Laboratorio di sicurezza informatica

(seconda parte)

Gabriele D'Angelo, Ludovico Gardenghi
{gda, garden}@cs.unibo.it

Università di Bologna
Dipartimento di Scienze dell'Informazione

Luglio, 2005

Scaletta della lezione

- Denial of Service (DoS)
- Flooding / Distributed Denial of Service (DDoS)
- Botnet + Spam
- Bug notevoli di TCP/IP
- {Man, Monkey} in the Middle
- Sniffing
- Wireless: cifratura WEP, WPA
- Note e bibliografia

Achtung!

- Quanto vi presenteremo oggi e nelle prossime lezioni è a puro

  scopo didattico

- Le intrusioni nei sistemi informatici sono punite dalla legge e quindi non è il caso di giocare senza capire bene cosa si sta facendo

- Esistono le macchine e le reti virtuali: usiamole!

- Vi impegnate ad usare quanto appreso a solo scopo difensivo?

Denial of Service (DoS)

- Lo scopo di un DoS è rendere un servizio inutilizzabile, ci sono vari modi per ottenere questo risultato:
  - sovraccaricare di richieste il servizio (lo slashdotting è un ottimo esempio di DoS involontario, in generale le tecniche di flooding)
  - interrompere il servizio provocando la sua disattivazione (sfruttare un exploit per mandare il server in segfault o in loop)
- In alcuni casi è possibile limitare gli effetti di un DoS attraverso opportune tecniche di filtraggio (ad esempio impostando una regola del firewall), in altri casi **non** è possibile alcuna reazione
- Casi notevoli:
  - banda fatturata a consumo (eventualmente con conteggio esterno alla nostro firewall)
  - flooding della mailbox / utilizzo di tutta la banda in entrata

In pratica...

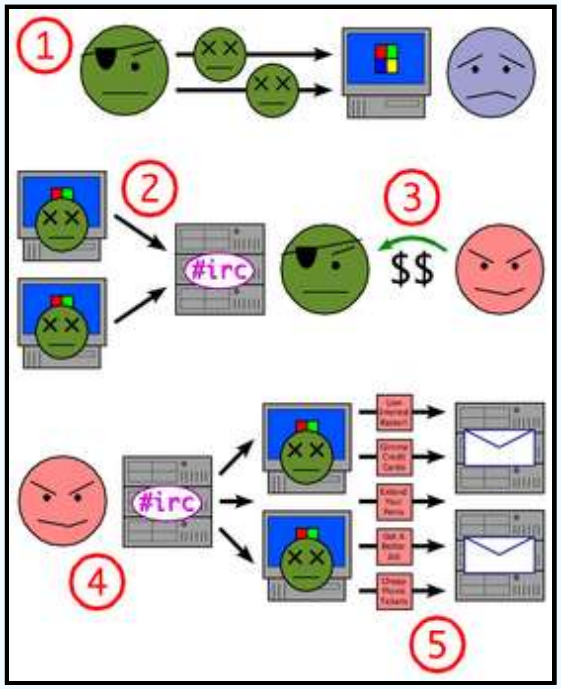
Vediamo nella pratica...
oftpd, ping

Flooding / Distributed Denial of Service (DDoS)

- L'attacco di tipo DDoS avviene spesso in modo **distribuito**, per aumentare la banda aggregata disponibile e per rendere improbabile l'identificazione dell'attaccante originario
- Si basa sull'uso di computer **zombie** che sono stati precedentemente infettati attraverso worm/virus/trojan horse, il coordinamento tra gli slave host avviene spesso via **IRC** (**botnet**)
- Una botnet può essere sfruttata non solo per attacchi di tipo DoS ma anche per l'invio massicco e distribuito di **spam**

Botnet + Spam = !!!

- Esempio tratto da: http://en.wikipedia.org/wiki/Botnet



1) Attraverso un virus o worm vari host connessi ad Internet vengono infettati

2) Gli host infettati formano una botnet e sono in grado di coordinarsi via IRC

3) Chi ha il controllo della botnet vende il suo "servizio" illecito ad uno spammer

4) Lo spammer impartisce una serie di comandi che viene propagata alla botnet

5) Tutti i componenti della botnet spediscono spam agendo ognuno sul proprio mailserver, su una lista di relay aperti o direttamente

Bug notevoli di TCP/IP: implementazione

- Un numero non indifferente di DoS sono, o sono stati, possibili a causa di bug nell'implementazione dello stack dei protocolli di rete
- Le conseguenze tipiche di attacchi verso queste vulnerabilità:
  - chiusura brusca di connessioni
  - isolamento della macchina dalla rete
  - crash del sistema
  - attraversamento di regole di net filtering (non si tratta di DoS)
- Per quanto riguarda TCP/IP, è stata spesso la gestione dei frammenti a causare problemi (es. il famoso "ping of death")
- Altri attacchi che hanno "fatto storia": Tiny Fragment, Teardrop, Overlapping Fragment
- Spesso usati per "ammutolire" un host durante uno spoofing

Bug notevoli di TCP/IP: errori di progettazione

- Circa un anno fa è stata rilevata una vulnerabilità nella struttura stessa di TCP
- Non si tratta di un bug di implementazione ed è quindi comune a praticamente **tutte** le architetture dotate di uno stack TCP/IP
- La vulnerabilità consente all'attaccante di chiudere connessioni TCP fra host remoti
- Chiudere connessioni fra un browser e un web server può essere seccante ma innocuo
- Altri protocolli (zone transfer DNS, protocolli di routing come BGP) possono essere molto penalizzati dalla chiusura delle connessioni
- In questo caso si è riusciti a “rappezzare” il bug. In futuro?

