

TEMA1. PRACTICA 3: DISPONIBILIDAD

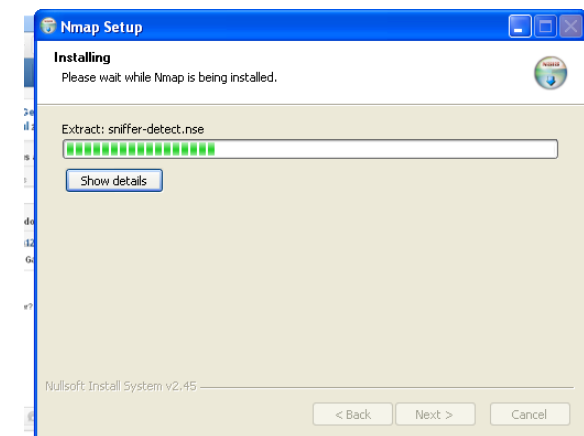
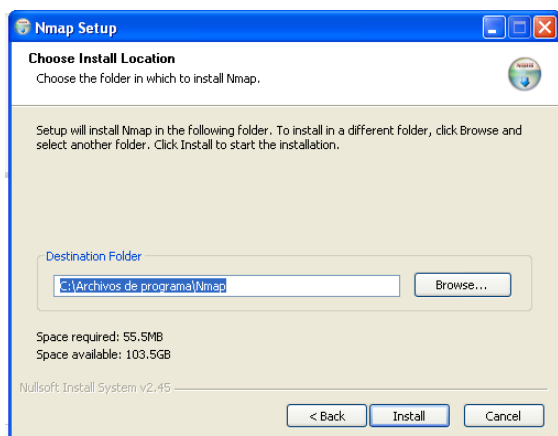
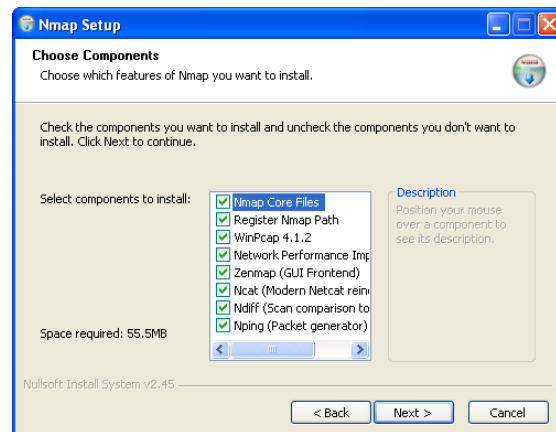
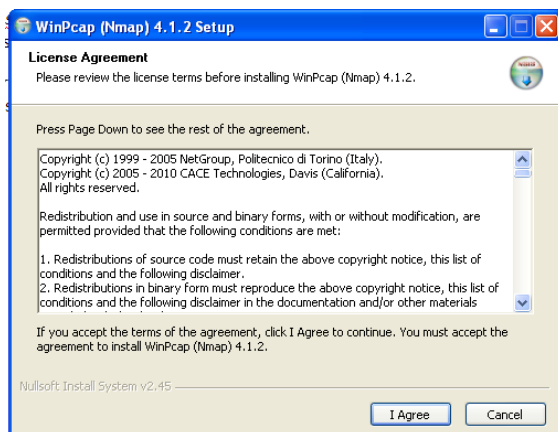
1. COMPROBAR DISPONIBILIDAD CON NMAP.

