TEMA1. PRACTICA 3: DISPONIBILIDAD

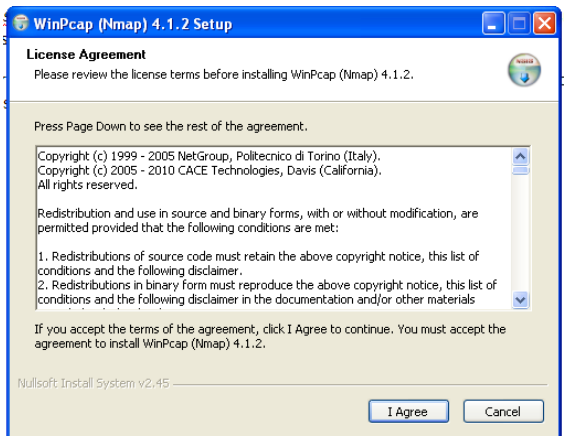
1. COMPROBAR DISPONIBILIDAD CON NMAP.

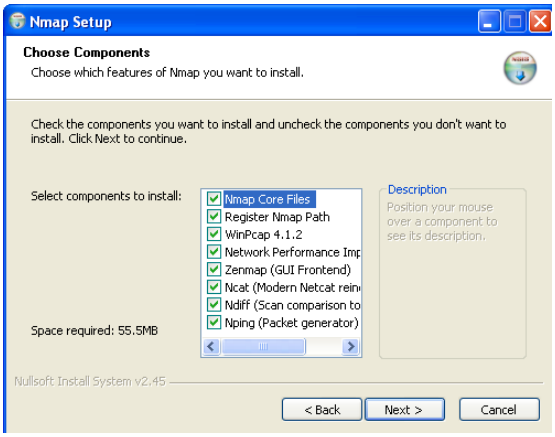
Nmap (“Network Mapper ") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Cuando ejecutamos comandos se lista una tabla.

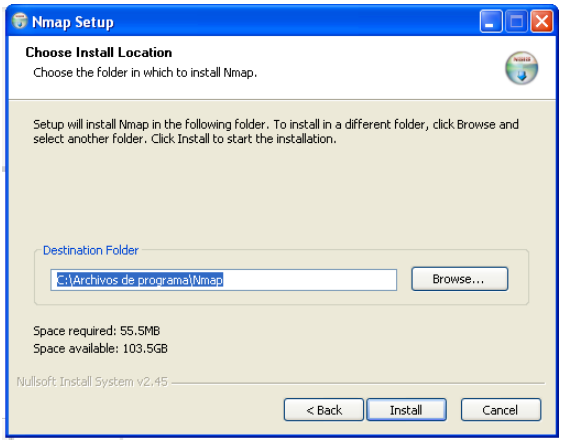
Dicha tabla lista el número de puerto y protocolo, nombre del servicio, y el Estado. El estado puede ser abierto, filtrado , cerrados , o sin filtrar . *Abierto* significa que una aplicación en la máquina de destino se encuentra esperando conexiones/paquetes en ese puerto. *filtrada* significa que un cortafuegos, filtro, o obstáculo en la red está bloqueando el puerto para que Nmap no puede saber si está abierto o cerrado . *Cerrado* los puertos no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como *no filtrados* son aquellos que responden a los sondeos de Nmap, pero que Nmap no puede determinar si están abiertas o cerradas

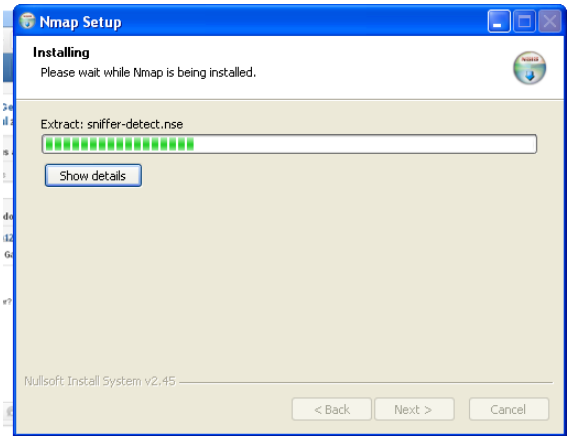
1.2 DISPONIBILIDAD EN WINDOWS.

- Vamos a buscar vulnerabilidades en los puertos con el programa nmap.
- Para instalar la aplicación la descargamos y ejecutamos el instalador y nos saldrá un asistente.

