Attacchi - panoramica

Metodi e strumenti per la Sicurezza informatica

Claudio Telmon
claudio@telmon.org

Tecniche di attacco

- Più passaggi prima del destinatario (stepstones)
- Accesso da sistemi poco controllati
  - Botnet: reti di molti PC, ad esempio domestici
- Attraversamento di confini nazionali
- “Qui la polizia ha altro a cui pensare”

Botnet

- Reti di PC sotto il controllo di un unico “master”
  - Ormai frequenti reti di decine di migliaia
- Struttura di comando e controllo articolata
  - Per non essere semplice da riconoscere
  - Per essere efficace
  - Per rendere difficoltoso risalire al master
- Uso di varie forme di malware
  - Poco “rumoroso”

Social Engineering

- Si attacca l'utente, che spesso è uno dei punti deboli delle difese di un sistema
- E` possibile soprattutto quando la politica di sicurezza non è ben definita
- Non è possibile proteggersi con soli mezzi tecnici

Denial of Service

- Bloccare un servizio di ostacolo per la realizzazione di un altro tipo di attacco.
- Bloccare una macchina per poterne prendere il posto nelle comunicazioni con la macchina sotto attacco.
- Bloccare una macchina per causare un danno

SYN flood

- Occupa lo spazio della memoria del kernel destinata ai buffer per le connessioni semiaperte
- Permette di impedire la ricezione di pacchetti SYN e RST (Mitnick)
- Soluzioni: SYN cookies, uso di firewall
- Altre tipologie di flooding

I Distributed Denial of Service

- È un problema sempre più comune
  - Uno dei punti di contatto fra hacking e criminalità
  - Banda dell'attacco in continuo aumento
  - es. Root nameserver
- Contatti preventivi con i provider possono aiutare
  - Strumenti di riconoscimento di traffico anomalo presso l'ISP (non così comuni...)

DDoS: possibili "soluzioni"

- Egress filtering: utile ma difficile da imporre
- Marcatura random dei pacchetti
- Notifica del path dei pacchetti al destinatario con nuovi pacchetti icmp
- Problemi di complessità, particolarmente quando gli IP mittenti e gli zombie sono molti
- Strumenti attuali: packet filter "intelligenti"

TCP/IP

- Packet storms
- Difetti nello stack
  - crash del sistema
  - 100% cpu usage
  - Resource starvation
- IP fragmentation:
  - superamento dei meccanismi di filtraggio (obsoleto?)
  - usato dagli scanner, poco implementato in attacchi specifici

Packet Sniffing

- I pacchetti attraversano parti di Internet sulle quali non si ha alcun controllo
- Non è possibile sapere se un pacchetto è stato letto durante il percorso
- Non è in generale possibile prevedere il percorso che seguiranno i pacchetti
- Il percorso spesso attraversa i confini nazionali

Switch e VLAN

- Sono strumenti nati per gestire le reti e ottimizzare l’uso delle risorse
- Esistono attacchi efficaci contro molti modelli di switch e contro molte implementazioni di vlan
- Es: si inonda lo switch di pacchetti con MAC address falsi, fino a riempirne la cache...
- Prodotti sempre più all'altezza...

Redirezione dei pacchetti

- I protocolli di routing di Internet prevedono una grande facilità nella ridirezione dei pacchetti
- E` possibile “estrarre” pacchetti da un path in modo trasparente
- I protocolli di routing prevedono un’autenticazione migliore fra le parti
  - Problemi: compromissione dei nodi, errata configurazione dei meccanismi di virtualizzazione...
- Problema molto ridotto, più comune il pharming

Man in the Middle

- Consiste nel modificare i pacchetti in transito nel nodo in modo trasparente
- Permette di impersonare completamente una delle parti
- Permette di assumere il controllo di una connessione dopo l'autenticazione iniziale

Connection hijacking

- La connessione è composta da più scambi di messaggi
- L’autenticazione avviene durante il primo scambio
- I messaggi successivi non vengono autenticati
- Quindi la connessione viene attaccata dopo l’autenticazione iniziale
- A questo dovrebbe servire SSL...

