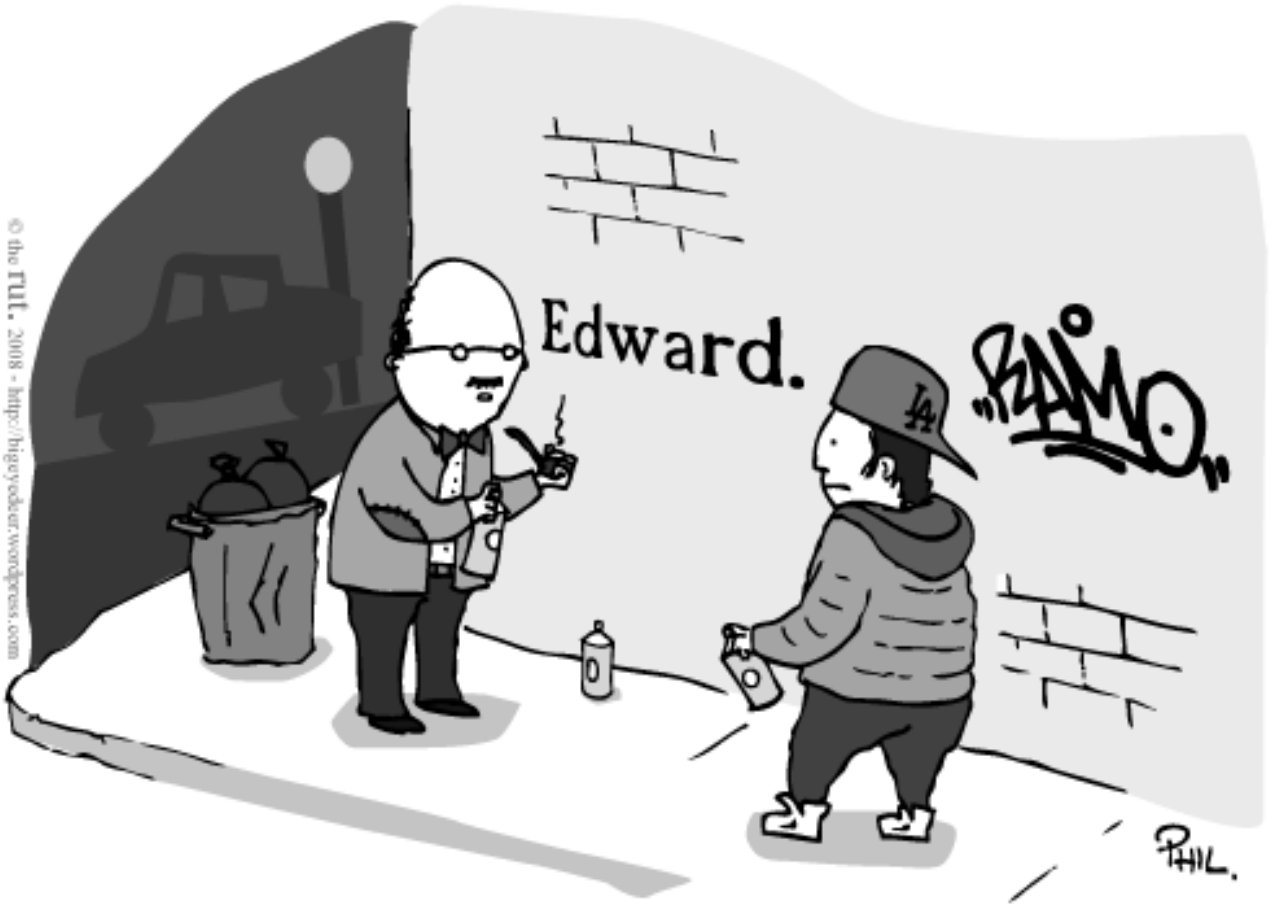
ENTERPRISE SECURITY

Softer than the foam on my Frappuccino

Lower Upper Middle Class Crew



'Yes well, legibility and correct punctuation might not be "street"... but that's how I roll, motherfucker.'

I AM

- Fionnbharr Davies
- thoth
- Securus Global
- Over The Wire
- Grew up in the ghetto of the eastern suburbz
- Serious business


SERIOUS BUSINESS

Outline

- Obvious mistakes
- Rant on enterprises and their software
- ‘security’ appliances
- iPhonez
- Suggestions on how Enterprises can help themselves relatively easily.

Obvious Mistakes

- Just sniff
  - Netbios
  - Wpad
  - Layer 2 (HSRP, OSPF, etc)
- Telnetz
- 10 billion web interfaces
- Enterprise software (in general)

Enterprises and their software

- What's bad (IMHO)
  - Centralised software
  - Automatic restarting
  - Unsigned updates
  - Multiple AV products on one machine
  - Backporting
  - Crappy distro’s like redhat/ubuntu
  - No asset management
  - Lotus notes facing the internet

Trend Micro

“It is apparent that we have reached a crossroads with Trend -- where they are unable or unwilling to sufficiently patch these eight critical vulnerabilities reported by X-Force. At this point, I feel it is important to let our customers know about the inherent and abundant security risks of running TrendMicro ServerProtect. “

-- http://blogs.iss.net/archive/trend.html

‘Security’ Appliances

- Hardened?
- Ancient OS
- Old old protections
- Mail appliances run AV over attachments
- Has to have high availability
- Some supress logs
- Unsigned updates
- Strip your binaries ☺
- They are software companies, not security

Sales Network

SALES NETWORK

HOW TO BUY

- warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /www/bluecoat2.0/sites/default/modules/salesrep_bluecoat/salesrep_bluecoat.module on line 315.
- warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /www/bluecoat2.0/sites/default/modules/salesrep_bluecoat/salesrep_bluecoat.module on line 321.

