

Actividad práctica numero 1:

Formato: Individual.

Asignatura: Seguridad en Sistemas Computacionales

Código: SSC 5501

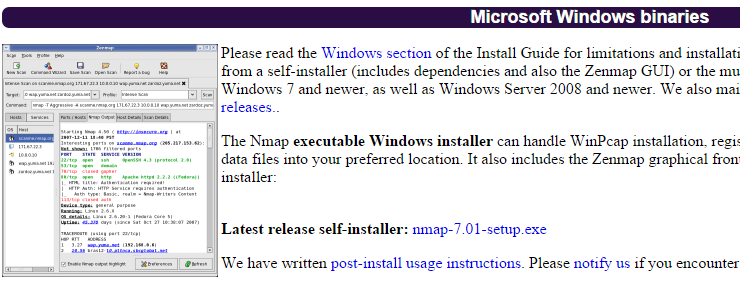
**Titulo: Aplicación NMAP**

1.- Inicie su computador en Windows 7.

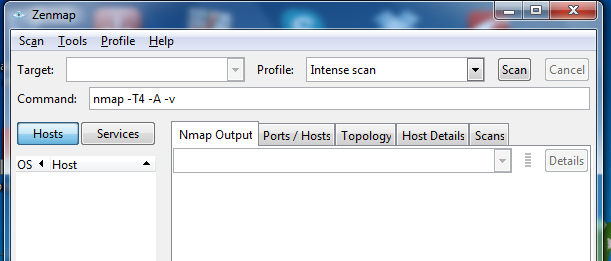
2.- Conéctese con el browser a la siguiente dirección:

<https://nmap.org/download.html>

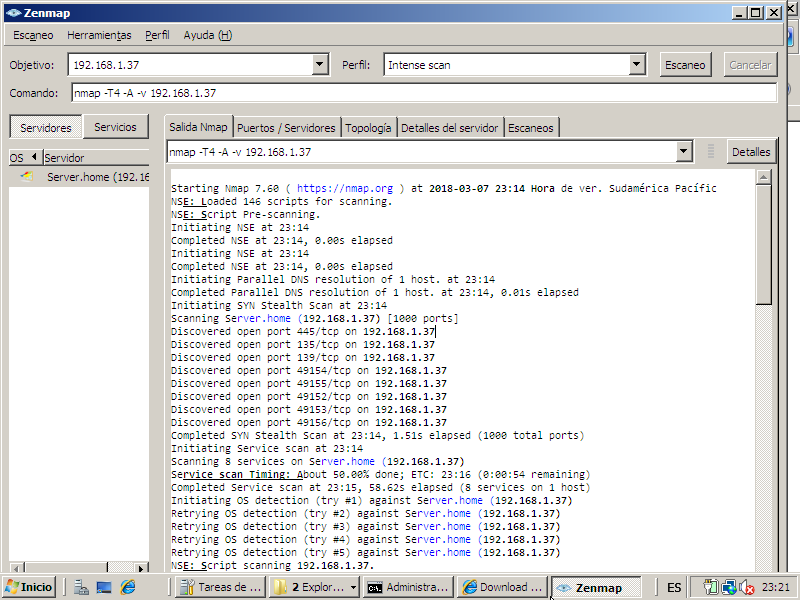
3.- Baje e instale la aplicación NMAP en su computador

