

Università degli studi di Salerno

Facoltà di Scienze MM. FF. e NN.

Corso di laurea in Informatica

Progetto di

Sistemi di elaborazione dell'informazione (Sicurezza su Reti)

Nmap (Network Mapper)

Prof. Alfredo De Santis

Coppola Mileva
Dell'Aversano Marco
Morzillo Alessio
Rago Aniello

Anno Accademico 2003-2004

Indice

→ Introduzione

■ Scanner di vulnerabilità

■ Nmap

caratteristiche, installazione, esempi di utilizzo

Introduzione -sicurezza-

- L'espansione della rete ha portato all'aumento dei tentativi d'intrusione che hanno inciso sul fattore sicurezza della rete stessa.
- Secondo il Computer Security Institute nel 2004 le 494 società esaminate hanno subito danni per circa 142 milioni di dollari.
- Causa principale di queste perdite economiche è stata la vulnerabilità delle proprie reti o dei propri sistemi.



Introduzione -vulnerabilità-

- Debolezza di un sistema che può essere utilizzata per causare danni.
- La vulnerabilità di un sistema può essere rappresentata da:
 - Disastri naturali
 - Errori umani
 - Buchi software o hardware
 - Attacchi



Introduzione -vulnerabilità-

- Le vulnerabilità sono catalogate dal SANS Institute attraverso dei codici chiamati CVE (Common Vulnerabilities and Exposures).
- Tra le principali vulnerabilità troviamo, ad esempio:
 - Sistemi di autenticazione
 - Browser Internet Explorer
 - Condivisioni con NETBIOS
 - Condivisioni Peer-to-Peer
 - Servizi in chiaro (telnet, FTP,...)

Introduzione -tipi di attacco-

- Probing e scanning
- Attacchi alle password
- Intercettazione di pacchetti
- Compromissione di account
- Denial of Service
- Codice malizioso
- Attacchi all'infrastruttura di rete


Probing

- Con un software di probing possiamo ottenere informazioni sul sistema allo scopo di conoscere le vulnerabilità relative a:
 - amministratori e utenti della rete
 - posizione del server
 - presenza o meno di intranet
 - sistemi di rilevamento delle intrusioni
 - server dns e sua configurazione
 - indirizzi IP assegnati
 - eventuale accesso telefonico

Scanning

- Con un software di scanning possiamo rilevare quali sono le macchine attive e raggiungibili via internet e quali servizi sono disponibili, usando tecniche come:
 - il *ping sweep* (utile per rilevare se un determinato host sia attivo o meno)
 - il *portscanning* (processo di connessione a porte TCP e UDP sul sistema nel quale si vuole tentare una penetrazione al fine di determinare quali servizi siano in esecuzione o in stato di LISTENING)
 - il rilevamento del sistema operativo tramite stack TCP/IP *fingerprinting*

Prevenzione

- Come difendersi? 
- Per poter identificare le debolezze della propria rete e dei propri sistemi esistono strumenti appositi: gli **scanner di vulnerabilità**.
- Il fine è quello di evitarne uno sfruttamento da parte di utenti maliziosi.

Indice

- Introduzione

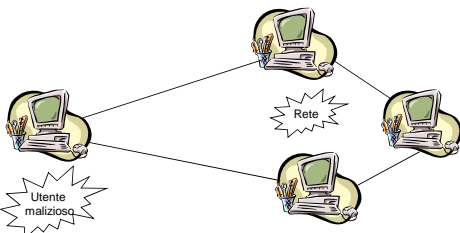
⇒ Scanner di vulnerabilità

- Nmap

caratteristiche, installazione, esempi di utilizzo

Scanner di vulnerabilità(1)

- Analizzando i tipi di software e di configurazioni presenti su una certa rete, gli scanner sono in grado di determinare i tipi di attacco che possono essere fatti ai danni della rete, consentendole di difendersi appropriatamente.



Scanner di vulnerabilità(2)

- Scanner di vulnerabilità:
 - Processo di controllo di tutti i potenziali metodi di attacco atti a manomettere la rete di un'organizzazione.
- Elementi a rischio in grado di rilevare:
 - bug delle applicazioni;
 - virus;
 - politiche deboli per il controllo degli accessi;
 - applicazioni configurate in modo non corretto.



