Analisi query Zeek per il threat hunting

capinfos -aeu <pcap file>

Capinfos è un tool di Wireshark che permette di visualizzare tutte le caratteristiche principali del file di cattura. In questa particolare configurazione ci consente di vedere la durata della cattura, la data di cattura del primo pacchetto e la data di cattura dell'ultimo pacchetto.

ngrep -q -I trace1.pcap host ipOrigine and host ipDestinazione | less

-q —> Mostra soltanto l'intestazione dei pacchetti ed i loro payload.
-I —> Prende l'input da un file .pcap compatibile.
less —> Stampa l'output, utile su grandi file poiché inizia subito a stampare l'output.

Bisogna sottolineare che zeek-cut utilizza come input i dati forniti da un lettore di file, è quindi necessario fare uso di un meccanismo basato sulle pipe per poter fornire input a zeek-cut, ma anche per elaborare gli output di quest'ultimo in modo da evidenziare le informazioni che possono essere utili per la nostra analisi.

•Identificazione delle connessioni lunghe

cat conn.log | zeek-cut id.orig_h id.resp_h duration | sort -k 3 -rn | head

Elenca le 10 connessioni singole con la durata maggiore in ordine decrescente.

catt conn.log —> Lettura del file conn.log.
zeek-cut id.orig_h id.resp_h duration —> Estrae dal file conn.log i campi citati, che rispettivamente nell'ordine simboleggiano: indirizzo ip di origine, indirizzo ip di destinazione e durata della connessione.
sort -k 3 -rn —> Riordina l'output ricevuto basandosi sulla terza colonna, tutto viene fatto seguendo un ordinamento aritmetico(-n) decrescente(-r).
head —> Mostra le prime 10 righe dell'output.

cat conn.log | zeek-cut id.orig_h id.resp_h duration | sort | grep -v '-' | datamash -g 1,2 sum 3 | sort -k 3 -rn | head

Elenca le 10 connessioni conta durata maggiore in ordine decrescente.

catt conn.log —> Lettura del file conn.log.
zeek-cut id.orig_h id.resp_h duration —> Estrae dal file conn.log i campi citati, che rispettivamente nell'ordine simboleggiano: indirizzo ip di origine, indirizzo ip di destinazione e durata della connessione.
sort—> Riordina l'output ricevuto considerando il primo carattere degli indirizzi ip di origine.
grep -v '-' —> Rimuove le linee contenenti almeno una volta il carattere '-'.
datamash -g 1,2 sum 3 —> Somma la durata delle medesime connessioni, in modo da avere la durata totale di ciascuna di esse.
sort -k 3 -rn —> Riordina l'output ricevuto basandosi sulla terza colonna, tutto viene fatto seguendo un ordinamento aritmetico(-n) decrescente(-r).

head —> Mostra le prime 10 righe dell'output.

•Identificazione dei beacons

cat conn.log | zeek-cut id.orig_h id.resp_h | sort | uniq -c | sort -rn | head

Elenca il numero di connessioni univoche.

catt conn.log —> Lettura del file conn.log.
zeek-cut id.orig_h id.resp—> Estrae dal file conn.log i campi citati, che rispettivamente nell'ordine simboleggiano: indirizzo ip di origine e indirizzo ip di destinazione.
sort—> Riordina l'output ricevuto considerando il primo carattere degli indirizzi ip di origine.
uniq -c —> Conta le connessioni univoche ed elimina le righe ripetute adiacenti.
sort -rn —> Ordina l'input ricevuto secondo un ordinamento numerico decrescente.
head —> Mostra le prime 10 righe dell'output.

cat conn.log | zeek-cut id.orig_h id.resp_h orig_bytes | grep ipOrigine | grep ipDestinazione | sort | uniq -c | sort -rn | head

Elenca la connessione specificata con associato il numero di byte trasmessi.

catt conn.log —> Lettura del file conn.log.
zeek-cut id.orig_h id.resp_h orig_bytes—> Estrae dal file conn.log i campi citati, che rispettivamente nell'ordine simboleggiano: indirizzo ip di origine, indirizzo ip di destinazione ed il numero di byte scambiati durante la connessione.
grep ipOrigine —> Seleziona righe dove è presente l'indirizzo ip di origine.
grep ipDestinazione —> Seleziona righe dove è presente l'indirizzo ip di destinazione.
sort—> Riordina l'output ricevuto considerando il primo carattere degli indirizzi ip di origine.
uniq -c —> Conta le connessioni univoche ed elimina le righe ripetute adiacenti.
sort -rn —> Ordina l'input ricevuto secondo un ordinamento numerico decrescente.
head —> Mostra le prime 10 righe dell'output.

