ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA

FACOLTÀ DI INGEGNERIA CON SEDE A CESENA

CORSO DI LAUREA IN INGEGNERIA E SCIENZE INFORMATICHE

ATTACCHI DOS IN AMBIENTE CLOUD

Elaborato in

Reti di Telecomunicazione

Relatore
Prof. Ing. FRANCO CALLEGATI

Presentato da
IVAN TESORO

SESSIONE IV

ANNO ACCADEMICO 2021/2022

A me
per aver sempre cercato un modo
e a tutti i miei amici e compagni di viaggio
che mi hanno supportato a trovarne almeno uno

Indice

Sommario

Gli attacchi DoS (Denial of Service) sono diventati un problema rilevante per gli utenti dei sistemi informatici connessi a Internet, specialmente dal momento in cui gli aggressori DDoS (Distributed Denial of Service, probabilmente la categoria più temibile di attacchi DoS) dirottano i sistemi delle vittime secondarie utilizzandoli per condurre un attacco coordinato su larga scala contro i sistemi delle vittime primarie. Man mano che vengono sviluppate nuove contromisure per prevenire o mitigare gli attacchi DoS, gli aggressori sviluppano costantemente nuovi metodi per aggirare queste nuove contromisure.

In questo documento, si descrivono i modelli di attacco DoS e viene proposta un'ampia tassonomia per identificare la portata di questi attacchi e le caratteristiche degli strumenti software utilizzati. Vengono illustrate somiglianze e modelli ricorrenti in attacchi e strumenti DoS differenti, auspicando di poter contribuire allo sviluppo di soluzioni più generalizzate per contrastare questo genere di attacchi.

Capitolo 1

Introduzione

Un sistema informatico si dice *distribuito* se è costituito da un insieme di nodi applicativi indipendenti che collaborano per ottenere obiettivi comuni attraverso un'infrastruttura di comunicazione hardware e software [1].

Il cloud computing include sia ciò che viene fornito come servizio su Internet, sia l'hardware alla base di tali servizi. Le risorse possono essere fornite e rilasciate molto facilmente, richiedendo poco o nessun intervento da parte del provider. Dal punto di vista dell'utente, le infrastrutture cloud sembrano fornire infinite risorse, adattabili alle proprie esigenze.

Nel concreto, una piccola start-up potrebbe non avere la necessità o le risorse finanziarie necessarie per acquistare determinate risorse informatiche, ma potrebbe non voler escludere del tutto le sue opzioni per una futura ed eventuale espansione, rendendo in tal caso il cloud computing particolarmente appropriato. In questo contesto, l'azienda pagherebbe semplicemente quanto effettivamente utilizzato, dato che le risorse possono essere rilasciate quando non sono più necessarie. In una rete cloud, gli utenti non possiedono i server di elaborazione. Possono accedere a numerosi servizi senza l'onere della gestione del cloud e i loro dati sono accessibili tramite più dispositivi come smartphone, tablet, portatili e così via. Più in generale, le caratteristiche principali del cloud computing sono le seguenti [2]:

• *Larga Scala*: per soddisfare le richieste dei clienti, aziende come Amazon, IBM, Microsoft, Yahoo e Google possiedono centinaia di migliaia di server distribuiti.

• *Pool di risorse*: i fornitori servono più clienti con servizi provvisori e scalabili. Questi servizi possono essere adattati in modo trasparente alle esigenze

dei clienti.

• *Accesso persistente alla rete*: gli utenti possono accedere ai servizi ovunque, attraverso qualsiasi tipo di terminale.

• *Elasticità rapida*: gli utenti possono aumentare e rilasciare le loro richieste in modo rapido e dinamico.

• *Self-service on-demand*: poiché un'infrastruttura cloud è un grande pool di risorse, gli utenti possono acquistare in base alle proprie esigenze. Il provider fornisce automaticamente i servizi e associa le risorse all'utente cloud, come richiesto.

• *Elevata estensibilità*: la portata di un'infrastruttura cloud può essere estesa per soddisfare le crescenti esigenze dei clienti.

La sicurezza nel cloud computing è fondamentale quando si sviluppano servizi. L'aggiornamento dei sistemi operativi delle macchine virtuali, la garanzia della disponibilità, l'isolamento dei dati individuali degli utenti, l'implementazione di meccanismi di autenticazione, la crittografia o la configurazione di VPN e VLAN sono solo alcuni esempi di ciò che deve essere considerato. Di seguito, i principali aspetti di sicurezza che mettono alla prova il cloud computing:

• *Identità, Autenticazione, Autorizzazione*

L'*identità* consente di caratterizzare un utente attraverso l'utilizzo di un login. L'*autenticazione* viene invece utilizzata per verificare le credenziali dell'utente. Questo avviene in modo sicuro, affidabile e gestibile [3]. Al termine dell'autenticazione, l'*autorizzazione* cloud verifica i diritti dell'utente. La guida include una directory centralizzata, la gestione delle identità, la gestione degli accessi e degli utenti con privilegi, il controllo degli accessi basato sui ruoli e la separazione dei compiti tra le funzioni principali. Inoltre, il fornitore di servizi può spesso offrire un periodo di prova gratuito.

Ad esempio, nell'estate del 2012, gli aggressori (utenti per un periodo gratuito) hanno avuto accesso ai dati di Mat Hona (scrittore per Wired Magazine) cancellando tutti i dati personali dai suoi account Apple, Gmail e Twitter [3].

• *Riservatezza*

Un utente malintenzionato in una macchina virtuale può ascoltare un'altra macchina virtuale [4] identificando facilmente il suo data center e ottenendo informazioni sul suo indirizzo IP e sul suo nome di dominio. Inoltre, una macchina virtuale può estrarre chiavi crittografiche private utilizzate in altre macchine virtuali sullo stesso server fisico, il che implica il rischio di perdita

di dati [3]. Risulta quindi importante proteggere la riservatezza dei dati della VM.

Esemplificando, la piattaforma Amazon EC2 (Seattle, Washington, WA, USA) era vulnerabile a problemi di riservatezza [4]. Tuttavia ora, con Amazon Web Service (AWS), il cliente ha la possibilità di gestire le proprie chiavi di crittografia.

• *Integrità*

Metodi come il phishing, lo sfruttamento delle vulnerabilità del software ed il dirottamento del traffico di rete possono intercettare attività e transazioni, manipolare dati, restituire informazioni falsificate e reindirizzare i clienti a siti illegittimi.

• *Isolamento*

Il cloud computing deve avere un livello di isolamento tra tutti i dati della VM e l'hypervisor [5]. In Infrastructure as a Service (IaaS), significa isolare l'archiviazione delle VM, la memoria di elaborazione e le reti di percorso di accesso. In Platform as a Service (PaaS): i servizi in esecuzione e le chiamate API devono essere isolati. Inoltre, nel Software as a Service (SaaS): deve essere raggiunto l'isolamento tra le transazioni.

• *Disponibilità*

Gli utenti illegittimi consumano gran parte della potenza di elaborazione, della memoria, dello spazio su disco o della larghezza di banda della rete della vittima. Inoltre provocano rallentamenti del sistema, impedendo agli utenti legittimi di utilizzare il servizio in questione. Di conseguenza, la VM diventa non disponibile, causando un Denial of Service (DoS) o Distributed Denial of Service (DDoS).

Per esempio, un attacco DDoS con dispositivi Internet of Things compromessi si è verificato su Dyn (infrastruttura DNS) e ha paralizzato alcuni siti basati su cloud computing come GitHub e Airbnb [6].

Con questa introduzione si intende solo presentare le caratteristiche fondamentali del cloud computing inteso come sistema informatico distribuito e alcuni aspetti di sicurezza.

Successivamente, il documento è stato redatto in modo tale da fornire una tassonomia ben articolata degli attacchi Denial of Service, trattati a partire dal capitolo 2 - catalogandone tipologie e scopi, con l'obiettivo ben preciso di fornire una panoramica quanto più ampia possibile delle vulnerabilità e delle metodologie offensive più o meno note e documentate.

Il capitolo 3 altresì esplora e puntualizza i bersagli di questi attacchi, approfondendo la descrizione dei componenti che fanno parte di un cloud e delle tecniche offensive utilizzate per comprometterne le funzionalità.

Il quarto ed ultimo capitolo analizza gli attacchi DoS condotti ai danni dell'infrastruttura di rete cloud, classificandoli in base al livello di rete nel quale operano.

Capitolo 2

Attacchi Denial of Service

Collocandosi in un contesto generico di sistemi distribuiti, con particolare riferimento agli ambienti cloud, un attacco DoS può essere descritto come un attacco progettato per impedire ad alcuni servizi o risorse di fornire le proprie legittime prestazioni per un certo periodo di tempo. Gli attacchi DoS compromettono la disponibilità delle risorse e dei servizi e spesso prendono di mira la larghezza di banda o la connettività delle reti di computer. In genere, gli attacchi DoS rientrano nelle seguenti categorie:

- Attacchi di larghezza di banda;
- Attacchi di connettività;
- Esaurimento delle risorse;
- Sfruttamento delle limitazioni;
- Interruzione dei processi;
- Corruzione dei dati;
- Disordine fisico.

Si puntualizza la differenza tra le prime due - apparentemente molto simili - poiché gli attacchi alla larghezza di banda mirano a inoltrare traffico di grandi dimensioni per consumare tutte le risorse di rete disponibili. Diversamente, gli attacchi alla connettività inondano la vittima inviando un volume elevato di richieste di connessione che causano il consumo di tutte le risorse del sistema operativo disponibili nella vittima e, di conseguenza, le richieste degli utenti legittime non riescono ad essere gestite [7].

2.1 Denial of Service Distribuito

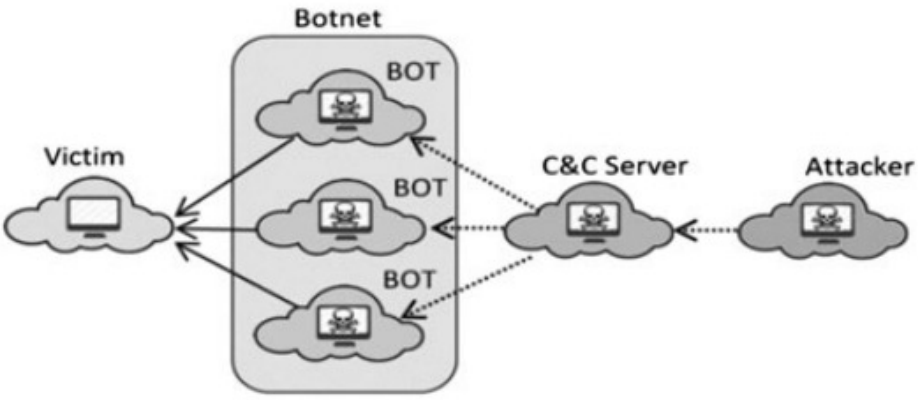
Negli attacchi DoS remoti, è molto importante per l'attaccante non essere rilevato, altrimenti potrebbe essere bloccato da firewall o sistemi di rilevamento delle intrusioni situati presso il sito della vittima. Per raggiungere questo scopo, l'attaccante può servirsi di molteplici sistemi intermedi e dispositivi di supporto per eseguire gli attacchi DoS e, in questo caso, si parla di attacco DoS distribuito (DDoS).

Abbreviation	Description
VM	Virtual machine
VMM	Virtual machine monitor
DoS	Denial of service
DDoS	Distributed denial of service
EDoS	Economic denial of service
CIDoS	Cloud-internal denial of service
XDoS	XML denial of service
HDoS	HTTP denial of service
LDoS	Low-rate denial of service
ADoS	Application denial of service

Figura 2.1: Acronimi ed abbreviazioni.