Scanner di vulnerabilità(3)

- Alcuni dei più noti scanner di vulnerabilità sono:
 - NESSUS
 - SAINT
 - PORTSCAN
 - NMAP

Indice

- Introduzione
- Scanner di vulnerabilità

⇒ Nmap
caratteristiche, installazione, esempi di utilizzo

Nmap -introduzione-

- È fra i più potenti e diffusi scanner di vulnerabilità.
- Utilizzabile sia per prevenire attacchi sia per effettuarli.
- I principi alla base del funzionamento sono molto complessi e inavvicinabili se non si ha una buona conoscenza dei protocolli di rete e dei sistemi operativi.
- Molto più semplice, ma non banale, risulterà l'uso di questo software.

Nmap -introduzione-

- Nmap è presente sulla rete ormai da anni e sono state rilasciate varie versioni.
- Quella di cui ci occupiamo è la 4.01, ma è possibile che nel frattempo sia stata pubblicata una nuova versione.
- Dalla versione 4.0 Nmap può girare anche su Windows (inizialmente solo su Linux).



Nmap -introduzione-

- 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.
- Utilizza la tecnica del *fingerprinting*: è in grado di ipotizzare quale sistema operativo sia utilizzato dal computer bersaglio.



Porte Aperte	Xx Xxx Xxxx ...
Sistema Operativo	Yyy

Nmap -introduzione-

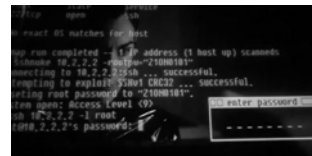
- Nmap è divenuto uno degli strumenti praticamente indispensabili della "cassetta degli attrezzi" di un amministratore di sistema, ed è usato per test di penetrazione e compiti di sicurezza informatica in generale.

Nmap -introduzione-

- Nmap può essere utilizzato sia dagli amministratori di sistema che dai cracker o script kiddies:
 - gli amministratori di sistema possono utilizzarlo per verificare la presenza di applicazioni server non autorizzate;
 - i cracker possono usarlo per analizzare i loro bersagli.
- **ATTENZIONE !!!** Nmap non può danneggiare l'hardware, ma può bloccare, in alcune condizioni, un sistema, fino a renderne necessario il riavvio. Per cui non deve essere usato contro sistemi che gestiscono servizi necessari.

Nmap -introduzione-

- 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).



Nmap -caratteristiche-

- Nmap (acronimo di "Network Mapper") è uno strumento open source utilizzato principalmente per l'esplorazione delle reti e il security auditing.
- Utilizza i pacchetti IP per ottenere informazioni come:
 - gli host presenti su una rete;
 - i servizi che tali host rendono disponibili;
 - i sistemi operativi presenti sulla macchina;
 - i tipi di firewall ed altre.
- Utilizzato anche da amministratori di rete per task secondari come il monitoraggio di host o il testing dei tempi di risposta dei servizi.

Nmap -caratteristiche-

- Flessibile
- Potente
- Portabile
- Facile
- Free
- Ben documentato
- Acclamato
- Popolare

Nmap -caratteristiche-

- L'output dell'applicazione è solitamente una lista di target osservati, con informazioni supplementari che si differenziano in base alle opzioni specificate.
- I risultati sono visualizzati all'interno di una tabella delle porte in cui vengono specificate il numero della porta e il protocollo, il nome e lo stato del servizio.
- Lo stato del servizio può essere:
 - open
 - filtered
 - closed
 - unfiltered

Nmap -esempio-

- "A" : per rilevare il tipo e la versione del sistema operativo che gira sulla macchina target.
- "T4" : per effettuare una scansione delle porte più veloce.
- "10.0.0.124" : indirizzo della macchina target.

```

C:\Documents and Settings\Spok\Desktop\Nmap 4.01\nmap-4.01\nmap -n -T4 10.0.0.124
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-04-11 14:50 ora solare Europa occidentale
Interesting ports on 10.0.0.124:
(1668 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 4.3p1
telnet    open  telnetd        0.17
Nmap finished: 1 IP address (1 host up) scanned in 119.328 seconds
C:\Documents and Settings\Spok\Desktop\Nmap 4.01\nmap-4.01_
  