Phishing

- Si convince l'utente ad autenticarsi ad un sito fasullo
  - Per sottrarre le credenziali
  - Per effettuare attacchi Man in the Middle
- Soluzioni?
  - Uso corretto di SSL: vedi frame di autenticazione
  - Rapporti chiari con gli utenti
  - One time password?
  - Rilevazione nel browser?

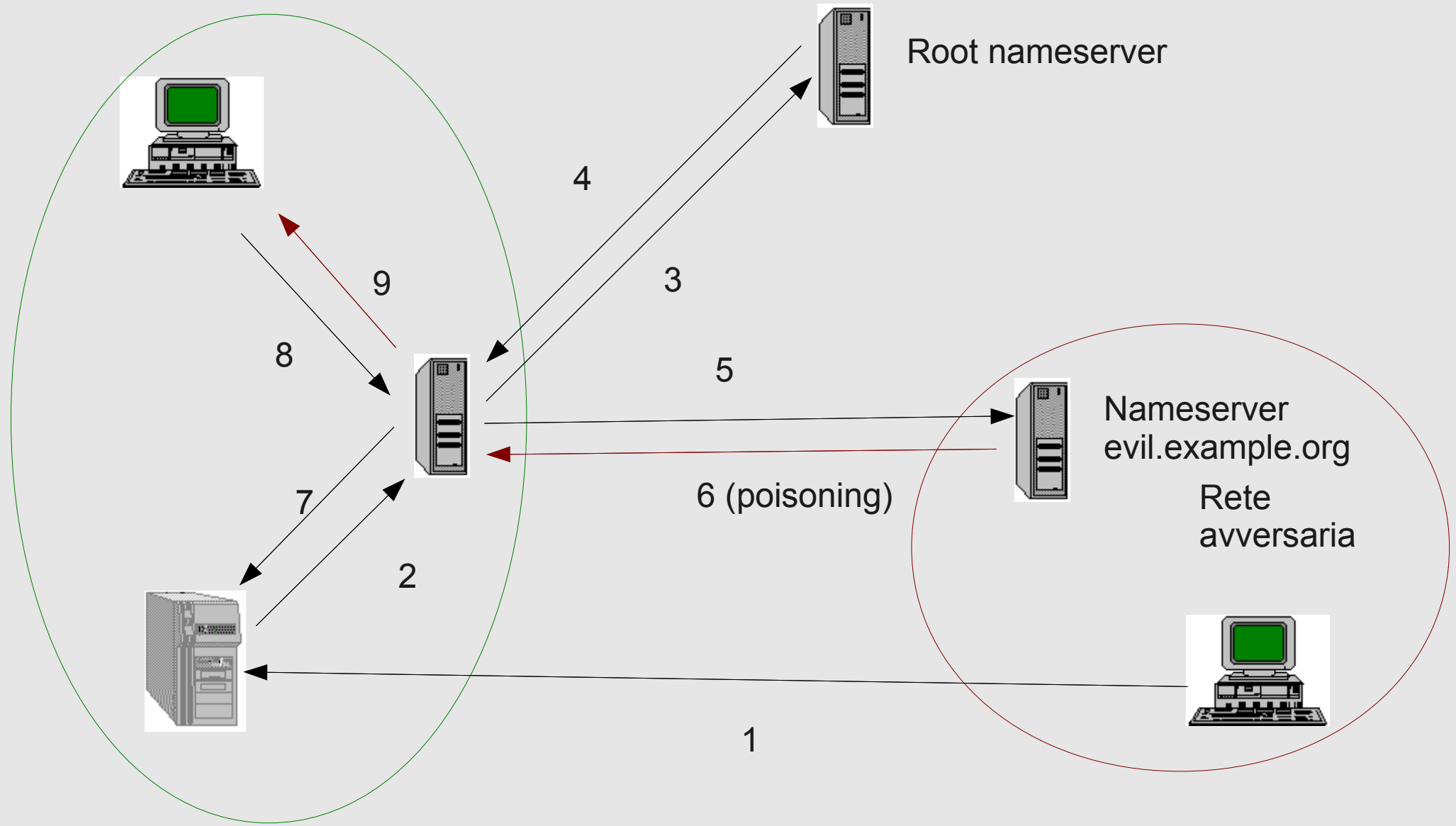
Replay attack

- Consiste nel ripetere una sequenza di operazioni corrispondente a una sessione appena conclusa
- Non è necessario comprendere il significato di ciò che si sta facendo