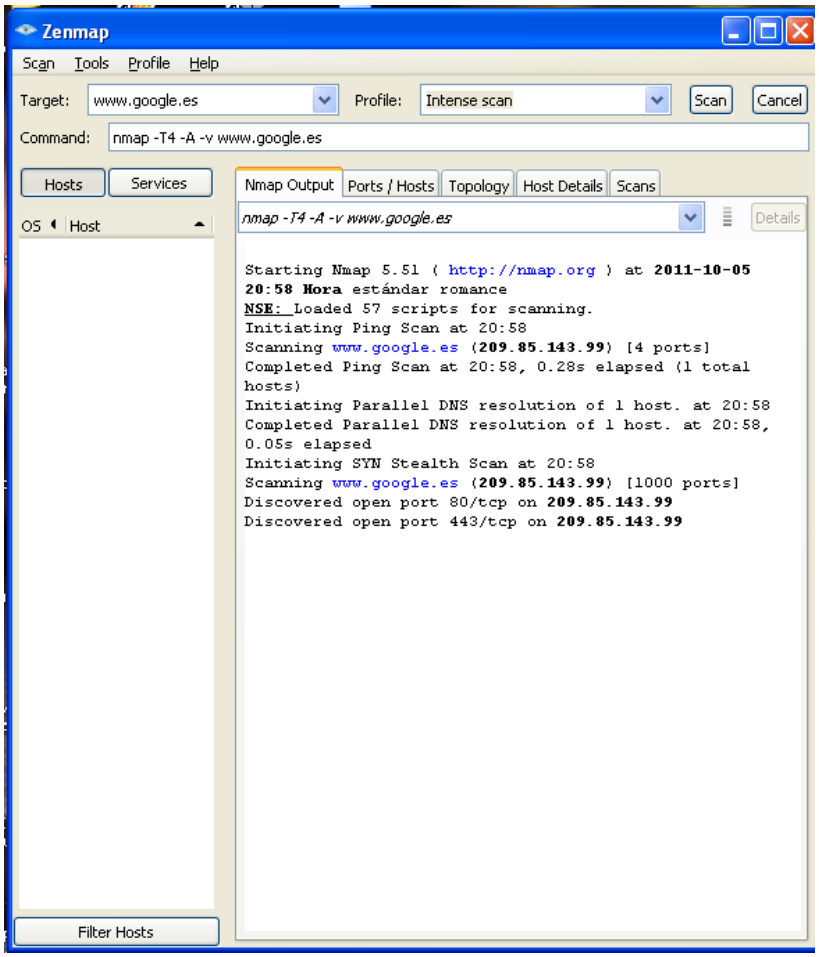


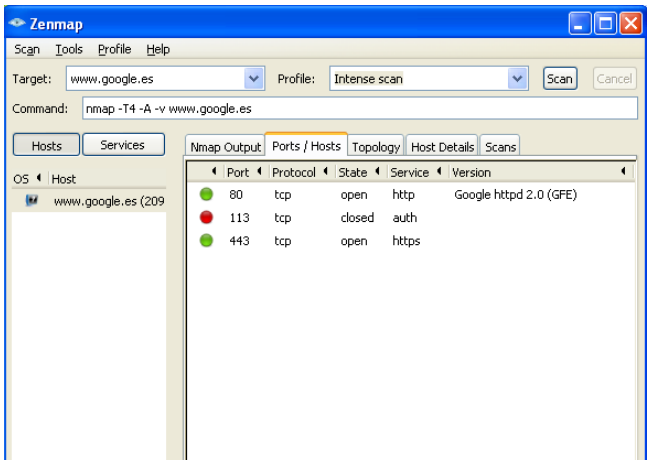




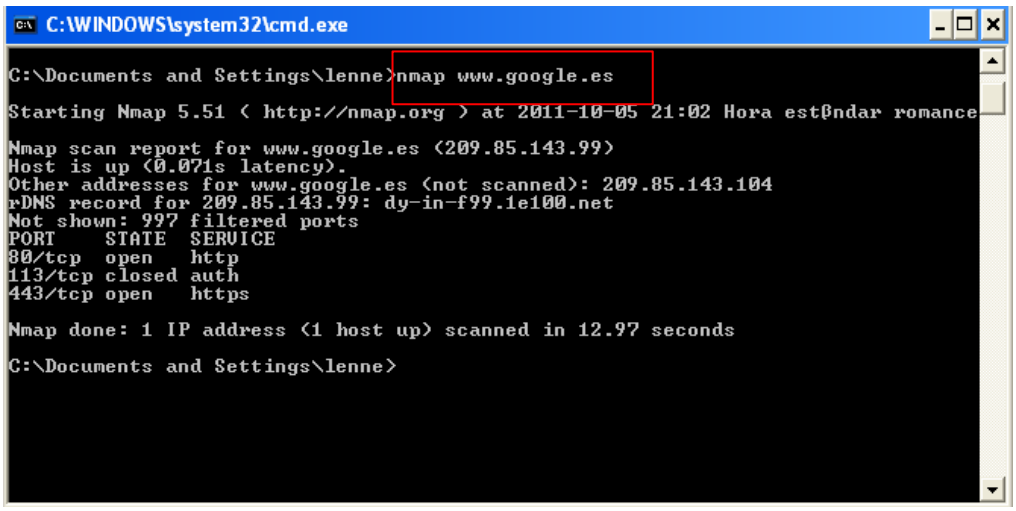


- Una vez instalado el programa lo ejecutamos y procedemos por ejemplo a realizar un escáner de los puertos de www.google.es

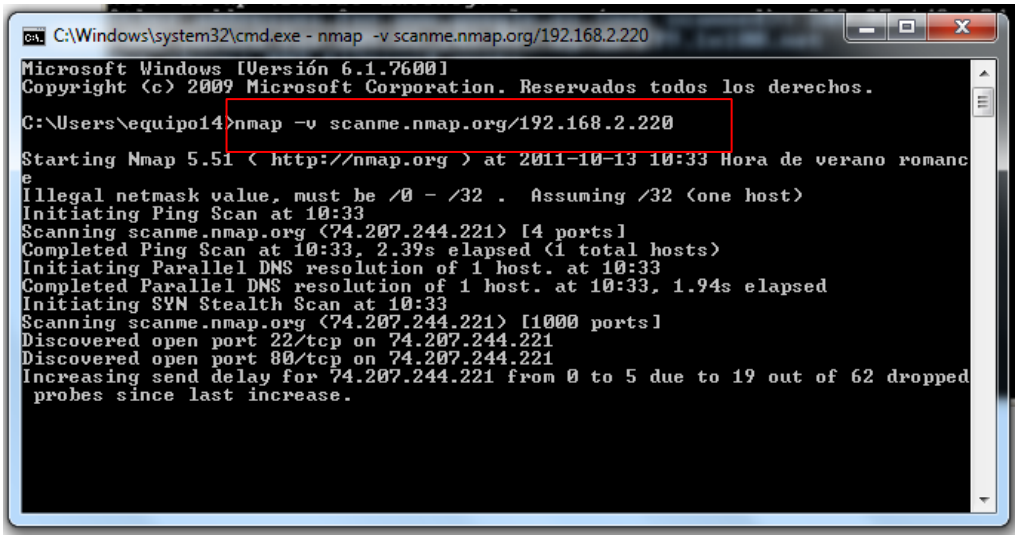




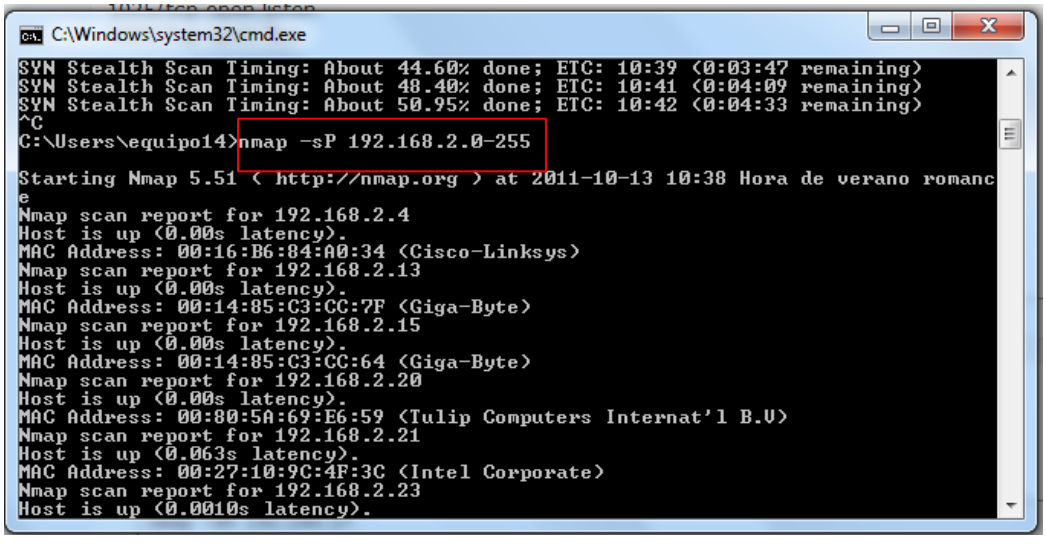
- También podemos realizar el escáner en modo consola. Nos muestra los puertos abiertos y cerrados.



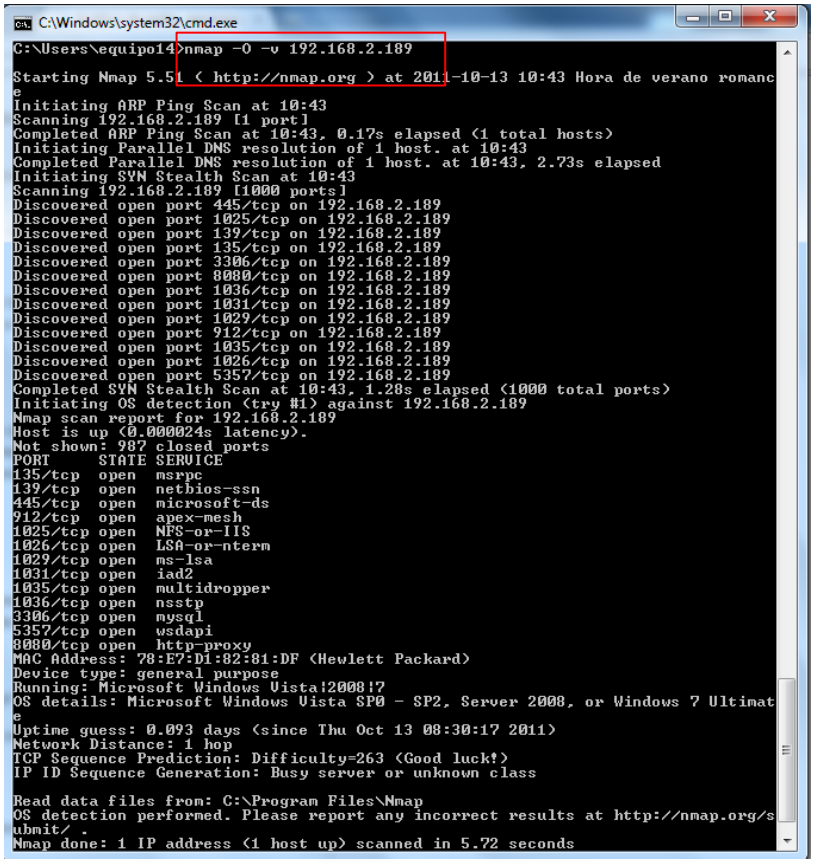
- Con el comando del siguiente ejemplo podemos ver los puertos abiertos de la ip que le indiquemos.



