

Network Scanning: Tecniche & Politiche

Gruppo 4

Cos'è il Network Scanning ?

E' una tecnica utilizzata per analizzare i computer presenti su una rete.

La utilizzano gli amministratori di sistema per individuare quali host sono attivi in un certo istante e come questi sono configurati

È il primo passo per la messa in “sicurezza” della propria rete.

Perchè fare Networking Scanning ?

- Analisi preventiva di una rete (es. sistemi operativi, servizi attivi e porte aperte in tutti gli host di una rete)
- Individuazione di eventuali “buchi” da sfruttare per eventuali intrusioni (sapendo i servizi che sono attivi e conoscendone i bug si può decidere di chiudere quel servizio oppure applicare un bug fix)

Cos'è il Network Scanner ?

Un Network Scanner è uno strumento che assolve al compito, appunto, di scansionare una rete.

Un amministratore di sistema o anche un singolo utente, possono usare tali programmi per testare la sicurezza del proprio sistema, adottando quindi le opportune contromisure.

Strumenti

- Nmap (che vedremo in questa dispensa)
- Satan
- Nessus

NMAP 4.01



CARATTERISTICHE DI NMAP

- Nmap (“Network Mapper”) è uno strumento open source per la network exploration ed è disponibile per tutti i sistemi operativi.
- È stato progettato per scansionare rapidamente reti di grandi dimensioni, ma è indicato anche per l'utilizzo verso singoli host.
- Molti sistemisti e amministratori lo trovano utile per tutte le attività giornaliere come ad esempio l'inventario delle macchine presenti in rete e per monitorare gli host e il loro uptime.

CARATTERISTICHE DI NMAP

- Nmap è un software freeware distribuito con licenza GNU GPL da Insecure.org.
- Creato per effettuare port scanning: individuare porte aperte e servizi disponibili su un computer bersaglio.
- Utilizzando la tecnica del “fingerprinting” è in grado di ipotizzare quale sistema operativo sia utilizzato dal computer bersaglio.

CARATTERISTICHE DI NMAP

- Utilizza i pacchetti IP per ottenere informazioni come:
 - gli host presenti su una rete;
 - i servizi che tali host rendono disponibili;
 - il sistema operativo presente sulla macchina;
 - i tipi di firewall ed altre.

CARATTERISTICHE DI NMAP

- Funzionamento da Linea di Comando
(necessari i privilegi di root per poter utilizzare tutte le opzioni di NMAP)
- Funzionamento con una GUI
(versioni per OSX, Linux, Windows)

Per l'installazione del pacchetto si veda
www.insecure.org

UTILIZZO DI NMAP (shell)

- Digitando nel terminale il comando **nmap** senza parametri si ottiene la lista di tutte le opzioni (...e sono veramente tante)
- Il prototipo di utilizzo è il seguente:
nmap -[tipi di scan] -[opzioni] <host o segmenti di rete>

SPECIFICA DELL'OBBIETTIVO

NMAP - <host o seg. di rete> (1/3)

Specifica del bersaglio:

È possibile specificare direttamente l'host name, l'indirizzo IP, i range di indirizzi IP e la subnetmask (nel formato numero di bit).

Esempio: www.dsi.unive.it , www.google.com/24, 192.168.0.1, 10.0-255.0-255.1-254

NMAP - <host o seg. di rete> (2/3)

Scansione di N host Casuali:

`-iR <num hosts>`: num host = numero di host

Se in un pomeriggio piovoso ci si trova ad essere annoiati, si puo` provare questo comando **nmap -sS -iR <quanti ne vuoi?> -p 80** per trovare in maniera casuale dei server web sui quali navigare.

Esclusione di certi host:

`--exclude <host1[,host2][,host3],...>`

NMAP - <host o seg. di rete> (3/3)

Accesso a liste su file:

E' possibile inoltre specificare un file dal quale prelevare i dati:

-iL <inputfilename>: Lista di hosts/networks

--excludefile <exclude_file>: Lista di host esclusi dalla scansione

OPZIONI DI SCANSIONE

Host Discovering (1/8)

Ciò che rende un host interessante dipende in larga misura dalle motivazioni della scansione, pertanto Nmap offre una notevole varietà di opzioni per la customizzazione delle tecniche usate.

Host Discovering (2/8)

-sT per CONNECT SCAN.

Utilizza una connessione completa TCP.

Svantaggi: facilmente rilevabile dal sistema che lo subisce.

-sS per SYN SCAN.

Non utilizza una connessione completa TCP.

Svantaggi: utilizzabile solo da root.

Host Discovering (3/8)

-sL (List Scan)

La list scan è una forma banale di host discovery che semplicemente elenca ogni host delle reti specificate, senza inviare alcun pacchetto agli host obiettivo.

Host Discovering (4/8)

-sP (Ping Scan)

Questa opzione indica a Nmap di effettuare solo un ping scan e di mostrare gli host che hanno risposto. Sapere quanti host sono attivi è più utile rispetto ad una semplice list scan di ogni indirizzo IP e nome di host.

