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 `\ExtendCapions` 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

Capitolo 1

Introduzione

1.1 Motivazione

Le piccole e medie imprese sono sempre più informatizzate e dipendenti da servizi informatici per poter continuare a lavorare. Per questo motivo scoprire e analizzare il traffico anomalo che passa sulle reti aziendali è sempre più importante, il nostro obiettivo è farlo ad un basso costo, senza aggiungere applicativi che richiedono molta potenza di calcolo o di banda ai router che compongono la rete. Punteremo a scoprire le anomalie nei dati di rete di singoli flussi e dati aggregati analizzando i dati su un server aggiuntivo che si occuperà anche di mitigare l'attacco informando i router sui flussi da bloccare. Gli attacchi maggiormente presi in considerazione in questa tesi sono gli attacchi di Distributed Denial of Service, ma i suoi principi possono essere applicati anche ad altre tipologie di anomalie. Inoltre raccogliere informazioni sull'utilizzo della rete può portare anche alla risoluzioni di problemi non derivanti da attacchi.

1.2 Scenario

Per fare questa tesi abbiamo preso in considerazione un tipico scenario aziendale, in cui esiste una sede centrale, ben protetta e su cui sono ospitati i servizi dell'azienda e tante sedi periferiche: uffici, negozi o altro, collegati ai servizi della sede centrale tramite un overlay MPLS o una VPN. Le sedi periferiche sono quelle più esposte sotto l'aspetto della sicurezza (todo: magari spiegare i motivi), per questo motivo il nostro obiettivo è quello di proteggere i servizi aziendali e la rete centrale dai pc connessi alle reti degli uffici. L'organizzazione di Tiesse e di molti suoi clienti è caratterizzata da questo scenario, per questo motivo le prove da me effettuate si basano sull'analisi del traffico proveniente dall'ufficio di Torino e mirano a proteggere i servizi aziendali presenti nella sede centrale di Ivrea a cui l'ufficio di Torino è collegato tramite una VPN. Un altro caso possibile di utilizzo di questa

soluzione è la distribuzione dei servizi in cloud, in cui l'azienda non ha il controllo dell'infrastruttura di rete.

1.3 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).

1.3.1 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 ana 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].

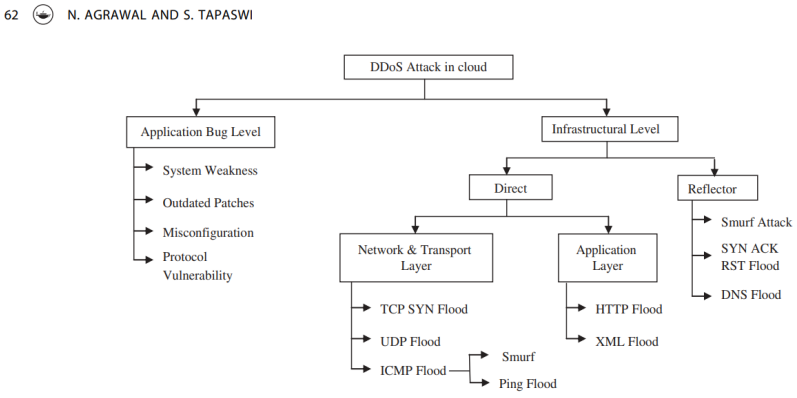

Figura 1.1. Tipologie di attacchi DDoS [4]

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

Attacchi basati sul flooding

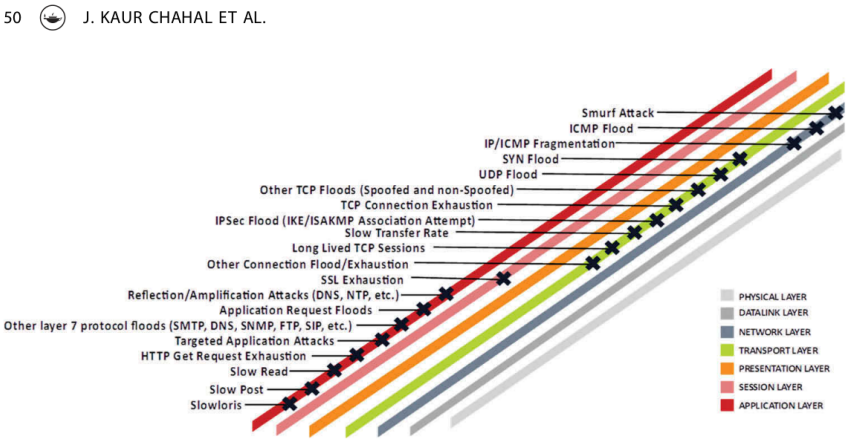

Figure 7. Distributed Denial of Service (DDoS) attack types across network layers.

