Università degli Studi di Salerno
Corso di Sicurezza su Reti 2000

Distributed Denial of Service

Autori: Roberto Gassirà
Enrico Luciano
Michele Masullo

Sommario

- Concetto attacco DOS
- Tipologia di attacchi
- Tecniche utilizzate
- Attacco DOS distribuito
- Metodologie di difesa

Cosa è ?

Lo scopo di un attacco DOS è essenzialmente quello di negare agli utenti legittimi l'uso totale o parziale di una o più componenti di un sistema informativo (Es. banda Internet, sistemi hardware e software).

Perché un attacco DOS?

- Frustrazione
  - L'attaccante non riesce ad introdursi illegalmente in un sistema e decide di farlo cadere
- Azione dimostrativa
  - Singoli o gruppi hanno motivi personali o politici di rivalsa nei confronti di singoli o organizzazioni
- Necessità pratiche
  - Necessità di operare un reboot per rendere effettive alcune modifiche al sistema

Tipologia di attacco

- Saturazione di banda
- Resource starvation
- Bug Software
- Attacchi basati sul routing
- Attacchi basati sul DNS

Saturazione di banda

Generare una quantità di traffico tale da consumare tutta la banda a disposizione di un sito.

Scenario 1.

un sito con a disposizione una banda molto ampia contro un sito con molta meno banda a disposizione

Scenario 2.

l'attaccante ha meno banda della vittima. Usa delle tecniche di "amplificazione" per portare l'attacco

Resource starvation

Si tende a saturare altre risolse del sistema piuttosto che i link di rete

Es. tempo di CPU, memoria, spazio su disco, handle di file, etc

In genere il sistema diventa inusabile oppure collassa

Bug Software

Si sollecita il sistema in modo da attivare situazione che non sono correttamente gestite dal software di sistema

Es. bug nello stack di rete (WinNuke, IP frag overlap)
Buffer overflow
Errori presenti in HW dedicato

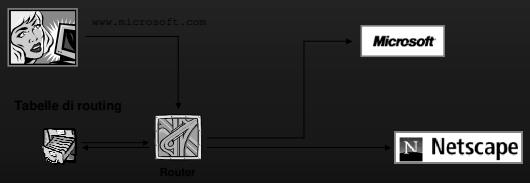
IP fragmentation overlap

Si basa sulla vulnerabilità presente nelle implementazioni software dello stack IP, per quanto riguarda il riassemblaggio della sequenza dei pacchetti

La tecnica consiste nel generare una sequenza di pacchetti costruita "ad arte" in modo da provocare il crash o il reboot del sistema

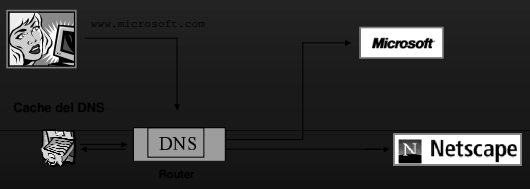
Attacchi basati su routing

L'attaccante manipola le tabelle di routing in modo da deviare tutto o parte del traffico della rete verso una destinazione diversa o verso un "buco nero"



Attacchi basati sul DNS

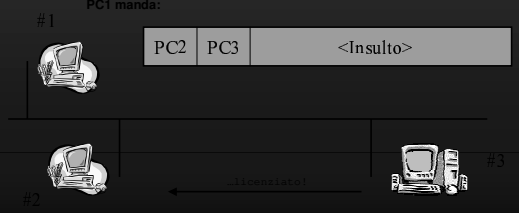
L'attaccante manipola la cache del sistema DNS in modo da deviare tutto o parte del traffico della rete verso una destinazione diversa o verso un "buco nero"



Tecniche utilizzate

Spoofing

Modifica del campo sorgente di un pacchetto dati, in modo che il destinatario non possa risalire correttamente al mittente



Smurfing

Attacco DOS usato per saturare la banda che basa la sua efficacia su una tecnica di amplificazione del traffico

L'amplificazione si ottiene con un ping (pacchetto ICMP) verso ad un indirizzo di broadcast di una rete

Smurfing

Broadcast

Ogni set di indirizzi IP ne ha uno particolare, detto di broadcast, che non può essere assegnato ad uno specifico elaboratore

