Tecniche di hacking

Franco Sivilli <*fsivilli@unich.it*>

Corso di informatica

Obiettivi

Conoscere:

- **Le vulnerabilità delle reti IP**
- **Le metodologie classiche di attacco**
- **Gli strumenti in dettaglio**
  - I fase: Recupero di informazioni sulla rete obiettivo dell'attacco
  - II fase: information gathering e identificazione dei componenti "trusted" della rete obiettivo
  - III Fase: attacco!
  - IV Fase: cancellazione delle tracce
  - V Fase: espansione dell'attacco
- **La teoria degli attacchi alle reti**
  - **Denial of service**
  - **Spoofing**
  - **Sniffing**
  - **highjaking**
- **Dove reperire documentazione / statistiche**

Vulnerabilità delle reti IP

Obiettivi

- Istituti finanziari e banche - frodi
- Service Provider - customer database e intercettazioni
- Pubbliche amministrazioni - sfida, frodi
- Agenzie governative e della difesa - sfida, spionaggio
- Aziende farmaceutiche - spionaggio
- Aziende multinazionali - spionaggio

- (fonte Network. Security Solutions ltd, http://www.ns2.co.uk)

Il concetto di vulnerabilità

Definizione: crepa in una applicazione o in un processo a fronte di situazioni inaspettate.

Attraverso una vulnerabilità gli hacker possono avere accesso a informazioni ed utilizzarle contro di noi, ad esempio per produrre un crash dei nostri Sistemi o svolgere attività di ***spyware*** (vendere le ns informazioni a chi le cerca).

Il 99% delle intrusioni risultano fatte sulla base di vulnerabilità conosciute o errori di configurazione.

Source: Cert, Carnegie Mellon University

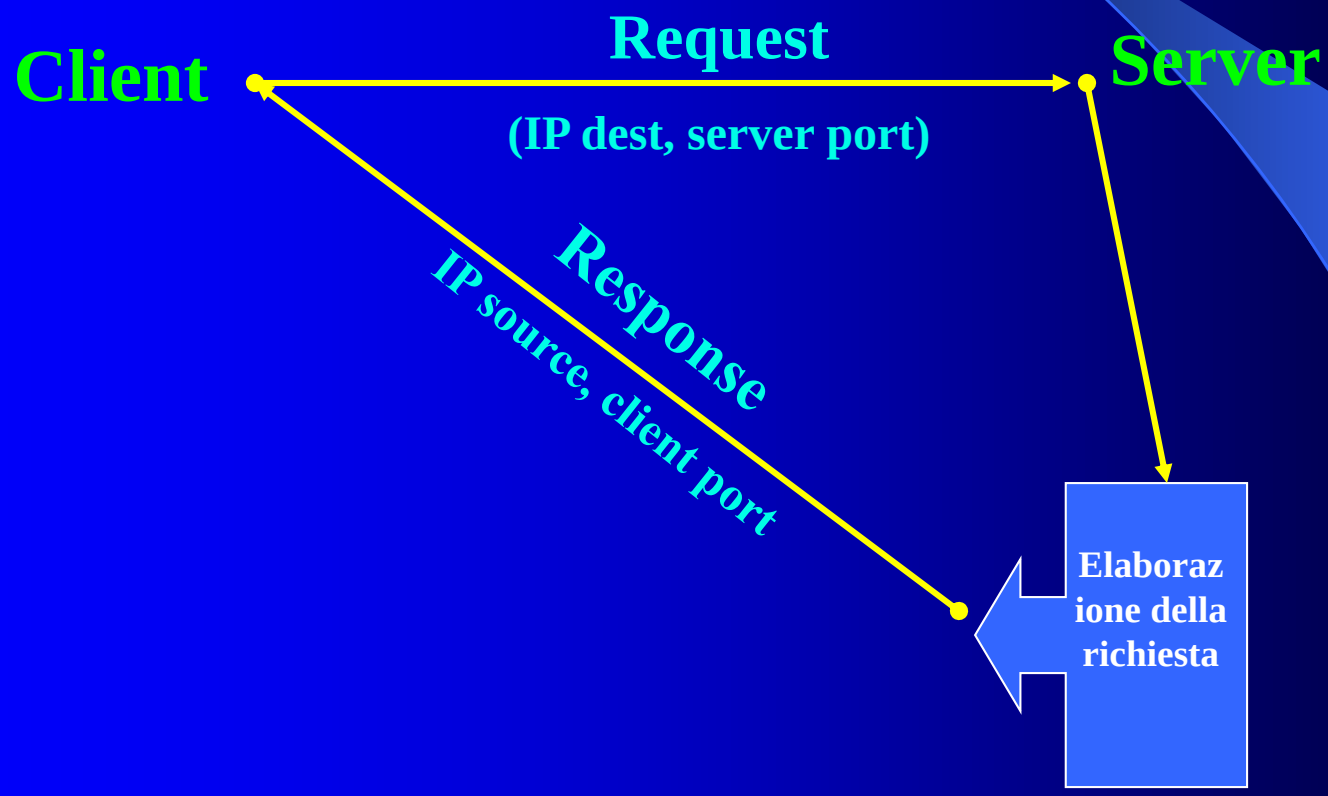
Vulnerabilità

- Le caratteristiche intrinseche di Internet che rendono possibili la grande maggioranza degli attacchi all'esterno: il modello client-server e la tecnologia di trasmissione del tipo "commutazione di pacchetto".

