SECCIÓN 4

Seguridad de redes, sistemas, aplicaciones y datos.

TEMAS QUE SERAN CUBIERTOS EN ESTA SECCIÓN

1. Controles de proceso, que incluyen:
   - Evaluaciones de riesgo
   - Gestión de vulnerabilidades
   - Pruebas de penetración
2. Seguridad de la red
3. Seguridad del sistema operativo
4. Seguridad de la aplicación
5. Seguridad de datos

OBJETIVOS DE LA SECCIÓN

Al completar esta sección, podrá:

- Determine, evalúe y responda a los riesgos y vulnerabilidades en la red a través de pruebas de penetración.
- Identifique los aspectos clave y los riesgos asociados a la seguridad de los datos, las aplicaciones, los sistemas operativos y la red.

TEMA 1:

Controles de proceso - Evaluación de riesgos

EVALUACIÓN DE RIESGOS

La evaluación de riesgos es un proceso utilizado para identificar y evaluar el riesgo y sus posibles efectos. Involucra tres entradas:

- Evaluación de activos
- Evaluación de amenazas
- Evaluación de vulnerabilidad

GESTIÓN DE RIESGOS

ORIENTACIONES DE EVALUACIÓN DE RIESGOS

ORIENTACIÓN	DESCRIPCIÓN
Activo	Primero se definen los activos importantes y luego se analizan las posibles amenazas a esos activos. Se identifican vulnerabilidades que pueden ser explotadas para acceder al activo.
Amenaza	Las amenazas potenciales se determinan primero y luego se desarrollan los escenarios de amenazas. En función de los escenarios, las vulnerabilidades y los activos de interés para el adversario se determinan en relación con la amenaza.
Vulnerabilidad	Primero se identifican las vulnerabilidades y deficiencias, luego se determinan los activos expuestos y los posibles eventos de amenaza.

CRITERIOS DE ÉXITO DE LA EVALUACIÓN DE RIESGOS

Elegir el método exacto de análisis, incluidos los enfoques cualitativos o cuantitativos, y determinar la orientación del análisis, requiere una planificación considerable y conocimiento de metodologías específicas de evaluación de riesgos. Para tener éxito, el proceso de evaluación de riesgos debe:

- Se ajustan a los objetivos de la organización.
- Abordar adecuadamente el entorno evaluado.
- Utilice metodologías de evaluación que se ajusten a los datos recopilados.
- Es importante recordar que la evaluación de riesgos es un proceso continuo.

ESTRATEGIAS DE RESPUESTA AL RIESGO

Reducción del riesgo

- Implementación de controles o contramedidas para reducir la probabilidad o el impacto del riesgo a niveles aceptables.

Evitar el riesgo

- Evite el riesgo al no participar en una actividad o negocio.

Transferencia o división de riesgo

- Transfiera el riesgo a un tercero (por ejemplo, un seguro) o comparta con un tercero a través de un acuerdo contractual.

Aceptación de riesgo

- Asuma el riesgo y absorba las pérdidas si el riesgo está dentro de la tolerancia o si el costo de la mitigación excede la pérdida potencial.

USO DE LOS RESULTADOS DE LA EVALUACIÓN DE RIESGOS

Los resultados de la evaluación de riesgos se utilizan para una variedad de funciones de administración de seguridad.

Deben evaluarse en términos de la misión de la organización, la tolerancia al riesgo, los presupuestos y otros recursos, y el costo de la mitigación.

- Con base en esta evaluación, se puede elegir una estrategia de mitigación para cada riesgo y se pueden diseñar e implementar controles y contramedidas apropiadas.
- Los resultados se pueden utilizar para comunicar las decisiones de riesgo y las expectativas de la administración en toda la organización a través de políticas y procedimientos.

También se pueden usar para identificar áreas en las que se deben desarrollar capacidades de respuesta a incidentes.

TEMA 2:

Controles de proceso: gestión de vulnerabilidades.

GESTIÓN DE VULNERABILIDADES

- Las organizaciones deben identificar y evaluar las vulnerabilidades para determinar la amenaza y el impacto potencial que presentan.
- La evaluación de vulnerabilidad ayuda a determinar el mejor curso de acción para abordar cada vulnerabilidad.
- Las vulnerabilidades pueden identificarse mediante la información proporcionada por los proveedores de software (por ejemplo, parches y actualizaciones) y mediante el uso de herramientas que identifican vulnerabilidades en el entorno específico de la organización.
- La gestión de vulnerabilidades comienza por comprender los activos de TI y dónde residen, tanto física como lógicamente. También incluye el seguimiento de vulnerabilidades y los esfuerzos de reparación para mitigarlas.