Negli attacchi DDoS, l'attaccante invia i suoi ordini a un sistema chiamato server di comando e controllo (server C&C) che coordina e attiva una botnet. In genere una botnet è un insieme di host compromessi che oscurano l'attaccante fornendo un livello di "indirezione". Il server C&C ordina alla botnet di lanciare un attacco DDoS contro la vittima e, successivamente, i bot inviano pacchetti di attacco al bersaglio, il cui contenuto dipende dal tipo di attacco [8]. Pertanto, l'host dell'attaccante è separato dalla sua vittima da uno o più strati intermedi di host "zombie".

Figura 2.2: Architettura dell'attacco DDoS in ambiente cloud.

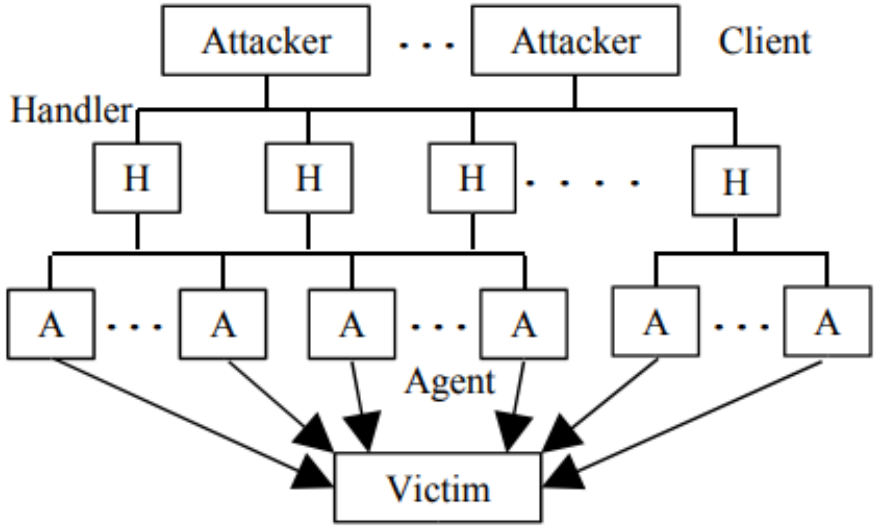


In genere, le reti di attacco DDoS basate su botnet rientrano nelle tre categorie seguenti [9]:

• *Modello agente-gestore*: comprende client, software gestori e agenti. Attraverso il client, l'attaccante comunica con il resto del sistema di attacco DDoS. I gestori sono pacchetti software dislocati su Internet che il client dell'attaccante utilizza per comunicare con gli agenti. Il software agente è collocato nei sistemi compromessi nei quali sarà eventualmente eseguito l'attacco. L'attaccante comunica con un numero qualsiasi di gestori per identificare quali agenti sono attivi e in esecuzione, per pianificare attacchi o per aggiornare gli agenti. Di solito, gli aggressori cercano di posizionare il software gestore su un router o un server di rete compromesso che gestisce grandi volumi di traffico. Ciò rende più difficile identificare i messaggi tra il client e il gestore e tra il gestore e gli agenti.

Nelle descrizioni degli strumenti DDoS, i termini "gestore" e "agenti" sono talvolta sostituiti rispettivamente con "master" e "daemons".

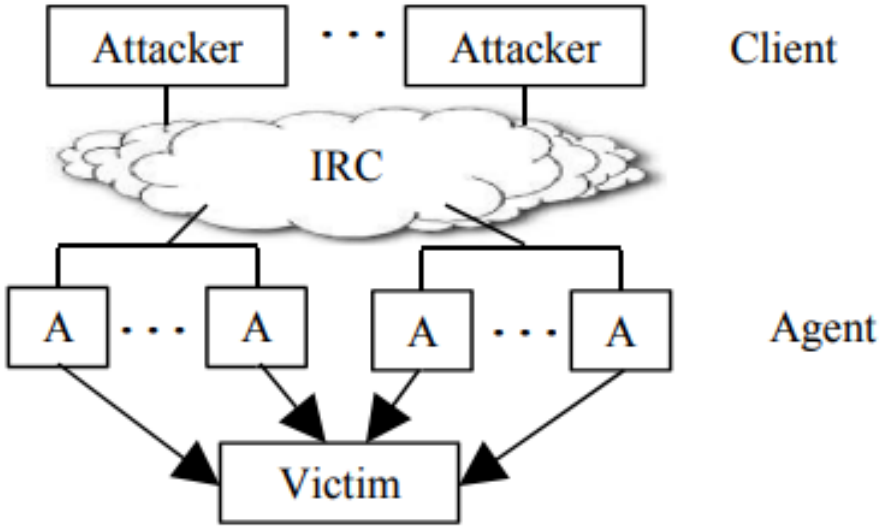
Figura 2.3: Architettura del modello agente-gestore.



• *Modello Internet Relay Chat* (IRC): a differenza del modello precedente il client è connesso agli agenti tramite un canale di comunicazione IRC per ostacolare il rilevamento dei pacchetti di comandi DDoS. Un canale IRC fornisce all'attaccante vantaggi aggiuntivi come l'uso di porte IRC "legittime" per inviare comandi agli agenti. Ciò rende più difficile il monitoraggio dei pacchet-

ti di comandi DDoS. Inoltre, i server IRC tendono a gestire grandi volumi di traffico, rendendo più facile per l'attaccante nascondere la propria presenza. Un altro vantaggio è che l'attaccante non ha bisogno di mantenere un elenco degli agenti, poiché può accedere al server IRC e visualizzare un elenco di tutti gli agenti disponibili. Il software dell'agente installato nella rete IRC di solito comunica con il canale IRC e notifica all'attaccante quando l'agente è attivo e in esecuzione.

Figura 2.4: Architettura del modello Internet Relay Chat.



• *Modello basato sul Web*: riporta semplicemente le statistiche a un sito Web e presenta alcuni vantaggi rispetto a IRC come la facilità di configurazione, una minore richiesta di larghezza di banda, accettazione di grandi botnet per il carico distribuito, occultamento del traffico e ostacolo al filtraggio e alla resistenza al dirottamento di botnet.

Gli attuali bot di attacco DDoS popolari sono i seguenti [10]:

• *AgoBot*: è uno dei bot più popolari, con il fornitore di antivirus "Sophos" che elenca oltre 600 versioni diverse. Le sue varianti sono Gaobot, Nortonbot, Phatbot e Polybot;

• *SDBot*: ha oltre 1800 varianti e viene fornito con strumenti di ping e di inondazione UDP, mentre la "SYN Flood Edition" include attacchi alluvione SYN del protocollo TCP (Transmission Control Protocol). SDBot è scritto in C++ per i sistemi Windows di destinazione;

• *RBot*: ha oltre 1600 varianti ed è scritto in C++ anch'esso per i sistemi Windows di destinazione.

• *SpyBot*: è scritto nel linguaggio di programmazione C e interessa ancora i sistemi Windows.

Queste botnet hanno da poche centinaia a migliaia di varianti a causa di molteplici persone che lavorano per migliorarne le funzionalità. Come indicato in precedenza, uno dei fattori importanti nella conduzione degli attacchi DoS è che l'attaccante e i vari componenti dell'attacco, come il server C&C e le botnet, non vengano rilevati. Attualmente vengono utilizzati i seguenti metodi per mantenere nascosti gli aggressori:

• "Spoofing" ("falsificazione") dell'indirizzo IP sorgente dei pacchetti attaccanti;

• "IP fluxing" e "domain fluxing";

• Utilizzo di botnet;

• Varietà di indirizzi IP nella botnet;

• Utilizzo di proxy specifici a seconda dei protocolli;

• Utilizzo di altri sistemi non sospettabili in quanto non compromessi, negli attacchi di riflessione e di amplificazione;

• Utilizzo su più livelli di sistemi compromessi e componenti di attacchi DoS per attaccare la vittima;

• Impedire il rilevamento dei componenti d'attacco (per esempio la botnet).

La gravità degli attacchi DoS dipende dai seguenti fattori:

• Tipo di attacco;

• Tipo di protocollo o evento utilizzato in modo improprio nell'attacco;

• Numero di host attaccanti compromessi;

• Numero di host non compromessi applicati nell'attacco;

• La quantità di risorse esaurite presso il sito della vittima;

• Topologia e meccanismo di difesa nel sito della vittima;

• La quantità di risorse di cui dispongono i componenti dell'attaccante;

• La quantità di risorse di cui dispone la vittima;

• Il tipo di cloud, dato che spesso i cloud accessibili al pubblico hanno più superficie di attacco rispetto ai cloud privati.

Inoltre, per lanciare con successo attacchi DoS, gli aggressori cercano di dichiararsi "in regola" nei confronti dei componenti di sicurezza applicando i seguenti metodi:

• Imitazione del traffico di rete legittimo;

• Eseguendo l'attacco "Flash Crowds" (attacco DDoS che inonda il bersaglio con numerose richieste di servizio dissimulandole come un picco di richieste regolari);

• Imitando determinati eventi legittimi nel cloud computing;

• Offuscamento, ad esempio crittografando il contenuto dei messaggi di attacco.

Tuttavia, gli attacchi DDoS possono essere più devastanti nell'ambiente cloud poiché esso è costituito da concetti, componenti e protocolli tendenzialmente recenti che presentano nuove vulnerabilità, le quali possono essere utilizzate in modo improprio per condurre nuove tipologie di attacchi DoS. Inoltre, nella figura 2.2 è indicata una delle principali differenze degli attacchi DDoS nelle reti convenzionali e nell'ambiente cloud, in cui i partecipanti stessi all'attacco potrebbero essere ambienti cloud. Ad esempio, l'attaccante stesso può essere un cloud, il server C&C, la botnet e la vittima possono essere essi stessi un cloud. Ciò rende più complicato sia il rilevamento che la prevenzione e la gestione degli attacchi DDoS perché, utilizzando queste tecniche, gli aggressori hanno più risorse disponibili per lanciare i propri attacchi. In genere, quando un cloud è vittima di un attacco DDoS, il primo obiettivo dell'attaccante è saturare il gateway Internet dell'infrastruttura. Tuttavia, se non può essere saturato, gli aggressori proveranno a saturare i server.

2.2 Classificazione degli attacchi Denial-of-Service distribuiti

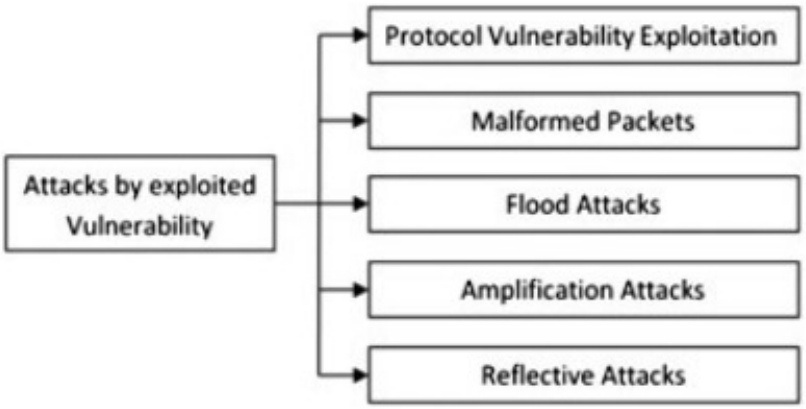
Gli attacchi denial-of-service distribuiti possono essere classificati in base alle loro varie caratteristiche. Ad esempio, in base all'origine dell'attacco, gli attacchi DDoS possono essere classificati come attacchi DDoS interni e attacchi DDoS esterni.

