

Escaneo de un sistema con Backtrack 4



El escaneo de un sistema es el siguiente paso a llevar después de haber conocido nuestro objetivo, debemos puerto o que medios de comunicación esta utilizando. Vamos a tener en cuenta los siguientes “tips” para poder llevar por finalizado este paso que es el escaneo.

- Escaneo del sistema

- 1 puertos habilitados
- 2 Servicios Corriendo de Cada Puerto
- 3 Identificación de Banners
- 4 Identificación del sistema operativo
- 5 Fingerprinting
- 6 Escaneos tipo conexión (vulnerabilidades)

- Escaneo de Puertos

En esta parte hablaremos de las diferentes formas que hay para poder averiguar que puertos tiene abiertos un sistema. De aquí podemos partir para decir por donde se esta comunicando y de que forma lo esta haciendo.

1# nmap



```
progresive@progresive-laptop: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
progresive@progresive-laptop:~$ nmap 192.168.57.128
Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-12-05 15:06 COT
Interesting ports on 192.168.57.128:
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
progresive@progresive-laptop:~$
```

lo que estamos haciendo es decirle al nmap que haga un escaneo muy básico hacia el sistema 192.168.57.128 (mi VM), después que interactuamos con la herramienta debemos saber que hace por debajo.

Línea amarilla = envía paquete de solicitud hacia un puerto

línea verde= envía paquete diciendo estado de puerto

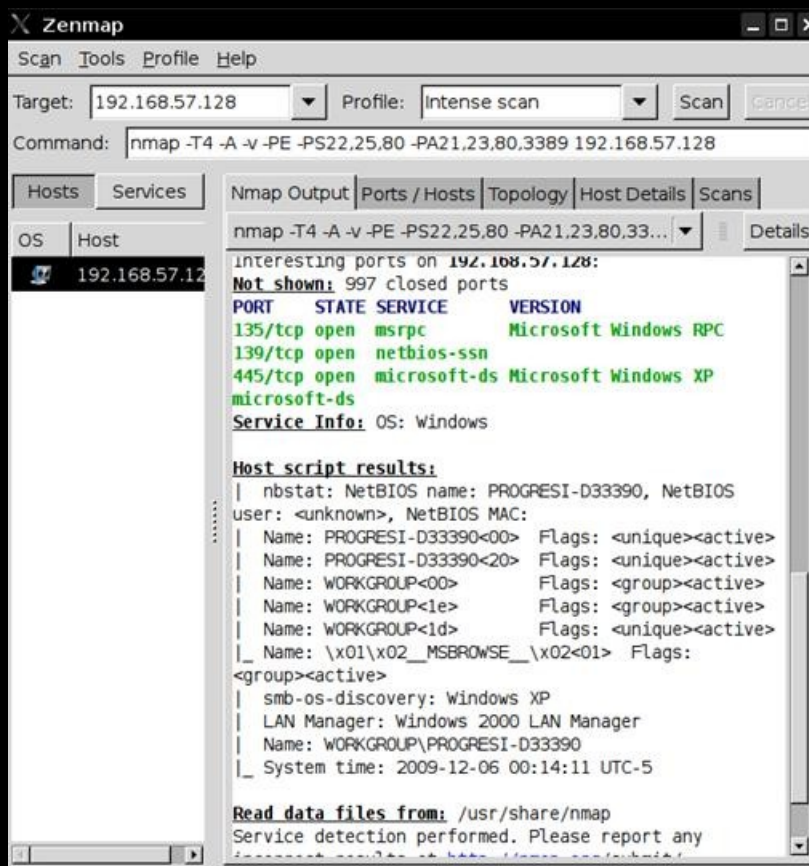
línea naranja = envía paquete diciendo que el paquete llegó bien

Atacante -----> Objetivo

Atacante <----- Objetivo

Atacante -----> Objetivo

esto es lo que pasa al nosotros dar enter con nmap ya configurado. Primeramente enviamos un paquete de solicitud hacia un puerto, luego el equipo objetivo nos envía un paquete diciendo que el puerto está habilitado o filtrado, luego nosotros enviamos un paquete que sería de control que estamos avisando que el paquete llegó bien. Nmap también ofrece una interfaz gráfica muy buena.



- Servicios de cada puerto

Ya sabiendo que puertos habilitados tiene nuestro objetivo podremos pasar a el siguiente paso que seria saber que servicios se esta ejecutando por cada puerto.

¿para que son estos dichos servicios?

Un 'servicio' es un programa que está ejecutándose en un puerto de un servidor conectado a Internet. Cada servicio es un programa que responde a ciertas órdenes.