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

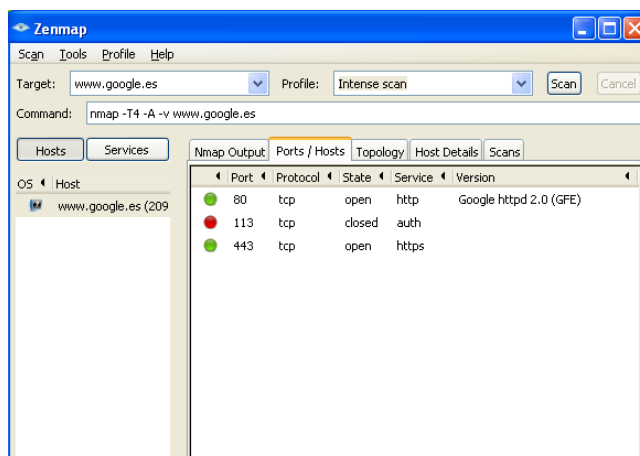
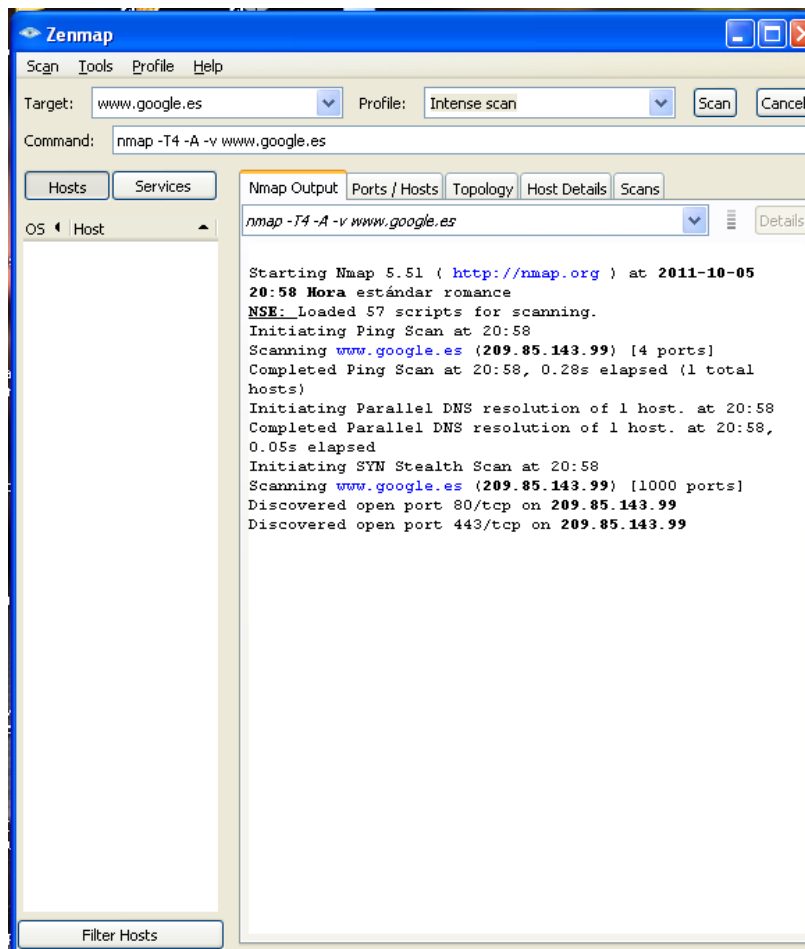
Dicha tabla lista el número de puerto y protocolo, nombre del servicio, y el Estado. El estado puede ser abierto, filtrado , cerrados , o sin filtrar . Abierto significa que una aplicación en la máquina de destino se encuentra esperando conexiones/paquetes en ese puerto. filtrada significa que un cortafuegos, 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.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\lenne>nmap www.google.es

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-05 21:02 Hora estándar romance
Nmap scan report for www.google.es (209.85.143.99)
Host is up (0.071s latency).
Other addresses for www.google.es (not scanned): 209.85.143.104
rDNS record for 209.85.143.99: dy-in-f99.1e100.net
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed auth
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 12.97 seconds
C:\Documents and Settings\lenne>
```

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

```
C:\Windows\system32\cmd.exe - nmap -v scanme.nmap.org/192.168.2.220

Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\equipo14>nmap -v scanme.nmap.org/192.168.2.220

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-13 10:33 Hora de verano romanc
e
Illegal netmask value, must be /0 - /32 . Assuming /32 (one host)
Initiating Ping Scan at 10:33
Scanning scanme.nmap.org (74.207.244.221) [4 ports]
Completed Ping Scan at 10:33, 2.39s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:33
Completed Parallel DNS resolution of 1 host. at 10:33, 1.94s elapsed
Initiating SYN Stealth Scan at 10:33
Scanning scanme.nmap.org (74.207.244.221) [1000 ports]
Discovered open port 22/tcp on 74.207.244.221
Discovered open port 80/tcp on 74.207.244.221
Increasing send delay for 74.207.244.221 from 0 to 5 due to 19 out of 62 dropped
probes since last increase.
```

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

```
C:\Windows\system32\cmd.exe

SYN Stealth Scan Timing: About 44.60% done; ETC: 10:39 (0:03:47 remaining)
SYN Stealth Scan Timing: About 48.40% done; ETC: 10:41 (0:04:09 remaining)
SYN Stealth Scan Timing: About 50.95% done; ETC: 10:42 (0:04:33 remaining)
^C
C:\Users\equipo14>nmap -sP 192.168.2.0-255

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-13 10:38 Hora de verano romanc
e
Nmap scan report for 192.168.2.4
Host is up (0.00s latency).
MAC Address: 00:16:B6:84:A0:34 (Cisco-Linksys)
Nmap scan report for 192.168.2.13
Host is up (0.00s latency).
MAC Address: 00:14:85:C3:CC:7F (Giga-Byte)
Nmap scan report for 192.168.2.15
Host is up (0.00s latency).
MAC Address: 00:14:85:C3:CC:64 (Giga-Byte)
Nmap scan report for 192.168.2.20
Host is up (0.00s latency).
MAC Address: 00:80:5A:69:E6:59 (Tulip Computers Internat'l B.U)
Nmap scan report for 192.168.2.21
Host is up (0.063s latency).
MAC Address: 00:27:10:9C:4F:3C (Intel Corporate)
Nmap scan report for 192.168.2.23
Host is up (0.0010s latency).
```

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

