# Universidad Politécnica de Cartagena


## Escuela Técnica Superior de Ingeniería de Telecomunicación

## SEGURIDAD EN REDES DE COMUNICACIONES

# Práctica 0: Escáneres de red.

**María Dolores Cano Baños**

**Natalio López Martínez**

# 1. Introducción (openvas)

La tarea de auditar un gran número de sistemas buscando posibles vulnerabilidades es bastante laboriosa. Para simplificar esta tarea se pueden utilizar herramientas de rastreo o escáneres de seguridad. Un escáner de seguridad es una herramienta que permite detectar la existencia de vulnerabilidades en una red de forma automática. Nmap y Openvas son dos ejemplos de este tipo de herramientas.

Nmap es un rastreador de puertos diseñado para explorar grandes redes y determinar qué equipos se encuentran activos y cuáles son los servicios TCP y UDP que ofrecen. Nmap es un programa gratuito, disponible en http://www.insecure.org/nmap. En esta dirección, también podemos encontrar el paquete Nmapfe, una interfaz gráfica para Nmap.

Openvas es un escáner de seguridad libre, fiable y muy flexible (se puede descargar desde http://www.Openvas.org). Está diseñado siguiendo una arquitectura cliente/servidor. El servidor/demonio, 0penvasd, se encarga de realizar la búsqueda de vulnerabilidades en los sistemas remotos (lanza ataques). Mientras que el cliente, 0penvas, proporciona al usuario una atractiva interfaz X11/GTK+, que permite conectarse al servidor, configurar y lanzar los rastreos. Una vez inspeccionado un equipo o una red, Openvas elabora un informe exhaustivo en el que se describen los riesgos encontrados, y posibles soluciones, junto con una referencia CVE (*Common Vulnerablities and Exposures*). CVE es una enorme base de datos, disponible en http://cve.mitre.org, donde se puede encontrar información sobre problemas de seguridad conocidos.

Los ataques reciben el nombre de “plugins” y son los encargados de detectar vulnerabilidades. Existen varias familias de *plugins*: puertas traseras, denegación de servicio o acceso *root* remoto. En la página WEB de Openvas se puede encontrar información sobre ellos. La librería de *plugins* no es algo estático, sino que se incrementa con la aparición y conocimiento de nuevas vulnerabilidades. Se pueden programar *plugins* utilizando lenguajes como C, o el lenguaje NASL (*Nessus Attack Sripting Language*).

# 2. Objetivos

El objetivo principal de esta práctica es familiarizarse con el uso de los escáneres de red, en particular, con las aplicaciones Nmap y Openvas. Al terminar esta práctica el alumno debe saber:

- Cómo instalar y ejecutar Nmap.
- Cómo instalar, configurar y ejecutar el servidor 0penvasd.
- Cómo añadir usuarios a la lista de usuarios autorizados para realizar una inspección usando 0penvas.
- Cómo lanzar una inspección.
- Cómo obtener e interpretar un informe de vulnerabilidades.
- Cómo actualizar la base de *plugins*.

# 3. Documentación

La documentación que acompaña a este guión de prácticas es la siguiente:

- Página de ayuda del programa `nmpafe`. En esta página se resumen las principales características de la aplicación nmap.
- Pagina de ayuda del programa `Openvasd`. En está página encontrará la información necesaria para ejecutar el servidor Openvas y sus distintas opciones de configuración.
- Página de ayuda del programa `Openvas`. En esta página encontrará ayuda sobre cómo ejecutar el cliente Openvas.
- Página de ayuda del comando `Openvas-adduser`. En esta página encontrará información sobre cómo añadir nuevos usuarios a la lista de usuarios autorizados a lanzar inspecciones.

# 4. Desarrollo de la práctica

Para ejecutar alguno de los comandos de esta práctica es necesario tener permisos de supervisor, por lo que se recomienda realizar la práctica como usuario **root**.

## 4.1 Instalación y ejecución de Nmap

Lo primero que tenemos que realizar es la instalación del programa Nmap para ello ejecutamos el comando:

# yast2 (También se puede ejecutar directamente desde el interfaz gráfico)

# buscamos el paquete 'NMAP'

En el directorio donde se encuentran estos dos programas podemos saberlo con el comando que nos proporciona linux mediante la instrucción whereis:.

- Compruebe que la instalación ha funcionado correctamente, por ejemplo, comprobando que existe la página de ayuda de `nmap` o `nmapfe`.

**Cuestión 1. ¿En qué directorio se encuentran estos dos programas?**

- Lance la aplicación `nmapfe`.
- Inicie un rastreo de puertos en toda la red del laboratorio.

**Cuestión 2. ¿Cuántas máquinas se han rastreado?**

**Cuestión 3. ¿Qué puede decir de la máquina cuya dirección es 192.168.5.x (indicada por el profesor)?**

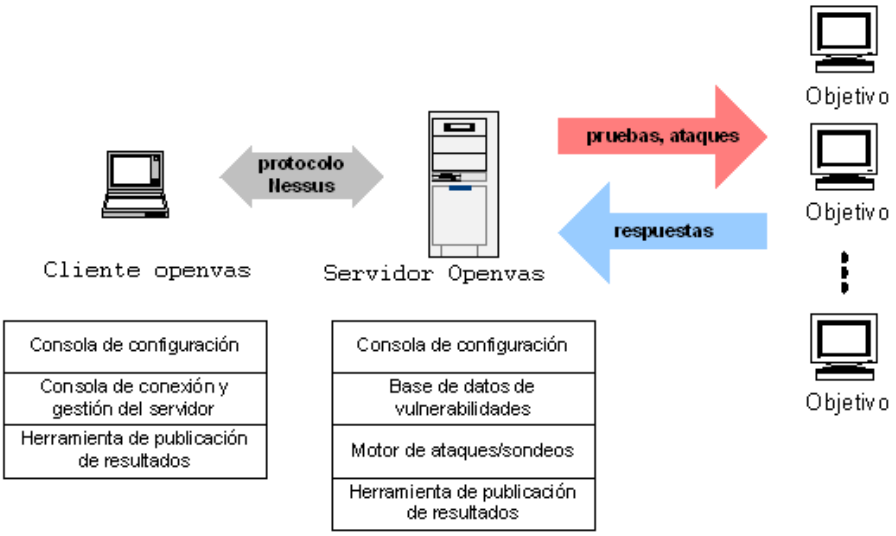
- Desinstale los dos paquetes con los siguientes comandos:

