Esame di Analisi Quantitativa dei Sistemi – Progetto

Appello del 26 Luglio 2013

Progetto per il gruppo n. 3 - Analisi Sperimentale

Riccardo Bernini - matricola 5435313

Tommaso Papini - matricola 5537529

Obiettivo del progetto è caratterizzare il comportamento temporale del tool Snort. La consegna del progetto dovrà essere:

- **una relazione che descrive la metodologia di valutazione sperimentale adottata e discute i risultati**
- **un archivio contente: file di log, eventuale codice sviluppato, dump di un eventuale database, eventuali regole di SNORT sviluppate.**

Riportiamo di seguito dettagli del progetto, al fine di chiarirne l'obiettivo. Il progetto richiede di affrontare un esercizio di valutazione sperimentale, con applicazione della metodologia descritta a lezione, volto a caratterizzare Snort e la sua capacità di attack detection da un punto di vista temporale. Riportiamo gli elementi principali del progetto (si noti bene che tali elementi non sono necessariamente gli unici o imprescindibili, e si lascia la possibilità di effettuare variazioni, specialmente sul livello di dettaglio):

- Creare il sistema di misura e configurare opportunamente il tool SNORT per agire come Intrusion Detection System. Presumibilmente, il sistema risultante sarà composto da due nodi connessi:
  - *Nodo A* svolge il ruolo di "nodo da proteggere", su cui è installato Snort
  - *Nodo B* svolge il ruolo di sistema attaccante. Notare che non si pongono comunque vincoli per l'utilizzo di differenti configurazioni.
- Definire un faultload da generare ed esercitare sul sistema. Non si pongono vincoli sulla complessità del faultload o sulla selezione degli strumenti per la sua generazione. Può essere necessario costituire delle regole Snort adeguate per identificare per il faultload definito.
  - Esempi di faultload che possono essere realizzati sono: iniettare un elevato numero di ping da parte di un singolo nodo, oppure effettuare un port scan, effettuare un SQL injection.
  - A titolo di esempio, menzioniamo alcuni strumenti che possono essere utilizzati per la generazione del faultload: ping, nmap, traceruote, MetaSploit, sqlsus.
- Introdurre nel sistema opportuni meccanismi di monitoring (sonde) per rilevare le misure di tempo richieste. Possibili misure da rilevare sono: i) l'istante di tempo in cui si inietta l'attacco sul nodo A; ii) l'istante di tempo in cui l'attacco è individuato da parte di Snort; iii) l'istante di tempo in cui l'attacco è generato dal nodo B; v) il ritardo di trasmissione tra i due nodi A e B; iv) l'istante di tempo in cui l'attacco si verifica sul sistema, nel caso in cui Snort non sia in grado di rilevarlo; v) etc.
  - Si noti che gli istanti di tempo menzionati sopra permettono di calcolare intervalli quali: i) il tempo di detection dell'attacco (dall'inizio dell'attacco sul nodo A alla sua rilevazione da parte di Snort); ii) la durata dell'attacco (dalla generazione dell'attacco su B alla sua rilevazione da parte di Snort, o al suo completamento); iii) etc.
- Eseguire gli esperimenti per il faultload selezionato, raccogliendo i dati.

- Presentare i risultati raccolti, cercando di motivarli opportunamente. È importante concentrarsi sulle misure temporali raccolte. Discutere in particolare i tempi di rilevazione (dall'iniezione dell'attacco alla sua rilevazione da parte di Snort), osservare la loro varianza ed identificare eventuali distribuzioni.

Suggerimento 1. Per raccogliere le misure temporali, si possono utilizzare varie soluzioni: leggere i dati contenuti nel log di snort, utilizzare strumenti per il monitoring della rete, oppure creare apposite procedure in un qualsiasi linguaggio.

Suggerimento 2. Si può esercitare il sistema utilizzando diverse configurazioni di Snort per cercare di studiare la perturbazione introdotta da Snort sul sistema. Ad esempio, si può osservare come variano le misure quando il numero di regole applicate da Snort sono ridotte al minimo indispensabile, oppure quando parallelamente al faultload si utilizzano differenti workload.

Per chiarimenti, contattare Andrea Ceccarelli andrea.ceccarelli@unifi.it ed il docente in CC.