Práctica III.: Protocolos Seguros y Auditorías de Seguridad (4 sesiones - 8 horas)

Prof. A. Santos del Riego
Legislación y Seguridad Informática (LSI)
Facultad de Informática. Universidad de A Coruña
Fecha propuesta.: enero-2004
Última revisión.: noviembre-2022

El objetivo de esta práctica es comprender la importancia de los algoritmos criptográficos, el uso de autoridades de certificación y su aplicación-funcionamiento en la forma de protocolos seguros. También se abordará el proceso de análisis de vulnerabilidades en el contexto de los procesos de auditoría de seguridad. Se deberán aplicar los conceptos adquiridos en la resolución de los siguientes apartados:

1. Tomando como base de trabajo el SSH pruebe sus diversas utilidades:
    a. Abra un *shell* remoto sobre SSH y analice el proceso que se realiza. Configure su fichero `ssh_known_hosts` para dar soporte a la clave pública del servidor.
    b. Haga una copia remota de un fichero utilizando un algoritmo de cifrado determinado. Analice el proceso que se realiza.
    c. Configure su cliente y servidor para permitir conexiones basadas en un esquema de autenticación de usuario de clave pública.
    d. Mediante túneles SSH securice algún servicio no seguro.
    e. "Exporte" un directorio y "móntelo" de forma remota sobre un túnel SSH.
    f. PARA PLANTEAR DE FORMA TEÓRICA.: *Securice su sevidor considerando que únicamente dará servicio ssh para sesiones de usuario desde determinadas IPs.*
2. Tomando como base de trabajo el servidor Apache2
    a. Configure una Autoridad Certificadora en su equipo.
    b. Cree su propio certificado para ser firmado por la Autoridad Certificadora. Bueno, y fírmelo.
    c. Configure su Apache para que únicamente proporcione acceso a un determinado directorio del árbol web bajo la condición del uso de SSL. Considere que si su la clave privada está cifrada en el proceso de arranque su máquina le solicitará la correspondiente frase de paso, pudiendo dejarla inalcanzable para su sesión ssh de trabajo.
3. Tomando como base de trabajo el openVPN deberá configurar una VPN entre dos equipos virtuales del laboratorio que garanticen la confidencialidad entre sus comunicaciones.

4. EN LA PRÁCTICA 1 se configuró una infraestructura con servidores y clientes NTP. Modifique la configuración para autenticar los equipos involucrados.
5. EN LA PRÁCTICA 1 se instalaron servidores y clientes de log. Configure un esquema que permita cifrar las comunicaciones.
6. En este punto, cada máquina virtual será servidor y cliente de diversos servicios (NTP, syslog, ssh, web, etc.). Configure un "firewall stateful" de máquina adecuado a la situación actual de su máquina.
7. Instale el SIEM splunk en su máquina. Sobre dicha plataforma haga los siguientes puntos.:
    a. Genere una query que visualice los logs internos del splunk
    b. Cargué el fichero `/var/log/apache2/access.log` y el `journald` del sistema y visualícelos.
    c. Obtenga las IPs de los equipos que se han conectado a su servidor web (pruebe a generar algún tipo de gráfico de visualización), así como las IPs que se han conectado un determinado día de un determinado mes.
    d. Trate de obtener el país y región origen de las IPs que se han conectado a su servidor web y si posible sus coordenadas geográficas.
    e. Obtenga los `hosts` origen, `sources` y `sourcestypes`.
    f. ¿cómo podría hacer que splunk haga de servidor de log de su cliente?
8. Ejecute la utilidad de auditoría de seguridad *lynis* en su sistema y trate de identificar las acciones de securización detectadas así como los consejos sobre las que se deberían contemplar.
9. EN LA PRÁCTICA 2 se obtuvo un perfil de los principales sistemas que conviven en su red, puertos accesibles, *fingerprinting*, paquetería de red, etc. Seleccione un subconjunto de máquinas del laboratorio de prácticas y la propia red. Elabore el correspondiente informe de análisis de vulnerabilidades. Puede utilizar como apoyo al análisis la herramienta Nessus Essentials (disponible para educación en https://www.tenable.com/tenable-for-education/nessus-essentials bajo registro para obtener un código de activación) para su instalación en la máquina debian de prácticas. Como opción alternativa, también podría instalar Greenbone Vulnerability Management (GVM). Como referencia-plantilla puede utilizar.:
    a. Writing a Penetration Testing Report del SANS (SysAdmmin Audit, Networking and Security) Institute. Muestra las etapas o fases del desarrollo de un "report", describe el formato del "report" y finaliza con un ejemplo. http://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343?show=writing-penetration-testing-report-33343&cat=bestprac
    b. Plantilla de vulnerabilityassessment.co.uk. http://www.vulnerabilityassessment.co.uk/report%20template.html