ESCANEOS DE VULNERABILIDADES

- Los análisis de vulnerabilidad se deben realizar regularmente.
- El escaneo de vulnerabilidades es el proceso de usar herramientas patentadas o de código abierto para buscar vulnerabilidades conocidas.
- Las mismas herramientas utilizadas por los adversarios para identificar vulnerabilidades son utilizadas de manera proactiva por las organizaciones para localizar vulnerabilidades.
- Existen muchas formas de herramientas de evaluación de vulnerabilidad.
- Las herramientas deben investigarse y seleccionarse en función de las necesidades corporativas y el retorno de la inversión.
- Tenga en cuenta que las combinaciones de herramientas a menudo proporcionan una mayor comprensión de la postura de seguridad de sus redes.

TIPOS COMUNES DE VULNERABILIDADES

Definición simple Vulnerabilidad: "Es una debilidad explotable que resulta en una pérdida".

TIPO	CAUSA	EJEMPLOS DE CIBERSEGURIDAD
Técnico	Errores en el diseño, implementación, colocación o configuración	• Errores de codificación • Contraseñas inadecuadas • Abrir puertos de red • Falta de monitoreo
Proceso	Errores en la operación	• Falla en monitorear registros • Error al parchar el software
Organizacional	Errores en la gestión, toma de decisiones, planificación o ignorancia.	• Falta de políticas • Falta de conciencia • Falta de implementación de controles
Emergente	Interacciones o cambios en los entornos.	• Fallas entre organizaciones • Errores de interoperabilidad • Implementando nueva tecnología

EVALUACIÓN DE VULNERABILIDAD

- Las vulnerabilidades deben analizarse en el contexto de cómo se explotan.
- El método utilizado para aprovechar una vulnerabilidad se llama explotan.
- Tanto las vulnerabilidades como las explosiones deben considerarse en las evaluaciones de vulnerabilidad.
- Una vez que se identifican y evalúan las vulnerabilidades, puede llevarse a cabo una reparación adecuada para mitigar o eliminar la vulnerabilidad.
- La remediación puede ser a través de un proceso de administración de parches o requerir la reconfiguración de los controles existentes o la adición de nuevos controles.

TEMA 3:

Controles de proceso - Pruebas de penetración

PRUEBAS DE PENETRACIÓN

Las pruebas de penetración utilizan métodos de explotación comunes para:

- Confirmar exposiciones.
- Garantizar el cumplimiento.
- Evaluar la efectividad y la calidad de los controles de seguridad existentes.
- Identifique cómo las vulnerabilidades específicas exponen los recursos y activos de TI.

PAUTAS DE PRUEBA

Antes de realizar una prueba de penetración:

