Eső után köpönyeg – mentsük ami menthető

Kalandjaim a bajverekkel feltört gép helyreállítása

Botka István
Dunaújvárosi Főiskola

Eső után köpönyeg – mentsük ami menthető

- Környezet:
  - Vmware virtualis gép
  - portál
  - Fizikai gép csak management hálózatban
  - Virtuális gép nyilvános hálózatban

Eső után köpönyeg – mentsük ami menthető

- Mi történt?
  - rohamtempóban telepítés
  - gyenge jelszó
  - ssh megnyitás a nagyvilágból
  - password auth
  - ”örökre vasalt” ideiglenes megoldások
- ~1 hétig bírta

Eső után köpönyeg – mentsük ami menthető

- Mi történt 2?
  - módosított root jelszó – lebukás
  - módosított binárisok
  - ext3fs attribútumok

Eső után köpönyeg – mentsük ami menthető

- Mit csináljunk miután beütött a krach?
  - először SEMMIT! - csak gondolkodjunk
  - izoláció
  - mentés
  - akcióterv készítése
  - ajtó bezár, telafon kikapcsol
  - mély levegő
  - Hó-rukk!

Eső után köpönyeg – mentsük ami menthető

- Eszközpark
  - debsums (debian és származékai)
  - live cd
  - tripwire – megelőzés
  - tiger

Eső után köpönyeg – mentsük ami menthető

- DEMO