I pacchetti spediti a tale indirizzo vengono inoltrati a tutti gli indirizzi IP della rete di appartenenza

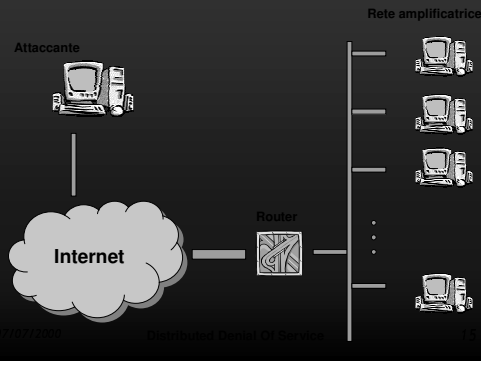
Smurfing

PING

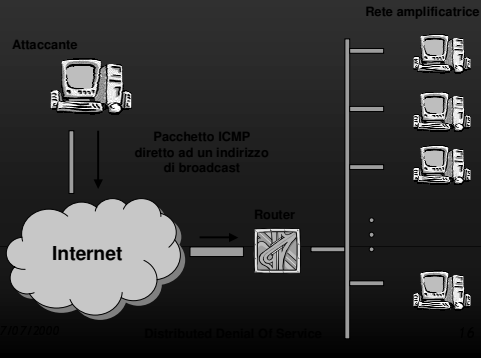
Trasmette un pacchetto di controllo ICMP ad un destinatario e ne aspetta la risposta

In genere viene usato per controllare la raggiungibilità di una certa destinazione o per calcolare le prestazioni della rete (Round trip delay)

