Pentesting Red Grupo GLUD

Leidy Marcela Aldana,* Andres Acosta Pulido,† Diego Andres Osorio,‡ and Miguel Angel Rodriguez§
Universidad Distrital Francisco José de Caldas.
GISEPROI Grupo de Investigación en Sistemas Empresariales y Protección de la Información
Curso Seguridad de la Información
Docente: Paulo Cesar Coronado

(Dated: March 4, 2017)

NOTA: ESTE TUTORIAL ESTA HECHO CON FINES EDUCATIVOS Y DE ENSEÑANZA. EL USO NO ADECUADO DEL MATERIAL ES BAJO SU RESPONSABILIDAD.

Se realiza una prueba de penetración (pentesting), el cual es un ataque a un sistema informático con la intención de encontrar las vulnerabilidades de seguridad, en diferentes puertos que tiene la red de Grupo GNU/LINUX de la Universidad Distrital.

Se utiliza nmap para generar el reporte de cuantas computadores estaban conectadas en la red del GLUD. Se generó un mapa de red, dando un reporte de cada computador gracias a la herramienta OpenVAS[a] (Open Vulnerability Assessment System), la cual tiene como funcionalidad identificar los tipos de vulnerabilidades que tiene cada computadora del Laboratorio de Tecnologías libres.

INTRODUCCIÓN

Como respuesta a la necesidad de detectar y prevenir intrusos surgen las herramientas OSSIM (Open Source Security Information Managment), clasificadas en dos grupos:

1. Pasivas: analizan sin generar tráfico dentro de la red *ejemplos: Snort, Ntop, NFdump, NFSnet, Kisnet*

2. Activas: generar tráfico dentro de la red en la que se encuentran *ejemplos: OpenVAS, nmap, Nagios, OSSEC, OCS*

Cada una de estas herramientas sirve para un propósito específico de seguridad, se definió previamente en el aula de clase utilizar en este laboratorio como

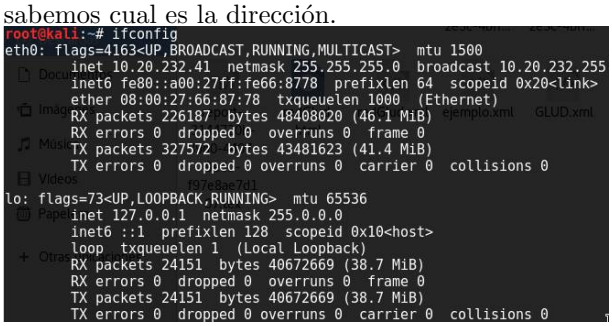
primera instancia dos herramientas OSSIM activas, llamadas **nmap** Y **OpenVAS**, las cuales detectan el tipo de vulnerabilidades presentes en una red y pueden generar un mapa de red. Adicionalmente **openVAS** brinda algunas sugerencias para corregir los diversos tipos de vulnerabilidades encontrados.

PROCEDIMIENTO EXPERIMENTAL

1. **Dirección IP Red GNU/LINUX :** desde la terminal con el comando

```
ifconfig
ip addr
```

sabemos cual es la dirección.

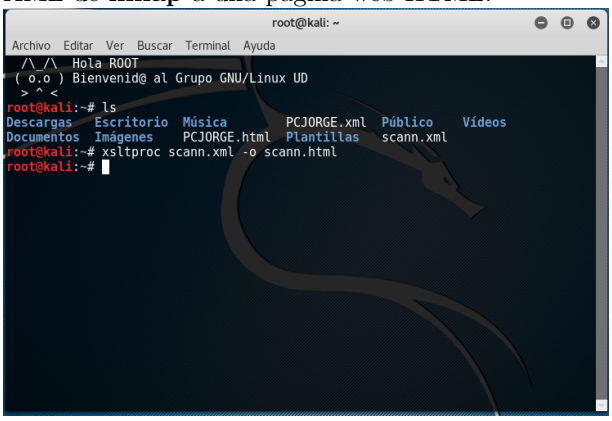


2. Uso de **nmap** desde la terminal con el comando
nmap -A -O -V 192.168.1.* -oX scann.xml
se genera el primer reporte de cuantos dispositivos estaban conectados a la red en ese momento.

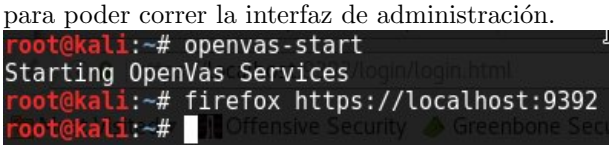
* lmaldanab@correo.udistrital.edu.co
† amacostap@correo.udistrital.edu.co
‡ daosoriog@gmail.com
§ marbrb1@gmail.com
[a] www.openvas.org/

-A: Escaneo agresivo y detección de la versión del sistema operativo.
-O: Detección del sistema operativo.
-v: Muestra el análisis que esta generando en consola.
-oX: Genera un archivo XML el cual contiene el reporte de las IP's conectadas y los puertos activos y cerrados.