Vulnerabilità delle reti: il modello client-server

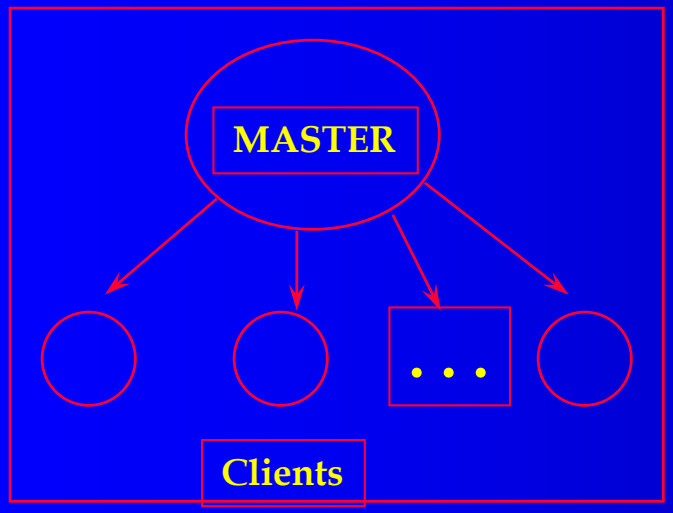
- *Server* : qualsiasi programma che offre un servizio utilizzabile tramite una rete. Un server accetta richieste che gli arrivano via rete, fornisce il servizio e restituisce il risultato al richiedente. Ogni servizio è associato ad una *porta* diversa.
- *Client* : e' un programma che invia una richiesta ad un server, esplicitando l'indirizzo destinatario e la porta associata al servizio, ed attende da questi una risposta.

Il modello client-server



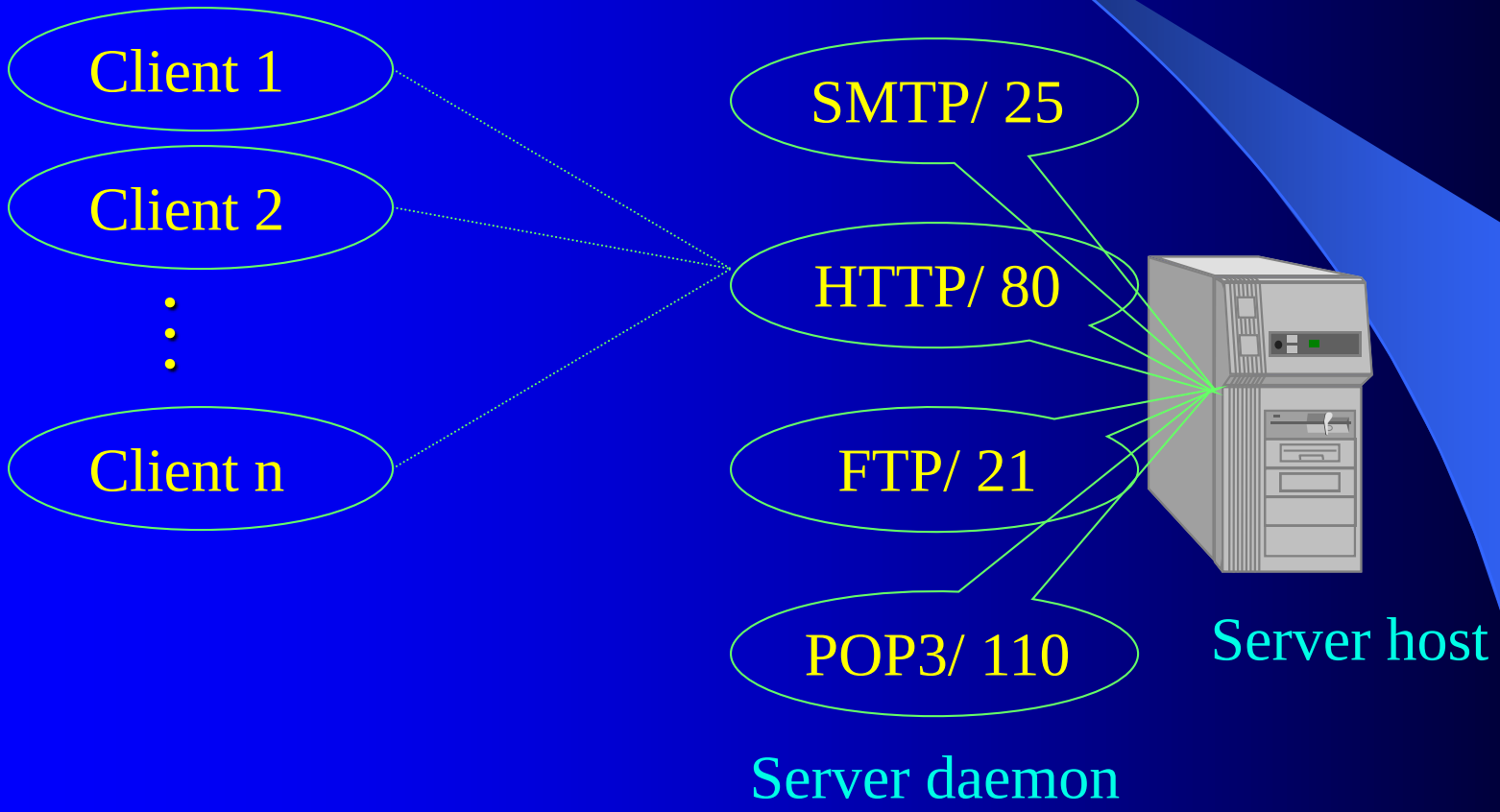
Il modello client-server - 2

Un server deve essere in grado di processare più richieste concorrenti (es. più file transfer)



