IENA

Un modello alternativo per la rivelazione delle intrusioni in una rete locale.

OutLine.

L’ odierna crescita di servizi distribuiti ha generato una vera e propria problematica nel settore informatico; se fino ad oggi le principali minacce alla sicurezza venivano dall’ infrastruttura di rete e dai S.O. la diffusione delle applicazioni Web, la condivisione di risorse, la possibilità di software auto aggiornanti, la nascita di pagine dinamiche, di webServices e la realizzazione di script client-side hanno creato nuovi pericolosi obiettivi.

Tipologie di attacco.

- *Information Gatering* (raccolta informazioni)
- *Know Vulnerability* (attacco alle applicazioni)
- *Cookie poisoning* (avvelenamento delle cookie)
- *SQL Injection* (attacco al data base)
- *Brute Force* (attacco di password)
- *Cross-Site scripting* (attacco all' utente)
- *Session Fixation* (cambio di sessioni)
- *Denial of Service* (negazione di servizio)
- *Man In The Middle* (ridirezione di traffico)

Tecniche di difesa.

- Progettare una rete solida e ben strutturata.
- Installazione di *Firewall*
- Installazione di *Intrusion Detection System*
- Installazione di *Intrusion Prevention System*
- Tecniche *Forensi* per il recovery di dati
- Monitoring di *Arp Request.*
- **Utilizzo di validi modelli per *l' aggiornameto* "della rete"**

Modello ICT Attuale:

Visione.

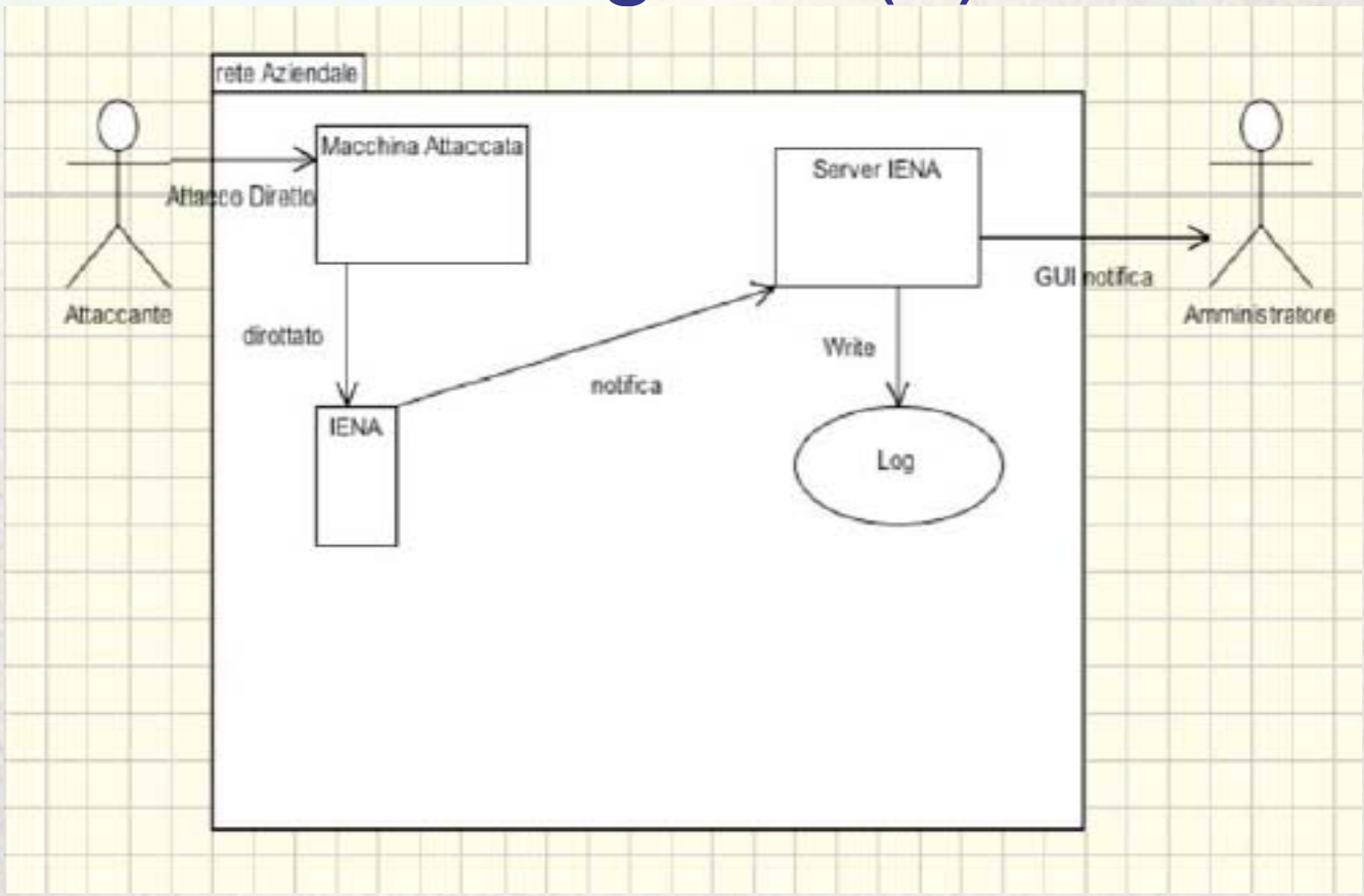
- Deve esistere un modello che elimina (o che abbassa) il livello di complessità del modello attuale.
- Lo scopo del progetto IENA consiste nel rivedere la logica del paradigma attacco/difesa degli odierni sistemi di sicurezza, presentando un modello che trova il suo fondamento in un approccio opposto a quello fino ad ora adottato nelle politiche basate sul principio di “chiusura”.

