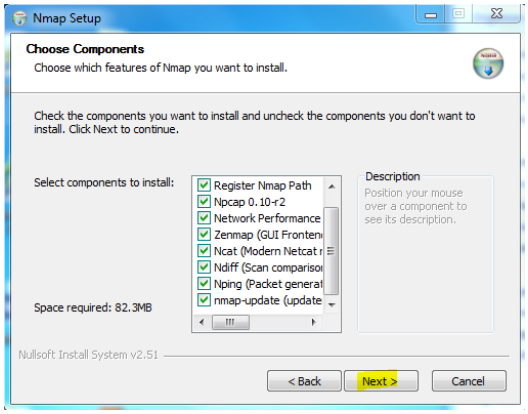
Práctica Disponibilidad

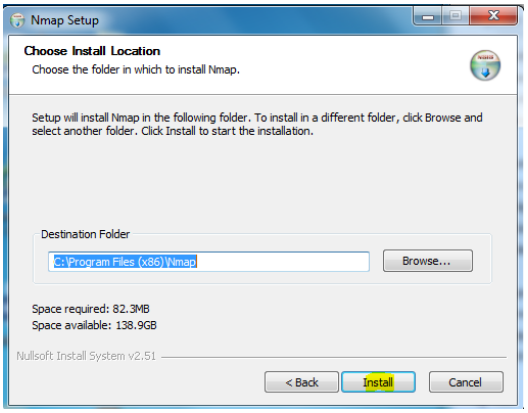
1-COMPROBAR DISPONIBILIDAD CON NMAP

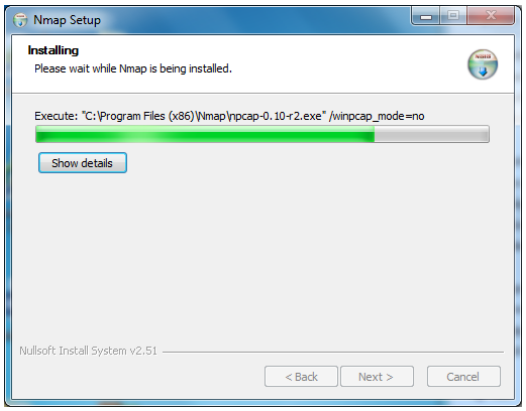
Nmap (“Network Mapper ") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Cuando ejecutamos comandos se lista una tabla. Dicha tabla lista el número de puerto y protocolo, nombre del servicio, y el Estado. El estado puede ser abierto, filtrado , cerrados , o sin 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

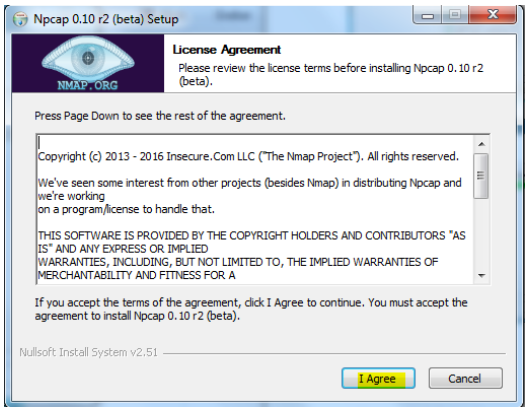
1.1DISPONIBILIDAD EN WINDOWS.

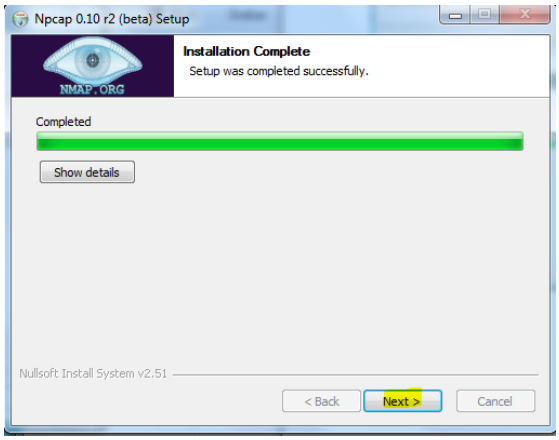
- Vamos a buscar vulnerabilidades en los puertos con el programa nmap.
- Para instalar la aplicación la descargamos y ejecutamos el instalador y nos saldrá un asistente.