Entonces lo que vamos a hacer es saber cual es el servicio que se están corriendo por los tres puertos habilitados antes mostrados con nmap (Grafico y Shell).

```
1# nmap
```



```
progressive@progressive-laptop: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
progressive@progressive-laptop:~$ nmap -sV 192.168.57.128
Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-12-06 00:54 COT
Interesting ports on 192.168.57.128:
Not shown: 997 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     (done)
445/tcp   open  microsoft-ds    Microsoft Windows XP microsoft-ds
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
progressive@progressive-laptop:~$
```

Como podemos ver nuestro objetivo nos muestra que en los puertos habilitados tiene unos servicios ejecutándose.

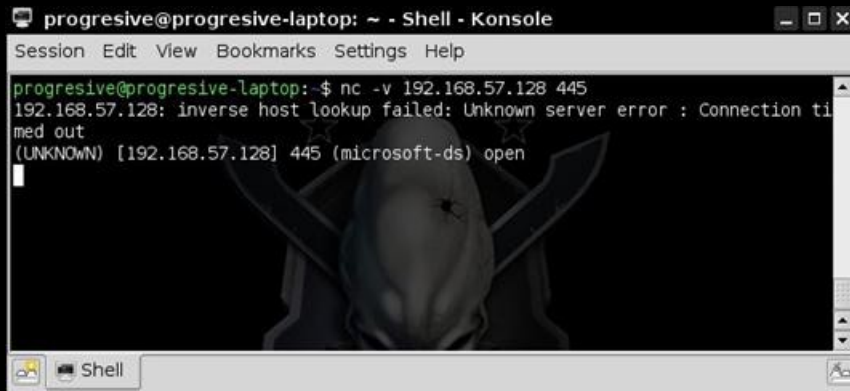
Puerto	Estado	Servicio	Versión
135	abierto	msrpc	Microsoft Windows RPC
139	abierto	netbios-ssn	(done)
445	abierto	microsoft-ds	Microsoft Windows XP microsoft-ds

Lo que pasa por debajo es la misma “estructura” que la de la del escaneo de puerto, solo que aquí hace conexión con el puerto habilitado y verifica la versión y dependiendo de la respuesta el NMAP busca en su Base de datos para saber que servicio se esta ejecutando y luego lo muestra en pantalla.

- Identificación de banners

En este método se basa en tener conexión hacia los puertos ya habilitados para poder rectificación de información, una breve explicación de este método es conectarse a algunos de los puertos ya habilitados y al concluir la conexión nos mostrara un “banner” que seria una información del el puerto al que uno se esta intentando conectar.

1# Netcat



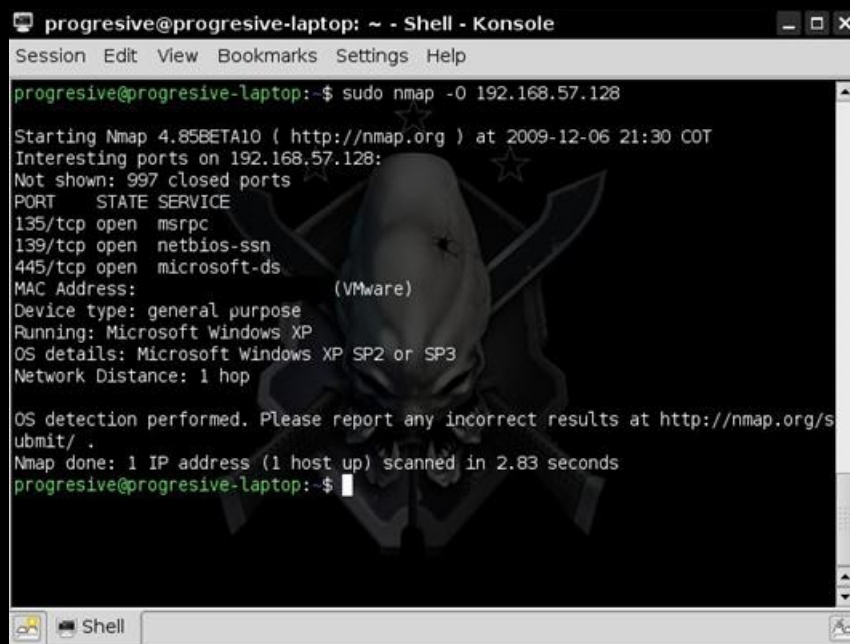
```
progressive@progressive-laptop: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
progressive@progressive-laptop:~$ nc -v 192.168.57.128 445
192.168.57.128: inverse host lookup failed: Unknown server error : Connection ti
med out
(UNKNOWN) [192.168.57.128] 445 (microsoft-ds) open
```