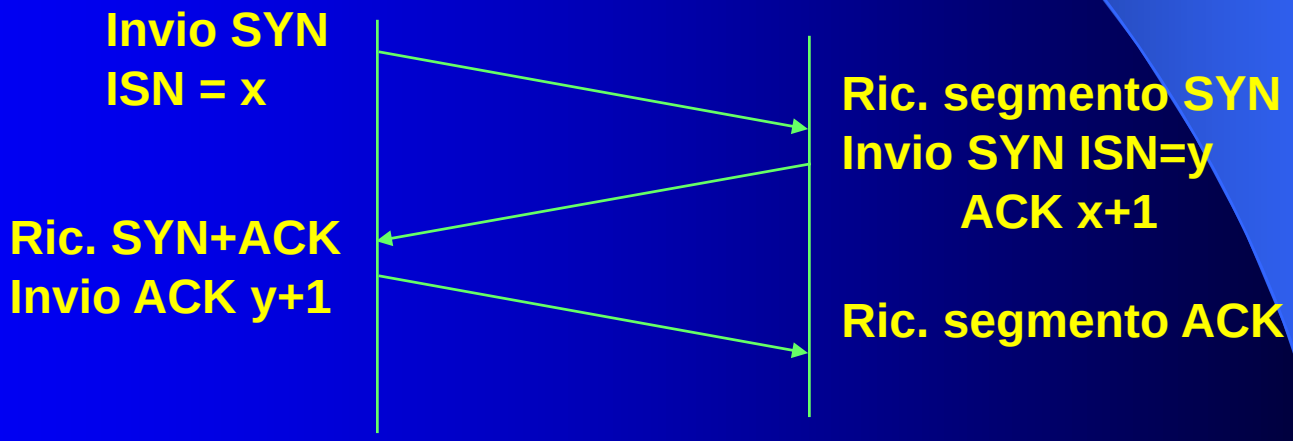
Generalmente la struttura di un server e' quella in figura.
Il master e' incaricato di accettare le richieste svolgendo anche compiti di controllo sugli accessi.
Accettata una richiesta si " sdoppia " generando uno slave che si occuperà di processare la richiesta.
Il master nel frattempo si e' rimesso in attesa.

Modello generale



Connection estabilishment protocol

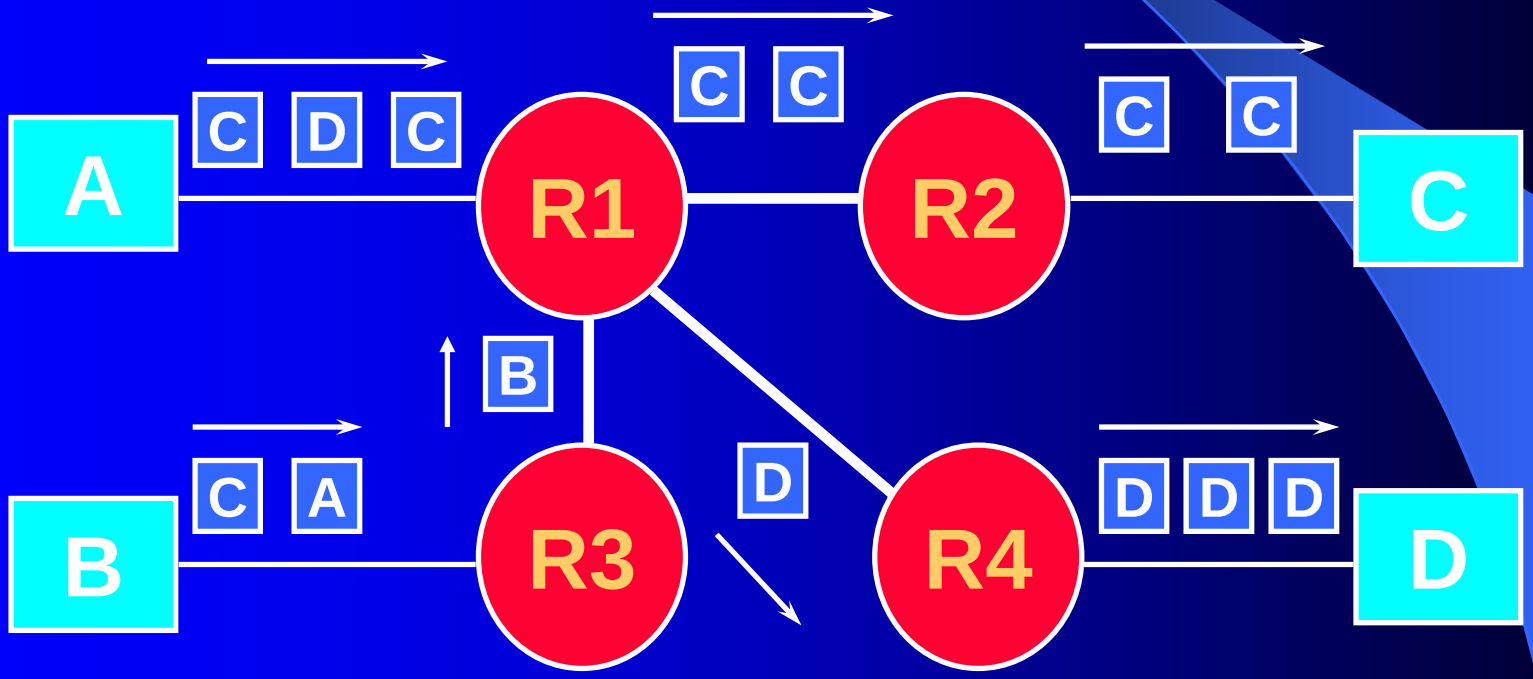
Connessione TCP fra client e server three-way handshake



