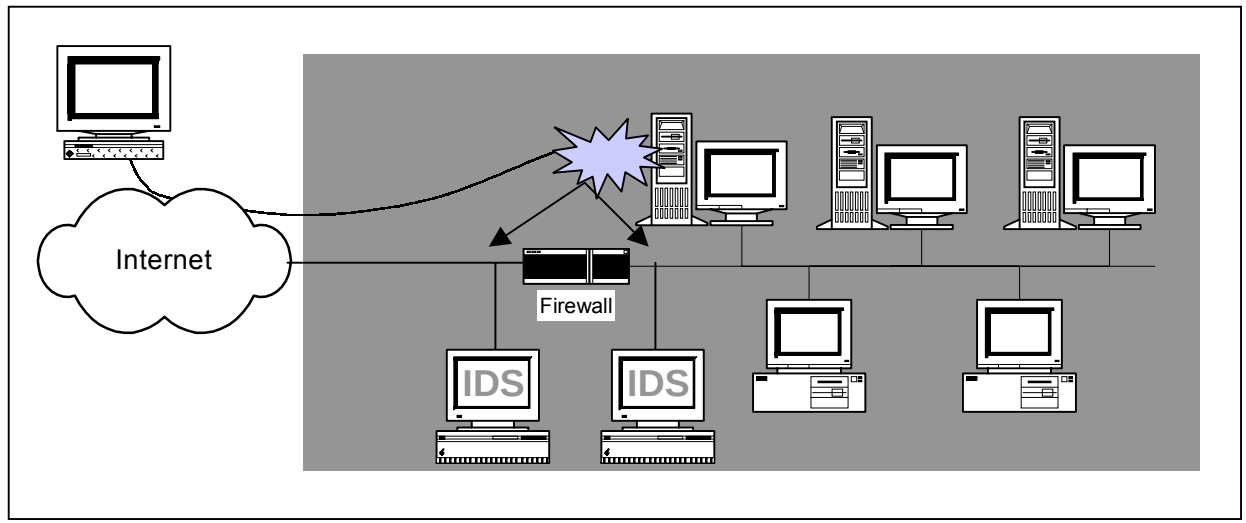
Características generales

- Host IDS (HIDS)
  - Se instala sobre la plataforma a proteger
  - Tiene caracteristicas intrusivas
  - No dispone de información de contexto en relación a todo el entorno a proteger



Características generales

- Network IDS (NIDS)
  - Se instala como monitor pasivo del trafico de red
  - Tiene caracteristicas no intrusivas
  - No dispone de información de contexto en relación a recursos específicos a proteger



Clasificación funcional

- Detección de anomalías (AD)
  - Detectan desviaciones sobre los patrones de uso normal de los recursos monitoreados.
- Detección de mal uso (MD)
  - Detectan técnicas de explotación conocidas para ataques específicos conocidos
- Análisis y detección en tiempo real
  - Generalmente NIDS
- Análisis y detección *off line*
  - Generalmente HIDS

Características Técnicas

- Extendiendo modelo de antivirus NIDS
  - Captura del tráfico de red
  - Reconstrucción de sesiones
  - Identificación de ataques HIDS
  - Captura de llamadas a funciones de API o system calls
  - Análisis de logs, configuración y software instalado
  - Identiciación de conducta anormal
- Modelo Consola-Agentes
- IDS Reactivos/Integrados

El estado actual

- Multiples limitaciones técnicas propias
  - Funcionalidad parcial
  - Vulnerabilidades inherentes

    “Intrusion, Evasion and Denial of Service: Eluding Network Intrusion Detection”, Newsham/Ptacek, 1998, www.snort.org/IDSpaper.pdf
  - Vulnerabilidades específicas
- Limitaciones técnicas externas
  - Disponibilidad constante de mayor ancho de banda
  - Descubrimiento constante de nuevos problemas de seguridad
  - Lanzamiento constante de nuevas tecnologías, plataformas, sistemas operativos, software de base y aplicaciones
- Complejidad creciente para su administración eficiente

Otras herramientas

Otras herramientas de SI

- Honeypots
  - Berferd!
  - CyberCop Sting
  - Honeynet Project
- OS fingerprinting
  - Nmap, Queso
  - Integrado con NVS
- Auditoría automática de código fuente
  - Purify
  - ITS4, Flawfinder, RATS
- Protección contra vulnerabilidades de un tipo específicos
  - StackGuard/ProPolice /StackShield
  - SecureIIS

El futuro

El futuro

- Claves tecnológicas:
  - Herramientas con “inteligencia”
  - Procesamiento cooperativo
  - Integración de componentes
  - Madurez del proceso de investigación y desarrollo
  - Certificación y control independiente
  - Espacio para la innovación
- Claves estratégicas:
  - Modifcar el enfoque con respecto a las tecnologías de base

    (networking, software de base, aplicaciones)
  - Modificar el enfoque con respecto a los actores involucrados

    (atacantes, usuarios finales, desarrolladores, implementadores)

El futuro

- Penetration Test
  - Automatización del proceso
  - Herramientas comprensivas
  - Formalización de las metodologías
  - Profesionalización de la práctica
- Vulnerability Scanner NG
  - Flexible
  - Confiable
  - Eficiente
- IDS-NG
  - Robusto
  - Seguro
  - Realista!!

Conclusiones

Conclusiones

- Cambio de paradigma:
  - Se tiene en cuenta al posible atacante y los recursos de los que dispone
- Las prácticas y herramientas en uso reflejan el cambio de paradigma
- Sin embargo, la tecnología de la que se nutren esta todavía en una etapa temprana de desarrollo
- Conocer sus limitaciones permitirá tomar las decisiones acertadas
- El desafio para la industria de IS en los proximos años:
  - Alcanzar a un nivel de madurez similar al de otras industrias (automotriz, aeroespacial, química)

Gracias!

CORE
SECURITY TECHNOLOGIES

Iván Arce
ivan.arce@corest.com

www.corest.com