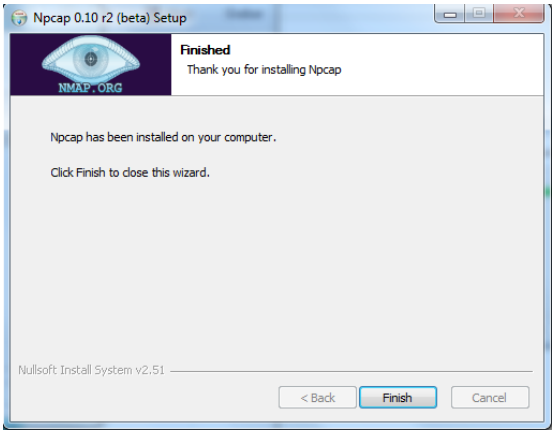




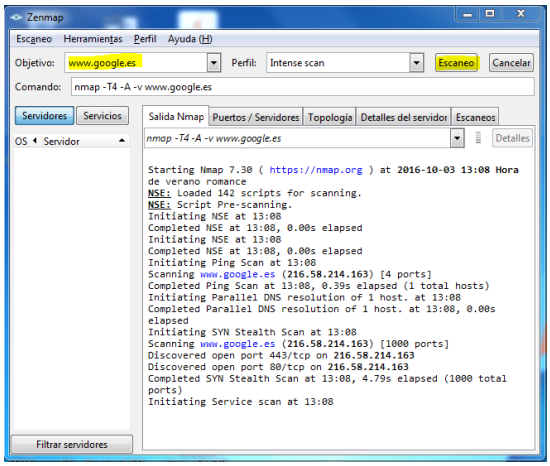


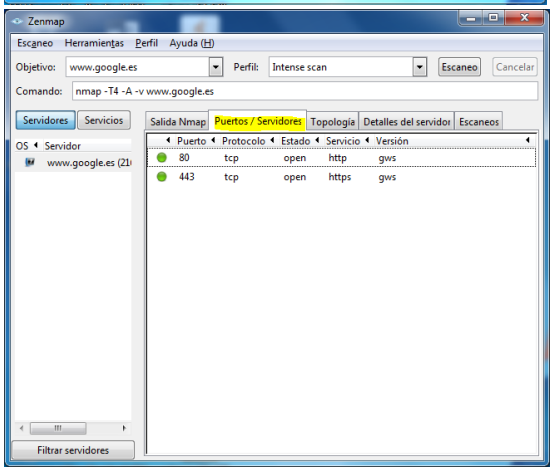


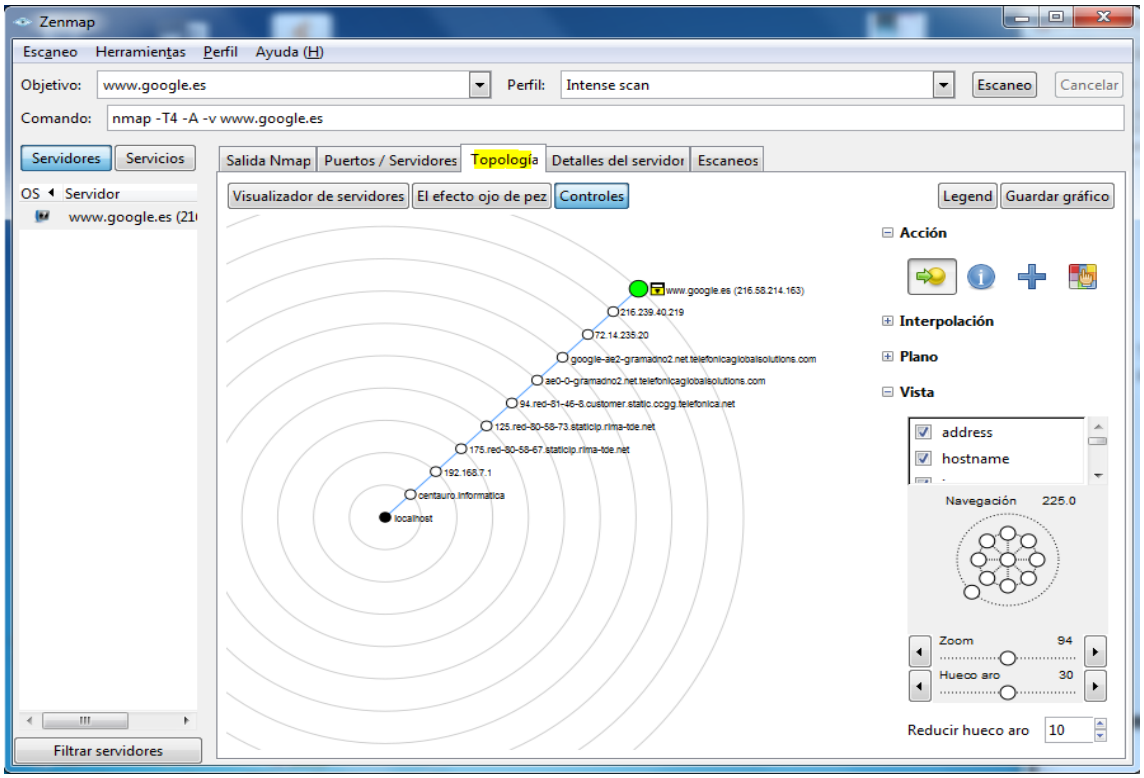




- Una vez instalado el programa lo ejecutamos y procedemos por ejemplo a realizar un escáner de los puertos de www.google.es







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

```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\windows\system32>nmap www.google.es

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-03 13:19 Hora de verano roman
ce
Nmap scan report for www.google.es (172.217.23.35)
Host is up (0.026s latency).
rDNS record for 172.217.23.35: lhr35s02-in-f3.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds
```

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

```
C:\windows\system32>nmap -v scanme.nmap.org /192.168.4.104

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-03 13:22 Hora de verano roman
ce
Unable to split netmask from target expression: "/192.168.4.104"
Initiating Ping Scan at 13:22
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 13:22, 0.56s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:22
Completed Parallel DNS resolution of 1 host. at 13:22, 0.00s elapsed
Initiating SYN Stealth Scan at 13:22
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed SYN Stealth Scan at 13:22, 3.77s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
161/tcp   filtered snmp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.43 seconds
           Raw packets sent: 1005 (44.196KB) | Rcvd: 1007 (40.312KB)
```

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

```
C:\windows\system32>nmap -sP 192.168.4.104

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-03 13:24 Hora de verano roman
ce
Nmap scan report for 192.168.4.104
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 14.26 seconds