Sicurezza dei server

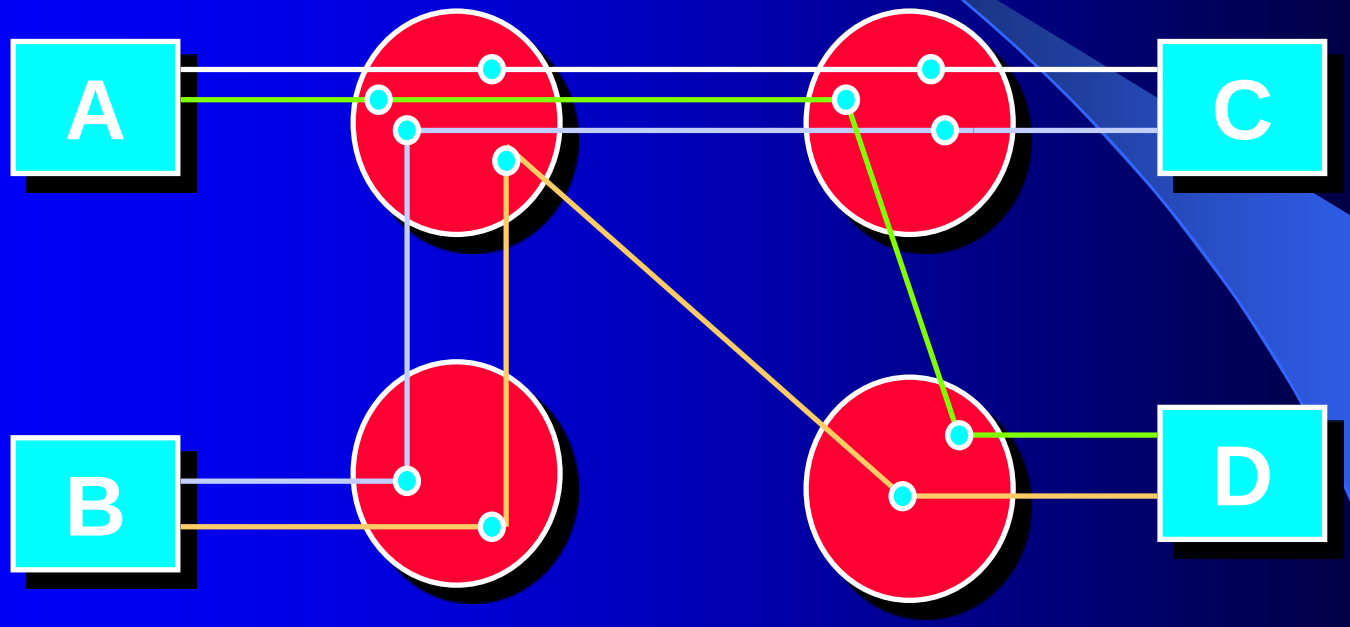
- *I server ricoprono un ruolo primario nella sicurezza delle reti. Una volta ottenuto un accesso non autorizzato a un server, il resto della rete è facilmente attaccabile.*

Vulnerabilità delle reti: la trasmissione a commutazione di pacchetto



L'informazione è raggruppata in pacchetti.