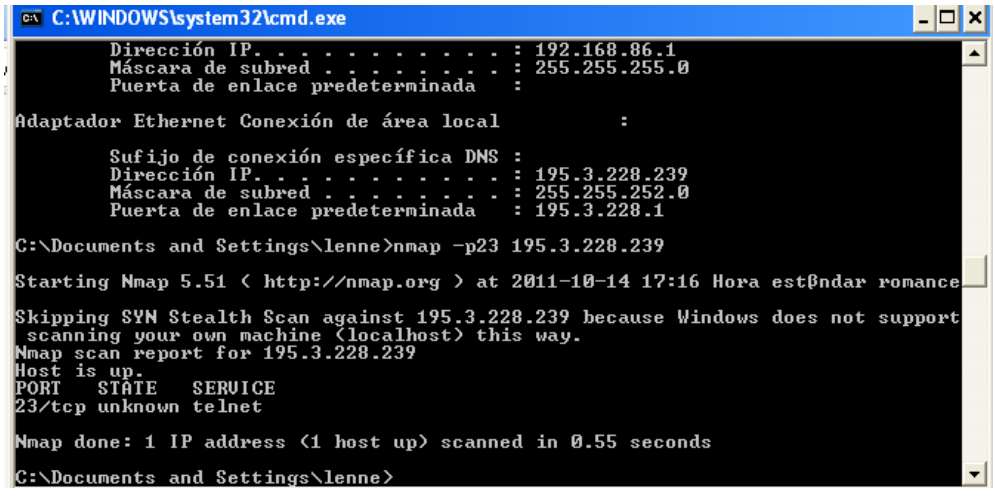
- Con el comando del siguiente ejemplo podemos ver los equipos de la red que están disponibles.



- Con el comando del siguiente ejemplo podemos ver el sistema operativo de un equipo y además los puertos abiertos del mismo.



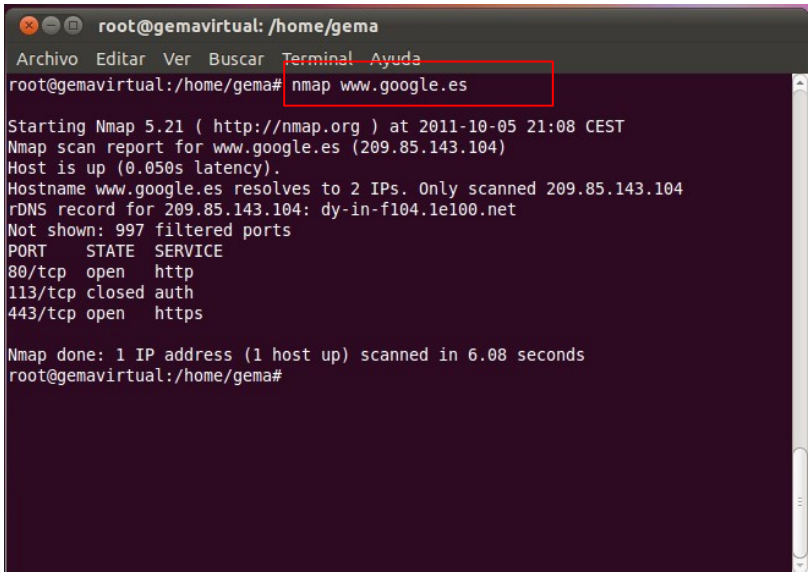
- Por ejemplo para ver si un determinado puerto está abierto ó cerrado (lo haremos con telnet, puerto 23) ponemos el siguiente comando:
  >nmap –p23 192.3.228.239



1.2 DISPONIBILIDAD EN LINUX.

- Una vez instalada la aplicación con el comando >apt-get install nmap procedemos a realizar el primer escáner.

- Hacemos un nmap a www.google.es y nos muestra los puertos abiertos y cerrados.

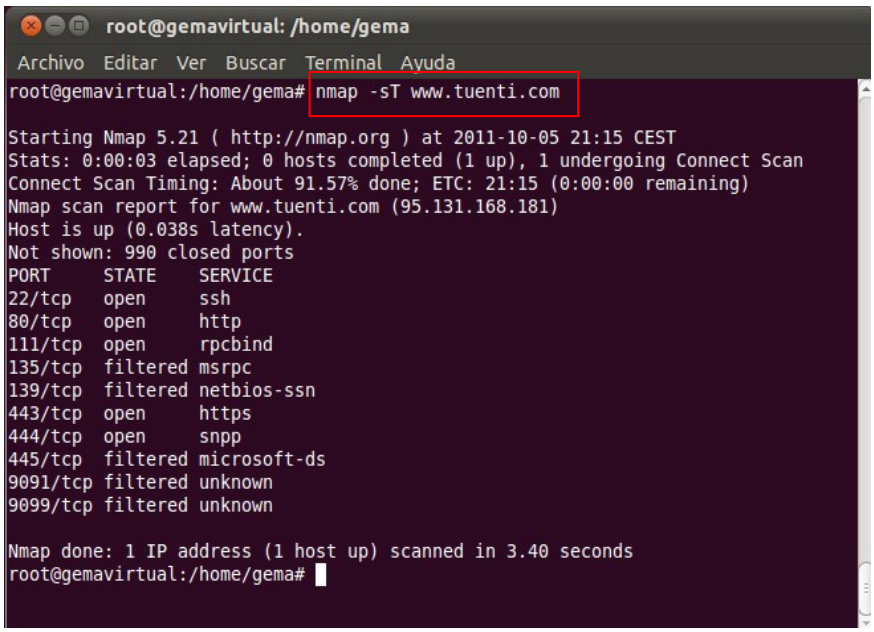


Cabe resaltar que existen varios tipos de modificadores de scan lo más importante es lograr identificar la combinación más apropiada, los modificadores que se pueden utilizar para realizar el scan son los siguientes:

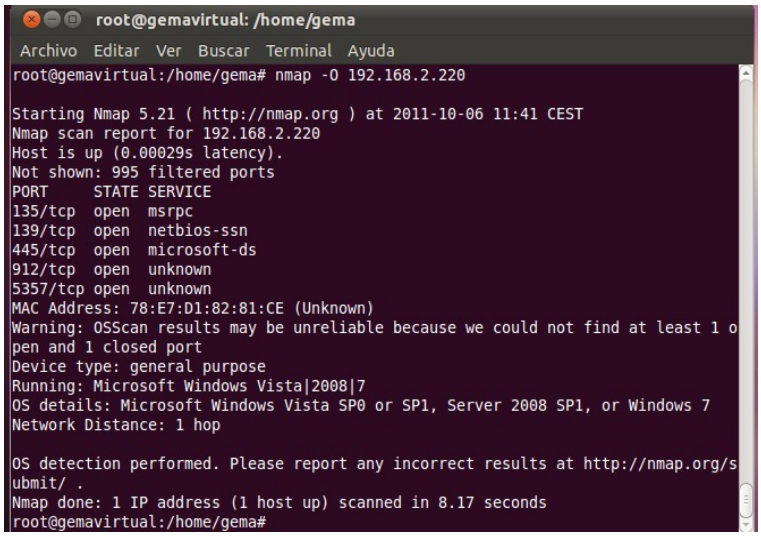
- **sT** se intenta hacer un barrido de puertos por TCP.
- **sU** se intenta hacer un barrido de puertos por UDP, es útil cuando se intentan descubrir puertos de nivel superior que pueden estar detrás de un firewall.
- **sA** se usan mensajes de ACK para lograr que sistema responda y así determinar si el puerto está abierto.
- **sX** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red
- **sN** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red
- **sF** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red
- **sP** similar a Ping.
- **sV** intenta identificar los servicios por los puertos abiertos en el sistema esto permite evaluar cada servicio de forma individual para intentar ubicar vulnerabilidades en los mismos.
- **sO** con esta opción se identifica que protocolos de nivel superior a capa tres (Red o Network) responden en el sistema, de esta manera es más fácil saber las características de la red o el sistema que se intenta evaluar.

EJEMPLO:

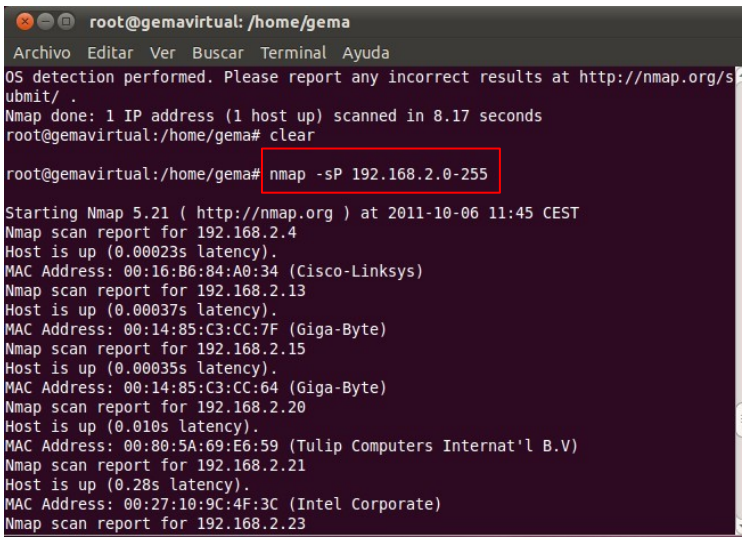
- Hacemos un nmap a www.tuenti.com y nos muestra un barrido de puertos por tcp.