```

Indice

- Introduzione
- Scanner di vulnerabilità

→ Nmap

caratteristiche, installazione, esempi di utilizzo

Nmap -installazione-

- Controllare se Nmap è già installato nel proprio sistema (sui sistemi UNIX eseguire il comando `nmap -version` da terminale).
- Se Nmap è presente e si trova nella propria \$PATH, dovrebbe comparire la seguente schermata di output:

```

$ nmap -version
nmap version 3.95 ( http://www.insecure.org/nmap )
$
  
```

- Se Nmap non è presente sul sistema (o la propria \$PATH non è settata correttamente), verrà mostrato un messaggio di errore: "nmap: Command not found".

Nmap -installazione-

- Per scaricare i sorgenti o i binari di Nmap (o di NmapFE) basta semplicemente visitare il sito ufficiale Insecure.Org.



- Il codice sorgente è distribuito sottoforma di files compressi (Bzip2 e Gzip).
- I binari sono disponibili sia per Windows che per Linux (formato RPM).
- Il link per il download è:
<http://www.insecure.org/nmap/download.html>.

Nmap -installazione-

- Nmap è nato come un'applicazione utilizzabile tramite una shell UNIX e, più recentemente, tramite il prompt dei comandi di Windows.
- Solo di recente sono state create diverse interfacce grafiche per gli utenti che preferiscono una GUI piuttosto che digitare semplicemente i comandi da tastiera.
- La GUI più nota per i sistemi UNIX è NmapFE.

Nmap -Windows-

Installare Nmap tramite file binari compressi (.zip):

- Leggere il [Nmap Win32 support page](#) per gli ultimi aggiornamenti;
- Scaricare i binari in formato .Zip dal sito <http://www.insecure.org/nmap/download.html> ;
- Decomprimere il file .zip nella directory in cui si vuole installare Nmap;
- Nmap richiede la libreria WinPcap packet capture, reperibile al sito <http://www.winpcap.org>, in forma di eseguibile autoinstallante.

Nmap -Windows-

Eseguire Nmap:

- Assicurarsi di essersi loggati con privilegi di amministratore;
- Aprire il prompt dei comandi di Windows;
- Raggiungere la directory in cui si è installato Nmap;
- Eseguire nmap.exe.

```

C:\cmd.exe (running as PLAYGROUND\root)
E:\>cd nmap
E:\nmap>nmap -h -T4 scanme.insecure.org
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2003-12-20 03:20 Pacific
Standard Time
Interesting ports on scanme.insecure.org (205.217.153.55):
(The 1652 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
23/tcp    open  nmap     Nmap 3.48
25/tcp    open  smtp     ISC Binc 4.7.1
80/tcp    open  http     Apache/2.0.39 ((Ubuntu) mod_perl/1.99.07-dev Perl/5.00
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.21.15.2
OS details: Linux Kernel 2.4.8 - 2.5.28
uptime 215.653 days since Sat May 21 12:48:35 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 54.588 seconds
E:\nmap>
  
```

Nmap -Unix-

- Scaricare l'ultima versione di Nmap nel formato .tar.bz2 oppure .tgz;
- Decomprimere i file scaricati con un comando come:
bzip2 -cd nmap-VERSION.tar.bz2 | tar xvf -;
- Andare nella directory creata: **cd nmap-VERSION;**
- Configurare il sistema: **./configure;**
- Costruire Nmap: **make;**
- Si faccia accesso al sistema in modo da avere i privilegi necessari: **su root;**
- Installare Nmap, i file di supporto, etc.: **make install.**
- Si lanci **./configure --help** per avere una lista riassuntiva di opzioni.

Nmap -rimozione-

- Per aggiornare Nmap all'ultima versione, è possibile utilizzare l'opzione "**upgrade**" fornita dalla maggior parte dei binary package managers.
- Per rimuovere Nmap è sufficiente eseguire il comando :
rpm -e nmap nmap-frontend
da root.