Commutazione di Circuito



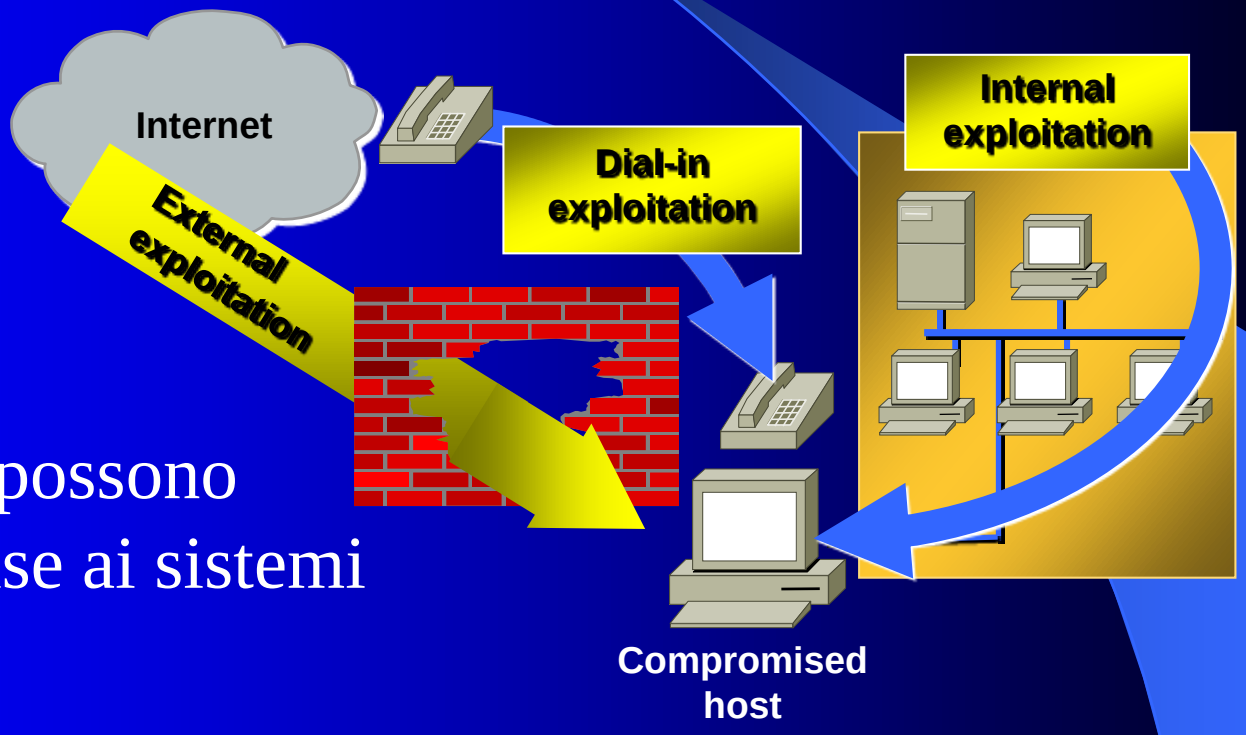
I commutatori creano dei circuiti punto-punto

Commutazione di pacchetto

- Trasmissioni contemporanee
- Non c’è impegno di linea
- Il cammino viene ricalcolato ogni volta dai computer reinstradatori [***Router***] (e quindi può seguire strade diverse
- I ritardi sono un fattore normale, intrinseco in questa tecnologia di trasporto.

Metodologie classiche di attacco alle reti informatiche

Tipologie di attacco



- Gli attacchi possono variare in base ai sistemi target.

Gli hacker

- Maschio, età fra 16 e 25 anni, molti interessati a forzare le protezioni per aumentare il proprio skill o per poter disporre di ulteriori risorse di rete. Hanno molto tempo a disposizione e possono rendere i loro attacchi diluiti nel tempo e, soprattutto, persistenti, concentrando gli interventi nelle ore notturne o del fine settimana.
- (fonte: Front Line Infornmation Security Team – FIST)

Classificazione hacker

Hacker comune: è paragonato all'artista di graffiti. Ha nececcità di acquisire supremazia in un gruppo.

Hacker tecnologico: contribuisce, con le sue sfide a sostenere lo sviluppo Hw/Sw

Hacker politico: è in genere un attivista che ha un messaggio che vuole sia ascoltato

Hacker economico: spionaggio industriale, frodi di carte di credito per puro profitto personale.

Servizi di una rete

- Servizi generalmente attivi in una network classica
  - Web aziendale (in casa o in hosting dal proprio provider)
  - E.Mail per le comunicazioni globali
  - Rete locale per l'accesso ad Internet
  - Accesso remoto
  - DNS

Attacchi dall'esterno

- L'attacco dall'esterno rappresenta la parte difficile, una volta entrati, il resto della rete è facilmente prendibile

Tipologia degli attacchi

- **Bisogna distinguere i problemi di insicurezza delle reti in due grandi classi:**
- 1) Debolezze strutturali del protocollo TCP/IP
- 2) Mancanza di correttezza delle implementazioni dei programmi per la gestione dei servizi
- *Nella seconda classe si concentrano la maggioranza degli attacchi*

Profilo delle strategie tipiche

- Azioni di scan della rete
  - Per individuare reti o porzioni di reti che possono essere vulnerabili agli attacchi
  - Per individuare i singoli host e le loro caratteristiche: sistema operativo, porte TCP aperte
- Azione intrusiva
  - acquisizione dei diritti di super-utente (root)
  - Installazione di una backdoor
  - Patch al sistema operativo per nascondere le successive intrusioni

Profilo delle strategie tipiche - 2

- Azione protettiva
  - patch al sistema operativo per rendere inaccessibile il sistema ad altri hacker. (gli hacker sono i maggiori esperti di sicurezza!)
  - installazione di backdoor
- Azione intercettiva
  - in base all'obiettivo:
    - Sniffer
    - password cracker
    - Back Orifice
    - ……...

Metodologie di attacco: gli strumenti in dettaglio

I fase: Recupero di informazioni sulla rete obiettivo dell'attacco

Visibilità esterna della rete.