- Con el comando del siguiente ejemplo podemos ver los puertos abiertos y el sistema operativo del host al que le corresponda la ip que le indiquemos.

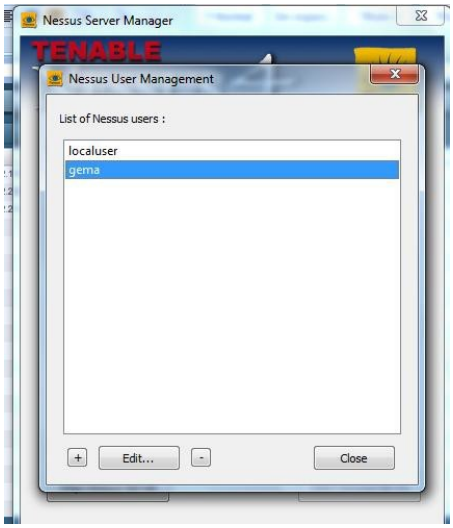


- Con el comando del siguiente ejemplo podemos ver los host que están disponibles dentro de la red que le indiquemos.


root@gemavirtual: /home/gema
Archivo Editar Ver Buscar Terminal Ayuda
OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds
root@gemavirtual:/home/gema# clear
root@gemavirtual:/home/gema# nmap -sP 192.168.2.0-255
Starting Nmap 5.21 (http://nmap.org) at 2011-10-06 11:45 CEST
Nmap scan report for 192.168.2.4
Host is up (0.00023s latency).
MAC Address: 00:16:B6:84:A0:34 (Cisco-Linksys)
Nmap scan report for 192.168.2.13
Host is up (0.00037s latency).
MAC Address: 00:14:85:C3:CC:7F (Giga-Byte)
Nmap scan report for 192.168.2.15
Host is up (0.00035s latency).
MAC Address: 00:14:85:C3:CC:64 (Giga-Byte)
Nmap scan report for 192.168.2.20
Host is up (0.010s latency).
MAC Address: 00:80:5A:69:E6:59 (Tulip Computers Internat'l B.V)
Nmap scan report for 192.168.2.21
Host is up (0.28s latency).
MAC Address: 00:27:10:9C:4F:3C (Intel Corporate)
Nmap scan report for 192.168.2.23

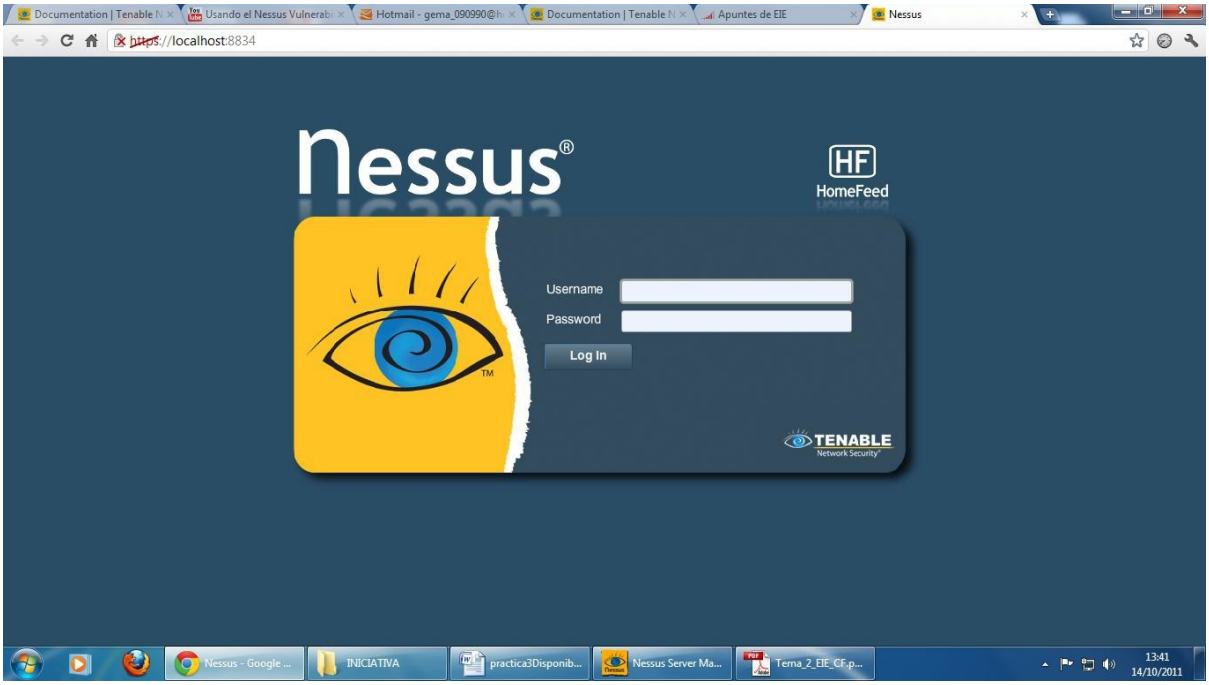
2. COMPROBAR DISPONIBILIDAD CON NESSUS.

- Una vez instalada la aplicación Nessus e introducida la clave de validación nos creamos un usuario para entrar más tarde a la aplicación.

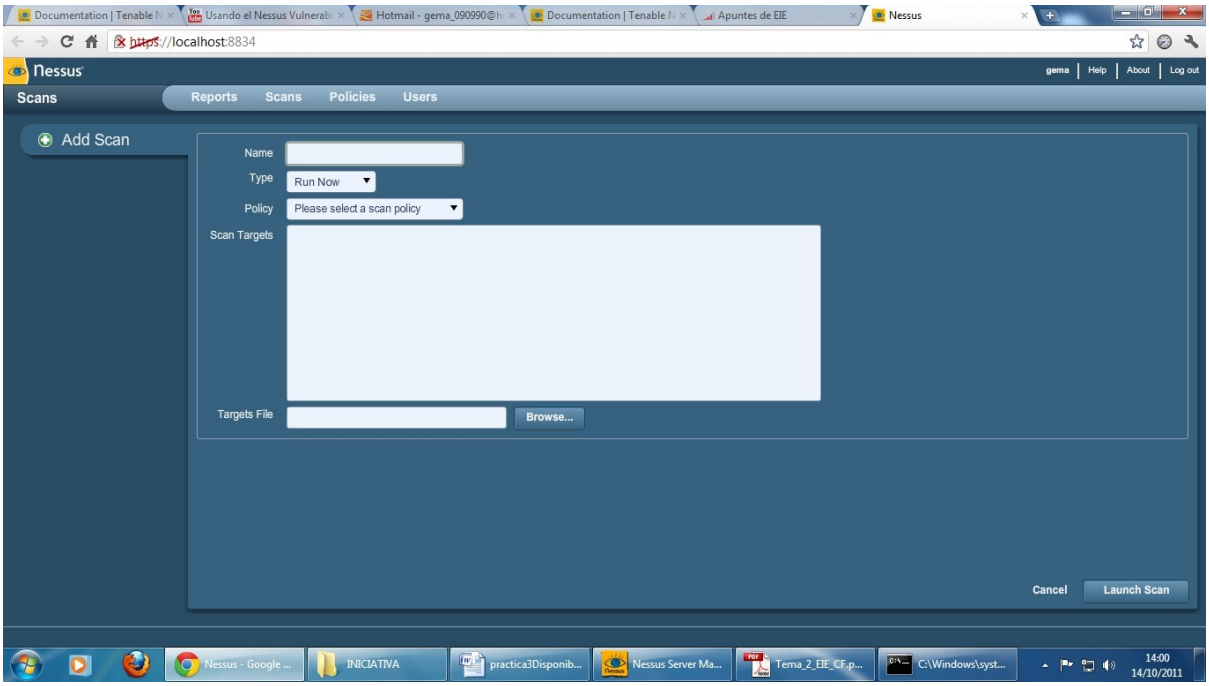


- Cuando hayamos creado el usuario damos a start en el servidor y ejecutamos el cliente, este se ejecutará en el navegador que usemos por defecto.