```

```
C:\windows\system32>nmap -sP 192.168.4.104-255

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-03 13:26 Hora de verano roman
ce
Nmap scan report for 192.168.4.104
Host is up.
Nmap scan report for 192.168.4.105
Host is up (0.00s latency).
MAC Address: A0:D3:C1:06:AC:59 (Hewlett Packard)
Nmap scan report for 192.168.4.106
Host is up (0.00s latency).
MAC Address: A0:48:1C:8F:67:5D (Hewlett Packard)
Nmap scan report for 192.168.4.108
Host is up (0.00s latency).
MAC Address: A0:D3:C1:06:AD:2E (Hewlett Packard)
Nmap scan report for 192.168.4.109
Host is up (0.016s latency).
MAC Address: A0:D3:C1:0F:8E:BA (Hewlett Packard)
Nmap scan report for 192.168.4.110
Host is up (0.016s latency).
MAC Address: A0:D3:C1:06:DF:AF (Hewlett Packard)
Nmap scan report for 192.168.4.111
Host is up (0.016s latency).
MAC Address: A0:D3:C1:0F:8E:81 (Hewlett Packard)
Nmap scan report for 192.168.4.112
Host is up (0.016s latency).
MAC Address: A0:D3:C1:0F:8D:D4 (Hewlett Packard)
Nmap scan report for 192.168.4.113
Host is up (0.016s latency).
MAC Address: A0:D3:C1:06:E0:F8 (Hewlett Packard)
Nmap scan report for 192.168.4.114
Host is up (0.016s latency).
MAC Address: A0:D3:C1:0F:8D:BF (Hewlett Packard)
Nmap scan report for 192.168.4.115
Host is up (0.016s latency).
MAC Address: A0:D3:C1:06:E0:E9 (Hewlett Packard)
Nmap scan report for 192.168.4.116
Host is up (0.016s latency).
MAC Address: A0:D3:C1:06:DD:74 (Hewlett Packard)
Nmap scan report for 192.168.4.125
Host is up (0.00s latency).
MAC Address: 00:01:E6:50:37:DA (Hewlett Packard)
Nmap scan report for 192.168.4.135
Host is up (0.00s latency).
MAC Address: 00:0C:29:6F:07:36 (VMware)
Nmap scan report for 192.168.4.209
Host is up (0.00s latency).
MAC Address: 00:0C:29:4C:BC:CA (VMware)
Nmap done: 152 IP addresses (15 hosts up) scanned in 41.67 seconds
```