- Interrogazioni al nameserver
- Web page
- Ftp repository
- Interrogazioni al sistema di posta

L'hacker ottiene una lista degli host e un piano delle relazioni esistenti fra questi

Recupero informazioni sugli host

- Sistema Operativo e release corrente del software installato
  - connessioni alle porte con programmi reperibili su internet
  - Es.: queso
    - rpcinfo,snmp,telnet,SendMail version, download binaries from the public-ftp (analyzing its format)
    - *http://www.apostols.org/projectz/queso/*

Macchine definite “trusted”

- Una macchina si definisce “trusted” quando, essendo considerata affidabile, gode diritti particolari di accesso, non autenticato, su altre macchine della rete
- Generalmente si assegnano questi diritti a server o a macchine utilizzate per l’amministrazione allo scopo di agevolare le operazioni di manutenzione e di accesso ai servizi

II fase: information gathering e identificazione dei componenti "*trusted*" della rete obiettivo

Macchine di amministrazione, server, router

Identificazione delle vulnerabilità più semplici

- spazio disco condivisibile lasciato senza controllo degli accessi
- finger per identificare gli utenti che si collegano più spesso

Identificazione delle vulnerabilità più complesse

- Uso di strumenti per verificare i servizi attivi
- *Portscanning*
  - Azione di scansione remota delle porte note per rilevare l'elenco dei servizi attivi su una certa macchina
  - si manda un pacchetto particolare "costringendo" la macchina target a una determinata risposta, da cui si possono trarre le informazioni del caso

Identificazione delle vulnerabilità più complesse -2

- Uso di suite reperibili sulla rete per l'identificazione automatica della vulnerabilità e il reperimento del tool di attacco
- Ricerca sui database di Internet

I tool più usati per la rilevazione automatica delle vulnerabilità

- ADMhack
  - la guida completa per tutti i tipi di hacker
  - *ftp://ADM.isp.at/ADM/*
- Mscan
  - Nessuna home page: utilizzare un potente mezzo per il rintracciamento del software
  - *http://ftpsearch.lycos.com/?form=medium*
- Nmap
  - l'arte del portscanning
  - *http://www.dhp.com/~fyodor/nmap*
- Nessus *http://www.nessus.org*
- Satan *http://www.fish.com/~zen/satan/satan.html*

III Fase: attacco!

- Durante le ore di chiusura (l'attacco è normalmente rilevabile nel momento in cui è in corso) preferiti i trusted external host (mailserver e nameserver), che possono essere utilizzati da "ponte", avendo accessibilità a brevi segmenti di rete interna
- Viene sfruttata la porta di accesso rilevata, ed utilizzata per l'installazione di "*backdoor*" (porte nascoste per consentire un accesso non autorizzato e non rilevabile).

Attacco!

- Vengono modificati i comandi stessi del sistema operativo, soprattutto quelli che servono per l'accesso al sistema e per il controllo di processi ed utenti
  - data, permessi e in molti casi anche lo stesso filesize

IV Fase: cancellazione delle tracce

- pulizia dei log, cioè della “scatola nera di sistema” dove viene registrata tutta l’attività.
- Installazione di software preconfezionati per la modifica di un sistema operativo.
- Operazione rapida, di solito non rilevabile.

V Fase: espansione dell'attacco

- Dipende dal reale obiettivo:
  - installazione backdoor su altri sistemi
  - password cracker
  - back orifice per il controllo remoto dei sistemi
  - distruzione e cancellazione di files
  - Denial of Service

Sniffer

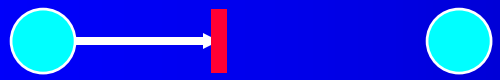
- Software che consentono sofisticate intercettazioni di tutto il traffico dei dati sulla rete.
- Producono un enorme mole di dati, ma le ultime versioni sono in grado di isolare le informazioni sensibili e i dati di interesse da tutto il resto.

Rilevamento

- Molti tool che si spacciano per rilevatori di BO, installano invece il virus
- *http://www.symantec.com*
- da una finestra DOS: *netstat -an* se il risultato è *UDP 0.0.0.0:31337 *.** un server BO è in attesa di comandi dall'hacker
- Prevenzione con anti-virus
- *http://www.mcafee.com*

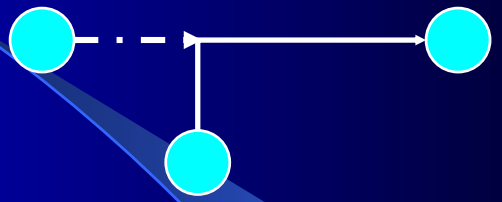
Teoria degli attacchi alle reti

Tipologie



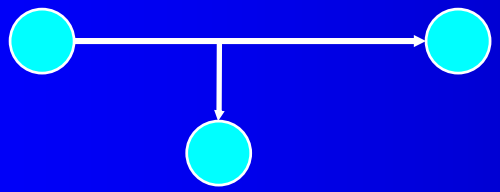
Interruzione

(DoS)



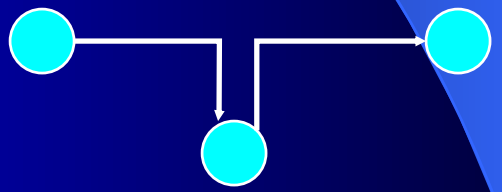
Fabbricazione

(spoofing)



Intercettazione

(sniffing)



Modifica

(highjacking)

DoS (Denial of Service)