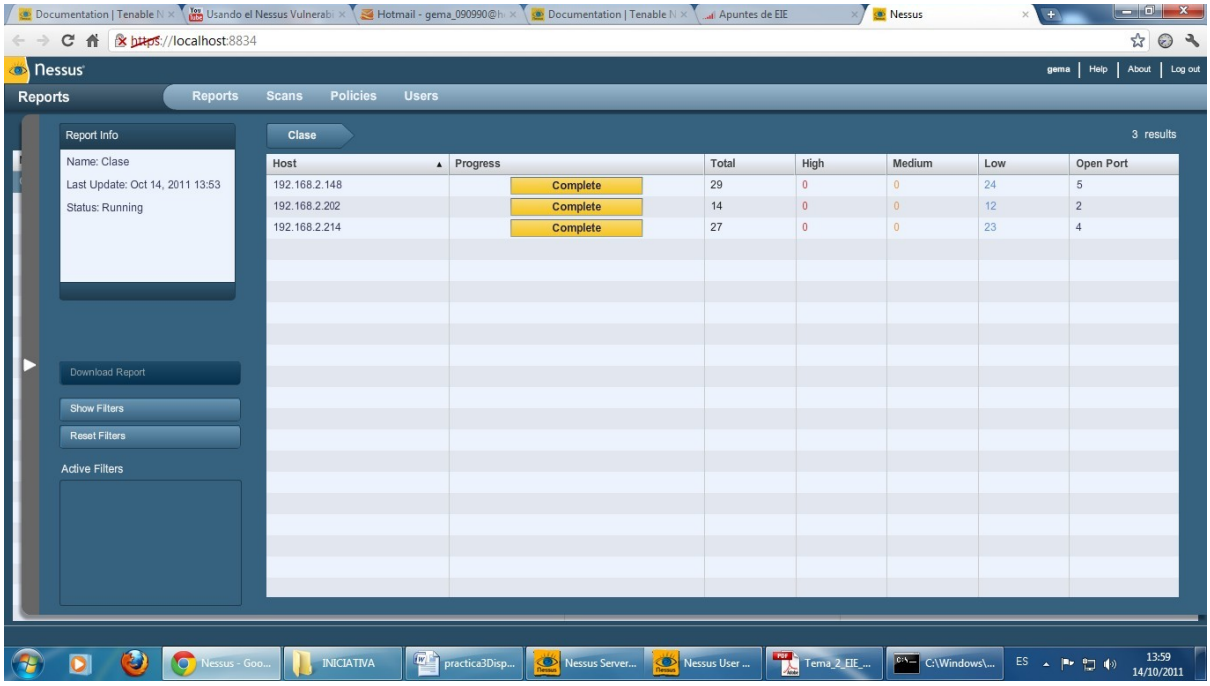
- Cuando ejecutemos el cliente debemos poner el nombre de usuario que hemos creado anteriormente.



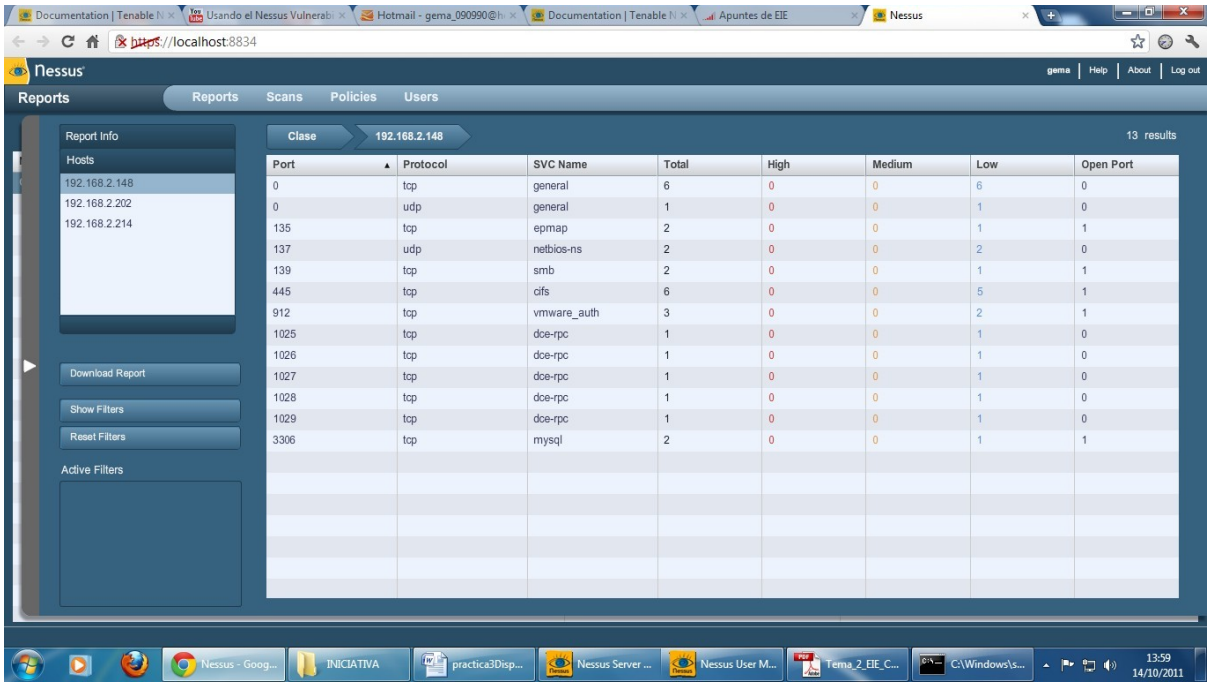
- Una vez iniciada la sesión pinchamos en añadir, para añadir un nuevo escáner.
- Le ponemos un nombre, el que queramos, en nuestro caso Clase.
- En el tipo elegimos “escanear ahora”.
- En policy elegimos hacer un escáner interno.
- En el cuadro de Targets ponemos la ó las ip que vamos a escanear, en nuestro caso serán tres.
- Y finalmente damos al botón “Launch Scan”, para que comience el escáner.