Nmap -Utilizzo da linea di comando-

- E' il modo più efficiente e veloce di usare Nmap (solo apparentemente più difficile da usare).
- Per utilizzare tutte le funzionalità di Nmap si deve essere loggati come root.

Nmap -Utilizzo da linea di comando-

- Tramite le svariate opzioni è possibile effettuare delle operazioni di scansione di interi sistemi o di singoli host, ottenendo informazioni più o meno dettagliate.
- Quando viene eseguito Nmap senza argomenti, viene stampato un riassunto delle opzioni che aiuta l'utente a ricordare le opzioni più comuni.

Nmap -Utilizzo da linea di comando-

- Il prototipo di utilizzo è il seguente:

> **nmap -[tipi di scan] -[opzioni] <host o segmenti di rete>**

Nmap -esempio(1)-

- Per verificare una rete dall'interno basterà digitare:

> **nmap -sT -PI 10.0.0.0/24**

- effettua lo scanning della rete 10.0.0.0 con subnetmask 255.255.255.0;
- pingando gli IP con pacchetti icmp echo (-PI);
- analizza le porte tramite connessioni complete (-sT).

Nmap -esempio(2)-

- L'output prodotto potrebbe essere:

Starting nmap 4.01 (<http://www.insecure.org/nmap/>) at 2006-11-10 21:29 CEST
Host 10.0.0.0 seems to be a subnet broadcast address (returned 2 extra pings). Skipping host.

Nmap :

- sta per analizzare il segmento di rete identificato tramite l'indirizzo di broadcast e la netmask;
- ha identificato, tramite i ping, 2 host attivi.

Nmap -esempio(3)-

- Interesting ports on 10.0.0.2:

(The 1658 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
80/tcp	open	http
255/tcp	open	unknown

Nmap:

- ha analizzato il primo host 10.0.0.2;
- ci informa che risultano aperte solo 2 porte: la 80 tipicamente dedicata ai servizi http e la 255 sconosciuta.

Nmap -Utilizzo tramite interfaccia grafica-

- Quello nella figura è il pannello che si presenta al momento del lancio dell'applicazione.
- È semplice, ma molto funzionale.



Nmap -Utilizzo tramite interfaccia grafica-

- **Scan Type**
Consente di scegliere la "politica di attacco" ai vari host individuati.
- **Scanned Ports**
Consente di decidere quale intervallo di porte esaminare.
- **Scan Extensions**
Consente di richiedere ad Nmap di fornire informazioni supplementari, alcune molto utili.

Nmap -Utilizzo tramite interfaccia grafica-

- Tramite il tab Discover è possibile selezionare il tipo di sondaggio da effettuare per identificare gli host attivi, cioè il tipo di "ping" che si preferisce.
- È molto utile quando si vuole analizzare un segmento di rete, o comunque una lista consistente di host.



Nmap -Utilizzo tramite interfaccia grafica-

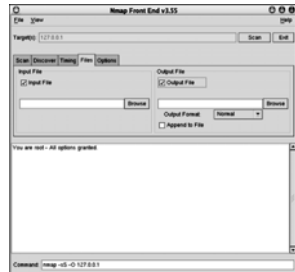
- Nel tab Timing è possibile regolare l'atteggiamento di Nmap, inteso come impegno della rete, e i time out.
- È fondamentale sia allo scopo di non farsi scoprire che di preservare la rete da malfunzionamenti.



Nmap

-Utilizzo tramite interfaccia grafica-

- Nel tab **Files** si possono indicare:
 - gli indirizzi di file per l'input in cui stoccare i nomi;
 - gli IP degli host da verificare;
 - gli indirizzi di file di output in cui conservare i risultati degli scan in vari formati.



Nmap

-Utilizzo tramite interfaccia grafica-

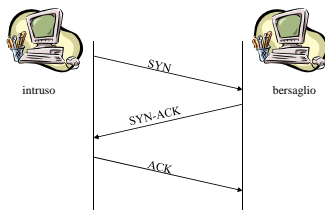
- In questo tab si possono impostare varie opzioni relative alla:
 - risoluzione inversa dei nomi (da IP a nome);
 - quantità di informazioni fornite in output;
 - identificazione della fonte dello scan;
 - altre più complesse.



