Seminario IV.: Protocolos Seguros y Auditorías de Seguridad (2 sesiones – 4 horas)

Prof. A. Santos del Riego
Legislación y Seguridad Informática (LSI)
Facultad de Informática. Universidad de A Coruña
Fecha propuesta.: enero-2004
Última revisión.: septiembre-2013

El objetivo de este seminario es comprender la importancia de los protocolos seguros y la necesidad, en nuestras organizaciones, de procesos de auditoría y análisis de vulnerabilidades. Se deberán aplicar los conceptos adquiridos en la resolución de los siguientes apartados:

1. EN LA PRÁCTICA 1 se configuró una infraestructura con servidores y clientes NTP. Modifique la configuración para permitir cifrar el tráfico entre los equipos.
2. EN LA PRÁCTICA 1 se instalaron servidores y clientes de log. Configure un esquema que permita cifrar las comunicaciones.
3. EN EL SEMINARIO 2 se obtuvo un perfil de los principales sistemas que conviven en su red, puertos accesibles, *fingerprinting*, paquetería de red, etc. Instale el paquete openvas para hacer un análisis de vulnerabilidades contra alguno de esos sistemas. Por ejemplo, contra una de las debian con autenticación de usuario lsi, firewall o servidor DNS. ¿Ha detectado alguna vulnerabilidad?. ¿Cómo solucionaría el problema?.
4. APARTADO OPCIONAL PARA HACER EN CASA. Durante muchos años nessus ha sido uno de los analizadores de vulnerabilidades por excelencia. Las restricciones en este paquete introducidas en los últimos años ha hecho que elijamos openvas como la opción de pruebas en la asignatura. De todas formas, recomiendo que se pruebe la versión home de nessus para ver el funcionamiento de este entorno (en vuestras casas con la versión home atendiendo a las licencias de TNS).
5. Instale el analizador de vulnerabilidades web nikto2. Analice alguno de los servicios web del laboratorio, como por ejemplo el propio del backuppc, entre otros posibles. ¿Ha detectado algún problema de seguridad?. ¿Cómo solucionaría el problema?.
6. Instale el analizador de aplicaciones web w3af. Pruebe dicho entorno sobre aplicativo web disponible en la red del laboratorio de prácticas y, o, sobre entornos de prueba-labs disponibles en la red. Haga pruebas con alguna vulnerabilidad típica del aplicativo web, como XSS o SQLi.
7. 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.
8. Seleccione un subconjunto de máquinas del laboratorio de prácticas y la propia red. Considerando todos lo realizado hasta la fecha en las prácticas y seminarios de la asignatura, elabore el correspondiente informe de análisis de vulnerabilidades. 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. Pen test "report" modelo-plantilla de niiconsulting.com. Incluye plantilla. http://www.niiconsulting.com/services/security_assessment/NII_Sample_PT_Report.pdf
   c. Vulnerability Assessment and Pen testing de Cynergi Solutions. http://digitalencode.net/ossar/ossar_v0.5.pdf
   d. Plantilla de vulnerabilityassessment.co.uk. http://www.vulnerabilityassessment.co.uk/report%20template.html
   e. Ejemplo de "report" de pen test de Offensive Security. http://www.offensive-security.com/penetration-testing-sample-report.pdf