Universidad de La Laguna

Práctica de Laboratorio #11. Hardening con SELinux y AppArmor

En esta práctica vamos a instalar dos máquinas virtuales (una Ubuntu Server 16.04 y una CentOS7) para estudiar las configuraciones de hardening del S.O. basados en un control de acceso MAC implementadas en estos sistemas con AppArmor y SELinux respectivamente.

Utilizaremos [DVWA], una aplicación web vulnerable para realizar las pruebas en los dos servidores y realizar una comparativa con las diferentes soluciones para securizar el sistema. El repositorio de GitHub de DVWA tiene información actualizada. ¡¡OJO!! DVWA no funciona con php7. Hay que usar versiones más antiguas. Por eso no usamos Debian9 como plantilla base.

Como guía puede consultar la información especificada en este tutorial: Using DVWA to Test Hardening Apache Techniques. Puede estar algo desactualizada. También pueden consultar este curso en Computer Security Student (CSS)

Ejercicios

1. Instalar una máquina virtual de Ubuntu server y una máquina virtual para CentOS. Realizaremos las pruebas en estos dos sistemas.
2. Instalaremos apache en los dos sistemas y configuraremos el servidor web para la aplicación vulnerable [DVWA]. Para CentOS/Fedora hay una guía, en el curso de CSS.
3. Una vez tengamos los dos sistemas en sus instalaciones por defecto y con DVWA implantada, comprobar las vulnerabilidades que se presentan.
4. En Ubuntu Server comprobaremos si existe un [perfil de seguridad en AppArmor para Apache]. Activarlo y comprobar nuevamente las vulnerabilidades ahora evitadas.
5. Podemos también probar SELinux en Ubuntu server. Para ello hay que desinstalar apparmor e instalar selinux (no son compatibles):

   ```
   # apt-get remove apparmor
   # apt-get install selinux
   ```

   Editar `/etc/selinux/config` y activar SELinux con `SELINUX=enforcing`

Entrega

Escribir un informe comentando las pruebas y configuraciones realizadas. Describir las vulnerabilidades disponibles en el test y cuales se resuelven con las técnicas de hardening sin tener que tocar la aplicación. El informe final debe incluir un tabla similar a la de la de la figura ():

	A	B	C	D	E	F
1		Ubuntu 10.10 64-bit Default Install	CentOS 5.5 Default Install	Ubuntu App Armor	Ubuntu Chroot	Ubuntu SElinux (enforcement default)
2	Creating file in temp folders /var/tmp	✓	X	X	X	X
3	create file in web root	X	X	X	X	X
4	Command injection (successful)	✓	Limited	X	X	
5	cat /etc/passwd	✓	✓	X	X	✓
6	Create a crontab	✓	X	X	X	X
7	wget a file	✓	X	X	X	✓
8	Reverse Shell	✓	X	X	X	✓
9						
10						
11						
12	**Remote File Upload**					
13	web proxy	✓	X	✓	✓	✓
14	dns lookup	✓	X	✓	✓	✓