Strumenti per la sicurezza delle LAN

Versione 2.0 del 19 Dicembre 2005

Allo scopo di implementare un buon livello di sicurezza su una rete locale, oltre ad accertarsi della sicurezza sui singoli host [ref 1], e' sicuramente essenziale una organizzazione della LAN basata sull'uso di un **firewall** perimetrale, che puo' essere implementato sul router mediante ACL oppure con l'uso di una appliance dedicata, e che svolga una fondamentale funzione di filtro "in ingresso" alla LAN, bloccando sulla porta di casa gran parte delle minacce [2].

Oltre a cio' e' anche necessario tenere sotto controllo varie altre categorie di oggetti, quali *i protocolli che circolano sulla rete, i servizi di rete a cui sono rivolti gli accessi, le porte ben note di TCP/IP che corrispondono ai vari servizi.*
Per fare questo e' utile disporre di strumenti di analisi di traffico e di monitoraggio della rete in generale.
Gli strumenti che permettono questo tipo di controllo sulle LAN sono numerosi e molti di essi, anche alcuni fra i migliori, sono disponibili gratuitamente (freeware software).

Questo elenco include alcuni fra i piu' diffusi:

- **NAGIOS**, tool di monitoring di oggetti informatici (servizi, elaboratori o apparecchiature di rete);
- **NESSUS**, un tool per il controllo del livello di sicurezza implementato sugli elaboratori della propria rete;
- **NTOP**, un tool per l'analisi in tempo reale del traffico di rete in termini di protocollo usato e di coppie provenienza ←→ destinazione;
- **SNORT**, un tool per l'analisi in tempo reale del traffico di rete a fini di Network Intrusion Detection.

NTOP e SNORT offrono prestazioni simili, anche se non uguali, e vale sicuramente la pena di installarli entrambe. In particolare, NTOP consente sofisticate analisi di traffico, mentre SNORT e' piu' orientato all'Intrusion Detection, attraverso il riconoscimento automatico dei piu' comuni tipi di attacco.

In centri di calcolo di dimensioni almeno medie il flusso di traffico da analizzare ed il numero di oggetti da monitorare puo' essere tale da richiedere di dedicare un elaboratore (PC di media potenza con sistema operativo Linux) per ognuno dei tool indicati (tranne NESSUS, che viene lanciato "a richiesta", periodicamente, per analizzare il grado di sicurezza della propria rete). Anche il loro uso simultaneo, pero', non richiede dopo la configurazione iniziale una significativa quantita' di tempo uomo da dedicare: in media basta circa un'ora al giorno per esaminare le statistiche, i messaggi e i log prodotti dai tre software ed accertarsi che tutto vada bene. Se invece non tutto va bene, allora questi tool si rivelano preziosi per l'identificazione e l'eliminazione del problema.

Nel seguito viene esposta una breve presentazione di ognuno dei prodotti.

NAGIOS
LAN & WAN Monitoring tool

Nagios [3] [4] e' un tool per il monitoraggio di oggetti informatici, siano essi risorse fisiche degli host (elaboratori), quali ad es. lo spazio disco, l'occupazione di memoria centrale, l'uso della cpu, eccetera, o servizi di rete offerti dagli stessi, quali ad esempio la posta elettronica, il web, le news, eccetera, oppure apparecchiature di rete.
Il controllo puo' avvenire sia su rete locale che in remoto.

In particolare, esso:

- consente il controllo di singoli host o gruppi di host configurati con alto grado di liberta' dall'Amministratore della Rete, il quale puo' adattare il layout del tool alle esigenze specifiche del suo sito;

- permette di configurare i servizi da monitorare su base di ogni singolo host;

- permette una pratica visualizzazione grafica delle risorse e dei servizi monitorati mediante web server, sul quale e' possibile configurare piu' username e password: ciascun account puo' essere abilitato a visualizzare solo gli host e/o i servizi desiderati, creando quindi una sorta di subset del layout generale di rete che e' sotto controllo;

- ha la possibilita' di effettuare sofisticati controlli remoti sulle apparecchiature di rete attraverso l'accesso alle stesse via protocollo SNMP;

- consente di definire dei "contacts" ai quali inviare via e-mail o via sms le notifiche dei problemi che si presentano sugli oggetti controllati; e' possibile personalizzare le notifiche, informando per ogni singolo problema la persona "giusta";

- offre la possibilita' di intraprendere azioni in risposta al raggiungimento delle soglie di allarme prefissate; queste azioni possono essere semplicemente l'avviso alla contact person giusta, ma anche lo shutdown di un elaboratore, o il lancio di un particolare job.

