NMAP

La scansione delle porte è un passaggio obbligato per studiare la sicurezza di un Sistema Informatico.

Analizziamo Nmap, uno degli strumenti più completi nel suo genere.

Nmap è uno strumento tanto versatile quanto potente che presenta come punto negativo soltanto una relativa difficoltà di utilizzo.

Lanciando il comando di help dalla console si può rimanere un po' disorientati davanti alle numerose opzioni che sono state implementate in questo strumento dal suo sviluppatore, Fyodor. Nmap, infatti, non offre soltanto le funzionalità di base di un qualsiasi port scanner ma comprende anche altre tecniche di scansione che ci forniscono informazioni più dettagliate sull'host o sulla rete analizzati.

Prima di vedere perché NMap è considerato uno strumento potente dagli "addetti ai lavori", è necessario analizzare le diverse tecniche di scansione. Uno dei pionieri nell'implementazione di queste tecniche di scansione è Fyodor, che ne ha implementate un buon numero anche nel suo software. Il **port scanning** (o

scansione delle porte) consiste nella connessione alle porte TCP e UDP dell'obiettivo analizzato. Esistono differenti modalità di scansione. Andiamo ad analizzare in dettaglio alcune di queste.

Le tecniche di scansione

Tcp connect scan: Vengono inviati dei pacchetti ad una determinata porta secondo una procedura a tre fasi, **SYN, SYN/ACK e ACK**. Questa tecnica è la più semplice da portare a termine ma anche quella più facile da

intercettare. Se non specifichiamo nessun parametro dalla riga di comando, Nmap porterà a termine questo tipo di scansione perché questa è la **tecnica impostata di default.**

Tcp syn scan: con questa tecnica di scansione non viene realizzata una connessione completa. Infatti viene inviato un pacchetto SYN alla porta del nostro obiettivo e si attende una risposta. In base al pacchetto che riceveremo, possiamo capire se la porta è in stato di listening o meno. Se infatti la risposta sarà SYN/ACK la porta è in ascolto, mentre se riceviamo un pacchetto RST/ACK la porta non è in ascolto. Il sistema dell'attacker risponderà con RST/ACK, in modo che la connessione non venga mai completata. Questa tecnica consente all'attaccante di muoversi in modo più discreto, evitando di lasciare la sua "firma" nel file di log. L'opzione da digitare per effettuare questa scansione è **–sS.**

Tcp Fin scan: utilizzando questa tecnica invieremo un pacchetto di tipo FIN sulla porta dell'obiettivo. Il sistema sottoposto a scansione dovrebbe rispondere con RST per tutte le porte che non sono in ascolto. Di solito questa tecnica **funziona in ambiente Unix**. In Nmap questa scansione viene implementata con l'opzione **–sF.**

Tcp windows scan: analizzando la dimensione della finestra TCP, con questa tecnica di scansione è possibile individuare sia le porte in ascolto, sia quelle filtrate in alcuni sistemi,come in FreeBSD.

Tcp rpc scan: questa tecnica viene utilizzata per riconoscere e identificare le porte RPC (acronimo che sta per Remote Procedure Call) insieme al loro numero di versione. In Nmap possiamo realizzare una scansione di questo tipo con l'opzione **–sR.**

Udp scan: questa tecnica prevede l'invio di un pacchetto UDP sulla porta del nostro obiettivo. Se questo risponde con un messaggio di errore ci indica che la porta è chiusa. Ovviamente se non riceveremo tale messaggio possiamo facilmente intuire che la porta da noi analizzata sia aperta. Questa tecnica viene eseguita sfruttando il protocollo UDP, quindi il processo di scansione sarà estremamente lento ed inoltre non ci garantisce risultati affidabili. Nmap supporta anche la scansione UDP, inserendo come parametro l'opzione **–sU.**

Un po' di pratica

Oltre a queste tecniche esistono altri tipi di scansione supportati da Nmap, che senza dubbio lo differenziano dai tanti software simili che si trovano sulla rete. Dopo avere installato il port scanner (alcune distro Linux già lo includono), digitate il comando:

nmap - -help

A questo punto vedrete comparire una serie di comandi che vi permetteranno di utilizzare le più svariate tecniche di scansione. È possibile effettuare la **scansione TCP** con connessione semplicemente digitando

nmap <indirizzoIP-host>

Infatti, questa è la tecnica di scansione di default e quindi è possibile omettere l'opzione relativa a questo tipo di scansione.

