Nmap

Riferimenti

- Sito web
  https://nmap.org
- The Official Nmap Project Guide to Network Discovery and Security Scanning:
  https://nmap.org/book/toc.html

Formato dei comandi nmap

```
nmap [ <Options> ] { <target specification> }
```

Se `nmap` viene lanciato senza nessuna opzione, per esempio

```
nmap 192.168.0.1
```

viene lanciata una scansione sulle 1000 porte note come nmap-services

Definizione del target

https://nmap.org/book/man-target-specification.html
Esempi di formati utilizzabili

- CIDR: 192.168.0.0/24
- 192.168.0-255.1-254
- 192.168.3-5,7.1
- `-iL <inputfilename>` (Input from list)
- `--exclude <host1>[,<host2>[,...]]` (Exclude hosts/networks)
- `--excludefile <exclude_file>` (Exclude list from file)

Opzioni disponibili

Se `nmap` viene lanciato senza nessun argomento, viene visualizzato l'elenco di tutte le opzioni disponibili. Lo stesso elenco (aggiornato all'ultima versione di `nmap`) è riportate anche alla pagina:
https://nmap.org/book/man-briefoptions.html
Alcune opzioni usate comunemente sono le seguenti.

- `-n` (No DNS resolution)
- `-R` (DNS resolution for all targets)
- `--dns-servers <server1>[,<server2>][,...]];` (Servers to use for reverse DNS queries)

Risultati

https://nmap.org/book/man-port-scanning-basics.html
Per ogni porta/protocollo `nmap` può dare una delle seguenti risposte.

- **open**
  Un'applicazione accetta attivamente su questa porta connessioni TCP, datagrammi UDP o o associazioni SCTP (Stream Control Transmission Protocol).
- **closed**
  Una porta chiusa è accessibile (riceve e risponde ai pacchetti di probe di Nmap) ma non vi è alcuna applicazione in ascolto su di essa. Esse possono rendersi utili nel mostrare che un host è attivo su un indirizzo IP (durante l'host discovery o il ping scanning) o in quanto parte integrante dell'Operating System discovery. Poiché una porta chiusa è raggiungibile, può essere interessante effettuare una scansione più tardi nel caso alcune vengano aperte. Chi amministra una macchina o una rete può voler bloccare tali porte con un firewall ed in questo caso esse apparirebbero come filtrate, come mostrato in seguito.
- **filtered**
  In questo caso Nmap non può determinare con esattezza se la porta sia aperta o meno, perché un filtro di pacchetti impedisce ai probe di raggiungere la porta. Questo filtro può esser dovuto a un firewall dedicato, alle regole di un router, o a un firewall software installato sulla macchina stessa.
- **unfiltered**
  Lo stato "unfiltered" indica che una porta è accessibile, ma che Nmap non è in grado di determinare se sia aperta o chiusa. Solo la scansione di tipo ACK, usata per trovare e classificare le regole di un firewall, posiziona una porta in questo stato.
- **open|filtered**
  Nmap posiziona le porte in questo stato quando non è in grado di determinare se una porta sia aperta o filtrata. Questo accade in quelle scansioni per le quali una porta aperta non risponde in alcun modo. La mancanza di informazioni può significare inoltre che un filtro di pacchetti ha lasciato cadere ("drop") il probe o qualsiasi risposta sia stata generata in seguito a questo.
- **closed|filtered**
  Questo stato è usato quando Nmap non è in grado di determinare se una porta sia chiusa o filtrata.

Formati di output

https://nmap.org/book/man-output.html

- `-oN <filespec>` (normal output)
  Richiede che il normal output venga rediretto al file specificato. Come sopra, quest'output diverge leggermente da `interactive output`.

- `-oX <filespec>` (XML output)
  Richiede che l'output XML sia rediretto al file specificato
- `-oG <filespec>` (grepable output)
  Sebbene il suo uso sia deprecato, il grepable output è ancora discretamente usato. È un formato semplice che lista ogni host su una riga e può essere facilmente cercato e interpretato dai tool standard di UNIX, come `grep`, `awk`, `cut`, `sed`, `diff`, ...
- `-oA <basename>` (Output to all formats)
  In caso di bisogno, si potrebbe specificare `-oA _`<basename>`_` per salvare i risultati dello scan nei formati normal, XML e grepable in una sola volta. Questi vengono salvati rispettivamente nei file *<basename>*.nmap, *<basename>*.xml e *<basename>*.gnmap.