NESSUS
Vulnerability scanner

Nessus [5] [6] e' un software che esegue operazioni non solo di "network mapping", ma anche di "vulnerability scanner".
In altri termini Nessus svolge funzioni di controllo di quali porte ben note associate a servizi di rete dal protocollo TCP/IP sono aperte ed accessibili sulle macchine della rete.
A queste funzioni Nessus associa quelle di "vulnerability scanner", ossia di controllo se il software di sistema che risponde su ogni macchina ad ogni data porta e' affetto da virus noti oppure se e' completamente funzionale o se e' stato maliziosamente alterato o anche se ci sono errori di configurazione che aprono spazi di vulnerabilita'.

In particolare, esso:

- cerca i servizi di rete attivi su un elaboratore, anche su porte non standard (ad es. un web server che utilizza la porta 1234 invece della 80) o che rispondono su piu' porte;

- identifica le versioni dei programmi che li gestiscono;

- per ogni servizio, prova gli exploits (ossia le tecniche fraudolente di attacco informatico) che ha nel proprio database (ovviamente aggiornabile) e riferisce in un log citando anche le possibili tecniche di difesa;

- identifica il sistema operativo della macchina oggetto di controllo;

- e' in grado di lanciare attacchi di tipo DoS (Denial of Service); questa possibilita' e' utile per simulare attacchi da parte di un hacker e verificare la "robustezza" delle proprie difese di fronte ad un eventuale attacco "vero".

NTOP
Network traffic probe

NTOP [7] e' un tool per l'analisi in tempo reale del traffico di rete. Esso consente di analizzare il traffico in corso per macchina e per tipo di protocollo attraverso l'analisi dei singoli pacchetti "sniffati" sulla rete e offre una interfaccia Web molto "user friendly".

In particolare, esso permette di:

- suddividere il traffico di rete secondo i vari protocolli;
- presentare delle analisi di traffico in base a vari criteri molto flessibili;
- mostrare statistiche di traffico;
- presentare la distribuzione del traffico IP nei vari protocolli della suite;
- analizzare il traffico IP e ordinarlo in base a coppie provenienza ← → destinazione sia a livello di network che di subnet che di host;
- produrre statistiche di traffico assai simili a quelle prodotte dal software RMon, con il valore aggiunto di una presentazione grafica web molto meglio accessibile; questa caratteristica permette di vedere NTOP come un agente Rmon dotato di interfaccia grafica.

SNORT
Network Intrusion Detection Tool

SNORT [8] e' un software che svolge funzioni di intrusion detection system grazie all'analisi del flusso di traffico di rete. Il suo tipico uso consiste nel connettere il sistema Linux su cui e' installato a una porta di uno switch su cui sia ripetuto, con una procedura di mirror, tutto il traffico da e per il router principale di connessione alla rete esterna alla LAN. Cio' consente al software di analizzare il traffico e di scoprire in tempo reale i piu' comuni tipi di attacco informatico a cui il centro di calcolo e' sottoposto dall'esterno (o anche eventuali attacchi verso l'esterno originati dalla propria LAN).

In particolare, esso e' in grado di:

- effettuare il "packet logging", ossia acquisire statistiche (a basso livello della pila OSI) in tempo reale su tutto il traffico che attraversa la rete;

- offrire tabelle di "protocol analysis", cioe' statistiche di uso dei diversi protocolli della suite TCP/IP (cioe' delle applicazioni di alto livello OSI) che sono utilissime per capire l'uso che della rete viene fatto da parte degli utenti (sia a fini statistici che per l'individuazione di usi non consentiti);

- evidenziare in tempo reale le scansioni provenienti dall'esterno sulle porte ben note delle macchine della LAN (o anche all'interno della LAN, o dalla LAN verso l'esterno);

- segnalare in tempo reale tutta una (ampia) serie di attacchi informatici alla LAN, permettendo l'identificazione del tipo di attacco e della sua provenienza **nel corso dell'attacco stesso**.

Bibliografia

[1] Gruppo Harmony, Linux/Unix host security, 2005

[2] Gruppo Harmony, Firewall e Router, 2005

[3] www.nagios.org , sito ufficiale del prodotto

[4] G. Sava e G. Tortone, “Nagios: un tool per resource & LAN / WAN monitoring”, presentato al “Workshop sulle problematiche di Calcolo e Reti nell’INFN, Elba 2002” e disponibile alla pagina http://www.ts.infn.it/conferences/ccr2002/agenda.shtml

[5] www.nessus.org , sito ufficiale del prodotto

[6] F. Taurino, “Nessus: vulnerability scanner”, presentato al “Workshop sulle problematiche di Calcolo e Reti nell’INFN, Elba 2002”, disponibile su http://www.ts.infn.it/conferences/ccr2002/agenda.shtml

[7] www.ntop.org , sito ufficiale del prodotto

[8] www.snort.org , sito ufficiale del prodotto