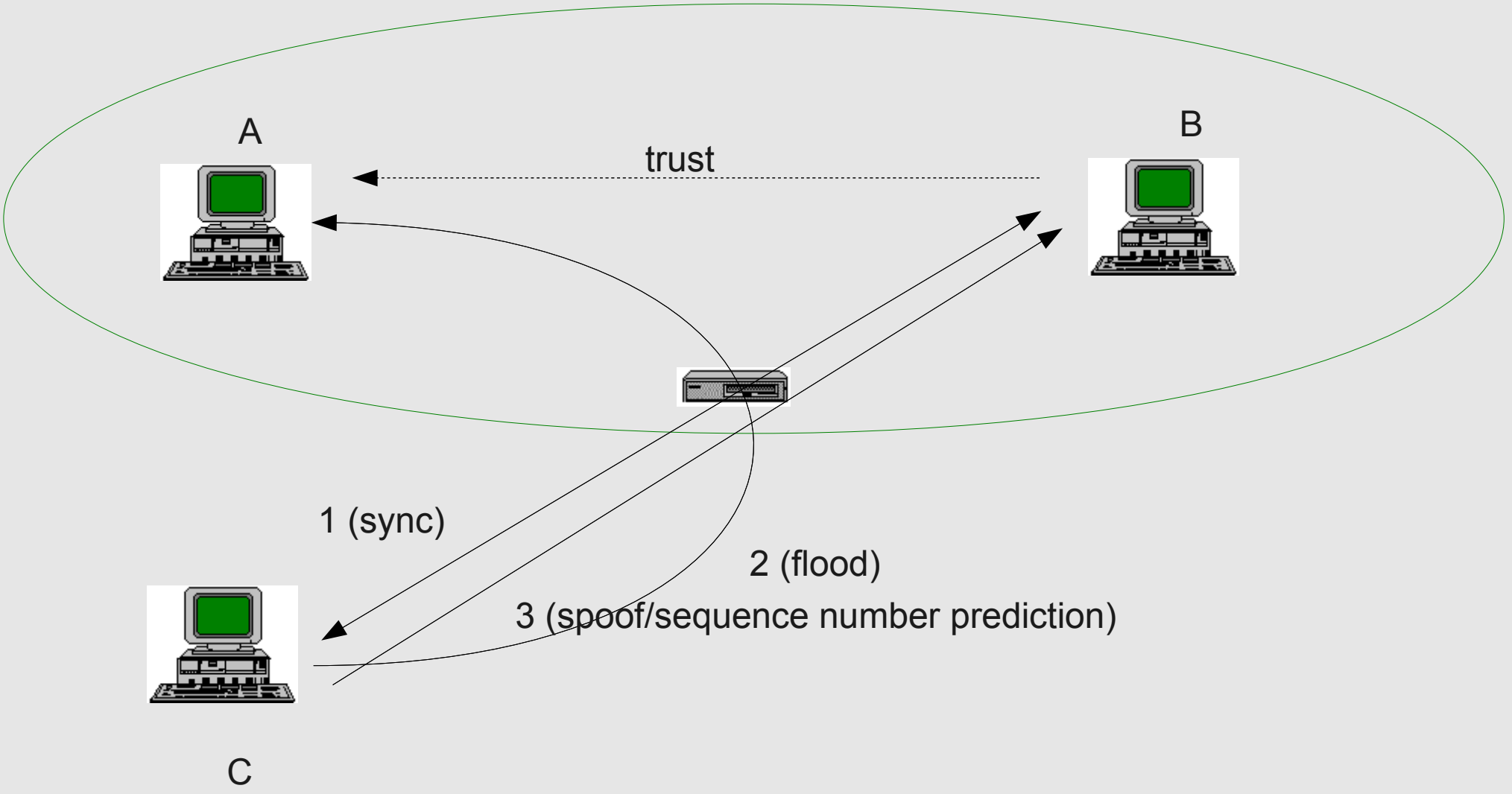
Il DNS

- Le risposte a richieste DNS sono sostanzialmente non autenticate
- È possibile aggiungere informazioni false a query legittime (cache corruption)
- I meccanismi di log generalmente prevedono la risoluzione dei nomi...
- Il double reverse lookup offre qualche protezione in più
- DNSSEC?
- Pharming

