NMAP 6: Listado de comandos

ESPECIFICACIÓN DE OBJETIVOS			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-iL <fich>	Objetivos en fichero	Se pasan los objetivos en un fichero, cada uno en una línea[1].	
-iR <num>	Objetivos aleatorios	Elige los objetivos de forma aleatoria.	
--exclude <hosts>	Lista exclusión	Indica equipos a excluir del análisis.	
--excludefile <fich>	Fichero exclusión	Se pasan en un fichero los equipos a excluir del análisis[1].	

DESCUBRIMIENTO DE EQUIPOS			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-Pn	No ping	No realiza ninguna técnica de descubrimiento. Pasa directamente al análisis de puertos.	Considera a todos los objetivos como aptos para un análisis de puertos.
-sL	List Scan	Sólo lista equipos. No envía ningún paquete a los objetivos.	Hace resolución inversa DNS.
-sn	Ping Sweep	Implica un *-PE* + *-PA 80* + *-PS 443*. Si misma subred, también *-PR*. No hace análisis de puertos posterior.	Si usuario sin privilegios: *connect()* a 80 y 443. Hace resolución inversa DNS.
-PR	Ping ARP	Sólo para objetivos de nuestra red local (activo por defecto). Envía un ARP Request.	*Host Up:* Se recibe un ARP Reply. *Host Down*: Expira el *timeout*.
-PS<ports>	Ping TCP SYN	Envía un SYN, por defecto al puerto 80. Acepta lista de puertos. Se ejecuta este si usuario sin privilegios.	*Host Up*: Se recibe un SYN/ACK o RST. *Host Down:* Expira el *timeout*.
-PA<ports>	Ping TCP ACK	Envía un ACK vacío, por defecto al puerto 80. Acepta lista de puertos. Traspasa cortafuegos sin estado.	*Host Up:* Se recibe un RST. *Host Down:* Expira el *timeout*.
-PU<ports>	Ping UDP	Envía un UDP vacío al puerto 31338. Acepta lista de puertos. Traspasa cortafuegos que sólo filtran TCP.	*Host Up:* Se recibe un ICMP port unreachable. *Host Down:* Otros ICMPs, expira el *timeout*.
-PY <ports>	Ping SCTP	Envía un paquete SCTP INIT al puerto 80. Acepta lista de puertos. Solo usuarios privilegiados.	*Host Up:* Se recibe ABORT o INIT-ACK. *Host Down:* Expira el *timeout*.
-PE	Ping ICMP Echo	Envía un *ICMP Echo Request*. Poco fiable. Filtrado en la mayoría de cortafuegos.	*Host Up:* Se recibe ICMP Echo Reply. *Host Down:* Expira el *timeout*.
-PP	Ping ICMP Timestamp	Envía un *ICMP Timestamp Request*. Muchos cortafuegos no filtran este ICMP.	*Host Up:* Se recibe ICMP Timestamp Reply. *Host Down:* Expira el *timeout*.
-PM	Ping ICMP Address mask	Envía un *ICMP Address Mask Request*. Muchos cortafuegos no filtran este ICMP.	*Host Up:* Se recibe ICMP AddMask Reply. *Host Down:* Expira el *timeout*.
-PO<proto>	IP Protocol Ping	Envía sondas IP con protocolo 1, 2 y 4. Acepta lista de protocolos.	*Host Up:* Respuesta o ICMP Prot. Unreachable. *Host Down:* Expira el *timeout*.
Modificadores			
-n	DNS	No realiza nunca resolución inversa de DNS.	Más sigiloso y más rápido.
-R		Realiza la resolución inversa de DNS incluso a los objetivos que aparecen como *Down*.	
--dns-servers <srv>		Especifica la lista de servidores DNS a utilizar para hacer la resolución	
--system-dns		Utiliza el sistema de resolución DNS del sistema operativo	
--tracetoute	Ruta	Descubre la ruta seguida por los paquetes hasta el equipo objetivo.	

[1] Los objetivos, ya sean nombres de máquina, direcciones IP, o cualquier otro formato aceptado por Nmap, deben aparecer cada uno en una línea distinta.

