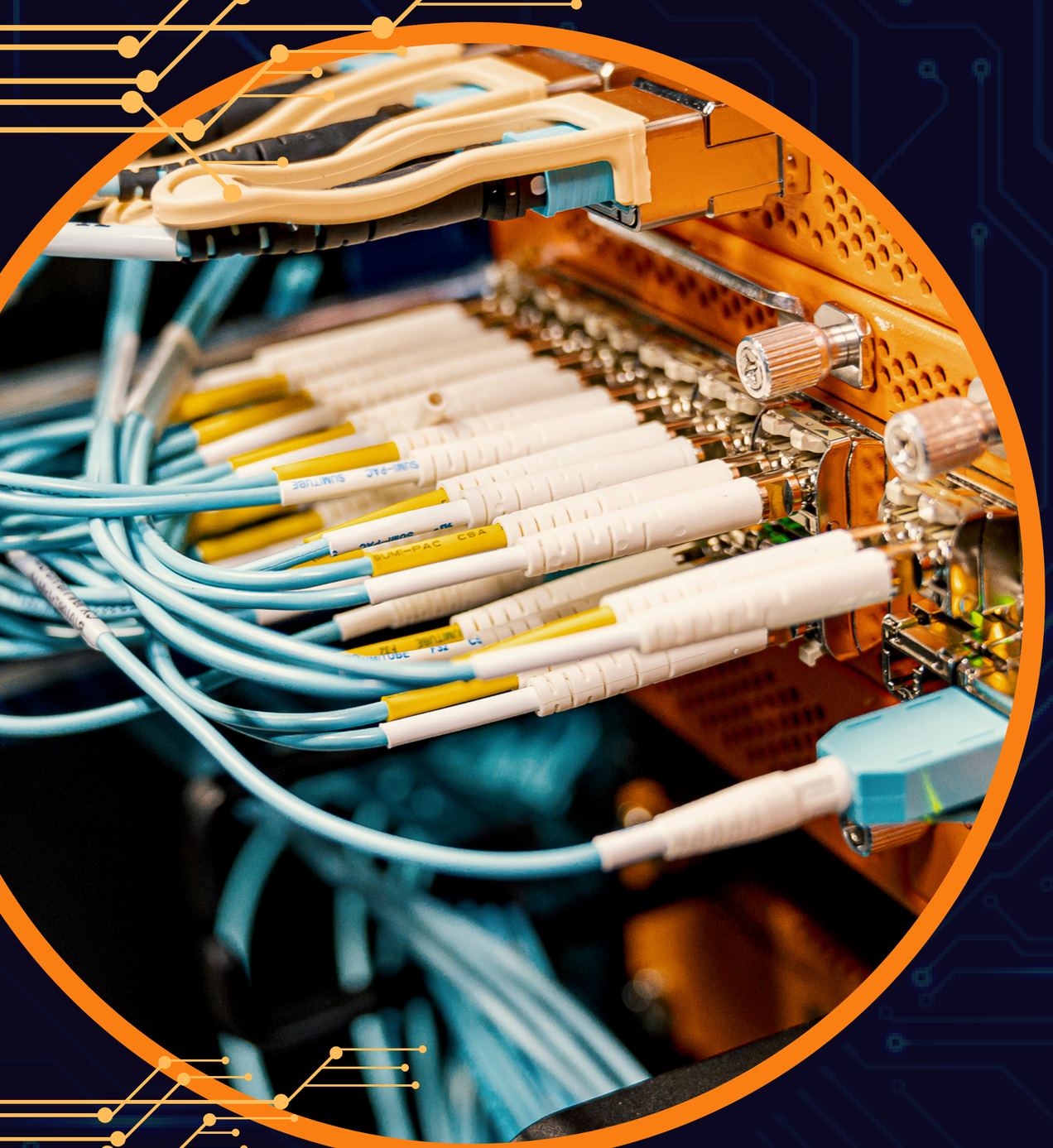

TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 1 –UNIDAD 2

Universidad Tecnológica de Pereira

faceIT

Hardening en sistemas informáticos

El hardening es el proceso de fortalecer la seguridad de un sistema, aplicación o red mediante la reducción de sus vulnerabilidades. Esto implica la eliminación de servicios innecesarios, la configuración adecuada de permisos, la actualización de software y la implementación de políticas de seguridad. El objetivo principal es minimizar la superficie de ataque, dificultando la explotación de posibles fallos y garantizando que el sistema sea más resistente frente a ciberataques.

Es necesario realizar hardening debido a que no todas las soluciones de software requieren de los mismos servicios activos. Un sistema operativo cualquiera, puede tener muchos servicios activos que le permiten a un computador o a un servidor compartir información en diferentes puertos, permiten conexiones entrantes y salientes, e incluso, los sistemas operativos suelen venir con múltiples programas y utilidades que pueden no requerirse en ciertos escenarios. Por ejemplo, un computador configurado como servidor de bases de datos no requiere interfaz de usuario y no debe admitir el ingreso de usuarios administradores fuera de su red local.

Sistemas Windows:

Es muy probable que la mayoría de usuarios de computadores portátiles y de mesa empleen como su sistema operativo principal Windows. También existen muchas soluciones que lo utilizan como el sistema operativo de sus servidores. Por este motivo es un objetivo atractivo para los atacantes ya que aprovechan de muchas de las características y servicios que ofrece Windows con el fin de atacarlo si no está correctamente configurado.

Algunas herramientas que permiten reforzar la seguridad son:

1. Realizar actualizaciones automáticas periódicamente, así como activar las actualizaciones automáticas.

2. Crear puntos de restauración del sistema con cierta frecuencia, que permitan retornar las configuraciones a un estado conocido.

