

NIDS: next generation

Milani Giacomo [mainman@tiscalinet.it]

Hack-it 2004

Nuovi attacchi hanno dimostrato la totale inefficacia degli attuali network IDS.

Di che attacchi si tratta e quali sono i modi di fronteggiarli ?

Contenuti

Attacchi verso l' implementazione tcp:

- insert
- evasion

Attacchi verso la pattern machine:

- inquinamento nop zone
- shellcode polimorfici o alfanumerici

Difese:

- active mapping
- ricerche euristiche
- spectrum analysis
- data meaning
- microcode emulation

Struttura generica di un attuale network IDS

Componenti

sniffing

stack tcp/ip semplificato

pattern matching

signature db

Attacchi

d.o.s. / falsi positivi

insert - evasion

offuscare nop/shellcode

0 day / varianti di exp



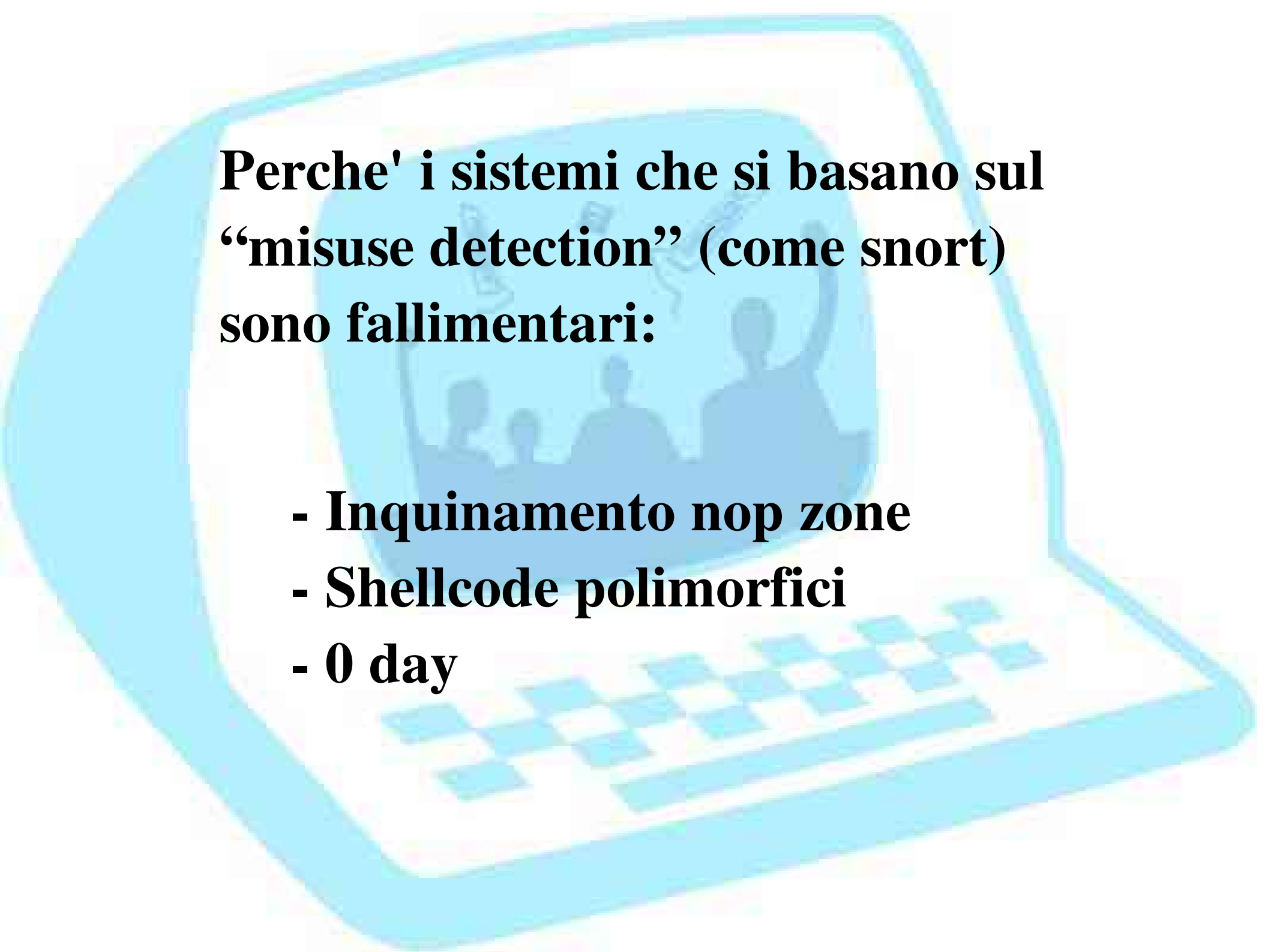
Attacchi a network layer:

- Insert (ttl,checksum)**
- Evasion (frammentazione, fake ack)**
- D.o.s. (aumento banda, false sessioni)**

A stylized blue laptop is shown from a slightly elevated perspective. The screen displays a dark blue background with white silhouettes of several people standing and one person with their arm raised. Above the silhouettes, there are faint white lines and shapes representing a map or data visualization. The laptop's keyboard is visible at the bottom, rendered in a lighter blue color.

Cos'e' l'active mapping ?

**Quali sono i vantaggi
contro evasion e falsi positivi ?**



**Perche' i sistemi che si basano sul
“misuse detection” (come snort)
sono fallimentari:**

- Inquinamento nop zone**
- Shellcode polimorfici**
- 0 day**

Inquinamento nop zone:

0x90 (null operation)

mov 00 -> mov 0x02 (mov to next instruct)

inc %eax – dec %ebx (giochi sui registri)

xor 0x41,0x41 – 0x41 = inc %ecx

(istruzioni inutili con possibilità di salto)

Cosa si intende per “microcode emulation”

- emulatori di macchina (ex. bochs)**
- wrapper di registri (ex. wmvare)**
- wrapper di api (ex. wine)**
- interpreti javascript (contro XSS)**
- parser php/asp + interprete SQL (contro inj)**



**Risolvere il problema computenziale:
i filtri**

- filtri statistici**
- filtri in base a correlazioni**

Punteggi di anomalia

Statistica (payload):

- type of request (ex. named)**
- length of request (ex. iis)**
- payload distribution**

Statistica (time):

- duration of session**
- time of session (dopo una fase di learning)**
- aumento di traffico rispetto lo storico (worm)**
- risposte negative ripetute (brute forcing)**

Correlazione eventi

- **type of service (banner?, contro falsi positivi)**
- **type of attack (diversi alberi di previsione)**
- **previsioni eventi (heuristic research)**
- **replica traffico (contro infezione worm)**
- **data meaning (ex. telnet traffic)**