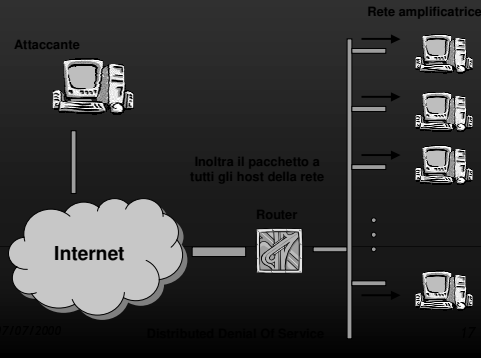
Ping broadcast

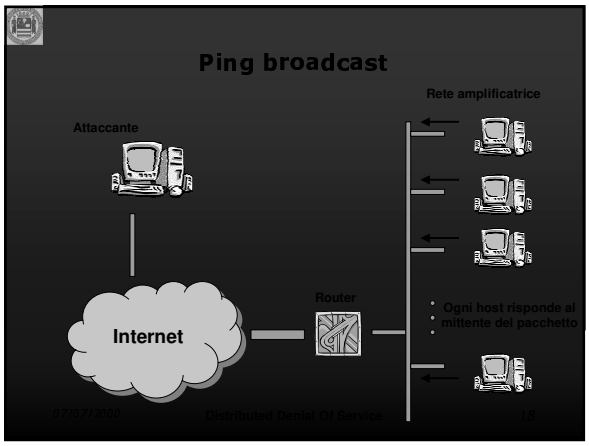


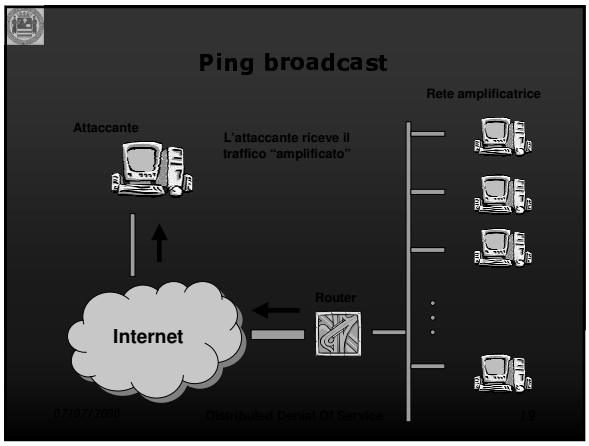
Ping broadcast

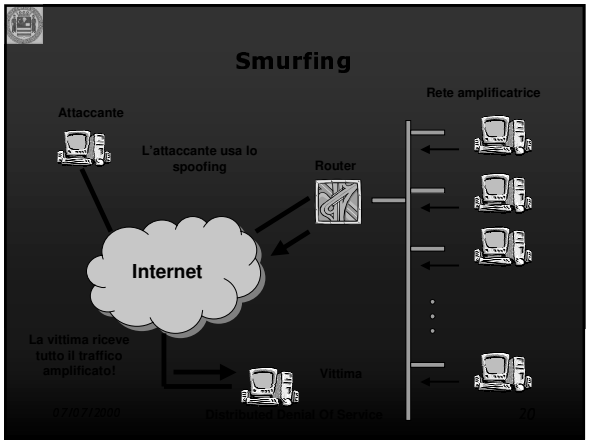


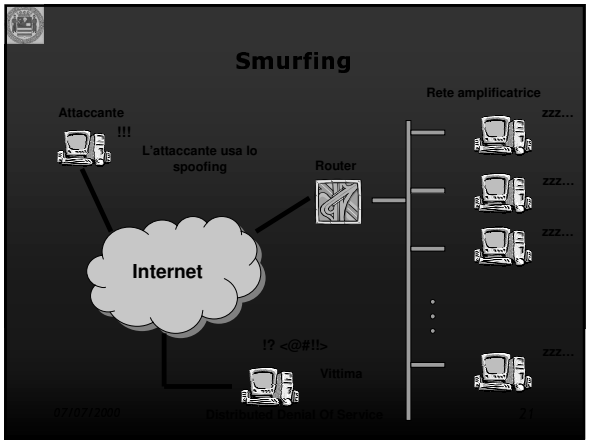
Ping broadcast

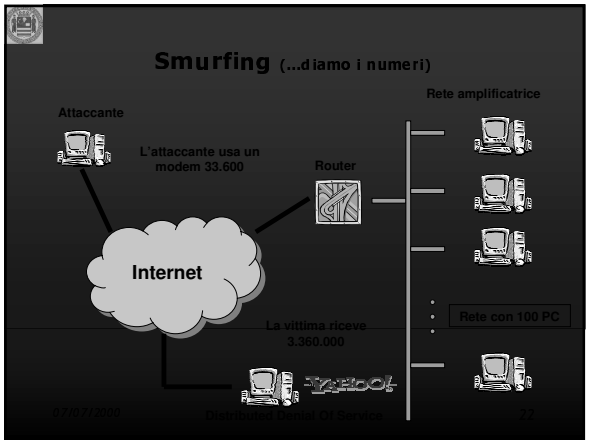



Ping broadcast
Rete amplificatrice
Attaccante
Internet
Router
Ogni host risponde al mittente del pacchetto
07/07/2000
Distributed Denial Of Service
18


Ping broadcast
Rete amplificatrice
Attaccante
L'attaccante riceve il traffico "amplificato"
Internet
Router
07/07/2000
Distributed Denial Of Service
19


Smurfing
Rete amplificatrice
Attaccante
L'attaccante usa lo spoofing
Router
Internet
La vittima riceve tutto il traffico amplificato!
Vittima
07/07/2000
Distributed Denial Of Service
20


Smurfing
Rete amplificatrice
Attaccante
!!!
L'attaccante usa lo spoofing
Router
zzz...
Internet
!? <@#!!>
Vittima
07/07/2000
Distributed Denial Of Service
21


Smurfing (...diamo i numeri)
Rete amplificatrice
Attaccante
L'attaccante usa un modem 33.600
Router
Internet
Rete con 100 PC
La vittima riceve 3.360.000
YAHOO!
07/07/2000
Distributed Denial Of Service
22

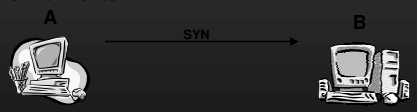
Fraggle attack
Variante dello smurfing:
usa il protocollo UDP al posto di ICMP
Genera comunque traffico
Se gli host sulla rete "amplificatrice" non sono configurati per rispondere ai pacchetti UDP, trasmettono indietro un pacchetto ICMP "unreachable"
07/07/2000
Distributed Denial Of Service
23