3. No utilizar usuarios administradores en los sistemas. Por el contrario, restringir los permisos que un usuario puede tener para que no haga cambios que puedan dañar un equipo. Por ejemplo, si un usuario no requiere instalar programas o lo hace con muy poca frecuencia, se puede limitar su funcionalidad. De esta forma se mitiga el riesgo de que un usuario instale software malicioso.

4. Configure el cifrado de los datos en disco para que no puedan ser leídos sin que un usuario autorizado con la clave de desencriptado pueda iniciar sesión ni leer archivos. Esto mitiga el riesgo de que un atacante pueda robar información.

5. Ajustar la configuración de privacidad. No todos los usuarios / soluciones necesitan que todas las funcionalidades estén activas. Por ejemplo, si un grupo de usuarios solo necesita aplicaciones ofimáticas se les puede restringir el acceso por puertos ssh o RDP con el fin de evitar que atacantes intenten descifrar claves por fuerza bruta.

6. Limpieza: Un paso en el fortalecimiento de sistemas operativos es eliminar programas que no se necesitan. Con esto también se eliminan potenciales fallas de seguridad. Por ejemplo, si los usuarios no requieren editores de video nativos de Windows, se pueden eliminar. Si un servidor no tiene acceso de usuarios se puede utilizar una versión de Windows que no tenga entorno de escritorio. De esta forma se mitigan riesgos.

7. Escanear software instalado: Se recomienda emplear antivirus para verificar el que software que se instala no agregue brechas de seguridad. También es recomendable utilizar reglas de bloqueo de puertos para que un programa no pueda comunicarse por determinado puerto si no lo tiene autorizado.

8. Actualizar los controladores: Existen técnicas de hackeo que se basan en vulnerabilidades del hardware. Mantener los controladores actualizados mitiga las fallas.
9. Usar sandboxes. Son herramientas que permiten probar software sin que este se instale en un sistema, con eso se valida si este software tiene riesgos en la seguridad.

10. Usar el aislamiento de núcleo: Con el aislamiento de núcleo los equipos Windows protegen el sistema a nivel de hardware.

11. Usar contraseñas seguras: Existen versiones antiguas de Windows que permiten contraseñas poco seguras. Para evitar riesgos es mejor crear políticas de seguridad en los grupos de usuarios para que estos tengan que emplear contraseñas seguras (mas de 8 caracteres, números y caracteres especiales en la clave).

12. Configurar el firewall. Como se ha mencionado en otros apartados, el firewall debe configurarse para bloquear todos los puertos excepto los estrictamente necesarios.

13. Prepararse para los fallos: Es importante considerar que un sistema no es invulnerable, por lo que se recomienda mantener copias de seguridad automáticas y respaldos que, en caso de fallos, permitan reestablecer un sistema.

14. Ubicaciones y prácticas de seguridad: Los servidores deben ubicarse en lugares seguros, donde atacantes no puedan alcanzarlos. También es importante formar en seguridad informática básica a los usuarios de los sistemas. Prácticas sencillas como bloquear un equipo cuando no está siendo utilizado pueden mitigar muchos riesgos.

Fortalecimiento de sistemas Linux:

Los sistemas Linux son comúnmente usados en servidores, también hay computadores personales que emplean este sistema operativo. Las prácticas de hardening son similares al caso de Windows. Algunas prácticas extra y orientadas a los sistemas Linux son:

1. **Eliminar componentes** y funciones innecesarias
2. **Restringir los accesos** y las configuraciones de permisos tanto de archivos como de aplicaciones.
3. **Eliminar claves** por defecto.
4. **Compartimentar los servidores.** Una buena práctica de seguridad es aislar responsabilidades de servidores. En lugar de tener un único servidor para todas las aplicaciones que puede incrementar su vulnerabilidad, es preferible tener servidores virtualizados. Con esto, cada servidor virtualizado tiene sus accesos y restricciones independiente a otros. Además, mantener copias de seguridad y recuperar equipos con servidores virtualizados es mucho más fácil. En caso de que hayan brechas, solo se expone una parte de todo el sistema, evitando el desplazamiento horizontal.

5. Evitar el software innecesario. Muchas veces durante la configuración y el despliegue de servidores se instalan ciertas utilidades o programas de pruebas. Prácticas sencillas como eliminar estos programas y escanear constantemente los servidores mitigan los riesgos de seguridad.

6. Utilizar firewalls y reglas de acceso

7. Eliminar las cuentas no utilizadas y llevar un control de los usuarios autorizados.

8. Registrar y revisar constantemente la actividad, realizar auditorías de forma periódica. Con los registros de actividad es posible dar seguimiento a todo lo que ha sucedido en el sistema. Por ejemplo, si ocurre un cambio en la configuración se puede rastrear quien lo hizo y cuando. En caso de que esa actividad no sea reconocida, es más fácil detectar intrusiones al sistema. También es importante registrar advertencias y restringir los permisos a los registros del sistema para evitar su manipulación.

9. Automatizar la instalación de parches de seguridad

10. Eliminar controladores innecesarios. Por ejemplo, un servidor puede no requerir controladores de impresoras ni otros dispositivos que no serán conectados nunca.

Actividad: Guíe a sus estudiantes a instalar Virtual Box y una distribución de Linux de su preferencia. Una vez instalado realice el hardening del sistema limitando que por SSH no pueda iniciar sesión el usuario root. Guíe los estudiantes a eliminar software innecesario y a crear un firewall que permita bloquear puertos para proteger el acceso.