Altre opzioni relative al formato di output.

- `-v` (Increase verbosity level), `-v<level>` (Set verbosity level)
- `-d` (Increase debugging level), `-d<level>` (Set debugging level)
- `--reason` (Host and port state reasons)
  - Mostra il motivo per cui ad ogni singola porta è stato assegnato quello stato e la ragione per cui ogni host è attivo o meno.
- `--append-output` (Append to rather than clobber output files)
- `--resume <filename>` (Resume aborted scan)
  Alcune esecuzioni di Nmap possono richiedere molto tempo - dell'ordine di giorni. Tali scansioni non arrivano sempre alla fine; alcune restrizioni possono impedire a Nmap di funzionare durante le ore del giorno, la rete può diventare irraggiungibile, la macchina sulla quale Nmap sta girando può subire un riavvio pianificato o improvviso o Nmap stesso può andare in crash. L'amministratore che sta usando Nmap può interromperlo per qualsiasi ragione, premendo **ctrl-C**. Ricominciare l'intera scansione dall'inizio può diventare fastidioso. Fortunatamente se sono rimasti i log in formato "normal" (`-oN`) o "grepable" (`-oG`), l'utente può richiedere a Nmap di ricominciare la scansione dall'host sul quale stava lavorando quando l'esecuzione è stata interrotta. Semplicemente basta specificare l'opzione `--resume` e passargli il file di output in formato normal/grepable come argomento. Non è permesso nessun altro argomento, poiché Nmap farà il parsing del file di output per usare le stesse opzioni specificate in precedenza. È quindi sufficiente invocare Nmap come **nmap --resume** *<logfilename>*. Nmap aggiungerà i nuovi risultati ai file specificati nell'esecuzione precedente. La ripresa di un'esecuzione non supporta il formato di output XML poiché sarebbe troppo difficile combinare le due esecuzioni in un unico file XML valido

Host discovery

https://nmap.org/man/it/man-host-discovery.html

- `-sL` (List Scan)
  Esegue solo una risoluzione inversa mediante DNS sugli host per ottenerne il nome completo (FQDN). Non viene inviato nessun pacchetto agli host.

- `-sn` (No port scan)
  Questa opzione indica a Nmap di non effettuare un port scan dopo un host discovery e di mostrare gli host che hanno risposto. VIene spesso indicata come "ping scan".
- `-Pn` (No ping)
  Questa opzione evita del tutto il passaggio di ricerca degli host di Nmap. Normalmente Nmap usa questo passaggio per trovare le macchine attive da sottoporre ad una scansione più approfondita. Di default, Nmap esegue un probing approfondito (come ad esempio un port scan, una version detection dei servizi o un Operating System detection) solo sugli host che sono stati trovati attivi. Disabilitare l'host discovery attraverso l'opzione `-Pn` obbliga Nmap a tentare la scansione richiesta su *tutti* gli host destinazione specificati.
- `-PS <port list>` (TCP SYN Ping)
- `-PA <portlist>` (TCP ACK Ping)
- `-PU <portlist>` (UDP Ping)
- `-PY <port list>` (SCTP INIT Ping)
- `-PE`; `-PP`; `-PM` (ICMP Ping Types)
- `-PO <protocol list>` (IP Protocol Ping)
- `-PR` (ARP Ping)

Port scanning

Definizione delle porte da passare a scansione

https://nmap.org/book/man-port-specification.html

Di default Nmap effettua la scansione delle 1.000 porte più comuni per ogni protocollo.