cat http.log | zeek-cut id.orig_h id.resp_h uri | grep ipDestinazione | sort | uniq -c | sort -rn

Elenca la connessione specificata tramite l'ip di destinazione ed il suo URI.

cat http.log —> Lettura del file http.log.
zeek-cut id.orig_h id.resp_h orig_bytes—> Estrae dal file conn.log i campi citati, che rispettivamente nell'ordine simboleggiano: indirizzo ip di origine, indirizzo ip di destinazione e l'URI, cioè la sequenza di caratteri che identifica univocamente una risorsa.
grep ipDestinazione —> Seleziona righe dove è presente l'indirizzo ip di destinazione.
sort—> Riordina l'output ricevuto considerando il primo carattere degli indirizzi ip di origine.
uniq -c —> Conta le connessioni univoche ed elimina le righe ripetute adiacenti.
sort -rn —> Ordina l'input ricevuto secondo un ordinamento numerico decrescente.

•C2 legati ai DNS

cat dns.log | zeek-cut query | sort | uniq | rev | cut -d . -f 1-2 | rev | sort | uniq -c | sort -rn | head

Elenca il numero di host associato a ciascun dominio.

cat dns.log —> Lettura del file dns.log.
zeek-cut query —> Estrae dal file dns.log il campo query.
sort—> Riordina l'output ricevuto considerando il primo carattere delle query DNS.
uniq —> Elimina le righe ripetute adiacenti.
rev —> Inverte l'ordine dei caratteri di una stringa.
cut -d . -f 1-2 —> Il comando cut elimina la porzione selezionata da ogni riga del file dato come input. -d permette di modificare il delimitatore, selezionandone uno diverso da quello di default; mentre -f permette di selezionare specifici settori di stringa separati dal delimitatore, in questo caso il primo ed il secondo.
uniq -c —> Conta le connessioni univoche ed elimina le righe ripetute adiacenti.
sort -rn —> Ordina l'input ricevuto secondo un ordinamento numerico decrescente.
head —> Mostra le prime 10 righe dell'output.

cat dns.log | zeek-cut qtype_name query | grep dominioInteresse | cut -f 1 | sort | uniq -c | sort -rn

Elenca le tipologie di record DNS associati al dominio preso in analisi.

cat dns.log —> Lettura del file dns.log.
zeek-cut qtype_name query —> Estrae dal file dns.log il tipo di record DNS ed il campo query.
grep dominioInteresse—> Seleziona righe dove è presente il dominio di destinazione.
cut -f 1 —> Mantieni solo il primo campo della riga del file.
sort—> Riordina l'output ricevuto considerando il primo carattere delle query DNS.
uniq -c —> Conta le connessioni univoche ed elimina le righe ripetute adiacenti.
sort -rn —> Ordina l'input ricevuto secondo un ordinamento numerico decrescente.

RECORD A *—> Indica la corrispondenza tra un nome ed uno (o più) indirizzi IPv4.*
MX RECORD *—> Indica a quali server debba essere inviata la posta elettronica per un certo dominio.*
RECORD CNAME *—> Sono usati per creare un alias, ovvero per fare in modo che lo stesso host sia noto con più nomi. Uno degli utilizzi di questo tipo di record consiste nell'attribuire a un host che offre più servizi un nome per ciascun servizio. In questo modo, i servizi possono poi essere spostati su altri host senza dover riconfigurare i client, ma modificando solo il DNS.*
RECORD PTR *—> Il DNS viene utilizzato anche per realizzare la risoluzione inversa, ovvero per far corrispondere a un indirizzo IP il corrispondente nome di dominio. Per questo si usano i record di tipo "PTR" (e una apposita zona dello spazio dei nomi in-addr.arpa).*
RECORD AAAA *—> È come il Record A, ma lavora con l'IPv6 e restituisce un indirizzo IPv6.*
RECORD MX *—> Collega un nome di dominio ad una lista di server di posta autorevoli per quel dominio. I record indicano anche la preferenza di un server rispetto ad un altro.*

RECORD SRV *—> Identificano il server per un determinato servizio all'interno di un dominio. Possono essere considerati una generalizzazione dei record MX.*
RECORD TXT *—> Associano campi di testo arbitrari a un dominio. Questi campi possono contenere una descrizione informativa, oppure essere utilizzati per realizzare servizi.*
RECORD NS *—> Utilizzato per indicare quali siano i server DNS autorevoli per un certo dominio, ovvero per delegarne la gestione.*
RECORD SOA *—> (Start of Authority) usato per la gestione delle zone DNS.*