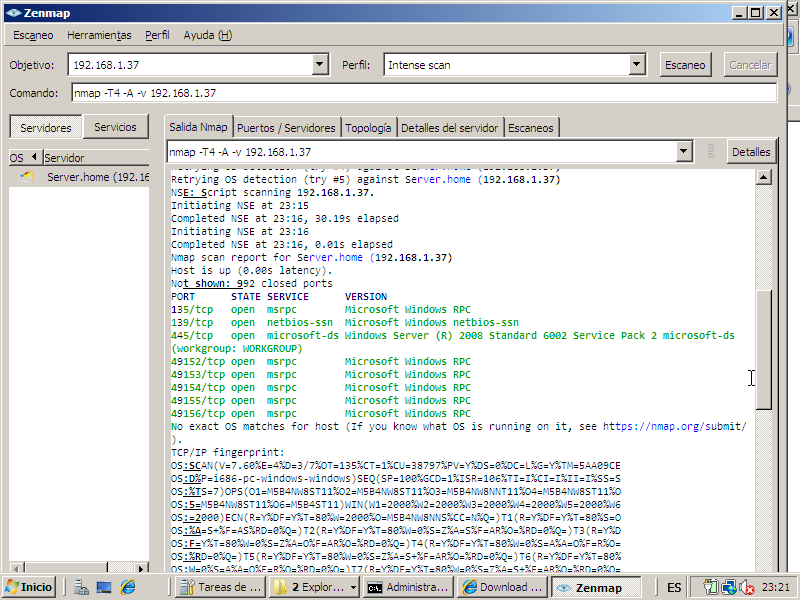


4.- Una vez instalada, realice los siguientes ejercicios:

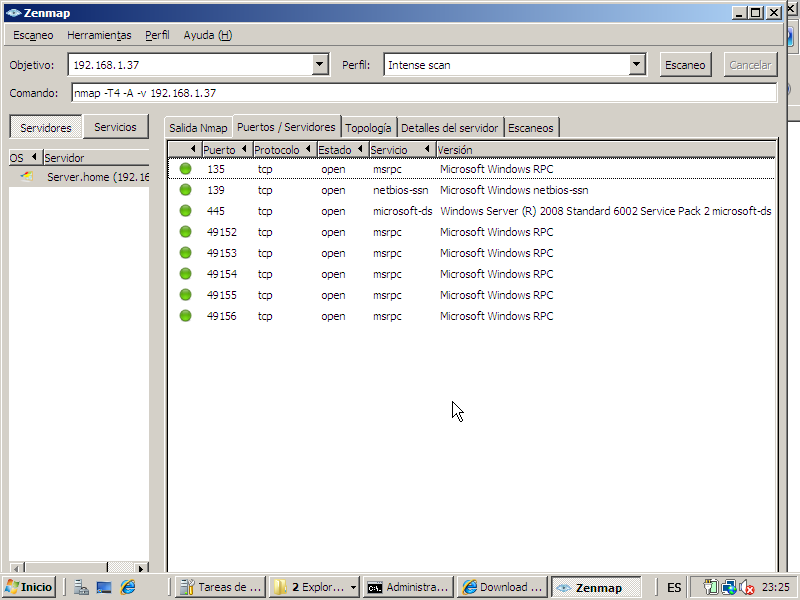


1. Levante el servidor Windows 2008 de su máquina virtual y realice un “Intensive Scan” a la dirección IP del servidor, la interfaz de red de la maquina virtual debe estar en modo puente, comente el resultado y anote el comando ejecutado por la herramienta. ¿Qué información entrego?

