Caratterizzazione e traccia delle inondazioni di pacchetti tramite router Cisco

Sommario

Introduzione

Gli attacchi DoS (Denial of Service) sono comuni su Internet. Il primo passo per rispondere a un attacco di questo tipo è scoprire esattamente che tipo di attacco è. Molti degli attacchi DoS comunemente utilizzati sono basati su pacchetti a larghezza di banda elevata o su altri flussi ripetitivi di pacchetti.

I pacchetti in molti flussi di attacco DoS possono essere isolati quando li si confronta con le voci dell'elenco degli accessi al software Cisco IOS®. Ciò è utile per filtrare gli attacchi. È utile anche quando si caratterizzano attacchi sconosciuti e quando si tracciano flussi di pacchetti "falsificati" verso le loro fonti reali.

Le funzionalità dei router Cisco, quali la registrazione del debug e l'accounting IP, possono a volte essere utilizzate per scopi simili, in particolare con attacchi nuovi o insoliti. Tuttavia, nelle versioni più recenti del software Cisco IOS, gli elenchi degli accessi e la registrazione degli elenchi degli accessi sono le funzionalità principali per la caratterizzazione e la traccia degli attacchi comuni.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Gli attacchi DoS più comuni

Èpossibile eseguire una vasta gamma di attacchi DoS. Anche se si ignorano gli attacchi che usano bug software per arrestare i sistemi con poco traffico, rimane il fatto che qualsiasi pacchetto IP che può essere inviato attraverso la rete può essere usato per eseguire un attacco DoS flooding. Quando sei sotto attacco, devi sempre considerare la possibilità che quello che vedi sia qualcosa che non rientra nelle solite categorie.

Fatta salva questa riserva, tuttavia, è bene ricordare che molti attacchi sono simili. Gli aggressori scelgono gli exploit comuni perché sono particolarmente efficaci, particolarmente difficili da tracciare, o perché sono disponibili strumenti. Molti attacchi DoS non hanno le abilità o la motivazione per creare i propri strumenti e utilizzare i programmi che si trovano su Internet. Questi strumenti tendono a cadere di moda.

Al momento della stesura di questo documento, nel luglio 1999, la maggior parte delle richieste di assistenza da parte dei clienti riguarda l'attacco "smurf". Questo attacco ha due vittime: un "obiettivo finale" e un "riflettore". L'aggressore invia un flusso stimolante di richieste echo ("ping") ICMP all'indirizzo di broadcast della subnet del riflettore. Gli indirizzi di origine di questi pacchetti sono stati falsificati in modo da essere l'indirizzo della destinazione finale. Per ogni pacchetto inviato dall'autore dell'attacco, molti host della subnet del reflector rispondono. Questo inonda il bersaglio finale e spreca larghezza di banda per entrambe le vittime.

Un attacco simile, chiamato "fraggle", usa le trasmissioni dirette nello stesso modo, ma usa le richieste echo UDP invece delle richieste echo ICMP (Internet Control Message Protocol). Fraggle di solito ottiene un fattore di amplificazione più piccolo rispetto a smurf, ed è molto meno popolare.

Gli attacchi Smurf vengono in genere notati perché un collegamento di rete diventa sovraccarico. Una descrizione completa di questi attacchi e delle misure di difesa è disponibile nella pagina delle informazioni sugli attacchi Denial of Service .

