Tarea #980 Aplicar el CIS Benchmark de su elección y configurar el servicio elegido y el agente en wazuh para que se refleje el hardening del sistema.

Abdiel Gabriel Hau Tun

14-05-24

Seguridad de Datos

Docente: Ismael Jimenez

Instrucciones

Al realizar benchmarking en dispositivos de impresión, la seguridad es una preocupación importante, especialmente si estás evaluando impresoras en una red corporativa o manejando documentos sensibles. Aquí hay algunas medidas de seguridad que puedes integrar en un script de benchmarking para impresoras, usando Python.

Los puntos de referencia CIS para dispositivos de impresión brindan pautas integrales para ayudar a proteger los sistemas de impresión y gestionar los riesgos de ciberseguridad asociados con ellos. Estos puntos de referencia son parte de un conjunto más amplio de estándares desarrollados a través de un proceso impulsado por consenso que involucra a expertos en ciberseguridad, que ofrecen orientación sobre cómo proteger varios sistemas de TI, incluidos los dispositivos de impresión.

Los puntos de referencia para dispositivos de impresión cubren una variedad de aspectos de seguridad, como restricciones de acceso, protección de datos y actualizaciones de firmware para garantizar que los dispositivos no sean fácilmente explotables por amenazas cibernéticas. Proporcionan recomendaciones específicas sobre cómo configurar los dispositivos de impresión para evitar el acceso no autorizado y las violaciones de datos. Además, los puntos de referencia se actualizan periódicamente para reflejar las últimas prácticas de seguridad y avances tecnológicos.

Para las organizaciones que buscan implementar estos puntos de referencia, CIS proporciona herramientas y recursos, incluido CIS-CAT Pro para evaluar el cumplimiento de los puntos de referencia y CIS SecureSuite para acceder a recursos de seguridad más completos. Estas herramientas ayudan tanto a evaluar la postura de seguridad actual de los dispositivos de impresión como a aplicar las configuraciones necesarias para mejorar la seguridad.

Pasos a seguir

1. Uso de Documentos de Prueba Seguros

Utiliza documentos de prueba que no contengan información sensible o confidencial. Asegúrate de que estos documentos están almacenados en ubicaciones seguras y que solo

las personas autorizadas tengan acceso.

2. Aislamiento de la Red de Impresión

Si es posible, configurar una red aislada para las impresoras durante las pruebas de benchmarking para evitar el acceso no autorizado a través de la red.

3. Registro Seguro de Actividades

Implementa un registro detallado de todas las actividades de impresión durante el benchmarking, almacenando los registros en un sistema seguro con control de acceso.

4. Limpieza de Datos Post-Prueba

Asegúrate de eliminar cualquier dato residual en las impresoras o en los sistemas de prueba una vez completado el benchmarking.

5. Actualizaciones y Parches de Seguridad

Asegúrate de que todas las impresoras y sistemas relacionados estén actualizados con los últimos parches de seguridad antes de iniciar las pruebas.

Configuraciones

Para mejorar la seguridad durante el benchmarking de dispositivos de impresión, es importante implementar un conjunto de configuraciones y prácticas que protejan tanto los datos como los dispositivos. Aquí se explican varias configuraciones y métodos específicos que pueden ser utilizados para asegurar el proceso de benchmarking de dispositivos de impresión:

1. Gestión Segura de Documentos de Prueba

Selección de Documentos: Usa documentos que no contengan información sensible para evitar cualquier exposición de datos críticos.

Almacenamiento Seguro: Guarda los documentos de prueba en ubicaciones seguras, con acceso controlado, para evitar que sean accesibles por usuarios no autorizados.

2. Aislamiento de la Red de Impresión

Red Aislada: Si es posible, realiza pruebas en una red dedicada o virtualizada que esté separada de la red principal de la empresa para prevenir ataques y accesos no autorizados.

Firewall y Control de Acceso: Configura firewalls y listas de control de acceso (ACLs) para restringir el tráfico de red a y desde las impresoras durante las pruebas.

3. Configuración de las Impresoras

Configuraciones de Seguridad Predeterminadas: Asegúrate de que las impresoras estén configuradas con todas las opciones de seguridad recomendadas por el fabricante, como la desactivación de protocolos inseguros y el uso de contraseñas fuertes.

