Zeek e le query principali per il threat hunting

•Cosa è Zeek?

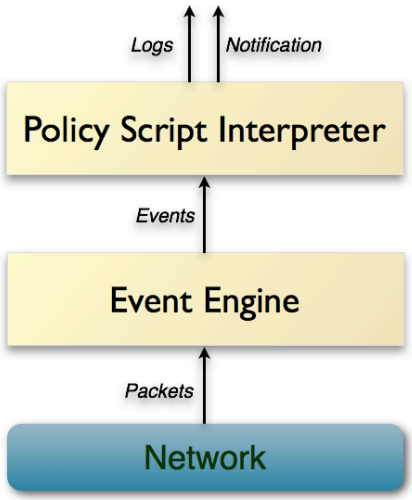
Zeek è un tool open-source passivo di analisi del traffico, usato da molti come NSM(network security monitor), inoltre supporta funzioni di analisi delle performance di rete e di risoluzione dei problemi.

•Perchè Zeek?

Zeek si occupa di analizzare la categoria dei “network data”, a questa categoria appartengono quattro tipologie di dati; Zeek ne riesce a gestire 3: transaction data, extracted data and alert data.
Zeek è conosciuto per lo più per i log derivati dall’analisi di rete e ciò produce dei transaction data.
Molti esperti del settore preferiscono questo strumento a Wireshark per la sua flessibilità ed estensibilità della piattaforma. Inoltre risulta essere molto veloce nell’analisi di grandi datalog senza essere molto esigente dal punto di vista hardware; infine essendo basato su script, non presenta interfaccia grafica, permettendo un controllo diretto di maggiore precisione da parte del programmatore.

•Come funziona Zeek?

Da un punto di vista di alto livello, Zeek è organizzato architetturalmente in due macro componenti. Presenta un “event engine” che trasforma il flusso di pacchetti in arrivo in una serie di “events” ad alto livello. Questi eventi descrivono cosa è stato visto, ma non perché e nemmeno se è significativo.
Gli “events” generati dall’ “event engine” passano al secondo macro componente: lo “script interpreter”. Questo componente esegue una serie di “event handlers” scritti nel linguaggio di scripting proprietario di Zeek, questi script possono, ad esempio, esprimere la policy di sicurezza di un sito web; essi infatti indicano come agire in caso di rilevamento di particolari attività. In generale, gli script possono derivare qualunque proprietà e statistica dal traffico di input e rispondere in real-time a ciò che rilevano, impostando così una possibile active response al problema rilevato.



•Formati dei log di Zeek ed analisi

```
zeek -C -r ../nomeFile.pcap
```

-r —> indica a Zeek dove trovare il file; -C —> ignora gli errori di checksum TCP.

Dopo questo comando Zeek crea i file TSV contenenti le principali informazioni riguardanti la connessione analizzata.

```
zeek -C -r ../nomeFile.pcap LogAscii::use_json=T
```

Dopo questo comando Zeek crea i file TSV contenti le principali informazioni riguardanti la connessione analizzata, gestendo però il tutto in formato JSON

•Zeek ed i suoi logs principali
conn.log —> È uno dei principali log di Zeek, se non il più importante, e raccoglie le informazioni prevalentemente legate al livello di trasporto(livello 4) e al livello di rete(livello 3).

dns.log —> Contiene informazioni relative alle procedure di domain name resolution, livello applicazione(livello 7).

http.log —> Contiene informazioni legate alle connessione http, oggi sempre meno frequenti a causa del passaggio ad https.

files.log —> File trasmessi lungo la rete. Zeek ha il vantaggio di riuscire ad intercettarli e scriverli su disco

ssl.log —> contiene il traffico HTTPS(Zeek non lo cataloga nativamente) tramite il protocollo di crittografia TLS

x509.log —> cattura dettagli dei certificati scambiati durante alcune negoziazioni TLS

ntp.log —> analizza dettagli riguardanti protocollo NTP, che permette di regolare l'ora sulle varie macchine contattando appositi server.