Host Discovering (5/8)

-PS [portlist] (TCP SYN Ping)

Questa opzione invia un pacchetto TCP vuoto con il flag SYN attivo. La porta di destinazione di default è la 80 ma in questo caso se ne può specificare un'altra oppure una lista separata da virgola (ad esempio -PS22,23,25,80...).

Il flag SYN indica al sistema remoto che si sta tentando di stabilire una connessione.

Host Discovering (6/8)

Se la porta fosse aperta, il destinatario effettuerebbe il secondo passo della connessione TCP a tre vie (3-way-handshake) rispondendo con un pacchetto TCP SYN/ACK.

Nmap interromperà la connessione inviando un pacchetto RST dal kernel della macchina.

Non interessa se la porta è aperta o chiusa ma che l'host sia disponibile e risponde alle connessioni.

Host Discovering (7/8)

-PA [portlist] (TCP ACK Ping)

Il ping TCP ACK e` molto simile al ping SYN appena discusso. La differenza consiste nel fatto che viene usato il flag TCP ACK al posto del SYN. Un tale pacchetto ACK finge di confermare dei dati inviati in una connessione TCP gia` stabilita, anche se tale connessione non esiste. In questo modo un host remoto rispondera` sempre con un pacchetto RST, svelando cosi` la propria esistenza e il fatto che sia attivo.

Host Discovering (8/8)

-PE; -PP (ICMP Ping Types)

Nmap può, oltre a mandare i pacchetti standard come il famoso programma ping anche la "echo request" (-PE) e la "timestamp request" (-PP) sempre allo scopo di sapere se l'host è attivo

Port Scanning (1/3)

Inizialmente NMAP nasce come port scanner e tale tuttora è il suo scopo.

Il semplice comando `<nmap target>` effettua una scansione su più di 1660 porte TCP sull'host target.

Port Scanning (2/3)

NMAP Divide le porte in sei categorie o stati:

- open (aperta)
- closed (chiusa)
- filtered (filtrata)
- unfiltered (non filtrata)
- open|filtered (aperta|filtrata)
- closed|filtered (chiusa|filtrata).

Port Scanning (3/3)

- **-p <lista porte>**

E' possibile specificare l'elenco delle porte da controllare sugli host target

Service e Version Detection (1/4)

Utilizzando Nmap e dirigendo la scansione su una macchina remota è possibile scoprire quali porte sono aperte e utilizzando il suo database di circa 2200 servizi noti, contenuto nel file nmap-services, sarà in grado di indicare di quale servizio si tratta.

Service e Version Detection (2/4)

Il database contenuto nel file `nmap-service-probes` contiene istruzioni per interrogare i vari servizi e per interpretarne le risposte.

Nmap cerca quindi di determinare di che servizio si tratta (Es.: ftp, ssh, telnet, http), di che applicazione (Es.: ISC, Bind, Apache httpd, Solaris telnetd), la versione, l'hostname, il tipo di device, la famiglia del sistema operativo (Es.: Windows, Linux...) e altri dettagli.

Service e Version Detection (3/4)

Quando Nmap riceve delle risposte da un Servizio ma non e` in grado di trovarne una interpretazione nel suo database, visualizza una particolare "FingerPrint" e una URL per permettere di inviare quanto rilevato nel caso si conosca a priori che cosa sta effettivamente girando su quella porta.

Service e Version Detection (4/4)

- **-sV** (Version detection)
- **--allports** (Non esclude alcuna porta dal V.Det.)
- **--version_intensity <n>** (Imposta l'accuratezza del Version Scan 1<n<9)
- **--version_light** (Attiva la modalita` Light come dire **--version_intensity <2>**)
- **--version_all** (Prova ogni singolo pacchetto-sonda in ogni livello 1...9)

OS Detection (1/2)

Una delle più famose caratteristiche di NMap è la possibilità di identificare remotamente il sistema operativo di un host attraverso il "Fingerprint" dello stack TCP/IP.

Nmap invia una serie di pacchetti TCP ed UDP all'Host Remoto ed esamina ogni bit ricevuto con il suo database (nmap-os-fingerprints) contenente più di 1500 "OS Fingerprints" conosciuti e ne visualizza i dettagli se ne trova riscontro.

OS Detection (2/2)

- **-O (Enable OS detection)**

È possibile utilizzare l'opzione **-A** per attivare sia l'OS detection che il Version Detection.

Output dei Dati (1/3)

Nmap fornisce opzioni per il controllo della verbosità dell'output come anche dei messaggi di debugging. I tipi di output possono essere mandati allo standard output o a files, ai quali Nmap può accedere o sovrascrivere contenuto.

