

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	3
1.2.3	Diffusione attacchi DDoS	3
1.3	Organizzazione della tesi	5
2	Riconoscimento anomalie	7
2.1	Motivazione	7
2.2	Reti neurali e funzionamento	7
2.2.1	Autoencoders	7
2.2.2	Modello della rete	7
2.3	Selezione features	7
2.3.1	Collectd	7
2.3.2	NDPI	7
2.4	Test sulle anomalie	7
2.4.1	Tool utilizzati	7
2.4.2	Risultati	7
3	Mitigazione degli attacchi	9
3.1	Introduzione	9
3.1.1	Bloccare l'ip spoofing	9
3.2	Funzionamento	9
3.2.1	eBPF	9
3.2.2	BCC	9
3.3	Test sulle anomalie	9
3.3.1	Tool utilizzati	9
3.3.2	Risultati	9
4	Lavoro futuro	11

5 Conclusioni	13
Elenco delle figure	15
Bibliografia	17

Capitolo 1

Introduzione

1.1 Motivazione

Prova

1.2 Gli attacchi DDoS

Gli attacchi di Denial of Service (DoS) sono degli attacchi nel campo della sicurezza informatica che mirano a interrompere la fruizione di un servizio, fornito da un host connesso a internet, da parte di utenti legittimi. L'attacco ha l'obiettivo di esaurire le risorse dell'host in modo da non consentirgli di erogare le risposte ai richiedenti. Nel caso in cui la sorgente del traffico che mira a creare disservizi non sia unica, si parla di attacchi di denial of service distribuiti (Distributed Denial of Service).

1.2.1 Tipologia di attacchi DDoS

Gli attacchi DDoS possono essere suddivisi in due categorie principali in base al loro funzionamento. La prima si basa sul mandare alla vittima pacchetti malformati in grado di sfruttare un bug o una falla a livello applicativo. La seconda categoria invece si basa su tecniche per colpire l'infrastruttura del servizio, per il funzionamento di questa tecnica vengono usati uno o entrambi i seguenti metodi: uno punta sull'interruzione della connessione di rete grazie all'esaurimento della banda o della capacità di processamento dei router o di entrambe, nel secondo caso l'obiettivo dell'attaccante è di esaurire le risorse (es. sockets, CPU, memoria) del server che ospita il servizio [1].

L'obiettivo di questa sarà concentrato sul rilevamento e la mitigazione della seconda categoria di attacchi, basata sull'esaurimento delle risorse.

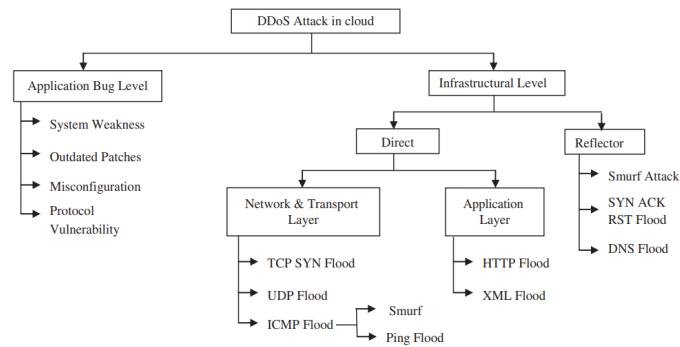


Figure 1. DDoS attack typology of cloud computing. (Adapted with permission from Osanaiye et al., 2016.]

Figura 1.1. Tipologie di attacchi DDoS [3]

Attacchi basati sul flooding

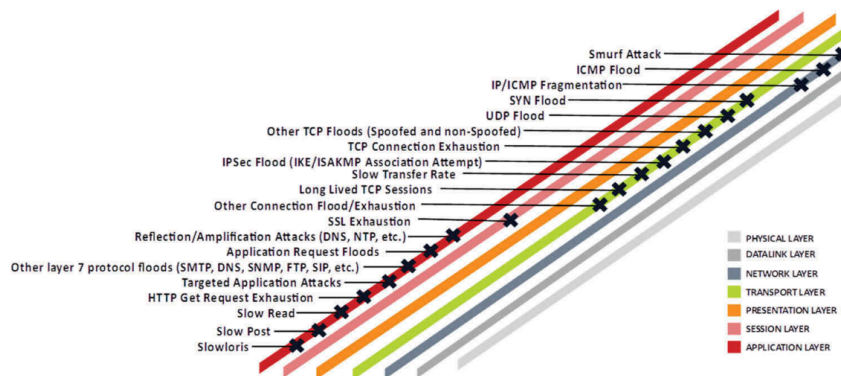


Figure 7. Distributed Denial of Service (DDoS) attack types across network layers.