SYN flood attack

Usa una debolezza nella implementazione – configurazione del protocollo di connessione "three way handshake"

SYN flood attack

Normalmente…

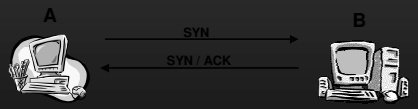


Stato porta:

LISTEN > SYN_RECV

SYN flood attack

Normalmente…

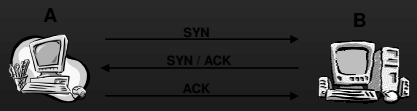


Stato porta:

LISTEN > SYN_RECV

SYN flood attack

Normalmente…

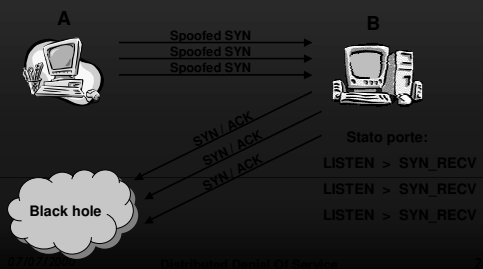


Stato porta:

SYN_RECV > ESTABILISHED

SYN flood attack

Durante l'attacco…



Stato porte:

LISTEN > SYN_RECV

LISTEN > SYN_RECV

LISTEN > SYN_RECV

SYN flood attack

- Lo scopo è di far riempire la coda delle connessioni "potenziali" fino ad esaurire tutte le risorse allocate allo scopo, che normalmente sono limitate

Vantaggi:

- permette attacchi "stealth"
- Necessita di poca banda

Evoluzioni

Attacchi Stream

Consiste nello spedire pacchetti TCP con ACK o SYN-ACK contemporaneamente. Siccome questi pacchetti non fanno parte di una connessione, prendono un certo tempo per essere gestiti dalla vittima

Se il numero di pacchetti è elevato, l'host che li deve gestire può sovraccaricarsi ed andare in crash

Evoluzioni

Confondere IDS (Intrusion Detection System)

Si inseriscono nel traffico diretto alla vittima particolari stringhe che possono essere scorrettamente interpretate dall'IDS come tentativi di intrusione, generando falsi allarmi

Se il numero di pacchetti di questo tipo è elevato l'IDS si sovraccarica

Vantaggio: Si elimina una difesa del sito

Attacchi DOS distribuiti

Cosa è?

E' un sistema per automatizzare e coordinare un attacco DOS nel quale gli attaccanti siano molteplici

Filosofia

Come per le challenge DES, RSA: dividere il carico di lavoro su diverse macchine, mentre una o più sovrintendono allo svolgimento del lavoro

Attacchi DOS distribuiti

Origine

implementati in prodotti commerciali per il CAPACITY MANAGEMENT

Scopo

- Dimostrare che saturare un link piuttosto grande non è difficile quanto si crede
- Dimostrare la scarsa "sicurezza di fondo" di Internet

Strategie di attacco

Strategie di attacco

- Scelta della vittima
- Scelta del tipo di attacco
- Basi di un attacco

Scelta della vittima

- Tale scelta deve essere oculata
- Bisogna assicurarsi che la rete sia *debole*
- Prima dell'attacco bisogna eseguire dei "sopralluoghi" per rendersi conto delle precauzioni prese dalla vittima

Scelta del tipo di attacco

- ICMP ECHO ed ECHO FRAGGLE
- TCP/SYN FLOOD
- DNS ATTACK (BIND)
- UDP FLOOD
- ICMP/UDP ILLEGALY FRAGMENTED (MS IP STACK)

Basi di un Attacco

- Bisogna scegliere una rete mal configurata a larga banda che fungerà da amplificatore
- Acquisire privilegi di *superuser*
- Mandare pacchetti "*spooffati*" alla vittima
- Utilizzare macchine *"sicure"* per iniziare l'attacco

Tribe Flood Network 2K

Che cosa e'?