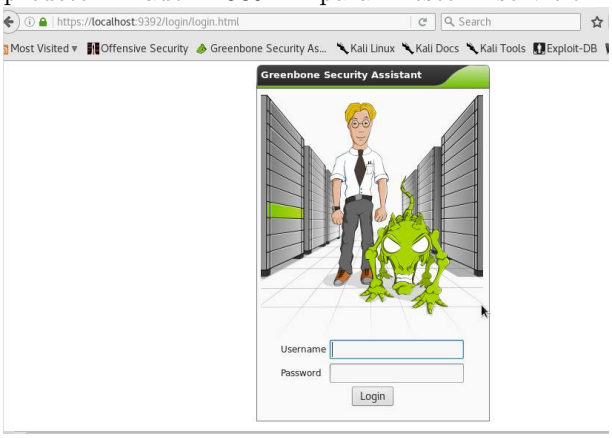
3. **xsltproc:** herramienta que transforma el reporte XML de **nmap** a una página web HTML.



4. **openvas-start:** inicia el servicio de **OpenVAS** para poder correr la interfaz de administración.

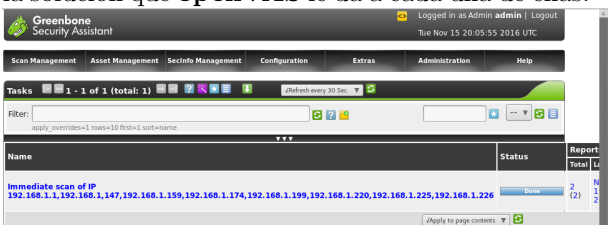


5. **localhost:9392 :** Desde el navegador Firefox ingresamos a la interfaz de administración de **OpenVAS** por el puerto predeterminado 9392 para este servicio.

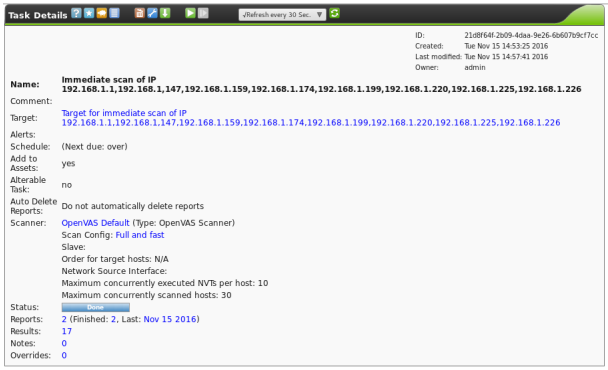


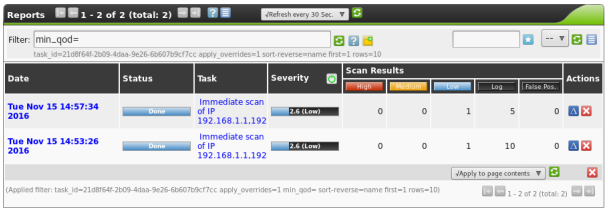
Inician sesión en OpenVas, dependiendo del nombre de usuario que ustedes coloquen en el momento de la instalacion de esta herramienta y pueden generar una contraseña con el comando openvas-setup desde la terminal, También pueden crear un usuario nuevo con una contraseña con el comando openvasad -c add user -u your new login here -r Admin

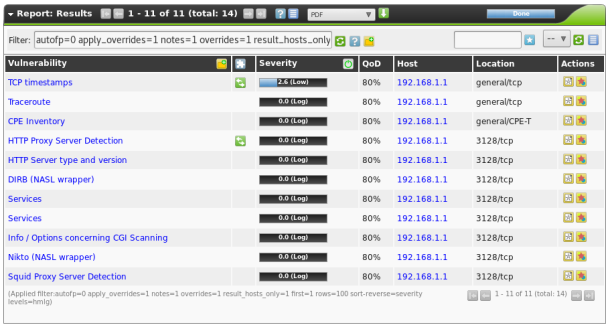
6. **IP'S :** Se digitan en **OpenVAS** todas las ip's activas que mostró **nmap** en el momento de la inspección, para saber el tipo de vulnerabilidad y la solución que **openVAS** le da a cada una de ellas.



Pueden observar la descripción general que nos da OpenVAS con dos reportes los cuales indican los tipos de vulnerabilidades que tiene cada puerto detectado y cada IP junto con su gateway, ademas puedes descargar cada reporte en diferentes tipos de formatos como: HTML, XML, PDF, entre otros.







CONCLUSIONES

Al explorar vulnerabilidades en la red del Laboratorio de Tecnologías Libres, se analizó cada puerto de las direcciones IP's activas. En cada computador conectado a la red se reconocieron los proyectos y servicios que estaban corriendo, el sistema operativo, los tipos de vulnerabilidades y el estado de los puertos usados (detectando la disponibilidad de conexión a estos) concluyendo que no todos los puertos abiertos son vulnerables.
Adicionalmente, ante las vulnerabilidades detectadas, una de las soluciones más comunes de **OpenVAS** era "Bloquear los paquetes no deseados fugados de la red".

A. Citas y Referencias

[?] Documentacion oficial **OpenVAS**
`http:\/\/docs.greenbone.net\/index.html\#user\_documentation`
[?] Documentacion oficial **nmap**
`https://nmap.org/docs.html`