Estensioni di NfSen per il monitoraggio delle reti

Autori: Massimo Ianigro – Claudio Marotta – CNR ISSIA

Abstract
NfSen è una interfaccia grafica web-based nata per la gestione dei flussi di dati attraverso apparati di rete, mediante l'analisi delle informazioni prodotte tramite il protocollo NetFlow.

- Oltre alle funzionalità di gestione e presentazione dei dati, NfSen adotta una architettura modulare che permette l'aggiunta di nuove caratteristiche, sia in termini di elaborazione delle informazioni (processing tramite plugin) che di segnalazione degli eventi (notifiche a mezzo alert).
- Utilizzando quindi il framework messo a disposizione da NfSen, presso il CNR ISSIA sono stati sviluppati dei plugin ad-hoc finalizzati al supporto della attività quotidiana di chi si occupa di gestione di infrastrutture di rete.
- Partendo dalla considerazione che gli strumenti interattivi (frontend-web) richiedono una costanza e una disponibilità di tempo che non sempre sono a disposizione di chi gestisce le infrastrutture, si è cercato di automatizzare, ove possibile, alcune attività quali, ad esempio:
- individuazione di nuovi host sulle reti interne e verifica della registrazione nel DNS;
- segnalazione di host sulle reti interne che effettuano attività anomale (es. traffico peer-to-peer, attivazione di servizi, etc);
- segnalazione di host sulle reti esterne che effettuano attività potenzialmente ostili (es. scanning vari);
- monitoraggio ed alerting del throughput di singole classi di indirizzi IP all'interno di un flusso uscente da un unico peer, con possibilità di definire destinatari differenti e valori differenti per ogni classe, eventualmente anche organizzati per fasce orarie, in modo da poter gestire con un unico plugin le segnalazioni ai vari Istituti afferenti all'infrastruttura;
- segnalazione dei top-host all'interno di ciascuna rete interna;

Inoltre in alcuni casi sono state sperimentate delle azioni di “reazione” automatica mediante riconfigurazione delle regole di firewalling sugli apparati di frontiera.

Verranno quindi presentati i risultati ottenuti in un contesto reale quale l'infrastruttura di rete dell'Area di Ricerca del CNR.
Il software è sviluppato con licenza GNU GPL.