ANÁLISIS DE PUERTOS			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-sT	Connect	Envía un SYN, luego un RST para cerrar conexión. Puede utilizarse sin privilegios de root . Se utilizan llamadas del SO. Menos eficiente que SYN Stealth.	*Closed*: Recibe RST. *Open:* Recibe SYN/ACK. *Filtered: ICMP unreachable* o expira el *timeout*.
-sS	SYN Stealth	Envía un SYN. Es la técnica usada por defecto. Rápida, fiable y relativamente sigilosa. También denominada *half-open scan.*	*Closed:* Recibe RST. *Open:* Recibe SYN/ACK. *Filtered: ICMP unreachable* o expira el *timeout*.
-sU	UPD Scan	Envía UDP vacío. Más lento que un análisis TCP. Se puede realizar en paralelo a otras técnicas. Para diferenciar entre *Open* y *Filtered* se puede usar el detector de versiones (*-sV*).	*Closed:* Recibe *ICMP port unreachable*. *Filtered:* Recibe otros *ICMP unreachable*. *Open:* Ha habido una respuesta. *Open|Filtered:* Expira el timeout.
-sI <zombie[:port]>	Idle Scan	Compleja. Usa IP origen de un equipo intermedio (Zombie) para analizar el objetivo. Según los cambios en el IPID del zombie, se deduce el estado de los puertos del objetivo.	Técnica muy avanzada y sigilosa. No queda registro de ningún paquete directo al objetivo.
-sA	TCP ACK	Envía ACK vacío. Sólo determina si los puertos están o no filtrados.	*Unfiltered*: Recibe RST. *Filtered: ICMP error*; expira el *timeout*.
-sN	TCP NULL	Envía TCP con todos los *flags* a 0.	*Closed*: Recibe RST. *Filtered*: Recibe *ICMP unreachable*. *Open|Filtered*: expira el *timeout*.
-sF	TCP FIN	Envía TCP con el *flag* FIN a 1.	
-sX	XMas Scan	Envía TCP con los *flags* FIN, PSH y URG a 1.	
-sM	TCP Maimon	Envía ACK con el *flag* FIN a 1.	
-sW	TCP Window	Envía ACK vacío. Muy parecido a ACK Stealth. Diferencia entre puertos open y closed. No siempre es fiable.	*Open*: Recibe RST con *Window size* positivo. *Closed*: Recibe RST con *Window size* cero. *Filtered: ICMP error*; expira el *timeout*.
--scanflags <flags>	TCP Personal.	Envía TCP con los *flags* que se indiquen. Por defecto, trata estado de puertos como lo hace *-sS*, pero se puede especificar otro *scan*.	*Flags posibles:* URG, ACK, PSH, RST, SYN, y FIN. Sin espacios.
-sO	IP Protocol	Envía paquetes IP con la cabecera vacía (excepto para TCP, UDP e ICMP) iterando sobre el campo *IP Protocol*. Determina los protocolos de transporte soportados por el objetivo.	*Open*: Recibe cualquier respuesta (no error). *Closed*: Recibe *ICMP protocol unreachable*. *Filtered*: Recibe otros *ICMP unreachable*. *Open|Filtered*: expira el *timeout*.
-sY	SCTP INIT	Envía paquetes SCTP INIT (inicio conexión). Equivalente a TCP SYN.	*Open:* Recibe SCTP INIT-ACK. *Closed:* Recibe SCTP ABORT. *Filtered:* Recibe *ICMP unreachable* o expira el *timeout*.
-sZ	SCTP Cookie Echo	Envía paquetes SCTP Cookie Echo (3ª fase conexión). Útil si hay cortafuegos sin estado.	*Closed:* Recibe SCTP ABORT. *Open|Filtered:* Expira timeout. *Filtered:* Recibe *ICMP unreachable*.
-b <ftpsrv>	FTP Bounce	Usa la funcionalidad Proxy-FTP para recorrer puertos del objetivo. Las respuestas FTP indican estado del puerto. Parámetro: *username:pwd@server:port*	Explota las conexiones *Proxy-FTP, poco extendidas.* Se usa para traspasar cortafuegos.