aquí estamos intentando conectarnos al puerto 445 (microsoft-ds) entonces como podemos ver colocamos `nc -v <ip de nuestro objetivo>`, entonces luego el netcat nos responde que la conexión al host a sido nula o incompleta, luego nos muestra conexión terminada después sale a mostrarse nuestro primer banner que nos dice (microsoft-ds) que seria el servicio que se esta ejecutándose por este puerto. (Este paso lo hacemos con el fin en si de hacer como una rectificación de la información de lo que hemos llevado para poder estar seguros de la información recolectada con estos ataques pasivos)

- Identificación del sistema operativo

El siguiente paso a seguir es poder determinar cual es el Sistema operativo de nuestro objetivo, este es uno de los pasos mas importantes para poder determinar los métodos mas adelante (Intrusiones, Rootkits, etc.)

1# nmap



```
progressive@progressive-laptop: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
progressive@progressive-laptop:~$ sudo nmap -O 192.168.57.128
Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-12-06 21:30 COT
Interesting ports on 192.168.57.128:
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
progressive@progressive-laptop:~$
```

Con el nmap nos ofrece la opción de detención del sistema operativo de nuestro objetivo, la sintaxis del comando sería `sudo nmap -O 192.168.57.128` primeramente sudo es para acceder/ejecutar la herramienta nmap como súper usuario luego `nmap -O xxx.xxx.xxx.xxx` le decimos al nmap que haga la detención del sistema operativo de la IP remota. Debajo de la Shell esta pasando lo siguiente, nmap esta haciendo conexión hacia el objetivo indicado, pero al hacer conexión el recibe un paquete que le avisa que Sistema operativo esta de anfitrión en el equipo, luego ese paquete llega a la maquina del atacante y nmap busca en su base de datos sobre ese paquete de S.O y de allí determina que Sistema operativo tiene.

- Fingerprinting

El fingerprinting es el método enfocado hacia tomarle “huellas dactilares” hacia el sistema remoto, es buscar sobre la información ya recolectada un poco mas a fondo.

Comentario: Finger es un protocolo que proporciona una información detallada de nuestro objetivo o de cualquier otro ordenador, de allí es donde sale el nombre fingerprinting es obtener información mas detallada del objetivo por medio de otros protocolos y herramientas.