Figura 1.2. Attacchi per livello [5]

Network/transport-level DDoS flooding attacks Gli attacchi di denial of service che mirano ad esaurire le risorse di rete si basano sull'invio di molti pacchetti che consumino totalmente la banda della vittima, queste tipologia di attacco può essere effettuata in maniera diretta: *flooding attacks* e *protocol exploitation attacks*, nel primo caso la vittima viene inondata di pacchetti (UDP flood, ICMP flood, DNS flood, VoIP flood an etc.), in questo caso la banda aggregata in uscita di tutti gli attaccanti deve essere superiore a quella del servizio che si vuole interrompere, nel secondo caso vengono sfruttane delle caratteristiche dei protocolli della vittima in modo da consumare una grande quantità di risorse (es. TCP SYN flood, TCP SYN-ACK flood, RST/FIN flood e ecc).

Gli attacchi che non vengono che non vengono effettuati in maniera diretta invece sfruttano la riflessione o l'amplificazione: nella *Reflection-based flooding attacks* chi attacca manda un particolare pacchetto, indirizzandolo ad un riflettore e questo riflettore manda le sue risposte alla vittima, in modo da esaurire le risorse della vittima. Un esempio di questo attacco sono lo Smurf e il Fraggle, nel primo vengono mandati ICMP Echo Request ad una sottorete, usando come ip di destinazione l'indirizzo broadcast e con ip spoofing, specificando come ip sorgente l'ip della vittima, causando la risposta di tutti gli host verso l'indirizzo della vittima [2]. Gli *Amplification-based flooding attacks* sfruttano servizi che restituiscono risposte più grandi della richiesta ricevuta, un esempio è il DNS amplification, che riesce

a moltiplicare più di 20 volte il pacchetto in arrivo e sfruttando l'ip spoofing la risposta viene manda alla vittima [1].

Application-level DDoS flooding attacks Gli attacchi DDoS al livello applicativo hanno lo scopo di terminare le risorse del server(sockets, cpu, memory, disk/db bandwidth, I/O bandwidth) e di solito usano meno banda, rispetto gli attacchi di alla rete, per questo motivo è anche più difficile identificarli. Le tecniche utilizzate sono simili alle precedenti. Degli esempi sono l'HTTP flooding che grazie con molte richieste, obbliga il server a produrre risposte che possono essere computazionalmente pesanti, oppure l'SQL Injection per imporre un lock sul database e bloccare il funzionamento dell'applicazione, altri attacchi possono essere l'HTTP fragmentation, lo slowpost attack, slowreading attack e lo slowloris attack, tutte che mirano a mantenere la connessione aperta mandando o ricevendo pochi dati per volta [1]. Gli attacchi di tipo applicativo possono essere molto eterogenei e non possono essere mitigati a livello di rete/trasporto, per questo motivo questa tesi prenderà in considerazione solo gli attacchi trattati al paragrafo precedente.

DDoS con obiettivo la riduzione della qualità del servizio L'unico obiettivo possibile degli attacchi DDoS non è la sola interruzione del servizio, ma un altro risultato è la degradazione del servizio, consumando una parte di risorse destinate agli utenti legittimi e creando loro ritardi nelle risposte. Questo risultato può essere raggiunto utilizzando dei packet rate più bassi, e di conseguenza meno rilevabili o dei rate variabili [4, 5].

1.3.2 Vittime attacchi DDoS

I target degli attacchi DDoS possono variare molto da un utente domestico ad un governo [3].

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][3]:

- 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 mesi 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.

1.3.3 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* [6] [7].

Attacchi DDoS famosi

Prova prova

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 dell'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.

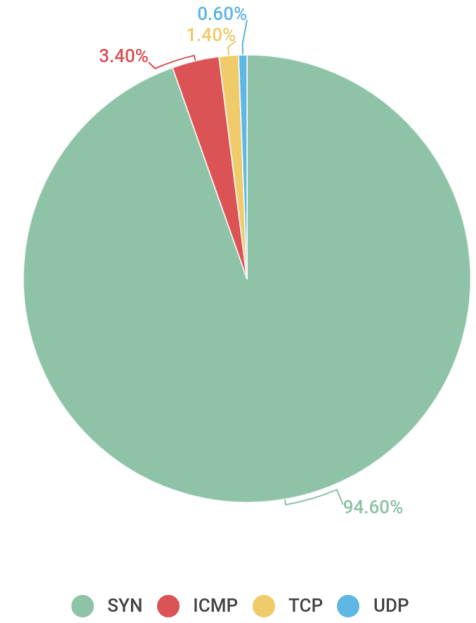

Figura 1.3. Distribuzione di attacchi DDoS per tipologia, Q3 2020 [7]