{Man, Monkey} in the Middle

- Un buon esempio di attacco attivo: inserirsi fra i due estremi della comunicazione per carpire informazioni o modificare i dati
- In qualche modo (spoofing a vari livelli, DNS poisoning) si costringe il client a connettersi non all'host di destinazione ma a una macchina controllata dall'attaccante
- L'host "intruso" finge di essere ciascuno dei due estremi nei confronti dell'altro e ha il controllo completo di ciò che viene trasmesso
- Può essere applicato anche su connessioni cifrate con chiavi pubbliche! (es. SSH, HTTPS)
- In questo caso ci si può rendere conto del problema solo prestando attenzione e comunque non sempre

In pratica...

Vediamo nella pratica...
ssh, ettercap

Sniffing

- Per sniffing usualmente si intende l'intercettare in modo **passivo** i dati che transitano su una rete
- In presenza di un **bus** come mezzo trasmissivo o di un **hub**, lo sniffing risulta facile: attivare la **modalità promiscua** della scheda di rete e catturare tutto il traffico passante
- Le reti attuali sono quasi tutte con **topologia a stella** e basate sulla presenza di uno o più **switch**. Visto il funzionamento degli switch sono necessarie tecniche più sofisticate per sniffare (ad esempio ARP spoofing, ARP poisoning)
- Su rete wireless le cose sono decisamente diverse, come vedremo in seguito

In pratica...

Vediamo nella pratica...
dsniff, tcpdump, ethereal

Wireless: WEP

- La sicurezza delle reti wireless è nota per la sua... insicurezza
- Chi ha in casa o in azienda una rete wireless spesso non si preoccupa della sicurezza (basta fare un giro con un portatile...)
- Il protocollo WEP (Wired Equivalent Protocol) è strutturalmente debole e si presta a diversi attacchi
- La chiave WEP è composta da una parte definita dall'utente e da una pseudocasuale (IV, initialization vector) generata dalla scheda
- L'IV "dovrebbe" cambiare per ogni pacchetto, ma non sempre questo avviene per vari motivi (spazio troppo piccolo o implementazioni stupide)
- Due pacchetti cifrati con lo stesso IV aiutano a scoprire la chiave

Wireless: WPA - Kismet

- Per risolvere i problemi di WEP, è stato introdotto un altro protocollo, WPA (WiFi Protected Access)
- Per quanto riguarda i difetti di WEP, WPA cerca di risolverli
- Anche WPA ha una debolezza: password brevi sono attaccabili offline con una ricerca su dizionario
- In sintesi: usare protocolli "in chiaro" su una rete wireless non è una buona idea, a prescindere dal protocollo di cifratura
- Esistono molti strumenti per "osservare" il traffico di una rete wireless e cercare di risalire alla chiave
- Come sempre, si possono usare (anche) per avere un'idea della robustezza della propria rete wireless

In pratica...

Vediamo nella pratica...
kismet

Note

- Nella realizzazione di queste slide non è stato fatto alcun male a **server reali** con bit reali: solamente **server e reti virtuali**, si prega vivamente di fare altrettanto!
- La sicurezza è molto divertente (almeno fino a quando non si viene bucati) ma pone di fronte anche a vari problemi etici. Spesso è il caso di riflettere anche su questi e non solamente sulla parte prettamente tecnica
- Molte intrusioni non vengono rilevate se non dopo molto tempo o eventualmente mai. Non sei mai stato bucato o non ti sei mai accorto di esserlo stato?

- I tool posso aiutare molto ma a fare la differenza sono comunque la preparazione e le capacità

Note e bibliografia

- Botnet. http://en.wikipedia.org/wiki/Botnet
- DoS Attacks on the Internet. http://vayner.net/dos/dos.html
- An Analysis of Fragmentation Attacks. http://www.ouah.org/fragma.html
- Ettercap. http://ettercap.sourceforge.net/
- Dsniff. http://www.monkey.org/~dugsong/dsniff/
- Ethereal. http://www.ethereal.com/
- Kismet. http://www.kismetwireless.net/
- 802.11 WEP: Concepts and Vulnerability. J. Geiger. http://www.wi-fiplanet.com/tutorials/article.php/1368661
- SSH: The Secure Shell, The Definitive Guide. http://www.wi-fiplanet.com/tutorials/article.php/1368661
- CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks. http://www.cert.org/advisories/CA-1998-01.html
- Wardriving. http://www.wardriving.com/