• *Attacchi DDoS esterni*: l'autore dell'attacco dovrebbe essere in grado di caricare un cavallo di Troia nelle macchine virtuali dei client in esecuzione nel cloud. Se il cavallo di Troia è in grado di diffondersi su centinaia o migliaia di VM, verrà creata una botnet per l'attaccante che potrà essere utilizzata come origine degli attacchi DDoS alle vittime esterne;

• *Attacchi DDoS interni*: la botnet interna attacca una vittima interna. Questi attacchi sono più gravi degli attacchi esterni e possono causare la "rottura" completa di tutte le infrastrutture cloud [11].

Pertanto, quando la sicurezza del cloud viene trascurata, esso stesso può diventare l'origine di molti attacchi DDoS interni ed esterni. La figura 2.5 indica una classificazione basata sugli exploit degli attacchi DDoS. Il resto di questa sezione descrive in dettaglio questi tipi di attacchi.

Figura 2.5: Classificazione degli attacchi Denial of Service.



2.2.1 Sfruttamento delle vulnerabilità di protocollo

Questi attacchi sfruttano le vulnerabilità note dei protocolli come difetti di progettazione o implementazione per causare comportamenti inappropriati e modificare le informazioni che vanno verso o provengono da un obiettivo specifico. A seconda della loro progettazione, alcuni passaggi dei protocolli possono creare la breccia per attacchi DoS. Inoltre, sebbene determinati protocolli possano essere ben progettati e sicuri, l'applicazione con altri protocolli può far scaturire una situazione compromettente [12].

Ad esempio, in un attacco DDoS TCP SYN, l'attaccante ordina agli zombie di inviare false richieste TCP SYN a un server vittima per vincolare le risorse del processore del server e quindi impedire al server di rispondere a richieste legittime. L'attacco TCP SYN sfrutta l'handshake a tre vie tra il sistema di invio e il sistema di ricezione inviando grandi volumi di pacchetti TCP SYN al sistema vittima con indirizzi IP di origine falsi, in modo che il sistema vittima risponda a un sistema non richiedente con ACK+SYN. Quando un grande volume di richieste SYN viene elaborato da un server e nessuna delle risposte

ACK+SYN viene restituita, il server alla fine esaurisce le risorse del processore e della memoria e non è in grado di rispondere agli utenti legittimi.

Altresì, in un attacco PUSH + ACK, gli agenti attaccanti inviano pacchetti TCP con i bit PUSH e ACK impostati su uno. Questi trigger nell'intestazione del pacchetto TCP istruiscono il sistema vittima a scaricare tutti i dati nel buffer TCP (indipendentemente dal fatto che il buffer sia pieno o meno) e a inviare un riconoscimento una volta completato. Se questo processo viene ripetuto con più agenti, il sistema ricevente non sarà in grado di elaborare il grande volume di pacchetti in entrata e il sistema vittima andrà in "crash".

2.2.2 Pacchetto malformato

Tendenzialmente, questi attacchi si basano sull'invio di pacchetti formati in modo volutamente errato dagli aggressori alla vittima per mandare in crash il sistema di riferimento. È possibile lanciare questo tipo di attacco contro molti protocolli. Ad esempio, durante un attacco di pacchetto malformato basato su IP, i pacchetti di attacco contengono gli stessi indirizzi IP di origine e di destinazione, che confondono il sistema operativo della vittima potendolo bloccare. Diversamente, in altri attacchi con opzioni di pacchetto IP, i pacchetti malformati possono randomizzare i campi opzionali all'interno di un pacchetto IP e impostare tutti i bit di qualità del servizio su uno, il che potrebbe causare più elaborazione nella vittima per la gestione dei pacchetti [13].

2.2.3 Attacchi alluvione

In un attacco alluvione (flood), chiamato anche BW-DDoS (BandWidthDistributed DoS), l'attaccante inonda la vittima con traffico indesiderato per impedire che il traffico legittimo raggiunga il sistema della vittima. Gli attacchi alluvione differiscono per il tipo di protocollo utilizzato per inondare la vittima.

In un attacco UDP Flood, ad esempio, un gran numero di pacchetti UDP viene inviato a porte specifiche o casuali sul sistema vittima. Il sistema vittima tenta di elaborare i dati in entrata per determinare quali applicazioni hanno richiesto i dati. Se il sistema vittima non esegue alcuna applicazione sulla porta di destinazione, invierà un pacchetto ICMP al sistema di invio indicando un messaggio "porta di destinazione irraggiungibile". Spesso, lo strumento DDoS offensivo falsifica anche l'indirizzo IP di origine dei pacchetti attaccanti.

Questo aiuta a nascondere l'identità delle vittime secondarie poiché i pacchetti di ritorno dal sistema delle vittime non vengono rispediti agli zombie, ma agli indirizzi falsificati. Gli attacchi flood UDP possono anche riempire la larghezza di banda delle connessioni che si trovano attorno al sistema vittima. Ciò, quindi, ha spesso un impatto anche sui sistemi situati vicino alla vittima [14].

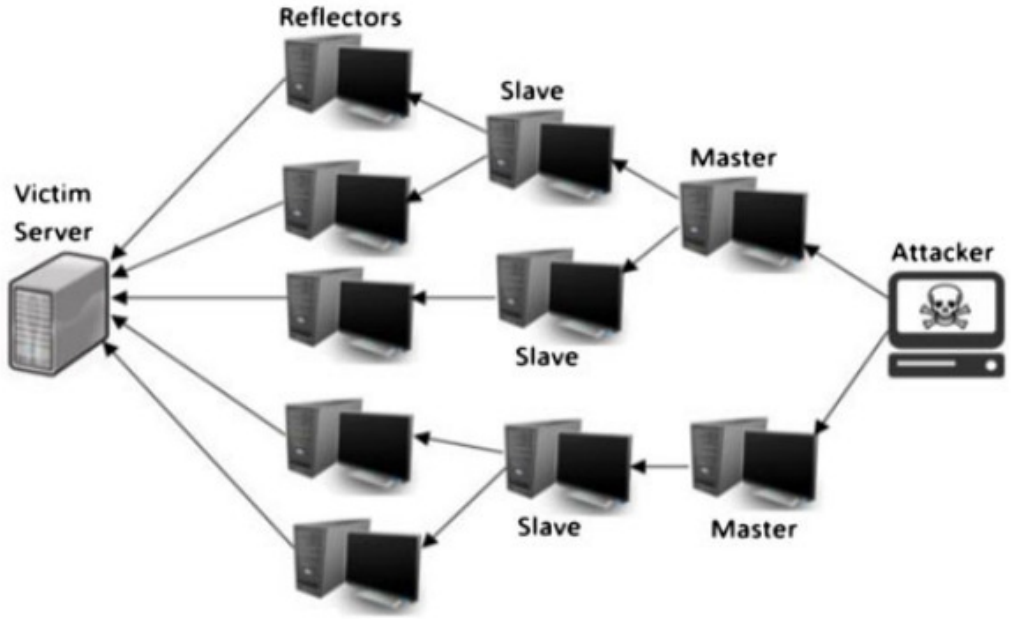
Un attacco ICMP flood invece, si verifica quando gli zombie inviano grandi volumi di pacchetti ICMP_ECHO_REPLY ("ping") al sistema vittima. Questi pacchetti segnalano al sistema vittima di rispondere saturando, attraverso la combinazione di traffico, la larghezza di banda della connessione di rete della vittima. Durante questo attacco, anche l'indirizzo IP di origine del pacchetto ICMP potrebbe essere oggetto di spoofing. Inoltre, alcuni attacchi BW-DDoS creano attacchi più complicati utilizzando tecniche di riflessione e amplificazione con effetti più devastanti oltre che più difficili da affrontare [14].

2.2.4 Denial of Service basato sulla Riflessione

Un altro metodo applicato dagli aggressori DDoS è il metodo di riflessione, utilizzando server non sospettabili (per esempio DNS e/o NTP) poiché non compromessi per inoltrare il traffico alla vittima e aiutare a consumare la larghezza di banda di cui quest'ultima dispone. Questo metodo aiuta l'attaccante a non essere rilevato inviando traffico alla vittima indirettamente. In questo modo, tutti i pacchetti di attacco inviati dall'attaccante contengono l'indirizzo IP della vittima nel campo dell'indirizzo IP sorgente, così, nel momento in cui il server riceve queste richieste di servizio, invia la sua risposta al nodo vittima e non al nodo di origine effettivo del pacchetto.

L'attacco Distributed Reflective DoS (DRDoS) è un tipo sofisticato di attacco DoS in cui, come indicato nella figura 2.6, l'attaccante controlla gli zombie master e slave e impartisce loro istruzioni per inondare di pacchetti di richiesta il nodo riflettore per abbattere il bersaglio. Nell'ottica di prevenire il rilevamento, gli aggressori possono utilizzare le botnet per condurre attacchi riflessivi più imponenti [15]. Gli attacchi DRDoS vengono utilizzati per sfruttare i protocolli come TCP, UDP, Domain Name System (DNS) e ICMP.

Figura 2.6: Architettura dell'attacco Distributed Reflective Denial-of-Service.



2.2.5 Amplificazione degli attacchi denial-of-service distribuiti

Gli attacchi di amplificazione sono una versione più devastante degli attacchi DoS riflessivi - i quali utilizzano la natura intrinseca di alcuni protocolli di rete per aumentare la quantità di traffico che si riflette sulla vittima. In questo caso, il volume del traffico di risposta generato dai server riflettori coinvolti è maggiore del traffico dei messaggi di richiesta emesso dall'attaccante. Di conseguenza, il traffico che raggiunge la vittima viene amplificato dal server riflettore e questo sovraccarica le risorse e la larghezza di banda della vittima [16]. Ciò consente all'attaccante di lanciare l'attacco DoS anche con botnet più ridotte.

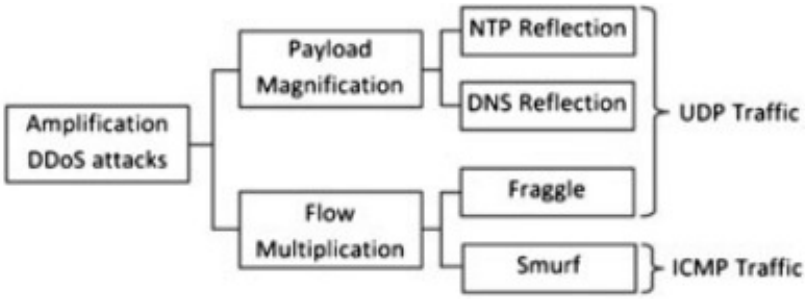
Un attacco DDoS "Smurf" è un esempio di attacco di amplificazione in cui l'attaccante invia pacchetti a un amplificatore di rete (un sistema che supporta l'indirizzamento broadcast) con l'indirizzo di ritorno falsificato con l'indirizzo IP della vittima. I pacchetti che attaccano sono tipicamente ICMP ECHO REQUEST, pacchetti (simili a un "ping") che richiedono al ricevitore di generare un ICMP ECHO REPLY [17]. L'amplificatore invia i pacchetti ICMP ECHO

REQUEST a tutti i sistemi all'interno dell'intervallo di indirizzi di trasmissione e ciascuno di questi sistemi restituirà un ICMP ECHO REPLY all'indirizzo IP della vittima bersaglio. Questo tipo di attacco amplifica il pacchetto originale decine o centinaia di volte.