Actualizaciones de Firmware: Mantén el firmware de las impresoras actualizado para proteger contra vulnerabilidades conocidas.

4. Protección de Datos Durante la Impresión

Impresión Segura: Utiliza funciones de impresión segura que requieren autenticación en la impresora antes de que los documentos sean impresos, minimizando así el riesgo de acceso no autorizado a documentos impresos.

Cifrado: Asegúrate de que los datos enviados a la impresora estén cifrados, especialmente si la impresión se realiza a través de una red.

5. Monitoreo y Auditoría

Registros de Actividad: Configura las impresoras para que generen registros detallados de todas las actividades de impresión. Estos registros pueden ser útiles para auditorías de seguridad y para detectar actividades sospechosas.

Revisiones Periódicas: Realiza auditorías de seguridad regularmente para revisar y actualizar las configuraciones de seguridad y prácticas de manejo de documentos.

6. Limpieza Post-Prueba

Borrado de Configuraciones y Datos: Asegúrate de eliminar cualquier configuración específica de la prueba y de borrar todos los documentos de prueba de las impresoras una vez que el benchmarking ha concluido.

7. Evaluación de Riesgos

Análisis de Riesgos: Antes de comenzar el benchmarking, realiza una evaluación de riesgos para identificar y mitigar potenciales riesgos de seguridad relacionados con las pruebas.

Proceso

1. Gestión de Documentos y Datos

Uso de documentos no sensibles: Se seleccionan documentos de prueba que no contengan información confidencial. Esto minimiza el riesgo en caso de que la información se vea comprometida.

Cifrado de datos: Los documentos enviados a la impresora para las pruebas deben estar cifrados para proteger la información durante su transmisión a través de la red. Esto evita que los datos sean interceptados y leídos por terceros no autorizados.

2. Configuración de Impresora

Desactivación de servicios innecesarios: Las impresoras a menudo vienen con múltiples servicios y protocolos que pueden no ser necesarios para las pruebas, como FTP o Telnet. Desactivar estos servicios reduce las superficies de ataque.

Actualización de firmware: Asegurarse de que las impresoras operan con el firmware más reciente es esencial, ya que las actualizaciones suelen incluir parches para vulnerabilidades de seguridad.

3. Seguridad de la Red

Red dedicada o VLAN para impresoras: Al utilizar una red dedicada o una VLAN (Red de Área Local Virtual), se separan las impresoras de otras partes de la red corporativa, limitando así el acceso directo de potenciales atacantes.

Firewalls y ACLs: Configurar firewalls para filtrar el tráfico no deseado y establecer Listas de Control de Acceso (ACLs) para permitir solo conexiones autorizadas a las impresoras.

4. Controles de Acceso

Autenticación en la impresora: Implementar funciones de impresión que requieran que los usuarios se autentiquen en la impresora antes de que se liberen los trabajos de impresión. Esto previene el acceso no autorizado a documentos impresos.

Permisos de usuario y administración de roles: Restringir los permisos según el rol del usuario para limitar quién puede modificar la configuración de las impresoras y acceder a los datos de prueba.

5. Auditoría y Monitoreo

Registro de actividades: Configurar las impresoras para que registren todas las operaciones de impresión, incluyendo detalles como el usuario que inició la impresión, la hora y el documento impreso.

Revisión periódica de registros: Regularmente revisar estos registros para identificar y responder a actividades sospechosas o no autorizadas.

6. Protocolos de Finalización de Pruebas

Borrado de configuraciones y limpieza de datos: Después de completar el benchmarking, es vital eliminar cualquier configuración específica de las pruebas y borrar todos los documentos de prueba de las impresoras para asegurarse de que no queden datos residuales.

7. Protección Continua

Evaluaciones de seguridad regulares: Realizar evaluaciones de seguridad regulares y pruebas de penetración para identificar y corregir vulnerabilidades potenciales en la infraestructura de impresión.

