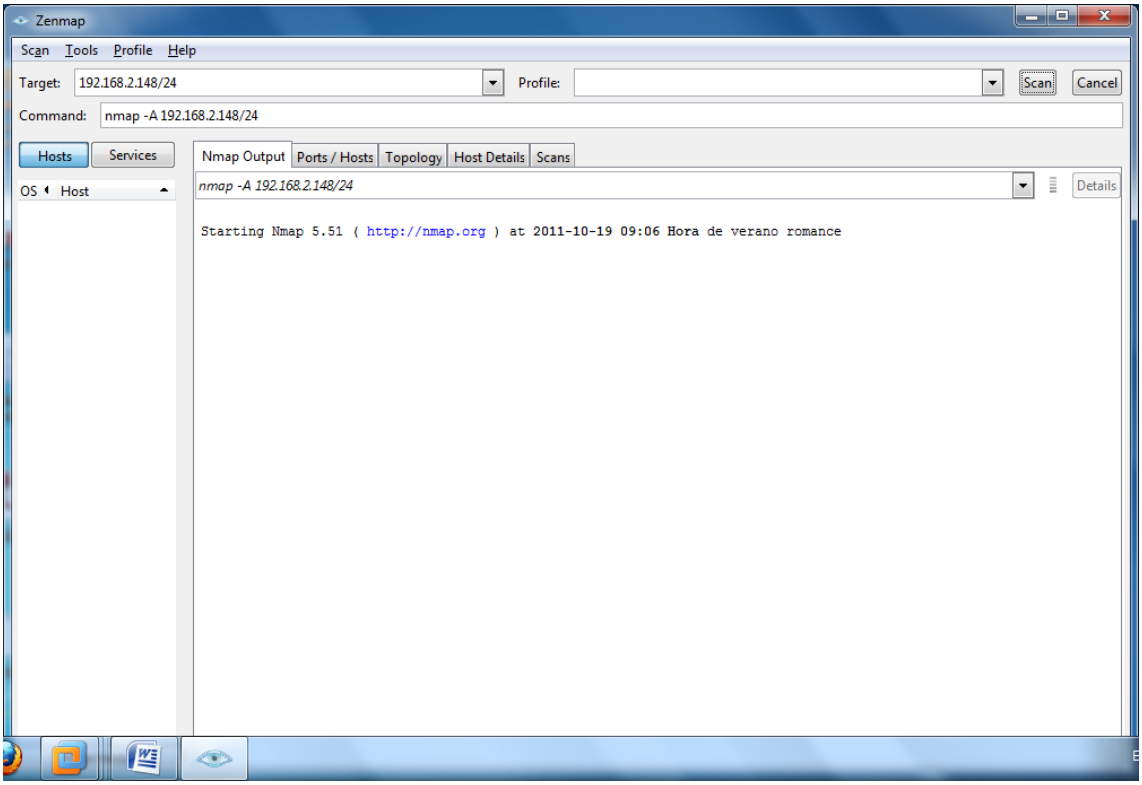
## TEMA 1 PRÁCTICA 3: DISPONIBILIDAD

### Nmap

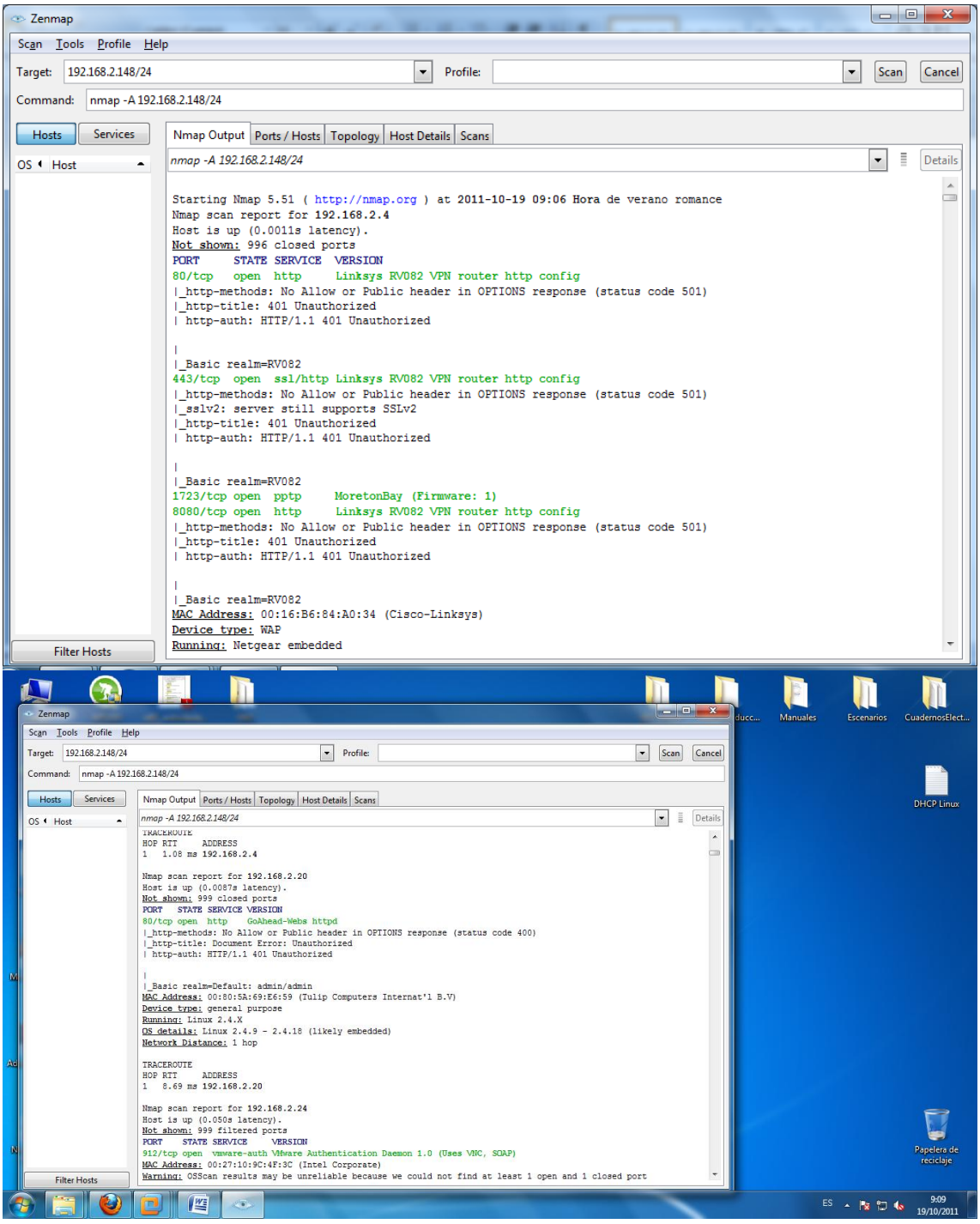
Vamos a utilizar la aplicación zenmap, que es el nmap modo gráfico en este caso para Windows.