```
C:\Windows\system32\cmd.exe
C:\Users\nequipo14>nmap -O -v 192.168.2.189
Starting Nmap 5.51 < http://nmap.org > at 2011-10-13 10:43 Hora de verano romanc
e
Initiating ARP Ping Scan at 10:43
Scanning 192.168.2.189 [1 port]
Completed ARP Ping Scan at 10:43, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:43
Completed Parallel DNS resolution of 1 host. at 10:43, 2.73s elapsed
Initiating SYN Stealth Scan at 10:43
Scanning 192.168.2.189 [1000 ports]
Discovered open port 445/tcp on 192.168.2.189
Discovered open port 1025/tcp on 192.168.2.189
Discovered open port 139/tcp on 192.168.2.189
Discovered open port 135/tcp on 192.168.2.189
Discovered open port 3306/tcp on 192.168.2.189
Discovered open port 8080/tcp on 192.168.2.189
Discovered open port 1036/tcp on 192.168.2.189
Discovered open port 1031/tcp on 192.168.2.189
Discovered open port 1029/tcp on 192.168.2.189
Discovered open port 912/tcp on 192.168.2.189
Discovered open port 1035/tcp on 192.168.2.189
Discovered open port 1026/tcp on 192.168.2.189
Discovered open port 5357/tcp on 192.168.2.189
Completed SYN Stealth Scan at 10:43, 1.28s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.2.189
Nmap scan report for 192.168.2.189
Host is up (0.000024s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
912/tcp    open  apex-mesh
1025/tcp   open  NFS-or-iis
1026/tcp   open  LSR-or-nterm
1029/tcp   open  ns-lsa
1031/tcp   open  iad2
1035/tcp   open  multidropper
1036/tcp   open  nsstp
3306/tcp   open  mysql
5357/tcp   open  wsdapi
8080/tcp   open  http-proxy
MAC Address: 78:E7:D1:82:81:DF (Hewlett Packard)
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS details: Microsoft Windows Vista SP0 - SP2, Server 2008, or Windows 7 Ultimate
Uptime guess: 0.093 days (since Thu Oct 13 08:30:17 2011)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Read data files from: C:\Program Files\Nmap
OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/
Nmap done: 1 IP address (1 host up) scanned in 5.72 seconds
```

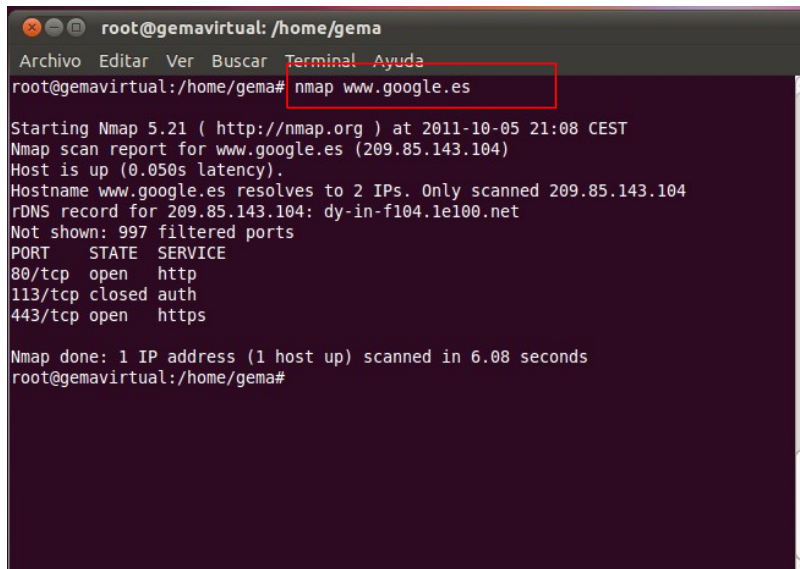
- Por ejemplo para ver si un determinado puerto está abierto ó cerrado (lo haremos con telnet, puerto 23) ponemos el siguiente comando:
`>nmap -p23 192.3.228.239`

```
C:\WINDOWS\system32\cmd.exe
Dirección IP. . . . . : 192.168.86.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada :
Adaptador Ethernet Conexión de área local :
Sufijo de conexión específica DNS :
Dirección IP. . . . . : 195.3.228.239
Máscara de subred . . . . . : 255.255.252.0
Puerta de enlace predeterminada : 195.3.228.1
C:\Documents and Settings\lenne>nmap -p23 195.3.228.239
Starting Nmap 5.51 < http://nmap.org > at 2011-10-14 17:16 Hora estándar romance
Skipping SYN Stealth Scan against 195.3.228.239 because Windows does not support
scanning your own machine (localhost) this way.
Nmap scan report for 195.3.228.239
Host is up.
PORT      STATE SERVICE
23/tcp    unknown telnet
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
C:\Documents and Settings\lenne>
```

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.



```
root@gemavirtual: /home/gema
Archivo Editar Ver Buscar Terminal Ayuda
root@gemavirtual:/home/gema# nmap www.google.es

Starting Nmap 5.21 ( http://nmap.org ) at 2011-10-05 21:08 CEST
Nmap scan report for www.google.es (209.85.143.104)
Host is up (0.050s latency).
Hostname www.google.es resolves to 2 IPs. Only scanned 209.85.143.104
rDNS record for 209.85.143.104: dy-in-f104.1e100.net
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed auth
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 6.08 seconds
root@gemavirtual:/home/gema#
```

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.