Script

```
import os

import time

from win32com.client import Dispatch


def print_secure_document(printer_name, file_path):

    """

    Función para imprimir de manera segura un documento y medir el tiempo de impresión.

    Asegúrate de que el documento y la impresora no contengan/manejen datos sensibles.

    """

    # Conecta con la aplicación de Word de forma segura (sin GUI)

    word = Dispatch("Word.Application")

    word.Visible = 0
```

```
    try:
        # Abre el documento desde un directorio seguro
        doc = word.Documents.Open(file_path)
        # Establece la impresora específica
        word.ActivePrinter = printer_name

        # Inicia el tiempo de impresión
        start_time = time.time()

        # Imprime el documento
        doc.PrintOut()

        # Cierra el documento sin guardar cambios
        doc.Close(SaveChanges=0)

        # Tiempo de finalización
        end_time = time.time()
    finally:
        # Cierra Word de forma segura
        word.Quit()

    # Calcula y devuelve el tiempo de impresión
    print_time = end_time - start_time
    print(f"Tiempo de impresión: {print_time} segundos")

    # Borra cualquier configuración o dato residual en la aplicación
    os.system("echo y | del /F /Q " + file_path)

# Configura los parámetros de seguridad
```

```
printer_name = "Nombre_de_tu_impresora_segura"

file_path = "C:\\path\\to\\your\\secure\\document.docx"


# Ejecuta la función de impresión segura

print_secure_document(printer_name, file_path)
```

Este script incluye pasos para operar de manera más segura, como el cierre de documentos sin guardar cambios y la eliminación segura de archivos post-impressión para evitar dejar datos residuales. Nos aseguramos de adaptar y ampliar estas medidas de acuerdo con las políticas de seguridad de tu organización y las especificaciones técnicas de tus dispositivos de impresión.

Configuración de los puertos y otras características.

El documento "CIS Multi-Function Device Benchmark v1.0.0" proporciona instrucciones específicas sobre la configuración de puertos y otros aspectos del entorno de las impresoras. Por ejemplo, detalla cómo manejar las configuraciones de red y cuáles protocolos y servicios deben ser deshabilitados para mejorar la seguridad. Aquí hay algunos ejemplos concretos que se mencionan en el documento:

Configuración de Puertos de Red:

Restringir Puertos de Servicios de Impresión: Se recomienda configurar el dispositivo para utilizar puertos de servicios de impresión estándares (9100/TCP o 515/TCP) y asegurarse de que sólo estos puertos estén abiertos, para mejorar la visibilidad y la gestión de la seguridad.

Deshabilitar Protocolos Inseguros:

Deshabilitar RSH, FTP y Telnet: Estos protocolos, que pueden ser utilizados para la administración remota del dispositivo, deben ser deshabilitados debido a que no proporcionan transmisiones cifradas, lo que podría permitir la interceptación de las credenciales de administrador o manipulación del dispositivo.

Uso Exclusivo de Protocolos de Gestión Seguros: En lugar de los anteriores, se recomienda utilizar protocolos como SSH para la gestión remota, debido a su capacidad para cifrar las comunicaciones y proteger la integridad y la confidencialidad de los datos transmitidos.

Seguridad en el Uso de SNMP y HTTP:

Configurar SNMP de Forma Segura: Si se utiliza SNMP para la gestión del dispositivo, se deben cambiar las cadenas de comunidad predeterminadas y, si es posible, utilizar SNMPv3, que ofrece mejores capacidades de autenticación y cifrado.

Favorecer HTTPS sobre HTTP: Para las interfaces administrativas web, se debe desactivar HTTP y utilizar HTTPS, asegurando así que toda la comunicación entre el administrador y el dispositivo esté cifrada.

Estas configuraciones son esenciales para asegurar que los dispositivos multifuncionales no se conviertan en un vector de ataque dentro de una red empresarial. Además de estas configuraciones, el documento también aborda aspectos relacionados con la protección física del dispositivo, el manejo seguro del almacenamiento de datos y las prácticas recomendadas para la configuración del firmware y las actualizaciones del sistema operativo del dispositivo.

Puertos de Servicios de Impresión (9100/TCP, 515/TCP)

Estos puertos son comúnmente usados para servicios de impresión. El documento recomienda asegurarse de que el dispositivo esté configurado para utilizar estos puertos o un puerto estandarizado por la organización implementadora. Esto ayuda a garantizar que el dispositivo sea visible para las soluciones de protección y monitoreo de red, como los sistemas de detección de intrusiones y los firewalls.