- P2P based: [5] pagina 46

1.4 Organizzazione della tesi

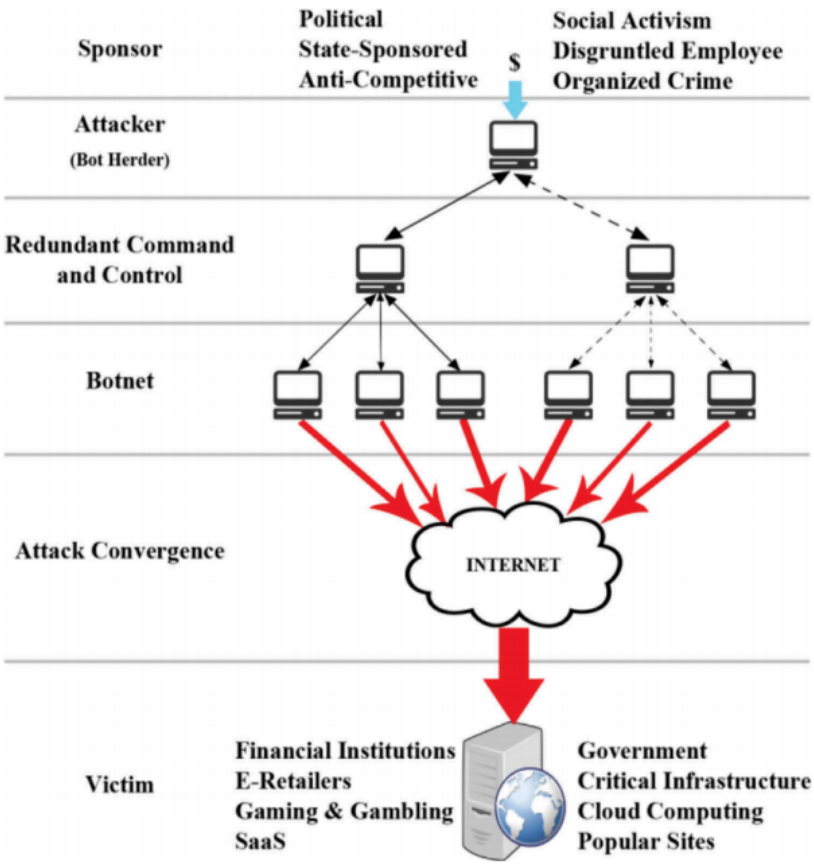

Figura 1.4. Struttura di lancio di attacchi DDoS [5]

Capitolo 2

Stato dell'arte dei sistemi anti-DDoS

2.1 Riconoscimento DDoS

La fase di riconoscimento degli attacchi DDoS è un importante passo per la mitigazione degli attacchi, questa fase diventa più facile maggiormente ci avviciniamo alla vittima dell'attacco, ma più ci si allontana dalla sorgente dell'attacco e più diventa difficile identificarla. In letteratura esistono due tecniche per identificare i flussi malevoli: signature-based detection e anomaly-based detection.

2.1.1 Signature-based detection

La signature-based detection è un meccanismo che si basa su attacchi DDoS conosciuti per differenziare la loro firma, dai normali flussi della rete. Queste soluzioni hanno un buon successo con attacchi DDoS conosciuti, ma non sono in grado di rilevare nuove tipologie ti attacco di cui non si conosce ancora la signature. Questi sistemi si possono basare su pattern matching (es. Bro/Zeek), su regole (es. Snort), sulla correlazione di informazioni di management sul traffico, o sull'analisi spettrale.

2.1.2 Anomaly-based detection

I meccanismi di rilevamento delle anomalie possono riconoscere attacchi anche su attacchi non conosciuti, basandosi su soglie per differenziare il traffico normale e malevolo, ma la scelta di esse è una grande sfida per questa tipologia di tecniche. I metodi più diffusi si basano su metodi statistici, di data mining o intelligenze artificiali.

2.2 Contromisure attacchi DDoS

Gli attacchi DDoS si ramificano ad imbuto dalle sorgenti verso la vittima, per questa ragione più si è vicini alla vittima e più l'attacco sarà facile da riconoscere, ma più difficile da mitigare. Per questa ragione le tecniche di mitigazione vengono suddivise in base al luogo in cui vengono azionate.

2.2.1 Soluzioni alla sorgente

Questa tipologia di soluzioni sono adottate vicino alle sorgenti dell'attacco per impedire agli utenti della sottorete di generare attacchi DDoS. Queste soluzioni possono essere applicate agli edge router degli Autonomous System (AS) di accesso.

Degli esempi di soluzioni sono:

- Filtri in ingresso e uscita agli edge router delle sorgenti:
- D-WARD:
- MULTOPS:
- MANAnet's Reverse Firewall:

I problemi di questa soluzione sono che dovrebbe essere implementata su gli edge router ti tutti gli AS di accesso per permettere una copertura totale, inoltre è difficile differenziare il traffico legittimo, da quello malevolo e non meno importante non è chiaro chi sia il responsabile del mantenimento economico di questo servizio [1].

