Nmap per "hackers"

Escaneig de xarxes

nmap -sn { ipInici-ipFinal [altraIP ...] | ipAmbAsterisks } — Mostra quins ordinadors estan presents a la xarxa/rang indicat.

Per indicar el rang a escanejar, es poden escriure diferents alternatives (a combinar):

- -Una IP de host individual o diferents IPs de hosts individuals separades per espais
- -Un rang d'IPs indicat per guions (p. ex: 192.168.1.3-5 ó 10.0.0-255.1-254, etc)
- -Un conjunt d'IPs indicat per comes (p. ex: 192.168.1.3,5 ó 10.0.0,1,4.1, etc)
- -Una IP de classe C escrita amb el comodí * (p. ex: 192.168.1.*)
- -Una IP de xarxa amb la seva màscara corresponent (p. ex: 192.168.1.0/24)
- -Igualment, es poden indicar hostnames
- -El paràmetre *--exclude* o (*--excludefile)* per indicar, amb mateixes normes, subrangs exclosos

El paràmetre *-sn* permet veure si els ordinadors indicats estan presents a la xarxa però sense fer cap escaneig de ports (concretament, envia dos paquets ICMP -"echo-request" i "timestamp"- a cada destí a més de dos paquets TCP SYN -als ports 80 i 443 de cada destí respectivament-, per si els paquets ICMP estiguessin filtrats). Això fa que l'escaneig sigui més ràpid. No obstant, es pot canviar el tipus de paquets utilitzats (per ser encara més ràpids, o més sigilosos, etc) amb els paràmetres opcionals: *-PS, -PA,-PU,-PY, -PE, -PP, -PM, -PO ...*

Escaneig de ports

nmap -Pn -p nº,nº,nº-nº ipOrdinador : Comprova quins ports TCP (dels indicats amb el paràmetre *-p*) estan oberts a l'ordinador "objectiu". Si es vol que els ports indicats siguin considerats UDP cal afegir el paràmetre *-sU* Si no s'indica cap paràmetre *-p*, l'Nmap fa l'escaneig dels ports "més habituals".

Si ja sabem que la "víctima" està accessible a la xarxa (perquè, per exemple, ho hem vist amb l'escaneig de xarxa previ) i només ens interessa fer l'escaneig de ports directament sense haver de fer cap "ping" de comprovació podem estalviar-nos aquest "pas de descoberta" previ innecessari amb el paràmetre *-Pn*

Un altre paràmetre que se sol afegir quan es fan escanejos de ports és el paràmetre *-A* (o *-O* i/o *-sV*):

-O — Mostra el sistema operatiu de l'ordinador i els programes que hi ha escoltant "al darrera" dels ports oberts. Es pot combinar amb el paràmetre *-sV*, el qual mostra també les versions respectives. El paràmetre *-A* és la combinació dels dos. En qualsevol cas, tots tres paràmetres només funcionen si s'executen com a *root*

NOTA: Altre paràmetre interessant que podem acompanyar a l'escaneig és *--reason* (mostra la raó de per què cada port està en l'estat que està -tancat, obert, filtrat-). D'altra banda, si només volem veure informació sobre els ports oberts, podem afegir el paràmetre *--open*

Existeixen molts altres paràmetres (*-sS, -sT, -sA, -sW, -sM, -sU, -sN, -sF, -sX, -sY, -sZ, ...*) que permeten especificar la tècnica concreta a fer servir per esbrinar si un port està obert o no: algunes tècniques són més ràpides però a canvi són menys sigiloses i/o precises, o viceversa El tipus d'escaneig de ports per defecte que Nmap sol fer servir si no s'indica cap es correspon al que s'indicaria amb el paràmetre *-sS*

D'altra banda, a l'article https://thehackerway.com/2012/02/24/intentando-evadir-mecanismos-y-restricciones-de-seguridad-escaneo-con-nmap-evadiendo-firewalls-parte-vi s'expliquen diverses tècniques d'escaneig que permeten "saltar-se" la protecció d'un tallafocs/IDS per tal d'aconseguir confirmar si, efectivament, determinats ports estan oberts o no.