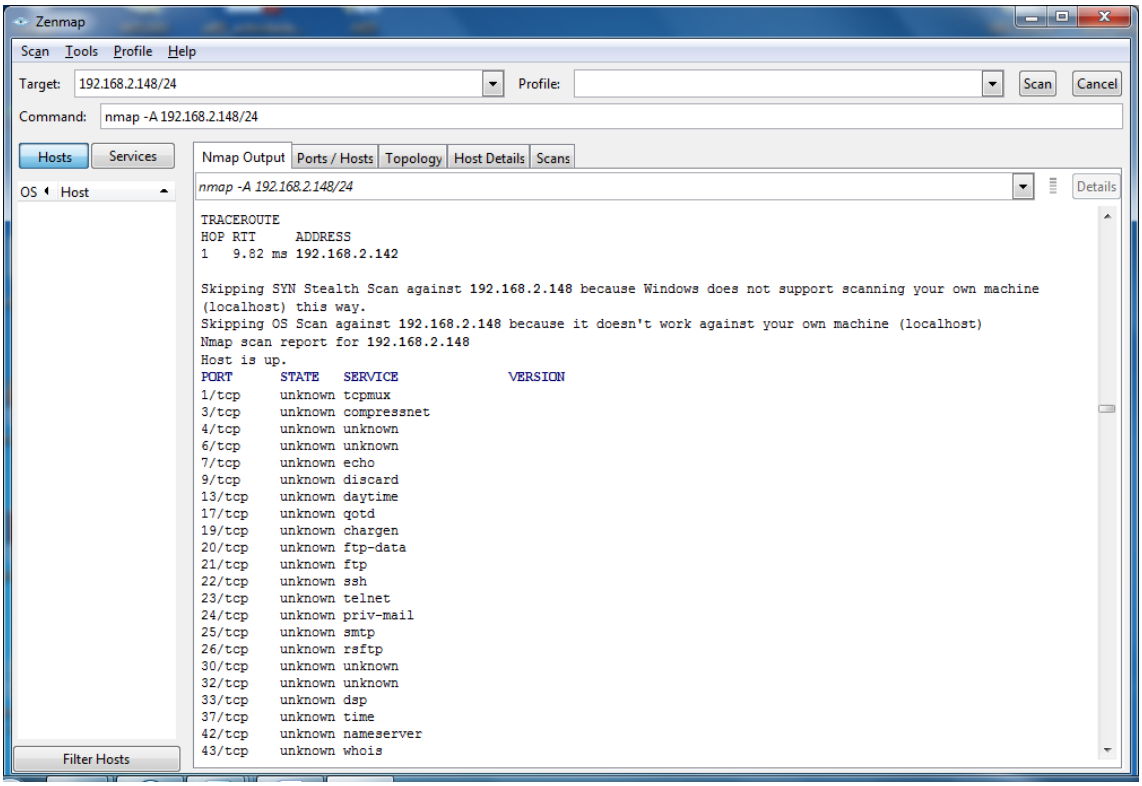
Vamos a escanear distintos equipos de la red.