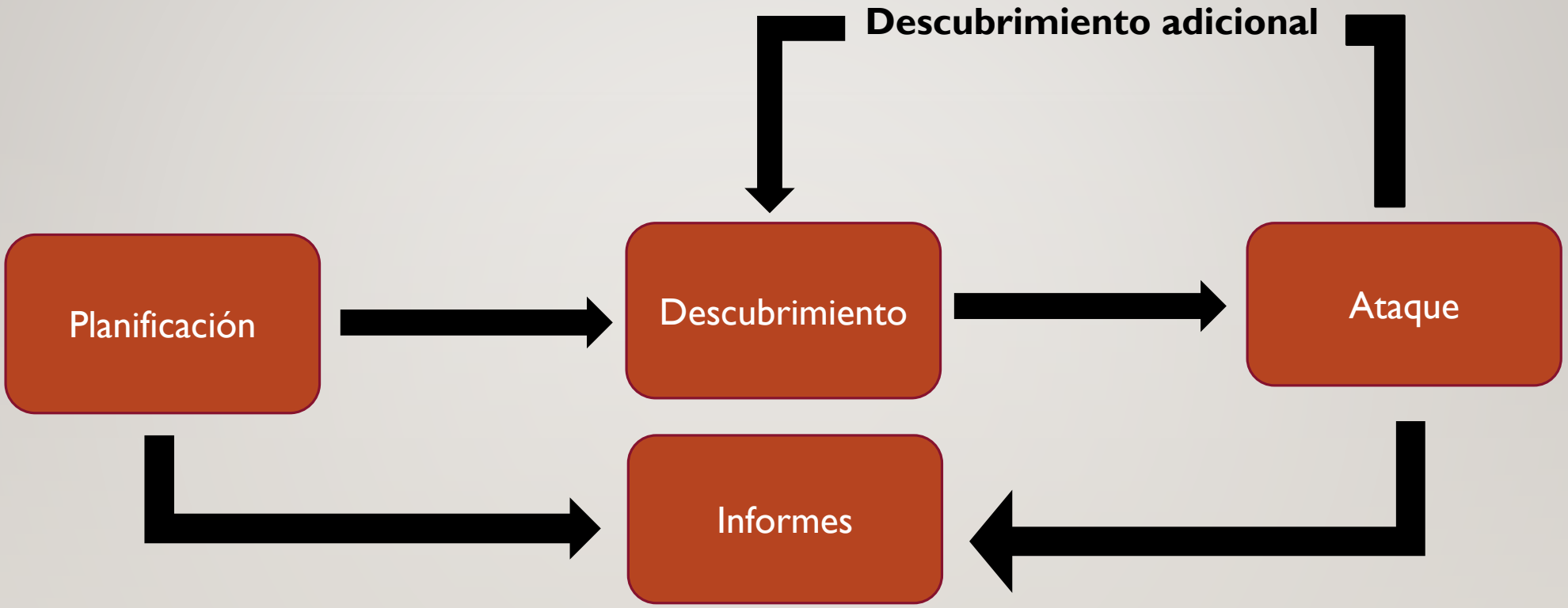
- Definir claramente el alcance de la prueba.
- Proporcione permiso explícito por escrito que autorice las pruebas.
- Implemente procedimientos de "no hacer daño" para garantizar que no se dañen los activos (por ejemplo, eliminaciones, denegación de servicio).
- Tener planes de comunicación y escalamiento.

MARCOS DE PRUEBA DE PENETRACIÓN

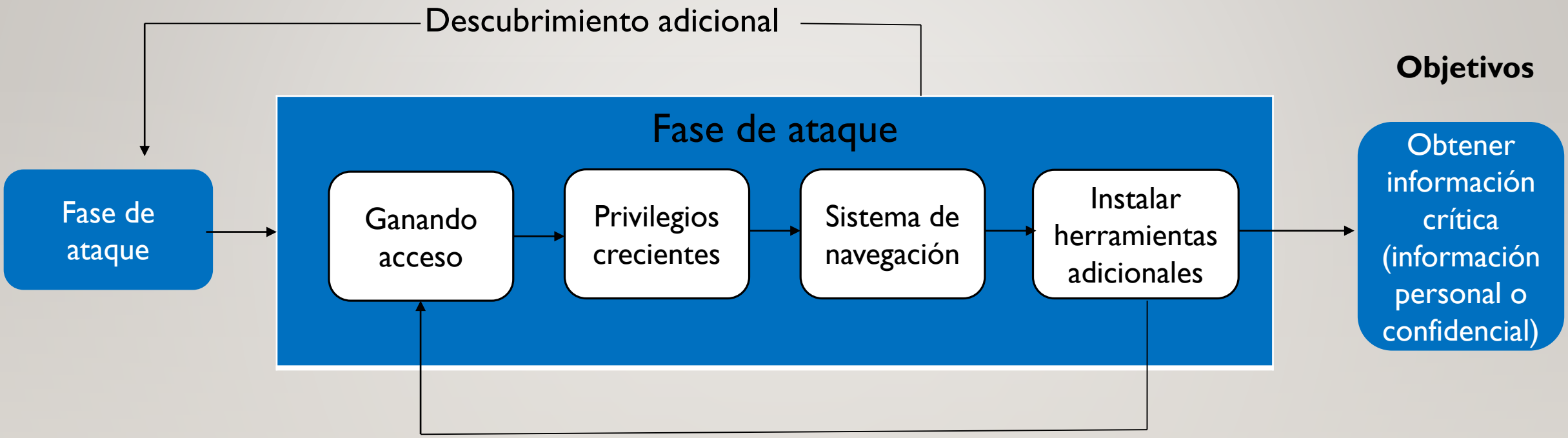
Las pruebas de penetración deben usar un marco para ofrecer repetitividad, consistencia y alta calidad en varios tipos de pruebas de seguridad. Estos marcos incluyen:

- Guía de prueba de penetración PCI: proporciona una buena introducción a las herramientas de prueba.
- Estándar de ejecución de pruebas de penetración: proporciona orientación técnica práctica sobre pruebas de penetración.
- Marco de evaluación de la seguridad de los sistemas de información (ISSAF): proporciona una guía técnica de penetración integral.
- Manual de metodología de pruebas de seguridad de código abierto (OSSTMM): proporciona una metodología para probar la seguridad operativa y puede admitir ISO 27001.