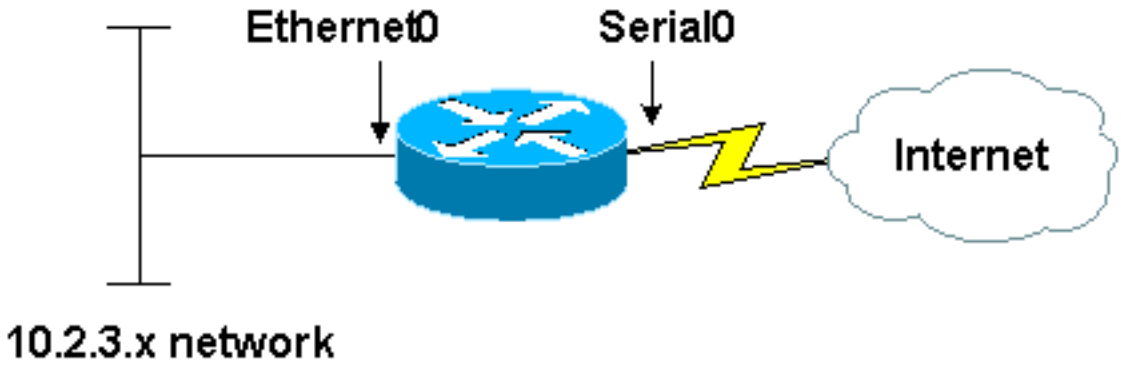
Un altro attacco comune è l'alluvione SYN, in cui un computer di destinazione è invaso da richieste di connessione TCP. Gli indirizzi di origine e le porte TCP di origine dei pacchetti di richiesta di connessione sono casuali. Lo scopo è forzare l'host di destinazione a mantenere le informazioni sullo stato per molte connessioni che non sono mai state completate.

Gli attacchi di tipo flood SYN vengono in genere notati perché l'host di destinazione (spesso un server HTTP o SMTP) diventa estremamente lento, si blocca o si blocca. Inoltre, il traffico che ritorna dall'host di destinazione può causare problemi ai router. Infatti, il traffico di ritorno va agli indirizzi di origine casuali dei pacchetti originali, non ha le proprietà di località del traffico IP "reale" e può sovraccaricare le cache dei percorsi. Sui router Cisco, questo problema spesso si manifesta con la memoria insufficiente del router.

Insieme, gli attacchi smurf e SYN flood rappresentano la stragrande maggioranza degli attacchi DoS allagati segnalati a Cisco, e riconoscerli rapidamente è molto importante. Entrambi gli attacchi (nonché alcuni attacchi di "secondo livello", ad esempio i ping flood) vengono facilmente riconosciuti quando si usano gli elenchi degli accessi Cisco.

Elenco accessi caratterizzazione DoS

Si immagini un router con due interfacce. Ethernet 0 è collegato a una LAN interna di un'azienda o a un ISP di piccole dimensioni. La porta seriale 0 fornisce una connessione Internet tramite un ISP upstream. La velocità dei pacchetti di input sul numero di serie 0 viene sottoposta a "pegging" sull'intera larghezza di banda del collegamento e gli host sulla LAN funzionano lentamente, si arrestano in modo anomalo, si bloccano o mostrano altri segni di un attacco DoS. Il piccolo sito a cui il router si connette non dispone di un analizzatore di rete e le persone che si trovano lì hanno poca o nessuna esperienza nella lettura delle tracce di analizzatore, anche se le tracce sono disponibili.



Si supponga ora di applicare un elenco degli accessi come illustrato nell'output seguente:

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

L'elenco non filtra affatto il traffico; tutte le iscrizioni sono permessi. Tuttavia, poiché i pacchetti vengono classificati in modo utile, l'elenco può essere utilizzato per diagnosticare provvisoriamente tutti e tre i tipi di attacchi: smurf, SYN flood e fraggle.

Smurf Ultimate Target

Se si usa il comando **show access-list**, l'output visualizzato è simile al seguente:

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

La maggior parte del traffico che arriva all'interfaccia seriale è costituita da pacchetti di risposta echo ICMP. Questa è probabilmente la firma di un attacco con il morso, e il nostro sito è il bersaglio finale, piuttosto che il riflettore. Quando si rivede l'elenco degli accessi, è possibile raccogliere ulteriori informazioni sull'attacco, come mostrato nell'output:

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

In questo caso, la parola chiave **log-input** viene aggiunta alla voce dell'elenco degli accessi che corrisponde al traffico sospetto. (Le versioni del software Cisco IOS precedenti alla 11.2 non contengono questa parola chiave. Utilizzare la parola chiave "**log**".) In questo modo, il router registra le informazioni sui pacchetti che corrispondono alla voce dell'elenco. Se si presume che la **registrazione** nel **buffer** sia configurata, è possibile visualizzare i messaggi risultanti con il comando **show log** (l'accumulo di messaggi potrebbe richiedere alcuni minuti a causa della limitazione della velocità). I messaggi sono simili a questo output:

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

Gli indirizzi di origine dei pacchetti di risposta echo sono raggruppati nei prefissi di indirizzo 192.168.212.0/24, 192.168.45.0/24 e 172.16.132.0/24. (Gli indirizzi privati nelle reti 192.168.x.x e 172.16.x.x non sarebbero in Internet; questa è un'illustrazione di laboratorio.) Questo è molto caratteristico di un attacco di smurf, e gli indirizzi di origine sono gli indirizzi dei riflettori di smurf. Se si cercano i proprietari di questi blocchi di indirizzi nei database Internet "whois" appropriati, è possibile trovare gli amministratori di queste reti e chiedere il loro aiuto per affrontare l'attacco.

Èimportante a questo punto, in un incidente mortale, ricordare che questi riflettori sono altre vittime, non attentatori. È estremamente raro che gli aggressori usino i propri indirizzi di origine su pacchetti IP in qualsiasi tipo di inondazione del DoS, e non è possibile che lo facciano in un attacco mirato funzionante. Qualsiasi indirizzo in un pacchetto di allagamento dovrebbe essere considerato o completamente falsificato, o l'indirizzo di una vittima di qualche tipo. L'approccio più produttivo per l'obiettivo finale di un attacco di tipo smurf è quello di contattare i riflettori, o per chiedere loro di riconfigurare le loro reti per chiudere l'attacco, o per chiedere il loro aiuto nel tracciare il flusso di stimolo.

Poiché il danno al bersaglio finale di un attacco di tipo smurf è solitamente causato dal sovraccarico del collegamento in entrata da Internet, spesso non c'è risposta se non quella di contattare i riflettori. Quando i pacchetti arrivano a qualsiasi macchina sotto il controllo del destinatario, la maggior parte dei danni è già stata fatta.

Una misura temporanea consiste nel chiedere al provider di rete a monte di filtrare tutte le risposte echo ICMP o tutte le risposte echo ICMP di riflettori specifici. Si consiglia di non lasciare questo tipo di filtro in posizione permanente. Anche per un filtro temporaneo, devono essere filtrate solo le risposte echo, non tutti i pacchetti ICMP. Un'altra possibilità è quella di fare in modo che il provider a monte utilizzi le funzionalità di limitazione della qualità del servizio e della velocità per limitare la larghezza di banda disponibile per le risposte echo. Una limitazione ragionevole della larghezza di banda può essere lasciata in posizione indefinita. Entrambi questi approcci dipendono dalle apparecchiature del fornitore a monte che dispone della capacità necessaria e talvolta tale capacità non è disponibile.

Riflettore Smurf

Se il traffico in arrivo è costituito da richieste echo anziché da risposte echo (in altre parole, se la prima voce dell'elenco degli accessi, anziché la seconda, contava molte più corrispondenze di quante si potesse ragionevolmente prevedere), si potrebbe sospettare un attacco di tipo smurf in cui la rete viene utilizzata come riflettore, o forse una semplice inondazione di ping. In entrambi i casi, se l'attacco ha successo, ci si aspetterebbe che il lato in uscita della linea seriale e quello in entrata siano invasi. Infatti, a causa del fattore di amplificazione, ci si aspetterebbe che il lato in uscita sia ancora più sovraccarico del lato in entrata.

