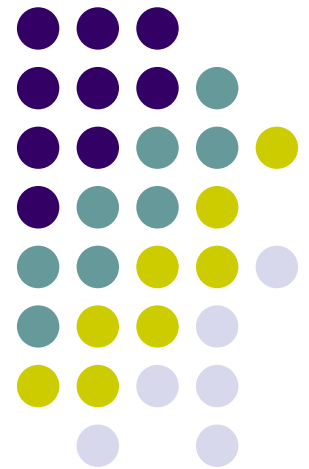
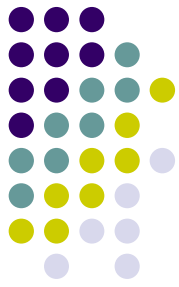


# Anàlisi de les vulnerabilitats

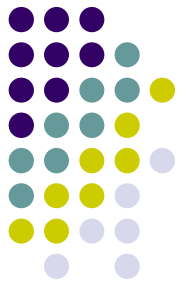
Com descobrir les vulnerabilitats,  
prevenir-les i evitar-les



# Introducció



- Que son les vulnerabilitats?
  - Errades o problemes de qualsevol element que donen la possibilitat de realitzar un atac.
- Quin risc comporten?
  - Per si soles cap, però és un risc potencial que pot ser aprofitat en qualsevol moment
- Com s'eviten?
  - Amb una correcta administració i seguiment dels sistemes. Tot i així MAI les eliminarem totes.



# Origen de les vulnerabilitats

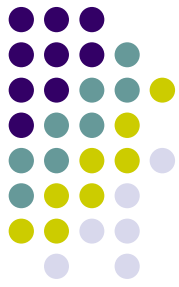
- 3 principals fonts d'origen de les vulnerabilitats:
  - Errors de programació
    - Variables, buffers, tractament d'errors, etc...
  - Errors de l'usuari
    - Passwords, ...
  - Mala administració
    - Manca d'actualitzacions
    - Software inadequat o innecessari
    - Proteccio insuficient

# Descobriments de noves vulnerabilitats (I)

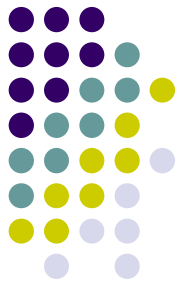


- Tècniques usades per a descobrir errors potencials d'un sistema:
  - Estudi del codi font
    - Es necessari poder tenir-hi accés
    - Cal tenir un coneixement molt avançat
  - Tècniques de força bruta
    - Provar diferents combinacions utilitzant la potència de càlcul
  - Tècniques de força guiada
    - Seleccionar aquelles combinacions que sapiguem que donen més problemes.

# Descobriments de noves vulnerabilitats (II)



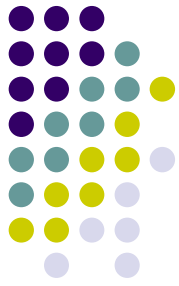
- Anàlisi de les variables del sistema
  - Monitorització dels recursos gastats per cada aplicació
  - Es necessari l'accés a la màquina.
- Aplicació de vulnerabilitats semblants
  - Provar si un problema es repeteix en diferents plataformes / serveis diferents
- Casualitat
  - Impossible de predir...



# Vulnerabilitats existents

- Varies pàgines i llistes de distribució mantenen informació constantment actualitzada per a informar de tots aquells problemes existents
- Poden contenir:
  - Descripció del problema
  - Solució del mateix
  - Codi per a aprofitar-se del problema
- Nomenclatura: necessària per a organitzar tot el volum de vulnerabilitats (CVE, CAN, Bid,...)

# Pàgines de vulnerabilitats (I)



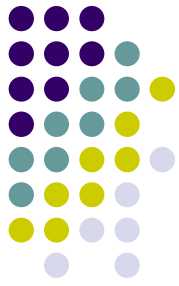
- **CVE Database:**

- <http://cve.mitre.org/>
- "Common Vulnerabilities and Exposures project"
- Les vulnerabilitats tenen el format CAN-Any-Num mentre són estudiades, i passen a CVE-Any-Num un cop són aprovades.
- sistema més estandard per a etiquetar vulnerabilitats.

- **CERT-Advisories**

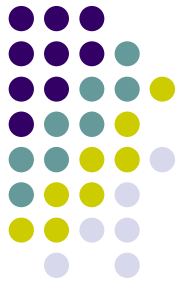
- <http://www.cert.org/advisories/>
- Informació emesa pel CERT/CC.
- Descriu àmpliament el problema detectat i aporta possibles solucions.
- El sistema de classificació/notació són els Cert Advisories, CA-XXXX.
- És una de les webs de referència en la seguretat informàtica.

