Politecnico di torino
Dipartimento di . . . (DIMEA)

CORSO DI LAUREA IN INGEGNERIA AEROSPAZIALE

TITOLO

Relazione tecnica:
Nome Cognome

Advisor:
Prof. ????

Tutor:
Prof. ????

Supervisor of the Doctoral Program:
Prof. ???

Maggio 2021

Sommario

Qua metti quello che hai fatto.

Indice

Introduzione 1

Le citazioni come Cretu et al. (2008) sono nel database bibtex che si trova nel file di nome `bibliography.bib`.

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

1.1 I *work package*

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi

quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

1.2 Struttura della relazione

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

Sviluppo del *work package* 3

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

3.1 Valutazione aerodinamica della soluzione “*pod*”

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto

vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

3.2 Valutazione aerodinamica della soluzione "fusoliera"

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

3.3 Risultati

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto

vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

Conclusione 4

Scrivi quello che vuoi e quanto vuoi. Scrivi quello che vuoi e quanto vuoi.

5.1 Code

La Figura 5.1 contiene un esempio di codice scritto in un ambiente "float" come la figura, appunto. È possibile scrivere codice inlined `for (i = n; i>=0; i--)` con la macro che vedrai nel sorgente. Infine, in Figura 5.1.

5.2 A Table

Riferimento ad una tabella è "Come si vede in Tabella 5.1 ...".

5.3 A Sideways Table

```
Fixpoint inv f :=
  match f with
  | Id n => Id n
  | Ne => Ne
  | Su => Pr
  | Pr => Su
  | Sw => Sw
  | Co f g => Co (inv g) (inv f)
  | Pa f g => Pa (inv f) (inv g)
  | It f => It (inv f)
  | If f g h => If (inv f) (inv g) (inv h)
  end.

Lemma inv_involute : forall f, inv (inv f) = f.
Proof. induction f; try constructor; simpl;
    congruence. Qed.

(* Notare che è possibile comporre funzioni di arità
    diverse: non è una grande differenza rispetto
    alle RPP originali, in effetti se si hanno arità
    diverse si può immaginare di applicare la
    funzione cast definita più avanti. *)
```

Figura 5.1: Copia incolla da `definitions.v`.

Feature	Misuse-based	Anomaly-based
Modeled activity:	**Malicious**	Normal
Detection method:	Matching	Deviation
Threats detected:	Known	Any
False negatives:	High	Low
False positives:	Low	High
Maintenance cost:	High	Low
Attack desc.:	Accurate	Absent
System design:	Easy	Difficult

Tabella 5.1: Duality between misuse- and anomaly-based intrusion detection techniques. Note that, an anomaly-based **IDS!** can detect "Any" threat, under the assumption that an attack always generates a deviation in the modeled activity.

content...

```
1   match f with
2   | Id n => Id n
3   | Ne => Ne
4   | Su => Pr
5   | Pr => Su
6   | Sw => Sw
7   | Co f g => Co (inv g) (inv f)
8   | Pa f g => Pa (inv f) (inv g)
9   | It f => It (inv f)
10  | If f g h => If (inv f) (inv g) (inv h)
11  end.
12
13 (* Differenza: è possibile comporre funzioni di ariet
        à diverse (ma nella pratica ciò non cambia nulla).
       *)
14
15 Fixpoint arity f :=
16  match f with
17  | Id n => n
```

Listing 5.1: Qesto snippet è l'inclusione diretta da riga 26 a riga 42 di `definitions.v`

Approach	Time	Header	Payload	Stochastic	Determ.	Clustering
(Mahoney and Chan, 2001)		•				•
(Kruegel et al., 2002)		•	•	•		
(Sekar et al., 2002)		•		•	•	
(Ramadas, 2003)			•			•
(Mahoney and Chan, 2003)	•		•		•	
(Zanero and Savaresi, 2004)		•	•			•
(Wang and Stolfo, 2004)			•	•		
(Zanero, 2005)		•	•			•
(Bolzoni et al., 2006)		•	•			•
(Wang et al., 2006)			•	•		

Tabella 5.2: Taxonomy of the selected state of the art approaches for network-based anomaly detection.

5.4 A Figure

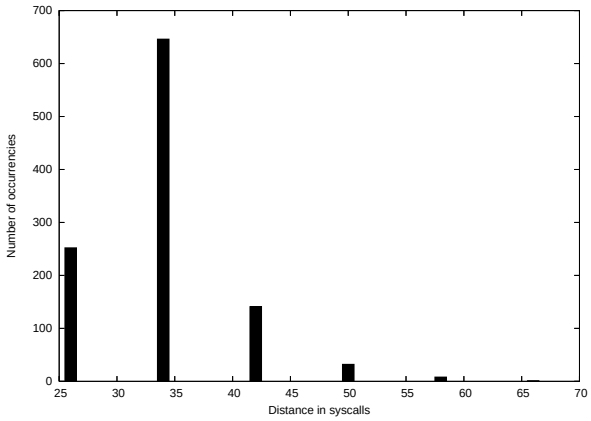

FIGURA 5.2: `telnetd`: distribution of the number of other system calls among two `execve` system calls (i.e., distance between two consecutive `execve`).

Riferimento ad una figura è "Come si vede in FIGURA 5.2 . . . ".

5.5 Bulleted List

- O ="Intrusion", $\neg O$ ="Non-intrusion";
- A ="Alert reported", $\neg A$ ="No alert reported".

5.6 Numbered List

1. O ="Intrusion", $\neg O$ ="Non-intrusion";
2. A ="Alert reported", $\neg A$ ="No alert reported".

5.7 A Description

Time refers to the use of *timestamp* information, extracted from network packets, to model normal packets. For example,

normal packets may be modeled by their minimum and maximum inter-arrival time.