Figura 1.2. Attacchi per livello [4]

Network/transport-level DDoS flooding attacks Gli attacchi di denial of service che mirano

Application-level DDoS flooding attacks

DDoS con obiettivo la riduzione della qualità del servizio

1.2.2 Vittime attacchi DDoS

I target degli attacchi DDoS possono variare molto da un utente domestico ad un governo [2].

Per capire maggiormente chi possono essere le vittime di un attacco bisogna analizzare le motivazioni che spingono gli attaccanti e con le diverse motivazioni può cambiare anche la portata dell'attacco. Per semplicità possiamo dividere gli incentivi di un attacco in cinque principali categorie [1][2]:

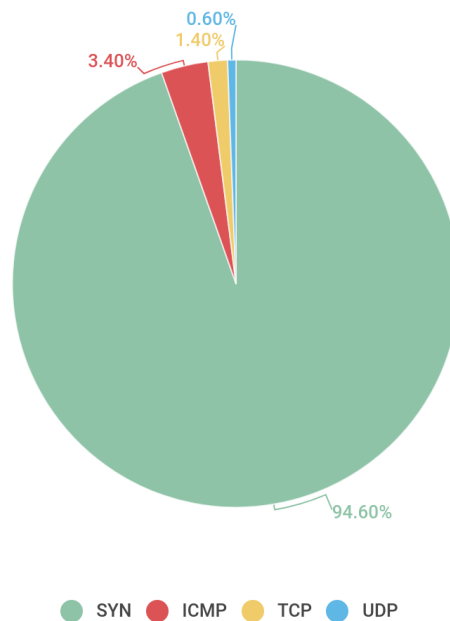
- Beneficio economico o finanziario: sono gli attacchi che riguardano principalmente le aziende, sono considerati i più pericolosi e difficili da fermare, perché mirano ad ottenere benefici finanziari dagli attacchi. I creatori dell'attacco normalmente sono persone con esperienza.
- Vendetta: questa Tipologia di attacchi sono messi in atto da persone, solitamente con uno scarso livello tecnico, a fronte di un'apparente ingiustizia percepita.
- Credo ideologico: alcuni attaccanti si trovano ad effettuare attacchi contro degli obiettivi per motivi ideologici. È una motivazione di attacco meno comune delle altre, ma può portare ad attacchi di grande entità.
- Sfida intellettuale: gli utenti che sviluppano attacchi per questa motivazione che vogliono imparare e sperimentare a lanciare attacchi, spesso sono giovani appassionati di hacking che grazie alla facilità con cui si possono affittare botnets o utilizzare semplici tool riescono ad effettuare con successo DDoS.
- Cyberwarfare: gli attaccanti di questa categoria appartengono ad organizzazioni terroristiche o militari di un paese e sono politicamente motivati ad attaccare risorse critiche di un altro paese. Un grande numero di risorse viene usato per questa tipologia di attacco e può paralizzare le infrastrutture critiche di un paese, portando ad un grave impatto economico.

1.2.3 Diffusione attacchi DDoS

Nel mondo gli attacchi a fine 2020 la quasi totalità degli attacchi DDoS proveniva da botnets, con target principali in Cina e negli Stati Uniti. Le tipologie di attacco maggiormente utilizzate sono guidate dal *Syn Flood* che copre più del 90% della totalità degli attacchi, seguito da *ICMP flooding* e *UDP flooding* [5] [6].

Attacchi DDoS famosi

Prova prova



kaspersky

Figura 1.3. Distribuzione di attacchi DDoS per tipologia, Q3 2020 [6]

Attacchi basati su botnets

Gli attacchi basati su botnets sono un grande problema per l'implementazione di sistemi anti-DDoS perché un grande numero di “zombie” rende l'attacco più distruttivo e spesso utilizzano ip spoofing, il che rende più difficile il tracciamento all'indietro per determinare i bot. [1] I bot possono essere controllati dall'artefice dell'attacco tramite tre architetture:

- IRC-based: architettura client-server in cui ad ogni server si possono collegare centinaia di dispositivi, utilizza un protocollo testuale e utilizzando porte non standard rende molto difficile il riconoscimento del comando per lanciare un DDoS, il quale si può nascondere facilmente nel grande traffico dei server IRC, ma il singolo server a cui si connettono tutti i client può essere considerato un single point of failure.
- Web based: ogni bot scarica periodicamente delle informazioni tramite una richiesta web ad un server, i comandi di questa tipologia di controllo sono i più difficili da tracciare.