FASES DE UNA PRUEBA DE PENETRACIÓN



FASE DE ATAQUE



TEMA 4:

Seguridad de red

ADMINISTRACIÓN DE REDES

La administración de redes es el proceso de evaluar, monitorear y mantener dispositivos y conexiones de red. Las funciones recomendadas de gestión de red incluyen:

- Gestión de fallas: detección, aislamiento, notificación y corrección de fallas encontradas en la red.
- Gestión de configuración: gestión de archivos de configuración, gestión de inventario y gestión de software.
- Gestión contable: información sobre el uso de los recursos de la red.
- Gestión del desempeño: monitoreo y medición de varios aspectos de las métricas de desempeño para que se pueda mantener un desempeño aceptable.
- Administración de seguridad: provisión de acceso a dispositivos de red y recursos corporativos a personas autorizadas.

REDES DE ÁREA LOCAL

Una red de área local (LAN) cubre un área local pequeña, desde unos pocos dispositivos en una habitación individual hasta una red en varios edificios.

A medida que las LAN crecen y el tráfico aumenta, el requisito de planificar cuidadosamente la configuración lógica de la red se vuelve más importante.

El seguimiento de los volúmenes de tráfico, las tasas de error y los tiempos de respuesta es tan importante en las LAN más grandes como en los servidores y mainframes distribuidos.

COMPONENTES LAN

Los componentes comúnmente asociados con las LAN incluyen:

- Repetidores: dispositivos de capa física que extienden el alcance de una red o conectan dos segmentos de red separados.
- Hubs: dispositivos de capa física que sirven como el centro de una red de topología en estrella o un concentrador de red.
- Conmutadores de capa 2: los conmutadores de capa 2 son dispositivos de nivel de enlace de datos que pueden dividir e interconectar segmentos de red y ayudan a reducir los dominios de colisión en redes basadas en Ethernet.
- Enrutadores: dispositivos de capa de red OSI que enlazan dos o más segmentos de red separados físicamente e independientes.

COMPONENTES LAN (CONT.)

Conmutadores de capa 3 y 4: estos conmutadores actúan en la capa de red.

- Un conmutador de capa 3 analiza el protocolo de red de un paquete entrante y compara la dirección IP de destino con la lista de direcciones en sus tablas, calculando activamente la mejor manera de enviar un paquete a su destino. Esto crea un "circuito virtual".
- Un conmutador de capa 4 permite el cambio basado en políticas. Con esta funcionalidad, el conmutador puede descargar un servidor al equilibrar el tráfico en un grupo de servidores, según la información y el estado de la sesión individual.
- Conmutadores de capa 4 a 7: también conocidos como conmutadores de contenido, conmutadores de servicios de contenido, conmutadores web o conmutadores de aplicaciones, estos se utilizan generalmente para equilibrar la carga entre grupos de servidores.

SEGURIDAD LAN Y WAN

Tanto las redes de área local como las de área amplia son susceptibles a las amenazas.

Afortunadamente, las versiones más nuevas del software de red tienen significativamente más capacidades de control y administración. para identificar la causa de las interrupciones.

El control de acceso a la red (NAC) tiene como objetivo controlar el acceso a una red mediante políticas que describen cómo los dispositivos pueden asegurar el acceso a los nodos de la red cuando primero intentan acceder a una red. Algunas características de NAC incluyen:

- Integrar un proceso de remediación automático que corrige nodos no conformes antes de permitir el acceso.
- Permitir que la infraestructura de red funcione con los servicios de back office y la informática del usuario final para garantizar que la red sea segura antes de permitir el acceso.