```
root@gemavirtual: /home/gema
Archivo Editar Ver Buscar Terminal Ayuda
root@gemavirtual:/home/gema# nmap -sT www.tuenti.com

Starting Nmap 5.21 ( http://nmap.org ) at 2011-10-05 21:15 CEST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 91.57% done; ETC: 21:15 (0:00:00 remaining)
Nmap scan report for www.tuenti.com (95.131.168.181)
Host is up (0.038s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open  https
444/tcp   open  snpp
445/tcp   filtered microsoft-ds
9091/tcp  filtered unknown
9099/tcp  filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 3.40 seconds
root@gemavirtual:/home/gema#
```

- 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.

```
root@gemavirtual: /home/gema
Archivo Editar Ver Buscar Terminal Ayuda
root@gemavirtual:/home/gema# nmap -O 192.168.2.220

Starting Nmap 5.21 ( http://nmap.org ) at 2011-10-06 11:41 CEST
Nmap scan report for 192.168.2.220
Host is up (0.00029s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
912/tcp    open  unknown
5357/tcp   open  unknown
MAC Address: 78:E7:D1:82:81:CE (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS details: Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds
root@gemavirtual:/home/gema#
```

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

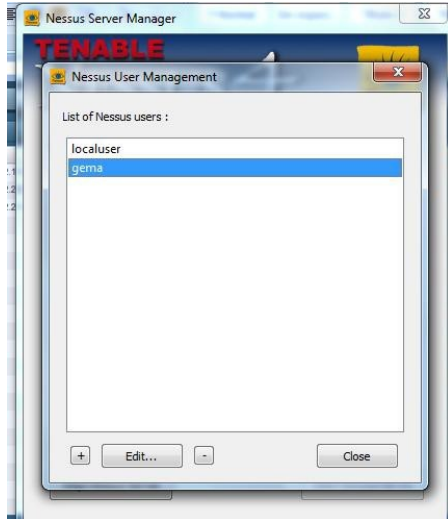
```
root@gemavirtual: /home/gema
Archivo Editar Ver Buscar Terminal Ayuda
OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds
root@gemavirtual:/home/gema# clear

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.**

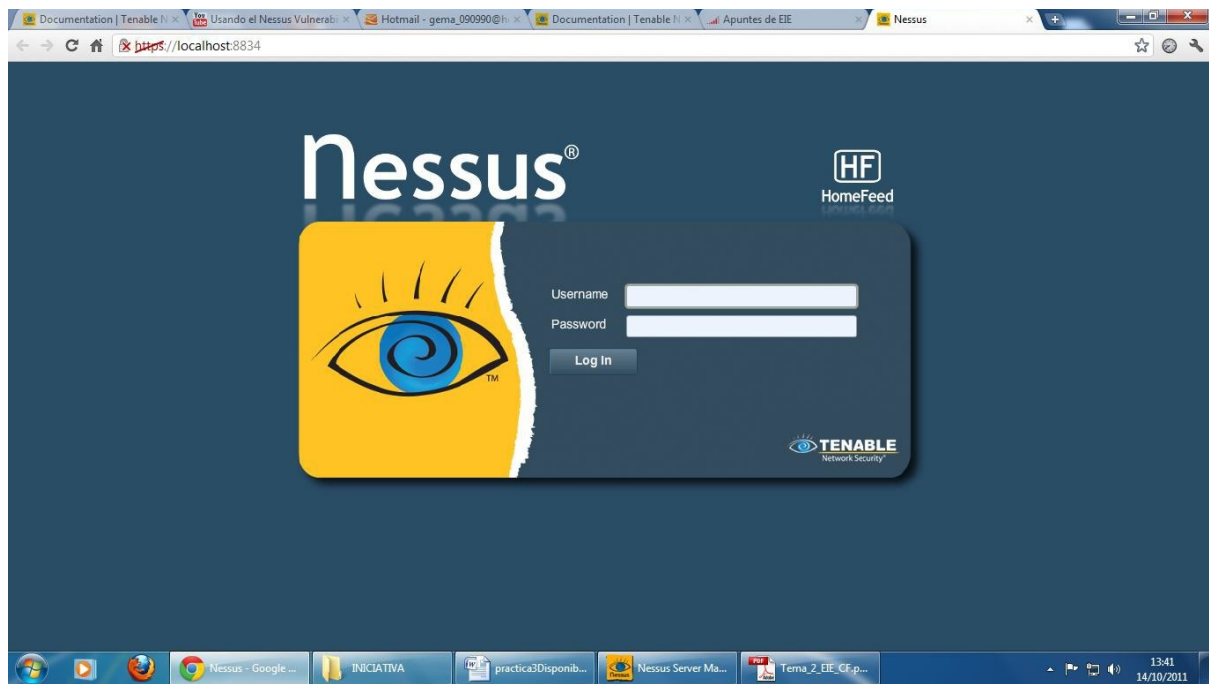
- Una vez instalada la aplicación Nessus e introducida la clave de validación nos creamos un usuario para entrar más tarde a la aplicación.



