Universita' degli studi di Roma "Tor Vergata"
Teoria della sicurezza e crittografia

Authors: Marcello Politi, Samir Salman, Angelo Silvestri

December 2019

1 Risoluzione Esercizi

1.1 Esercizio 1

x(t1)=0.45,0.45,0.1

x(t2)=0.3,0.6,0.1

x(t3)=0.1,0.9,0.0

E(x(t1))=$\sum_{n=1}^{3} P(X = x_i)log(P(X = x_i) = 2,3025$

$E(x(t2)) = \sum_{n=1}^{3} P(X = x_i)log(P(X = x_i)) = 2,9702$

$E(x(t3)) = \sum_{n=1}^{3} P(X = x_i)log(P(X = x_i)) = 2,3025$

Notiamo come al variare delle probabilità date l'entropia tende ad aumentare tra x(t1) e x(t2) e poi si riabbassa nuovamente su x(t3)

1.2 Esercizio 2

Dopo aver analizzato il traffico di rete su varie porte del pc in varie face temporali abbiamo ricavato che:

Mattina:

TCP 80 12/00 P=0.12
SSH 22 20/00 P=0.20
SMTP 187 15/00 P=0.15

Pomeriggio:

TCP 80 8/00 P=0.8
SSH 22 18/00 P=0.18
SMTP 187 12/00 P=0.12

Sera:

TCP 80 24/00 P=0.24
SSH 22 9/00 P=0.9
SMTP 187 13/00 P=0.13

Assumendo queste probabilita possiamo rispondere alle richieste dell' esercizio. Ricordiamo le formule per il calcolo dell' entropia e dell' entropia congiunta:

E(X)=$\sum_{n=1}^{\infty} P(X = x_i)log(P(X = x_i)$

E(X)=$\sum_{k} P(X = x_i)log(\frac{p_k}{q_k})$
Dai nostri valori ricaviamo che:

E(X)=0,2459
d=0,2134

Abbiamo pensato se potessero esistere altre variabili condizionanti oltre a quelle suggerite dall'esercizio:

- Variazioni in base alla rete
  ci aspettiamo che in una rete piu trafficata (come in un bar), il traffico sia maggiore
- In base al numero di connession che il dispositivo ha verso alti dispositivi esterni

1.3 Esercizio 3

Abbiamo localizzato la cartella in cui il borwser scrive i files e ricavato la distribuzione di frequenza delle date di ultima modifica del file utilizzando il prompt dei comandi listando i file e redigendo e processando tali dati abbiamo ottenuto la seguente tabella: In fine calcolato l'entropia assouluta Dati raccolti:

Differenza in giorni da oggi	Numero file assoluto	Numero file relativo
10	16	1
14	16	2
27	16	3
29	16	4
31	16	5
33	16	6
34	16	7
35	16	8
36	16	9
43	16	10
44	16	11
45	16	12
56	16	13
57	16	14
58	16	15
58	16	16

Shannon Entropy = 0.389

1.4 Esercizio 3B

Data una distribuzione di probabillità, es. una distribuzione discreta, in cui ho 3 eventi A, B, C con probabilità pA,Pb;pC, supponiamo di osservare n realizzazioni dei 3 eventi. Provare a suggerire delle regole per stabilire quando la sequenza osservate è anomala. Es. osservo n=10 e la sequenza A,A,A,A,A,A,A,A,A,A.. Tale sequenza è anomala? Ovviamente dipende da pA. Provare a sugggerire un algoritmo regola che data una distribuzione di probabilità, una sequenza n di eventi restituisce un indice di animalia sulla frequenza.
Supponiamo inizialmente pB=pA=0 e Pc=1 ne consegue che una sequenza di tutte C non risulterebbe anomala.

Esempio 1:
Se ipotizziamo una distribuzione di probabilità pari a pA=pB=pC=0.333
Messaggio:a b c
Stringa input: aaaaaaaaaabbbbbbbbbbccccccccccc
frequenza simboli: 0.333 - a 0.333 - b 0.333 - c

Esempio2:
Stringa input: aaaaaaaaaabbbbbbacbababcabcbcbcbababacbbccbcbcbababacbcbcbcbabcbabcbabccacacaccaaabbbaccacabacabaccbcbcbcbbbccacacaacbbbbcccccccccc
frequenza simboli: 0.298 - a 0.351 - b 0.351 - c
H(X) = -[(0.298log20.298)+(0.351log20.351)+(0.351log20.351)] H(X) = -[(-0.52)+(-0.53)+(-0.53)] H(X) = -[-1.58076] H(X) = 1.58076
L'entropia di Shannon ci dice qual è il numero minimo di bit per simbolo necessario per codificare le informazioni in forma binaria (se la base di log è 2). Dato

l'entropia di Shannon calcolata sopra, arrotondata per eccesso, ogni simbolo deve essere codificato da 2 bit e la necessità di utilizzare 262 bit per codificare la stringa i-n modo ottimale.