Ejecutamos por ejemplo el comando nmap –A 192.168.2.148/24

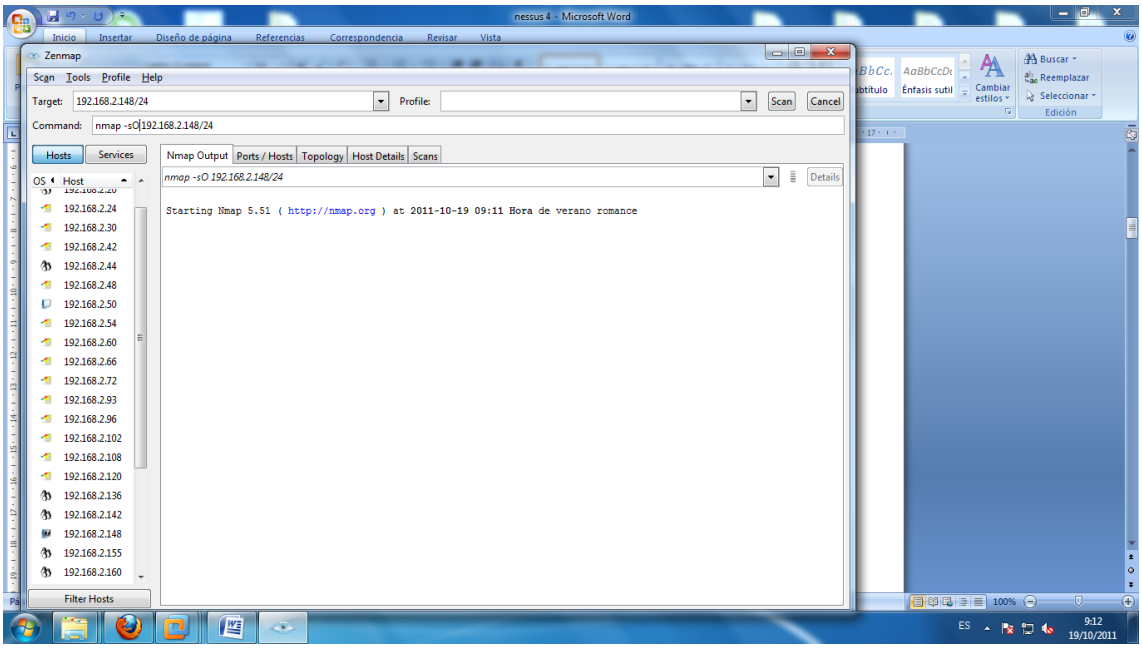


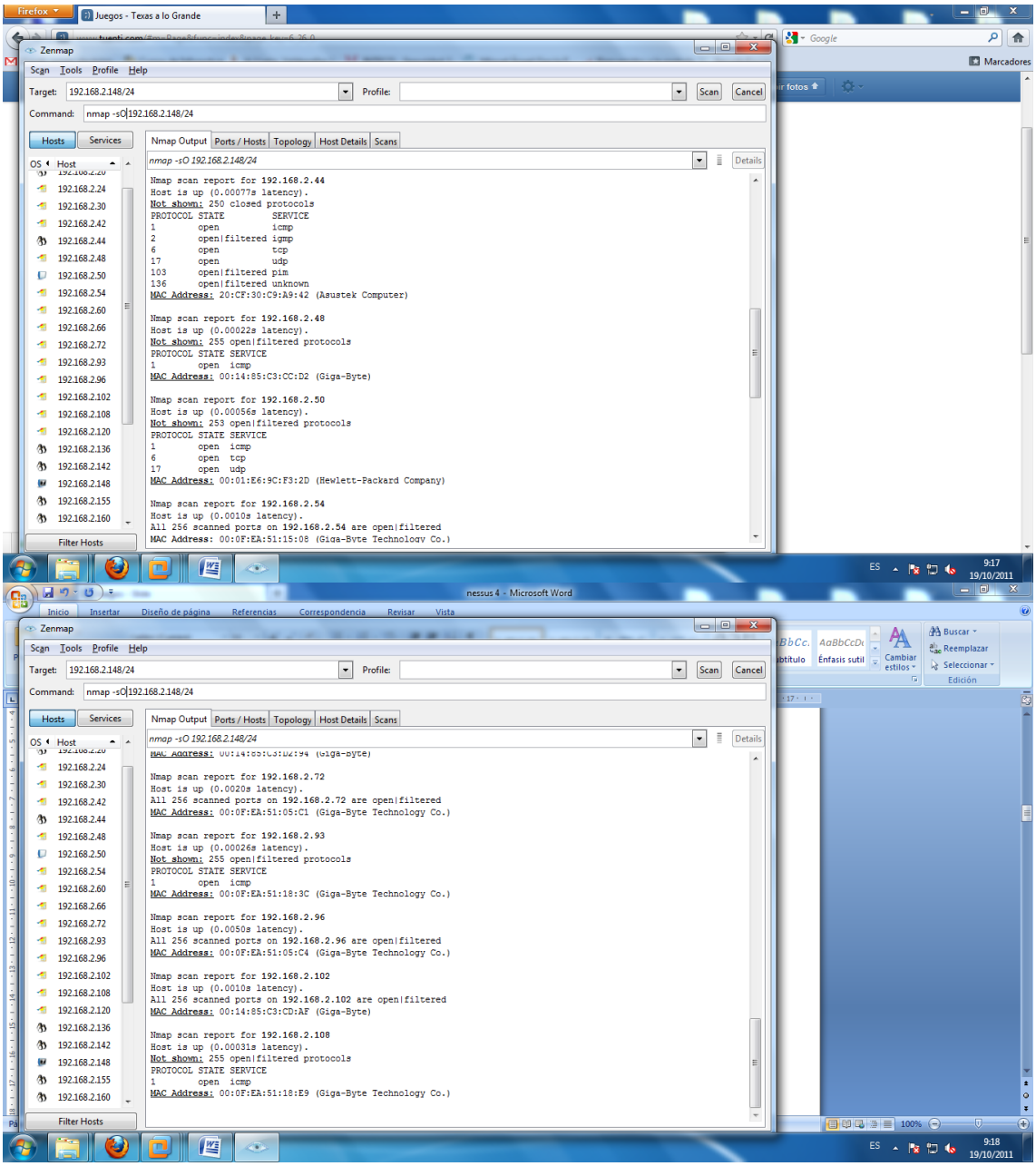

Con este comando podemos ver información, acerca de su sistema operativo, puertos disponibles y aplicaciones ejecutándose.


Zenmap
Scan Tools Profile Help
Target: 192.168.2.148/24
Profile:
Scan
Cancel
Command: nmap -A 192.168.2.148/24
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -A 192.168.2.148/24
Details
Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-19 09:06 Hora de verano romance
Nmap scan report for 192.168.2.4
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
80/tcp open http Linksys RV082 VPN router http config
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
|_http-title: 401 Unauthorized
| http-auth: HTTP/1.1 401 Unauthorized
|
|_Basic realm=RV082
443/tcp open ssl/http Linksys RV082 VPN router http config
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
|_sslv2: server still supports SSLv2
|_http-title: 401 Unauthorized
| http-auth: HTTP/1.1 401 Unauthorized
|
|_Basic realm=RV082
1723/tcp open pptp MoretonBay (Firmware: 1)
8080/tcp open http Linksys RV082 VPN router http config
|_http-methods: No Allow or Public header in OPTIONS response (status code 501)
|_http-title: 401 Unauthorized
| http-auth: HTTP/1.1 401 Unauthorized
|
|_Basic realm=RV082
MAC Address: 00:16:B6:84:A0:34 (Cisco-Linksys)
Device type: WAP
Running: Netgear embedded
Filter Hosts
Manuales
Escenarios
CuadernosElect...
DHCP Linux
Papelera de reciclaje
ES
9:09
19/10/2011