2.2.2 Soluzioni alla destinazione

Esistono soluzioni che si possono applicare agli edge router della vittima, possono analizzare il comportamento della vittima e il suo traffico usuale e riconoscere le anomalie [1, 2]. Delle soluzioni posizionate in questi luoghi possono essere dei proxy, firewall che gestiscono le connessioni semi aperte in caso di syn flood, l'utilizzo sistemi di tracciamento implementati in alcuni router (in caso di ip spoofing), Questi sistemi di difesa possono diventare i target degli attacchi, poiché spesso richiedono una grande quantità di memoria e potenza di processamento per effettuare le osservazioni delle misure statistiche [5].

2.2.3 Soluzioni sulla rete

I sistemi anti-DDoS sulla rete si basano sui router o su firewall installati sulla rete dell'operatore. Una prima soluzione adottata è quella del Router based packet filter, la quale si basa sui criteri dell'ingress filtering, ma applicandola ai router

nel core della rete. Il traffico per ogni link tendenzialmente viene generato da un ristretto intervalli di indirizzi ip, quando appare un indirizzo ip sospetto viene filtrato, questa soluzione è adatta a rilevare attacchi che utilizzano ip spoofing, ma è inutile nel caso di utilizzo di ip genuini. Altre soluzioni mirano ad identificare i router nel core di internet che sono stati compromessi e si comportano in anomalo, oppure mirano all'installazione di detection systems (DSs) che permettono di rilevare pattern anomali, ma sono computazionalmente molto dispendiose.

2.2.4 Soluzioni distribuite

Le soluzioni distribuite creano una cooperazione tra i luoghi di installazione delle difese, alla sorgente vengono installati i sistemi di difesa per filtrare l'attacco, mentre sulla rete della vittima viene effettuato il riconoscimento dell'attacco. Questa soluzione porta sia il vantaggio della facilità di riconoscimento degli attacchi possibile alla destinazione, sia l'efficienza dei sistemi per mitigare gli attacchi alla sorgente.

2.3 Tolleranza

Capitolo 3

Riconoscimento anomalie

3.1 Stato dell'arte dell'anomaly detecion - trovare titolo

3.1.1 Sfide dell'anomaly detection

3.1.2 Tipologia delle anomalie

Tipologia degli attacchi di rete

3.1.3 Sistemi di rilevamento delle anomalie

Basati sulla classificazione

Basati sulla statistica

3.2 Motivazione

Prova

3.3 Reti neurali e funzionamento

3.3.1 Autoencoders

3.4 Selezione features

3.4.1 Collectd

3.4.2 NDPI

3.5 Il mio tool

3.5.1 Struttura

3.5.2 Modello della rete

3.5.3 Train

3.5.4 Evaluate

3.6 Test sulle anomalie

3.6.1 Tool utilizzati

Parlare come funzionano i tool che ho fatto

3.6.2 Risultati

Capitolo 4

Mitigazione degli attacchi

4.1 Introduzione

Prova

4.1.1 Bloccare l'ip spoofing

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

4.2 Funzionamento

Prova prova

4.2.1 eBPF

4.2.2 BCC

4.3 Test sulle anomalie

4.3.1 Tool utilizzati

4.3.2 Risultati

Capitolo 5

Lavoro futuro

Capitolo 6

Conclusioni

Elenco delle figure

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] s

[3] 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)

[4] 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)

[5] 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)

[6] kaspersky securitylist.com *DDoS Report - DDoS attacks in Q4 2020* , 2020. (https://securelist.com/ddos-attacks-in-q4-2020/100650/)

[7] kaspersky securitylist.com *DDoS Report - DDoS attacks in Q3 2020* , 2020. (https://securelist.com/ddos-attacks-in-q4-2020/100650/)

[8] Michael A. Nielsen *Neural Networks and Deep Learning* , Determination Press, 2015. (http://neuralnetworksanddeeplearning.com/)

[9] Keras documentation

[10] Mohiuddin Ahmed, Abdun Naser and Mahmood Jiankun-Hu, *A survey of network anomaly detection techniques* , 2016. (https://doi.org/10.1016/j.jnca.2015.11.016)

[11] Raghavendra Chalapathy and Sanjay Chawla, *Deep Learning for Anomaly Detection: A Survey* , 2019. (https://arxiv.org/abs/1901.03407v2)

[12] Varun Chandola, Arindam Banerjee and Vipin Kumar, *Anomaly detection: A survey*, 2009. (https://dl.acm.org/doi/abs/10.1145/1541880.1541882)