- Ovvero le azioni finalizzate ad impedire il normale svolgimento di un servizio nella macchina che viene attaccata, saturando le capacità di comunicazione che una organizzazione ha a disposizione. Se proviene da molti computer (agenti) prende il nome di DDOS (distributed DOS)
- Quasi tutti i tipi di DoS non sfruttano dei *bugs* software ma piuttosto una caratteristica intrinseca del protocollo

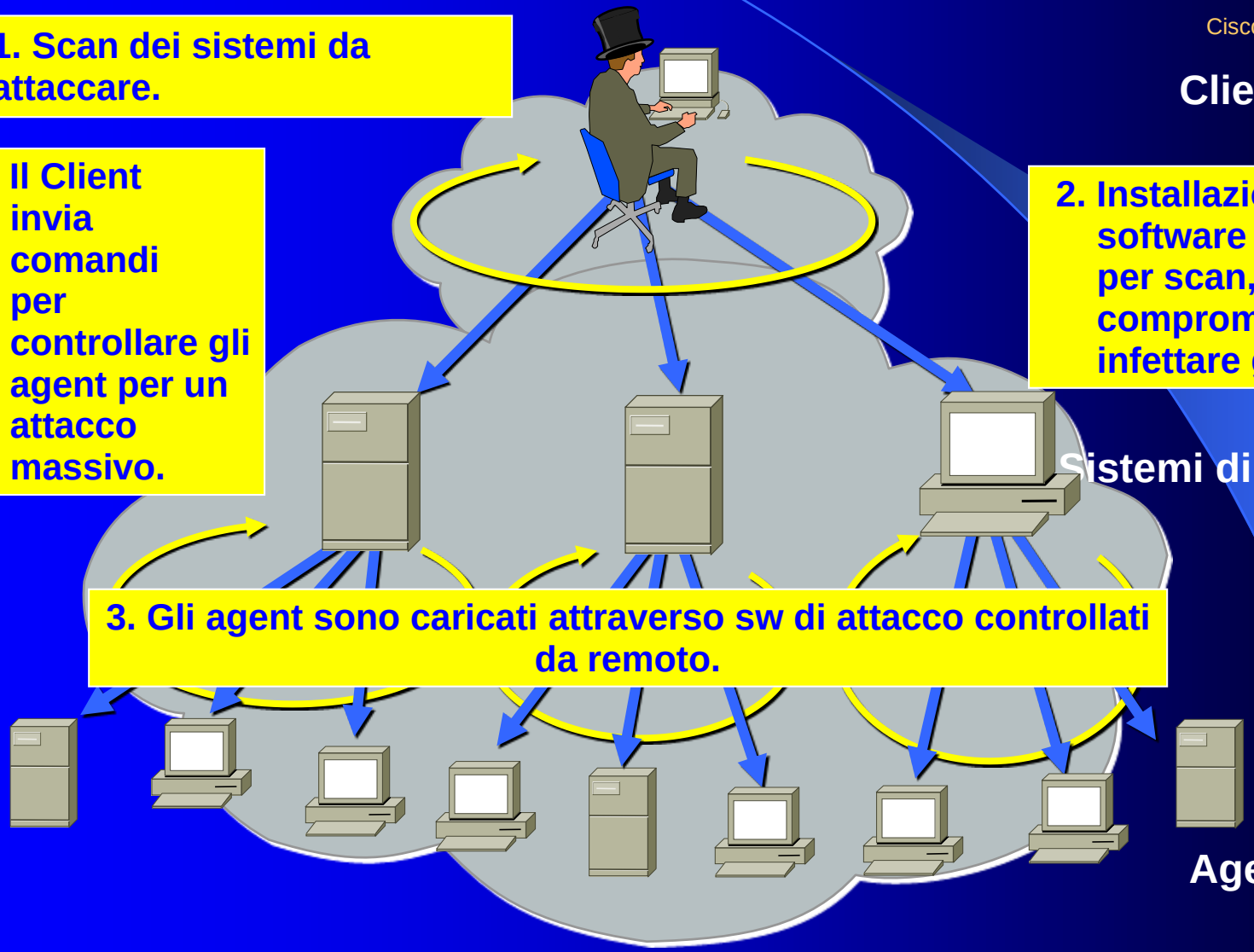
Esempio di DDOS

1. Scan dei sistemi da attaccare.

2. Installazione del software per scan, compromettere e infettare gli agent.

3. Gli agent sono caricati attraverso sw di attacco controllati da remoto.

4. Il Client invia comandi per controllare gli agent per un attacco massivo.



Client

Sistemi di controllo

Agent

IP spoofing

- Per ottenere l'accesso, l'intrusore crea dei pacchetti con il source address IP "*spoofed*" cioè alterato, mascherandosi per un altro. Questo fa sì che applicazioni che usano l'autenticazione basata sul controllo dell'indirizzo IP concedano l'accesso a persone e host non autorizzati. E' possibile bypassare anche firewall i cui filtri non sono stati disegnati per fermare pacchetti entranti con un source address locale. E' possibile compiere degli attacchi anche senza ricevere i pacchetti di risposta da parte del target host

Altri tipi di spoof

- Web spoofing
  - altera il percorso reale di collegamento a un sito
- Mail spoofing
  - spedizione di mail con l'indirizzo alterato
  - spam
- IRC spoofing
  - dialogo in chat line con false identità o alterando le frasi che due utenti si stanno scambiando