ESPECIFICACIÓN DE PUERTOS		
Opción	**Funcionamiento**	**Observaciones**
-F	Limita el análisis a los 100 puertos más comunes (ver archivo *nmap-services*).	Por defecto, se usan los 1000 puertos más comunes.

-r	Los puertos se analizan en orden secuencial creciente.	Por defecto, la lista de puertos se recorre aleatoriamente.
-p<rango>	Especifica el rango de puertos a analizar. ***-p-*** escanea todos los puertos. U: indica sólo UDP; T: sólo TCP; S: sólo SCTP.	Ej: *-p U:53,111,T:21-25,80,139,S:9* Sin espacios.
--top-ports <num>	Analiza los <num> puertos más comunes, según clasificación de Nmap.	
--port-ratio <ratio>	Analiza los puertos cuyo ratio de uso sea superior a <ratio>.	

DETECCIÓN DE VERSIONES		
Opción	**Funcionamiento**	**Observaciones**
-sV	Interroga al conjunto de puertos abiertos detectados para tratar de descubrir servicios y versiones en puertos abiertos.	También usado para distinguir entre puertos marcados como *open|filtered*.
--allports	Incluye todos los puertos en la fase de detección de versiones. Por defecto se excluyen algunos.	
--version-intensity <num>	Intensidad con que se realizan pruebas para comprobar servicios y versiones disponibles. Valores de 0 (ligera) a 9 (todas pruebas disponibles).	
--version-light	Alias de *--version-intensity 2*	
--version-all	Alias de *--version-intensity 9*	
--version-trace	Muestra traza de actividad del análisis de versiones y servicios.	Útil para tareas de depuración.

DETECCIÓN DE SISTEMA OPERATIVO		
Opción	**Funcionamiento**	**Observaciones**
-O	Envía paquetes TCP y UDP al objetivo. Analiza las respuestas para conocer qué tipo de implementación de la pila TCP/IP tiene el objetivo.	Muy efectivo si al menos existe un puerto abierto y otro cerrado.
--osscan-limit	Limita la detección del SO a objetivos prometedores.	
--osscan-guess	Realiza un proceso más agresivo para la detección del SO.	Alias: *--fuzzy*
--max-os-tries	Fija máximo de intentos para detectar el SO.	Por defecto, 5 intentos.

EVASIÓN DE CORTAFUEGOS/IDS Y SPOOFING			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-f	Fragmentar paquetes	Divide los paquetes en fragmentos de 8 bytes después de la cabecera IP. Cada *f* extra aumenta en 8 bytes más el tamaño de los fragmentos.	Usado para dividir las cabeceras TCP y complicar su análisis.
--mtu		Especifica el tamaño deseado. En múltiplos de 8 bytes.	
--data-length	Tamaño del paquete	Añade datos aleatorios a los paquetes enviados. Por defecto, las sondas se envían vacías.	Usado debido a que un paquete no vacío es menos sospechoso.
--randomize-hosts	Objetivos aleatorios	Divide la lista de objetivos en grupos de hasta 16384 equipos y los analiza en orden aleatorio.	Evita flujo de paquetes hacia IP consecutivas (suele ser sospechoso).
-D <host1>[,<hostN>]	Señuelos	Permite especificar un conjunto de IP válidas que se usarán como dirección origen en el análisis a modo de señuelos. Las respuestas de los objetivos llegarán también a los señuelos.	Usado para enmascarar la propia IP en el escaneo y dificultar la traza del origen. Los señuelos deben estar activos.
-S <IP>	Falsear dirección/ puerto origen	Envía paquetes IP con la dirección origen especificada.	Usado para hacer creer al objetivo que hay otra persona escaneándolo. Algunos ISP filtran las IP origen falseadas. No se reciben respuestas.
--spoof-mac <mac>		Envía tramas Ethernet con la dirección origen especificada. Si no se especifica completa, el resto se completa de forma aleatoria.	
-g <port> **--sourceport <port>**		Envía paquetes usando el puerto especificado, cuando sea posible.	Usado porque muchos cortafuegos aceptan conexiones entrantes a puertos típicos como p.e. TCP20 ó UDP53.

