./images/

Alla mia famiglia,
che mi ha sempre sostenuto
in ogni mia scelta.

Introduzione

Questa è l'introduzione.

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Lo stato dell'Arte

In questo capitolo si va ad illustrare lo stato dell'Arte delle tecnologie utilizzate. Si illustreranno le principali qualità degli Intrusion Detection Systems e le caratteristiche principali che hanno portato durante i test alla scelta di un software rispetto che un altro. Si passerà poi a presentare sFlow, illustrandone i benefici e le principali differenze con NetFlow e di come esso viene attualmente utilizzato per affiancare un IDS. Infine si darà una breve presentazione dello stack ELK, (Elasticsearch-Logstash-Kibana) e di come esso sia utilizzato nell'ambito della Network Security.

1.1 Intrusion Detection System

Il panorama degli Intrusion Detection System (IDS) è al giorno d'oggi in continua evoluzione. Tuttavia è possibile classificarli secondo due criteri principali che ne determinano il funzionamento:

- Sistemi signature based
- Sistemi basati su anomaly detection

Un IDS signature based analizza i pacchetti passanti su una rete utilizzando un set di regole appositamente scritte per rilevare un determinato tipo di attacco. Questo ci mette al riparo da una grandissima quantità di

attacchi conosciuti e si è rilevato nel corso degli anni un sistema efficiente e ampiamente utilizzato.

I secondi invece utilizzano tecniche di intelligenza artificiale per determinare se un comportamento sia lecito oppure no basandosi su quello che è stato definito in fase di installazione come uno "stato normale".

Sebbene nell'ultimo periodo l'intelligenza artificiale stia facendo la sua comparsa in ogni ambito dell'informatica gli IDS signature based rappresentano tuttora un'importante fetta (se non la maggioranza) degli IDS in uso nei più importanti data center del mondo ed è per questo che vale la pena studiarli.

Tra i maggiori esponenti degli IDS attualmente utilizzati abbiamo:

- Snort: Un IDS sviluppato a partire dagli anni '90, acquisito da Cisco nel 2013 e che è tuttora il più utilizzato in ambito enterprise.
- Suricata: Un IDS del nuovo millennio, sviluppato a partire dal 2009 da Open Information Security Foundation (OISF) e che vanta molteplici vantaggi sopra gli altri IDS.

In questo elaborato si è preferito utilizzare per motivi di performance e di implementazione, Suricata. I dettagli di questa scelta saranno chiari più avanti quando saranno state introdotte le principali caratteristiche di Suricata.

1.1.1 Suricata, una breve introduzione

Suricata è un IDS che fa uso di pattern matching per il riconoscimento di threat capace di effettuare un'analisi molto approfondita. Il funzionamento del pattern matching può essere riassunto dalla figura 1.1. Mentre una tipica regola per il patter matching è fatta in questo modo:

```
rule header    alert tcp any any -> 192.168.1.0/24 111
```

E' stato dimostrato infatti (trovare il paper) che data la sua natura multi threaded Suricata è di gran lunga più veloce di Snort, il quale invece è single

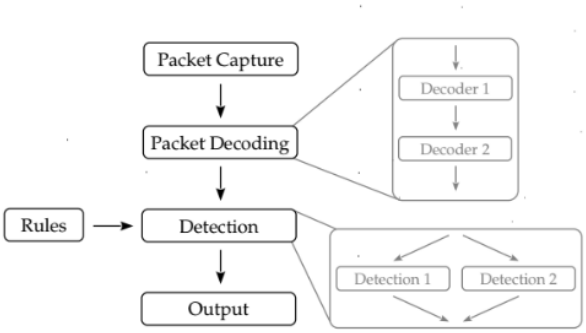

Figura 1.1: Funzionamento del patter matching

thread. La preferenza dell'uno rispetto all'altro non è tuttavia fondamentale dal punto di vista dei risultati generati dai nostri test. Infatti Suricata utilizza lo stesso rule-set di Snort.

1.2 Seconda Sezione

Ora vediamo un elenco puntato:

- primo oggetto
- secondo oggetto

1.3 Altra Sezione

Vediamo un elenco descrittivo:

OGGETTO1 prima descrizione;

OGGETTO2 seconda descrizione;

OGGETTO3 terza descrizione.

1.3.1 Altra SottoSezione

SottoSottoSezione

Questa sottosottosezione non viene numerata, ma è solo scritta in grassetto.

1.4 Altra Sezione

Vediamo la creazione di una tabella; la tabella 1.1 (richiamo il nome della tabella utilizzando la label che ho messo sotto): la facciamo di tre righe e tre colonne, la prima colonna "incolonnata" a destra (r) e le altre centrate (c):

$(1,1)$	$(1,2)$	$(1,3)$
$(2,1)$	$(2,2)$	$(2,3)$
$(3,1)$	$(3,2)$	$(3,3)$

Tabella 1.1: legenda tabella

1.5 Altra Sezione

1.5.1 Listati dei programmi

Primo Listato

```
        In questo ambiente     posso scrivere      come voglio,
lasciare gli spazi che voglio e non % commentare quando voglio
e ci sarï¿½ scritto tutto.
Quando lo uso ï¿½ meglio che disattivi il Wrap del WinEdt
```

Conclusioni

Queste sono le conclusioni.
In queste conclusioni voglio fare un riferimento alla bibliografia: questo è il mio riferimento [3, 4].

Appendice A

Prima Appendice

In questa Appendice non si è utilizzato il comando: `\clearpage{\pagestyle{empty}\cleardoublepage}`, ed infatti l'ultima pagina 8 ha l'intestazione con il numero di pagina in alto.

Appendice B

Seconda Appendice

Bibliografia

[1] Primo oggetto bibliografia.

[2] Secondo oggetto bibliografia.

[3] Terzo oggetto bibliografia.

[4] Quarto oggetto bibliografia.

Ringraziamenti

Qui possiamo ringraziare il mondo intero!!!!!!!!!!
Ovviamente solo se uno vuole, non è obbligatorio.