Poniendo -255 al final nos da más información

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

```
C:\windows\system32>nmap -sP 192.168.4.104

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-03 13:27 Hora de verano roman
ce
Nmap scan report for 192.168.4.104
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 14.24 seconds

C:\windows\system32>nmap -p23 192.168.4.104

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-03 13:30 Hora de verano roman
ce
Nmap scan report for 192.168.4.104
Host is up (0.00s latency).
PORT   STATE  SERVICE
23/tcp closed telnet

Nmap done: 1 IP address (1 host up) scanned in 14.44 seconds
```

1.2 DISPONIBILIDAD EN LINUX.

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

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
rafael@Debian04:~$ su
Contraseña:
root@Debian04:/home/rafael# apt-get install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
nmap ya está en su versión más reciente.
```

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

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@debian:/home/rafael# apt-get install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
nmap ya está en su versión más reciente.
fijado nmap como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
root@debian:/home/rafael# nmap www.google.es

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-04 18:32 CEST
Nmap scan report for www.google.es (216.58.214.67)
Host is up (0.018s latency).
rDNS record for 216.58.214.67: fra15s10-in-f67.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 90.44 seconds
```

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.facebook.com y nos muestra un barrido de puertos por tcp.

```
root@debian:/home/rafael# nmap -sT www.facebook.com

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-04 18:45 CEST
Nmap scan report for www.facebook.com (31.13.83.36)
Host is up (0.011s latency).
rDNS record for 31.13.83.36: edge-star-mini-shv-01-mad1.facebook.com
Not shown: 997 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
843/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 34.21 seconds
```

- 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@debian:/home/rafael# nmap -O 192.168.1.135

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-04 18:49 CEST
Nmap scan report for 192.168.1.135
Host is up (0.38s latency).
Not shown: 985 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
514/tcp   filtered shell
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
2869/tcp  open     icslap
3306/tcp  open     mysql
5357/tcp  open     wsdapi
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49167/tcp open     unknown
Device type: general purpose
Running: Microsoft Windows 7|XP
OS CPE: cpe:/o:microsoft:windows_7:::enterprise cpe:/o:microsoft:windows_xp::sp3
```

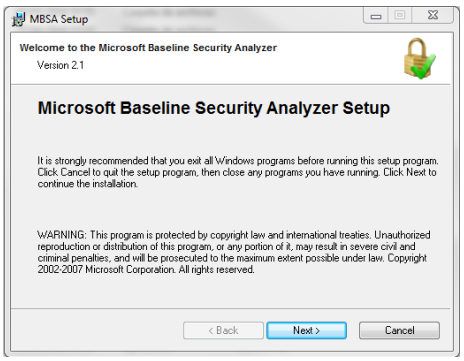
¬ Con el comando del siguiente ejemplo podemos ver los host que están disponibles dentro de la red que le indiquemos:

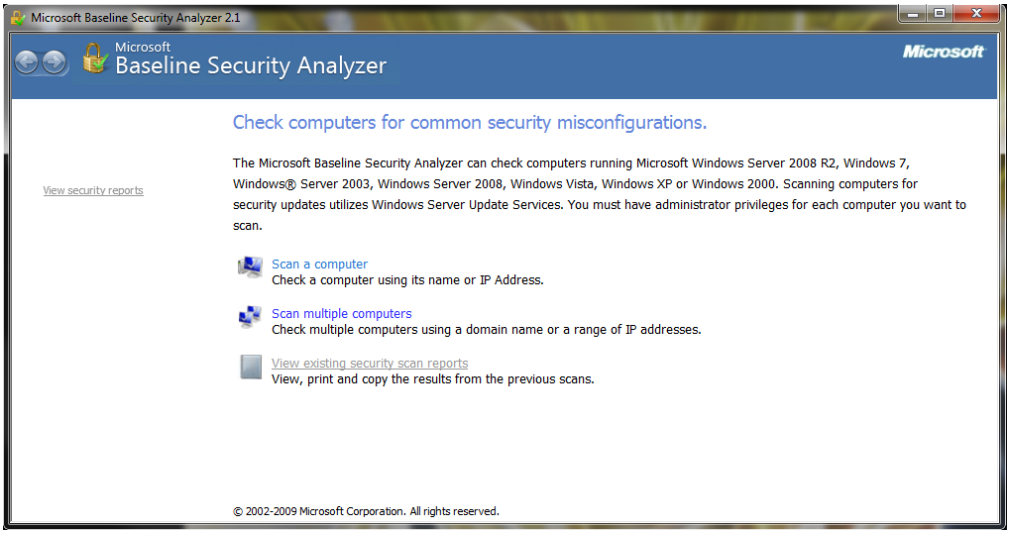
```
root@debian:/home/rafael# nmap -sP 192.168.1.0-255