-e <iface>	Definir interfaz	Define la interfaz de red, en caso de existir múltiples, por la que Nmap lanzará el análisis.	
--ip-options <opts>	Opciones IP	Permite fijar opciones del protocolo IP. Routers bloquean muchas de ellas. Útil para definir o reconocer rutas.	Más info y ejemplos en: http://seclists.org/nmap-dev/2006/q3/52
--ttl <valor>	TTL	Fija el tiempo de vida de las sondas enviadas.	
--badsum	Checksums incorrectos	Usa checksum inválidos para TCP, UDP y SCTP.	Usado porque muchos Cortafuegos/IDS no procesan este campo y los objetivos sí.
--adler32	SCTP Checksum	Utiliza método de cálculo de resumen Adler32, en lugar del actual CRC-32C, para paquetes SCTP.	Útil para obtener respuestas de implementaciones SCTP antiguas.

TEMPORIZACIÓN Y RENDIMIENTO[2]			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
--min-hostgroup <num> --max-hostgroup <num>	Objetivos en paralelo	Establece los límites mínimo y máximo de objetivos que se pueden analizar de forma concurrente.	
--min-parallelism <num> --max-parallelism <num>	Pruebas en paralelo	Establece los límites mínimo y máximo de pruebas que pueden estar llevandose a cabo de forma concurrente. Por defecto valor dinámico basado en el rendimiento de la red.	Útil en redes o equipos lentos. Valor demasiado alto puede afectar precisión.
--min-rtt-timeout <time> --max-rtt-timeout <time> --initial-rtt-timeout <time>	Tiempo de respuesta de las sondas	Modifica el tiempo de espera de respuestas a sondas enviadas. Si vence el tiempo de espera, Nmap considera que no hay respuesta y sigue con la siguiente sonda. Por defecto valor dinámico basado en tiempo de sondas anteriores.	Útil en redes rápidas o cuando muchos puertos están cerrados.
--max-retries <num>	Retransmisiones	Especifica el número de retransmisiones para cada sonda, en caso de no recibir respuesta.	Por defecto 10 reintentos.
--host-timeout <time>	Tiempo de análisis de equipo	Especifica el tiempo máximo que ocupa Nmap en el análisis de un equipo completo. Si vence este tiempo, no se muestra nada sobre el mismo en el análisis final.	Útil para análisis grandes en redes poco fiables o lentas, a costa de perder algunos resultados.
--scan-delay <time> --max-scan-delay <time>	Tiempo entre sondas	Define el tiempo inicial y máximo que espera Nmap entre cada prueba. Nmap trata de ajustar ese tiempo de forma dinámica.	Útil si la red limita la tasa de transferencia o de respuestas. P.ej. equipos que solo envían 1 respuesta ICMP por segundo.
--min-rate <num> --max-rate <num>	Tasa de envío de sondas	Controla la tasa de envío de sondas. Ámbito global del análisis, no por objetivo.	
--defeat-rst-ratelimit	Límite de respuestas RST	Muchos equipos limitan, además del número de ICMP, el número de RST que envían. Por defecto Nmap se ajusta al límite. Este parámetro hace que Nmap no tenga en cuenta este límite.	Puede reducir precisión.
--nsock-engine <motor>	Motor E/S nsock	Fuerza el uso de un motor de control de entrada salida.	Valores posibles: *epoll* y *select*.
-T <plant>	Plantillas de tiempo	Define una plantilla genérica de tiempos, que configura varios de los parámetros vistos anteriormente.	Valores (de + a - lento): *paranoid*, *sneaky*, *polite*, *normal*, *aggressive*, *insane*. Alias: 0 a 5 (p.ej. -T4). Por defecto: Normal (3).