2# Xprobe2

```
root@progressive-laptop: ~ - Shell - XProbe2
Session Edit View Bookmarks Settings Help
[x] [13] fingerprint:snmp - SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.57.128. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.57.128. Module test failed
[-] No distance calculation. 192.168.57.128 appears to be dead or no ports known
[+] Host: 192.168.57.128 is up (Guess probability: 50%)
[+] Target: 192.168.57.128 is alive. Round-Trip Time: 0.00049 sec
[+] Selected safe Round-Trip Time value is: 0.00099 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2003 Server Standard Edition" (Guess probability: 100%)
[+] Other guesses:
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2003 Server Enterprise Edition" (Guess probability: 100%)
[+] Host 192.168.57.128 Running OS: "Microsoft Windows XP SP2" (Guess probability: 100%)
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2000 Workstation" (Guess probability: 100%)
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2000 Workstation SP1" (Guess probability: 100%)
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2000 Workstation SP2" (Guess probability: 100%)
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2000 Workstation SP3" (Guess probability: 100%)
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2000 Workstation SP4" (Guess probability: 100%)
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2000 Server" (Guess probability: 100%)
[+] Host 192.168.57.128 Running OS: "Microsoft Windows 2000 Server Service Pack 1" (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

Con el xprobe2 podemos ver que el activa varios módulos ya predefinidos en el programa principal de el (son 13 módulos) luego de allí empieza a tomar huellas dactilares del objetivo ósea información mas especifica de el. Por debajo de la Shell lo que hace el es por medio del protocolo TCP es tomar información, ejemplo:

Host 192.168.57.128 ejecutandose S.O "Microsoft Windows XP SP2"
TCP puerto 139 445 ejecutándose

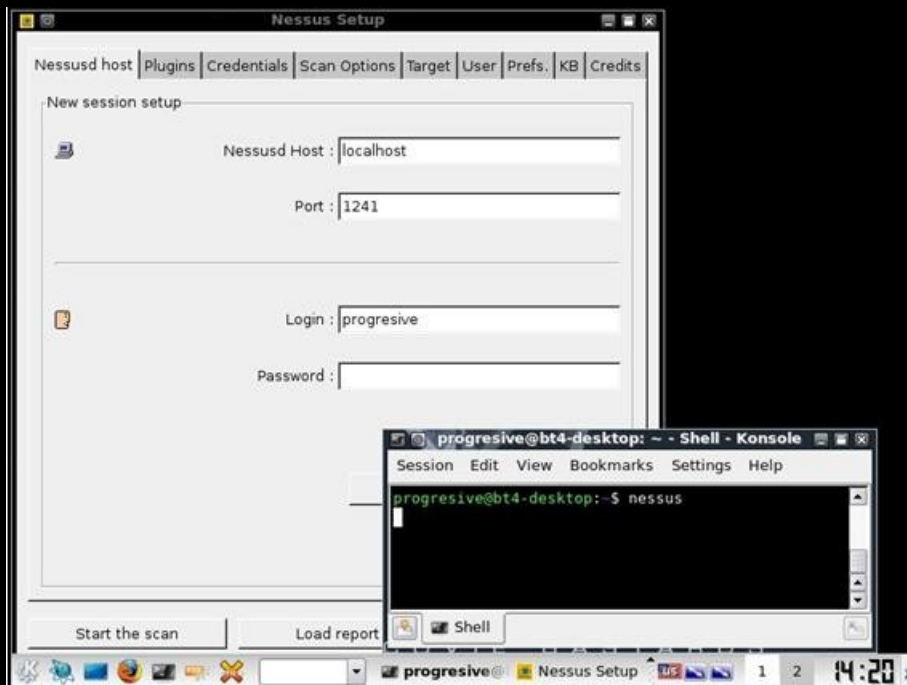
- Escaneos tipo conexión (vulnerabilidades)

Los escaneos tipo conexión son enfocados hacia determinar fallas o vulnerabilidades del sistemas que estamos auditando o accediendo a el. Vamos a utilizar 2 herramientas muy utilizadas en este paso, que son **NESSUS** y **OPENVAS**, para poder instalar el NESSUS en su backtrack solo tienes que abrir un terminal y teclear lo siguiente.

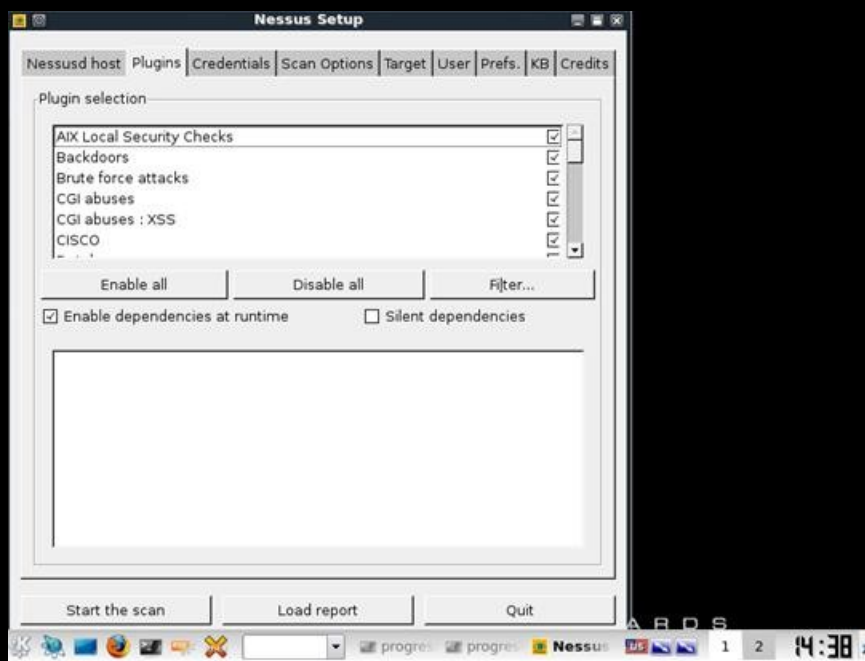
1# NESSUS