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-04 19:06 CEST
Nmap scan report for 192.168.1.0
Host is up (0.00023s latency).
Nmap scan report for 192.168.1.1
Host is up (0.0053s latency).
Nmap scan report for 192.168.1.2
Host is up (0.17s latency).
Nmap scan report for 192.168.1.8
Host is up (0.18s latency).
Nmap scan report for 192.168.1.9
Host is up (0.48s latency).
Nmap scan report for 192.168.1.11
Host is up (0.00022s latency).
Nmap scan report for 192.168.1.12
```

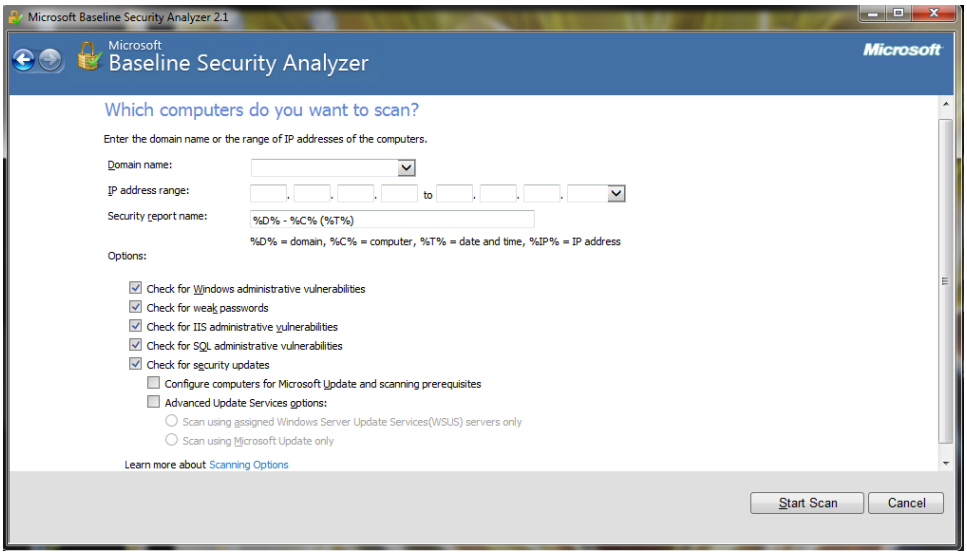
3. COMPROBAR DISPONIBILIDAD CON MBSA.

¬ 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.

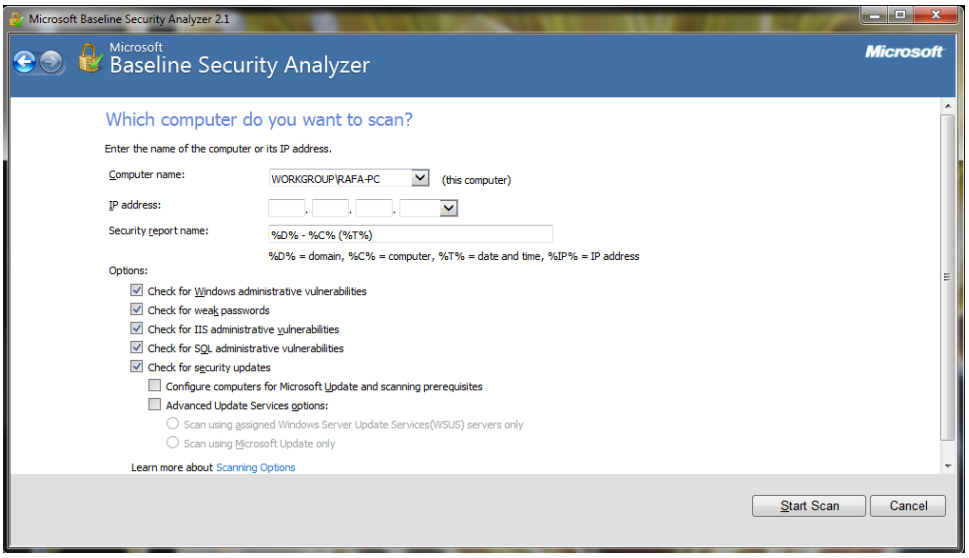


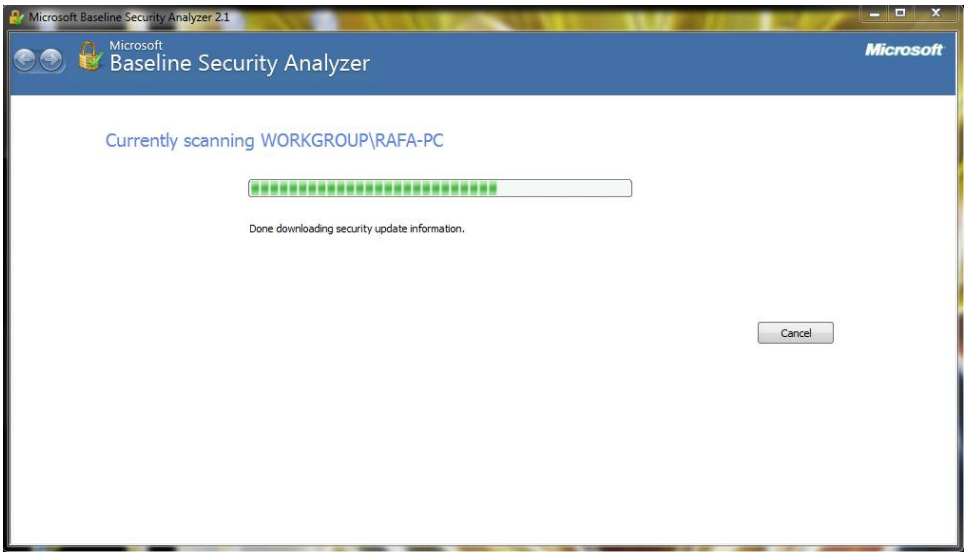


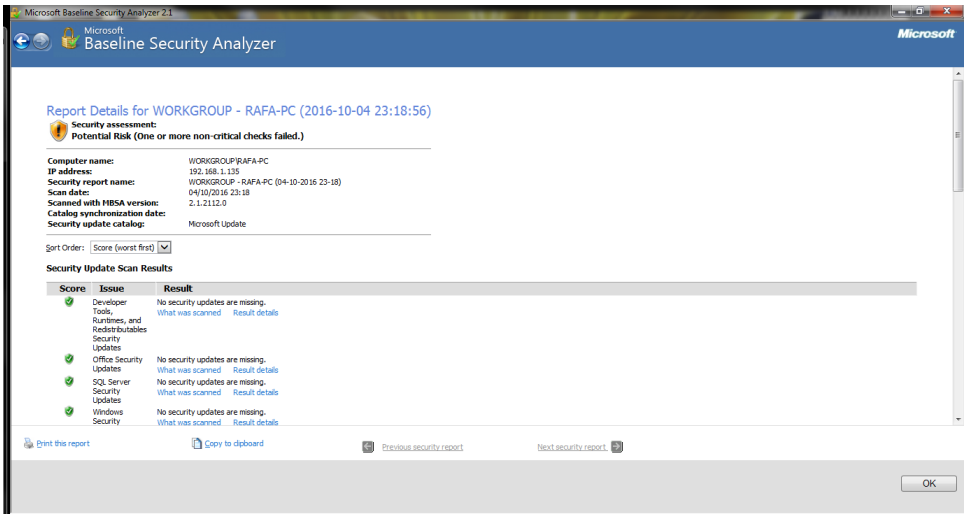
En la siguiente pantalla tenemos las opciones para analizar varios equipos.



Vamos a proceder a analizar nuestro equipo.






Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft
Report Details for WORKGROUP - RAFA-PC (2016-10-04 23:18:56)
Security assessment:
Potential Risk (One or more non-critical checks failed.)
Computer name: WORKGROUP\RAFA-PC
IP address: 192.168.1.135
Security report name: WORKGROUP - RAFA-PC (04-10-2016 23-18)
Scan date: 04/10/2016 23:18
Scanned with MBSA version: 2.1.2112.0
Catalog synchronization date:
Security update catalog: Microsoft Update
Sort Order: Score (worst first)
Security Update Scan Results
Score
Issue
Result
Developer Tools, Runtimes, and Redistributables Security Updates
No security updates are missing.
What was scanned
Result details
Office Security Updates
No security updates are missing.
What was scanned
Result details
SQL Server Security Updates
No security updates are missing.
What was scanned
Result details
Windows Security
No security updates are missing.
What was scanned
Result details
Print this report
Copy to clipboard
Previous security report
Next security report
OK