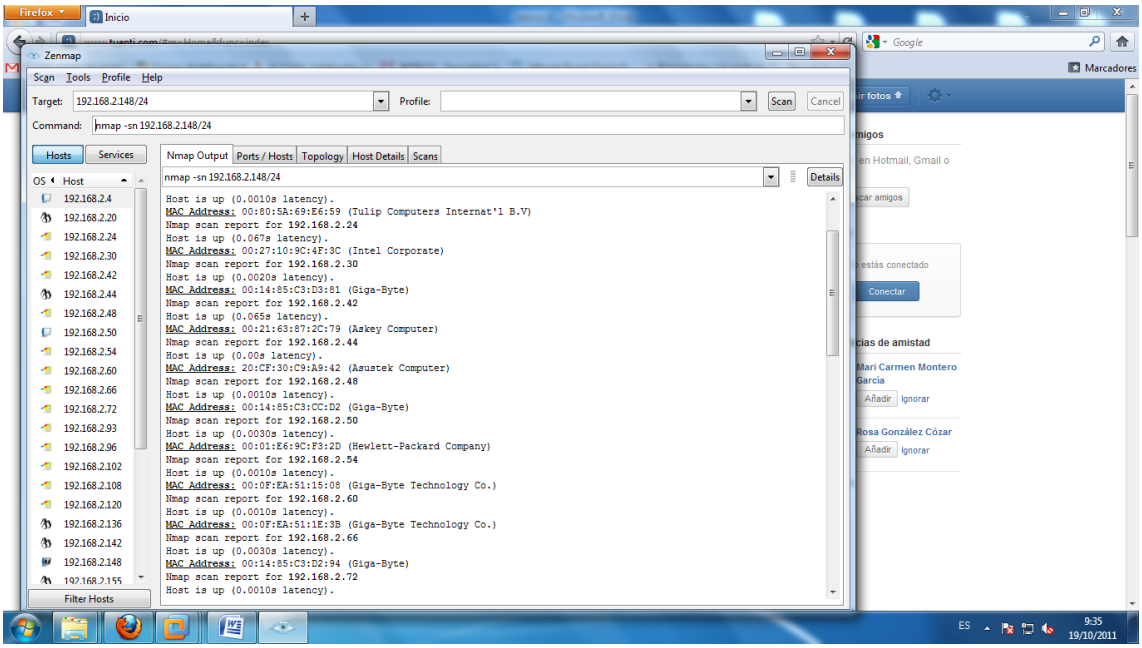



Ejecutamos el comando nmap –sO 192.168.2.148/24




Zenmap
Scan Tools Profile Help
Target: 192.168.2.148/24
Profile:
Command: nmap -sO 192.168.2.148/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sO 192.168.2.148/24
Details
OS Host
Filter Hosts
Nmap scan report for 192.168.2.44
Host is up (0.00077s latency).
Not shown: 250 closed protocols
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open tcp
17 open udp
103 open|filtered pim
136 open|filtered unknown
MAC Address: 20:CF:30:C9:A9:42 (Asustek Computer)
Nmap scan report for 192.168.2.48
Host is up (0.00022s latency).
Not shown: 255 open|filtered protocols
PROTOCOL STATE SERVICE
1 open icmp
MAC Address: 00:14:85:C3:CC:D2 (Giga-Byte)
Nmap scan report for 192.168.2.50
Host is up (0.00056s latency).
Not shown: 253 open|filtered protocols
PROTOCOL STATE SERVICE
1 open icmp
6 open tcp
17 open udp
MAC Address: 00:01:E6:9C:F3:2D (Hewlett-Packard Company)
Nmap scan report for 192.168.2.54
Host is up (0.0010s latency).
All 256 scanned ports on 192.168.2.54 are open|filtered
MAC Address: 00:0F:EA:51:15:08 (Giga-Byte Technology Co.)
nessus 4 - Microsoft Word
Nmap scan report for 192.168.2.72
Host is up (0.0020s latency).
All 256 scanned ports on 192.168.2.72 are open|filtered
MAC Address: 00:0F:EA:51:05:C1 (Giga-Byte Technology Co.)
Nmap scan report for 192.168.2.93
Host is up (0.00026s latency).
Not shown: 255 open|filtered protocols
PROTOCOL STATE SERVICE
1 open icmp
MAC Address: 00:0F:EA:51:18:3C (Giga-Byte Technology Co.)
Nmap scan report for 192.168.2.96
Host is up (0.0050s latency).
All 256 scanned ports on 192.168.2.96 are open|filtered
MAC Address: 00:0F:EA:51:05:C4 (Giga-Byte Technology Co.)
Nmap scan report for 192.168.2.102
Host is up (0.0010s latency).
All 256 scanned ports on 192.168.2.102 are open|filtered
MAC Address: 00:14:85:C3:CD:AF (Giga-Byte)
Nmap scan report for 192.168.2.108
Host is up (0.00031s latency).
Not shown: 255 open|filtered protocols
PROTOCOL STATE SERVICE
1 open icmp
MAC Address: 00:0F:EA:51:18:E9 (Giga-Byte Technology Co.)

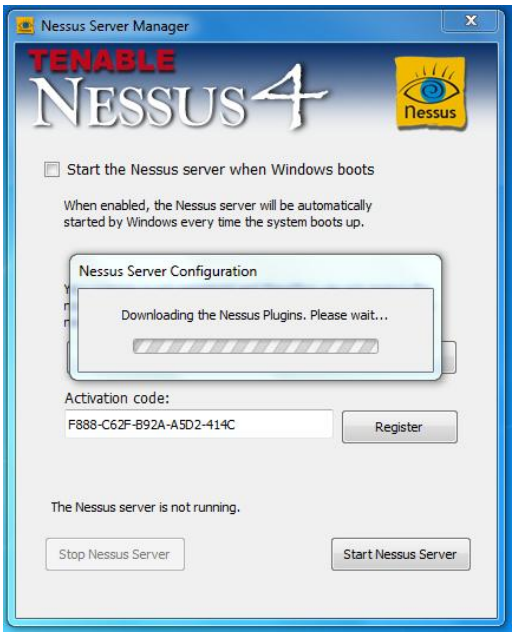
Ejecutamos el comando –sn 192.168.2.148/24



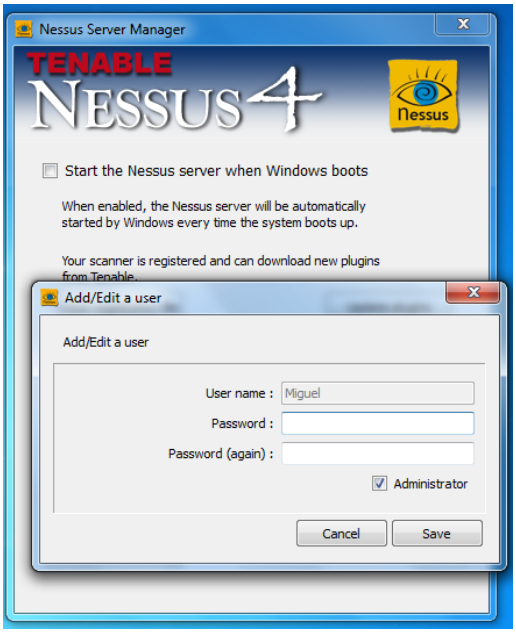
**NESSUS 4.**

Sirver para comprobar los puertos de un equipo determinado.