```
progressive@bt4-desktop: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
progressive@bt4-desktop:~$ sudo apt-get install nessus
```

Luego debemos agregar un usuario con `sudo nessus adduser` y listo tenemos nessus, Después de haber instalado el nessus en nuestro sistema vamos a llamarlo desde el terminal para que se ejecute.

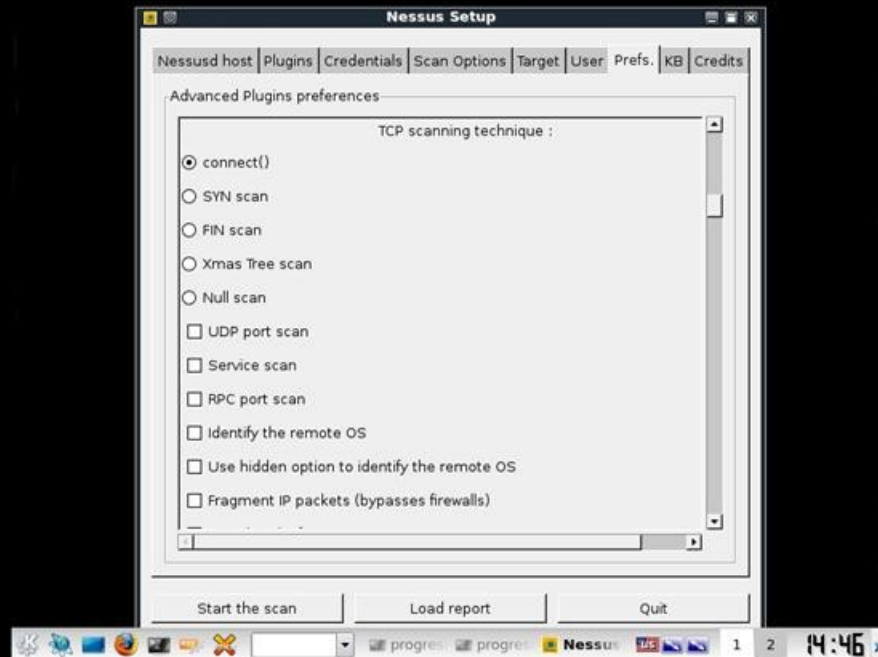


Luego nos logueamos y vamos a empezar a hacerle un escaneo básico nuestro objetivo. Seleccionamos todos los Plugins.

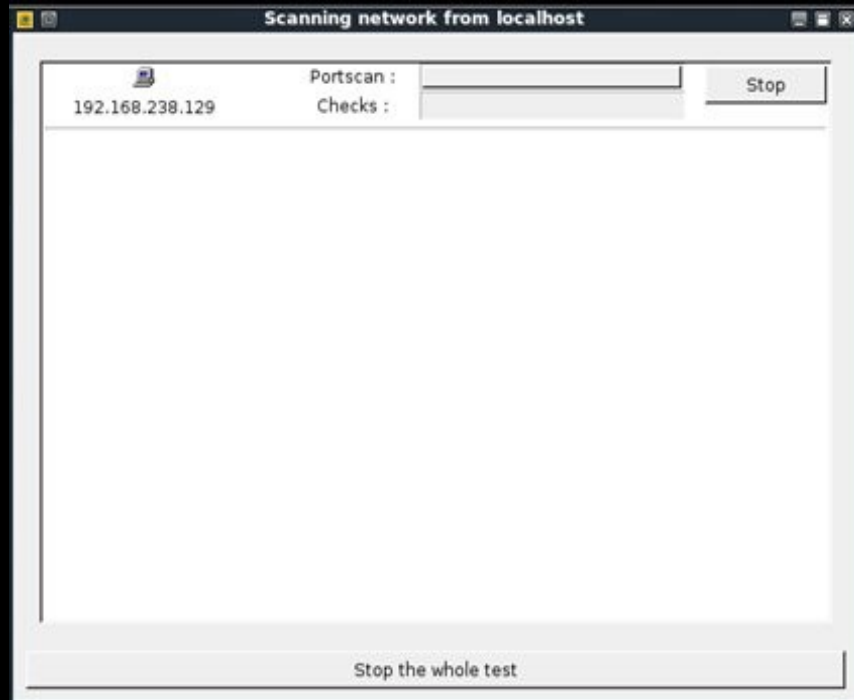


Nos dirigimos hacia Target y donde dice target(s) hay tecleamos la ip de nuestro objetivo.

Como les decía esta técnica es de escaneos tipo conexión, nos dirigimos hacia Prefs y buscamos TCP Scanning technique, allí esta seleccionado Connect.