E' uno dei tool piu' evoluti e potenti per eseguire un attacco di tipo Distributed Denial of Service

Il creatore e' Mixter, programmatore tedesco che scrive applicativi "Ostili" per compagnie specializzate nel testing di Firewall e altri tipi di protezioni

Il motivo di fondo del tool è dimostrare le insicurezze di internet che non vengono totalmente risolte (Nuovo protocollo di comunicazioni, IPv6)

Che cosa e'?

Trae il meglio dei suoi predecessori che sono:

- TrinOO (Phifly)
- TFN (Mixter)
- Stacheldraht (Randomizer)
- Shaft (?)
- TFN2k (Mixter)

Caratteristiche

Il tool è formato da:

- Client (tfn) che trasmette i comandi (compilato su macchine definite Master)
- Server (td) che esegue i comandi ricevuti dal/i Master (compilato su macchine definite Agent)
- Piu' Master comandano piu' Agent
- I client e i server vengono eseguiti con un nome "camuffato"
- I sistemi operativi che vengono colpiti principalmente sono Solaris, Unix, Windows NT

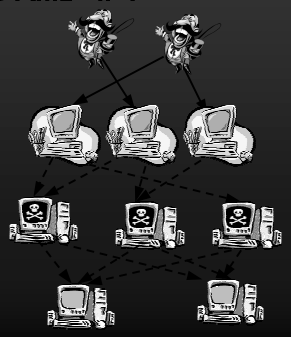
Come Funziona?

Uno o più Attacker (Cracker)...

...utilizzando uno o più client...

...comanda i vari server ...

...di attaccare uno o più target (Vittime dell'attacco)!



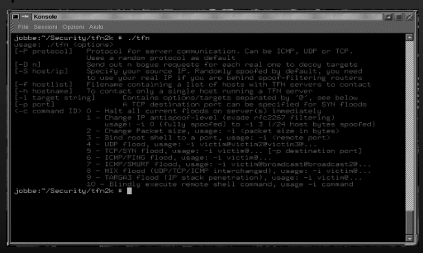
Configurazione degli Agent

Poiché il tool deve essere eseguito con i privilegi di SuperUtente (per esempio root in ambiente Linux) per attaccare i target, un attacker deve:

- Entrare nel sistema conoscendo la password di SuperUtente (molto difficile)
- Utilizzare qualche "bug" dei servizi offerti dal sistema operativo (exploit oppure altri Ddos)

Configurazione dei Master

- Il client Tfn viene eseguito a "Linea di comando" e in base al tipo di attacco che si ordina cambia la sintassi



Modalità di Attacco

Gli attacchi possibili sono:

- TCP/SYN Flood
- UDP/SYN Flood
- ICMP Flood
- SMURF
- TARGA 3

Inoltre:

- Fa il "bind" di una "root shell" su una porta
- Esegue comandi in remoto come superutente

Comunicazione Client-Server

- I comandi sono mandati dai Master agli Agent usando come protocollo TCP, UDP, ICMP oppure uno a caso
- I vari Agent sono "silenziosi" ovvero i comandi avvengono in modalità One-Way
- I comandi non sono in "String Based" ma usano una forma del tipo "+<ID>+<DATA>"
- I comandi sono criptati usando come algoritmo di cifratura il CAST 256, uno dei possibili candidati all'AES, e come chiave un password inserita in fase di compilazione

Comunicazione Client-Server

- Tutti i dati sono codificati in Base 64, la stessa codifica ASCII degli allegati delle e-mail
- Le comunicazioni possono essere miscelate con "Decoy Packet"
- I pacchetti vengono mandati con la tecnica dello "Spoofing"

Web Sites Attacked

- Seconda settima di Febbraio 2000: Bloccati e rallentati alcuni tra i siti più famosi e visitati del mondo con attacchi di tipo DDOS
- Le macchine utilizzate dagli attacker erano principalmente computer di Università Americane e Tedesche
- Alcuni attacchi sono stati compiuti da un ragazzo 15-enne canadese di nome "MafiaBoy" arrestato il 15 Aprile 2000

Qualche Esempio ...

YAHOO!