Header means that the ***TCP!*** (**TCP!**) header is decoded and the fields are modeled. For example, normal packets may be modeled by the observed ports range.

Payload refers to the use of the payload, either at ***IP!*** (**IP!**) or **TCP!** layer. For example, normal packets may be modeled by the most frequent byte in the observed payloads.

Stochastic means that stochastic techniques are exploited to create models. For example, the model of normal packets may be constructed by estimating the sample mean and variance of certain features (e.g., port number, content length).

Deterministic means that certain features are modeled following a deterministic approach. For example, normal packets may be only those containing a specified set of values for the ***TTL!*** (**TTL!**) field.

Clustering refers to the use of clustering (and subsequent classification) techniques. For instance, payload byte vectors may be compressed using a ***SOM!*** (**SOM!**) where class of different packets will stimulate neighbor nodes.

5.8 An Equation

$$d_a(i,j) := \begin{cases} K_a + \alpha_a \delta_a(i,j) & \text{if the elements are different} \\ 0 & \text{otherwise} \end{cases} \tag{5.1}$$

5.9 A Theorem, Proposition & Proof

Theorem 5.9.1 $a^2 + b^2 = c^2$

Proposition 5.9.2 $3 + 3 = 6$

Proof 5.9.1 *For any finite set* $\{p_1, p_2, ..., p_n\}$ *of primes, consider* $m = p_1 p_2 ... p_n + 1$. *If* m *is prime it is not in the set since* $m > p_i$

for all i. If m is not prime it has a prime divisor p. If p is one of the p_i then p is a divisor of $p_1p_2...p_n$ and hence is a divisor of $(m - p_1p_2...p_n) = 1$, which is impossible; so p is not in the set. Hence a finite set $\{p_1, p_2, ..., p_n\}$ cannot be the collection of all primes.

5.10 Definition

Definition 5.10.1 (Anomaly-based IDS!) *An* anomaly-based **IDS!** *is a type of **IDS!** that generate alerts $\mathbb{A}$ by relying on normal activity profiles.*

5.11 A Remark

Remark 1 *Although the network stack implementation may vary from system to system (e.g., Windows and Cisco platforms have different implementation of **TCP!**).*

5.12 An Example

Example 5.12.1 (Misuse *vs.* Anomaly) *A misuse-based system M and an anomaly-based system A process the same log containing a full dump of the system calls invoked by the kernel of an audited machine. Log entries are in the form:*

```
<function_name>(<arg1_value>, <arg2_value>, ...)
```

5.13 Note

Note 5.13.1 (Inspection layer) *Although the network stack implementation may vary from system to system (e.g., Windows and Cisco platforms have different implementation of **TCP!**), it is important to underline that the notion of IP, TCP, HTTP* packet *is well defined in a system-agnostic way, while the notion of* operating system activity *is rather vague and by no means standardized.*

Bibliografia

Damiano Bolzoni, Sandro Etalle, Pieter H. Hartel, and Emmanuele Zambon. Poseidon: a 2-tier anomaly-based network intrusion detection system. In *IWIA*, pages 144–156. IEEE Computer Society, 2006. ISBN 0-7695-2564-4.

Gabriela F. Cretu, Angelos Stavrou, Michael E. Locasto, Salvatore J. Stolfo, and Angelos D. Keromytis. Casting out demons: Sanitizing training data for anomaly sensors. *Security and Privacy, IEEE Symposium on*, 0:81–95, 2008. doi: http://doi.ieeecomputersociety.org/10.1109/SP.2008.11.

Christopher Kruegel, Thomas Toth, and Engin Kirda. Service-Specific Anomaly Detection for Network Intrusion Detection. In *Proceedings of the Symposium on Applied Computing (SAC 2002)*, Spain, March 2002.

Matthew V. Mahoney and Philip K. Chan. Learning rules for anomaly detection of hostile network traffic. In *Proceedings of the 3rd IEEE International Conference on Data Mining*, page 601, 2003. ISBN 0-7695-1978-4.

M.V. Mahoney and P.K. Chan. Detecting novel attacks by identifying anomalous network packet headers. Technical Report CS-2001-2, Florida Institute of Technology, 2001.

M. Ramadas. Detecting anomalous network traffic with self-organizing maps. In *Recent Advances in Intrusion Detection 6th International Symposium, RAID 2003, Pittsburgh, PA, USA, September 8-10, 2003, Proceedings*, Mar 2003.

R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou. Specification-based anomaly detection: a new approach for detecting network intrusions. In *CCS '02: Proceedings of the 9th ACM Conference on Computer and communications security*, pages 265–274, New York, NY, USA, 2002. ACM Press. ISBN 1-58113-612-9.

Ke Wang and Salvatore J. Stolfo. Anomalous payload-based network intrusion detection. In *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID 2004)*. Springer-Verlag, September 2004.

Ke Wang, Janak J. Parekh, and Salvatore J. Stolfo. Anagram: A content anomaly detector resistant to mimicry attack. In *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID 2006)*, Hamburg, GR, September 2006. Springer-Verlag.

Stefano Zanero. Analyzing tcp traffic patterns using self organizing maps. In Fabio Roli and Sergio Vitulano, editors, *Proceedings 13th International Conference on Image Analysis and Processing - ICIAP 2005*, volume 3617 of *Lecture Notes in Computer Science*, pages 83–90, Cagliari, Italy, Sept. 2005. Springer. ISBN 3-540-28869-4.

Stefano Zanero and Sergio M. Savaresi. Unsupervised learning techniques for an intrusion detection system. In *Proceedings of the 2004 ACM Symposium on Applied Computing*, pages 412–419. ACM Press, 2004. ISBN 1-58113-812-1.

Indice analitico