Un altro esempio è l'attacco DDoS "Fraggle", in cui l'attaccante invia pacchetti a un amplificatore di rete utilizzando pacchetti UDP ECHO. Esiste una variante dell'attacco Fraggle in cui i pacchetti UDP ECHO vengono inviati alla porta che supporta la generazione di caratteri ("chargen", porta 19 nei sistemi Unix), con l'indirizzo di ritorno falsificato al servizio eco della vittima ("echo", porta 7 nei sistemi Unix) creando un ciclo infinito [18]. Il pacchetto UDP Fraggle punterà al generatore di caratteri nei sistemi raggiunti dall'indirizzo di trasmissione. Ciascuno di questi sistemi genera un carattere da inviare al servizio di eco nel sistema vittima, che invierà un pacchetto di eco al generatore di caratteri ripetendone il processo. Questo attacco può generare più traffico nocivo e causare più danni di un attacco Smurf.

Pertanto, gli attacchi di amplificazione possono inoltrare più traffico verso la vittima con un numero inferiore di zombie intermedi e risultano quindi più gravi sia degli attacchi riflessivi che degli attacchi DDoS.

Figura 2.7: Classificazione degli attacchi Denial of Service Distribuiti Amplificati.

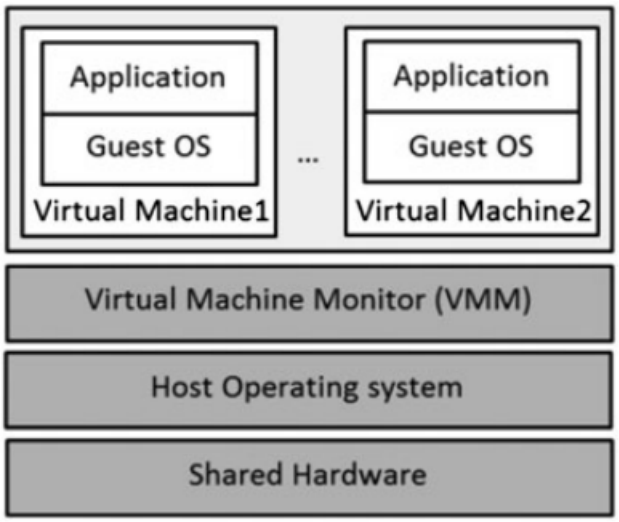


Capitolo 3

Attacchi ai componenti cloud

Il cloud computing è costituito in gran parte da tecnologie come SOA (Architettura Orientata ai Servizi, metodo di sviluppo che utilizza componenti software chiamati servizi per creare applicazioni aziendali) e virtualizzazione, vulnerabili a vari problemi di sicurezza interni ed esterni. Questi problemi sono significativi soprattutto nei cloud pubblici. La figura 3.5 inserita a fine capitolo mostra la classificazione degli attacchi DoS comuni all'ambiente di cloud computing.

Figura 3.1: Organizzazione della virtualizzazione.



3.1 Attacchi contro macchine virtuali

La virtualizzazione è diventata una tecnologia indispensabile per l'infrastruttura cloud odierna e offre numerosi vantaggi nella condivisione, gestione e isolamento delle risorse. Essa consente a più VM di risiedere su una singola macchina fisica e le VM possono essere create, espanse, ridotte o spostate dinamicamente al variare della domanda.

La figura 3.1 indica l'organizzazione della virtualizzazione. Un livello software è denominato VM monitor (VMM) (hypervisor), che crea, gestisce e mantiene l'isolamento tra le VM. L'hypervisor dovrebbe anche monitorare i sistemi operativi guest e le relative applicazioni per rilevare eventuali comportamenti dannosi.

Le minacce alla sicurezza in un ambiente virtualizzato sono le stesse che si basano sui difetti di sicurezza nei sistemi fisici. In genere, in un ambiente virtuale, gli attacchi alla sicurezza possono essere condotti tra i seguenti elementi:

- Tra le VM;
- Tra le VM e il loro host;
- Monitor della VM dall'host;
- Monitor della VM da un'altra VM;
- Attacco da ospite a ospite;
- Modifica esterna di una macchina virtuale;
- Modifica esterna di un hypervisor.

Poiché il sistema operativo guest (OS) può accedere alla rete, sono necessari metodi di sicurezza in ogni macchina virtuale. Alcuni attacchi DoS nei cloud vengono condotti abusando della funzionalità di migrazione delle macchine virtuali e riducendo la capacità del provider di servizi di soddisfare i requisiti del contratto di servizio (SLA). La migrazione delle macchine virtuali fornisce un utilizzo efficiente delle risorse e migliora il risparmio energetico nei data center cloud. Normalmente, quando un server è in sovraccarico, le sue VM possono essere migrate su server il cui carico di lavoro risulta più leggero. Inoltre, quando alcuni server sono sottoutilizzati, le loro macchine virtuali possono essere consolidate in un numero inferiore di server per risparmiare energia. Ma la migrazione di VM è un'operazione dispendiosa attraverso la quale lo stato di una VM viene trasferito da un host all'altro [19].

3.1.1 Attacchi di migrazione delle VM

Quando un server fisico è sovraccaricato da attacchi DDoS, la migrazione della VM non solo non allevia il problema, ma può anche deteriorare la situazione generale del sistema. L'attacco di migrazione delle macchine virtuali è condotto dall'aumento dannoso del consumo di risorse delle macchine virtuali che, provocando molte dispendiose migrazioni di VM, degrada sensibilmente le prestazioni del cloud.

3.1.2 Attacchi DoS interni al cloud

L'attacco DoS interno al cloud è un attacco in cui un numero di VM dannose nello stesso host fisico tenta di attaccare il proprio host. Queste macchine virtuali applicano canali nascosti ed un protocollo per il coordinamento. Per lanciare questo attacco, ogni macchina virtuale aumenta l'utilizzo delle risorse per interrompere la capacità dell'host di far fronte al carico. L'attacco CIDoS è difficile da rilevare poiché i comportamenti degli aggressori risultano simili al normale carico di lavoro di un host impegnato a gestire molte richieste.

Ad esempio, gli aggressori possono sfruttare i periodi di prova dei servizi cloud di alcuni fornitori per sovraccaricarne le risorse. Di conseguenza, attraverso un utente autorizzato all'interno dell'ambiente cloud risulterebbe possibile lanciare un attacco DoS sulla macchina della vittima. Infatti, la diffusione di immagini di macchine virtuali infette potrebbe consentire a un utente malintenzionato di controllare e utilizzare queste VM con lo stesso principio con cui vengono impiegate le botnet, per eseguire internamente un attacco DDoS sulla macchina presa di mira all'interno dello stesso sistema di cloud [20].

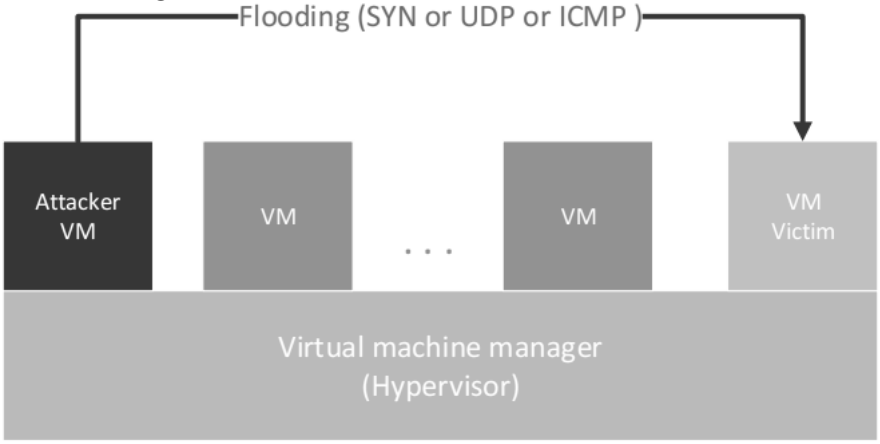
3.1.3 Attacchi a distesa

In un sistema virtuale, una politica di gestione inappropriata delle VM può portare ad un attacco in cui il numero di VM aumenta di continuo e a dismisura, mentre esse risultano inattive o non tornano dal loro stato di "riposo". Questo attacco spreca a tutti gli effetti le risorse cloud, creando più punti d'accesso per gli aggressori.

3.1.4 Attacchi al vicino

Uno dei potenziali attacchi DoS al sistema di virtualizzazione cloud è l'attacco al vicino, indicato nella figura 3.2. Qualsiasi macchina virtuale può attaccare le sue macchine virtuali vicine nella stessa macchina fisica causando il massimo carico di lavoro su di essa. Questo attacco DoS può ridurre le prestazioni del cloud e causare effetti dannosi sugli altri server. Questi attacchi sono causati da configurazioni errate e vulnerabilità nell'hypervisor.

Figura 3.2: Architettura dell'attacco al vicino.



3.1.5 Attacchi di fuga

In un attacco di fuga, l'applicazione dannosa eseguita in una VM sarà in grado di bypassare completamente l'hypervisor e ottenere l'accesso alla macchina host. Quando ottiene l'accesso al sistema host, ottiene anche i privilegi di root e fuoriesce dai privilegi della VM. Ciò si traduce in una rottura completa del quadro di sicurezza del sistema host. Tuttavia, questo problema può essere risolto configurando correttamente le interazioni host/guest.

3.2 Attacchi contro gli hypervisor

Un cliente di un cloud potrebbe affittare una VM ospite per installare un sistema operativo dannoso e attaccare l'hypervisor modificandone il codice sorgente, ottenendo l'accesso ai contenuti di memoria delle VM vicine [21].

3.2.1 Attacchi mimetici

Per prevenire il rilevamento, l'attaccante DDoS può nascondere i suoi attacchi imitando il carico di richieste legittime. Gli aggressori imitano il susseguirsi di queste richieste per ingannare i metodi di rilevamento degli attacchi DoS basati sul monitoraggio del traffico di rete. Ad ogni modo, discriminare gli attacchi DDoS mimetici dal traffico elevato degli utenti legittimi è un problema tutt'ora da risolvere.

3.3 Attacchi contro i clienti cloud

Nell'attacco EDoS (Economic Denial of Sustainability), l'attaccante invia molte richieste false ai servizi cloud e ne aumenta il carico per incrementare il conto dell'utente. L'attacco EDoS dipende dalla configurazione del server, dalle risorse disponibili per gli utenti cloud e dall'accessibilità delle risorse. I servizi cloud tendenzialmente sono forniti sotto forma di SLA (Service Level Agreement, strumenti contrattuali attraverso i quali si definiscono le metriche di servizio che devono essere rispettate da un fornitore di servizi nei confronti dei propri clienti/utenti). Gli attacchi EDoS sono molto dannosi per lo SLA che, per essere soddisfatto, comporta l'attivazione di più risorse al fine di fornire la disponibilità del servizio all'utente sotto attacco. Questo provoca ovviamente costi aggiuntivi sia per il cliente che per il gestore del cloud [22]. La figura 3.3 indica i diversi attacchi ai componenti cloud.

Figura 3.3: Attacchi contro i componenti cloud.

Attack	Protocol vulnerability exploitation	Spoofing	Using VM migration	Incurring high load	Flooding	Gain access to hypervisor
VM migration	–	–	✓	✓	–	–
CIDoS	✓	–	–	✓	–	–
VM sprawling	–	–	–	✓	–	–
Neighbor attacks	–	–	–	✓	–	–
VM escape	–	–	–	–	–	✓
Mimicking DoS	–	–	–	–	–	✓
EDoS	–	✓	–	✓	✓	✓
ADoS	✓	–	–	–	–	–
Energy-oriented DoS	–	–	–	✓	–	–

3.4 Attacchi contro lo scheduler

Il monitor o l'hypervisor della macchina virtuale può gestire diverse VM, ma il suo scheduler potrebbe essere vulnerabile ai comportamenti dannosi di queste VM e ciò potrebbe comportare una pianificazione non corretta o imprecisa.

