Introduzione

Il tema portante di questo lavoro è l'analisi dell'IP Traceback, tecnica che permette di trovare la sorgente di un attacco informatico DoS e DDoS. Per poter arrivare a parlare di questa tecnica si studieranno a fondo, inizialmente, i concetti di Rete di Telecomunicazione, per una conoscenza maggiore nel campo, le maggiori problematiche legate alla sicurezza nelle reti, gli attacchi informatici più importanti e dannosi e al come proteggersi da questi. Solamente dopo aver approfondito tutte queste tematiche, si potrà avere un quadro generale sui concetti legati all'IP Traceback.

La tesi è suddivisa in quattro parti:

Nella prima parte viene introdotto il concetto di "rete di telecomunicazione", tema centrale della tesi, andando ad analizzare in modo dettagliato le diverse tipologie di reti partendo da quelle basate sulla dimensione (LAN, MAN, ecc.) e i principi sulle quali si basano (commutazione di pacchetto e circuito), fino ad arrivare al concetto di "comunicazione". Una volta introdotto il concetto di rete si scende nei particolari andando ad esaminare tematiche connesse ad esso come: le diverse architetture di rete (ISO/OSI e TCP/IP) con le loro strutture a livelli, analizzando le principali differenze tra le due; i servizi, quindi la loro funzione ed il loro funzionamento; le informazioni, che viaggiano attraverso i diversi canali di comunicazione. Vedremo anche come, in base alla topologia, le reti possono essere divise in bus, anello, stella, ecc. e quali sono i principali mezzi di trasmissione, partendo dal cavo coassiale, alla più attuale fibra ottica. Passeremo poi all'analisi delle problematiche di accesso multiplo (per evitare le cosiddette collisioni) e alla descrizione dei diversi protocolli ad esso connessi quali ALOHA, SLOTTED ALOHA, CSMA e CSMA/CD; le principali reti standardizzate dell'IEEE quali la 802, con le particolari divisioni a livello collegamento, gli indirizzi MAC con le varie trame utilizzate (come sono composte) e le principali funzioni quali framing, controllo di errori e ritrasmissioni. Una volta definite queste caratteristiche delle reti, andremo ad approfondire la differenza tra "indirizzamento" ed "instradamento", funzioni basilari di una rete: la prima indica come vengono assegnati gli indirizzi IP quindi la suddivisione di questi in classi (A, B, C, D ed E), le differenze tra indirizzamento diretto ed indiretto, le Subnet Mask, la tecnica del VLSM ed il Supernetting; la seconda funzione, invece, permette di guidare l'informazione da una

sorgente ad una destinazione, grazie ad algoritmi di routing e protocolli vari. Concludiamo questa prima parte con un'analisi dettagliata sull'andamento dei mercati delle telecomunicazioni e dei servizi, di rete mobile e fissa, concentrandosi sulle differenze tra Nord e Sud Italia. Sarà presente anche un confronto, per quanto concerne la banda larga ed ultralarga, tra la situazione attuale in Italia e all'estero, con particolare attenzione sui servizi di cui potremmo usufruire se non fossimo "arretrati" rispetto agli altri paesi.