Ci sono diversi modi per distinguere l'attacco di un puffo dalla semplice inondazione di ping:

- I pacchetti Smurf stimolus vengono inviati a un indirizzo di broadcast diretto, anziché a un indirizzo unicast, mentre le ordinarie inondazioni ping utilizzano quasi sempre unicast. È possibile visualizzare gli indirizzi che utilizzano la parola chiave **log-input** nella voce dell'elenco degli accessi appropriata.
- Se si utilizza un riflettore smurf, il display dell'**interfaccia show** sul lato Ethernet del sistema visualizza un numero sproporzionato di trasmissioni in uscita, e in genere il numero di trasmissioni inviate nel display **show ip traffic**. Un ping flood standard non aumenta il traffico di broadcast in background.
- Se si è utilizzati come smurf reflector, il traffico in uscita verso Internet è maggiore di quello in entrata da Internet. In generale, sull'interfaccia seriale sono presenti più pacchetti di output che pacchetti di input. Anche se il flusso di stimolazione riempie completamente l'interfaccia di input, il flusso di risposta è più grande del flusso di stimolazione e vengono contate le perdite di pacchetti.

Un riflettore ha più opzioni rispetto al bersaglio finale di un attacco di tipo smurf. Se un riflettore sceglie di arrestare l'attacco, in genere è sufficiente utilizzare **no ip direct-broadcast** (o comandi non IOS equivalenti). Questi comandi appartengono a tutte le configurazioni, anche se non vi è alcun attacco attivo. Per ulteriori informazioni su come impedire che le apparecchiature Cisco vengano utilizzate in un attacco con arma da fuoco, consultare il documento sul miglioramento della sicurezza sui router Cisco. Per informazioni più generali sugli attacchi di tipo smurf in generale e per informazioni sulla protezione di apparecchiature non Cisco, vedere la pagina delle informazioni sugli attacchi Denial of Service .

Un riflettore è un passo più vicino all'aggressore di quanto sia il bersaglio finale, ed è quindi in una posizione migliore per tracciare l'attacco. Se si sceglie di rintracciare l'attacco, è necessario collaborare con gli ISP coinvolti. Se desideri che vengano intraprese delle azioni quando completi la traccia, devi lavorare con le forze dell'ordine appropriate. Se si cerca di rintracciare un attacco, si consiglia di coinvolgere le forze dell'ordine il prima possibile. Vedere la sezione Traccia per informazioni tecniche sulla traccia degli attacchi flooding.

Frammentare

L'attacco fraggle è analogo all'attacco smurf, con la differenza che le richieste echo UDP vengono usate per lo streaming stimolo invece delle richieste echo ICMP. La terza e la quarta riga della lista identificano attacchi fraudolenti. La risposta appropriata per le vittime è la stessa, con la differenza che l'eco su UDP è un servizio meno importante nella maggior parte delle reti rispetto all'eco su ICMP. Pertanto, è possibile disabilitarli completamente con meno conseguenze negative.

SYN Floods

La quinta e la sesta riga dell'elenco degli accessi sono:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

La prima di queste righe corrisponde a qualsiasi pacchetto TCP con bit ACK impostato. Ai nostri scopi, ciò che questo realmente significa è che corrisponde a qualsiasi pacchetto che non è un TCP SYN. La seconda riga corrisponde solo ai pacchetti che sono SYN di TCP. Un'inondazione SYN è facilmente identificabile dai contatori su queste voci di elenco. Nel traffico normale, i pacchetti TCP non SYN superano i pacchetti SYN di almeno un fattore di due, e di solito più di quattro o cinque. In un'inondazione SYN, in genere i SYN superano di molto i pacchetti TCP non SYN.

L'unica condizione senza attacchi che crea questa firma è un enorme sovraccarico di richieste di connessione autentiche. In generale, un tale sovraccarico non arriverà inaspettatamente, e non coinvolgerà tanti pacchetti SYN quanto una vera e propria inondazione SYN. Inoltre, i flooding SYN spesso contengono pacchetti con indirizzi di origine non validi; utilizzando la parola chiave **log-input**, è possibile verificare se le richieste di connessione provengono da tali indirizzi.

C'è un attacco chiamato "attacco a tabella di processo" che ha alcune somiglianze con l'inondazione della SYN. Nell'attacco alla tabella del processo, le connessioni TCP vengono completate, quindi lasciate scadere senza ulteriore traffico di protocollo, mentre nell'inondazione SYN vengono inviate solo le richieste di connessione iniziali. Poiché un attacco alla tabella del processo richiede il completamento dell'handshake iniziale TCP, in genere deve essere avviato utilizzando l'indirizzo IP di un computer reale a cui l'utente non autorizzato ha accesso (accesso in genere rubato). Gli attacchi da tabella di processo si distinguono facilmente dai flood SYN con l'uso della registrazione dei pacchetti. Tutti i SYN in un attacco di tabella di processo provengono da uno o alcuni indirizzi o al massimo da una o alcune subnet.