Brevi sul Progetto (1).

- Introdurre IENA in un host, significa ingannare l'attaccante.

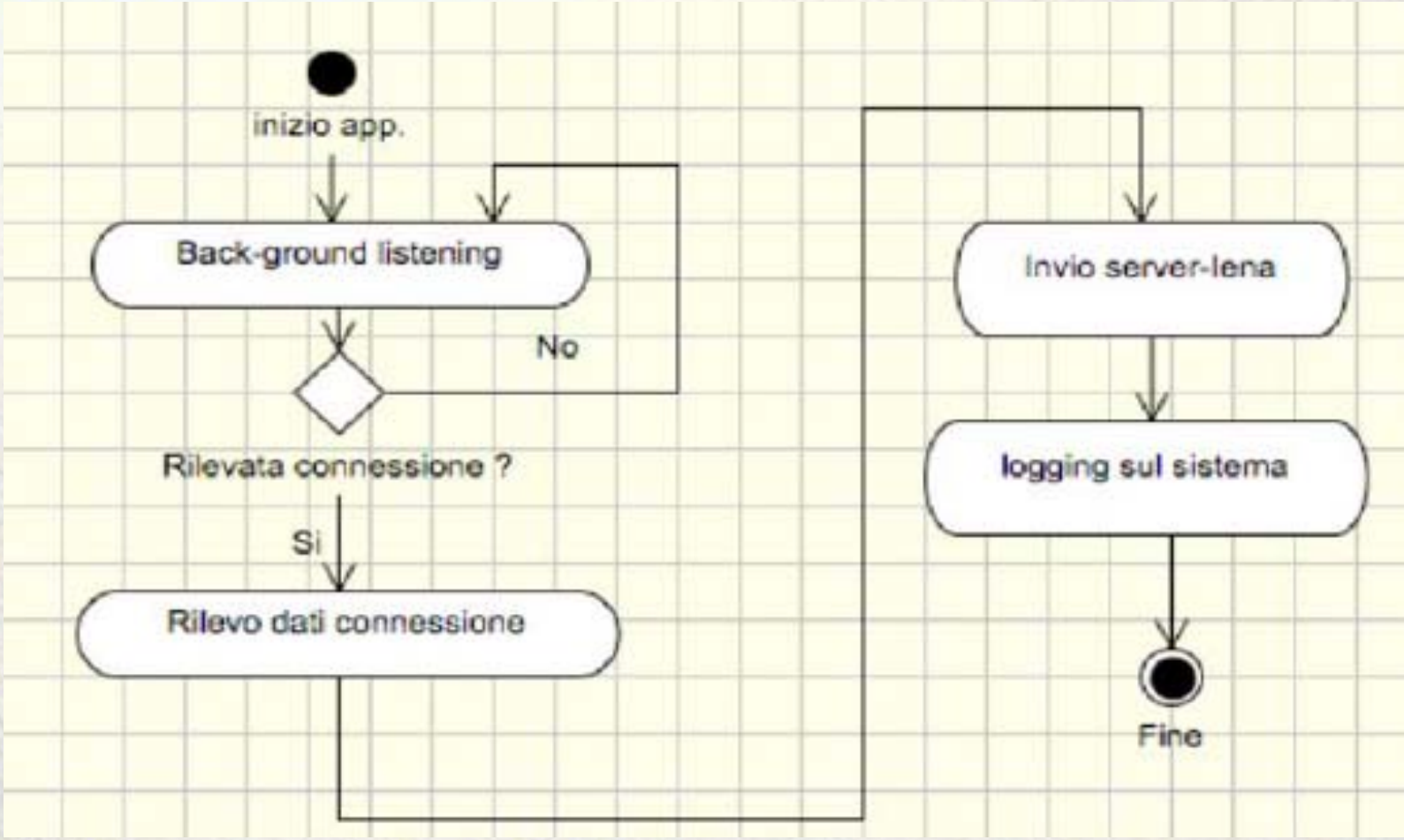
•La IENA non vuole simulare un falso servizio ma si pone in ascolto verso la rete esterna avvisando l'amministratore di rete appena capta qualche segnale "fuori norma".