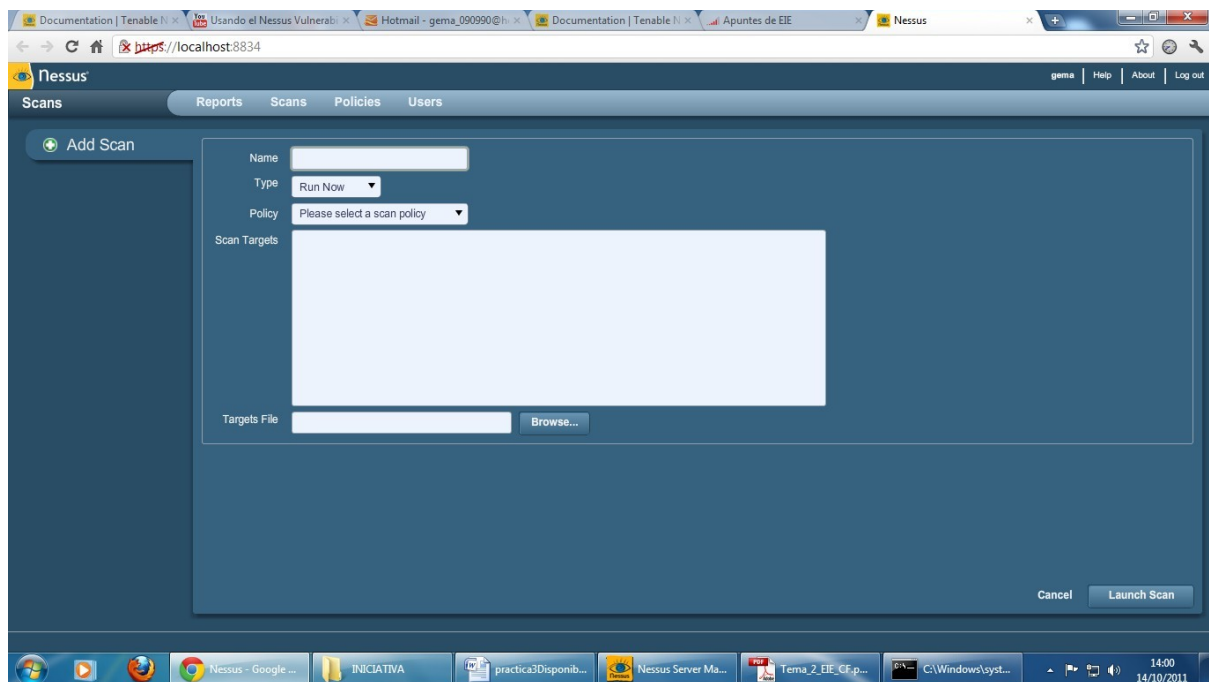
- Cuando hayamos creado el usuario damos a start en el servidor y ejecutamos el cliente, este se ejecutará en el navegador que usemos por defecto.



- 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.

The screenshot shows the Nessus web interface. The 'Reports' tab is active, displaying a summary of a scan for three hosts. The 'Report Info' sidebar on the left shows the report name 'Clase', last update 'Oct 14, 2011 13:53', and status 'Running'. The main table lists the hosts and their scan progress.

Host	Progress	Total	High	Medium	Low	Open Port
192.168.2.148	Complete	29	0	0	24	5
192.168.2.202	Complete	14	0	0	12	2
192.168.2.214	Complete	27	0	0	23	4

- 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.

The screenshot shows the Nessus web interface with a detailed view of the scan results for host 192.168.2.148. The 'Report Info' sidebar on the left shows the report name 'Clase', last update 'Oct 14, 2011 13:53', and status 'Running'. The main table lists the ports, protocols, and services scanned.

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	doe-rpc	1	0	0	1	0
1026	tcp	doe-rpc	1	0	0	1	0
1027	tcp	doe-rpc	1	0	0	1	0
1028	tcp	doe-rpc	1	0	0	1	0
1029	tcp	doe-rpc	1	0	0	1	0
3306	tcp	mysql	2	0	0	1	1

The screenshot shows the Nessus Reports page for host 192.168.2.202. The interface includes a sidebar with 'Report Info' and 'Hosts' (192.168.2.148, 192.168.2.202, 192.168.2.214). The main table displays scan results for the selected host.