Giorno: 7 Febbraio 2000

Durata Attacco: 1:15 p.m. - 4:25 p.m. ET

Tipo Di Attacco: ICMP Smurf (trinOO)

Traffico Generato: 1 Gigabyte al secondo da 50 punti differenti

Note: Yahoo! Era tra i 5 siti mondiali più "Available" con 465 milioni di pagine visitate al giorno

Qualche Esempio ...

CNN.com

Giorno: 8 Febbraio 2000

Durata Attacco: 7:00 p.m. - 8:45 p.m. ET

Tipo Di Attacco: TCP/SYN Flood

Traffico Generato: Non dichiarato

Note: L'attacco è continuato anche dopo. L'attacker è stato Mafiaboy

Qualche Esempio ...

ZDNet

Giorno: 9 Febbraio 2000 – 20 Febbraio 2000

Durata Attacco: 7:11 a.m. - 9:43 a.m. PT – 7:05 a.m. - 9:12 a.m. PT

Tipo Di Attacco: TCP/SYN Flood

Traffico Generato: 800 MegaByte al secondo

Note: Ha un numero medio di visitatori all'anno vicino ad un milione

Metodologie di difesa

E' possibile proteggersi da attacchi DDOS?

- ICMP ECHO ed ECHO FRAGGLE
- SYN FLOOD
- DNS ATTACK (BIND)
- ICMP/UDP ILLEGALY FRAGMENTED (MS IP STACK)
- TFN2K (esempio)

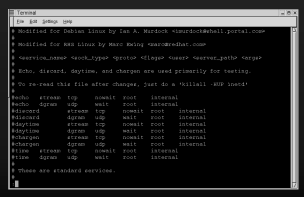
ICMP ECHO ed ECHO FRAGGLE

- Una rete per evitare di essere utilizzata come amplificatore deve:
  - Utilizzare un router abilitando la voce 'no ip directed-broadcast'
  - Configurare un firewall in modo tale da bloccare pacchetti ICMP destinati all'indirizzo di rete o di broadcast

ECHO FRAGGLE: ESEMPIO

- Disattivare il servizio ECHO
- Esempio Linux:

  commentare la linea relativa al servizio echo (porta 7) nel file /etc/inetd.conf



DNS ATTACK (BIND)

- Le nuove versioni di bind, a decorrere dalla 8.1.1, non sono più vulnerabili a questa tipo di attacco
- Soluzione: upgradare la propria versione di bind (Ultima Versione 8.2.2-P5).

SYN FLOOD

- Come rilevare un attacco SYN FLOOD?
  - Utilizzare "Tool di Monitoraggio" per rilevare le connessioni nello stato SYN_RECV
- Come difendersi?
  - Incrementare la coda delle connessioni
  - Decrementare i tempi di timeout
  - Utilizzare soluzioni software
  - Utilizzare un IDS (Intrusion Detection System)

ICMP/UDP Illegaly Fragmented (MS IP STACK)

Microsoft ha rilasciato nella seconda meta' di maggio 2000 delle patch per S.O. win9x, NT (tutte le versioni), e per tutte le versioni di win 2000. Esse sono reperibili al sito della Microsoft

TFN2K: Prevenzione

- Le soluzioni viste in precedenza possono non bastare contro un DDOS
- Evitare di diventare ospiti del server 'td' o del client 'tfn' con una buona amministrazione del sistema
  - FindDdos (rileva la presenza di td o tfn)
  - Cracktfn2k (password recovery)
- Evitare con dei router che possano partire pacchetti con indirizzi diversi da quelli della rete di appartenenza
- Utilizzare tools di monitoraggio (sniffer, etc.,etc.)

TFN2K: come rilevare un attacco

Sintomi:

- Un alto traffico di pacchetti proveniente da differenti host

  anche inesistenti
- Taglie anomale di pacchetti ICMP e UDP
- Pacchetti TCP non facenti parte di una connessione
- Il contenuto dei pacchetti è del tutto alfanumerico

TFN2K

- E se siamo gia sotto attacco?

Mettiamoci a pregare!!!

TFN2K: come riprendersi dall'attacco

- Contattare il proprio ISP chiedendo di bloccare i pacchetti responsabili dell'attacco
- Contattare altri ISP in modo tale da far bloccare anche nei loro punti tali pacchetti
- Riconfigurare i router e/o i firewall