Le opzioni di risposta per le vittime delle inondazioni SYN sono molto limitate. Il sistema sotto attacco è di solito un servizio importante, e il blocco dell'accesso al sistema di solito compie ciò che l'aggressore vuole. Molti prodotti router e firewall, inclusi quelli di Cisco, dispongono di funzionalità che possono essere utilizzate per ridurre l'impatto dei problemi di SYN. Ma l'efficacia di queste caratteristiche dipende dall'ambiente. Per ulteriori informazioni, fare riferimento alla documentazione sul set di funzionalità di Cisco IOS Firewall, alla documentazione sulla funzionalità Cisco IOS TCP Intercept e al documento Miglioramento della sicurezza sui router Cisco.

Èpossibile rintracciare le inondazioni SYN, ma il processo di rintracciamento richiede l'assistenza di ogni ISP lungo il percorso dall'aggressore alla vittima. Se decidi di cercare di tracciare un'inondazione SYN, contatta le forze dell'ordine al più presto e collabora con il tuo provider di servizi a monte. Per i dettagli sul tracciamento con l'uso di apparecchiature Cisco, vedere la sezione Traccia di questo documento.

Altri attacchi

Se si ritiene di essere sotto attacco e si è in grado di caratterizzare tale attacco utilizzando indirizzi di origine e di destinazione IP, numeri di protocollo e numeri di porta, è possibile utilizzare gli elenchi degli accessi per verificare l'ipotesi formulata. Creare una voce dell'elenco degli accessi che corrisponda al traffico sospetto, applicarla a un'interfaccia appropriata e guardare i contatori

delle partite o registrare il traffico.

Avvertenze relative a registrazione e contatori

Il contatore di una voce dell'elenco accessi conta tutte le corrispondenze con quella voce. Se si applica un elenco degli accessi a due interfacce, i conteggi visualizzati sono conteggi aggregati.

La registrazione dell'elenco degli accessi non visualizza tutti i pacchetti che corrispondono a una voce. La registrazione è limitata alla velocità per evitare il sovraccarico della CPU. La registrazione mostra che si è un campione ragionevolmente rappresentativo, ma non una traccia completa del pacchetto. Tenere presente che vi sono pacchetti che non vengono visualizzati.

In alcune versioni software, la registrazione degli elenchi degli accessi funziona solo in determinate modalità di commutazione. Se una voce dell'elenco accessi contiene molte corrispondenze, ma non registra nulla, provare a cancellare la cache route per forzare la commutazione dei pacchetti. Fare attenzione se si esegue questa operazione su router con carichi pesanti con molte interfacce. Durante la ricostruzione della cache è possibile che venga interrotta una notevole quantità di traffico. Se possibile, utilizzare Cisco Express Forwarding.

Gli elenchi degli accessi e la registrazione hanno un impatto sulle prestazioni, ma non di grandi dimensioni. Prestare attenzione ai router che vengono eseguiti a un carico della CPU superiore all'80% o quando si applicano elenchi di accesso a interfacce ad altissima velocità.

Traccia

Gli indirizzi di origine dei pacchetti DoS sono quasi sempre impostati su valori che non hanno nulla a che fare con gli aggressori stessi. Pertanto, non sono utili nell'identificazione degli aggressori. L'unico modo affidabile per identificare la fonte di un attacco è tracciarlo hop dopo hop attraverso la rete. Questo processo comporta la riconfigurazione dei router e l'esame delle informazioni del log. È necessaria la cooperazione di tutti gli operatori di rete lungo il percorso dall'aggressore alla vittima. Per garantire tale cooperazione è in genere necessario il coinvolgimento delle forze dell'ordine, che devono essere coinvolte anche nel caso in cui si intenda intraprendere qualsiasi azione contro l'aggressore.