En qualsevol cas, altres paràmetres que es poden indicar en tot tipus d'escaneig (de xarxes o de ports) són:

-v	Mode verbós (*-vv* és més verbós). També està *-d* (mode "debug")
-n	No resol noms. També està el paràmetre *--dns-servers* , que permet indicar altres servidors DNS a usar per resoldre noms diferents dels predefinits al sistema
-e nomTarja	Fa servir explícitament la tarja de xarxa indicada per l'escaneig
-T{0-5}	Estableix retard entre paquet i el següent, per fer l´escaneig més o menys sigilós, o el que és el mateix, de més a menys lent (de 0 a 5): "paranoid", "sneaky", "polite", "normal" -per defecte-, "aggressive", "insane".
-iL nomFitxer.txt	Indica el fitxer des d'on s'agafaran les IPs i noms dels rangs o ordinadors a escanejar (si ha vàries poden estar separades per espais en blanc, tabuladors o salts de línia) en comptes de pel terminal directament.
-oN nomFitxer.txt	El resultat de l'escaneig el guarda en un fitxer. El paràmetre *-oN* treu la sortida "normal", però també es pot fer servir *-oX* per a què la sortida sigui en XML o *-oG* per a què sigui fàcilment processable per Grep, entre altres. La combinació dels 3 formats es pot fer amb *-oA*
--packet-trace	Mostra la traça de tots els paquets enviats pel Nmap en realitzar la seva feina (va bé per estudiar)
--host-timeout <n>	Estableix un temps (del tipus "3s", "2m", "7h", etc) màxim després del qual, si no s'ha finalitzat l'escaneig abans, aquest s'aturarà.

Escaneig de vulnerabilitats

Nmap incorpora un motor d'scripting propi anomenat NSE ("Nmap Scripting Engine", https://nmap.org/book/nse.html) que proporciona la capacitat d'interpretar scripts escrits en el llenguatge Lua i que fan ús de llibreries especialitzades en l'automatització de tasques de descoberta i enumeració de xarxa, d'escaneig de ports/SOs/vulnerabilitats/backdoors i fins i tot d'explotació de vulnerabilitats.

De fet, el propi Nmap incorpora "de sèrie" un conjunt d'scripts ja prefabricats llestos per fer servir (per saber on es troben ubicats, es pot executar la comanda *locate *.nse*, per exemple (a Fedora estan dins de la carpeta "/usr/share/nmap/scripts"). Concretament, per fer-ne ús d'aquests scripts podem afegir alguns dels següents paràmetres a la comanda *nmap -Pn -sV -p nºportAProvar x.x.x.x* :

--script tipusScript, unaltreTipus,... : Executa tots els scripts prefabricats que siguin del tipus indicat. Els tipus predefinits són:

discovery : Scripts dissenyats per descobrir més informació sobre la xarxa indicada
broadcast : Scripts dissenyats per trobar nous hosts a la xarxa

vuln : Scripts dissenyats per trobar vulnerabilitats al host indicat
auth : Scripts dissenyats per trobar vulnerabilitats al host indicat relacionades amb diversos mètodes d'autenticació
dos : Scripts dissenyats per trobar vulnerabilitats a possibles a atacs DoS
fuzzer : Scripts dissenyats per trobar vulnerabilitats a atacs "fuzzing" (és a dir, per saber com respón a entrades inesperades/aleatòries per part del client)
malware : Scripts dissenyats per detectar la presència de malware al host indicat

brute : Scripts dissenyats per provar contrasenyes per força bruta contra el host indicat
exploit : Scripts dissenyats per explotar una vulnerabilitat concreta al host indicat

external : Categoria genèrica que indica que l'script envia tràfic a un tercer (un SGBD...)
intrusive : Categoria genèrica que indica que l'script pot afectar greument el host
safe : Categoria genèrica que indica que l'script no afectarà al funcionament del host

default : Selecció d'scripts més comuns. Equivalent a escriure el paràmetre *-sC*

--script nomScript,unaltreScript,... : Executa l'script/s concret/s indicat/s. Es poden escriure comodins ("*") per indicar varis scripts a la vegada. Si algun d'aquests scripts necessités d'algun paràmetre per funcionar, el seu nom<->valor respectiu es pot indicar amb el paràmetre addicional *--script-args nom1=valor1,nom2=valor2,...* (o bé *--script-args-file /ruta/fitxer* , on "/ruta/fitxer" representa un fitxer on estan escrits les parelles nom<->valor necessàries)

--script-help nomScript : Mostra l'ajuda per l'script concret indicat (funcionalitat, ús, trucs...). La llista completa de tots els scripts oficials i la seva respectiva pàgina d'ajuda es pot trobar a https://nmap.org/nsedoc

--script-updatedb : Actualitza els scripts disponibles, incorporant-ne de nous si n'hi hagués (bé perquè els haguem afegit nosaltres manualment dins de la carpeta d'scripts o bé perquè s'hagin afegit al repositori remot oficial).

NOTA: Existeix un script de tercers molt interessant anomenat "vulnscan" (https://github.com/scipag/vulscan), que ve acompanyat de tot un conjunt de bases de dades de vulnerabilitats (obtingudes de diferents butlletins) i que s'encarrega de repassar-les per tal de convertir el Nmap en tot un escanejador de vulnerabilitats completíssim.