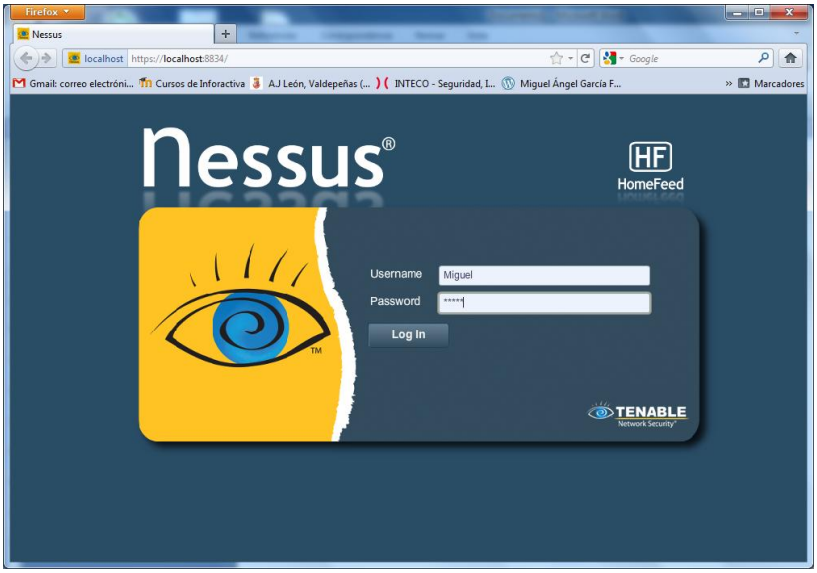
Procedemos a instalar Nessus, introducimos el código que nos ha llegado al correo y arrancamos el server.



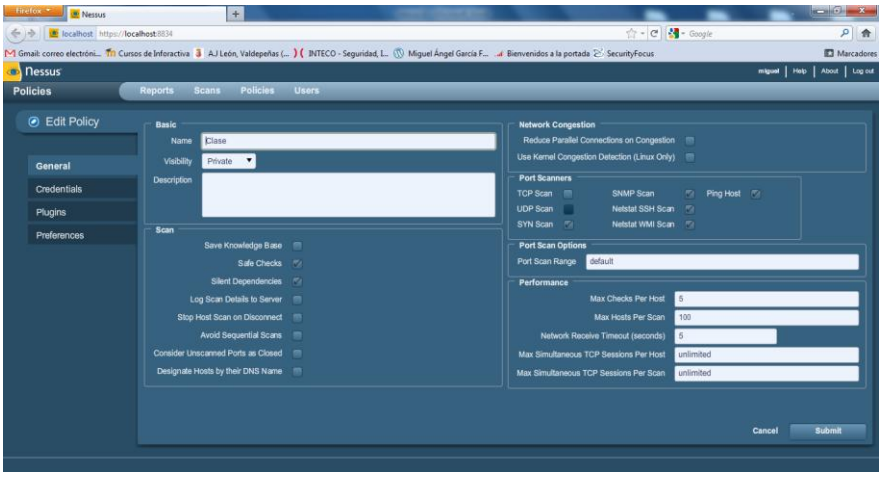

Introducimos un usuario y contraseña para cuando accedamos al modo cliente.



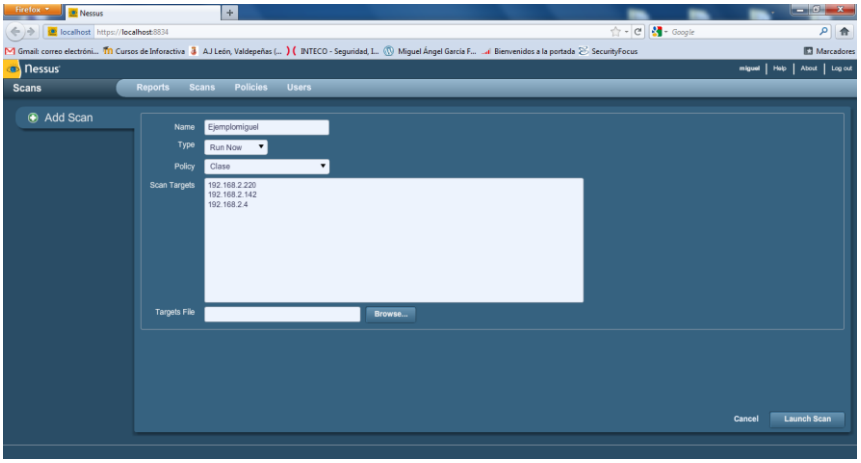
Ejecutamos el navegador, y nos vamos al localhost, en la ventana de login ponemos los datos anteriores.



