TRICK YOUR HACK

Fonti:cesena.ing2.unibo.it

Dott. Ing. Paolo Burnacci

burnacci@gmail.com

www.nacci.tk

→ Cos'è IENA?

- Sistema di difesa per la sicurezza di reti locali
- Sovvertimento dei canoni tradizionali della sicurezza
- Sicurezza come inganno dell'attaccante

→ Obiettivi fondamentali (1/2)

- Eliminare ramo destro del tradizionale piano di sicurezza
- Evitare aggiornamenti: scoccianti e pericolosi

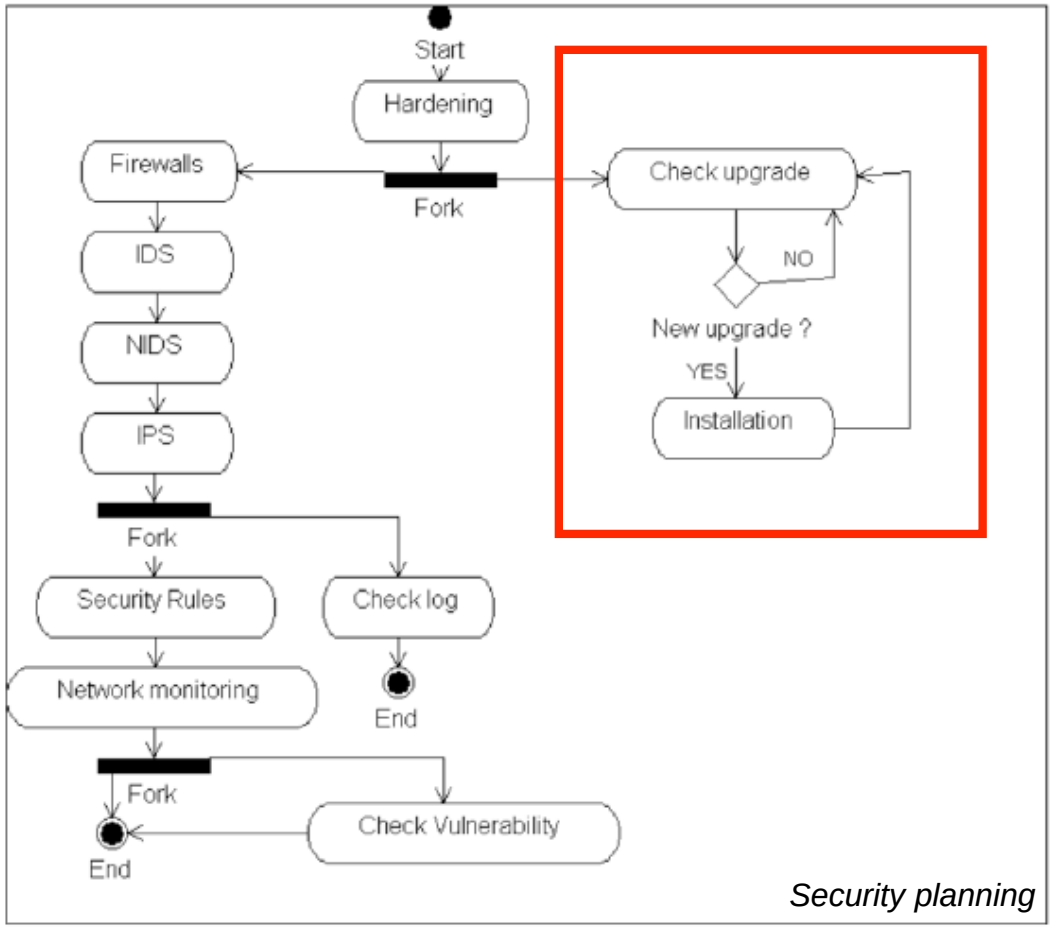
Es: difesa con vulnerabilità

↓

Attaccante trova e pubblica

↓

Software house risolve e distribuisce patch



Security planning

→ Obiettivi fondamentali (2/2)

