DATOS DE LA ACTIVIDAD							
No. de Actividad:	**1.5**	**Investigación**	**Investigación de SSH, SNMP, NTP**				
Unidad:	Unidad: 1: Riesgos de seguridad informática en infraestructura de red						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**Seguridad en ITI**					Clave	**MPF3608DSO**
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	26/02/2021
Compet. Genéricas	4.1, 4.5, 5.2, 5.5			Competencia Profesional		CP1-1	

1. Objetivo(s) de la actividad

Conocer los protocolos de configuración remota, de sincronización de tiempo y administración de registros en una red.

2. Instrucciones (Descripción) de la actividad

- Investigar la función y descripción de los protocolos SSH, SNMP y NTP.
- Usar el archivo de ejemplo de actividades, para realizar esta actividad.
- Subir el archivo terminado y dar clic para marcar como entregada la actividad.

3. Desarrollo de la actividad

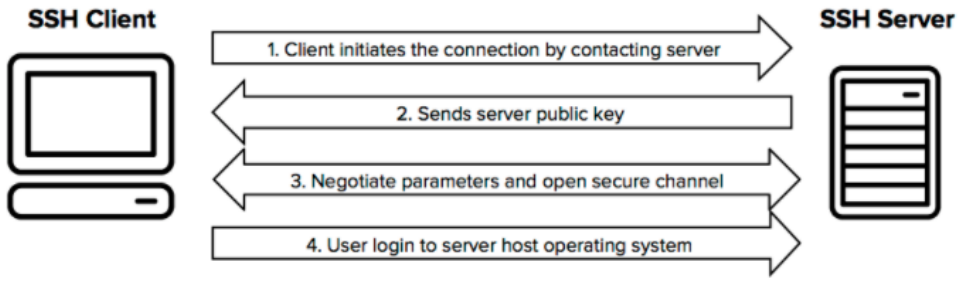
SSH

El protocolo SSH (también conocido como Secure Shell) es un método para el inicio de sesión remoto seguro de una computadora a otra. Proporciona varias alternativas para una autenticación sólida y protege la seguridad e integridad de las comunicaciones con un cifrado sólido. Es una alternativa segura a los protocolos de inicio de sesión no protegidos (como telnet, rlogin) y los métodos de transferencia de archivos inseguros (como FTP). El protocolo se utiliza en redes corporativas para:

- Proporcionar acceso seguro para usuarios y procesos automatizados
- Transferencias de archivos interactivas y automatizadas
- Emitir comandos remotos
- Administrar la infraestructura de red y otros componentes del sistema de misión crítica.

El protocolo funciona en el modelo cliente-servidor, lo que significa que la conexión la establece el cliente SSH que se conecta al servidor SSH. El cliente SSH dirige el proceso de configuración de la conexión y utiliza criptografía de clave pública para verificar la identidad del servidor SSH. Después de la fase de configuración, el protocolo SSH utiliza un cifrado simétrico fuerte y algoritmos hash para garantizar la privacidad e integridad de los datos que se intercambian entre el cliente y el servidor.

La siguiente figura presenta un flujo de configuración simplificado de una conexión SSH.



SNMP

El Protocolo simple de administración de red (SNMP) es un protocolo ampliamente utilizado para monitorear la salud y el bienestar de los equipos de red (por ejemplo, enrutadores), equipos informáticos e incluso dispositivos como UPS. Net-SNMP es un conjunto de aplicaciones que se utilizan para implementar SNMP v1, SNMP v2c y SNMP v3 utilizando tanto IPv4 como IPv6. La suite incluye:

- Aplicaciones de línea de comandos para:
  - recuperar información de un dispositivo compatible con SNMP, ya sea mediante solicitudes únicas (snmpget, snmpgetnext) o solicitudes múltiples (snmpwalk, snmptable, snmpdelta).
  - manipular la información de configuración en un dispositivo compatible con SNMP (snmpset).
  - recuperar una colección fija de información de un dispositivo compatible con SNMP (snmpdf, snmpnetstat, snmpstatus).
  - convertir entre formas numéricas y textuales de MIB OID, y mostrar el contenido y la estructura de MIB (snmptranslate).
- Un navegador gráfico MIB (tkmib), usando Tk / perl.
- Una aplicación demonio para recibir notificaciones SNMP (snmptrapd).
- Las notificaciones seleccionadas se pueden registrar (en syslog, NT Event Log o en un archivo de texto sin formato), reenviar a otro sistema de administración SNMP o pasar a una aplicación externa.
- Un agente extensible para responder a consultas SNMP de información de gestión (snmpd). Esto incluye soporte integrado para una amplia gama de

módulos de información MIB y se puede ampliar utilizando módulos cargados dinámicamente, scripts y comandos externos, y los protocolos de multiplexación SNMP (SMUX) y Agent Extensibility (AgentX).
- Una biblioteca para desarrollar nuevas aplicaciones SNMP, con API de C y perl.

NTP

El Network Time Protocol (NTP) es un protocolo de red para la sincronización del reloj entre sistemas informáticos a través de redes de datos de latencia variable y conmutación de paquetes. En funcionamiento desde antes de 1985, NTP es uno de los protocolos de Internet más antiguos que se utilizan actualmente. NTP fue diseñado por David L. Mills de la Universidad de Delaware.

NTP está diseñado para sincronizar todas las computadoras participantes en unos pocos milisegundos de la hora universal coordinada (UTC). Utiliza el algoritmo de intersección, una versión modificada del algoritmo de Marzullo, para seleccionar servidores de tiempo precisos y está diseñado para mitigar los efectos de la latencia variable de la red. NTP generalmente puede mantener el tiempo dentro de decenas de milisegundos en la Internet pública y puede lograr una precisión superior a un milisegundo en redes de área local en condiciones ideales. Las rutas asimétricas y la congestión de la red pueden provocar errores de 100 ms o más.

El protocolo generalmente se describe en términos de un modelo cliente-servidor, pero puede usarse fácilmente en relaciones de igual a igual donde ambos pares consideran que el otro es una fuente de tiempo potencial. Las implementaciones envían y reciben marcas de tiempo usando el Protocolo de datagramas de usuario (UDP) en el puerto número 123. También pueden usar transmisión o multidifusión, donde los clientes escuchan pasivamente las actualizaciones de tiempo después de un intercambio inicial de calibración de ida y vuelta. NTP proporciona una advertencia de cualquier ajuste de segundo intercalar inminente, pero no se transmite información sobre las zonas horarias locales o el horario de verano.

El protocolo actual es la versión 4 (NTPv4), que es un estándar propuesto como se documenta en RFC 5905. Es compatible con la versión 3, especificada en RFC 1305.

4. Reflexión

Con base a esta investigación hemos desarrollado los conocimientos relacionados a una serie de protocolos que son de suma importancia para garantizar un grado de seguridad dentro de la infraestructura de los sistemas de información. Cada uno de estos protocolos de manera independiente favorece de un modo particular a la seguridad de la red, pero en conjunto se apoyan para generar un grado de seguridad aún más alto.

Referencias:

- Anónimo (2020). SSH Protocol. Recuperado el 26 de febrero de 2021 desde: https://www.ssh.com/ssh/protocol/
- Anónimo (febrero 26, 2013). Net-SNMP. Recuperado el 26 de febrero de 2021 desde: http://www.net-snmp.org/
- Mills, D. (mayo 13, 2021). Network Time Synchronization Research Project. Recuperado el 26 de febrero de 2021 desde: https://www.eecis.udel.edu/~mills/ntp.html