-oN invece sarà possibile salvare il risultato delle nostre scansioni in un file da noi specificato, mentre inserendo come parametro **–oM** l'output del programma sarà inserito in un file di testo

formattato, cioè i campi saranno separati da caratteri di tabulazione. Quest'ultimo comando può essere di grande aiuto quando si effettuano scansioni di un certo range di IP, per cui la quantità di dati andrà formattata in modo da essere leggibile più chiaramente. Vediamo quindi come possiamo utilizzare questo parametro dalla riga di comando:

nmap <indirizzoIP-host>/ 24 –oM risultati_scan.txt

In questo caso il risultato della scansione del range IP da <indirizzoIP-host> a <indirizzoIP-host+24> sarà salvato nel file di testo, in modo da poter essere consultato anche dopo avere terminato le ricerche.

Ingannare i firewall

Se inoltre non si riuscisse a effettuare un port scanning in una macchina perché questa utilizza come firewall un dispositivo di filtro dei pacchetti, si **possono tranquillamente spezzare i pacchetti** in più frammenti. L'opzione che ci permette di utilizzare tale tecnica è il parametro **–f**. In pratica, questa opzione suddivide l'intestazione TCP su più pacchetti,

quindi un sistema IDS (Intrusion Detection System) avrà difficoltà a riconoscere la scansione.

Questa opzione tuttavia non ci offre un elevata discrezione. Infatti i moderni firewall accodano i frammenti di pacchetti IP prima di esaminarli. Anche in questo caso, però, Nmap fornisce opportunità di “camuffamento” senza dubbio più discrete rispetto a quella precedente. L’opzione che ci permette di confondere l’host obiettivo della nostra scansione è –**D (decoy)**. Questo termine

tradotto letteralmente vuol dire “inganno” ed effettivamente rispecchia benissimo la tipologia di scansione che viene usata specificando questa opzione dalla riga di comando. Utilizzando questa tecnica, infatti, verranno lanciate una **serie di scansioni fasulle insieme a quella vera**. In questo modo il sistema che stiamo analizzando risponderà sia agli indirizzi contraffatti sia a quello vero.

La difficoltà dell’host target sarà quindi quella di risalire a tutte le scansione e di riuscire a individuare quella vera tra tutte quelle false. Bisogna fare attenzione a che gli indirizzi fasulli siano effettivamente attivi, altrimenti il sistema obiettivo si troverà sommerso da pacchetti SYN e questo potrebbe causare un DoS (Denial of Service).

Eccovi un esempio dell’utilizzo di questa tecnica:

```
nmap 192.124.1. 1 –D 10.1.1.1
```

Questa opzione è assente nella maggior parte dei port scanner e rende Nmap uno strumento davvero unico nel suo genere, tanto da farlo spesso catalogare come tool malizioso invece che come legittimo strumento di analisi di una rete.

Raccolta di informazioni

Un’altra opzione interessante di Nmap è quella che ci permette di individua- re il sistema operativo che utilizza l’host che stiamo analizzando. Sfruttando alcune caratteristiche proprie dei pacchetti ricevuti, come per esempio la dimensione della finestra iniziale TCP, Nmap riesce ad i**ndividuare con precisione il sistema operativo utilizzando l’opzione –O**. Se nella macchina obiettivo è aperta soltanto la porta 80 possiamo risalire con alta precisione al tipo di sistema operativo utilizzato. Eccovi un esempio

```
nmap –p80 –O 192.124.1.1
```

Attraverso l’opzione **–p possiamo specificare la porta da andare ad analizzare** e con l’opzione –O risaliamo invece al sistema operativo

Raccomandazioni finali: attenti all’illecito!

È bene ricordare ai più ”distratti” che le tecniche di port scanning sono al limite della legalità (tuttora la questione è controversa). Infatti, se in pochi avreb- bero da obiettare se qualcuno effettuasse la scansione delle porte di una classe ristretta di indirizzi IP e su porte che corrispondono ai servizi più comuni (come ad esempio la 25, 110, 80...), è davvero difficile giustificare legalmente qualcuno che effettua scansioni a tappeto su un

ampio range di IP, magari intento a individuare proprio le porte utilizzate da alcuni trojan. Ovviamente, l'utilizzo di nmap per verificare e analizzare la propria macchina o la propria rete è perfettamente lecito. Per esempio, potrebbe essere usato sul proprio PC per vedere se è veramente sicura o per verificare di avere configurato in modo ottimale il vostro nuovo firewall. Oppu- re, un amministratore di rete potrebbe effettuare una scansione delle macchine alla ricerca di porte utilizzate dai trojan, e ripulire la macchina in questione.