Listo después de a ver configurado el nessus vamos a empezar a hacer nuestro escaneo.



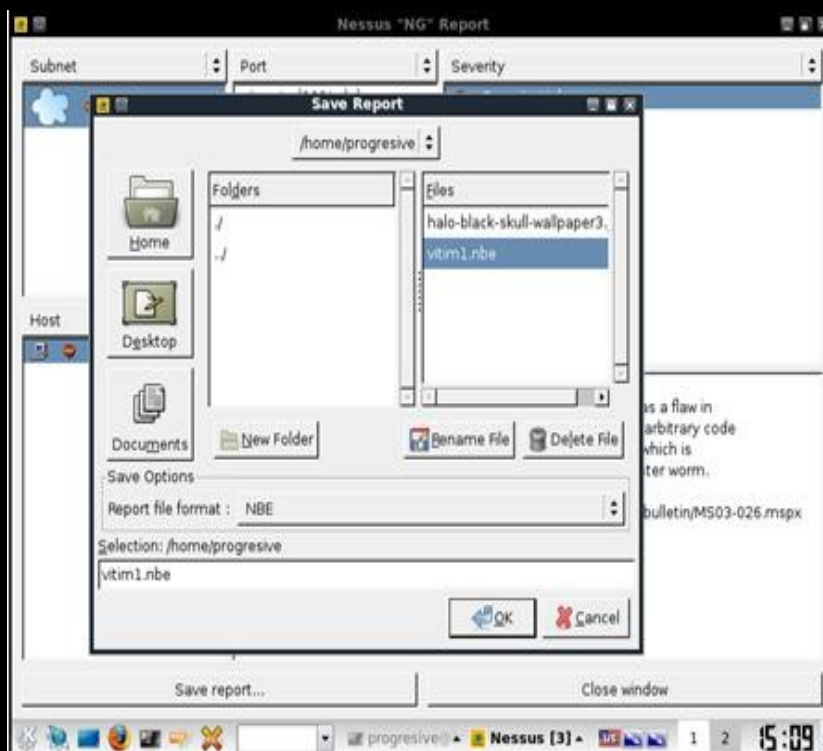
Después de haber hecho nuestro escaneo el nessus nos va a mostrar la siguiente ventana mostrándonos el resultado.



En este ejemplo el nessus escaneo todos los puertos del sistema, aquí nos podemos dar cuenta donde esta la el fallo del sistema nos muestra que 3 servicios de 3 puertos diferentes tiene advertencia (ósea que no están vulnerables en este momento pero pueden ser vulnerados).

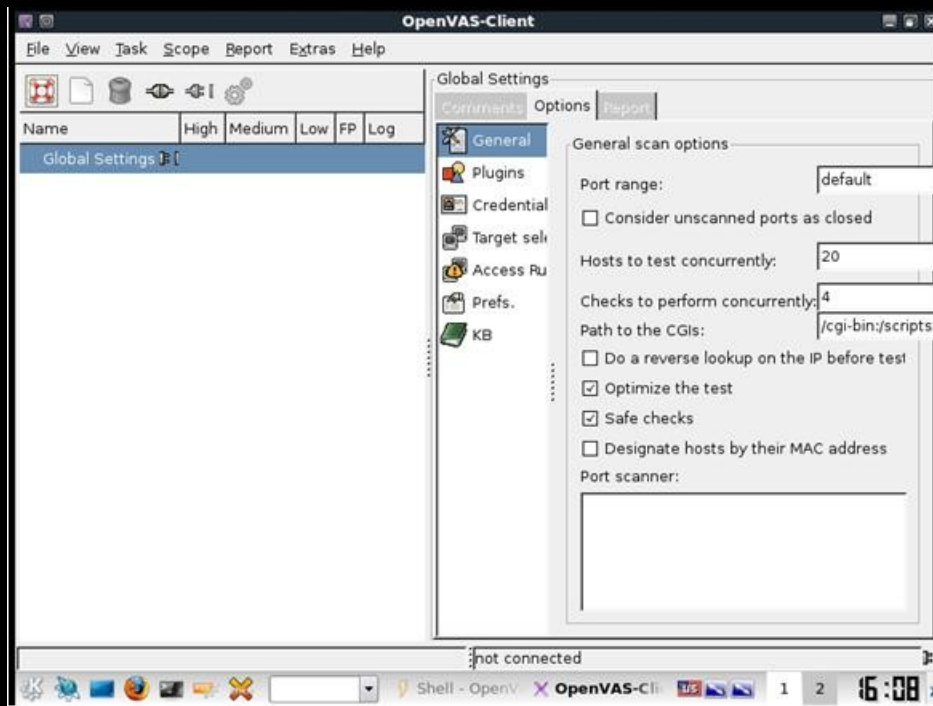
Bueno nos aparece que "135 open RPC Remote Procedure Call (RPC) is used in client/server applications based on MS Windows operating systems" esta habilitado depende de donde estemos mirando este fallo es bueno o malo.

