

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
```

^{*} lmaldanab@correo.udistrital.edu.co

[†] amacostap@correo.udistrital.edu.co

[‡] daosoriog@gmail.com

[§] marbrb1@gmail.com

^a www.openvas.org/

sabemos cual es la dirección.

```
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.20.232.41 netmask 255.255.255.0 broadcast 10.20.232.255  
    inet6 fe80::a00:27ff:fe66:8778 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:66:87:78 txqueuelen 1000 (Ethernet)  
    RX packets 226187 bytes 48408020 (46.1 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 327572 bytes 43481623 (41.4 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1 (Local Loopback)  
    RX packets 24151 bytes 40672669 (38.7 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24151 bytes 40672669 (38.7 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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.

```
root@kali:~# nmap -A -O -v 192.168.1.* -oX scann.xml  
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-11-15 10:29 COT  
NSE: Loaded 138 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 10:29  
Completed NSE at 10:29, 0.00s elapsed  
Initiating NSE at 10:29  
Completed NSE at 10:29, 0.00s elapsed  
Initiating Ping Scan at 10:29  
Scanning 256 hosts [4 ports/host]  
Completed Ping Scan at 10:29, 4.05s elapsed (256 total hosts)  
Initiating Parallel DNS resolution of 256 hosts. at 10:29  
Completed Parallel DNS resolution of 256 hosts. at 10:29, 0.01s elapsed  
Nmap scan report for 192.168.1.0 [host down]  
Nmap scan report for 192.168.1.3 [host down]  
Nmap scan report for 192.168.1.4 [host down]  
Nmap scan report for 192.168.1.5 [host down]  
Nmap scan report for 192.168.1.6 [host down]  
Nmap scan report for 192.168.1.7 [host down]  
Nmap scan report for 192.168.1.8 [host down]  
Nmap scan report for 192.168.1.9 [host down]  
Nmap scan report for 192.168.1.10 [host down]  
Nmap scan report for 192.168.1.11 [host down]
```

```

Completed Service scan at 10:29, 10.04s elapsed (1 service on 2 hosts)
Initiating OS detection (try #3) against 2 hosts
Retrying OS detection (try #2) against 2 hosts
Completed Traceroute at 10:29, 0.03s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 10:29
Completed Parallel DNS resolution of 4 hosts. at 10:29, 6.50s elapsed
NSE: Script scanning 2 hosts.
Initiating NSE at 10:29
Completed NSE at 10:29, 1.78s elapsed
Initiating NSE at 10:29
Completed NSE at 10:29, 0.00s elapsed
Nmap scan report for 192.168.1.1
Host is up (0.00037s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    closed ftp
110/tcp   closed pop3
143/tcp   closed imap
993/tcp   closed imaps
995/tcp   closed pop3s
5128/tcp  open  http-proxy Squid http proxy 3.1.10
|_ http-open-proxy: Potentially OPEN proxy.
|_ Methods supported: CONNECTION, GET
|_ http-server-header: squid/3.1.10
|_ http-title: ERROR: El URL solicitado no se ha podido conseguir
5222/tcp  closed xmpp-client
8080/tcp  closed xmpp
Aggressive OS guesses: Linux 2.6.32 - 3.10 (96%), Linux 2.6.32 - 3.13 (95%), Linux 3.10 (93%), Linux 3.2 - 3.8 (93%), Linux 3.4 (93%), Synology DiskStation Manager 5.2-5644 (92%), Linux 2.6.39 (92%), Openwrt Attitude Adjustment (Linux 3.2) - Barrier Breaker (Linux 3.8) (80%), Linux 3.16 - 3.19 (90%), HP P2000 G3 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 12.156 days (since Thu Nov 3 06:46:00 2016)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 143/tcp)
HOP RTT ADDRESS
1 0.42 ms 10.20.232.1
2 0.37 ms 192.168.1.1

Nmap scan report for 192.168.1.2
Host is up (0.00044s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    closed ftp
110/tcp   closed pop3
143/tcp   closed imap
993/tcp   closed imaps
995/tcp   closed pop3s
5222/tcp  closed xmpp-client
8080/tcp  closed xmpp
Too many fingerprints match this host to give specific OS details
Network Distance: 3 hops

TRACEROUTE (using port 143/tcp)
HOP RTT ADDRESS
1 0.26 ms proxy.udistrital.edu.co (10.20.4.15)
2 0.36 ms 192.168.1.2

NSE: Script Post-scanning.
Initiating NSE at 10:29
Completed NSE at 10:29, 0.00s elapsed
Initiating NSE at 10:29
Completed NSE at 10:29, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (2 hosts up) scanned in 34.75 seconds
Raw packets sent: 6137 (265.364KB) | Rcvd: 254 (13.84KB)
root@kali:~#

```

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

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
/\ /\  Hola ROOT
( o.o ) Bienvenido al Grupo GNU/Linux UD
> ^ <
root@kali:~# ls
Descargas  Escritorio  Música  PCJORGE.xml  Público  Videos
Documentos  Imágenes  PCJORGE.html  Plantillas  scann.xml
root@kali:~# xsftproc scann.xml -o scann.html
root@kali:~#

```

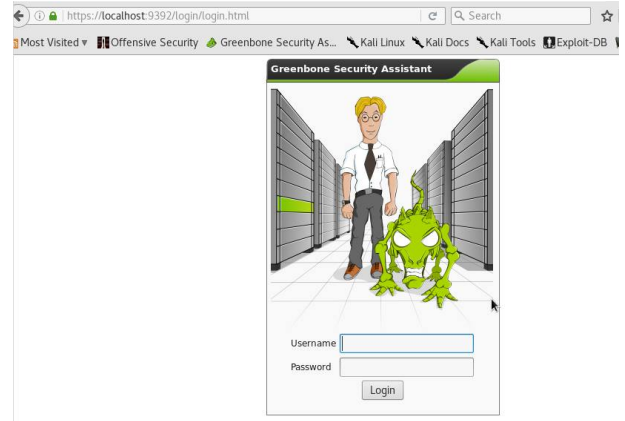
4. **openvas-start**: inicia el servicio de **OpenVAS** para poder correr la interfaz de administración.

```

root@kali:~# openvas-start
Starting OpenVas Services /login/login.html
root@kali:~# firefox https://localhost:9392
root@kali:~#

```

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 instalación 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, además puedes descargar cada reporte en diferentes tipos de formatos como: HTML, XML, PDF, entre otros.

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