Inoltre, è possibile calcolare altre formule, una delle più semplici è l'entropia metrica che è l'entropia di Shannon divisa per la lunghezza della stringa. L'entropia metrica ci aiuterà a valutare la casualità del messaggio. Può assumere valori compresi tra 0 e 1, dove 1 significa una stringa casuale equamente distribuita. L'entropia metrica per l'esempio precedente è: **0,01207**

Esempio 3:
Messaggio: A, B, C à: pA=1/2, pB=1/3, pC=1/6
Contenuto di informazione del messaggio=1.46 bit

1.5 Esercizio 4

Considerare l'attacco ransomware (dove i file attaccati sono testi oppure immagini) e provare a suggerire un antivirus basato sull'approccio visto.

Soluzione: l'attacco cripta i file per poi chiedere un riscatto. Questo significa che il conteuto orginale del file è sostituito con delle sequennze che , essendo prodotte da algoritmi di crittografia, sono pseudo-random. Esse cancellano la semantica dei file stessi. Quindi se in una cartella ci sono tutt le immagini, le lastre al torace di un ospedale, ho una bassa entropia perchè sono tutte immagini. L'attacco man mano che si realizza, fa schizzare l'entropia. Provare a formalizzare in modo preciso questo approccio. Qual'è precisamente l'entropia alla quale ci si riferisce?

I tre metodi di attacco più comuni per gli attacchi ransomware sono: infezioni silenziose dai kit di exploit, allegati e-mail malevoli e collegamenti malevoli nelle e-mail.

Al fine di prevenire meglio i ransomware, è fondamentale comprendere le tattiche utilizzate dagli aggressori per fornire questa minaccia. Esistono più varianti ransomware in uso su più vettori di attacco, anche attraverso la rete, le applicazioni basate su SaaS e direttamente all'endpoint. Queste informazioni ti permetteranno di focalizzare i tuoi controlli di sicurezza sulle aree più probabili da sfruttare e ridurre il rischio di infezione.

Kit di exploit I kit di exploit sono sofisticati toolkit che sfruttano le vulnerabilità. Molto spesso, i kit di exploit vengono eseguiti quando una vittima visita un sito Web compromesso. Il codice dannoso nascosto sul sito, spesso in una pubblicità (malvertisement), ti reindirizza alla pagina di destinazione del kit di exploit inosservata. Se vulnerabile, verrà eseguito un download drive-by di un payload dannoso, il sistema verrà infettato e i file verranno conservati per il riscatto.

Allegati e-mail dannosi Con allegati di posta elettronica dannosi, l'utente malintenzionato crea un'e-mail, probabilmente proveniente da una fonte credibile,

come risorse umane o IT, e allega un file dannoso, come un file eseguibile portatile (PE), un documento di Word o un file .JS. Il destinatario apre l'allegato pensando che l'e-mail sia stata inviata da una fonte attendibile. Una volta aperto il file, il payload del ransomware viene scaricato inconsapevolmente, il sistema è infetto e i file vengono conservati per il riscatto.

Collegamenti e-mail dannosi Simile agli allegati di posta elettronica dannosi, i collegamenti di posta elettronica dannosi sono URL nel corpo dell'email. Allo stesso modo, queste e-mail vengono inviate da qualcuno o da qualche organizzazione che ritieni sia una fonte attendibile. Quando si fa clic, questi URL scaricano file dannosi sul Web, il sistema è infetto e i file vengono conservati per il riscatto.

Questa evoluzione e la facilità con cui vengono eseguiti questi attacchi, significa che qualsiasi organizzazione può essere la prossima vittima ed è probabilmente già un obiettivo attuale. Tuttavia, ci sono soluzioni. La prevenzione è fondamentale per proteggere le organizzazioni. La strategia più efficace per fermare un attacco ransomware si basa sull'impedire che l'attacco entri nella tua organizzazione.