Universidad de Puerto Rico
Oficina de Sistemas de Información
UPR Administración Central

Guía de Configuración de Servicios Electrónicos

(System Hardening Standards)

Agosto 2022

Introducción

La Universidad de Puerto Rico, en su objetivo de proveer servicios eficientes y seguros, define las siguientes guías de configuración mínima requerida para todo nuevo sistema, aplicación o dispositivo, con la intención de establecer una línea de integridad y seguridad básica. Estas configuraciones son exclusivamente para las redes bajo la jurisdicción de la Universidad de Puerto Rico y siempre requiere de evaluación caso a caso para ser ajustadas basado en los requerimientos particulares de cada ambiente de trabajo.

Propósito

El objetivo de asegurar un sistema es eliminar cualquier funcionalidad innecesaria y configurar adecuadamente los requeridos de forma segura. Cada aplicación, servicio, o equipo instalado o habilitado en un sistema puede presentar riesgos por configuraciones genéricas o sin las debidas actualizaciones. El propósito de este documento es proveer a todos los administradores de sistemas de información, personal de tecnologías de información o el personal autorizado la información apropiada para cumplir con requisitos básicos de seguridad y configuración.

Servicios y Equipos de Comunicación

A continuación, se presenta una lista de los servicios típicos y la configuración mínima requerida:

1. SSH
    a. SSH deberá estar configurado con versión 2 de protocolo.[1]
    b. Hacer *login* directo de cuentas de administrador/root no será permitido.
    c. Aviso de la poítica institucional es requerido siempre y cuando el sistema así lo facilite (Apéndice A).
    d. Es altamente recomendado y preferido que la autenticación al sistema deberá ser utilizando certificados o llaves criptográficas.
    e. El servicio de SSH será configurado para resistir ataques de fuerza bruta
        i. Se aplicará un límite de 3-5 de intentos de login.

[1] https://sshcheck.com
https://www.sshaudit.com

ii. Activar “lock out” del sistema después de 5 intentos fallidos.

f. La habilidad de hacer “*TCP/X11 forwarding*” deberá estar deshabilitada.
g. SSH LogLevel debe ser apropiado para el registro de eventos a bitácora.
h. Utilizar "ciphers", algoritmos MAC, algoritmos de "key excahge" y algoritmos de "host key" considerados como seguros por la industria.

2. HTTP/HTTPS [2]
    a. Para servicios de producción se tienen que utilizar certificados de una autoridad (CA) reconocida.
    b. Todo servicio HTTPS publicado deberá ser configurado utilizando certificados auténticos y registrados bajo la UPR.
    c. El cifrado debe ser por medio de llaves de 2048 bits o mejor
    d. El protocolo TLS 1.2 y 1.3 serán utilizados por defecto. Cualquier versión anterior no es permitida.
    e. No se deben utilizar cifrados considerados inseguros (ADH, RC4, 3DES, etc.)
    f. Se recomienda hacer uso de "*Forward Secrecy Forward Secrecy*" y "*Strict Transport Security* (HSTS)".
    g. El servicio HTTP no será utilizado bajo ninguna circunstancia para la autenticación de usuarios o la transferencia de información sensitiva.
3. Remote Desktop Services
    a. No habrá acceso directo a ningún servicio RDP accesible desde el Internet.
    b. El acceso RDP solo deberá ser permitido a través de VPN o RDP Gateway.
4. Telnet y FTP
    a. El servicio de Telnet y/o FTP no será publicado al Internet o en redes públicas en ninguna circunstancia si no hace uso de un mecanismo de cifrado.
    b. SSH será la alternativa para Telnet, aún en redes privadas.
    c. SFTP será la alternativa en redes públicas o privadas.
5. LDAP
    a. El servicio de LDAP no será publicado al Internet o en redes públicas en ninguna circunstancia.
    b. El acceso al servicio tiene que ser por medio de LDAPS (cifrado) y restringido por IP.
    c. Se recomienda el uso de tecnologías como SAML o OpenID para propósitos de autenticación de servicios.
6. SIP/IAX
    a. Todo servicio de VoIP utilizado deberá utilizar mecanismos de cifrado de datos para autenticación y transmisión de datos.
7. SNMP
    a. El servicio de SNMP no deberá ser publicado al Internet o en redes públicas en ninguna circunstancia.
    b. El servicio no tendrá en ninguna circunstancia "public" o "private" como *community string*.