Bueno ahora este reporte lo podemos guardar mas adelante para poder acceder al sistema lo vamos a necesitar.

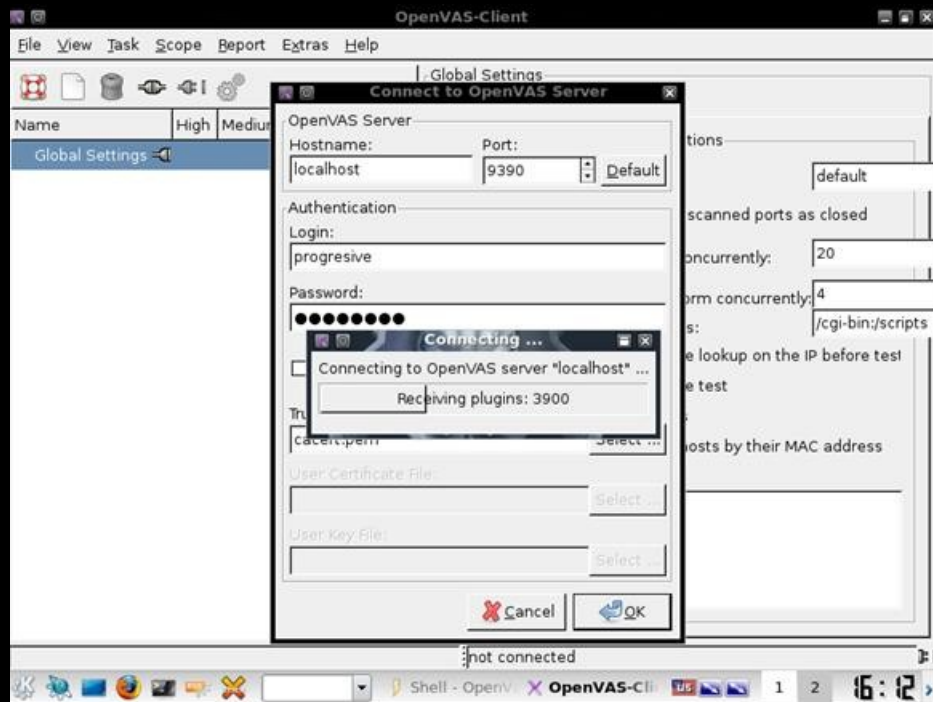


2# OpenVas

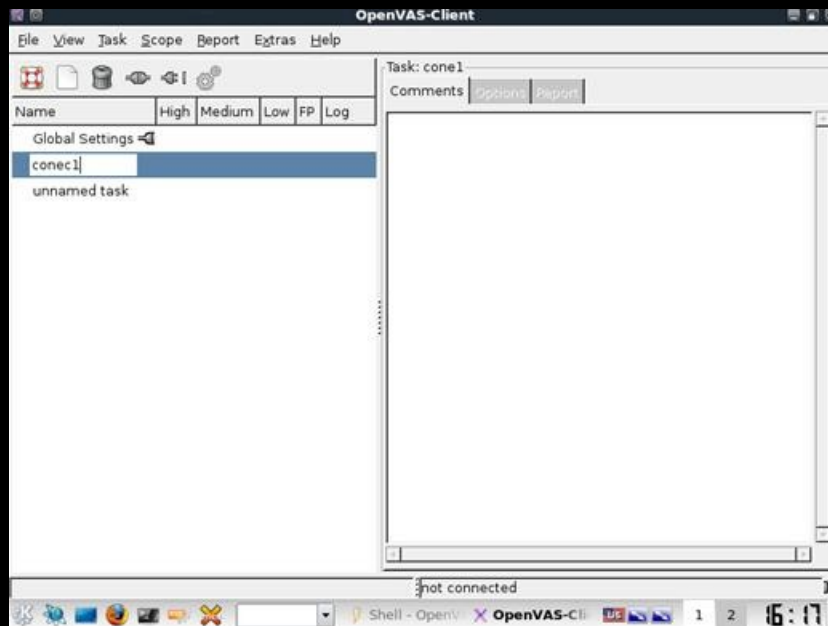
El OPENVAS es otro escáner de vulnerabilidades, muy parecido al nessus, bueno vamos a hacer lo mismo que hicimos con el nessus un escaneo básico de vulnerabilidades. Después de haberle actualizado todos lo plugins lo ejecutamos.



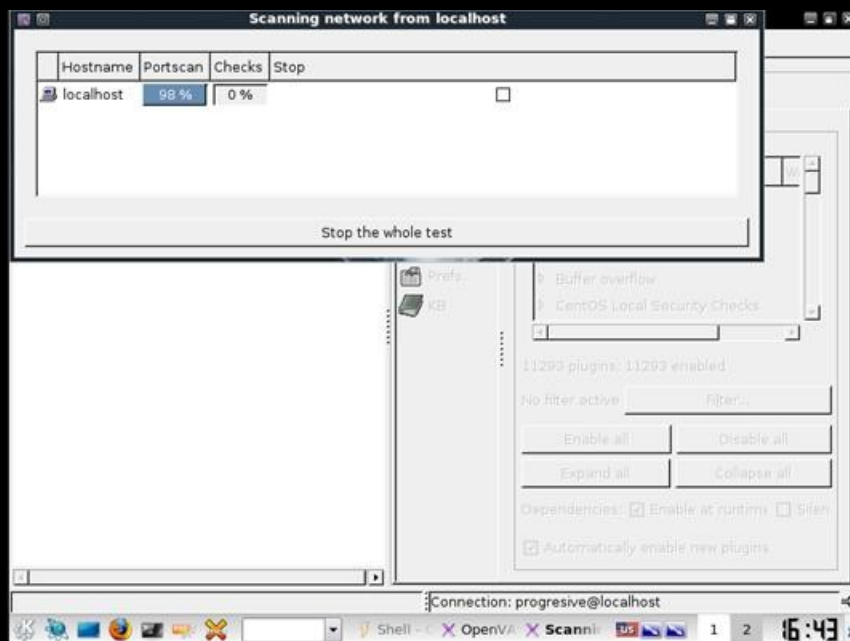
Nos conectamos a nuestro servidor 127.0.0.1 el local host



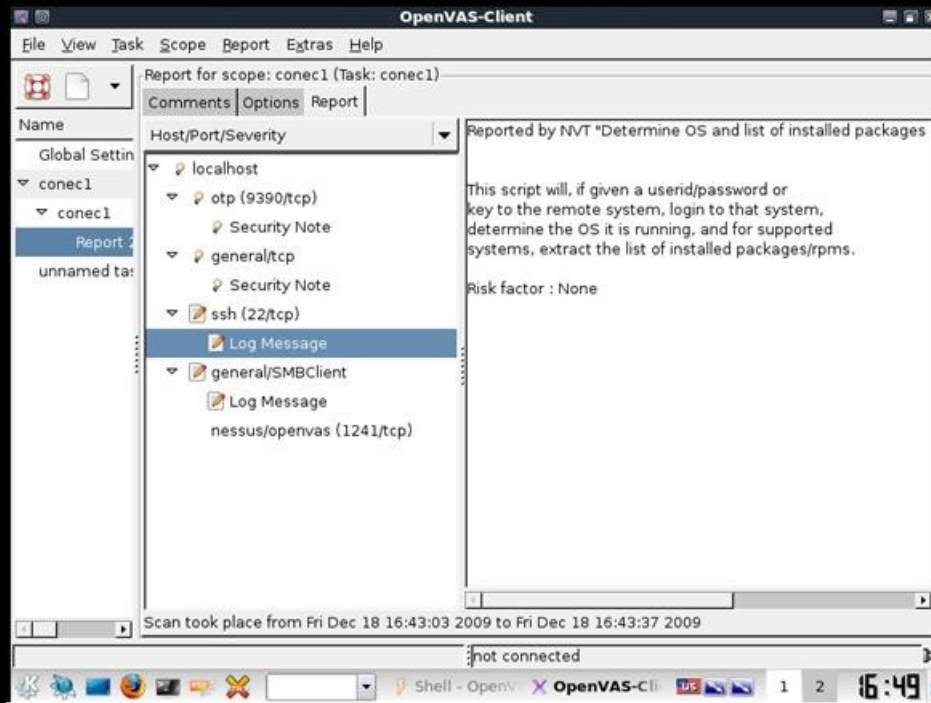
Creamos una nueva tarea o Task



Vamos y seleccionamos todos los plugins en el botón **Enable all** y actualizamos la lista de los plugins y ejecutamos el scope.



Con este escáner no nos dio ninguna vulnerabilidad, pero nos proporciona información que nos podría ayudar a la hora de lanzar ataques hacia el sistema ¿Por qué? Por que todos los plugins de cada escáner son diferentes, por eso es que debemos tener varias herramientas de este tipo a mano a la hora de hacer una auditoria.



-----> by Progressive Death <-----

Blog: <http://electr0s0ft.blogspot.com>

Correo: electrosoul_22@hotmail.com

dprogresive@gmail.com

Espero que esta documentación les haya servido.

PD: Si tengo algún error no duden en avisarme

PD2: Si vas a colocar este manual en algún otro lado por favor pon el autor

....

Saludos