- Realizzare la sicurezza in modo non convenzionale

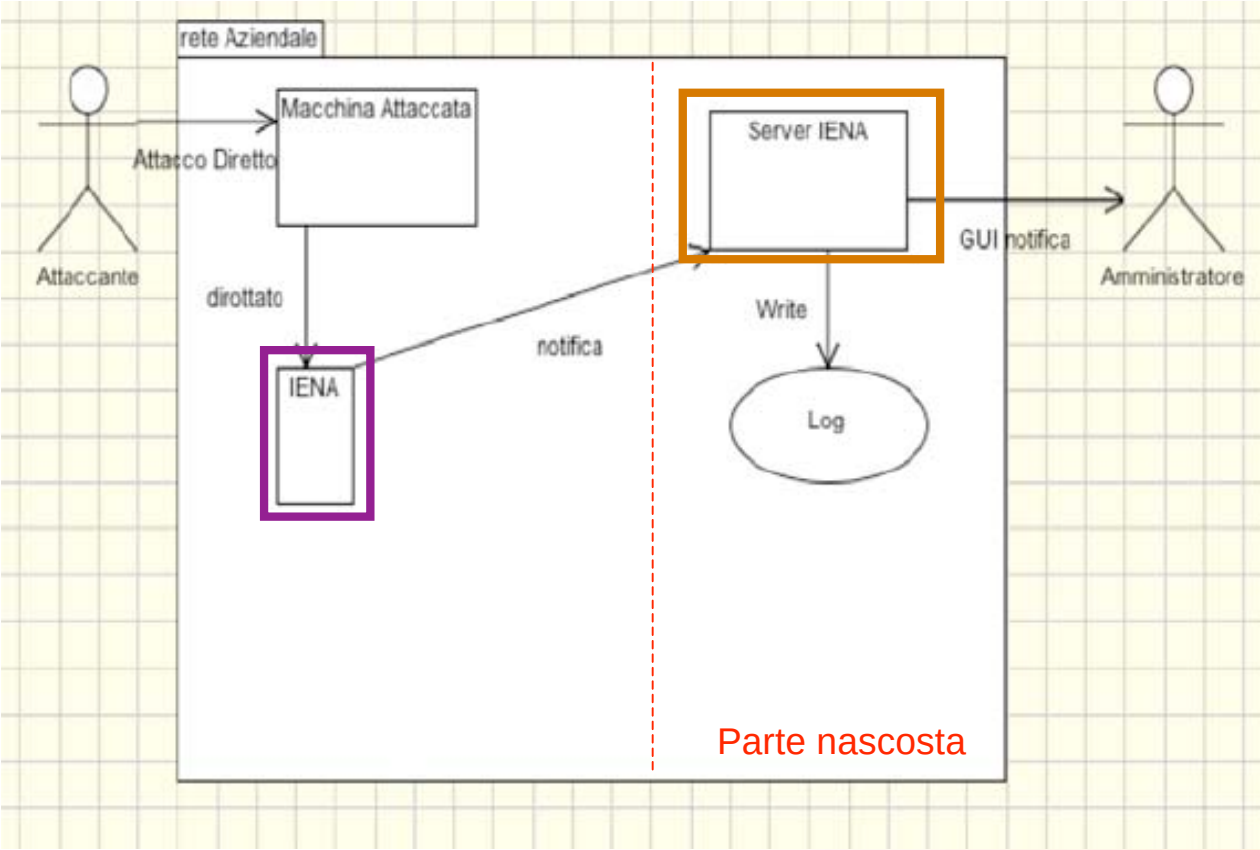
CONVINZIONE TRADIZIONALE

Più applicazioni per la sicurezza sono attive su una macchina più la macchina è sicura (antivirus, firewall…)

INNOVAZIONE DI IENA

Più applicazioni aperte senza sicurezza più IENA rende sicura la macchina

→ Installazione di IENA?



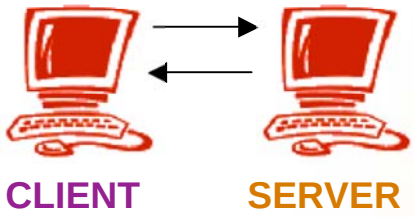
- ✓ Installazione di un client Java su ogni macchina da proteggere
- ✓ Installazione del server IENA (modulo Kernel) unico in una parte nascosta della rete

→ Installazione di IENA?Versioni

- Sono disponibili 2 versioni di IENA:
  - *IENA standard: classica, client-server*
  - *IENA Stand Alone: disponibile su PerSeo, un sistema operativo Live CD Knoppix Based*

