

POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea Magistrale

Sistemi anti-DDoS distribuiti

Relatore

prof. Guido Marchetto

Studente

Stefano LOSCALZO

matricola: s267614

Supervisore aziendale

Centro Ricerche FIAT

dott. ing. Giovanni Giacosa

ANNO ACCADEMICO 2020-2021

Abstract

This short abstract, is typeset with the **abstract** environment (from the **report** document class) just to test if it works. or what concerns working, it works, but in Italian ist title turns out to be “Sommario” in bold face series and normal size; its apperance looks like a bad copy of what one obtains with the `\summary` command. In English, though, its title is “Abstract”, as it should be, since at the beginning of this template a suitable `\ExtendCapiions` command was issued.

Please, read the documentation in Italian (file `toptesi-it.pdf` in order to fully understand the difference beteesn “abstract” and “summary” in the context of this bundle.

Abstract

Gli attacchi di denial of Service distribuiti (DDoS) sono uno dei maggiori problemi di sicurezza delle reti. Hanno lo scopo di impedire ad utenti legittimi l'accesso a dei servizi o degradare loro le prestazioni. In questa tesi proveremo a identificare anomalie riconducibili ad attacchi DDoS, in un contesto di una rete aziendale con più sedi, usando un riconoscimento delle anomalie effettuato tramite rete neurale allenata su dati provenienti dai router di più sedi aziendali e una successiva mitigazione degli attacchi tramite un agent sugli stessi.

Indice

1	Introduzione	1
1.1	Motivazione	1
1.2	Gli attacchi DDoS	1
1.2.1	Tipologia di attacchi DDoS	1
1.2.2	Vittime attacchi DDoS	1
1.2.3	Diffusione attacchi DDoS	1
1.3	Organizzazione della tesi	1
2	Riconoscimento anomalie	3
2.1	Motivazione	3
2.2	Reti neurali e funzionamento	3
2.2.1	Autoencoders	3
2.2.2	Modello della rete	3
2.3	Selezione features	3
2.3.1	Collectd	3
2.3.2	NDPI	3
2.4	Test sulle anomalie	3
2.4.1	Tool utilizzati	3
2.4.2	Risultati	3
3	Mitigazione degli attacchi	5
3.1	Introduzione	5
3.2	Funzionamento	5
3.2.1	eBPF	5
3.2.2	BCC	5
3.3	Test sulle anomalie	5
3.3.1	Tool utilizzati	5
3.3.2	Risultati	5
4	Lavoro futuro	7
6	Conclusioni	11

Capitolo 1

Introduzione

1.1 Motivazione

Prova

1.2 Gli attacchi DDoS

Prova prova

1.2.1 Tipologia di attacchi DDoS

1.2.2 Vittime attacchi DDoS

1.2.3 Diffusione attacchi DDoS

1.3 Organizzazione della tesi

Capitolo 2

Riconoscimento anomalie

2.1 Motivazione

Prova

2.2 Reti neurali e funzionamento

Prova prova

2.2.1 Autoencoders

2.2.2 Modello della rete

2.3 Selezione features

2.3.1 Collectd

2.3.2 NDPI

2.4 Test sulle anomalie

2.4.1 Tool utilizzati

2.4.2 Risultati

Capitolo 3

Mitigazione degli attacchi

3.1 Introduzione

Prova

3.2 Funzionamento

Prova prova

3.2.1 eBPF

3.2.2 BCC

3.3 Test sulle anomalie

3.3.1 Tool utilizzati

3.3.2 Risultati

Capitolo 4

Lavoro futuro

Capitolo 5

Conclusioni

Bibliografia

- [1] G. Galilei, *Nuovi studii sugli astri medicei*, Manuzio, Venetia, 1612.
- [2] E. Torricelli, in “La pressione barometrica”, *Strumenti Moderni*, Il Porcellino, Firenze, 1606.
- [3] E. Torricelli e A. Vasari, in “Delle misure”, *Atti Nuovo Cimento*, vol. III, n. 2 (feb. 1607), p. 27–31.
- [4] Duane J.T., *Learning Curve Approach To Reliability Monitoring*, IEEE Transactions on Aerospace, Vol. 2, pp. 563-566, 1994
- [5] Chiesa S., *Affidabilità, sicurezza e manutenzione nel progetto dei sistemi*, CLUT, gennaio 2008
- [6] Chiesa S., Fioriti M., Fusaro R., *On Board System Technological Level Improvement Effect on UAV MALE*
- [7] Bigliano M., *Sicurezza nell’installazione di un velivolo senza pilota MALE; applicazione di metodologia di Zonal Safety Analysis al velivolo del Progetto SAvE*, Politecnico di Torino, maggio 2010
- [8] Chiesa S., Di Meo G.A., Fioriti M., Medici G., Viola N., *ASTRID - Aircraft on board Systems sizing and TRade-off analysis in Initial Design*, Research Bulletin, Warsaw University of Technology, Institute of Aeronautics and Applied Mechanics, p. 1-28, 17-19, ottobre 2012