Ad esempio, Xen è un VMM open source per la piattaforma ×86/×64, che utilizza un meccanismo di pianificazione che potrebbe non tenere conto dell'utilizzo della CPU da parte di VM mal funzionanti. Un caso concreto può essere la vulnerabilità in Elastic Compute Cloud (EC2) di Amazon, che consente ai clienti malintenzionati di ottenere un servizio avanzato a spese di altri. È stato scoperto che le applicazioni, sfruttando questo problema, sono in grado di utilizzare fino al 98% di un core della CPU, indipendentemente dalla concorrenza di altre VM. Per risolvere questo problema, Amazon Elastic Compute Cloud ha dovuto utilizzare una versione patchata di Xen [23].

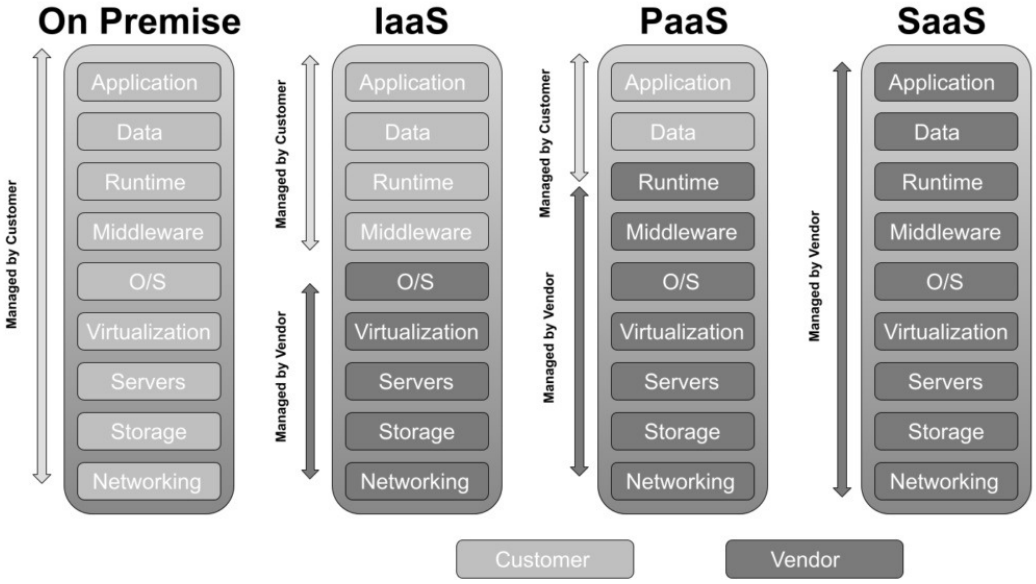
3.5 Attacchi contro i SaaS

Gli attacchi applicazione DoS si concentrano sul cloud inteso come Software as a Service, sfruttando i difetti delle applicazioni per impedire l'accesso legittimo ai diversi servizi della vittima. È più difficile risalire a questi attacchi e le soluzioni di monitoraggio della sicurezza esistenti potrebbero non rilevarli. Spesso questi attacchi utilizzano protocolli HTTP o HTTPS e applicano server proxy per offuscare l'origine dell'attaccante.

3.6 Attacchi contro le IaaS

L'attacco DoS orientato all'energia è un nuovo tipo di attacco che si concentra sul cloud inteso come Infrastructure as a Service con l'obiettivo di compromettere le infrastrutture e i data center per portarli a consumare quanta più energia possibile. Le attività dannose di questo attacco causano un carico di lavoro elevato sul bersaglio e lo tengono completamente occupato. I risultati di questo attacco sono l'aumento dei costi del consumo energetico e la penalizzazione a causa delle emissioni di gas serra per i fornitori di servizi cloud.

Figura 3.4: Confronto tra le vari soluzioni contrattuali.



3.7 Attacchi contro i servizi web

I servizi web sono componenti software che utilizzano vari protocolli e standard basati su XML come SOAP (Simple Object Access Protocol) per lo scambio di dati.

Gli attacchi DoS comuni condotti contro i servizi web sono i seguenti:

• *Attacco di analisi coercitiva*: in questo attacco vengono inviati al server documenti XML altamente nidificati che possono causare errori di memoria o persino un utilizzo elevato della CPU quando un parser basato su Document Object Model li elabora;

• *Attacco all'array SOAP*: forza il servizio web a inviare messaggi SOAP molto grandi;

• *Attacco al conteggio degli attributi XML*: vengono inviati al bersaglio messaggi SOAP con un numero elevato di attributi;

• *Attacco al conteggio degli elementi XML*: vengono inviati al server messaggi SOAP con molti elementi non nidificati;

• *Attacco di collisione hash* (Hash DoS): viene inviato un POST di grandi dimensioni riempito con molte variabili di modulo, che richiedono un'elaborazione relativa all'hash;

• *Entità esterna XML DoS*: il server viene forzato a risolvere una grande entità informtiva esterna definita nella definizione del tipo di documento indicato;

• *Espansione di entità XML*: nota come "XML bombing", provoca un uso improprio della capacità di annidamento di XML;

• *Crittografia sovradimensionata*: l'attaccante allega una grande quantità di frammenti crittografati o firmati digitalmente nei messaggi;

• *Scansione WSDL* (Web Services Description Language): viene utilizzata per descrivere ed esporre le interfacce di un sistema. Consente agli utenti di creare un software che funzioni con servizi offerti da altri fornitori. Quando gli amministratori/sviluppatori codificano gli URL e gli ID utente nel software, perdono involontariamente informazioni sui loro sistemi. Queste informazioni possono essere utilizzate dagli hacker illegalmente per accedere ai loro sistemi utilizzando una serie di vulnerabilità come il cross-site scripting o gli attacchi SQL injection;

• *Spoofing dei metadati*: questo attacco ha lo scopo di riprogettare e manomettere le descrizioni dei metadati del servizio web;

• *Offuscamento degli attacchi*: utilizza la crittografia XML per nascondere il contenuto del messaggio dall'ispezione da parte del firewall o dell'IDS (Intrusion Detection System, dispositivo software o hardware - o a volte la combinazione di entrambi, sotto forma di sistemi stand-alone pre-installati e pre-configurati - utilizzato per identificare accessi non autorizzati ai computer o alle reti locali). Questi contenuti crittografati possono essere utilizzati per lanciare altri attacchi come payload oversize, analisi coercitiva o iniezione di XML e crittografia;

• *Attacco di deviazione dello stato BPEL* (Business Process Execution Language): il motore BPEL può fornire gli endpoint per il servizio web in questione, che accettano le eventuali richieste di servizio. A causa del fatto che un processo BPEL può avere molte istanze in esecuzione contemporaneamente, questi endpoint di comunicazione sono aperti per le connessioni in entrata in qualsiasi momento. Pertanto, un client di servizi web dannoso potrebbe attaccare questi endpoint aperti utilizzando messaggi corretti per quanto riguarda la loro struttura, senza che questi siano correlati a nessuna istanza di processo esistente. Questi messaggi di correlazione non valida verranno eliminati all'interno del motore BPEL, causando una smisurata quantità di lavoro ridondante. Ogni messaggio deve essere letto ed elaborato completamente, cercando una corrispondenza in tutte le istanze di processo esistenti, prima

che il messaggio possa essere eliminato in modo sicuro. Pertanto, le risorse di calcolo del motore BPEL vengono esaurite dall'elaborazione di tali messaggi non validi;

• *Instanziation flooding attack*: quando arriva un nuovo messaggio di richiesta, viene creata una nuova istanza del processo BPEL ed esegue le istruzioni fornite nella descrizione del processo. Un utente malintenzionato può attaccare il motore BPEL inviando una marea di richieste a un singolo processo BPEL;

• *Flooding indiretto*: questo attacco è possibile a causa della caratteristica di composizionalità del servizio web. Se la composizione di un servizio web viene presa di mira con un attacco alluvione di richieste valide, creerà contesti di flusso di lavoro per ogni messaggio in arrivo. Inizierà quindi a eseguire un'enorme quantità di flussi di lavoro, contemporaneamente, provocando la chiamata ad altri servizi web inondati dalle stesse richieste del motore BPEL;

• *Spoofing degli indirizzi dei servizi web* (WS): le richieste SOAP inviate al server contengono un'intestazione di indirizzi WS, che fa sì che il server emetta la risposta SOAP per un endpoint diverso utilizzato per inondare un altro servizio web;

• *Dirottamento del middleware*: questo attacco applica lo spoofing degli indirizzi WS, ma punta l'URL dell'endpoint dell'attaccante a un sistema di destinazione esistente che esegue un servizio reale all'URL specificato. Di conseguenza, il server del servizio web tenterà ripetutamente di rispondere alle richieste dell'attaccante.

3.8 Attacchi basati su XML

Gli attacchi DoS (X-DoS) basati su XML inviano messaggi alluvione XML a un servizio web per utilizzare tutte le risorse lato server. Gli attacchi DX-DoS sono la versione distribuita degli attacchi X-DoS, che utilizzano più host per lanciare l'attacco. In questo attacco, spesso il contenuto del messaggio viene manipolato per causare un arresto anomalo del server web. A causa della complessità dei documenti XML e della loro analisi, anche un piccolo messaggio XML manomesso o comunque non corretto può consumare un gran numero di risorse del server [24].