Output dei Dati (2/3)

- **-v (Aumenta il livello di verbosity)**
Aumenta il livello di verbosità, facendo in modo che Nmap stampi più informazioni riguardo allo scan in esecuzione.
- **-d [level] (Aumenta o setta il livello di debug)**
Quando anche il verbose mode non fornisce dati a sufficienza, è disponibile la modalità debugging

Output dei Dati (3/3)

- **-oN <filespec> (Normal output)**
Richiede che il normal output venga inviato al dato file <filespec>
- **-oX <filespec> (XML output)**
Richiede che l'output XML sia inviato al dato file <filespec>

Esempi di Utilizzo (1/3)

- Tutte le porte di un host ?
`nmap 127.0.0.1`
- Tutte le porte di un insieme di host ?
`nmap 192.168.1.2/24 (submask:255.255.255.0
=> 8*3=24)`
- Aumentare il livello di dettaglio ?
`nmap -v 127.0.0.1`
- Quali host sono attivi in una LAN ?
`nmap -sT 192.168.0.0/24`

Esempi di Utilizzo (2/3)

- Quale O.S usa un host ?
`nmap -O 127.0.0.1`
- Che servizi sono attivi in un host ?
`nmap -sV 127.0.0.1`
- Tutti i servizi attivi e il O.S. di un host ?
`nmap -sV -O 127.0.0.1`
- Salvare il risultato di una scansione in XML ?
`nmap -O -sV -oX myscan.xml 192.168.1.1/24`

Esempi di Utilizzo (3/3)

- Scansionare 100 host a caso nella porta 80 ?
`nmap -iR 100 -p 80`

GUI per Nmap 4.01

- NMAPGUI (Linux e lo trovate su source forge)
- XNmap (OSX)
- NMapFE (OSX)
- NMapView (Win)

Ogni GUI non fa altro che eseguire NMAP componendo la stringa delle opzioni tramite interfaccia grafica.

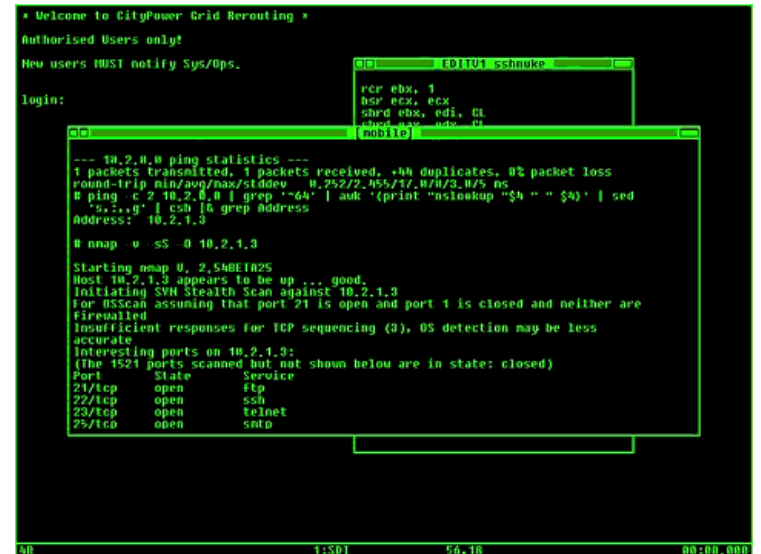
È legale ?

E' come andare a vedere se un negozio ha la porta aperta...non è mica reato ! Se poi si prova a forzare la serratura perchè questa è chiusa/socchiusa le cose cambiano.

Comunque è sempre importante chiedere l'autorizzazione per effettuare un port scanning (o un network mapping) onde evitare qualsiasi tipo di problema.

Linkografia e Filmografia

- <http://www.insecure.org>
- Nel film Matrix Reloaded, Trinity usa Nmap per penetrare nel sistema della centrale elettrica, tramite la forzatura dei servizi SSH e il bug CRC32 (scoperto nel 2001).



```

Welcome to CityPower Grid Rerouting *
Authorized Users only
New users MUST notify Sys/Ops.

login:
--- 10.2.0.0 ping statistics ---
1 packets transmitted, 1 packets received, 0% duplicates, 0% packet loss
round-trip min/avg/max/stddev = 0.252/2.455/17.010/3.075 ms
# ping -c 2 10.2.0.0 | grep '^64' | awk '{print "nslookup "$4 " " $4}' | sed
's/,g' | cut -f6 | grep Address
Address: 10.2.1.3

# nmap -u -sS -O 10.2.1.3
Starting nmap @ 2:50E1A2S
Host 10.2.1.3 appears to be up ... good.
Initiating SYN Stealth Scan against 10.2.1.3
for OSScan assuming that port 21 is open and port 1 is closed and neither are
firewalled
Insufficient responses for TCP sequencing (3), OS detection may be less
accurate
Interesting ports on 10.2.1.3:
(The 1521 ports scanned but not shown below are in state: closed)
Port      State  Service
21/tcp    open   ftp
22/tcp    open   ssh
23/tcp    open   telnet
25/tcp    open   smtp

```

images.insecure.org/nmap/images/matrix/