Come prevenire lo spoofing

- Access control— Il metodo più comune per prevenire l'IP spoofing è configurare bene il controllo degli accessi.
- Additional authentication che non usa autenticazione basata su IP come :
  - Crittografia (recommandata)
  - Strong, two-factor, one-time passwords

Sniffing

- intercettazione ed ascolto del traffico, inserendo un apposito programma sulla rete locale
- intercettazione e modifica del flusso, costringendolo a “transitare” su una macchine, in cui è installato uno sniffer

Sniffing applicato alle reti Wi-Fi:wardriving

Inserimento illecito in una rete wireless sfruttando la trasmissione in chiaro del Mac-address tra Nic e Access Point per sfruttare la banda (ad es. per navigare gratis ad alta velocità → è stata vittima Microsoft durante lo SMAU 2002)

Come prevenire lo sniffing

- Authentication—è raccomandata la strong authentication, come le one-time passwords.
- Switched infrastructure —Adottare una rete basata su switch per individuare l'uso di packet sniffers.
- Antisniffer tools.
- Crittografia.

HighJacking

- il controllo di una connessione viene preso da un attacker dopo che la fase di autenticazione è già stata passata. Tipiche modalità l'uso dell'ICMP o del RIP.
- inserimento di stream di dati non presenti all'origine
- i backorifice

Attacchi alle password

- Gli hackers possono realizzare questo tipo di attacco usando diversi metodi:
  - Attacchi a forza bruta
  - Trojans
  - IP spoofing
  - Packet sniffers

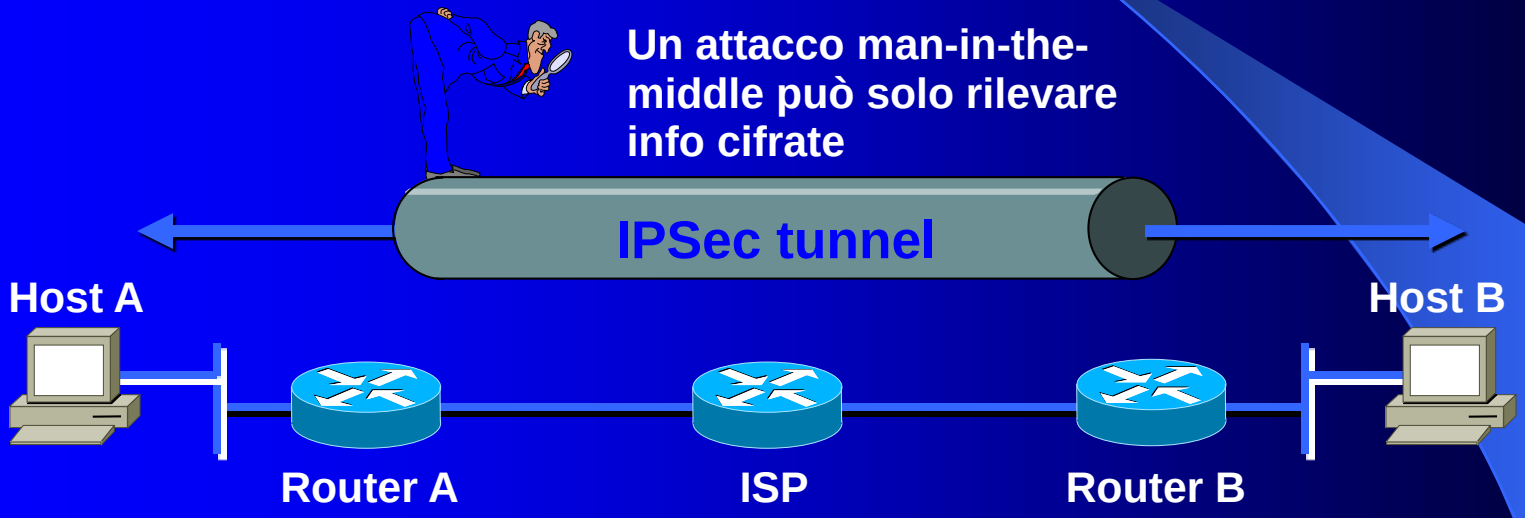
Come prevenire l'attacco alle password

- Non consentire l'uso della stessa password su più sistemi.
- Disabilitare gli account dopo un certo numero di tentativi di login non andati a buon fine.
- Non usare come password parole esistenti.
- Usare "strong" passwords. Le strong passwords sono lunghe al minimo 8 caratteri, contengono caratteri maiuscoli e minuscoli, numeri e caratteri speciali.

Attacchi man-in-the-middle

- Un attacco man-in-the-middle richiede che l'hacker abbia accesso ai pacchetti che attraversano la rete.
- Un attacco man-in-the-middle è implementato usando:
  - Network packet sniffers
  - Protocolli di routing e trasporto
- I possibili usi degli attacchi man-in-the-middle sono:
  - Furto di informazioni
  - Analisi del traffico
  - DoS
  - Alterazione dei dati trasmessi
  - Introduzione di nuove informazioni nelle sessioni di rete

Come prevenire gli attacchi man-in-the-middle



Gli attacchi man-in-the-middle si possono prevenire attraverso l'uso della crittografia

Fine

fsivilli@unich.it