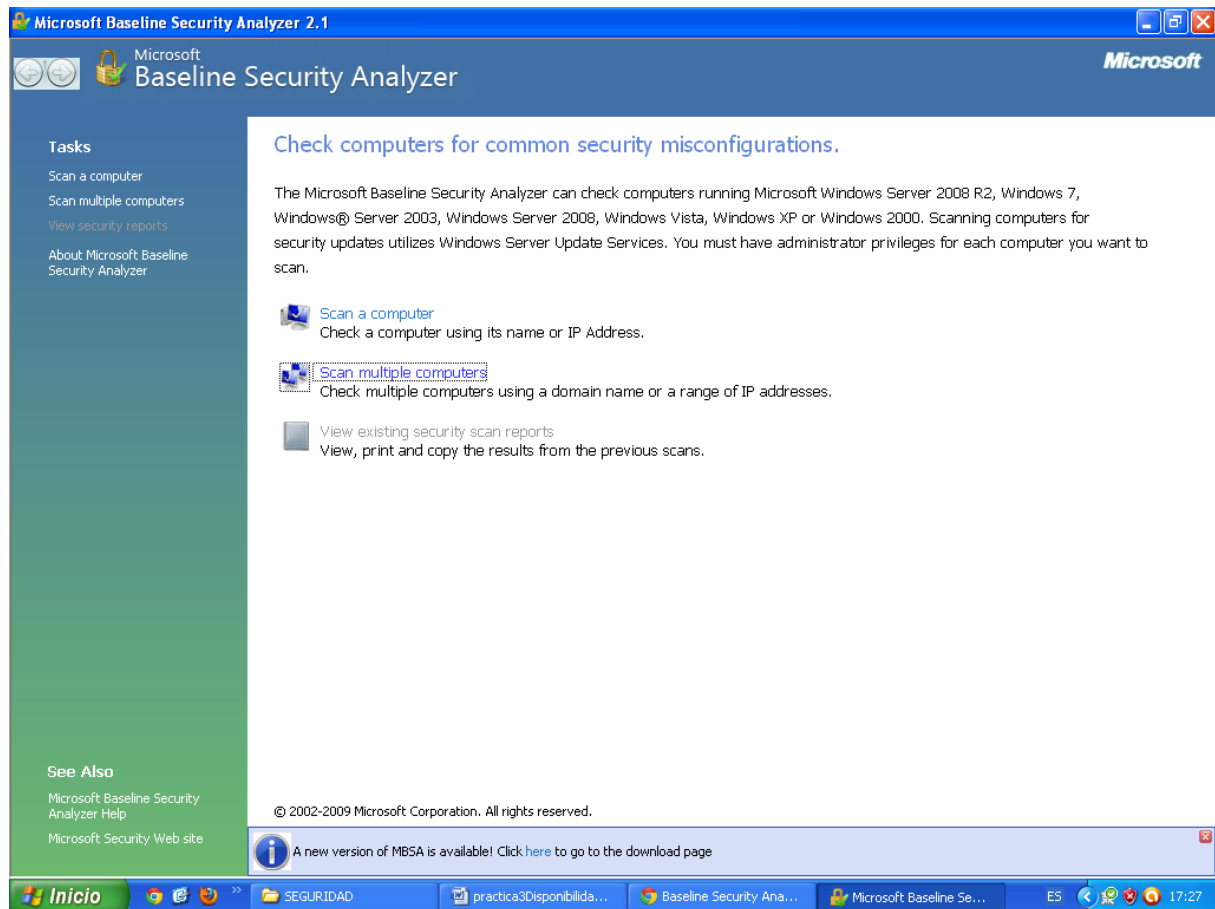
Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	6	0	0	6	0
0	udp	general	1	0	0	1	0
137	udp	netbios-ns	2	0	0	2	0
912	tcp	vmware_auth	3	0	0	2	1
3306	tcp	mysql	2	0	0	1	1

The screenshot shows the Nessus Reports page for host 192.168.2.214. The interface includes a sidebar with 'Report Info' and 'Hosts' (192.168.2.148, 192.168.2.202, 192.168.2.214). The main table displays scan results for the selected host.

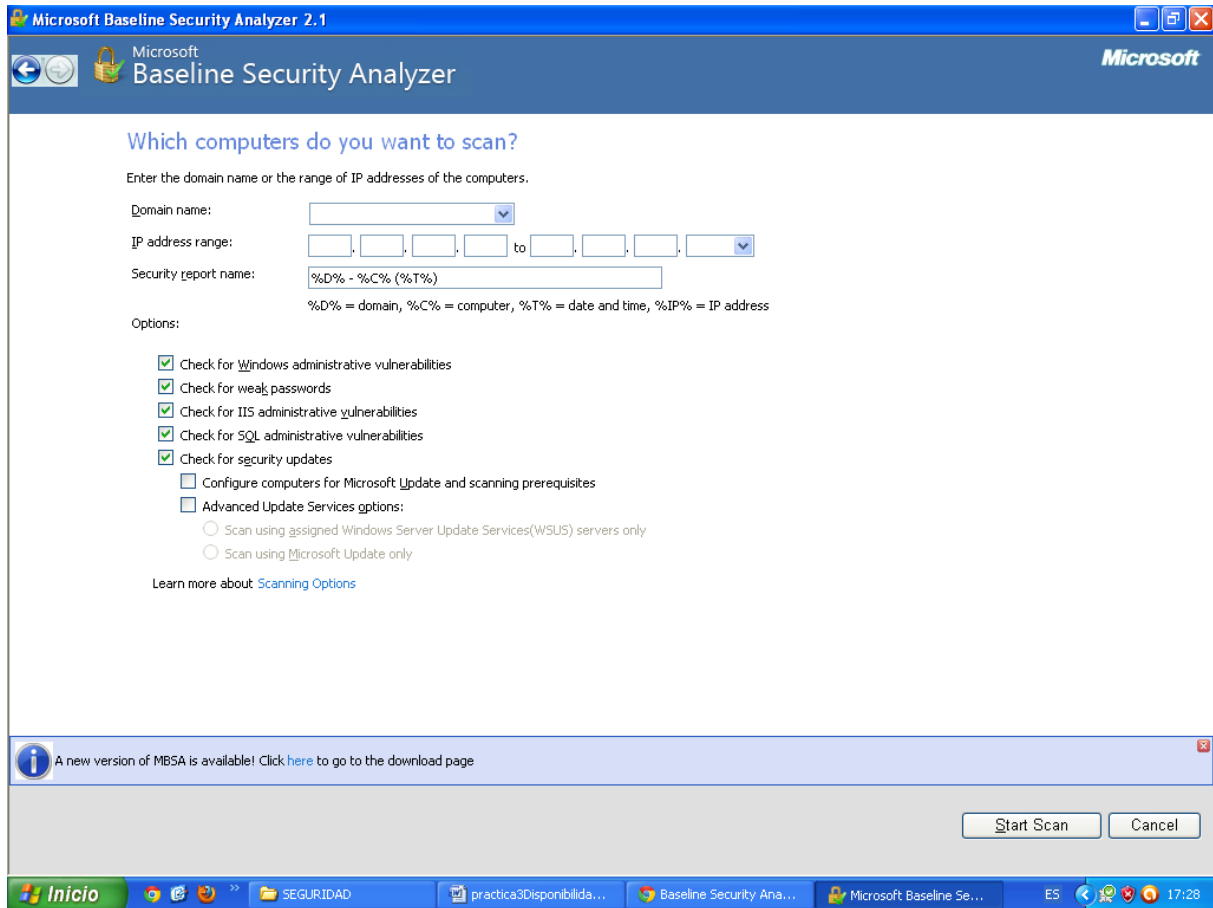
Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	6	0	0	6	0
0	udp	general	1	0	0	1	0
135	tcp	epmap	2	0	0	1	1
139	tcp	smb	2	0	0	1	1
445	tcp	cifs	8	0	0	7	1
912	tcp	vmware_auth	3	0	0	2	1
1025	tcp	dce-rpc	1	0	0	1	0
1026	tcp	dce-rpc	1	0	0	1	0
1028	tcp	dce-rpc	1	0	0	1	0
1029	tcp	dce-rpc	1	0	0	1	0
1030	tcp	dce-rpc	1	0	0	1	0