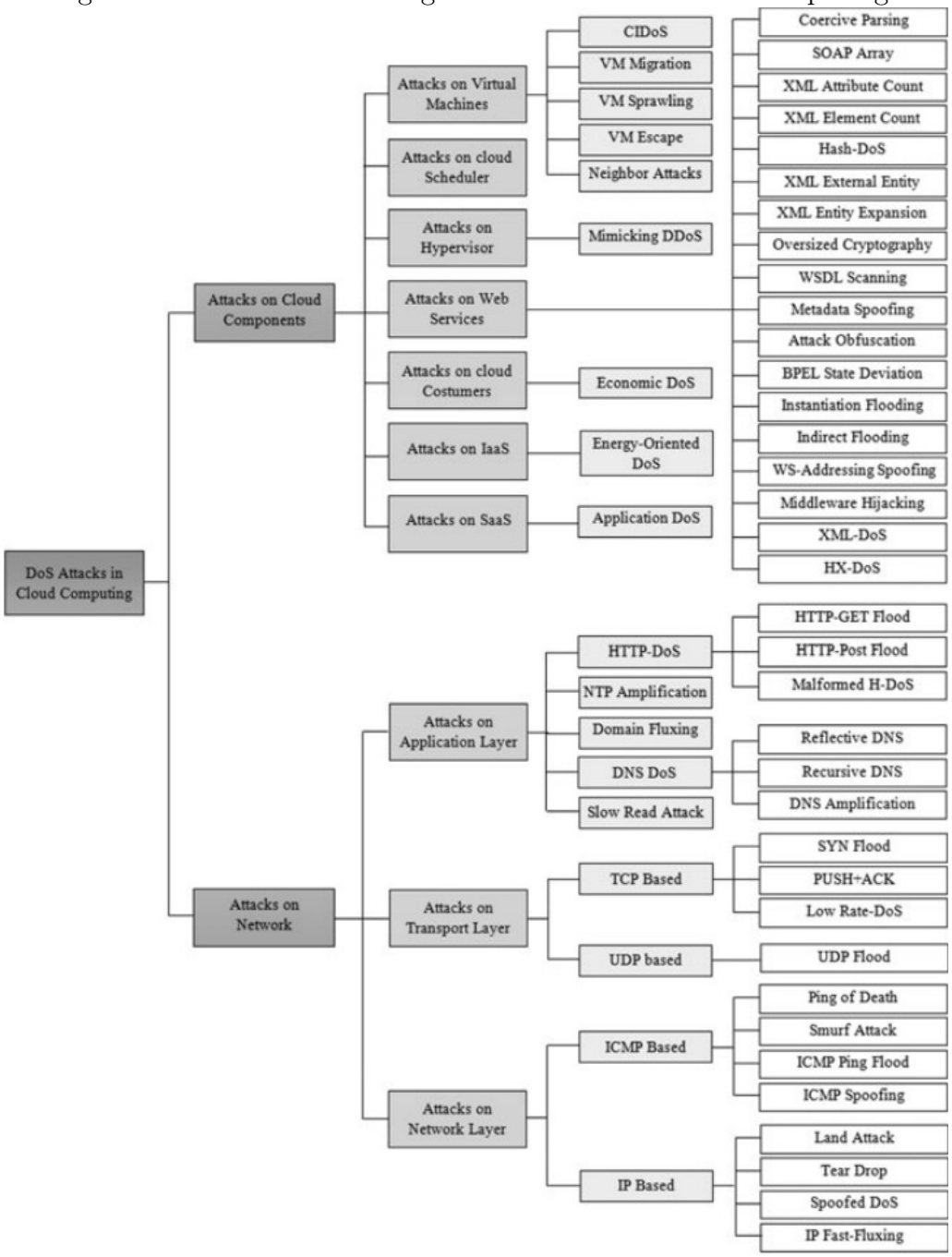
3.9 Attacchi HX-DoS

I servizi web cloud funzionano in base ai protocolli HTTP e XML, come SOAP. Una delle minacce con cui il provider di servizi cloud deve lottare è l'attacco HX-DoS o HX-DDoS, che opera sulla base dei protocolli HTTP e XML. L'attacco HX-DoS è una combinazione di messaggi HTTP e XML utilizzati per inondare il canale di comunicazione del provider cloud. Per affrontare il problema degli attacchi HX-DoS contro i servizi web cloud risulta necessario distinguere i messaggi illegittimi da quelli regolari [25]. Il confronto degli attacchi contro i servizi web è riportato nella figura 3.4.

Figura 3.5: Confronto degli attacchi contro i servizi web.

Attack	Protocol vulnerability exploitation	Malformed packet	Spoofing	Flooding
X-DoS	✓	✓	✓	✓
Coercive parsing attack	–	–	–	✓
SOAP array attack	–	–	–	✓
XML attribute count attack	–	–	–	✓
XML element count attack	–	–	–	✓
Hash collision attack (Hash-DoS)	–	–	–	✓
XML external entity DoS	–	–	–	✓
XML entity expansion	–	–	–	✓
Oversized cryptography	–	–	–	✓
WSDL scanning	–	–	✓	–
Metadata spoofing	–	–	✓	–
Attack obfuscation	–	–	–	–
BPEL state deviation attack	–	–	✓	✓
Instantiation flooding attack	–	–	–	✓
Indirect flooding	–	–	–	✓
WS-addressing spoofing	–	–	✓	–
Middleware hijacking	–	–	✓	✓

Figura 3.6: Classificazione degli attacchi DoS nel cloud computing.



Capitolo 4

Attacchi alle infrastrutture di rete cloud

Questa sezione analizza gli attacchi DoS condotti contro l'infrastruttura di rete dei cloud e li classifica in base al livello di rete nel quale operano.

4.1 Attacchi a livello d'applicazione

Poiché i servizi forniti dal cloud sono supportati principalmente dall'utilizzo del livello di applicazione, i protocolli di questo livello sono stati presi di mira da numerosi attacchi DDoS. Questi attacchi basati sul livello di applicazione rappresentano le principali minacce alla sicurezza del cloud computing e sono più difficili da rilevare poiché le tecniche di monitoraggio dovrebbero eseguire un'ispezione particolarmente approfondita di ogni pacchetto ricevuto.

Inoltre, talvolta questi attacchi utilizzano tecniche come proxy specifici di protocollo e crittografia del contenuto per rendere più difficoltose le operazioni di rintracciamento dell'attaccante.

4.1.1 Attacchi basati su HTTP

Una delle minacce critiche per le applicazioni basate sul web è l'attacco DoS basato su HTTP (H-DoS) attraverso il quale gli aggressori violano le restrizioni del proxy web utilizzando il programma browser di riferimento per l'attacco che viene lanciato sul server Web. Il server Web non è in grado di rilevare la

penetrazione di client dannosi attraverso i proxy web a causa delle informazioni nascoste dell'identità dell'attaccante [26].

Attacchi basati su HTTP malformato

In questi attacchi DoS, l'attaccante inonda la vittima inviando messaggi HTTP che contengono elementi non validi con campi non corretti. Questo attacco può causare determinate vulnerabilità come l'overflow del buffer o altri problemi di sicurezza.

Inoltre, è richiesto un traffico inferiore rispetto a H-DoS e può addirittura essere considerato come un flusso regolare di pacchetti. Il rilevamento di H-DoS malformati è più costoso rispetto al rilevamento di H-DoS regolari, poiché l'IDS deve applicare la Deep Packet Inspection (DPI) che consuma molte risorse di elaborazione. Infine, l'esecuzione dell'ispezione approfondita dei pacchetti prolunga il ritardo nella gestione delle richieste HTTP, riducendo la qualità del servizio (QoS) dei servizi HTTP in questione.

Attacchi alluvione HTTP-GET

In questo attacco l'attaccante utilizza la richiesta HTTP-GET del protocollo HTTP per inviare un gran numero di richieste dannose a un server di destinazione. Poiché questi pacchetti di richiesta GET hanno payload HTTP, firewall e IDS legittimi situati presso la vittima non riescono a distinguerli ed elaborarli tutti, esaurendo tutte le risorse del bersaglio. Gli attacchi a livello di applicazione sono confrontati nella figura 4.1.

Attacchi alluvione HTTP-POST

In questo attacco, alla vittima viene inviato un flusso di messaggi HTTP-POST. In genere, una richiesta POST contiene un corpo del messaggio, che può utilizzare qualsiasi codifica. L'autore dell'attacco invia prima la parte dell'intestazione HTTP per intero al server web, dopo di che invia il corpo del messaggio HTTP in più tranches, ad esempio un byte ogni 110 s. Il server web "obbedisce", rispettando le informazioni ottenute leggendo il campo della lunghezza del contenuto che risiede nell'intestazione HTTP e attende che il resto del corpo del messaggio venga inviato. Instaurare questo tipo di connessioni può portare ad attacchi DDoS.

Figura 4.1: Confronto degli attacchi a livello di applicazione.

Attack	Protocol vulnerability exploitation	Malformed packet	Spoofing	Reflection	Amplification	Flooding
H-DoS	✓	–	–	–	–	✓
HTTP-GET flood attack	–	–	–	–	–	✓
HTTP-POST flood attack	–	–	–	–	–	✓
HX-DoS	✓	–	–	–	–	✓
Malformed H-DoS	–	✓	–	–	–	✓
DNS server DoS	–	–	✓	✓	✓	–
NTP amplification	–	–	–	✓	✓	–
Domain fluxing	–	–	–	–	–	✓
Slow read attack	–	–	–	–	–	✓

4.1.2 Attacchi basati su DNS

Il Domain Name System è vulnerabile agli attacchi DDoS basati sullo spoofing. In questo caso, un server non può garantire che un pacchetto di richiesta provenga effettivamente dall'indirizzo IP indicato nella richiesta o meno. I pacchetti attaccanti falsificati provocano attacchi DoS, che possono sovraccaricare gli stessi server DNS o saturare la larghezza di banda della vittima tramite le risposte DNS amplificate [27].

Attacchi DNS riflessivi

Figura 4.2: Attacco DNS riflessivo.

Gli attacchi DNS riflessivi non prendono di mira i server DNS stessi, ma li utilizzano per condurre un attacco contro un altro sistema il cui indirizzo IP è contraffatto nelle query DNS. Come mostrato nella figura 4.2, nell'attacco DNS riflessivo, le richieste DNS vengono inviate ai server DNS che inoltrano la loro risposta alla vittima. Tuttavia, questa risposta è amplificata e la sua dimensione è maggiore delle richieste DNS che danno vita all'attacco.

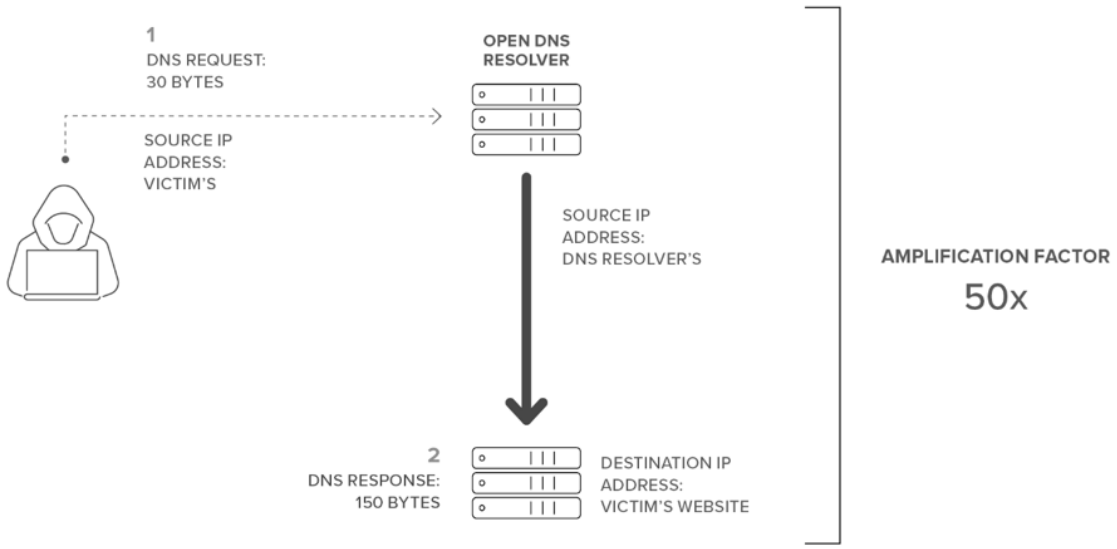
Attacchi DNS ricorsivi

Gli attacchi DNS ricorsivi prendono di mira i server DNS stessi e ne riducono la disponibilità per gli utenti della rete. Questi attacchi sfruttano le query DNS ricorsive ed emettono numerose richieste DNS per nomi di dominio inesistenti al server DNS della vittima. Non essendo trovati, verrà richiestà una ulteriore elaborazione e comunicazione, causando un maggiore esaurimento delle risorse.

Attacchi DNS amplificati

L'obiettivo di questo attacco non sono i server DNS ma un altro sistema vittima, che è specificato nell'indirizzo IP di origine dei pacchetti di attacco. Nell'attacco DNS amplificato, l'attaccante può indirizzare un grande volume di traffico di rete alla vittima inviando query DNS. Nello specifico, l'attaccante falsifica l'indirizzo IP della vittima per indirizzare ad essa il messaggio di risposta del server DNS. A tale scopo, un flusso di query DNS di tipo "ANY" viene inviato a un server DNS autorevole o non autorevole. Ciò restituisce tutte le informazioni su una zona DNS. Per aumentare il traffico, gli aggressori possono utilizzare le botnet per creare un gran numero di query DNS contraffatte. Nella figura 4.2 si esemplifica quanto esposto.

Figura 4.3: Attacco DNS amplificato.