Il processo di rilevamento delle inondazioni del servizio per la sicurezza è relativamente semplice. Partendo da un router (chiamato "A") che è noto come vettore del traffico di alluvione, si identifica il router (chiamato "B") da cui A sta ricevendo il traffico. Uno di loro accede quindi a B e trova il router (chiamato "C") da cui B sta ricevendo il traffico. Questa operazione continua fino a quando non viene trovata la fonte finale.

Questo metodo presenta diverse complicazioni descritte nell'elenco seguente:

- La "fonte ultima" può essere un computer compromesso dall'aggressore, ma che in realtà è di proprietà e gestito da un'altra vittima. In questo caso, il tracciamento dell'inondazione DoS è solo il primo passo.
- Gli aggressori sanno di poter essere rintracciati e di solito continuano i loro attacchi solo per un periodo di tempo limitato. Potrebbe non esserci abbastanza tempo per ricostruire l'alluvione.
- Gli attacchi possono provenire da molteplici fonti, soprattutto se l'aggressore è relativamente sofisticato. È importante cercare di identificare il maggior numero possibile di fonti.

- I problemi di comunicazione rallentano il processo di rilevamento. Spesso uno o più operatori di rete interessati non dispongono di personale adeguatamente qualificato.
- Le preoccupazioni legali e politiche possono rendere difficile l'azione contro gli aggressori, anche se viene trovato.

La maggior parte degli sforzi per rintracciare gli attacchi DoS fallisce. Per questo motivo, molti operatori di rete non cercano nemmeno di rintracciare un attacco se non sotto pressione. Molti altri tracciano solo attacchi "gravi", con definizioni diverse di ciò che è "grave". Alcuni assistono con una traccia solo se sono coinvolte le forze dell'ordine.

Traccia con "log-input"

Se si sceglie di tracciare un attacco che passa attraverso un router Cisco, il modo più efficace per farlo è costruire una voce dell'elenco degli accessi che corrisponda al traffico di attacco, associare la parola chiave **log-input** a tale voce e applicare l'elenco degli accessi in uscita sull'interfaccia attraverso cui il flusso di attacco viene inviato verso la destinazione finale. Le voci di log prodotte dall'elenco degli accessi identificano l'interfaccia del router attraverso cui arriva il traffico e, se l'interfaccia è una connessione multipunto, forniscono l'indirizzo di layer 2 del dispositivo da cui viene ricevuta. L'indirizzo di layer 2 può quindi essere utilizzato per identificare il router successivo nella catena, ad esempio tramite il comando **show ip arp** ***mac-address***.

SYN Flood

Per tracciare un'inondazione SYN, è possibile creare un elenco degli accessi simile al seguente:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

In questo modo vengono registrati tutti i pacchetti SYN destinati all'host di destinazione, inclusi i SYN legittimi. Per identificare il percorso effettivo più probabile verso l'autore dell'attacco, esaminare le voci del log in dettaglio. In generale, l'origine dell'inondazione è la fonte da cui proviene il maggior numero di pacchetti corrispondenti. Gli indirizzi IP di origine non hanno alcun significato. Stai cercando le interfacce di origine e gli indirizzi MAC di origine. A volte è possibile distinguere i pacchetti flood dai pacchetti legittimi perché i pacchetti flood possono avere indirizzi di origine non validi. È probabile che qualsiasi pacchetto il cui indirizzo di origine non sia valido faccia parte del flusso.

L'inondazione può provenire da fonti diverse, anche se questo è relativamente insolito per le inondazioni SYN.

Smurf Stimulus

Per tracciare un flusso di stimolazione del sorso, usare un elenco di accesso come questo:

```
access-list 169 permit icmp any any echo log-input
access-list 169 permit ip any any
```

La prima voce non si limita ai pacchetti destinati all'indirizzo del riflettore. Il motivo è che la maggior parte degli attacchi smurf utilizzano più reti di riflettori. Se non si è in contatto con la destinazione finale, è possibile che non si conoscano tutti gli indirizzi dei riflettori. Man mano che la traccia si avvicina all'origine dell'attacco, è possibile che le richieste echo inizino ad arrivare a

un numero sempre maggiore di destinazioni; questo è un buon segno.