- `-p <port ranges>` (Only scan specified ports)
- `--exclude-ports <port ranges>` (Exclude the specified ports from scanning)
- `-r` (Don't randomize ports)
- `--top-ports <n>`

Tecniche di port scanning

https://nmap.org/book/man-port-scanning-techniques.html

- `-sS` (TCP SYN scan)
  Il SYN scan è l'opzione di default ed è la più usata per buone ragioni. Può essere effettuato velocemente: effettua la scansione su migliaia di porte al secondo su una rete veloce non limitata da firewall restrittivi. Il SYN scan è relativamente nascosto e poco invasivo, poiché non completa mai le connessioni TCP. Funziona inoltre con ogni stack TCP compatibile e non dipende dai comportamenti particolari che possono avere pi piattaforme specifiche come fanno gli altri tipi di scan di Nmap quali FIN/NULL/Xmas, Maimon e Idle scan. Inoltre permette una differenziazione chiara ed affidabile tra le porte appartenenti agli stati `open`, `closed` e `filtered`.

Questa tecnica è spesso indicata come "scanning semi-aperto" (tradotto letteralmente per esigenze di comprensione, da "half-open scanning", NdT), perché non viene aperta una connessione TCP completa. Viene mandato un pacchetto SYN come se si fosse sul punto di aprire una connessione reale e si attende una risposta. Un SYN/ACK indica che la porta è in ascolto (aperta), mentre un RST (reset) indica che la porta non è in ascolto. Se non viene ricevuta nessuna risposta dopo diverse ritrasmissioni la porta viene marcata come filtrata. La porta viene marcata come tale anche se viene ricevuto un pacchetto di errore "ICMP unreachable" (tipo 3, codici 1, 2, 3, 9, 10, 13). La porta viene considerata aperta anche nel caso in cui un pacchetto SYN (senza il flag ACK) viene ricevuto in risposta.

- `-sT` (TCP connect scan)
- `-sU` (UDP scans)
  Può essere combinato con uno scan di tipo TCP come ad esempio un SYN scan (`-sS`) per controllare entrambi i protocolli nel corso della stessa sessione.
  Lo scan UDP funziona inviando pacchetti UDP ad ogni porta di destinazione. Per alcune porte comuni, come la 53 e la 161, un carico dati viene aggiunto per aumentare le probabilità di risposta, ma per la maggior parte delle porte il pacchetto viene inviato vuoto, a meno che non vengano specificate le opzioni `--data`, `--data-string` o `--data-length`. Se viene restituito un errore ICMP "port unreachable" (tipo 3, codice 3) significa che la porta è `closed` (chiusa). Altri errori ICMP di tipo "unreachable" (irraggiungibile) come quelli del tipo 3, codici 1, 2, 9, 10 o 13 andranno ad identificare la porta come `filtered` (filtrata). Talvolta un servizio risponderà con un pacchetto UDP, dimostrando quindi che lo stato della porta è `open` (aperta). Se non viene ricevuta alcuna risposta dopo alcune ritrasmissioni, la porta viene classificata come `open|filtered` (aperta|filtrata). Questo significa che la porta può essere aperta o che probabilmente un filtro di pacchetti sta bloccando la comunicazione. Un version detection (`-sV`) può essere usato per aiutare a differenziare le porte veramente aperte da quelle che sono filtrate.
  La sfida maggiore con l'UDP scan è la velocità. Le porte aperte e filtrate raramente inviano qualche risposta, lasciando Nmap in timeout e facendolo ritrasmettere per evitare il caso in cui il probe o la risposta siano andati perduti. Le porte chiuse sono spesso un problema ancora maggiore: esse generalmente rimandano un pacchetto ICMP "port unreachable error", ma a differenza dei pacchetti RST rimandati dalle porte chiuse TCP come risposta ad un SYN o connect scan, molti host limitano il tasso di invio di tali pacchetti di default. Linux e Solaris sono particolarmente restrittivi da questo punto di vista. Ad esempio, il kernel 2.4.20 limita i messaggi di "destination unreachable" a uno al secondo (definito in `net/ipv4/icmp.c`).
  Nmap si accorge di questi limiti sulla frequenza di invio e rallenta l'invio dei probe in maniera dinamica, per evitare di intasare la rete con pacchetti inutili che la macchina di destinazione ignorerà comunque. Sfortunatamente, un limite come quello di Linux di un pacchetto al secondo rende una scansione su 65.535 porte di una durata teorica di più di 18 ore. Suggerimenti per rendere più veloce gli scan UDP sono quelli di effettuare scansioni su più host in parallelo, fare uno scan veloce preliminare sulle porte più

usate, effettuare la scansione dall'interno del firewall ed infine usare l'opzione `--host-timeout` per evitare host troppo lenti nel rispondere.