[2] Los tiempos se miden por defecto en segundos. Se pueden utilizar otras unidades de medida añadiendo los sufijos 'ms' (milisegundos), 's' (segundos), 'm' (minutos), o 'h' (horas). Por ejemplo 30m, 500ms o 2h.

SCRIPTING		
Opción	**Funcionamiento**	**Observaciones**
-sC	Incluye en el análisis actual el conjunto por defecto de scripts (algunos pueden ser intrusivos).	Equivalente a: *--script default*
--script <valor>	Define el/los script a utilizar. Valor puede ser un nombre de fichero, categoría, directorio, expresión, etcétera. Alias *all* ejecuta todos los script (peligroso).	Valores separados por comas. Prefijo + hace que se ejecuten aunque no corresponda.
--script-args <args>	Argumentos a pasar a los scripts. Formato: *<nombre>=<valor>*	Argumentos separados por comas. Prioridad sobre los definidos en fichero.
--script-args-file <file>	Carga argumentos de un fichero.	Por defecto, 5 intentos.
--script-help <valor>	Muestra ayuda sobre los scripts. Valores como *--script*.	
--script-trace	Símil de *--packet-trace* una capa ISO por encima. Muestra todas las comunicaciones realizadas por un script.	
--script-updatedb	Actualiza la BBDD de scripts existente.	Útil si se realizan cambios a la carpeta de scripts por defecto.

SALIDA			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-oN <file>	Salida normal	Registra en un fichero una salida muy similar a la mostrada por pantalla en modo interactivo.	Debe definirse la extensión deseada (nmap para salida normal y gnmap para la "grepable"). Se pueden aplicar formatos de tiempo al estilo *strftime*: %H, %M, %S, %m, %d, %y, %Y, %T, %R, %D.
-oX <file>	Salida XML	Crea un fichero XML con los detalles del análisis. Se puede usar la plantilla XST incluida o cualquier reconocedor de XML para procesarla.	
-oS <file>	Salida Script Kiddie	Salida muy similar a la del modo interactivo, pero sustituyendo caracteres y capitalización para ajustarse al lenguaje utilizado por estos grupos en Internet como sello de identidad.	
-oG <file>	Salida "grepable"	Salida con formato especial que es fácilmente tratable con herramientas de consola como grep. Obsoleta.	
-oA <patrón>	Salida en todos los formatos	Crea un fichero para los tipos de salida normal, XML y "grepable", definidos anteriormente.	Sin extensión. Nmap usa el patrón definido y añade cada extensión.
-v[<nivel>]	Verbosidad	Aumenta la cantidad de información sobre el progreso del análisis que muestra Nmap por pantalla.	Para aumentar verbosidad se pueden añadir más v o incluir un número (p. ej. *-vvv* o *–v3*).
-d[<nivel>]	Depuración	Añade información de depuración a la salida que Nmap muestra por pantalla.	Se pueden añadir más d o incluir un número (p.ej *-ddd* o *-d3*) para aumentar el nivel de depuración.
--reason	Razón	Indica la razón por la que se ha concluido el estado de un puerto o equipo.	Permite diferenciar el tipo de respuestas que ha generado un puerto cerrado.
--stats-every <time>	Estadísticas	Indica cada cuanto tiempo se imprimen estadísticas sobre el tiempo restante del análisis.	Se imprime tanto por pantalla como en la salida XML.
--packet-trace	Traza de paquetes	Hace que Nmap imprima información sobre cada paquete que envía o recibe.	Incluye información de *--version-trace* y *--script-trace*.
--open	Puertos abiertos	Muestra en la salida los puertos identificados como (posiblemente) abiertos, obviando aquellos con otros estados (filtrados o cerrados).	Útil en grandes análisis para obtener listado de puertos alcanzables.
--iflist	Interfaces y rutas	Muestra únicamente el listado de interfaces y de rutas detectado por Nmap.	Útil para depuración.
--log-errors	Errores	Guarda los errores generados durante la ejecución del análisis en los ficheros de salida, además de mostrarlos por pantalla.	
--append-output	Ficheros de salida	Instruye a Nmap para añadir los resultados del análisis actual a un fichero de salida existente, en lugar de borrar el contenido de dicho fichero.	Puede causar problemas de tratamiento automático con ficheros XML.
--resume <file>	Continuar	Continua un análisis Nmap en el punto en que se quedó, si se indica como parámetro un fichero generado con los modificadores *-oN* o *-oG*.	Interesante para análisis muy largos o que necesitan ser interrumpidos por causas de fuerza mayor.