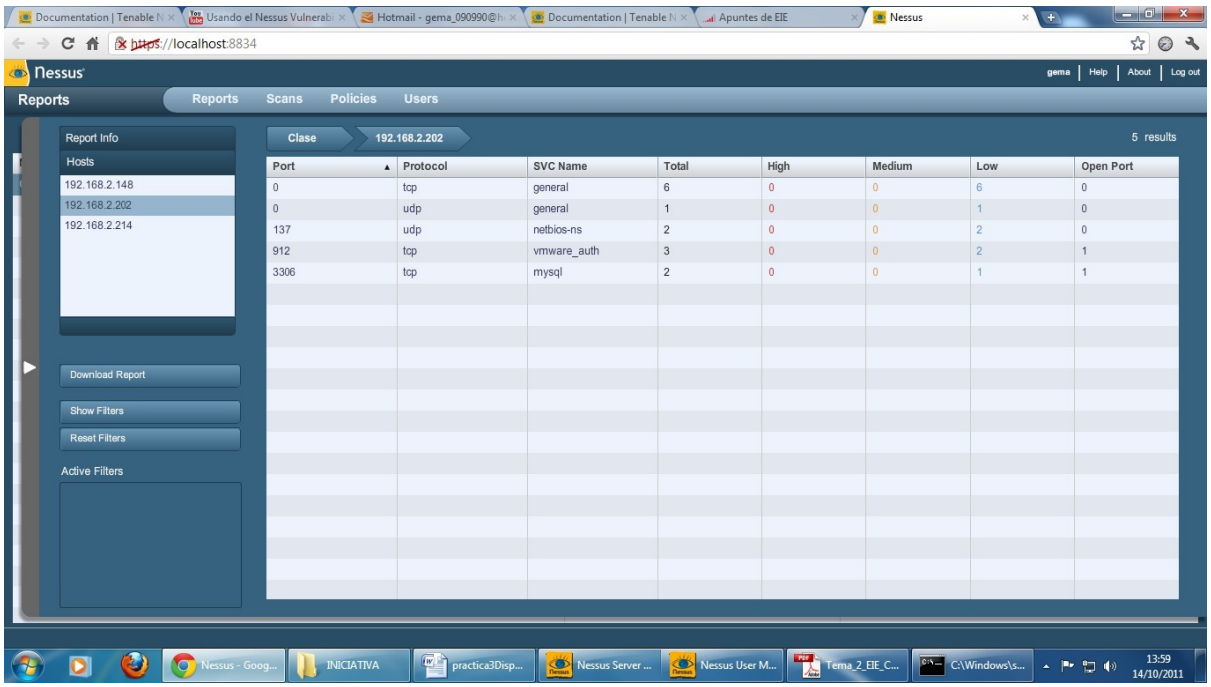


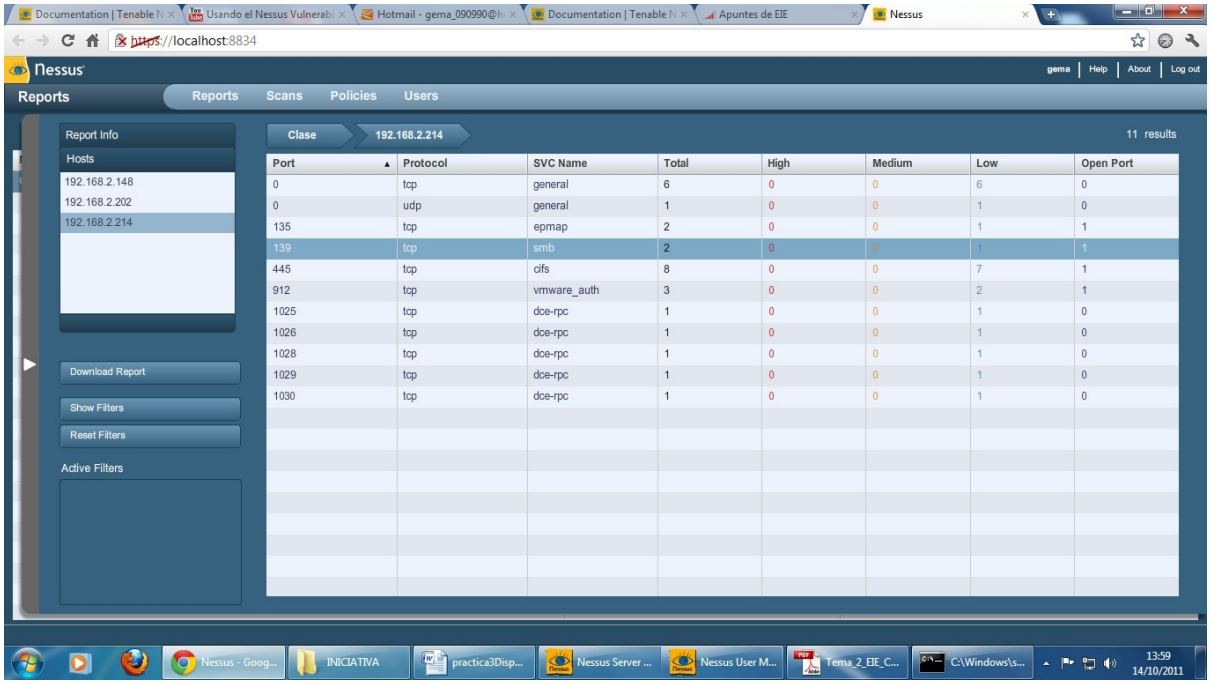
- Podemos ver que el escáner ha terminado.



- Pichando en cada una de las ip, podemos ver de forma más detallada el número de puerto, el protocolo que usa ó si está abierto o cerrado.

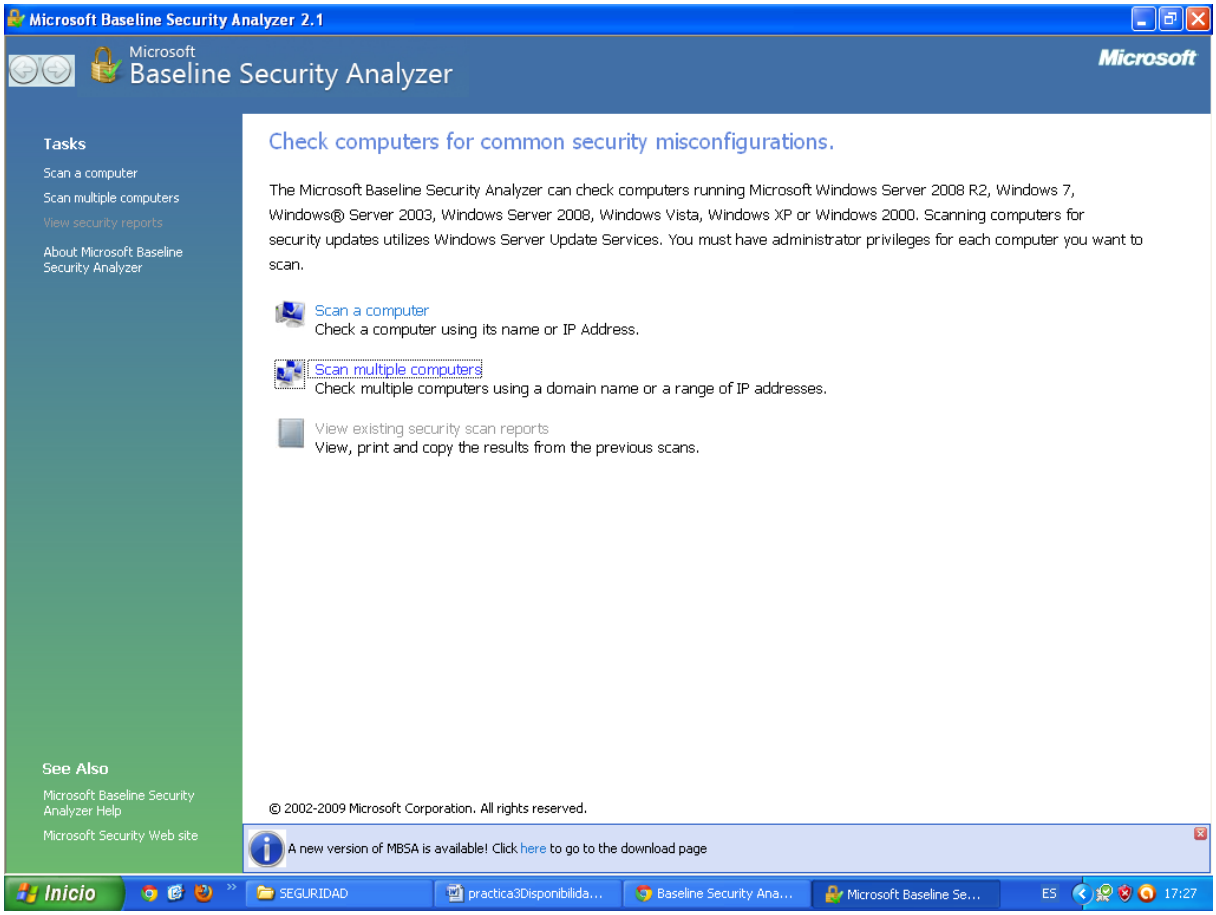



Nessus
https://localhost:8834
gema | Help | About | Log out
Reports
Reports Scans Policies Users
Report Info
Hosts
192.168.2.148
192.168.2.202
192.168.2.214
Download Report
Show Filters
Reset Filters
Active Filters
Clase
192.168.2.202
5 results
Port Protocol SVC Name Total High Medium Low Open Port
0 tcp general 6 0 0 6 0
0 udp general 1 0 0 1 0
137 udp netbios-ns 2 0 0 2 0
912 tcp vmware_auth 3 0 0 2 1
3306 tcp mysql 2 0 0 1 1
13:59
14/10/2011

