Università degli Studi di Milano
Facoltà di Scienze Matematiche, Fisiche e Naturali

# LaSeR: Laboratorio di Sicurezza e Reti

*Dott. Luca Giancane, Dott. Antonio Nappa*
http://security.dico.unimi.it/

14 febbraio 2009

# Attività del Laboratorio

- partecipazione costante a conferenze di livello internazionale
- attività "*underground*" ;-)

# Attività del Laboratorio

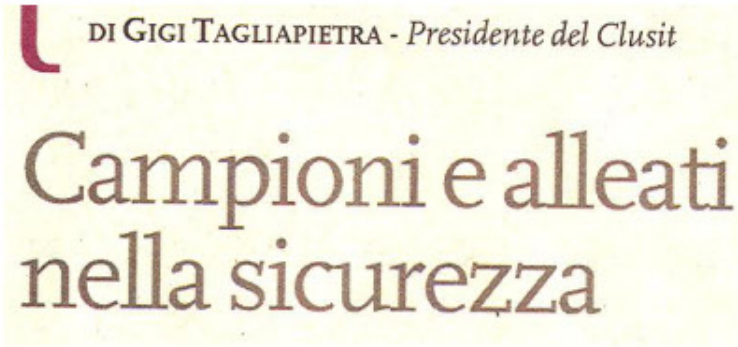
- partecipazione costante a conferenze di livello internazionale
- attività "*underground*" ;-)


La gara nella californiana Santa Barbara: i sistemi nemici violati con un software originale. Settimo il Politecnico

Che bravi i pirati della Statale

*Campioni del mondo nella sfida tra gli hacker*

DEFCON 16


DI GIGI TAGLIAPIETRA - *Presidente del Clusit*

Campioni e alleati nella sicurezza


Punto Informatico

ATTUALITÀ | SICUREZZA | TECNOLOGIA | DIGITAL LIFE | DI

Hacking, italiani campioni del mondo

**UCSB Hosts Largest Computer Hacking Competition Ever**

**Friday's Event Brought Together 35 University Teams from Argentina to India**

- team composto da studenti, dottorandi e docenti del laboratorio LaSeR
- terzo posto alle qualificazioni DEFCON 16 CTF ("*Largest Underground Hacking Convention*")
  - 31/05, 4:00 am → 2/06, 4:00 am
  - 370 squadre da tutto il mondo
  - accedono alla finale solo i primi 7
  - prima squadra italiana mai qualificata

# Guard@MyLan0 @ Las Vegas

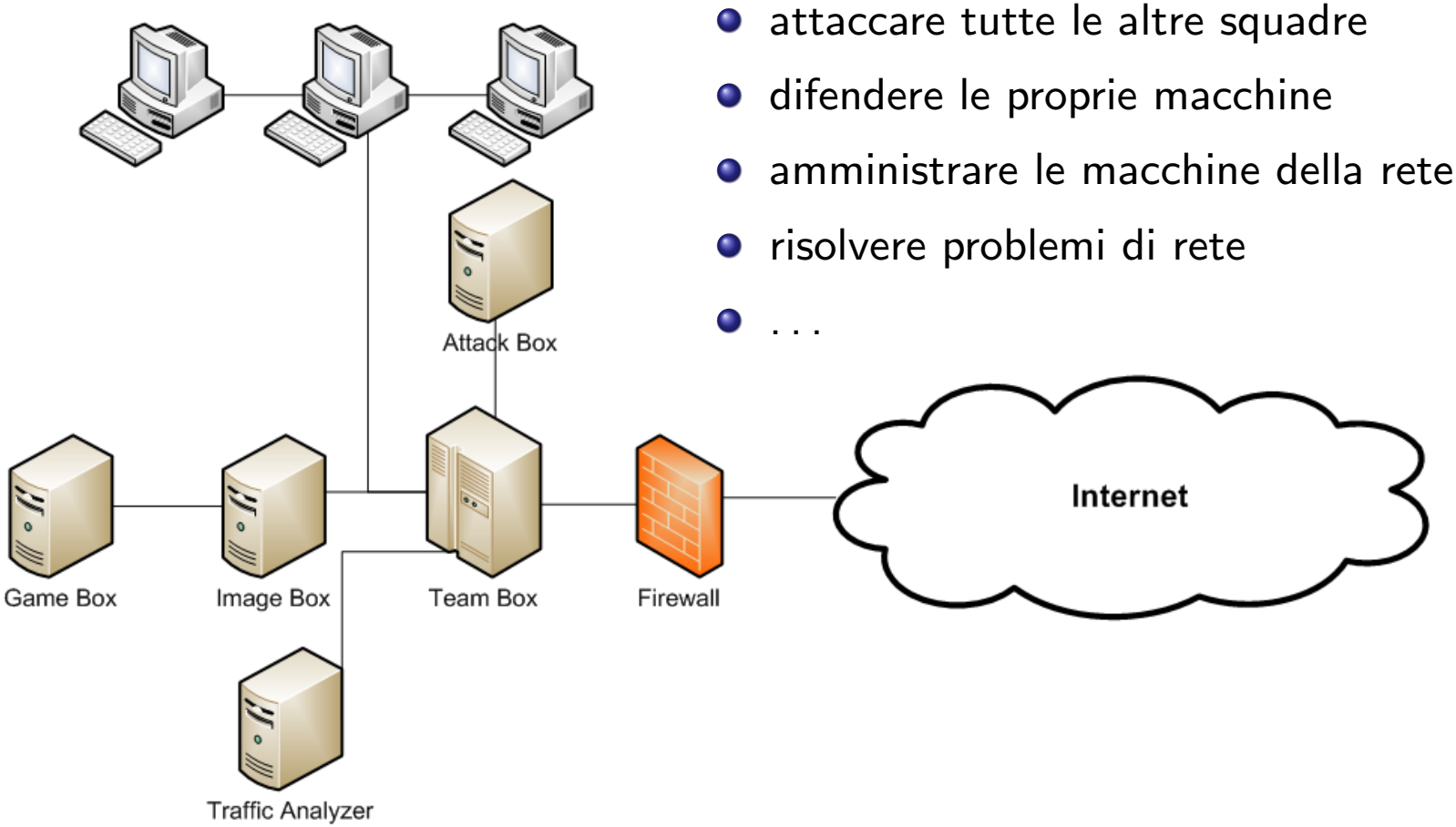
| Team Name | Steals | Overwrite | Breakthru | SLA | Penalties |
|---|---|---|---|---|---|
| sk3wl0fr00t | 1567 | 1046 | 9 | 69 | 0 |
| Routards | 687 | 515 | 6 | 67 | 0 |
| 3@stPlace | 310 | 303 | 5 | 70 | 0 |
| Taekwon-V | 521 | 276 | 5 | 68 | 0 |
| Guard@MyLan0 | 347 | 138 | 2 | 60 | 0 |
| Shellphish | 160 | 10 | 3 | 58 | 0 |
| Pandas with Gambas | 55 | 81 | 8 | 70 | 0 |
| WOWHACKER | 8 | 51 | 1 | 62 | 0 |

