



UNIVERSITÀ DEGLI STUDI DI MILANO
FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

International Capture the Flag 2007

Dott. Aristide Fattori, Dott. Luca Giancane
<http://security.dico.unimi.it/>

15 marzo 2008

- 8 tra studenti, dottorandi e docenti del laboratorio LaSeR
- 1° classificati iCTF 2007 (“*Largest Computer Hacking Competition Ever*”)
 - 8 dicembre 2007, 17:00 → 02:00
 - 36 squadre, 9 diverse nazioni
 - alcuni team con oltre 26 componenti!
 - 20% dei punti complessivi

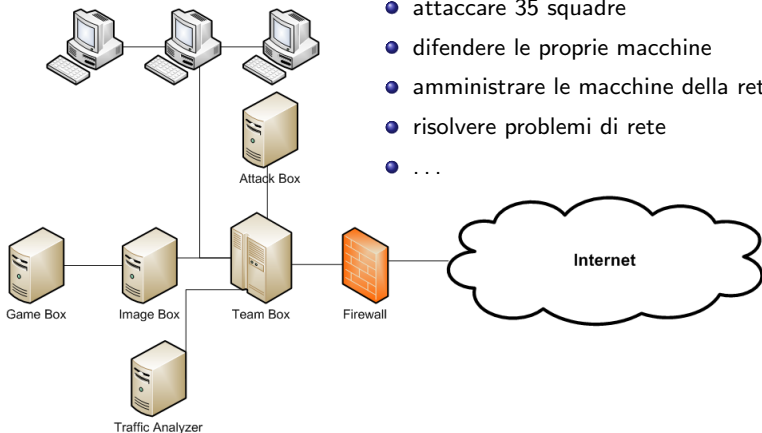


Capture The Flag (CTF)

- *hacking contest* organizzato da UCSB (Santa Barbara, California)
- 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!



- trovare nuove vulnerabilità
- preparare attacchi
- attaccare 35 squadre
- difendere le proprie macchine
- amministrare le macchine della rete
- risolvere problemi di rete
- ...



Demo

DON'T TRY THIS AT HOME



Applicazioni vulnerabili

- sulla macchina vulnerabile sono in esecuzione diverse applicazioni
- molte applicazioni contengono una o più *vulnerabilità*
- permettono di ottenere accesso ai *dati sensibili* presenti sulle macchine degli avversari

Vulnerabilità ad-hoc

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



- vulnerabilità *verosimili*
- **molte** applicazioni reali contengono problemi di sicurezza!
- *decine* di vulnerabilità scoperte ogni giorno in applicazioni reali

Solo un gioco?

- studio delle vulnerabilità non solo per imparare a trovarle e a sfruttarle
- imparare a *prevenirle*
- “*know your enemy*”





**WE WANT YOU
FOR LaSeR!**





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