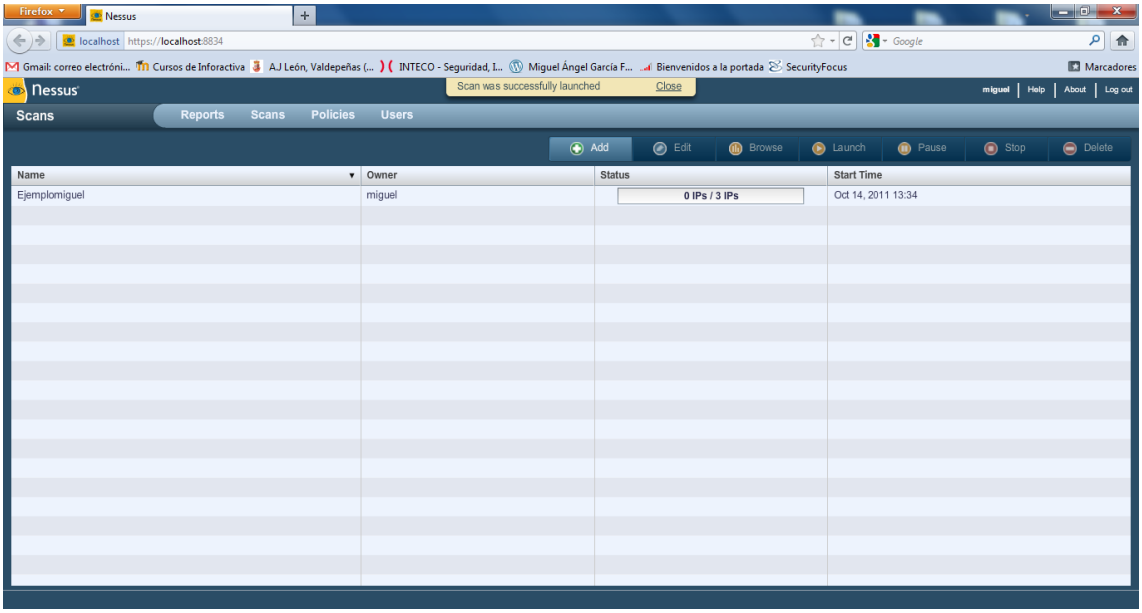

Para poder realizar una prueba, tenemos que configurar unos determinados parámetros, creamos una nueva política, la llamamos **Clase.** Marcamos la 2 y 3 opcion de los checkbox.



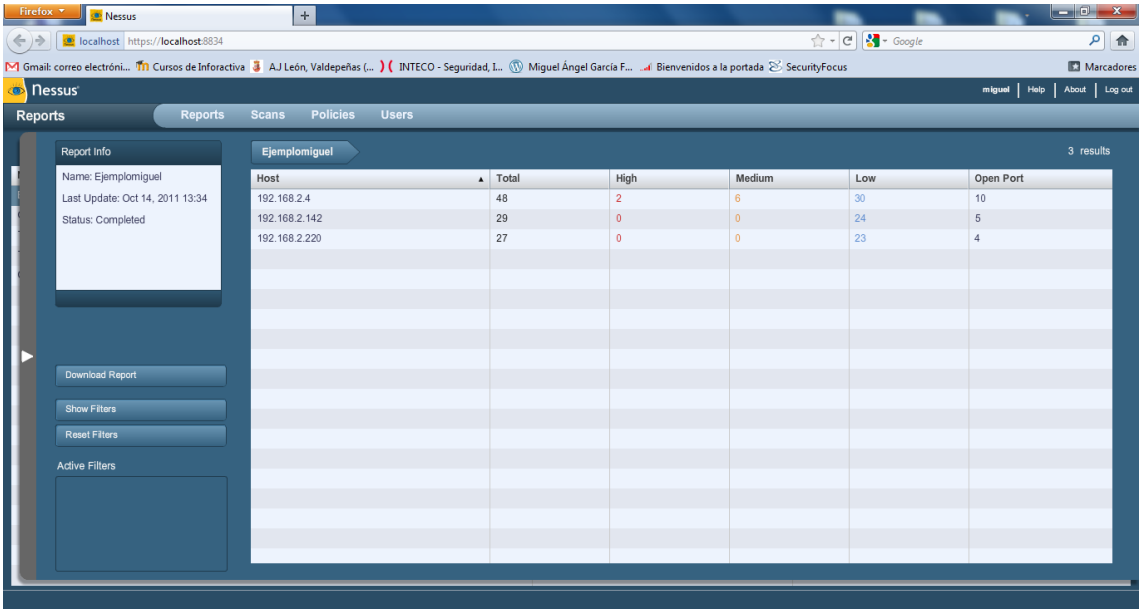
Una vez tengamos creado la política, vamos a realizar un escaneado de diferentes equipos, haciendo referencia las políticas que hemos configurado.



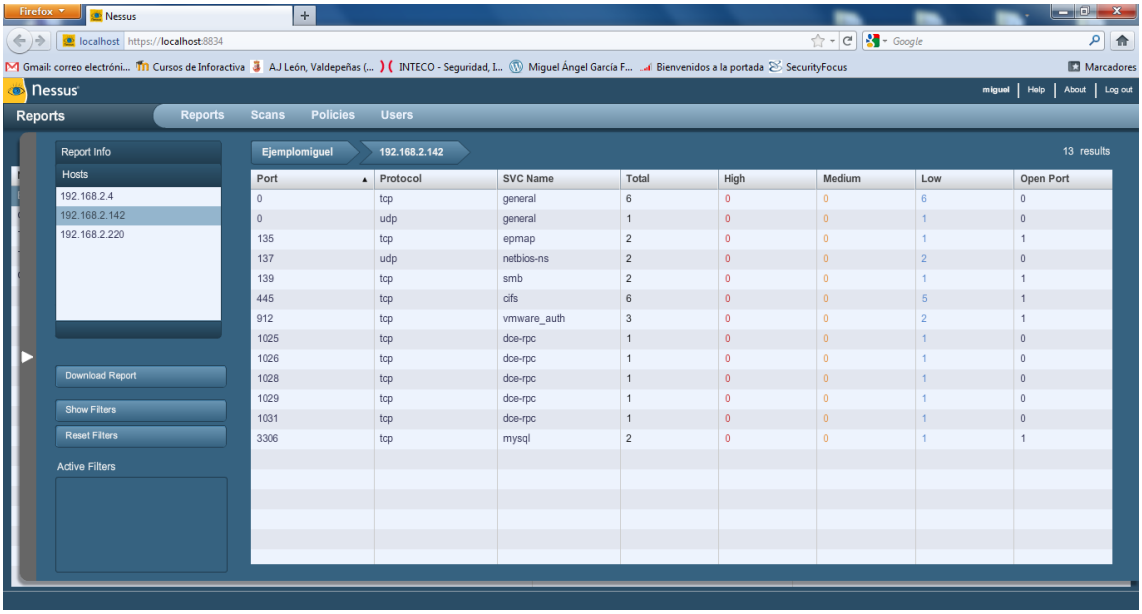

Comienza el escaneo.

