Indice

Introduzione

Il problema della sicurezza nelle reti è un tema *evergreen* che ha preoccupato, preoccupa e preoccuperà sempre non solo le grandi aziende e le grandi organizzazioni, che devono gestire incenti moli di dati, ma ogni singola persona.

Con l'evolversi della tecnologia, le reti si sono trovate a essere il bersaglio principale e, naturalmente, fin da subito, si è cercato, di contrastarle con appropriate misure.

Le tecnologie passate, a causa dei pochi strumenti a disposizione, non davano gli stessi risultati di quelle attuali, anche se, nel loro piccolo, hanno dato un contributo significativo, spianando il terreno "d'attacco" e, dando un *input* per creare tecniche sempre più efficienti.

Le nuove tecnologie, infatti, consentono di raggiungere risultati sempre più mirati e più efficaci nel bloccare gli "attacchi" informatici.

Alla luce di quanto detto, il presente lavoro si propone di analizzare i principali attacchi che interessano una rete, valutando delle soluzioni che già esistono in letteratura. Soluzioni utili per prevenire l'attacco o, quantomeno, per riuscire a risalire all'attaccante, per poter prendere provvedimenti e aumentare la sicurezza del computer, preso di mira, e bloccare la criminalità informatica.

Come noto, ci sono *hacker* che entrano nei sistemi di rete per danneggiarli e *hacker*, invece, che mettono la loro abilità al servizio della ricerca, dando un contributo alla soluzione dei problemi.

Alcuni *hacker*, infatti, una volta scoperti, hanno deciso di passare dalla parte dei "buoni", offrendo il loro "ingegno" per la soluzione di buone cause, come aiutare la polizia a incastrare i criminali.

Per riuscire a contrastare un attacco lo si deve conoscere a fondo, rilevarne tutti i punti di forza e di debolezza e agire sui punti deboli dei software "maligni" per contrastarli.

Nel primo capitolo si è cercato di fare una breve introduzione sull'evoluzione della comunicazione, dai primi segnali comunicativi fino alla nascita della grande rete di

Internet. Si è cercato, inoltre, di delineare i concetti base della sicurezza e come essi potrebbero essere compromessi. La ricerca, inoltre, ha focalizzato i principali tipi di attacco, in particolare quelli DoS e DDoS.

Tenendo ben presente che un attacco sfrutta dei particolari strumenti per arrivare alla "vittima", sono stati esaminati i *malware* (programmi malevoli, che si insediano all'interno delle vittime, facendo sì che l'attaccante riesca a prendere il pieno controllo della macchina).

Tra i vari *malware,* osservati, particolare attenzione è stata prestata ai virus informatici, ai *worm* e ai *Trojan horse*, cercando di mettere in evidenza anche i metodi di prevenzione, quali: anti-virus e nuovi approcci. A causa della crescita continua dei *malware,* infatti, gli studiosi che si occupano di sicurezza informatica sono alla continua ricerca di nuovi metodi per analizzare il comportamento di questi software maligni. Lo studio effettuato si propone, perciò, di delineare alcuni fra i principali approcci che l'attuale letteratura offre a questo proposito.

Quando si riscontra un problema, come trovare un programma che mostra un comportamento non del tutto normale, si lancia un allarme e si controlla nel *Database*, che contiene tutti i software maligni conosciuti, siccome, però, non sempre, il *Database* presenta il m*alware* rilevato, bisogna aggiornarlo continuamente.

Per l'analisi dei *malware* si è cercato di focalizzare l'attenzione su due approcci: Il TWMAN, che attraverso l'analisi comportamentale del software "anormale" riesce a trovare anche i *malware* che, il metodo basato sulla Virtual Machine non riesce a rilevare e il Behavior Image che analizza il comportamento sotto forma di immagini, e utilizzando, in particolare, una scala di colori.

A tal fine, sono stati presi in considerazione le tecniche per rilevare una tipologia particolare di *malware.*

Per quanto concerne i virus informatici la letteratura ha proposto vari approcci, ma in questa ricerca si porrà particolare attenzione su dei modelli che delineano la transazione del virus da uno stato all'altro cercando di mostrare come, quando il virus si trova in dei determinati stati è più soggetto a non infettare gli altri nodi e quindi vi è una diffusione molto lenta.

Per l'analisi dei *worm* si è cercato di delineare dei tipi particolari, detti NOC-*Worm* che rappresentano un giusto compromesso tra la rapida diffusione dei *Worm* e il loro rendersi invisibili.

Anche per questa tipologia di *worm,* la ricerca cercherà di illustrare dei processi che si basano sui passaggi di stato del *worm*.

