Sicurezza delle reti[1]

Mattia Monga

Dip. di Informatica e Comunicazione
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2010/11

Lezione XIII: Architettura dei NIDS

Aspetti architetturali

Data la natura di componente di monitoraggio, un NIDS è un componente che complementa altre soluzioni per la sicurezza aziendale contribuendo a formare un'architettura a diversi livelli di sicurezza (defense in-depth).
Sono quindi importanti aspetti architetturali quali:

- Quanti sensori installare nella rete
  - costo e complessità di gestione vs. ricchezza di dati
- Dove installarli
  - visibilità del traffico vs. ridondanza di informazioni
- Come gestire i dati
  - analisi e logging centralizzato vs. analisi e/o logging distribuito

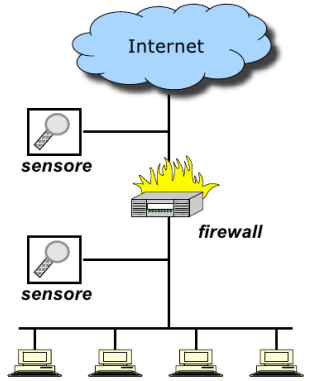
Sensori e firewall

Esterno

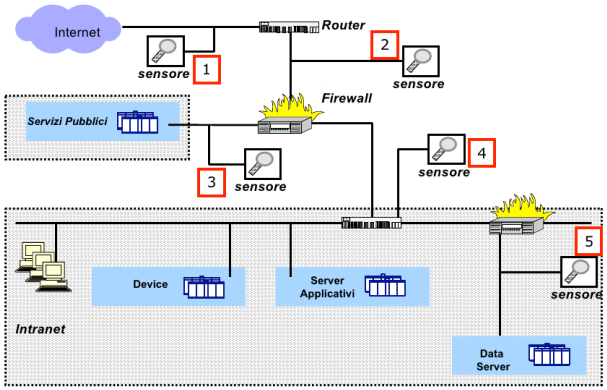
- Rileva l'intero traffico diretto alla rete
- Maggiore quantità di dati
- Maggiore incidenza di falsi allarmi

Interno

- Rileva solo il traffico che entra effettivamente nella rete
- Verifica l'efficacia del firewall
- Non fornisce info sugli attacchi bloccati dal firewall



Posizionamento nella rete aziendale



1. Esterno al border router
   - Rileva l'intero traffico diretto alla rete aziendale.
   - Informazione completa e non filtrata da nessun dispositivo.
   - Maggiore mole di dati ed allarmi, alta incidenza di falsi allarmi.
2. Tra border router e firewall
   - Tutto il traffico che entra nella rete tranne quello filtrato

Risposta di un NIDS

- La tipica risposta di un NIDS al verificarsi di un evento che verifica una firma è la generazione di un allarme
- La forma piú standard di allarme è la scrittura in un corrispondente file di log

Esempio di log su syslog

```
[1:1122:2 ] WEBMISC /etc/passwd [Classification: Attempted
Information Leak ] [Priority:2 ] 09/1610:04:15.826116
192.168.1.1:3143 >192.168.1.2:80 TCP TTL:128 TOS:0x0
ID:12832 IpLen:20 DgmLen:149 DF ***AP***Seq:0xDEFF5454
Ack:0x1A51AF74 Win:0x4470
```

Esistono molte varianti implementate dai diversi NIDS, tra cui salvataggio in formato tcpdump, scrittura su database (es. MySQL), visualizzazione a video ecc.

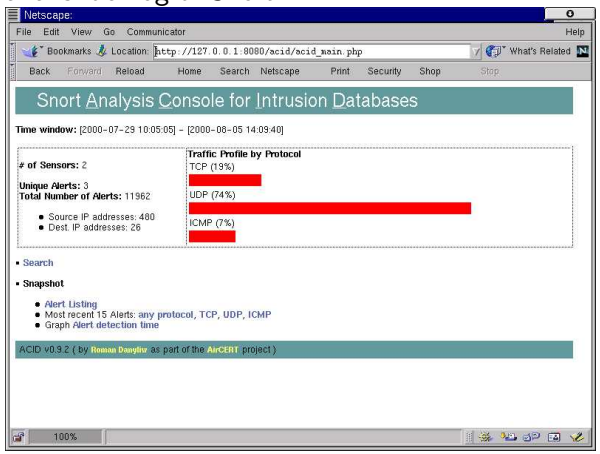
Analisi

Le scritture su log vanno successivamente analizzate: servono strumenti di supporto perché la mole di dati è spesso imponente.