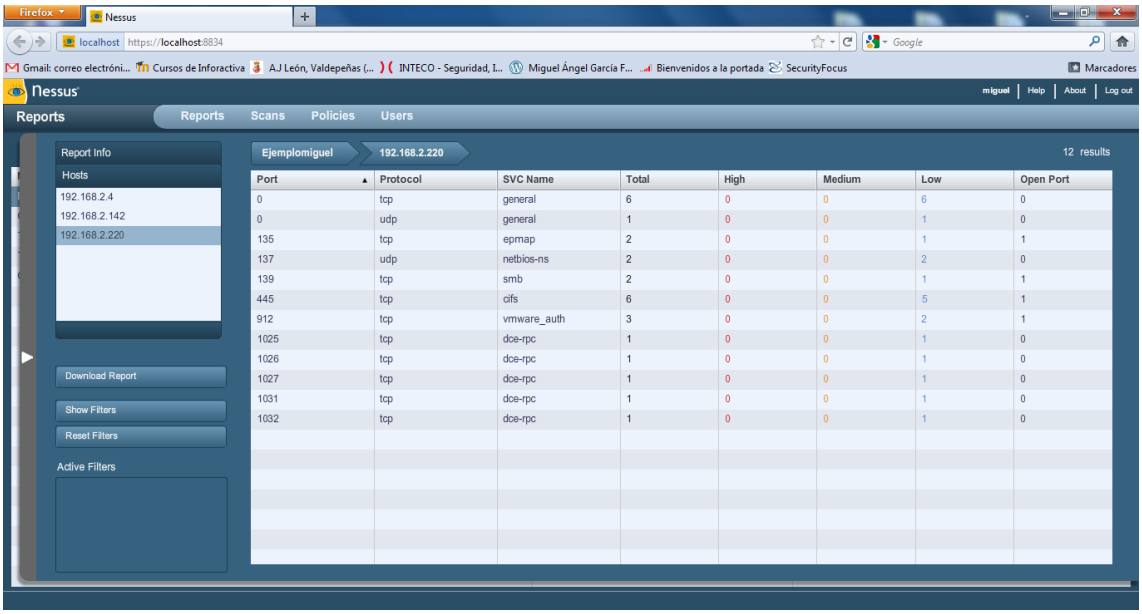


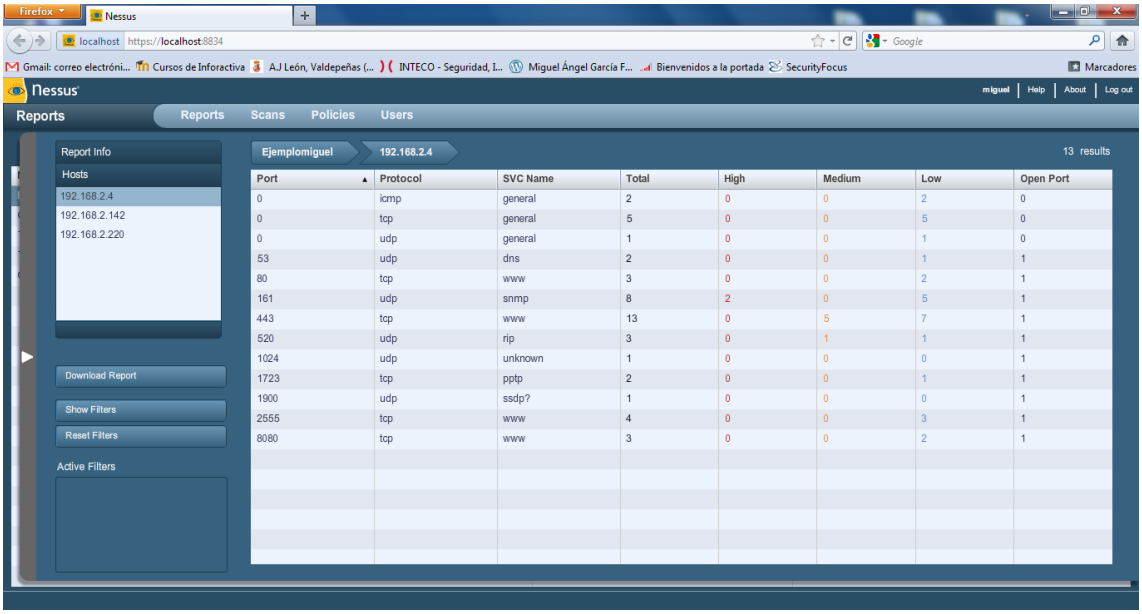
Una vez terminado, nos vamos al resultado, y comprobamos el número de puertos que ha podido escanear.




De cada una de las IP seleccionadas, nos mostrará los puertos que se estén usando, nombre, tipo de protocolo y otros términos.