# yast2

## 4.2 Aplicación Openvas

### 4.2.1 Arquitectura

La arquitectura que conforma una aplicación Openvas es la que se observa en la siguiente figura:




El cliente `Openvas` solicita al servidor `Openvasd` que lance una serie de ataques sobre una serie de equipos o redes objetivo ("*target*"). Aunque en la figura hay tres partes diferencias, cliente, servidor y *target* o diana, cada grupo de prácticas utilizará un solo ordenador que actuará como cliente, servidor.

### 4.2.2 Instalación de Openvas

En el directorio `/home/alumnos/src/software` se encuentra el archivo `Openvas-3.2.1-suse10.0.i586.rpm`. Copie este fichero en el directorio `/root` de su PC y ejecute los siguientes comandos:

(`rpm –vhU` *`nombre_paquete`*)

O utilice 'YAST2'.

Tras la instalación, compruebe que existen los programas `Openvasd` y `Openvas` (por ejemplo, usando el comando `whereis`).

**Cuestión 4. ¿En qué directorio se encuentra el programa `Openvas`? ¿Y `Openvasd`?**

### 4.2.3 Añadir un usuario

Consulte la página de ayuda del comando Openvas-adduser y añada un usuario con las siguientes características: (1) el usuario sólo podrá acceder al servidor desde PC situados en el laboratorio IT-5, (2) el usuario sólo podrá lanzar ataques a PC situados en el laboratorio IT-5, a excepción del servidor (192.168.5.254) y (3) el tipo de autenticación será "*pass*".

**Cuestión 5. Rellene la siguiente tabla:**

| | |
|---|---|
| PUESTO | |
| Login: | |
| Auth: | |
| One time Password: | |
| Rules | |

Ahora que tenemos nuestro usuario, vamos a crear un certificado para el servidor Openvasd.

Ésto se consigue ejecutando el comando:

# *Openvas-mkcert*

---
Creation of the Openvas SSL Certificate
---
This script will now ask you the relevant information to create the SSL certificate of Openvas. Note that this information will *NOT* be sent to anybody (everything stays local), but anyone with the ability to connect to your
Openvas daemon will be able to retrieve this information.
CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [FR]: ES
Your state or province name [none]: Murcia
Your location (e.g. town) [Paris]: Cartagena
Your organization [Openvas Users United]: UPCT
---

### 4.2.4 Modificar la configuración de Openvasd

**Cuestión 6. ¿En qué directorio se encuentra el fichero de configuración del servidor** Openvasd**? ¿Cuál es el nombre de ese fichero?**

Modifique la configuración por defecto del servidor para que el número máximo de PC que se pueden inspeccionar a la vez sean 10.

**Cuestión 7. ¿Cuál es el parámetro que tiene que modificar?**

Modifique la configuración por defecto del servidor para que el número de *plugins* lanzados de forma simultánea contra un PC, sea 5.

**Cuestión 8. ¿Cuál es el parámetro que tiene que modificar?**

### 4.2.5 Ejecución del servidor

Consulte la página de ayuda de Openvasd y ejecute el programa Openvasd en *background*.

**Cuestión 9. ¿Qué opción le permite ejecutar el servidor en background?**

**Cuestión 10. ¿Cuántos *plugins* existen actualmente?**

### 4.2.6 Ejecución del cliente Openvas e inspección la red

Consulte la página de ayuda del cliente Openvas y lance la aplicación. Conéctese al servidor y lance una inspección a todos los equipos de la red.

**Cuestión 11. ¿Qué usuario y contraseña ha utilizado para conectarse?**

### 4.2.7 Elaboración de un informe

Una vez finalizada la inspección, el cliente Openvas le permite elaborar un informe. Hágalo usando la opción "HTML with pies and Graphs".

**Cuestión 12. ¿Qué vulnerabilidades se han encontrado? ¿Cuál es su factor de riesgo? ¿Qué se propone como solución?**

**Cuestión 13. ¿En qué consiste el CEV-2003-0386? ¿Y el CEV-2000-0666?**

**Cuestión 14. ¿Qué otras vulnerabilidades existen en el laboratorio?**

### 4.2.8 Actualización de plugins

Puede actualizar el conjunto de ataques disponibles ejecutando el comando **openvas-nvt-sync**. Hágalo y compruebe si el número de *plugins* ha aumentado.

**Cuestión 15. ¿De cuántos *plugins* dispone ahora?**

**Cuestión 16. Vuelva a inspeccionar su equipo, ¿ha encontrado nuevas vulnerabilidades?**

### 4.2.9 Desinstalación de Openvas

Para terminar la práctica, desinstale el escáner de red.

**Cuestión 17. ¿Qué comando ha utilizado?**

# 5. Referencias

http://www.insecure.org/nmap

http://cve.mitre.org

http://www.Openvas.org

Nitesh Dhanjani, "*Hackers en Linux y Unix*, " 2003 McGrawHill. ISBN:84-481-4050-8.

Chris McNab, "*Seguridad de Redes*, " 2004 Anaya Multimedia. ISBN: 84-415-1751-7.