Come gli informatici che cercano di contrastare gli *hacker*, con questo studio ho provato, mediante l'analisi di una tecnica che utilizza dei *worm* benigni per contrastare quelli maligni, ad avvalorare la tesi che un rilascio celere dei *worm* benigni può diminuire il tasso di infezione.

Per quanto riguarda i *Trojan horse*, per i quali generalmente si fanno poche indagini specifiche (di solito le si fanno più per individuare un *malware* generico), per prima cosa si andrà a osservare il comportamento del *Trojan horse*, come si instaura su una macchina e cosa fa per permettere all'attaccante di interagire con la vittima.

Per rilevare un *Trojan horse* è stata fatta un'indagine che ha lo scopo di creare un *Trojan horse* su una distribuzione di Ubuntu Linux per poi rilevarlo attraverso il Process Explorer che mostra tutti i processi che sono in esecuzione in quella macchina, anche quelli che mettono in evidenza caratteristiche che sono comuni a un *Trojan horse*. Un'altra indagine, come vedremo, mostra come il tracciamento dei processi torna sempre utile per individuare il *Trojan horse*. Indagine che utilizza il processo di tracciamento in Windows.

Per trovare il processo, e quindi il programma, la letteratura ci propone due tecniche, il ProcessTracer e il ProgramTracer. Tecniche che in questo studio saranno utilizzate per mostrare come sono applicate all'interno di una architettura che è il NetWatcher.

Nel terzo capitolo particolare attenzione sarà dedicata agli attacchi Denial of Service e Distributed Denial of Service che mirano a negare il servizio a un utente autorizzato; essi nascono per scopi economici, politico/religioso o logistico.

Si illustreranno, inoltre, attacchi di tipo Flooding che mirano a far sì che sul computer vittima ci sia una vera e propria "alluvione" di pacchetti o messaggi; attacchi di tipo "amplification attack", cosiddetti perché amplificano la quantità di dati usati dall'attaccante. Si cercherà anche di mostrare un esempio pratico delineando anche cosa fare per difendersi dall'attacco.

In particolare nel sottoparagrafo il lavoro mirerà a illustrare delle tecniche di prevenzione perché, come afferma il detto: "è meglio prevenire che curare", anche se, a volte, non si può fare altro che trovare i nodi infetti sul computer ed eliminarli.

È possibile, comunque, utilizzare delle contromisure per evitare che i PC siano vittime di attacchi DoS sia come protagonisti principali sia secondari.

Nella sezione 3.4 il lavoro vuole mostrare delle tecniche atte a fare delle vere e proprie indagini per risalire al colpevole dell'attacco. Come sulla scena del crimine anche nel nostro caso bisogna ricostruire il quadro, "marcare" tutti gli elementi che potranno essere utili per l'indagine, interrogare i testimoni e solo alla fine, mettendo insieme tanti piccoli tasselli si potrà risalire al colpevole.

Un metodo proposto dalla letteratura è quello di ricostruire il percorso partendo dalla vittima, seguendo il percorso inverso che seguono i pacchetti per arrivare a destinazione è, infatti, possibile risalire all'attaccante.

Questo metodo chiamato IP TRACEBACK utilizza due tecniche: il packet marking e il packet logging.

Nel packet marking i *router* vanno a marcare i pacchetti IP con la loro identificazione, la marcatura può avvenire in maniera deterministica o probabilistica a seconda che si utilizza determinist packet marking o probabilist packet marking.

Nel packet logging ogni *router* registra il pacchetto che lo ha attraversato utilizzando un approccio di IP TRACEBACK basato sulla tecnica Hash.

A questo proposito saranno presentati quattro approcci proposti dalla letteratura.

Per primo un approccio ibrido che ha l'abilità di tracciare un singolo pacchetto come l'approccio IP TRACEBACK basato sulla tecnica Hash, e di ridurre, allo stesso tempo, il tempo di conservazione e di accesso al *router* con la tecnica del packet marking.

Il contributo di questo approccio è di ridurre il tempo di memorizzazione di circa la metà e di ridurre il tempo di accesso richiesto per memorizzare i pacchetti grazie al numero di *router* vicini. In questo modo si va a costruire il grafo dell'attacco.

Un altro approccio è quello basato su deterministc packet marking e packet logging che cerca di sfruttare i vantaggi di entrambi e poi uno schema di marcatura

deterministica più flessibile il cui vantaggio principale è di avere bisogno di un minor numero di pacchetti.

Infine si esaminerà l'approccio proposto dalla letteratura che concerne uno schema basato sulla predizione (che vuole non sovrascrivere le informazioni di marcatura), mostrando come risultato che per costruire il percorso dell'attacco si impiegheranno molti meno pacchetti.