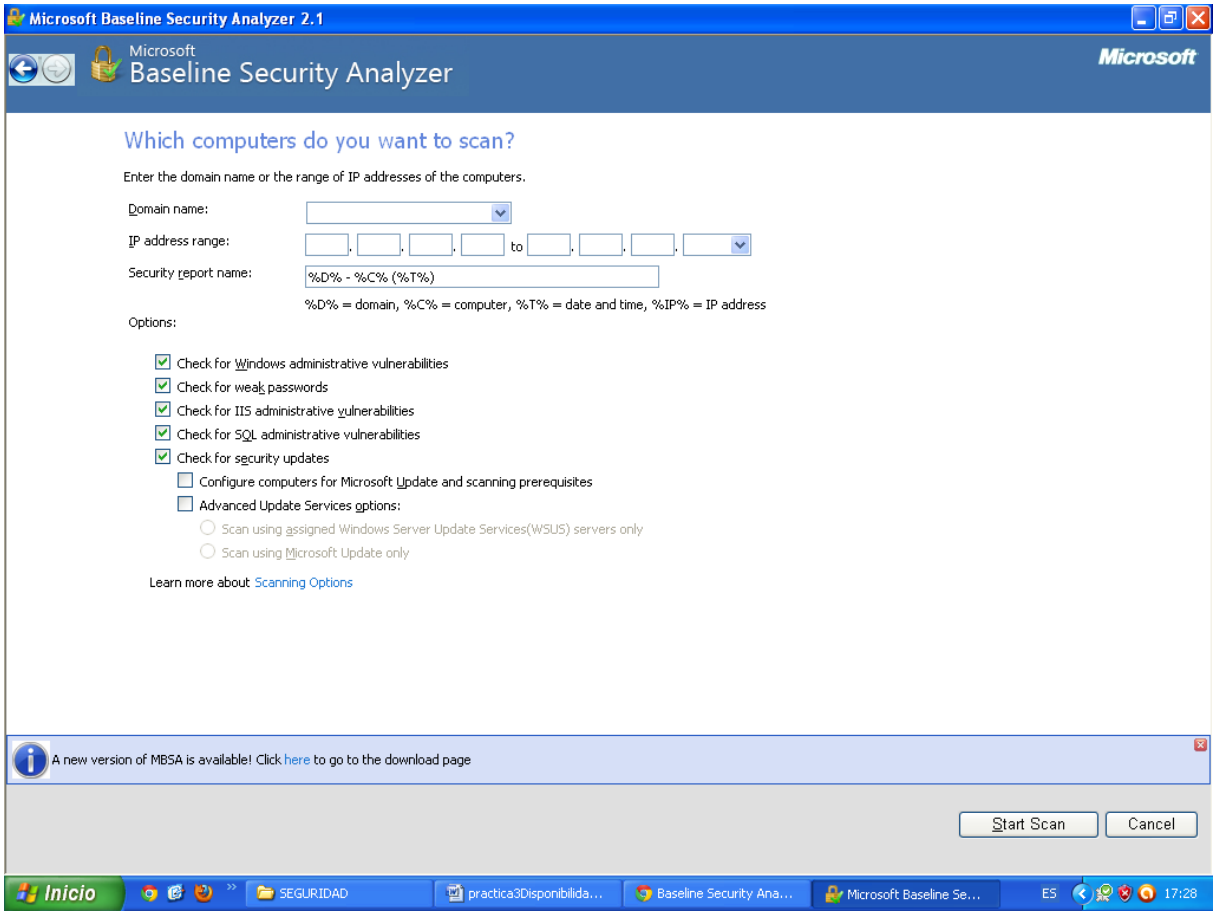

Nessus
https://localhost:8834
gema | Help | About | Log out
Reports
Reports Scans Policies Users
Report Info
Hosts
192.168.2.148
192.168.2.202
192.168.2.214
Download Report
Show Filters
Reset Filters
Active Filters
Clase
192.168.2.214
11 results
Port Protocol SVC Name Total High Medium Low Open Port
0 tcp general 6 0 0 6 0
0 udp general 1 0 0 1 0
135 tcp epmap 2 0 0 1 1
139 tcp smb 2 0 0 1 1
445 tcp cifs 8 0 0 7 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
1028 tcp dce-rpc 1 0 0 1 0
1029 tcp dce-rpc 1 0 0 1 0
1030 tcp dce-rpc 1 0 0 1 0
13:59
14/10/2011

3. COMPROBAR DISPONIBILIDAD CON MBSA.

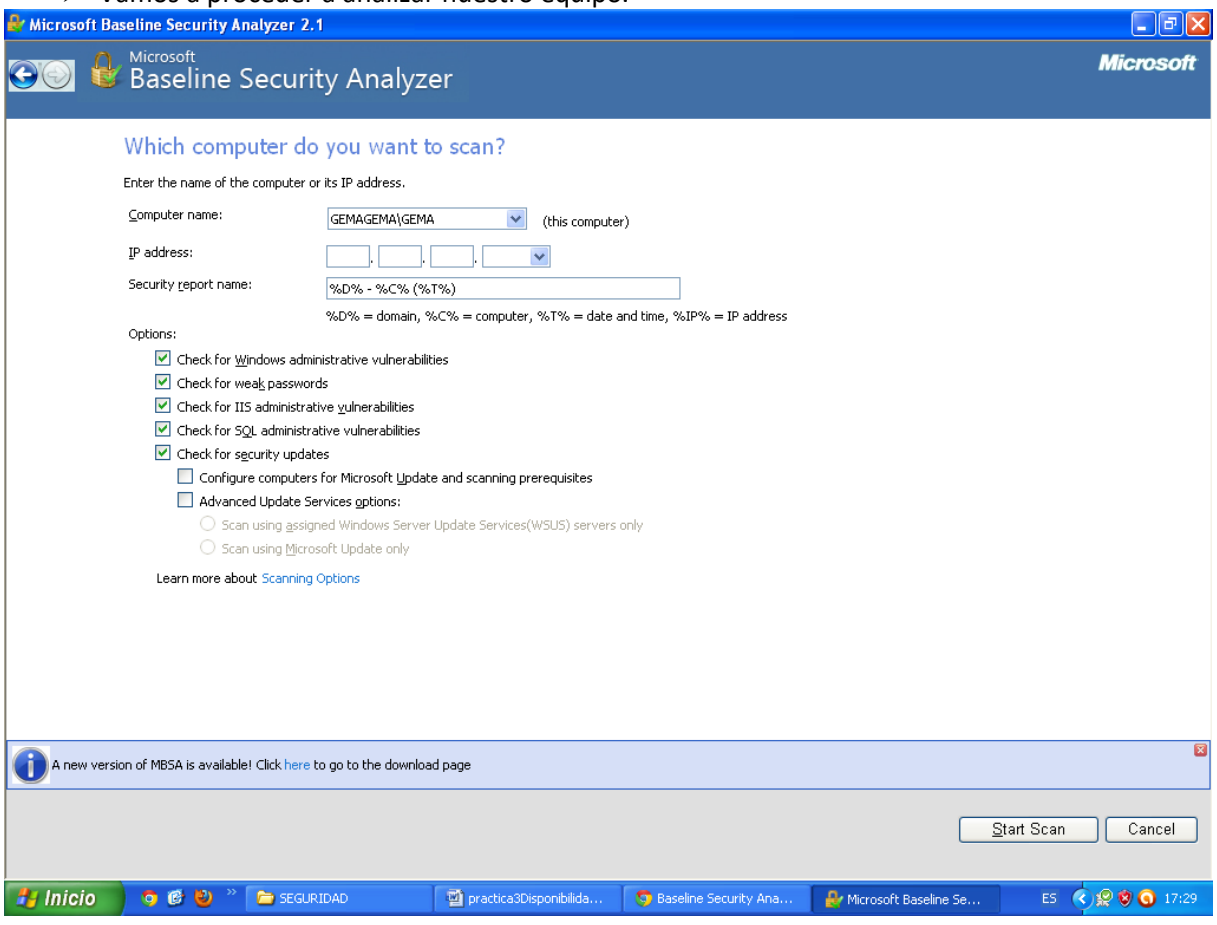
- Una vez descargado e instalado MBSA lo ejecutamos y podemos ver lo siguiente, podemos elegir hacer un escáner de nuestro equipo o de varios equipos.