--stylesheet <file>	Hoja de estilos	Indica que hoja de estilos XSL incrustar en la salida XML. Requiere ruta o URL completa.	Las hojas de estilos XSL definen como se traduce un fichero XML a uno HTML. Útil para visualizar informes en XML a través de un navegador web si el cliente no tiene Nmap instalado.
--webxml		Alias para *--stylesheet http://nmap.org/svn/docs/nmap.xsl*	
--no-stylesheet		Indica que no se incruste ningún enlace a hoja de estilos en la salida XML.	

MISCELÁNEA			
Opción	**Nombre**	**Funcionamiento**	**Observaciones**
-6	IPv6	Habilita el análisis en redes IPv6.	
-A	Análisis agresivo	Alias para *-O -sV -sC --traceroute*	
--datadir <dir>	Directorio de datos	Indica el directorio de donde Nmap lee algunos ficheros que necesita para su uso (nmap-service-probes, nmap-services, nmap-protocols, nmap-rpc, nmap-mac-prefixes y nmap-os-db).	
--servicedb <file>	Fichero de servicios	Indica una localización personalizada para el fichero de donde Nmap obtiene la información sobre servicios.	Fichero nmap-services. Más prioritario que *--datadir*. Activa *-F*.
--versiondb <file>	Fichero de versiones	Indica la ubicación del fichero de donde Nmap obtiene las sondas que debe enviar para detectar servicios (*-sV*).	Fichero nmap-service-probes. Más prioritario que *--datadir*.
--send-eth	Escribir en tramas ethernet	Escribe directamente tramas a nivel Ethernet sin usar el API de red ni transporte. Por defecto se decide de forma dinámica el tipo de tramas a enviar.	Usado para evitar limitaciones de algunas implementaciones de la pila TCP/IP. Activada por defecto en la versión para Windows.
--send-ip	Escribir tramas IP	Escribe paquetes a nivel IP, y los pasa al sistema operativo para que este se encargue de enviarlos.	Complementaria de la opción anterior.
--privileged	Modo privilegiado	Asume que tiene suficientes permisos para realizar operaciones que requieren elevación de privilegios, como apertura de sockets RAW y captura de paquetes, entre otros.	Útil si se permite a usuarios sin privilegios realizar dichas acciones. Alternativa: Fijar la variable de entorno NMAP_PRIVILEGED.
--unprivileged	Modo sin privilegios	Opuesto al anterior. Asume que no se tienen privilegios para realizar operaciones privilegiadas.	Útil para pruebas o depuración.
--release-memory	Liberar memoria	Hace que Nmap libere toda su memoria antes de finalizar su ejecución. Normalmente es el SO quien hace esta tarea.	Facilita descubrimiento de filtraciones de memoria.
-V --version	Versión	Imprime la versión de Nmap y finaliza la ejecución.	
-h --help	Ayuda	Imprime la página de ayuda resumida.	Alias: Lanzar nmap sin argumentos.

INTERACCIÓN EN TIEMPO DE EJECUCIÓN	
Comando	**Funcionamiento**
v / V	Aumenta / Disminuye el nivel de verbosidad.
d / D	Aumenta / Disminuye la cantidad de información de depuración que se muestra.
p / P	Activa / Desactiva la traza de paquetes (*--packet-trace*).
?	Muestra la pantalla de ayuda de interacción en tiempo de ejecución.
Cualquier otro	Imprime mensaje con estado actual del análisis.

CSIRT-cv: Centro de Seguridad TIC de la Comunidad Valenciana.
http://www.csirtcv.gva.es
http://www.facebook.com/csirtcv
http://twitter.com/csirtcv