DNS cache poisoning



TCP blind spoofing



TCP blind spoonfing

- Attacco che ha reso famoso Mitnick
- B ha una relazione di trust con B (r* utilities)
- C si sincronizza con B, in modo da poter prevedere l'ISN
- C pratica un SYN flood contro A, bloccandone le risposte
- C si connette a B con mittente A: non vede le risposte, ma prevede ISN; A non genera RST
- C invia “al buio” un comando

  echo “+ +” >> /root/.rhosts
- Difficilmente praticabile, ora qualsiasi firewall lo blocca

Vulnerabilità dei servizi

Password Guessing e simili

- Le password sono spesso scelte in modo prevedibile
- Con gli strumenti attuali è possibile provare alcuni milioni di password in poche ore
- Vi sono comunque dei limiti intrinseci alle capacità mnemoniche umane

Difetti del software

- Ogni programma ha dei difetti
- Molti di questi difetti possono essere sfruttati per eseguire azioni non previste
- I difetti in programmi critici per la sicurezza permettono di eseguire azioni critiche per la sicurezza

Difetti nei protocolli

- Molti protocolli sono stati progettati senza considerare la sicurezza
  - risalgono a parecchi anni fa
  - derivano da un'ottica host
  - sono progettati "in proprio" senza le competenze necessarie
  - "La sicurezza verrà aggiunta dopo"

Difetti realizzativi

- Pochi programmatori sanno come evitare i trabocchetti
- Ci si aspetta che la controparte (client/server) si comporti correttamente
- Le rifiniture andranno nella versione definitiva
- Semplici errori

Difetti di configurazione

- Una configurazione sicura è più scomoda da usare
- La configurazione di default spesso serve a far funzionare tutto subito
- La scelta fra le opzioni può non essere chiara all'utente/sistemista
- Configurazioni "temporanee"
- Errori

I browser

- La qualità aumenta
- Le funzionalità di più
  - Componenti
  - Applet e javascript
- Le operazioni devono essere trasparenti….
- Integrano funzionalità diverse, anche locali
  - la distinzione fra Internet e la rete locale è sempre più sfumata
  - Spesso le “cose interessanti” sono comunque tutte nel browser

Input validation

- Non bisogna fare assunzioni su cosa ci può arrivare dalla rete
  - può arrivare di tutto
  - dobbiamo verificare che corrisponda alla sintassi desiderata
  - l'attaccante non usa il nostro client, genera il traffico che vuole
- Errori di questo tipo (realizzativi o di progettazione) sono alla base della maggior parte dei problemi

Interazione con l'ambiente

- Le variabili d'ambiente possono influire sul comportamento
  - PATH
  - LD_PATH
- Alcune funzioni hanno un comportamento poco prevedibile
  - system()

Virus, worm e trojan horse

- Virus: quando eseguito, copia il proprio codice su altri programmi
- Worm: quando eseguito, installa copie del proprio codice su altri computer in rete
- Trojan Horse: ha una funzione evidente e una occulta

Trojan Horse

- Sono programmi che hanno:
  - una funzione evidente (quella per cui li usa la vittima)
  - una funzione nascosta (quella per cui sono stati creati)
- Possono essere creati ad hoc o modifiche di programmi esistenti
- Per le botnet sono utilizzati strumenti sofisticati

Cross site scripting

- Un sito presenta componenti che derivano da contesti diversi
  - Webmail
  - Motori di ricerca
  - Input (es. nel link) da parte dell'utente
- Il codice (javascript) contenuto viene presentato nel contesto del sito (violando la “same origin policy”)
  - Il browser gli concede l'accesso al contesto, es. cookies
  - Il codice invia le informazioni ad un altro sito, es. in un link
- Anche con javascript lato client

SQL injection

"SELECT * FROM users WHERE name = '" + userName + "';"

- Se userName è

  a' or 't'='t

- Diventa

  SELECT * FROM users WHERE name = 'a' OR 't'='t';

- Vera per ogni record
- Protezione: “escape” dei caratteri
  - Spesso troviamo il filtraggio, es. delle accentate ...
- Il caso generale è l'interpretazione dei caratteri speciali, es. separatori