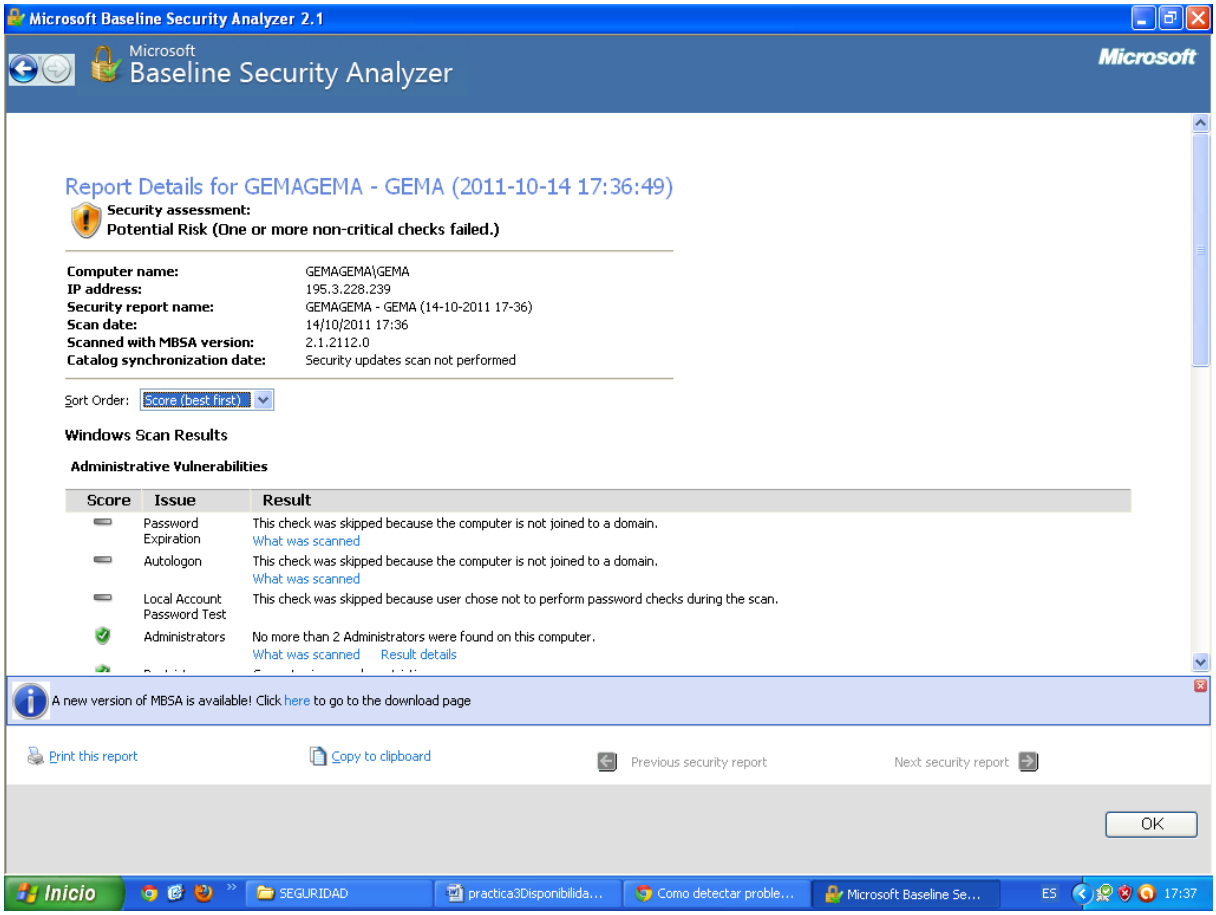


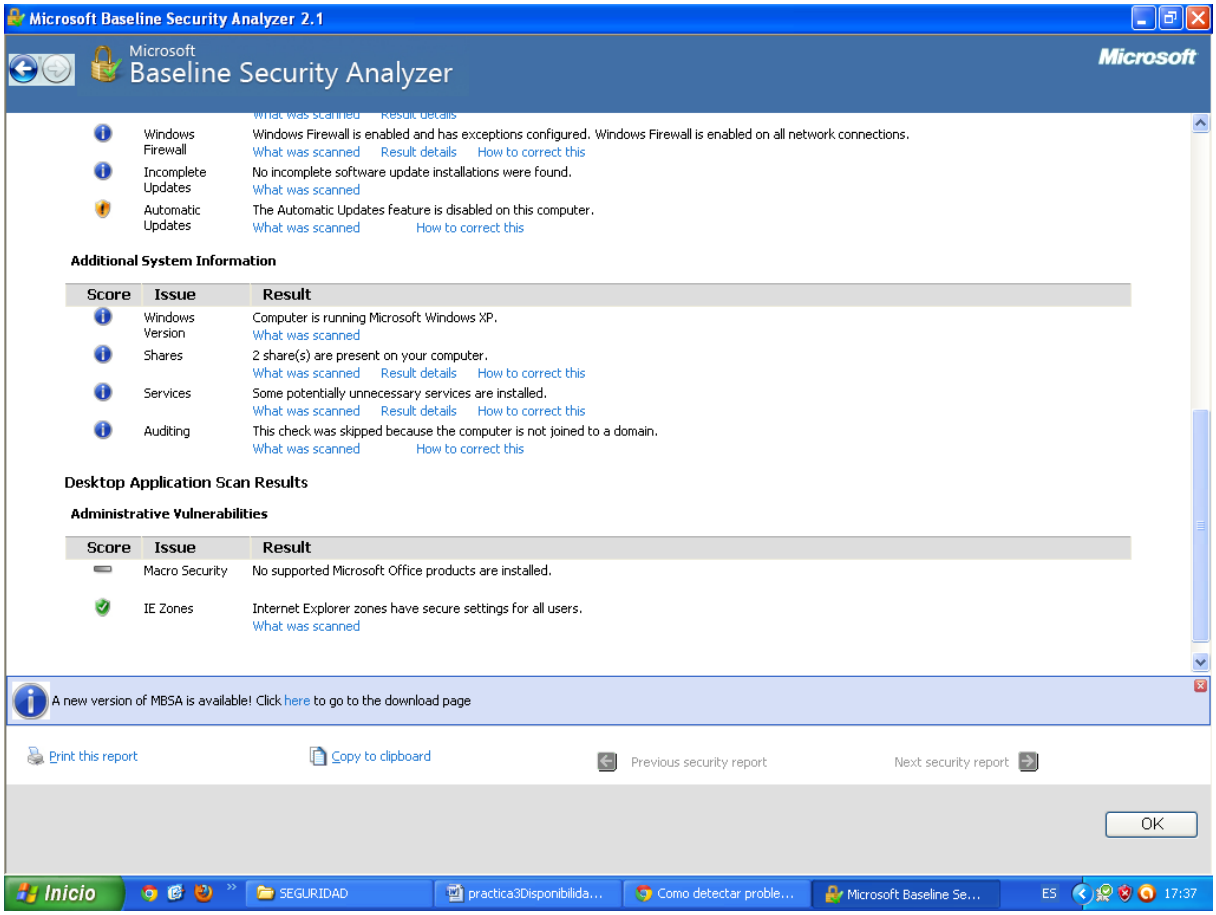
- En la siguiente pantalla tenemos las opciones para analizar varios equipos.



- Vamos a proceder a analizar nuestro equipo.




Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Report Details for GEMAGEMA - GEMA (2011-10-14 17:36:49)
Security assessment:
Potential Risk (One or more non-critical checks failed.)
Computer name: GEMAGEMA\GEMA
IP address: 195.3.228.239
Security report name: GEMAGEMA - GEMA (14-10-2011 17-36)
Scan date: 14/10/2011 17:36
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date: Security updates scan not performed
Sort Order: Score (best first)
Windows Scan Results
Administrative Vulnerabilities
Score
Issue
Result
Password Expiration
This check was skipped because the computer is not joined to a domain.
What was scanned
Autologon
This check was skipped because the computer is not joined to a domain.
What was scanned
Local Account Password Test
This check was skipped because user chose not to perform password checks during the scan.
Administrators
No more than 2 Administrators were found on this computer.
What was scanned
Result details
A new version of MBSA is available! Click here to go to the download page
Print this report
Copy to clipboard
Previous security report
Next security report
OK
Inicio
SEGURIDAD
practica3Disponibilida...
Como detectar proble...
Microsoft Baseline Se...
ES
17:37



Nota: esta práctica la he realizado en casa donde solo tengo un equipo con lo cual el escáner sólo lo he hecho de mi equipo.