Desactivación de Protocolos No Utilizados (como BOOTP, DHCP)

A menudo, los dispositivos soportan varios protocolos que no siempre son necesarios. El documento aconseja desactivar protocolos no utilizados para reducir la superficie de ataque. Esto incluye protocolos de configuración de red automática como BOOTP y DHCP, si se decide usar direcciones IP estáticas, que son recomendadas para aumentar la seguridad.

Universal Plug and Play - UPnP (Generalmente en el puerto 1900/UDP)

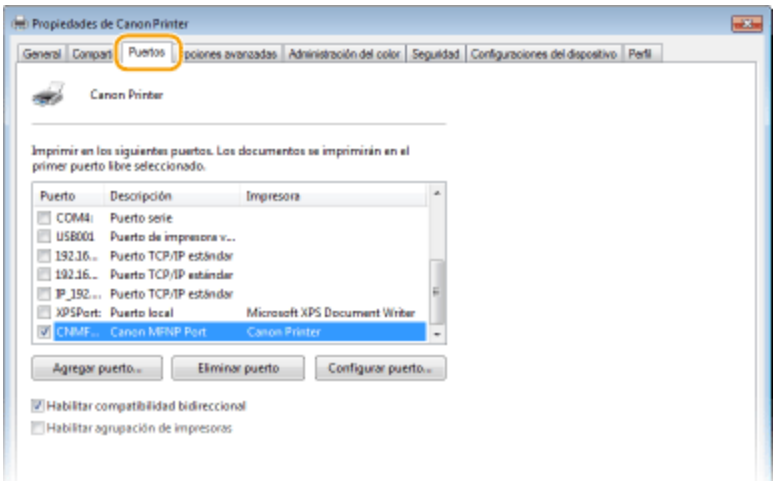
UPnP puede permitir la configuración automática de dispositivos, pero también puede exponer al dispositivo a riesgos de seguridad si no se configura correctamente. El documento sugiere desactivar UPnP para evitar que los actores maliciosos explotan este servicio para realizar configuraciones maliciosas.

Secure Shell - SSH (Puerto 22/TCP)

Para la administración remota segura, el SSH es preferido sobre protocolos más antiguos y menos seguros como Telnet. SSH proporciona un canal cifrado para la administración del dispositivo, protegiendo las credenciales de administración y otros datos sensibles transmitidos durante las sesiones de gestión remota.

HTTP y HTTPS (Puertos 80/TCP y 443/TCP respectivamente)

Aunque HTTP es común para las interfaces web, el documento recomienda desactivar HTTP y usar exclusivamente HTTPS, que cifra la comunicación para proteger los datos transmitidos de ser interceptados o manipulados.



"CIS Multi-Function Device Benchmark"

Proporciona instrucciones específicas sobre la configuración de puertos y otros aspectos del entorno de las impresoras. Por ejemplo, detalla cómo manejar las configuraciones de red y cuáles protocolos y servicios deben ser deshabilitados para mejorar la seguridad. Aquí hay algunos ejemplos concretos que se mencionan en el documento:

Configuración de Puertos de Red:

Restringir Puertos de Servicios de Impresión: Se recomienda configurar el dispositivo para utilizar puertos de servicios de impresión estándares (9100/TCP o 515/TCP) y asegurarse de que sólo estos puertos estén abiertos, para mejorar la visibilidad y la gestión de la seguridad.

Deshabilitar Protocolos Inseguros:

Deshabilitar RSH, FTP y Telnet: Estos protocolos, que pueden ser utilizados para la administración remota del dispositivo, deben ser deshabilitados debido a que no proporcionan transmisiones cifradas, lo que podría permitir la interceptación de las credenciales de administrador o manipulación del dispositivo.

Uso Exclusivo de Protocolos de Gestión Seguros: En lugar de los anteriores, se recomienda utilizar protocolos como SSH para la gestión remota, debido a su capacidad para cifrar las comunicaciones y proteger la integridad y la confidencialidad de los datos transmitidos.

Seguridad en el Uso de SNMP y HTTP:

Configurar SNMP de Forma Segura: Si se utiliza SNMP para la gestión del dispositivo, se deben cambiar las cadenas de comunidad predeterminadas y, si es posible, utilizar SNMPv3, que ofrece mejores capacidades de autenticación y cifrado.