- team di 12 persone vola a Las Vegas
- quinto posto al DEFCON 16 CTF
  - 8 agosto $\rightarrow$ 10 agosto
  - 8 squadre da USA, Italia, Francia, Spagna e Corea
  - sk3wl0fr00t vince con 26 persone

# DEFCON 16 Capture The Flag (CTF)

- *hacking contest* organizzato dal gruppo kenshoto
- ogni squadra difende una macchina *virtuale* e cerca di rubare le "bandierine" dalle macchine degli avversari
- le bandierine possono essere rubate tramite *attacchi informatici*
- chi ruba più bandierine vince!

# . . . sembra facile!




- trovare nuove vulnerabilità
- preparare attacchi
- attaccare tutte le altre squadre
- difendere le proprie macchine
- amministrare le macchine della rete
- risolvere problemi di rete
- . . .

# Cos'è una *vulnerabilità*?

Demo

# Realtà o finzione?

## Applicazioni vulnerabili

- **molte** applicazioni reali contengono problemi di sicurezza!
- *decine* di vulnerabilità scoperte ogni giorno in applicazioni reali
- difficile intervenire *correttamente* e *rapidamente* ($$$)

## Vulnerabilità ad-hoc

- vulnerabilità non presenti nel mondo reale ma *verosimili*
- impossibile prepararsi prima di avere accesso alla macchina vulnerabile

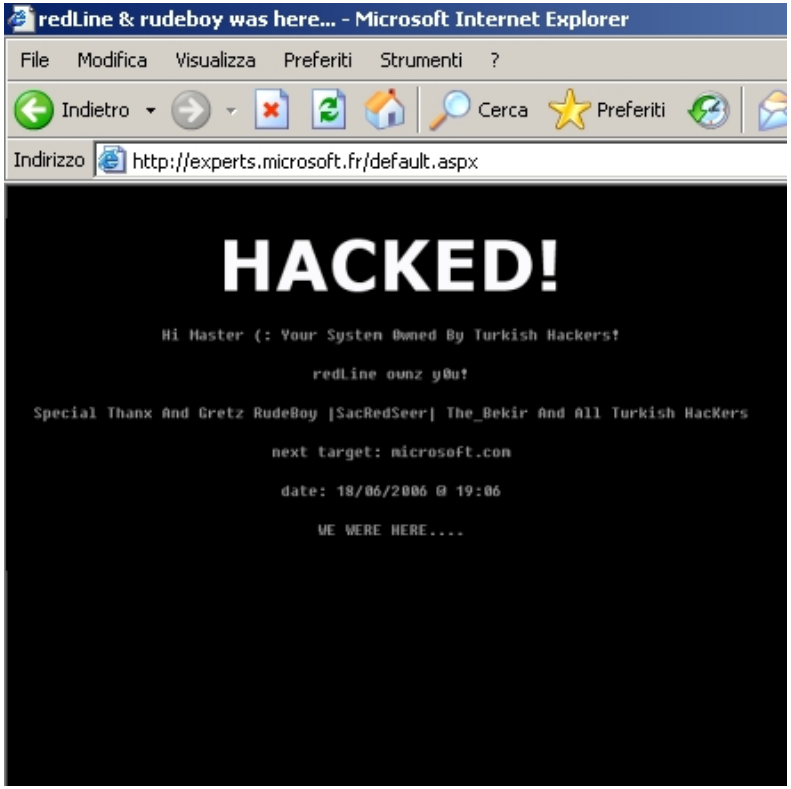
# . . . un buon allenamento

## Solo un gioco?

- permette di trattare un'ampia gamma di vulnerabilità
- contesto simulato ma completamente realistico
- utilizzo di tecniche innovative

- studio delle vulnerabilità non solo per imparare a trovarle e a sfruttarle
- imparare a *prevenirle*

- **FluXOR**: analisi e classificazione botnet
- **Phan**: analisi vulnerabilità PHP
- **Race Conditions** in Web Applications



# LaSeR Research

- **WUSStrace**: Analisi Malware
- **Smartfuzzer**: Analisi Vulnerabilità
- ...

# Saluti da Las Vegas

# Domande?

Laboratorio LaSeR

<http://security.dico.unimi.it/>