- `-sY` (SCTP INIT scan)
- `-sN`; `-sF`; `-sX` (TCP NULL, FIN, and Xmas scans)
- `-sA` (TCP ACK scan)
  Questo scan è diverso dagli altri discussi finora dal momento che non serve per determinare se le porte sono `open` (o `open|filtered`). Viene usato per mappare le regole di firewalling determinando se sono stateful o no e quali porte sono filtrate.
  I pacchetti dell'ACK scan hanno soltanto il flag ACK abilitato (a meno che non si usi `--scanflags`). Mentre si scansionano sistemi non filtrati, sia le porte `open` che le porte `closed` manderanno pacchetti RST. Nmap poi le cataloga come `unfiltered`, nel senso che è possibile raggiungerle con un pacchetto ACK, ma che siano aperte o chiuse non è determinabile. Le porte che non rispondono, o mandano certi errori ICMP (tipo 3, codice 1, 2, 3, 9, 10 o 13), sono etichettate come `filtered`.
- `-sW` (TCP Window scan)
- `-sM` (TCP Maimon scan)
- `--scanflags` (Custom TCP scan)
  L'opzione `--scanflags` consente di designare una scansione personalizzata specificando arbitrariamente i flag TCP necessari.
  I parametri dell'opzione `--scanflags` possono essere un valore numerico indicante i flag TCP, come ad esempio 9 (PSH e FIN) anche se l'utilizzo di nomi simbolici risulta comunque più semplice. Basta mettere creare una qualsiasi combinazione di `URG`, `ACK`, `PSH`, `RST`, `SYN` e `FIN`. Per esempio, `--scanflags URGACKPSHRSTSYNFIN` imposta tutti i flag, anche se non risulta molto utile al fine della scansione. L'ordine con cui vengono specificati non è rilevante.Oltre allo specificare i flag desiderati, è possibile indicare un tipo di scansione TCP (come `-sA` o `-sF`). Questo specifica come Nmap deve interpretare le risposte.
- `-sZ (SCTP COOKIE ECHO scan)`
- `-sO` (IP protocol scan)
  L'IP protocol scan permette di determinare che protocolli IP (TCP, ICMP, IGMP, ecc.) sono supportati dalle macchine obiettivo. Non è tecnicamente un port scan, dato che utilizza i numeri indicanti il protocollo IP e non i numeri di porta TCP o UDP. Utilizza comunque ancora l'opzione `-p` per scegliere il protocollo da scansionare, riporta i risultati nel normale formato della tabella delle porte ed utilizza lo stesso engine sottostante al port scanning reale.

Service and application version detection

https://nmap.org/book/man-version-detection.html

- `-sV` (Version detection)
- `--version-intensity <intensity>` (Set version scan intensity)
  Quando si effettua un version scan (`-sV`), Nmap invia una serie di probe, ognuno dei quali ha assegnato un valore compreso tra 1 e 9. I pacchetti con valore più basso sono

in grado di riconoscere i servizi comunemente diffusi, mentre quelli con valori più alti sono raramente necessari. Il livello di accuratezza specifica quali probe devono essere impiegati; più alto è il livello, più è probabile che il servizio venga correttamente identificato. D'altro canto, più una scansione è accurata e più tempo sarà necessario. I valori devono essere compresi tra 0 e 9; il valore di default è 7.

- `--version-light` (Enable light mode)
  Questa opzione è un alias di `--version-intensity 2`.
- `--version-all` (Try every single probe)
  Questa opzione è equivalente a `--version-intensity 9`, assicurando che ogni singolo probe venga utilizzato su ogni singola porta.

OS Detection

https://nmap.org/book/man-os-detection.html

- `-O` (Enable OS detection)
  Abilita l'OS detection, come descritto sopra. In alternativa, è possibile utilizzare l'opzione `-A` per attivare sia l'OS detection, tra le altre cose.