Favorecer HTTPS sobre HTTP: Para las interfaces administrativas web, se debe desactivar HTTP y utilizar HTTPS, asegurando así que toda la comunicación entre el administrador y el dispositivo esté cifrada.

Estas configuraciones son esenciales para asegurar que los dispositivos multifuncionales no se conviertan en un vector de ataque dentro de una red empresarial. Además de estas configuraciones, el documento también aborda aspectos relacionados con la protección física del dispositivo, el manejo seguro del almacenamiento de datos y las prácticas recomendadas para la configuración del firmware y las actualizaciones del sistema operativo del dispositivo.

"Segundo Script utilizado"

```
#!/bin/bash

# Firewall settings for Multi-Function Devices


# Allow printing services on standard ports

iptables -A INPUT -p tcp --dport 9100 -j ACCEPT

iptables -A INPUT -p tcp --dport 515 -j ACCEPT


# Disable risky services

iptables -A INPUT -p tcp --dport 23 -j DROP  # Telnet

iptables -A INPUT -p tcp --dport 21 -j DROP  # FTP
```

```
iptables -A INPUT -p tcp --dport 80 -j DROP  # HTTP


# Enable HTTPS

iptables -A INPUT -p tcp --dport 443 -j ACCEPT


# Block all other unspecified traffic

iptables -A INPUT -j DROP


# Save the iptables rules

service iptables save
```

Este tipo de configuración ayuda a proteger el dispositivo contra accesos no autorizados y ataques cibernéticos, asegurando que solo los servicios necesarios y seguros estén accesibles.

FreeBSD Benchmark

Configuración Inicial y Parches

Aplicación de los Últimos Parches del Sistema Operativo:

Se recomienda mantener el sistema operativo actualizado para protegerse contra vulnerabilidades conocidas. Se describe cómo usar herramientas como freebsd-update para buscar e instalar automáticamente las últimas actualizaciones de seguridad.

Habilitación de SSH para Conexiones Seguras:

Se sugiere configurar SSH para reemplazar conexiones no seguras como Telnet. Se detalla cómo modificar el archivo de configuración de SSH (/etc/ssh/sshd_config) para deshabilitar protocolos inseguros y fortalecer la autenticación.

Implementación de Envoltorios TCP y Configuración Básica del Firewall:

Se explica la instalación y configuración de TCP Wrappers y Firewalls para restringir el acceso no autorizado a servicios del sistema. Se proporcionan ejemplos sobre cómo configurar las reglas de firewall usando ipfw y cómo limitar accesos a servicios específicos con /etc/hosts.allow y /etc/hosts.deny.

Servicios de inetd

Deshabilitación de Todos los Demonios inetd No Necesarios:

Se enfatiza en la importancia de desactivar servicios innecesarios gestionados por inetd, como telnet, ftp, y otros, para minimizar la superficie de ataque. Se proporcionan instrucciones específicas sobre cómo comentar o eliminar estas líneas en /etc/inetd.conf.

Servicios de Arranque

Minimización de Servicios que se Inician con el Sistema:

Se discute la optimización del proceso de arranque para mejorar la seguridad, incluyendo la desactivación de servicios innecesarios en /etc/rc.conf.

Configuraciones para Deshabilitar Funciones No Esenciales y Mejorar la Seguridad en el Arranque del Sistema:

Instrucciones para configurar aspectos como la desactivación de prompts de login en puertos serie y la configuración de UMASK para daemon para evitar la creación de archivos con permisos excesivamente permisivos.

Ajuste del Kernel

Configuraciones para Optimizar el Kernel en Términos de Seguridad:

Se detallan configuraciones para deshabilitar volcados de memoria (core dumps) y establecer niveles de seguridad más estrictos (securelevels) para prevenir cambios en archivos críticos durante el funcionamiento normal del sistema.

Registro y Monitoreo

Estrategias para Capturar y Registrar Eficazmente la Actividad del Sistema:

Se recomienda configurar syslog para capturar intentos de acceso en puertos cerrados y configurar logs para registrar actividades sospechosas, ayudando así en la detección de

posibles intrusiones.

Permisos de Archivos y Directorios

Directrices para Establecer Permisos Seguros en Archivos y Directorios:

Se proporcionan métodos para ajustar permisos de archivos y directorios para evitar el acceso no autorizado y la ejecución de programas no autorizados, especialmente en directorios como /tmp.