[2] https://www.ssllabs.com/ssltest
https://www.digicert.com/help

   c. El servicio debe ser protegido por medio de un ACL o regla de "firewall".
   d. La versión 3 del protocolo snmp será preferido sobre sus versiones anteriores.
8. NTP
   a. El servicio de NTP no deberá estár acesible a menos que sea estrictamente necesario.
   b. El servicio de NTP deberá tener los controles necesarios para evitar ataques de amplificación UDP si está accesible desde la red de datos.
9. SMTP
   a. El servicio de SMTP no deberá estár acesible a menos que sea estrictamente necesario.
   b. El servicio de SMTP deberá tener los controles necesarios para evitar ser utlizado como "relay".
   c. El servicio de SMTP debe terner configurado los récords DNS para resolución, SPF, etc según sea su función.
10. DNS
   a. El servicio de DNS no deberá estar accesible a menos que sea estrictamente necesario para servir una zona y/o sea utilizado para recursión de recursos en la red de la unidad.
   b. El servicio de DNS no deberá permitir recursión para consultas desde el Internet.

Dispositivos de Comunicación

1. Se requiere el cambio de nombres de cuentas y contraseñas predeterminadas por los manufactureros (cuentas *default*). Siempre que sea posible, se deben deshabilitar dichos accesos en los dispositivos.
2. Se debe revisar la configuración de los *firewalls*, *routers* o *switches* con las configuraciones seguras estándar definidas para cada tipo de dispositivo de red en uso. La configuración de seguridad de dichos dispositivos debe documentarse, revisarse y aprobarse mediante un proceso de gestión de cambios. Cualquier desviación de la configuración estándar o actualizaciones a la configuración estándar deben documentarse y aprobarse en un proceso de gestión de cambios.
3. Los dispositivos de red deben administrarse mediante autenticación de dos factores y sesiones cifradas.
4. La infraestructura de la red debe administrarse a través de conexiones de red que estén separadas del tráfico de los usuarios y sistemas en producción, basándose en VLAN separadas o, preferiblemente, en una conectividad física completamente diferente.
5. Si IPv6 no se está utilizando en una red o dispositivo, debe deshabilitarse.
6. La última versión estable del sistema operativo de los dispositivos de redes (IOS) o el *firmware* de este con actualizaciones de seguridad críticas debe instalarse dentro de los 30 días posteriores a la publicación de la actualización por parte del proveedor del dispositivo.
7. Solo protocolos y puertos en uso en los dispositivos de la red deben estar activos. Todas las interfaces y los puertos que no se utilizan deben deshabilitarse para evitar accesos no autorizados.
8. Habilitar "*port security*"
9. Deshabilitar *IP direct-broadcast* y *IP proxy-arp*.

10. Limitar el número de conexiones de administración simultáneas.
11. Reducir el riesgo de exponer las interfaces administrativas al tráfico de usuarios mediante la aplicación de listas de control de acceso a direcciones de IP específicas.
12. Registrar y supervisar todos los intentos de acceder a los dispositivos de red.