Brevi sul Progetto (2).



Behavioural Diagram.

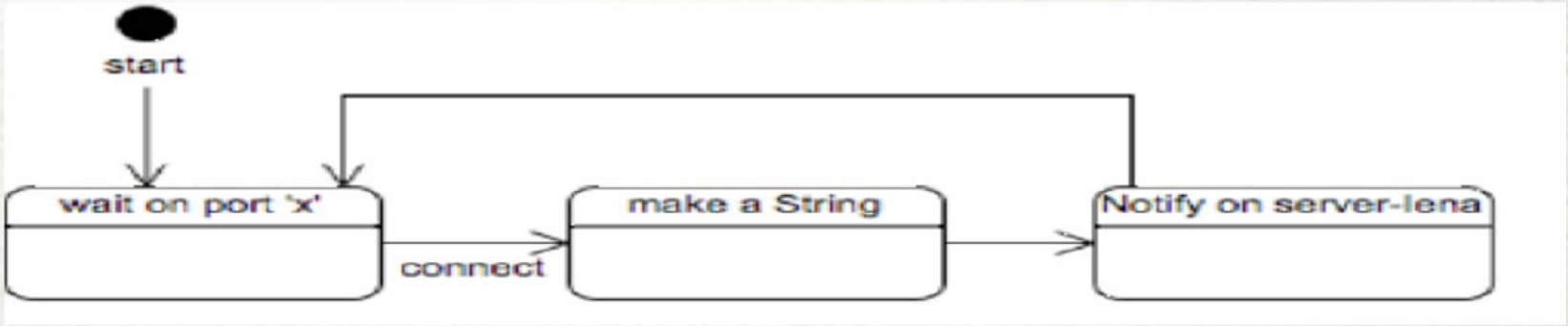
Brevi sul Progetto (3).



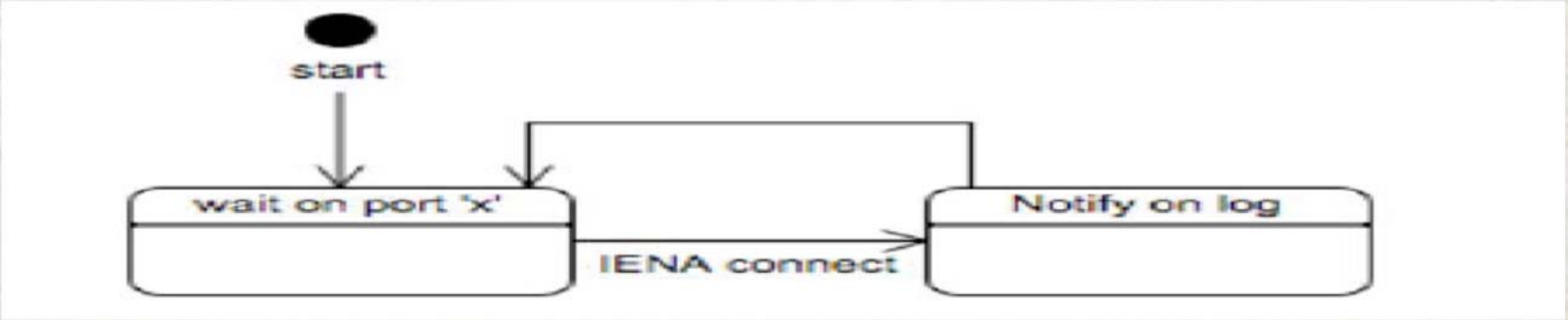
Activity Diagram

Brevi sul Progetto (4).