3. COMPROBAR DISPONIBILIDAD CON MBSA.

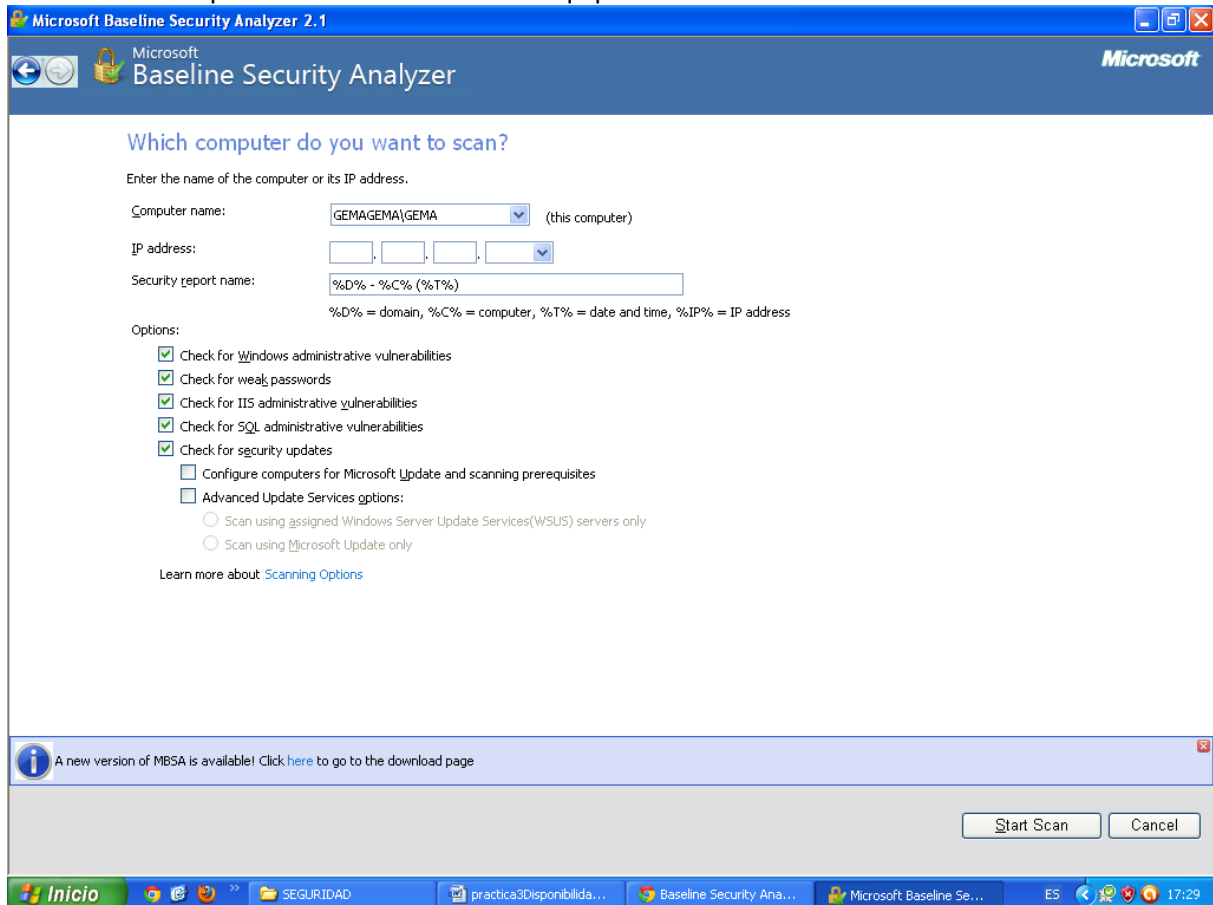
- Una vez descargado e instalado MBSA lo ejecutamos y podemos ver lo siguiente, podemos elegir hacer un escáner de nuestro equipo o de varios equipos.