4.1.3 Attacchi NTP amplificati

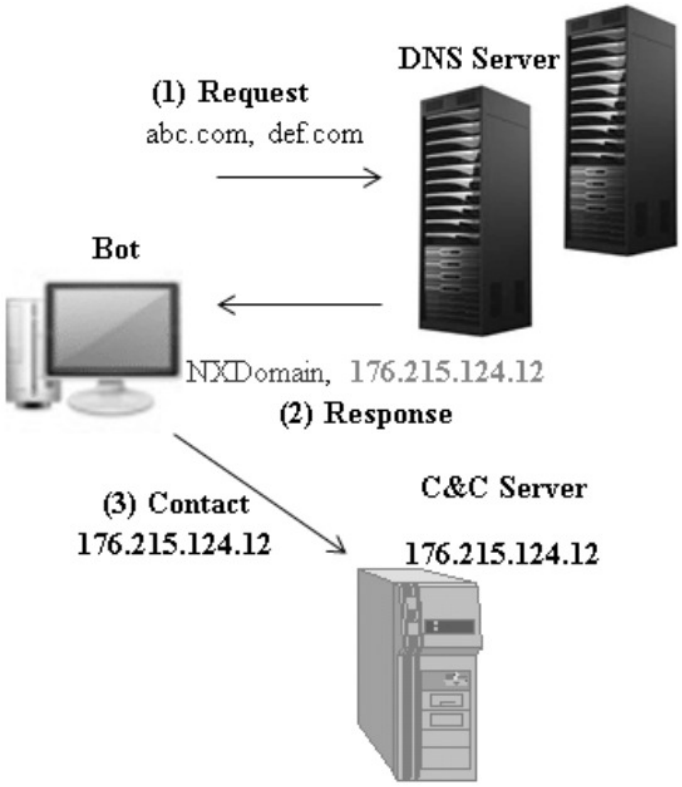
Il Network Time Protocol è soggetto agli attacchi di amplificazione perché uno dei suoi comandi invia una risposta relativamente lunga ad una richiesta relativamente breve. NTP contiene un comando chiamato monlist (MON_GETLIST), che può essere inviato a un server NTP per scopi di monitoraggio. Questo restituisce gli indirizzi delle ultime 600 macchine comunicate dal server NTP. Questa risposta è intuibilmente molto più grande della richiesta, il che la rende ideale per gli attacchi di amplificazione [28].

4.1.4 "Domain fluxing"

Il Domain fluxing è una tecnica in cui i nomi di dominio completamente qualificati collegati all'indirizzo IP dei server C&C vengono frequentemente modificati per mantenere le botnet in funzione. Per eseguire questa operazione, il bot master utilizza un DGA (Domain Generation Algorithm, algoritmo di generazione di domini) per generare nomi di dominio su larga scala, in grado di aggirare i metodi di blacklisting ed euristica per il rilevamento dei nomi di dominio DGA. La figura 4.4 mostra il diagramma di flusso di questo genere di attacchi. Il bot utilizza due domini: abc.com e def.com. Il dominio abc.com non è registrato e riceve una risposta NXDomain dal server DNS; def.com è invece registrato e quindi è in grado di contattare il server C&C. Quindi le botnet contattano il loro botmaster con nomi di dominio generati casualmente utilizzando un metodo "hit and trial". Nella maggior parte dei casi ciò genererebbe diverse query di risposta non esistenti (NX) per i domini che non hanno indirizzi IP (NXDomains). L'analisi delle query DNS aiuta a rilevare i domini generati da DGA e aiuta a rintracciare le botnet, per poi bloccare il punto di comunicazione tra il botmaster e il server C&C in un modo tempestivo. Inoltre, l'analisi delle query DNS aiuta a identificare gli attacchi nelle fasi iniziali o anche prima che si verifichino. Un DGA genera un gran numero di nomi di dominio utilizzando un seme casuale, che può essere una data, un numero o qualsiasi carattere casuale. Per costruire nomi di dominio, il generatore DGA utilizza una combinazione di operazioni bitshift, xor, divisioni, moltiplicazioni e modulo per generare una sequenza di caratteri che seguono una certa distribuzione, come un modello di distribuzione normale o uniforme. I generatori DGA normalmente utilizzano semi diversi e si aggiornano frequentemente. Per esempio, i semi possono cambiare nell'arco di una singola giornata. Ciò rende

le strategie di blacklisting inefficaci poiché i DGA procedono a creare nomi di dominio diversi continuamente [29].

Figura 4.4: Domain fluxing.



4.1.5 Attacchi a lettura lenta

In questo attacco, l'attaccante invia richieste a livello di applicazione legittime ma legge le risposte molto lentamente definendo una piccola dimensione della finestra di ricezione TCP per condurre una comunicazione particolarmente lenta con la destinazione. Se l'attaccante riesce ad inviare numerose richieste per un server web, quest'ultimo raggiungerà la sua capacità massima e potrebbe non essere disponibile per nuove richieste.

4.2 Attacchi a livello di trasporto

Gli attacchi Denial of Service a questo livello possono essere classificati come attacchi basati su TCP e attacchi basati su UDP.

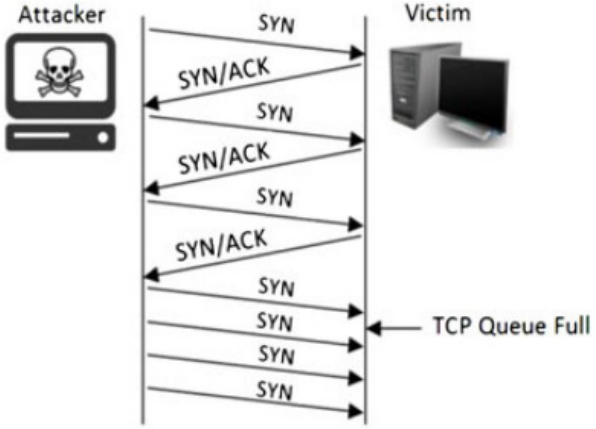
4.2.1 Attacchi basati su TCP

Varie funzionalità del protocollo TCP vengono utilizzate per lanciare attacchi DoS. Gli attacchi DoS basati su TCP più comuni sono i seguenti:

- Attacchi alluvione SYN;
- Attacchi PUSH + riconoscimento (ACK);
- Attacchi DoS (LDoS) a bassa frequenza.

Come anticipato nel secondo capitolo e mostrato nella figura 4.5, l'*attacco alluvione SYN* mira a saturare la disponibilità dei server web servendosi di uno o più host da cui poter inviare flussi di pacchetti TCP/SYN con l'indirizzo del mittente falsificato. Ciascuno di questi pacchetti viene gestito lato server come una richiesta regolare, che fa sì che venga creata una connessione semi-aperta. Il server quindi trasmette a sua volta un pacchetto TCP/SYN-ACK aspettandosi un pacchetto in risposta dal falso mittente, che non arriverà ovviamente mai. Queste connessioni semi-aperte saturano il numero di connessioni disponibili che il server può effettuare e, in linea col protocollo, vengono mantenute di default per almeno 75s in coda. Ne consegue che le connessioni più recenti non possono essere accettate, almeno temporaneamente.

Figura 4.5: Attacco alluvione SYN.



In un *attacco PUSH + ACK*, come già anticipato, vengono inviati pacchetti TCP con i flag PUSH e ACK impostati su 1. Questi trigger nell'intestazione del pacchetto TCP istruiscono il bersaglio a scaricare tutti i dati nel buffer TCP (a prescindere da quanto il buffer sia pieno) e a inviare un pacchetto di risposta una volta completato. Se questo processo viene ripetuto con più agenti, il sistema vittima non sarà in grado di elaborare il grande volume di pacchetti in entrata e andrà in "crash".

Un attacco DDoS a bassa frequenza (LR-DDoS: Low Rate - DDoS) è un attacco intelligente che satura la vittima creando un numero relativamente basso di connessioni in un certo periodo di tempo - lasciando aperte quelle sessioni il più a lungo possibile - per evitare che i sistemi IDS basati su anomalie possano rilevarli. LDoS è anche noto come "attacco del toporagno" e viene solitamente condotto dall'attaccante seguendo un modello intermittente che prevede l'utilizzo più o meno periodico di altre tipologie di attacchi, in modo da ridurre ulteriormente la possibilità che i sistemi di difesa della vittima possano rilevarlo. L'attaccante invierà un gran numero di medesime richieste dalle stesse fonti per degradare le prestazioni. L'attacco LDoS può essere suddiviso in attacco al protocollo TCP e attacco al meccanismo di Active Queue Management dei router. Il meccanismo deterministico del timeout per la ritrasmissione previsto dal protocollo TCP risulta quindi vulnerabile al traffico periodico e a bassa velocità generato da questo attacco [30].

4.2.2 Attacchi basati su UDP

Negli attacchi alluvione basati su UDP, molti pacchetti UDP vengono inviati alle porte casuali o specificate dal bersaglio per saturarne il traffico di rete. Quando la vittima elabora questi dati in entrata, se non è presente alcuna applicazione sulla porta specificata, genera e invia un messaggio di "destinazione irraggiungibile". Tuttavia, vengono utilizzate dagli aggressori le tecniche descritte in precedenza per nascondere la loro identità, come lo spoofing dell'indirizzo IP di origine [31]. La figura 4.6 mostra un confronto tra gli attacchi a livello di trasporto.

4.3 Attacchi a livello di rete

Gli attacchi DoS a livello di rete utilizzano in modo improprio i protocolli IP e ICMP per attaccare la vittima. Gli attacchi a livello di rete e la loro tipologia

Figura 4.6: Confronto degli attacchi a livello di trasporto.

Attack	Malformed packet	Spoofing	Reflection	Amplification	Flooding
ACK attack	–	✓	–	–	–
SYN flood	–	✓	–	–	✓
PUSH + ACK	–	✓	–	–	✓
LDoS	–	–	–	–	✓
UDP flood	–	✓	–	–	✓

sono mostrati nella figura 4.7.

Figura 4.7: Confronto degli attacchi a livello di rete.

Attack	Protocol vulnerability exploitation	Malformed packet	Spoofing	Reflection	Amplification	Flooding
LAND attack	–	–	✓	–	–	✓
Teardrop	–	–	✓	–	–	✓
Spoofed DoS	–	–	✓	–	–	–
IP fast fluxing	–	–	–	–	–	–
Ping of death	✓	✓	–	–	–	–
Smurf attack	–	–	–	✓	✓	✓
ICMP ping flood	–	–	✓	–	–	✓
ICMP spoofing	–	–	✓	–	–	–

4.3.1 Attacchi basati su IP

Uno dei maggiori problemi affrontati dagli host Internet sono gli attacchi DoS causati dall'inondazione di pacchetti IP [32].

Alcuni attacchi DoS basati su IP sono i seguenti:

• *Attacco LAND*: simile a SYN flood, ma in questo attacco l'indirizzo di origine del pacchetto SYN e l'indirizzo di destinazione sono entrambi indirizzi IP del server di destinazione. Nel momento in cui la macchina di destinazione tenta di rispondere, entra in un ciclo inviando ripetutamente risposte a se stessa capaci di provocare autonomamente un arresto anomalo;

• *Teardrop*: si verifica con pacchetti IP frammentati inviati alla vittima. Uno dei campi in un'intestazione IP è il campo "offset del frammento", che indica la posizione iniziale, o offset, dei dati contenuti in un pacchetto frammentato rispetto ai dati nel pacchetto originale. Se la somma dell'offset e della dimensione di un pacchetto frammentato differisce da quella del pacchetto frammentato successivo, i pacchetti si sovrappongono. Quando ciò accade,

un server vulnerabile agli attacchi teardrop non è in grado di riassemblare i pacchetti, causando una condizione di denial-of-service.

Attacchi basati su spoofed-IP

Figura 4.8: Opzioni del tool "responder".

In questi attacchi, gli aggressori utilizzano lo spoofing per rappresentare in modo errato l'indirizzo IP di origine dei pacchetti DoS e quindi per oscurarne l'identità. In generale, quando gli aggressori e le vittime sono posizionati in diverse reti connesse ad internet, la vittima non riesce a distinguere i pacchetti contraffatti da quelli legittimi, quindi vengono trattati allo stesso modo. Questi pacchetti di risposta, prodotti per i pacchetti IP contraffatti, sono spesso noti come "backscatter".