EL RIESGO ASOCIADO CON EL USO DE LAN INCLUYE:

- Pérdida de datos a través de cambios no autorizados.
- Falta de protección de datos actual por incapacidad para mantener el control de versiones.
- Exposición a actividad externa a través de la verificación limitada del usuario
- Infección por virus y gusanos
- Revelación incorrecta de datos debido al acceso general.
- Violar las licencias de software.
- Acceso ilegal al hacerse pasar por usuarios legítimos.
- Olfateando usuarios internos.
- Suplantación de usuarios internos
- Destrucción de datos de registro y auditoría.

DISPOSICIONES DE SEGURIDAD DE LAN

Las capacidades administrativas de seguridad de red comúnmente disponibles incluyen:

- Declarar la propiedad de programas, archivos y almacenamiento.
- Limitar el acceso a una base de solo lectura.
- Implementación de bloqueo de registros y archivos para evitar actualizaciones simultáneas.
- Hacer cumplir los procedimientos de inicio de sesión de ID de usuario / contraseña, incluidas las reglas relacionadas con la longitud de la contraseña, el formato y la frecuencia de cambio.
- Uso de conmutadores para implementar políticas de seguridad portuaria.
- Cifrar el tráfico local utilizando el protocolo IPSec (seguridad de IP)

TECNOLOGÍAS INALÁMBRICAS

Las tecnologías inalámbricas utilizan transmisiones de radiofrecuencia o señales electromagnéticas a través del espacio libre como medio para transmitir datos.

Las tecnologías inalámbricas van desde sistemas complejos hasta dispositivos simples e incluyen redes inalámbricas de área local (WLAN).

Las tecnologías WLAN se ajustan a una variedad de estándares y ofrecen diferentes niveles de características de seguridad.

El estándar más útil utilizado actualmente es el estándar IEEE 802.11.

802.11 se refiere a una familia de especificaciones para la tecnología WLAN, que define una interfaz inalámbrica entre un cliente inalámbrico y una estación base o entre dos clientes inalámbricos.

PROTECCIONES DE RED INALÁMBRICA

La transmisión inalámbrica de información confidencial debe protegerse con un cifrado seguro.

El cifrado de privacidad equivalente por cable (WEP) de IEEE 802.11 utiliza claves privadas simétricas.
El controlador de interfaz de red (NIC) basado en radio del usuario final y el punto de acceso deben tener la misma clave.

En la mayoría de los casos, estas claves permanecen sin cambios en las redes durante largos períodos.

Con las claves estáticas, varias herramientas de hacking rompen fácilmente los mecanismos de cifrado WEP relativamente débiles.

EVOLUCIÓN DE LOS ESTÁNDARES DE SEGURIDAD INALÁMBRICA

- El método más utilizado para redes inalámbricas de área local es 802.11i (WPA2) y acceso protegido Wi-Fi (WPA).
- Estos usan claves dinámicas y pueden usar un servidor de autenticación con credenciales para aumentar la protección contra hackers.
- WPA y WPA2 (preferido) son aplicables a la mayoría de las redes inalámbricas y se usan comúnmente en redes que involucran PC.
- Los mensajes transmitidos mediante dispositivos inalámbricos portátiles también deben protegerse con encriptación y, cuando sea posible, los métodos VPN pueden usarse para proporcionar seguridad adicional.

PUERTOS Y PROTOCOLOS

Cuando se utiliza el protocolo de comunicaciones de Internet, el Protocolo de control de transmisión / Protocolo de Internet (TCP / IP), designar un puerto es la forma en que un programa cliente especifica un programa de servidor particular en una computadora en una red.

Un número de puerto es una forma de identificar el proceso específico al que se debe reenviar un mensaje de Internet u otra red cuando llega a un servidor.

Estos son asignados por la Autoridad de Números Asignados de Internet (IANA).
Los números de puerto permitidos varían de 0 a 65535. Estos se dividen en tres rangos, de la siguiente manera:

- Los puertos conocidos: 0 a 1023: estos solo pueden ser utilizados por procesos del sistema (o raíz) o por programas ejecutados por usuarios privilegiados.
- Los puertos registrados — 1024 a 49151: pueden ser utilizados por procesos o programas de usuarios ordinarios ejecutados por usuarios normales.
- Los puertos dinámicos y / o privados: 49152 a 65535: no figuran en la lista de la IANA debido a su naturaleza dinámica.