- Esistono molti strumenti, sia open-source che integrati nei prodotti commerciali, di analisi dei log prodotti da un NIDS.
- Tipicamente vengono mostrati grafici, statistiche ecc. Sono utili per le analisi *post-mortem* e per il tuning dei sistemi, ma inefficaci per un'azione di contenimento real-time
- L'invio di email a un amministratore è un'altra modalità di risposta diffusa (e onerosa).

Tool di analisi

ACID (Analysis Console for Intrusion Databases) http://acidlab.sourceforge.net/ Interfaccia in PHP di analisi dei log di Snort



SGUIL (The Analyst Console for Network Security Monitoring) http://sguil.sourceforge.net/index.php Interfaccia per

Risposte automatiche

Risposta automatica

Una modalità di allarme che implica la generazione automatica di azioni allo scopo di rispondere attivamente ad una presunta intrusione senza richiedere l'intervento diretto di un operatore.

Esempio Snort:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-IIS cmd.exe access"; content:"cmd.exe";
react: block; ...)
```

L'opzione `react: block` fa sí che la connessione TCP nella quale si è verificato il tentativo di accesso a `cmd.exe` venga automaticamente terminata

Tipologia di risposte automatiche

Le tecniche più diffuse sono:

- Reset di sessioni (Session Sniping)
  - L'esempio precedente con Snort è di questo tipo
- Aggiornamento del Firewall

Reset di sessioni

Per realizzare lo sniping, il NIDS deve essere in grado di forzare la terminazione della connessione in corso tra client e server

- inviando un pacchetto contenente un RST ad entrambe le parti coinvolte nella connessione
- tali pacchetti devono apparire ai riceventi come inviati dalle corrispondenti controparti, non dal NIDS, altrimenti verrebbero ignorati
- devono quindi contenere valori corretti per i numeri di sequenza, numero di ack, ...

Aggiornamento dei firewall

La rilevazione di un allarme può essere sfruttata per riconfigurare automaticamente le regole di un firewall

- Esempio: la rilevazione di attività di scan viene utilizzata per impedire automaticamente ogni connessione da parte degli indirizzi IP sorgenti coinvolti.

Meno efficace di quel che potrebbe sembrare:

- Un intrusore può provocare riconfigurazioni che risultano dannose, ad esempio inviando pacchetti con IP spoofed
- Gli effetti possono essere di bloccare le connessioni provenienti da sorgenti legittime (denial-of-service)

Pericoli delle risposte automatiche

Qualunque meccanismo di risposta automatica ha il potenziale difetto di poter essere bypassato e/o sfruttato contro il sistema stesso che viene protetto

- Le risposte automatiche non sostituiscono l'intervento e l'analisi dell'operatore umano: un apparente risparmio di risorse può risultare in un aggravio di costi
- L'intrusion detection è per sua natura un'attività che necessariamente richiede una forte componente di analisi e di gestione manuale da parte di operatori specializzati (per questo è spesso esternalizzato).

Evasione di IDS

Spesso l'elusione del rilevamento è possibile sfruttando l'uso di alias o altri trucchi che aggirano l'identificazione di una risorsa o di un attacco
Esempio: Una regola che cerchi di verificare la condizione `content:/etc/passwd;` potrebbe essere bypassata da formati equivalenti quali `/etc//\//passwd` oppure `/etc/rc.d/../.\passwd`.
Occorre cercare di riportare la regola all'esame di nomi canonici.

Evasione di IDS

Tecniche di evasione più sofisticate utilizzano pacchetti frammentati per la loro difficoltà di gestione.
Per esempio, si supponga che il NIDS abbia un time-out per riassemblare i pacchetti frammentati inferiore rispetto al sistema vittima. Il NIDS considererebbe due frammenti come pacchetti indipendenti, il sistema destinatario come pacchetto unico.

Commenti generali sugli IDS

Un famoso (e controverso) rapporto di Gartner Group del 2003 afferma che gli IDS non valgono gli investimenti richiesti, perché:

- Troppi falsi positivi e negativi
- Richiedono staff dedicato al monitoraggio che dev'essere compiuto 24×7
- Il processo di risposta agli incidenti è molto oneroso
- Non si riescono a monitorare reti con traffico superiore ai 600MB/s senza inaccettabili decadimenti prestazionali

Per questo motivo commercialmente si è passati al termine IPS (intrusion protection s.), suggerendo cosí di avere a che fare con strumenti piú sofisticati...