PerSeO
Personal Security Operating System

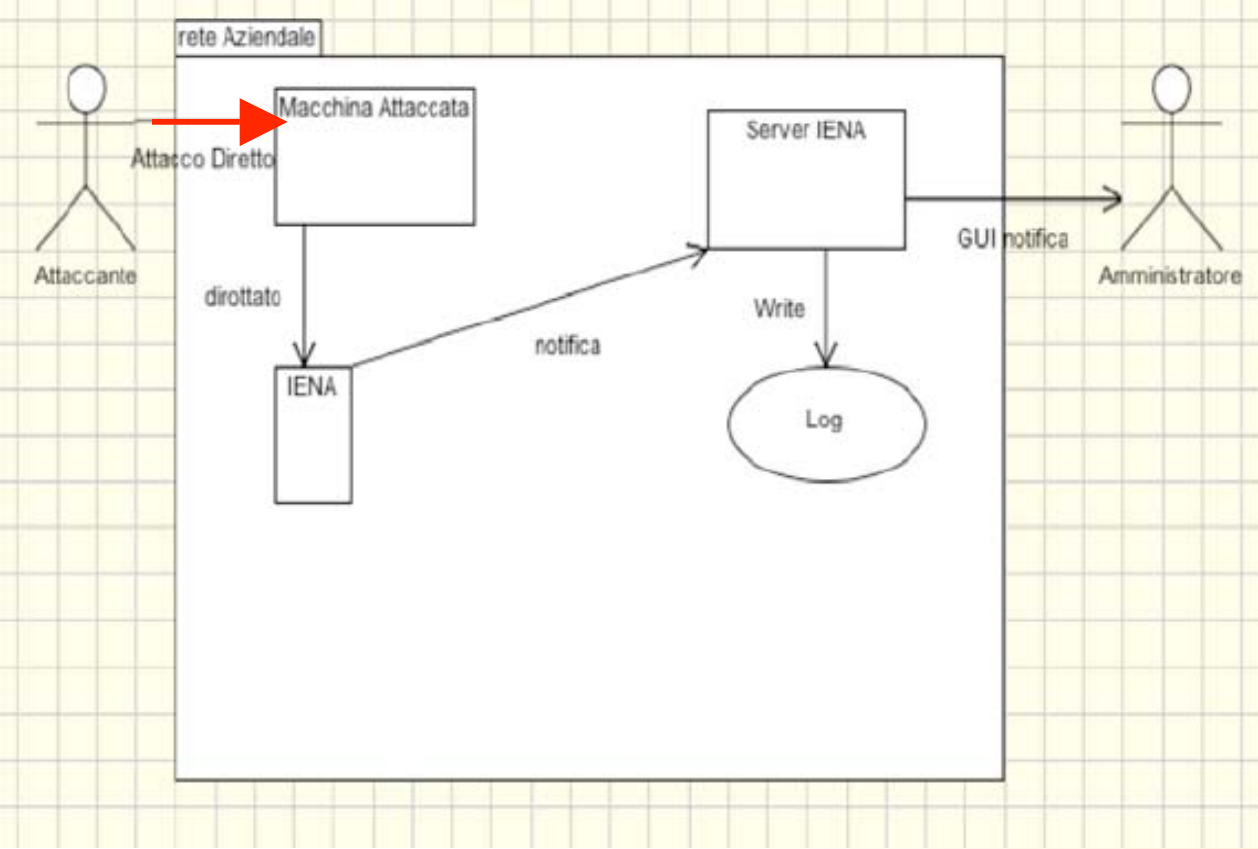
Server non in zona protetta ma su Localhost



→ Come funziona IENA?Criterio

- Tramite il client si associa una iena ad una porta aperta su cui viene simulato un servizio
- L'utente sceglie quante e quali iene collocare
- La configurazione consigliata prevede le porte
  - *12345: NetBus, uno dei trojan più diffusi*
  - *21: ftp*
  - *10000, 12000: per il worm NIMDA e la sua variante 2*
- Una iena su una porta simula un falso servizio

→ Come funziona IENA?Attacco (1/3)



- In caso di attacco diretto ad una porta considerata aperta
- L'attaccante tenta di exploitare i servizi offerti su quella porta