Tuttavia, se si gestisce una grande quantità di traffico ICMP, è possibile che vengano generate troppe informazioni di registrazione da leggere facilmente. In tal caso, è possibile limitare l'indirizzo di destinazione a uno dei riflettori utilizzati. Un'altra tattica utile è usare una voce che sfrutti il fatto che le netmask 255.255.255.0 sono molto comuni su Internet. E, a causa del modo in cui gli aggressori trovano i riflettori, gli indirizzi dei riflettori usati per gli attacchi con la scimmia hanno maggiori probabilità di corrispondere a quella maschera. Gli indirizzi host che terminano con .0 o .255 sono molto rari in Internet. Pertanto, è possibile costruire un riconoscitore relativamente specifico per i flussi di stimolo del sorso come mostra questo output:

```
access-list 169 permit icmp any host known-reflector echo log-input access-list 169 permit icmp any 0.0.0.255 255.255.255.0 echo log-input access-list 169 permit icmp any 0.0.0.0 255.255.255.0 echo log-input access-list 169 permit ip any any
```

Con questo elenco, è possibile eliminare molti dei pacchetti "rumore" dal vostro log, mentre si ha ancora una buona possibilità di notare ulteriori flussi di stimolo mentre si avvicina all'aggressore.

Traccia senza "log-input"

la parola chiave **log-input** viene usata nel software Cisco IOS versione 11.2 e successive e in alcune versioni 11.1 create appositamente per alcuni mercati. Non è supportata sulle versioni software meno recenti. Se si utilizza un router con un software precedente, sono disponibili tre opzioni:

- Creare un elenco degli accessi senza registrazione, ma con voci corrispondenti al traffico sospetto. Applicare l'elenco sul lato *input* di ciascuna interfaccia a turno e controllare i contatori. Cercare interfacce con alte percentuali di corrispondenza. Questo metodo ha un sovraccarico di prestazioni molto ridotto ed è utile per l'identificazione delle interfacce di origine. Il suo maggiore inconveniente è che non fornisce indirizzi sorgente del livello di collegamento ed è quindi utile soprattutto per le linee punto-punto.
- Creare le voci dell'elenco degli accessi con la parola chiave **log** (in contrapposizione a **log-input**). Applicare nuovamente l'elenco al lato in ingresso di ciascuna interfaccia. Questo metodo non fornisce ancora indirizzi MAC di origine, ma può essere utile per visualizzare i dati IP. Ad esempio, per verificare che un flusso di pacchetti sia effettivamente parte di un attacco. L'impatto sulle prestazioni può essere moderato o elevato e le prestazioni del software più recente sono migliori rispetto a quelle del software precedente.
- Per raccogliere informazioni sui pacchetti, usare il comando **debug ip packet detail**. Questo metodo fornisce indirizzi MAC, ma può avere un impatto significativo sulle prestazioni. È facile commettere un errore con questo metodo e rendere inutilizzabile un router. Se si utilizza questo metodo, verificare che il router commuti il traffico di attacco in modalità rapida, autonoma o ottimale. Utilizzare un elenco degli accessi per limitare il debug alle sole informazioni effettivamente necessarie. Registra le informazioni di debug nel buffer di registro locale, ma disattiva la registrazione delle informazioni di debug nelle sessioni Telnet e nella console. Se possibile, fare in modo che qualcuno sia fisicamente vicino al router, in modo che possa essere riacceso e riacceso, se necessario.Tenere presente che il comando **debug ip packet** non visualizza informazioni sui pacchetti a commutazione veloce. Per acquisire le informazioni, è necessario usare il comando **clear ip cache**. Ogni comando **clear** restituisce uno o due pacchetti di output di debug.

Informazioni correlate

- Kerberos
- Documentazione e supporto tecnico – Cisco Systems