Comportamento Client IENA



Comportamento Server IENA



Sistemi di Notifica

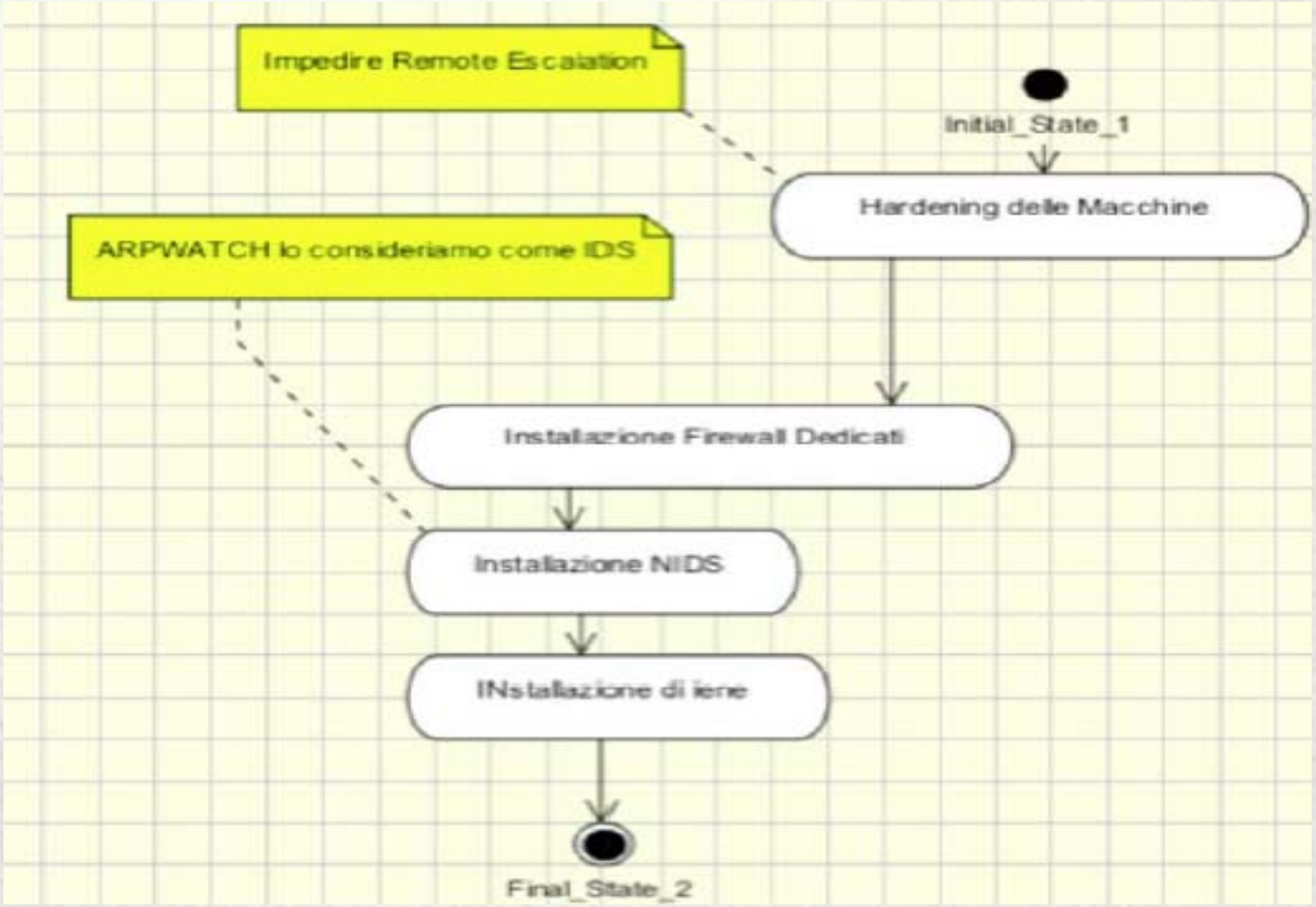
IENA V.S. HoneyPot.

- Molti potrebbero confondere le due tecniche di difesa, in realtà sono differenti.

IENA :
- Obiettivo: difesa
- Architettura: distribuita
- Complessità tecnica: bassa
- Processo: Leggero
- Distribuzione su host: alta

HoneyPot :
- Obiettivo: Ricerca
- Architettura : locale
- Complessità tecnica: alta
- Processo: pesante
- Distribuzione su host: bassa

Modello con IENA.



Modello ICT Attuale:

Implementazione.

- Il server IENA è stato implementato utilizzando tecnologia C-UNIX ergo dipendente dalla piattaforma.
- Il client IENA è stato implementato utilizzando una tecnologia platform indipendent, JAVA.

Sfruttando Nagios.

- Il sistema di alerting che il server IENA scatena, viene avviato (nella versione attuale di IENA) da un noto tool come Nagios.
- Nagios periodicamente confronta i log che IENA produce e ad ogni cambiamento forniscce un valido e immediato avviso allo amministratore di sistema.

Conclusioni.

- IENA non ha la pretesa di essere la soluzione definitiva ad ogni problema riguardante la sicurezza informatica, ma assieme ad altri sistemi di sicurezza può contriburire ad innalzare notevolmente il livello di sicurezza di una rete.

Sviluppi Futuri.

- Rendere piu’ sicura la comunicazione tra IENA e Server-IENA
- Utilizzo di apposite tecniche per il detect di stealth scan
- Inserire un interfaccia grafica per rendere l’ambiente pi’ user-friendly
- Implementazione di una rete IENA e Server-IENA basata su tecnologia Knock
- Integrazione di IENA e Server-IENA con i moderni IDS e IPS

Q.&A.