# Pàgines de vulnerabilitats (II)



- **Security Focus:**
  - <http://www.securityfocus.com/>
  - Recopilació de bugs i vulnerabilitats amb informació de l'atac,
  - La pagina també és la base de la llista de Bugtraq, una de les mes importants on es publiquen les principal vulnerabilitats actuals.
  - Per referir-se i classificar els atacs utilitza la notació BID (Inicials de Bugtraq ID), una de les mes importants, però no estàndards.
- **Internet Security Systems (ISS) X-Force Database:**
  - <http://www.iss.net/>
  - Consultora professional sobre seguretat que recopila també vulnerabilitats en una base de dades pròpia.
  - El més important és que recull molts links relacionats amb cadascuna de les vulnerabilitats estudiades.

# Pàgines de vulnerabilitats (III)



- **Denial of Service Database**

- <http://www.attrition.org/security/denial/>
- Completa base de dades d'atacs de denegació de servei organitzada amb un sistema de notació anomenat OSAT:
  - OS (Tipus de sistema operatiu) + A (Accés que cal per a poder realitzar l'atac: Shell, consola, Xwin, ...) + T (Tipus d'atac).

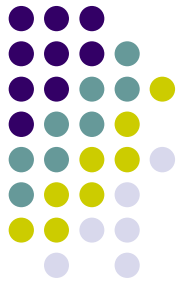
- **Enslaver.com**

- <http://www.enslaver.com>
- Pàgina underground on es poden descarregar alguns exploits. No és molt completa però s'hi pot trobar algun scàner de vulnerabilitats.

- **Fyodor's Exploit World**

- <http://www.insecure.org/sploits.html>
- Ampli recull d'exploits sobre vulnerabilitats i bugs amb la corresponent descripció del problema. Es troben ordenats pel sistema operatiu.

# Pàgines de vulnerabilitats (IV)



- **Gov-boi's exploit archive**

- <http://www.hack.co.za/>
- Un altre recull d'exploits que, a més, inclou alguns virus i altres codis malignes, eines de hacking i altres.

- **INFOSYSSEC**

- <http://www.infosyssec.org/infosyssec/>
- Compendi d'enllaços i notícies sobre seguretat i hacking. Inclou buscadors de vulnerabilitats a base de dades externes com la CVE i la ICAT, enllaços a Bugtraq i CERT, etc..

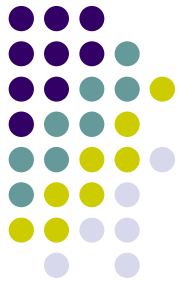
- **Hispacec**

- <http://www.hispasec.com/>
- Web de seguretat informàtica en castellà, coneguda per la llista de seguretat "una al dia", que informa als seus subscriptors sobre bugs, vulnerabilitats, virus, i altres amenaces per la seguretat. Es pot consultar la base de dades de notícies on es troben descripcions i solucions dels problemes detectats.

- **Kriptopolis**

- <http://www.kriptopolis.com/>
- Revista electrònica en castellà dedicada a la seguretat i privacitat informàtica. No hi ha cap exploit ni bases de dades sobre vulnerabilitats actualment, però els articles reflexen alguns problemes de seguretat i les seves solucions.

# Pàgines de vulnerabilitats (V)



- **Secureroot**
  - <http://www.secureroot.com/>
  - Recull d'avisos, exploits, eines de seguretat, etc... Durant molts anys va ser la referència en aquest camp, juntament amb la recopilació de rootshell. Actualment es troben molt desfasades i aporten poca informació interessant.
- **Securiteam**
  - <http://www.securiteam.com/exploits/>
  - Base de dades d'exploits amb una descripció de la vulnerabilitat, detalls del sistema afectat i codi necessari per atacar el servei. També conté apartats de notícies sobre seguretat, eines, i apartats independents separats per sistemes operatius ordenats en dos grans grups (UNIX i Windows NT).
- **Underground Security System Research**
  - <http://www.ussrback.com/>
  - Complerta recopilació d'exploits des dels més antics, que es troben més com a curiositat, fins als últims i més recents.
- **@stake**
  - <http://www.atstake.com/research/>
  - Consultoria de seguretat que recopila els diferents avisos de seguretat amb la seva descripció i recomanacions sobre com solucionar les vulnerabilitats.