Ad oggi esistono varie distribuzioni di Linux con tool anche pre-installati in grado di eseguire agevolmente azioni di questo genere [33]. Ne è un esempio "responder", strumento di sniffing e spoofing che risponde alle richieste del server in questione, con una serie di opzioni disponibili piuttosto eloquenti, riportate nella figura 4.8.

IP fast fluxing

L'IP fast flux (traducibile come "flusso rapido") è un metodo per modificare frequentemente l'indirizzo IP che appartiene a un nome di dominio. Questo

metodo impedisce il rilevamento delle botnet e del server C&C. Le reti che utilizzano le tecniche di flusso rapido sono appunto chiamate reti di flusso rapido.

Il flusso rapido può essere classificato nelle seguenti categorie [34]:

• *Flusso singolo*: la tipologia più semplice, caratterizzata da molti nodi che all'interno della rete registrano e de-registrano il proprio indirizzo come parte della lista degli indirizzi DNS di tipo A per un singolo dominio. Questo sistema unisce il "round robin DNS" con valori molto bassi di TTL (Time To Live) per creare una lista di indirizzi per un certo dominio, in continuo cambiamento. Questa lista può arrivare a comprendere centinaia di migliaia di indirizzi;

• *Doppio flusso*: un modo più sofisticato di controrilevamento che prevede la modifica ripetuta sia degli agenti di flusso che della registrazione nei server DNS.

4.3.2 Attacchi basati su ICMP

L'Internet Control Message Protocol è uno dei protocolli popolari, utilizzato in vari attacchi DoS [35].

Alcuni degli attacchi flooding basati su ICMP sono i seguenti:

• Attacco ping flood ICMP;
• Attacco ping of death;
• Attacco Smurf;
• Attacco spoofing ICMP.

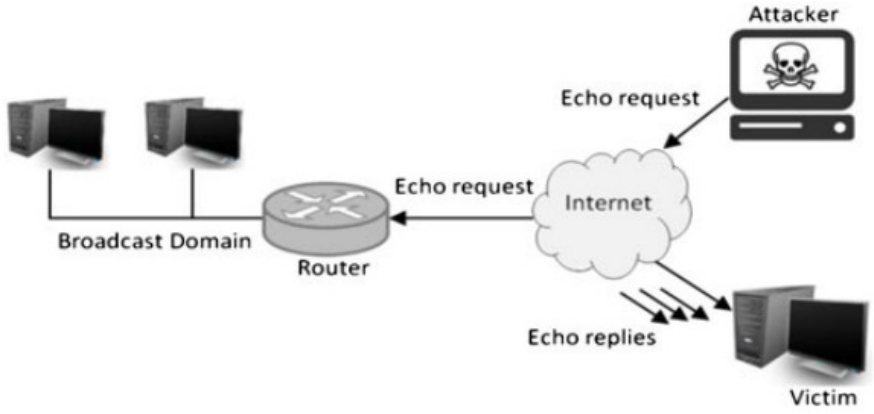
Nell'*attacco ping flood ICMP* - già affrontato - l'attaccante falsifica l'indirizzo IP di origine e invia alla vittima un numero enorme di pacchetti ping, di solito utilizzando letteralmente il comando ping. Un semplice attacco DDoS basato su ping può abbattere la vittima rendendola impegnata pressoché esclusivamente con le richieste di ping.

Il *Ping of death* è un altro attacco DoS basato su ping che comporta l'invio di un ping malformato o comunque dannoso a un bersaglio. Alcuni sistemi si sono rivelati non in grado di gestire e riassemblare correttamente un pacchetto ping più grande della dimensione massima del pacchetto IPv4 (65535 byte) [36]. Il pacchetto malintenzionato viene costruito generando proprio un frammento IP con valore di offset massimo ma con una quantità di dati associata pari o superiore al limite di otto byte. Questo, in fase di ricostruzione del pacchetto IP, porta ad ottenere una trama di dimensione superiore a quella consentita dal livello di rete, ossia superiore a 65535 byte. Ciò potrebbe

causare il sovraccarico del buffer utilizzato dal nodo ricevente per contenere il pacchetto (buffer overflow), causando il blocco del servizio. La vulnerabilità è legata quindi al meccanismo di riassemblaggio dei frammenti IP maliziosi, che potrebbero in teoria contenere qualunque tipo di protocollo (TCP, UDP, IGMP, ecc) e non solo messaggi di ping.

In questa categoria rientra anche l'*attacco Smurf* già trattato, un attacco di amplificazione basato su ICMP in cui l'attaccante utilizza reti intermedie non protette per amplificare il traffico di attacco. Come mostrato nella figura 4.9, prima l'attaccante invia un pacchetto di richiesta eco ICMP all'indirizzo di trasmissione di rete che viene inoltrato a tutti gli host all'interno della rete intermedia e in seguito invia le risposte eco ICMP alla vittima.

Figura 4.9: Architettura dell'attacco Smurf.



Capitolo 5

Conclusioni

Lo scopo degli attacchi DoS è quello di rendere un sistema o un servizio in rete non disponibile per gli utenti legittimi. Questi attacchi, certamente fastidiosi, possono risultare seriamente dannosi se la vittima principale è un sistema cruciale. La perdita di risorse di rete genera perdite economiche, ritardi nel lavoro e mancanza di comunicazione tra gli utenti della rete.

Devono essere introdotte soluzioni per prevenire questa tipologia di attacchi. In questo documento è stata avanzata una tassonomia di attacchi DoS e relativi strumenti per aiutare a definire il problema e agevolare lo sviluppo di contromisure che offrano il maggior numero di garanzie, poiché molti strumenti di attacco a disposizione degli aggressori, fino ai più semplici da implementare, possono avere effetti disastrosi.

Per quanto esistano metodi per impedire che questi attacchi abbiano successo, molti di questi sono ancora in fase di sviluppo e valutazione. È essenziale che, con l'espandersi di Internet e del suo utilizzo, vengano sviluppate, verificate e implementate soluzioni e contromisure più efficienti per le odierne e future tipologie di attacchi DoS.

Bibliografia

[1] `https://it.wikibooks.org/wiki/Sistemi_informativi/Architetture`, visitato il 15/12/2022.

[2] Zissis D., Lekkas D.; "Addressing cloud computing security issues", *Future Generation Computer Systems*, 2012

[3] Los R., Gray D., Shackleford D., Sullivan B.; "The Notorious Nine: Cloud Computing Top Threats in 2013", *CSA, Cloud Security Alliance*, 2013.

[4] Ristenpart T., Tromer E., Shacham H., Savage S.; "Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds", *ACM: New York, NY, USA*, 2009

[5] Hashizume K., Rosado D., Fernandez-Medina E., Fernandez E.; "An analysis of security issues for cloud computing", *Journal of Internet Services and Applications*, 2013

[6] `https://thehackernews.com/2016/10/dyn-dns-ddos.html`, visitato il 15/12/2022

[7] Jamil D., Zaki H.; "Security issues in cloud computing and countermeasures", *International Journal of Engineering Science and Technology (IJEST)*, 2011

[8] Yu S.; "Distributed Denial of Service Attack and Defense", 2014

[9] Alomari E., Manickam S., Gupta B.B., Karuppayah S., Alfaris R.; "Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art", 2012

[10] Thing V.L., Sloman M., Dulay N.; "A survey of bots used for distributed denial of service attacks." *New Approaches for Security, Privacy and Trust in Complex Environments*, 2007

[11] Latanicki J., Massonet P., Naqvi S., Rochwerger B., Villari M.; "Scalable cloud defenses for detection, analysis and mitigation of DDoS attacks", *Future Internet Assembly*, 2010

[12] Harrison K., White G.; "A taxonomy of cyber events affecting communities", *System Sciences (HICSS), 44th Hawaii International Conference on. IEEE*, 2011

[13] Douligeris C., Mitrokotsa A.; "DDoS attacks and defense mechanisms: classification and state-of-the-art", *Computer Networks*, 2004

[14] Paul J. Criscuolo; "Distributed Denial of Service", 2000

[15] Revathi P.; "Flow and rank correlation-based detection against Distributed Reflection Denial of Service attack", *Recent Trends in Information Technology (ICRTIT), International Conference on. IEEE*, 2014

[16] Colella A., Colombini C.M.; "Amplification DDoS Attacks: Emerging Threats and Defense Strategies, in Availability, Reliability, and Security in Information Systems", 2014

[17] `https://resources.sei.cmu.edu/asset_files/WhitePaper/1998_019_001_496180.pdf`, visitato il 10/11/2022

[18] `https://en.wikipedia.org/wiki/Smurf_attack#Fraggle_attack`, visitato l'11/11/2022

[19] Masdari M., Nabavi S.S., Ahmadi V.; "An overview of virtual machine placement schemes in cloud computing", *Journal of Network and Computer Applications*, 2016

[20] Darwish M., Ouda A., Capretz L.F.; "Cloud-based DDoS Attacks and Defenses", *Department of Electrical and Computer Engineering University of Western Ontario*, 2015

[21] Kazim M., Masood R., Shibli M.A., Abbasi A.G.; "Security aspects of virtualization in cloud computing", *IFIP International Conference on Computer Information Systems and Industrial Management*, 2013

[22] Masdari M., Salehi F., Jalali M., Bidaki M.; "A Survey of PSO-Based Scheduling Algorithms in Cloud Computing", *Journal of Network and Systems Management*, 2016

[23] `https://virtalica.com/2016/08/26/xen-vulnerability-allows-hackers-escape-os-vm-host-amazon-aws-rackspace-ibm-affected/`, visitato il 14/11/2022

[24] Falkenberg A., Mainka C., Somorovsky J., Schwenk J.; "A new approach towards DoS penetration testing on web services.", *Web Services (ICWS), IEEE 20th International Conference on. IEEE*, 2013

[25] Anitha E., Malliga S.; "A packet marking approach to protect cloud environment against DDoS attacks", *Information Communication and Embedded Systems (ICICES), International Conference on. IEEE*, 2013

[26] Jayan D., Babu P.; "Detection of malicious client-based HTTP/DoS attack on web server", *International Journal of Science and Research (IJSR)*, 2014

[27] Guo F., Chen J., Chiueh T.; "Spoof detection for preventing dos attacks against DNS servers", *Distributed Computing Systems, ICDCS*, 2006

[28] Graham-Cumming J.; "Understanding and mitigating NTP-based DDoS attacks", *CloudFlare*, 2014

[29] Vinayakumar R., Soman K., Prabaharan P., Mamoun A., Alireza J.; "Deep Learning Applications for Cyber Security", 2019

[30] Kurar B., Tahboub R.; "Internet scale DoS attacks. International Journal of Applied Mathematics, Electronics and Computers", 2015

[31] Hussain S.M., Beigh G.R.; "Impact of DDoS attack (UDP Flooding) on queuing models", *Computer and Communication Technology (ICCCT), 4th International Conference*, 2013

[32] Lakshminarayanan K.; "Taming IP packet flooding attacks", *ACM SIGCOMM Computer Communication Review*, 2004

[33] `https://linuxhint.com/top_sniffing_spoofing_tools_kali_linux/`, visitato il 17/11/2022

[34] https://it.wikipedia.org/wiki/Fast_Flux, visitato il 17/11/2022

[35] Prabadevi B., Jeyanthi N.; "Distributed denial-of-service attacks and its effects on cloud environment – a survey", *Networks, Computers and Communications, International Symposium*, 2014

[36] https://it.wikipedia.org/wiki/Ping_of_Death, visitato il 18/11/2022