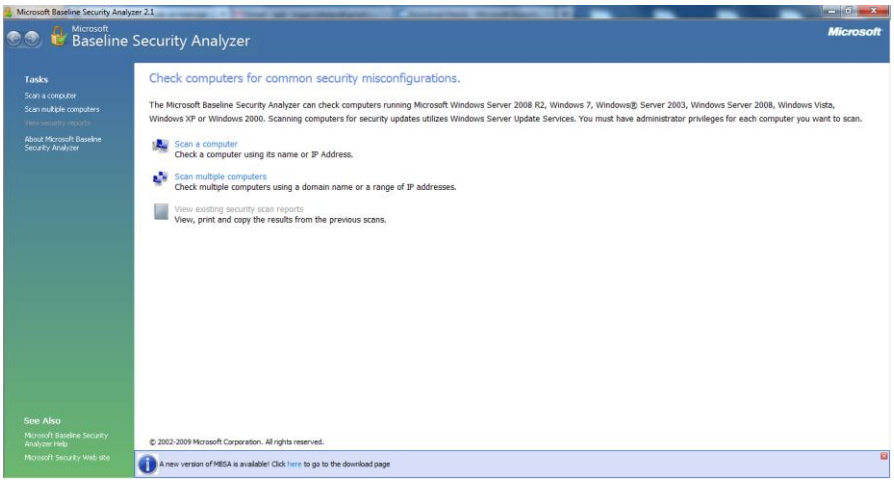

Firefox
Nessus
localhost https://localhost:8834
Google
Gmail: correo electróni... Cursos de Inforactiva A.J León, Valdepeñas (... INTECO - Seguridad, I... Miguel Ángel García F... Bienvenidos a la portada SecurityFocus
Marcadores
Nessus
miguel | Help | About | Log out
Reports
Reports Scans Policies Users
Report Info
Hosts
192.168.2.4
192.168.2.142
192.168.2.220
Download Report
Show Filters
Reset Filters
Active Filters
Ejemplomiguel
192.168.2.220
12 results
Port Protocol SVC Name Total High Medium Low Open Port
0 tcp general 6 0 0 6 0
0 udp general 1 0 0 1 0
135 tcp epmap 2 0 0 1 1
137 udp netbios-ns 2 0 0 2 0
139 tcp smb 2 0 0 1 1
445 tcp cifs 6 0 0 5 1
912 tcp vmware_auth 3 0 0 2 1
1025 tcp dce-rpc 1 0 0 1 0
1026 tcp dce-rpc 1 0 0 1 0
1027 tcp dce-rpc 1 0 0 1 0
1031 tcp dce-rpc 1 0 0 1 0
1032 tcp dce-rpc 1 0 0 1 0


Firefox
Nessus
localhost https://localhost:8834
Google
Gmail: correo electróni... Cursos de Inforactiva A.J León, Valdepeñas (... INTECO - Seguridad, I... Miguel Ángel García F... Bienvenidos a la portada SecurityFocus
Marcadores
Nessus
miguel | Help | About | Log out
Reports
Reports Scans Policies Users
Report Info
Hosts
192.168.2.4
192.168.2.142
192.168.2.220
Download Report
Show Filters
Reset Filters
Active Filters
Ejemplomiguel
192.168.2.4
13 results
Port Protocol SVC Name Total High Medium Low Open Port
0 icmp general 2 0 0 2 0
0 tcp general 5 0 0 5 0
0 udp general 1 0 0 1 0
53 udp dns 2 0 0 1 1
80 tcp www 3 0 0 2 1
161 udp snmp 8 2 0 5 1
443 tcp www 13 0 5 7 1
520 udp rip 3 0 1 1 1
1024 udp unknown 1 0 0 0 1
1723 tcp pptp 2 0 0 1 1
1900 udp ssdp? 1 0 0 0 1
2555 tcp www 4 0 0 3 1
8080 tcp www 3 0 0 2 1

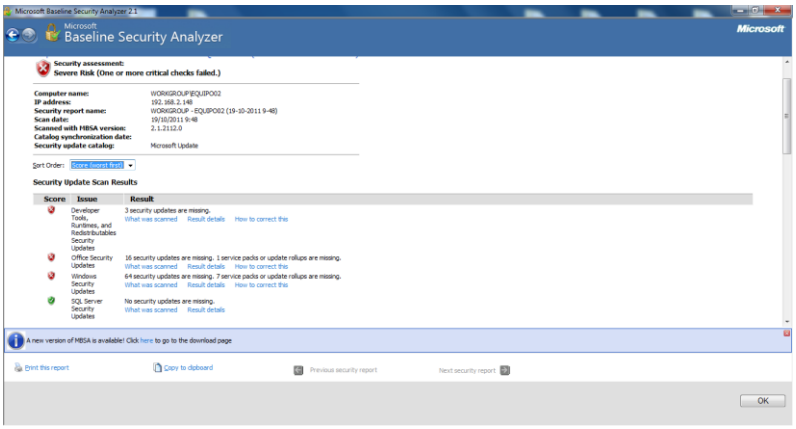
**Baseline Security Analyzer**

Es un analizador de vulnerabilidades del sistema de un equipo determinado.

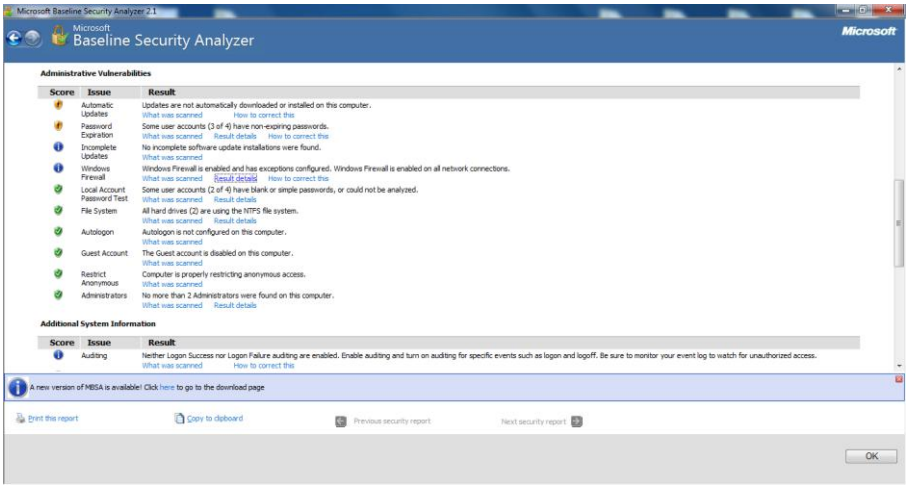
Una vez lo tengamos instalado. Tenemos diferentes opciones, escanear un ordenador, un grupo de ordenadores etc.




Si hacemos un nuevo escaneo, por ejemplo nuestra IP, 192.168.2.148/24, procederá a realizar una búsqueda de vulnerabilidades.




Una vez finalizado, nos hace un informe con las siguientes vulnerabilidades.



Podemos hacer un escáner mucho más amplio con varios ordenadores de la red, el proceso es lento y requiere tiempo. Algunos antivirus, pueden denegarnos su acceso.