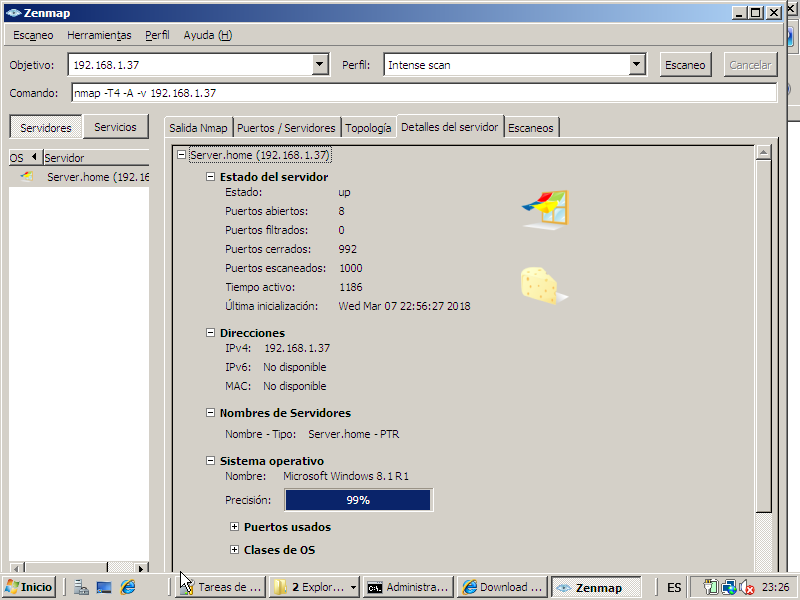




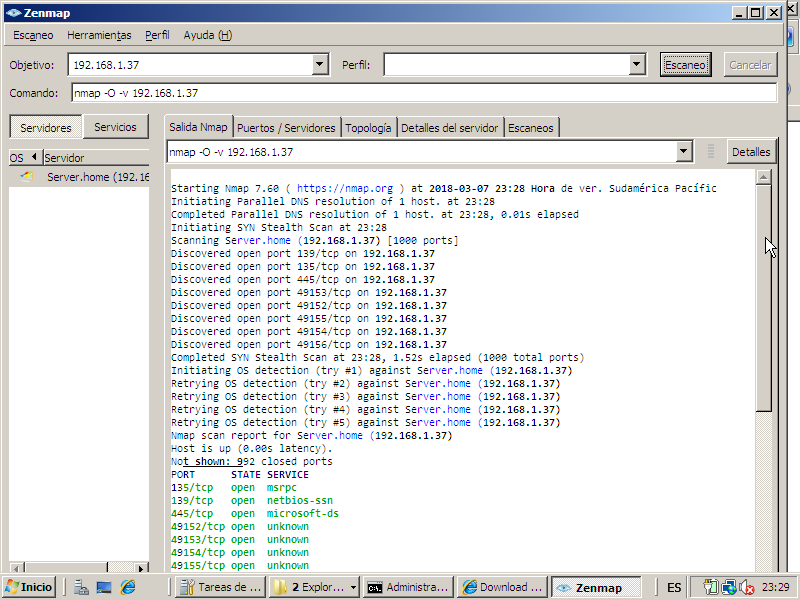
1. Revise la opción “Port/hosts” y describa la información encontrada.

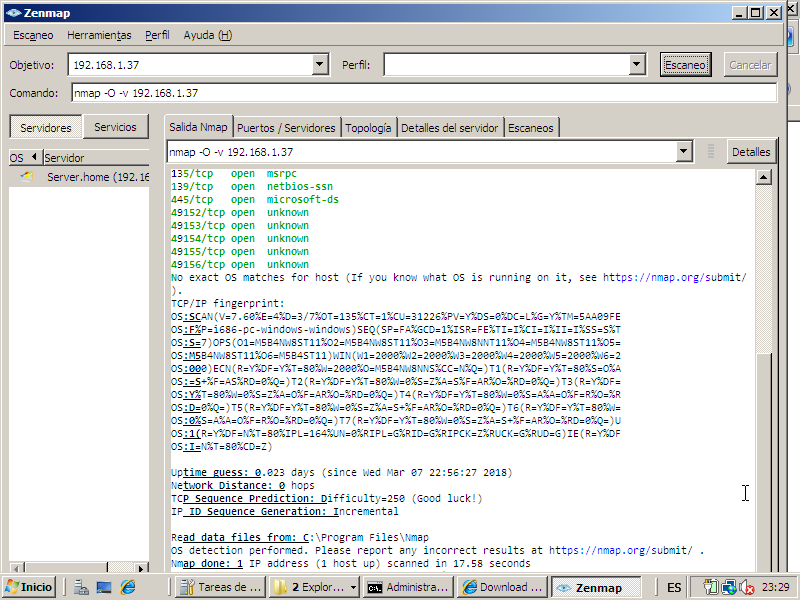


1. Vaya a la opción “Host details” y describa la información que ahí aparece



1. Escriba el siguiente comando en la línea “Command”: nmap –O –v *direccionIP* y ejecute Scan, ¿Qué resultado obtiene?





1. Conéctese al siguiente link

<http://www.linux.com/learn/tutorials/290879-beginners-guide-to-nmap>

y realice lo siguiente:

* Descubra como realizar un Scan a una red completa y descubra las direcciones IP de los computadores de laboratorio que están activas

### Múltiples hosts

Puede escanear más de un host a la vez usando nmap. Si usa direcciones IP, puede especificar un rango como 10.0.0.1-6 o un rango como 10.0.0.0/24. El 10.0.0.1-6 escanearía los hosts 10.0.0.1, 10.0.0.2, 10.0.0.3 a 10.0.0.6. El uso de la notación / 24 escaneará toda la gama de hosts de 10.0.0.0 a 10.0.0.255. Por ejemplo, para escanear 10.0.0.1 a 10.0.0.42 para saber qué sistema operativo podrían estar usando, usaría **nmap -O 10.0.0.1-42.**

* Verificación de puertos abiertos

Si le das a **Nmap** ninguna opción y solo lo apunta a un host determinado, buscará puertos abiertos e informará sobre aquellos que están abiertos y qué servicio se está ejecutando en ellos.