Nella seconda parte analizzeremo i principali attacchi informatici, classificati per tipo di attacco e vulnerabilità, ed il come avvengono grazie all'utilizzo di Backdoor, Exploit e quant'altro; le tecniche più importanti e pericolose come lo "Spoofing", falsificazione dell'identità di un soggetto o di una macchina, con i vari tipi di attacco in base al livello della pila protocollare attuato (o web), ed il "Network Sniffing", utilizzato per l'attività di intercettazione dei dati che transitano su una rete, con una descrizione dettagliata dei vari tipi attuabili. Ci concentreremo soprattutto sul concetto di "Virus", o software maligno, con la successiva classificazione in base al danno che può recare, seguita dall'analisi dei virus più famosi quali: i Worm, malware in grado di auto-replicarsi e capaci di modificare il computer infettato; i Trojan Horse, che non sono veri e propri virus ma veicoli per la loro trasmissione (da questo il nome); gli Spyware, programmi che comunicano con un server centrale scambiando informazioni di diverso genere sul conto della vittima,(siti visitati, preferenze e quant'altro) con particolare attenzione al caso "Echelon". Una volta analizzati in dettaglio i diversi tipi di virus, passiamo alla descrizione degli attacchi "Denial of Service", finalizzati non a violare la sicurezza di un sistema, ma ad utilizzare tecniche capaci di bloccare o rallentare quest'ultimo, classificati in attacchi diretti ed indiretti. Altra classificazione che possiamo fare è in base al tipo di attacco che può essere portato: da un singolo host o da più host. Per quanto riguarda quelli da singolo host troviamo: Syn-Flood, dal nome "inondazione di pacchetti di tipo SYN", è capace di bloccare un servizio o effettuare un crash del sistema; Smurf, consiste in una modalità di attacco più sofisticata che utilizza un flusso di pacchetti più grandi, in grado di passare attraverso una normale connessione via modem; RUDY, strumento utilizzato per eseguire attacchi lenti che durino a lungo. Per quanto riguarda invece quelli generati da più host, sono due quelli più dannosi: DDoS e DRDoS: DDoS funziona allo stesso modo del DoS portato da un singolo host, con l'unica differenza che, in questo caso appunto, è portato da più host (è proprio a questo che possiamo ricollegare il concetto di Zombie, Botnet e Botmaster); DRDoS invece

attacca con richieste al server molto veloci con indirizzo di provenienza coincidente con quello della vittima.

In conclusione andiamo ad analizzare il "perché" e quindi le possibili motivazioni che spingono questi utenti malevoli e il "come" potersi riparare in modo efficiente da questi attacchi. Alcuni metodi di protezione possono essere, ad esempio, il filtraggio dei pacchetti, la limitazione del traffico ed i sistemi di riconoscimento di intrusioni.

Nella terza parte ci si focalizza principalmente sul concetto di IP Traceback, argomento principale della tesi, che come accennato prima, è una tecnica capace di determinare in modo affidabile l'origine del traffico sulla rete. Molti sono i letterati che hanno cercato di dare definizioni chiare e precise in merito a questo argomento ed oggi sono continui i miglioramenti. Per poter classificare i regimi di traceback esistenti vi sono diverse categorie e tra le più importanti abbiamo il principio di base, le modalità di elaborazione e di posizione. La tecnica dell'IP Traceback utilizza criteri di marcatura sui pacchetti in transito sulla rete, dove ogni router decide se marcare o meno il pacchetto. Questa marcatura avviene su alcuni particolari bit, precisamente quelli destinati alla frammentazione con i relativi flag e può essere di due tipi: probabilistica o deterministica. Quando si utilizza la marcatura "probabilistica", ogni router calcola un valore che, se è minore della probabilità, marca positivamente il pacchetto, altrimenti lo marca negativamente (molto importante è anche il processo di ricostruzione del grafo, fondamentale per scovare la fonte cattiva). L'utilizzo di questa marcatura presenta vantaggi e svantaggi considerando overhead computazionali, falsi positivi, spoofing della fonte, ecc. Quando si utilizza la marcatura "deterministica", al contrario di quella probabilistica, vengono marcati tutti i pacchetti che transitano attraverso un determinato router. Come per la probabilistica, anche quella deterministica presenta dei pro e dei contro (solo successivamente verranno esaminate approfonditamente queste tecniche in modo da poterle confrontare secondo i principali criteri di valutazione). In conclusione vengono esaminati anche altri approcci per l'IP Traceback tipo quelli basati sui router e fuori banda.

Nella quarta ed ultima parte viene presentata una modifica del normale funzionamento dell'IP Traceback con marcatura probabilistica. Questa modifica consiste principalmente nella scelta dei bit da marcare: oltre ad utilizzare i bit di cui usufruisce il PPM di base, vengono aggiunti alcuni bit del campo Options; questo permette ad un pacchetto di contenere più "firme" e quindi di aumentare la velocità della ricostruzione

del pacchetto e di diminuire il numero dei pacchetti necessari, a discapito, però, di un tempo di elaborazione maggiore per ogni router.

Molteplici sono stati i test che hanno permesso un confronto tra la versione classica e quella implementata sulla base di criteri di valutazione quali, ad esempio, minimo numero di pacchetti, tempo di ritardo per nodo, tempo di ricostruzione del percorso d'attacco e numero di router appartenenti alla rete.