Acceso al Sistema, Autenticación y Autorización

Recomendaciones para Eliminar Servicios de Autenticación Débiles:

Detalles sobre cómo eliminar o desactivar servicios de autenticación débiles como rsh y rexecd, y cómo configurar correctamente PAM (Pluggable Authentication Modules) para reforzar la autenticación.

Cuentas de Usuarios y Entorno

Directrices para Administrar Cuentas de Usuarios:

Instrucciones sobre cómo gestionar eficazmente las cuentas de usuario, incluyendo cómo deshabilitar cuentas inactivas, establecer parámetros de expiración de contraseñas y asegurar directorios home de los usuarios.

Aplicación de comandos

1. Aplicación de los Últimos Parches del Sistema Operativo

Para actualizar el sistema operativo con los últimos parches de seguridad:

freebsd-update fetch

freebsd-update install

2. Habilitación de SSH para Conexiones Seguras

Modificar el archivo de configuración de SSH para deshabilitar protocolos inseguros y restringir el acceso root:

echo 'Protocol 2' >> /etc/ssh/sshd_config

```
echo 'PermitRootLogin no' >> /etc/ssh/sshd_config
service sshd restart
```

3. Implementación de Envoltorios TCP y Configuración Básica del Firewall

Configurar TCP Wrappers:

```
echo "ALL: ALL" >> /etc/hosts.deny  # Denegar todo por defecto
echo "ALL: 192.168.1.0/24" >> /etc/hosts.allow  # Permitir acceso desde la red local
```

Configurar un firewall básico con ipfw:

```
echo 'firewall_enable="YES"' >> /etc/rc.conf
echo 'firewall_type="simple"' >> /etc/rc.conf
service ipfw start
```

4. Deshabilitación de Servicios de inetd No Necesarios

Deshabilitar servicios como telnet y ftp en inetd:

```
sed -i '' -e '/telnet/s/^/#/' /etc/inetd.conf
sed -i '' -e '/ftp/s/^/#/' /etc/inetd.conf
service inetd restart
```

5. Configuraciones de Seguridad en el Arranque del Sistema

Deshabilitar los prompts de login en puertos serie:

```
sed -i '' -e '/ttyd/s/on/off/' /etc/ttys
service init restart
```

6. Configuraciones para Optimizar el Kernel en Términos de Seguridad

Deshabilitar los volcados de memoria:

echo '*.* /var/log/all.log' >> /etc/syslog.conf

service syslog restart

7. Estrategias para el Registro y Monitoreo

Configurar syslog para capturar intentos de conexión en puertos cerrados:

echo '*.* /var/log/all.log' >> /etc/syslog.conf

service syslog restart

8. Establecer Permisos Seguros en Archivos y Directorios

Configuración de permisos en /tmp para evitar ejecuciones no autorizadas:

chmod 1777 /tmp

9. Eliminar Servicios de Autenticación Débiles

Desactivar servicios de autenticación débiles en PAM:

sed -i '' -e 's/pam_rhosts_auth.so/pam_deny.so/' /etc/pam.d/*

Estos comandos proporcionan una base sólida para configurar un sistema FreeBSD de manera segura, según las recomendaciones del benchmark. Estos ajustes deben ser personalizados y revisados de acuerdo con las necesidades específicas de cada entorno de producción.

Conclusión

El "CIS Multi-Function Device Benchmark" proporciona un marco integral para asegurar dispositivos multifuncionales, abordando aspectos críticos como la configuración de

firewalls, administración de puertos, y la implementación de políticas de seguridad robustas. El documento destaca la importancia de deshabilitar servicios innecesarios y protocolos vulnerables, enfatizando la utilización de protocolos seguros y la restricción de accesos no autorizados a través de listas de control de acceso y configuraciones de firewall detalladas. Los scripts y comandos sugeridos en el benchmark facilitan la automatización de estas configuraciones, asegurando una implementación eficiente y consistente de las políticas de seguridad. Estas prácticas no solo buscan proteger los dispositivos contra amenazas externas e internas, sino también mejorar la gestión de los dispositivos en entornos empresariales, maximizando así la seguridad de la información y la infraestructura de red.