Servidores y estaciones de trabajo

1. Deshabilitar todos los puertos de comunicación que su uso no esté justificado.
2. Detener o eliminar servicios de sistema operativo que no estén en uso.
3. Desinstalar software preinstalado que no se hará uso de él. Esto incluye además cambiar o desactivar la configuración predeterminada (*default*) y eliminar funciones o aplicaciones innecesarias, incluyendo aquellas que los manufactureros habilitan para monitorear y reportar eventos en los sistemas.
4. Habilitar encriptación en los discos de almacenamiento locales en las estaciones de trabajo; Bitlocker para Windows y FileVault para MacOS. Para sistemas Linux se recomienda VeraCrypt.
5. El antivirus tiene que instalarse y activarse, además del firewall a nivel de sistema operativo.
6. Las actualizaciones de sistema operativo y de las aplicaciones deben alertarse y poner como requisito aplicarlas una vez están disponibles.
7. Aplicar política de contraseñas segura, deshabilitar el inicio de sesión automático y habilitar el bloqueo automático por inactividad en las consolas.
8. En los servidores que sea posible, restringir los accesos basados en IPs conocidos como permitidos a tener acceso.
9. Los servidores y servicios que corren en ellos deben configurarse en aplicaciones de monitoreo como Observium, Nagios y LibreNMS. (Ver https://eagle.upr.edu/noc).

Servicios Remotos Públicos

1. Servicios como Moodle, WordPress, entre otros que son comúnmente utilizados en nuestra institución y sin costos, deberán mantenerse en las últimas versiones y aplicando parchos según sea necesario. Servicios que no sean mantenidos adecuadamente, serán desactivados y bloqueados.
2. Los servicios de páginas web serán solo permitidos utilizando protocolos seguros. Ver sección de **Servicios y Equipos de Comunicación**.
3. De ser posible, requerir *two-factor authentication* para acceder servicios con acceso controlado.
4. Los servidores y servicios que corren en ellos deben configurarse en aplicaciones de monitoreo como Observium y/o Nagios. (Ver https://eagle.upr.edu/noc)

Servicios Remotos Privados

1. Accesos remotos a recursos internos de la universidad (ej. SIA), tienen que ser accedidos a través de servicio de *Virtual Private Network* (VPN).
2. De ser posible, requerir *two-factor authentication* para acceder servicios con acceso controlado.
3. Evite el uso de *Remote Desktop Protocol* (RDP) aún dentro de la red privada. Si es requerido su uso, asegure que se tiene los controles necesarios para proteger el acceso al servicio.

Monitoreo

Los sistemas críticos deberán ser integrados a la solución de monitores utilizado por la unidad institucional responsable de esta, proveyendo notificaciones automáticas cuando ocurren eventos inusuales.

Apéndice A

Mensaje para Desplegarse en los Sistemas Accesibles a los Usuarios

---

Política Institucional sobre el Uso y Acceso a los Recursos de la Tecnología de la Información

Derechos y responsabilidades de los Usuarios

La Universidad de Puerto Rico, según la Certificación Número 85 (2022-2023), aprobó la Política Institucional sobre el Uso y Acceso a los Recursos de la Tecnología de Información en la Universidad de Puerto Rico.

Las disposiciones contenidas en esta política se aplican a todos los usuarios de la TI de la Universidad sin limitarse a estudiantes, facultad, investigadores, empleados y terceros, tales como contratistas, suplidores externos, consultores y visitantes, además de las corporaciones afiliadas a la Universidad. Los terceros que usen alguna parte de la TI de la Universidad también están sujetos a esta Política, incluso con equipo o programados que sean o no propiedad de la Universidad.

Toda vez que el acceso a las redes y al ambiente de las tecnologías de información es un privilegio institucional que otorga la Universidad de Puerto Rico, todos los usuarios tienen la responsabilidad de usar estos recursos responsablemente para asegurar su integridad, seguridad y disponibilidad para actividades apropiadas de carácter educativo, investigativo, de servicio, y otras actividades de la institución.

Derechos y responsabilidades de la Universidad

La Universidad es dueña de toda la infraestructura tecnológica que compone la TI. De la misma forma, la Universidad es dueña de todos los datos que residen en dicha infraestructura tecnológica y es responsable de tomar las medidas necesarias para proteger la disponibilidad, integridad, seguridad y la confidencialidad de la TI.