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



➤ Vamos a proceder a analizar nuestro equipo.



The screenshot displays the Microsoft Baseline Security Analyzer (MBSA) 2.1 interface. The title bar reads "Microsoft Baseline Security Analyzer 2.1". The main window shows a report titled "Report Details for GEMAGEMA - GEMA (2011-10-14 17:36:49)". Below the title, a security assessment is shown with a yellow warning icon and the text "Security assessment: Potential Risk (One or more non-critical checks failed.)".

Metadata information is listed:

- 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

A "Sort Order" dropdown menu is set to "Score (best first)".

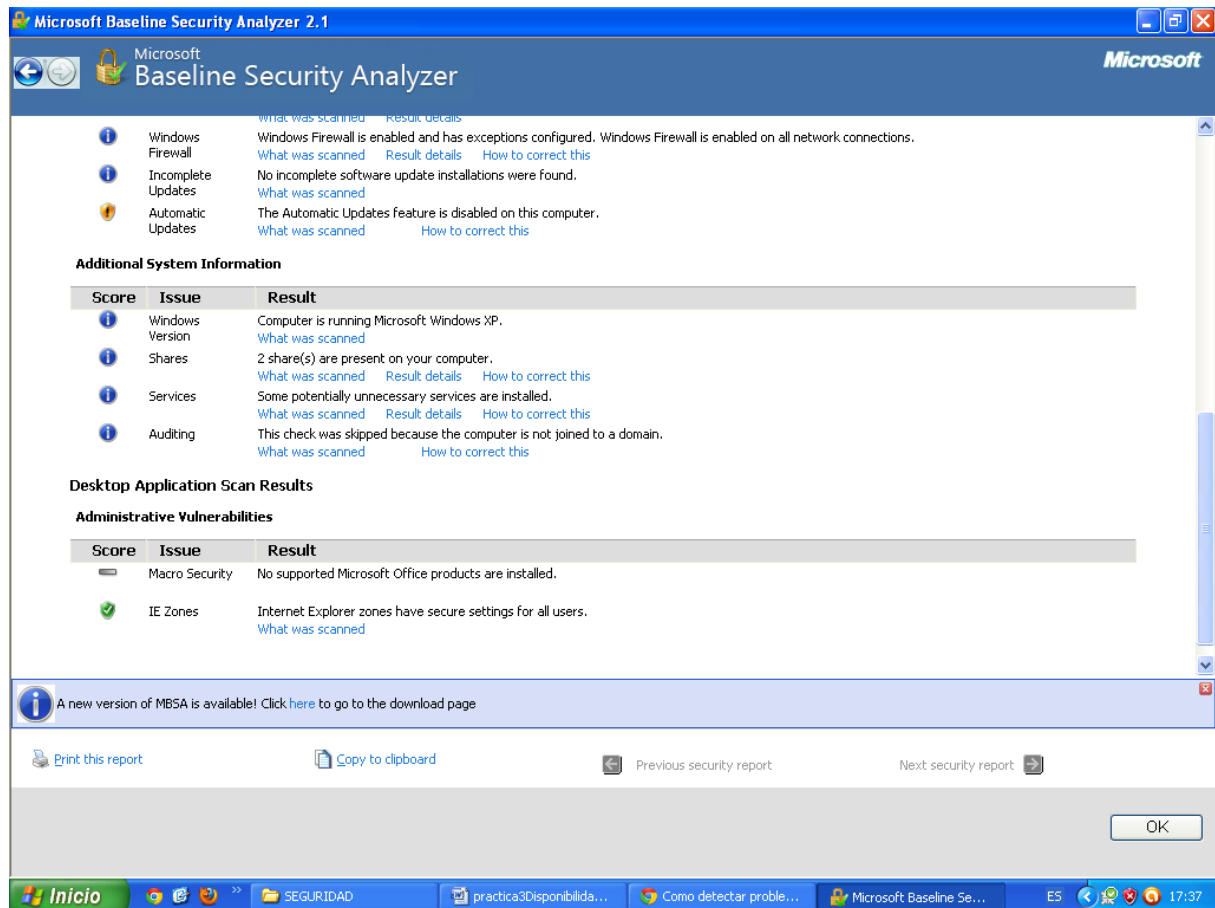
The "Windows Scan Results" section is titled "Administrative Vulnerabilities". It contains a table with three columns: "Score", "Issue", and "Result".

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

At the bottom of the report area, a blue banner states: "A new version of MBSA is available! Click [here](#) to go to the download page".

Below the banner are buttons for "Print this report", "Copy to clipboard", "Previous security report", and "Next security report". An "OK" button is located at the bottom right of the report area.

The Windows taskbar at the bottom shows the "Inicio" button, several open applications including "SEGURIDAD", "practica3Disponibila...", "Como detectar proble...", and "Microsoft Baseline Se...", and the system clock showing "ES" and "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.