Timing

https://nmap.org/book/man-performance.html

- `--min-hostgroup <numhosts>; --max-hostgroup <numhosts>` (Adjust parallel scan group sizes)
- `--min-parallelism <numprobes>; --max-parallelism <numprobes>` (Adjust probe parallelization)
- `--min-rtt-timeout <time>, --max-rtt-timeout <time>, --initial-rtt-timeout <time>` (Adjust probe timeouts)
- `--max-retries <numtries>` (Specify the maximum number of port scan probe retransmissions)
- `--host-timeout <time>` (Give up on slow target hosts)
- `--script-timeout <time>`
- `--scan-delay <time>; --max-scan-delay <time>` (Adjust delay between probes)
- `--min-rate <number>; --max-rate <number>` (Directly control the scanning rate)
- `--defeat-rst-ratelimit`
- `--defeat-icmp-ratelimit`
- `--nsock-engine iocp|epoll|kqueue|poll|select`
- `-T paranoid|sneaky|polite|normal|aggressive|insane` (Set a timing template)
  Mentre le opzioni mostrate sopra sono molto utili ed efficaci alcuni potrebbero trovarle troppo complicate da usare. Inoltre, la scelta dei valori più appropriati può a volte richiedere più tempo della scansione stessa che si sta cercando di ottimizzare. Nmap offre quindi un approccio più semplice mediante sei "timing templates", ovvero opzioni pre-impostate per regolare l'aggressività della scansione. Esse si specificano mediante

l'opzione `-T` seguita dal numero del template corrispondente o dal suo nome.
Essi sono:

- paranoico (0),
- furtivo (1),
- educato (2),
- normale (3),
- aggressivo (4),
- folle (5).
  I primi due vengono usati per evitare i sopracitati sistemi anti-intrusione (IDS). La modalità "gentile" rallenta la scansione in modo da usare meno banda e risorse sulla macchina bersaglio. La modalità "normale" è di default (e pertanto l'opzione `-T3` non modifica nulla). La modalità "aggressiva" incrementa la velocità assumendo che si è su una rete veloce ed affidabile. Infine la modalità "folle" dà per scontato che si è su una rete estremamente veloce ed affidabile o che si vuole sacrificare l'accuratezza in nome della velocità.

Nmap Scripting Engine (NSE)

https://nmap.org/book/man-nse.html

- `-sC`
  Esegue uno script scan utilizzando il set di script di default. È l'equivalente di `--script=default`. Alcuni degli script in questa categoria vengono considerati intrusivi e potrebbero non essere eseguiti su di un obiettivo di rete senza permessi.
- `--script <filename>|<category>|<directory>|<expression>[,...]`
  Esegue uno script scan utilizzando una lista, separata da virgole, di file, categorie di script e directory. Ogni elemento nella lista può anche essere un'espressione booleana che descrive un più complesso set di script. Gli elementi vengono interpretati prima come un'espressione, poi come una categoria e infine come il nome di file o di una directory.
- `--script-help`
  Esempio:
  `nmap --script-help /usr/share/nmap/scripts/dhcp-discover.nse`
- `--script-updatedb`
  Quest'opzione aggiorna il database degli script che si trova nel file `scripts/script.db`.

Esempio di comando di nmap

`nmap -d3 -v -Pn -sV -sT -sU -T3 -p U:7,19,21,53,T:21,22,23,25,53,80,443 192.168.0.0/24

- `-d3`
  Aumenta il debugging level a 3.
- `-v`
  Aumenta il livello di verbosità.

- `-Pn`
  Questa opzione evita del tutto il passaggio di ricerca degli host di Nmap. Normalmente Nmap usa questo passaggio per trovare le macchine attive da sottoporre ad una scansione più approfondita. Di default, Nmap esegue un probing approfondito (come ad esempio un port scan, una version detection dei servizi o un Operating System detection) solo sugli host che sono stati trovati attivi. Disabilitare l'host discovery attraverso l'opzione `-Pn` obbliga Nmap a tentare la scansione richiesta su *tutti* gli host destinazione specificati.
- `-sV`
  Version detection di servizi e applicazioni.
- `-sT`
  TCP connect scan.
- `-sU`
  UDP scans.
- `-T3`
  Timing templates: normal3 (3).
- `-p U:7,19,21,53,T:21,22,23,25,53,80,443`
  Scansione indirizzata solo verso le porte UPD 7,19,21,53 e TCP 21,22,23,25,53,80,443.
- `192.168.0.0/24`
  Target della scansione.