PUERTOS Y SERVICIOS COMÚNMENTE EXPLOTADOS

PUERTO #	SERVICIO	PROTOCOLO
7	Eco	TCP/UDP
19	Carga	TCP
20-21	FTP (Protocolo de transferencia de archivos)	TCP
23	Telnet (inicio de sesión remoto)	TCP
25	SMTP (transferencia de correo simple)	TCP
43	Whois	TCP/UDP
53	DNS (sistema de nombres de dominio)	TCP
69	TFTP (protocolo de transferencia de archivos trivial)	UDP
79	Finger	TCP
80	HTTP-low	TCP
107	Rtelnet	TCP/UDP

PUERTO #	SERVICIO	PROTOCOLO
110	POP3 (protocolo de la Oficina postal)	TCP
111/ 2049	SunRPC (llamadas a procedimiento remoto)	TCP/UDP
135-139	NBT (Net BIOS sobre TCP/IP)	TCP/UDP
161, 162	SNMP (Protocolo Simple de Manejo de Red)	UDP
512	Exec	UDP
513	Login	TCP
514	Shell	TCP/UDP
6000-xxx	X-Windows	TCP
8000	HTTP	TCP/UDP
8080	HTTP	TCP/UDP
31337	Back Orifice	UDP

TÚNELES

En los túneles, los intrusos maliciosos o los piratas informáticos externos utilizan el protocolo como una vía establecida, o túnel, que dirige el intercambio de información con fines maliciosos.

Los ejemplos de tipos de túneles incluyen:

- Túnel de ICMP: se utiliza para omitir las reglas de firewall a través de la ofuscación del tráfico real.
- Túnel HTTP: una técnica mediante la cual las comunicaciones realizadas mediante varios protocolos de red se encapsulan utilizando el protocolo HTTP.

TÚNEL VPN

Los tuneles transporta datos de capa superior a través de VPN con protocolos de capa 2(Capa de enlace de datos), Los tipos comunes de túneles incluyen:

- Protocolo de túnel punto a punto (PPTP): Es de capa 2 desarrollado por Microsoft que encapsula datos de protocolo punto a punto. Es simple, pero menos seguro que otros.
- Protocolo de túnel de capa 2 (L2TP): un protocolo que encapsula datos de protocolo punto a punto y es compatible entre los equipos de diferentes fabricantes.
- VPN: una forma de VPN de capa 3 (Capa de Red) que se puede usar con un navegador web estándar y utiliza protocolos de seguridad de capa de transporte (Capa 4) (TLS) para cifrar el tráfico.
- VPN IPSec: las VPN IPSec protegen los paquetes IP de capa 2 y 3 entre redes o hosts remotos y una escapada/ nudo IPSec ubicado en el borde de una red privada.

VOZ SOBRE PROTOCOLO DE INTERNET

- Los usuarios esperan que todas las comunicaciones de voz sean confidenciales.
- Cualquier dispositivo de Protocolo de Voz sobre Internet (VoIP) es un dispositivo IP; por lo tanto, es vulnerable a los mismos tipos de ataques.
- Las redes VoIP tienen una serie de características que hacen requisitos de seguridad especiales.
- También puede divulgarse información confidencial, lo que puede tener efectos adversos.

ACCESO REMOTO

La conectividad de acceso remoto a sus recursos de información es necesaria para muchas organizaciones para diferentes tipos de usuarios.

El uso de VPN para permitir el acceso remoto a sus sistemas puede crear agujeros en la infraestructura de seguridad de una organización, y el tráfico encriptado puede ocultar acciones no autorizadas o software malicioso que puede transmitirse a través de dichos canales.

- Para reducir los riesgos a la VPN, se pueden implementar controles arquitectónicos para restringir el tráfico de acceso remoto, protegidos contra virus, portales de acceso remoto y segmentos de red no sensibles.

RIESGO DE ACCESO REMOTO

El riesgo de acceso remoto incluye:

- Denegación de servicio (DoS)
- Terceros maliciosos
- Software de comunicaciones mal configurado
- Dispositivos mal configurados en infraestructura informática
- Sistemas host no asegurados adecuadamente
- Problemas de seguridad física

CONTROLES DE ACCESO REMOTO

Los controles de acceso remoto incluyen:

- Políticas y estándares.
- Autorizaciones adecuadas.
- Mecanismos de identificación y autenticación.
- Herramientas y técnicas de cifrado, como el uso de una VPN.
- Restricción de acceso a sistemas controlados, redes y aplicaciones.