- P2P based: [4] pagina 46

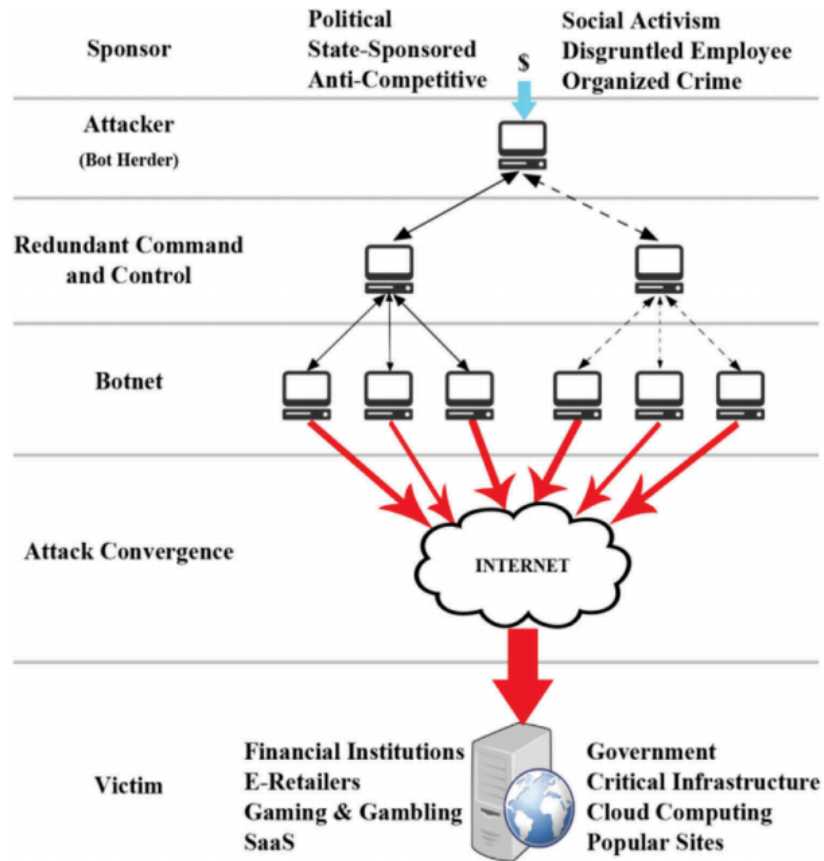


Figura 1.4. Struttura di lancio di attacchi DDoS [4]

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

3.1.1 Bloccare l'ip spoofing

L'ip spoofing permettere di usare la tecnica dell'amplification

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

Elenco delle figure

1.1	Tipologie di attacchi DDoS [3]	2
1.2	Attacchi per livello [4]	2
1.3	Distribuzione di attacchi DDoS per tipologia, Q3 2020 [6]	4
1.4	Struttura di lancio di attacchi DDoS [4]	5

Bibliografia

- [1] Saman Taghavi Zargar, James Joshi and David Tipper *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*, 2013. ()
- [2] Tasnuva Mahjabin, Yang Xiao, Guang Sun and Wangdong Jiang *A survey of distributed denial-of-service attack, prevention, and mitigation techniques*, 2017. (<https://journals.sagepub.com/doi/10.1177/1550147717741463>)
- [3] Neha Agrawal and Shashikala Tapaswi *Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey*, 2017. (<https://doi.org/10.1080/19393555.2017.1282995>)
- [4] Jasmeen Kaur Chahal, Abhinav Bhandari and Sunny Behal *Distributed Denial of Service Attacks: A Threat or Challenge*, 2019. (<https://doi.org/10.1080/13614576.2019.1611468>)
- [5] kaspersky securitylist.com *DDoS Report - DDoS attacks in Q4 2020* , 2020. (<https://securelist.com/ddos-attacks-in-q4-2020/100650/>)
- [6] kaspersky securitylist.com *DDoS Report - DDoS attacks in Q3 2020* , 2020. (<https://securelist.com/ddos-attacks-in-q4-2020/100650/>)