-Busque en el siguiente link las diferentes técnicas de Scan y descríbalos brevemente:

<http://nmap.org/book/man-port-scanning-techniques.html>

* + -sS (TCP SYN scan): El escaneo SYN es la opción de escaneo por defecto y más popular por buenas razones. Se puede realizar rápidamente, escaneando miles de puertos por segundo en una red rápida que no se ve obstaculizada por firewalls restrictivos.
  + -sT (Exploración de conexión TCP): El escaneo de conexión TCP es el tipo de escaneo TCP predeterminado cuando el escaneo SYN no es una opción. Este es el caso cuando un usuario no tiene privilegios de paquete sin procesar.
  + -sU (Escaneos UDP): Mientras que los servicios más populares en Internet se ejecutan sobre el protocolo TCP, los servicios [UDP](http://www.rfc-editor.org/rfc/rfc768.txt) se despliegan ampliamente. DNS, SNMP y DHCP (puertos registrados 53, 161/162 y 67/68) son tres de los más comunes
  + -sY (SCTP INIT scan): [SCTP](http://www.rfc-editor.org/rfc/rfc4960.txt) es una alternativa relativamente nueva a los protocolos TCP y UDP, que combina la mayoría de las características de TCP y UDP, y también agrega nuevas características como multi-homing y multi-streaming.
  + -sN; -sF; -sX(TCP NULL, FIN y escaneos de Navidad): Estos tres tipos de escaneo (incluso más son posibles con la --scanflagsopción descrita en la siguiente sección) explotan una laguna sutil en el [TCP RFC](http://www.rfc-editor.org/rfc/rfc793.txt) para diferenciar entre openy los closedpuertos.
  + -sA (TCP ACK scan): Este escaneo es diferente a los otros discutidos hasta el momento, ya que nunca determina open(o incluso open|filtered) los puertos. Se utiliza para mapear los conjuntos de reglas de firewall, determinar si son con estado o no y qué puertos se filtran.
  + -sW (Escaneo de ventana TCP): El escaneo de ventanas es exactamente igual que el escaneo de ACK, excepto que aprovecha un detalle de implementación de ciertos sistemas para diferenciar los puertos abiertos de los cerrados, en lugar de imprimir siempre unfilteredcuando se devuelve un RST.
  + -sM (TCP Maimon scan): El escaneo de Maimon lleva el nombre de su descubridor, Uriel Maimon. Describió la técnica en el número 49 de la revista *Phrack* (noviembre de 1996). Nmap, que incluía esta técnica, se publicó dos números más tarde.
  + --scanflags (Análisis TCP personalizado): Los usuarios verdaderamente avanzados de Nmap no necesitan limitarse a los tipos de escaneos enlatados que se ofrecen. La --scanflagsopción le permite diseñar su propia exploración especificando banderas TCP arbitrarias.
  + -sZ (SCTP COOKIE ECHO scan): SCTP COOKIE ECHO scan es una exploración SCTP más avanzada. Aprovecha el hecho de que las implementaciones de SCTP deberían colocar silenciosamente paquetes que contengan COOKIE ECHO en puertos abiertos, pero envían un ABORTO si el puerto está cerrado.
  + -sI *<zombie host>*[:*<probeport>*] (exploración inactiva): Este método de exploración avanzada permite un escaneo de puerto TCP verdaderamente ciego del objetivo (lo que significa que no se envían paquetes al destino desde su dirección IP real).
  + -sO (Escaneo de protocolo IP): La exploración del protocolo IP le permite determinar qué protocolos IP (TCP, ICMP, IGMP, etc.) son compatibles con las máquinas de destino. Esto técnicamente no es un escaneo de puertos, ya que pasa cíclicamente a través de números de protocolo IP en lugar de números de puerto TCP o UDP.
  + -b *<FTP relay host>* (Escaneo de rebote de FTP): Una característica interesante del protocolo FTP ( [RFC 959](http://www.rfc-editor.org/rfc/rfc959.txt) ) es el soporte para las llamadas conexiones FTP proxy. Esto permite que un usuario se conecte a un servidor FTP y luego solicite que los archivos se envíen a un servidor de terceros.