- Attivazione IENA: processo a basso livello

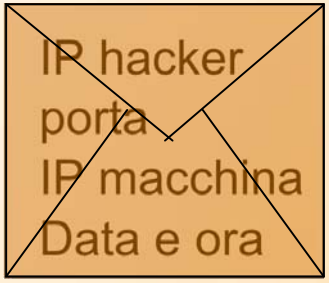
→ Come funziona IENA?Attacco (2/3)

Attivazione di IENA: 2 livelli di tricking

1. L'attaccante si impegna su servizi inesistenti → spreco di risorse
2. L'attaccante viene espulso: chi si connette su quella porta è un intruso che non conosce porte valide

CLIENT → Tutto il traffico viene dirottato al processo IENA

CLIENT → IENA campiona e analizza il traffico costruendo una struttura dati con *IP attaccante, porta di attacco, IP macchina attaccata, data e ora*



CLIENT → Invia i dati al server IENA

→ Come funziona IENA?Attacco (3/3)

- → Scrittura di log

```
**** AttaccoAttacco da /127.0.0.1:53016 in 80  **** Date: Wed Jul 20 18:30:54 2005
 *****
**** AttaccoAttacco da /127.0.0.1:57522 in 80  **** Date: Wed Jul 20 18:32:34 2005
 *****
**** AttaccoAttacco da /127.0.0.1:59249 in 00  **** Date: Wed Jul 20 10:33:16 2005
 *****
**** Attacco  **** Date: Wed Jul 20 18:37:13 2005
 *****
PowerBook:/Users/marcoramilli/Documents/TESI_NAGIOS/src#
```

- → Invio all'amministratore di una notifica: *e-mail, sms(Milano)…*
- → Aggiornamento del DB degli IP DENIED: viene aggiunto quello dell'attaccante

➢ *Riabilitazione dell'IP dopo un timeout (di 24 ore per default)* → *situazione paradossale in cui nessuno accede alla rete*

→ Come funziona IENA?SCAN PORT

- Un attacco con Scan Port rileva quanti e quali servizi sono attivi sulla macchina
- Chi conduce questo attacco deve ignorare quali servizi siano disponibili → INTRUSO!!!
- Infatti l'accesso viene negato: con scan si inciampa inevitabilmente in almeno una porta con una iena (le prova tutte)

→ Scenario tipico

Devo mettere un elevato numero di IENE? NO!!!

→ Se sono un utente autorizzato conosco i servizi consentiti e su quali porte siano attivi

→ Se sono un malintenzionato farò sicuramente SCAN PORT (non posso conoscere a priori le porte aperte)

→ Social engineering: condurre attacchi diretti dopo aver ottenuto informazione sulle porte

→ Obiezioni storiche

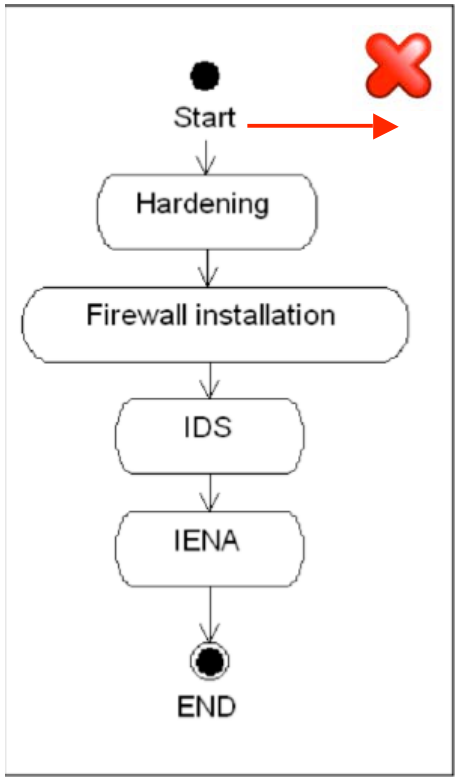
- IENA è un IDS oppure IENA è un IPS

→ No perché IENA lavora sulle connessioni illecite non su quelle lecite

- IENA è un Honey Pot

→ No perché l'Honey Pot ha come fine la ricerca, non l'espulsione, mentre IENA vieta subito l'accesso all'attaccante

→ Eliminazione del ramo



- Non c'è più necessità di aggiornare i vecchi servizi
- Detection di vecchi servizi vulnerabili con SCAN PORT risveglia la IENA
- Impensabile un attacco alla cieca

MISSIONE COMPIUTA