Nmap -tipi di scan-

-sT per CONNECT SCAN.

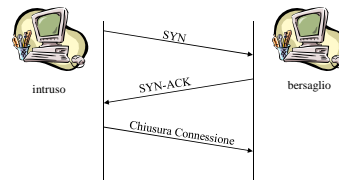
- Utilizza una connessione completa TCP.
- **Svantaggi:** facilmente rilevabile dal sistema che lo subisce.



Nmap -tipi di scan-

-sS per SYN SCAN.

- Non utilizza una connessione completa TCP.
- **Svantaggi:** utilizzabile solo da root.



Nmap -tipi di scan-

-sF -sX -sN per FIN SCAN, XMAS SCAN, NULL SCAN.

- Particolarmente difficili da rilevare; penetrano facilmente i firewall.
- **Svantaggi:** risultati dubbi.

-sP per PING SWEEP.

- Serve solo per scoprire quali host sono attivi su un segmento di rete.
- Usarlo solo se non si vuole effettuare uno scan delle porte.

-sU per UDP SCAN.

- Molto raffinato.
- Utile anche al difensore.
- **Svantaggi:** molto lento.

Nmap -tipi di scan-

-sA per ACK SCAN.

- Molto raffinato e utile.
- È possibile analizzare reti protette da semplici filtri, cosa non possibile con gli scan di tipo -sT e -sS.

-sW per WINDOW SCAN.

- Simile al precedente.

-sR per RPC SCAN.

- Funziona in combinazione con gli altri tipi di scan.
- Cerca di stabilire se vi è in ascolto un servizio RPC e la versione.

-sV per VERSION SCAN.

- Determina il nome e la versione degli applicativi in ascolto su una porta.

Indice

- Introduzione

- Scanner di vulnerabilità

⇒ Nmap

caratteristiche, installazione, esempi di utilizzo

Nmap -esempi-

(1) **nmap -v scanme.nmap.org**

- osserva tutte le porte TCP riservate sulla macchina scanme.nmap.org ;
- "-v" abilita la modalità "verbose".

(2) **nmap -sS -O scanme.nmap.org/24**

- lancia uno scan SYN contro ogni macchina che appartiene all'insieme delle 255 macchine sulla rete di classe C dove Scanme risiede ;
- cerca di determinare quale Sistema Operativo sia presente su ogni host che attivo in quel momento;
- richiedi privilegi di root.

Nmap -esempi-

(3) **nmap -v -iR 100000 -P0 -p 80**

- sceglie 100.000 host casuali e effettua lo scan della porta 80 (web server);
- enumerazione degli host disabilitata tramite l'opzione -P0.

(4) **nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20**

- scansiona 4096 indirizzi IP per ogni web server (senza pingarli);
- salva l'output in formato "greppabile" e XML.

Nmap -esempi-

(5) **nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127**

- lancia l'enumerazione degli host ed uno scan TCP per la prima metà dei 255 possibili 8 bits della subnet nello spazio degli indirizzi di classe B 198.116.;
- testa se i sistemi abbiano in esecuzione sshd, DNS, pop3d, imapd, oppure porta 4564;
- per ogni porta trovata aperta, viene eseguito il rilevamento della versione per determinare quale applicazione è in ascolto.

Bibliografia

- Sito ufficiale di Nmap e sottosezioni:
 - [<http://www.insecure.org>] - Home Page
 - [<http://www.insecure.org/nmap/>] - Introduzione all'uso di Nmap
 - [<http://www.insecure.org/nmap/ldlescan.html>] - Informazioni sull'ldlescan
 - [<http://www.insecure.org/nmap/data/nmap.xml>] - Foglio di stile XSL
- È possibile consultare una lista delle modifiche rispetto alla versione che si possiede semplicemente visitando l'indirizzo:
 - [<http://www.insecure.org/nmap/changelog.html>]
- Il codice sorgente è distribuito sottoforma di files compressi (Bzip2 e Gzip), mentre i binari sono disponibili sia per Windows che per Linux (formato RPM). Il link per il download di tali file è :
 - [<http://www.insecure.org/nmap/download.html>]