Contact our worldwide sales network

You can buy Blue Coat products through our global network of sales offices or through highly qualified distributors, system integrators and resellers who sell, install, and support our products.

If you would prefer a sales representative to contact you instead, please use our Contact form

Search Again

Ze iPhone

- A product not ready for the enterprise, that people want to push into it.
- Remembers *
- Terrible security record
- Unique 3G IP with some carriers (e.g. Optus)
- SSH woes :o the new cisco:cisco
- Will be interesting research coming out for it in the future

Help?

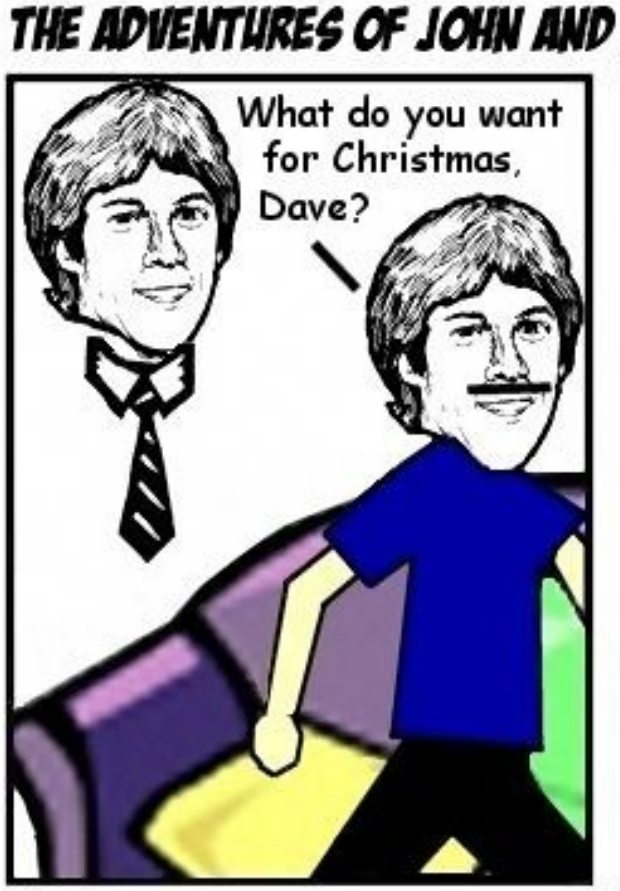
- Don’t do all the stuff I’ve just talked about! (like backporting, arrrggh)
- Don’t trust _any_ software
- !IDP
- Read logs, investigate crashes
- Run real OS’s (redhat can die in a chemical fire of dicks)
- Platform selection
- Appliance 0day is worth a lot less than OS 0day
- Let your pentesters crash services
- **Don’t listen to sales guys; they are all cunce**

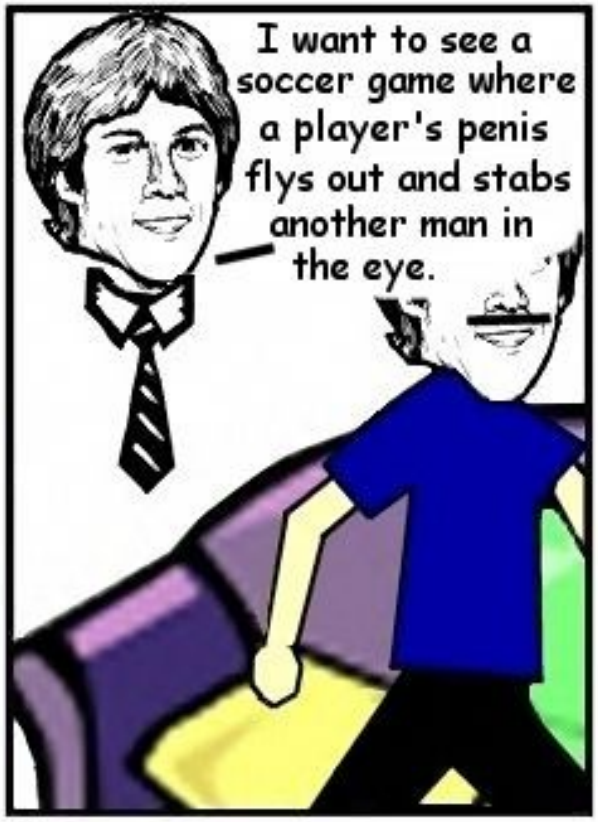
Greetz:

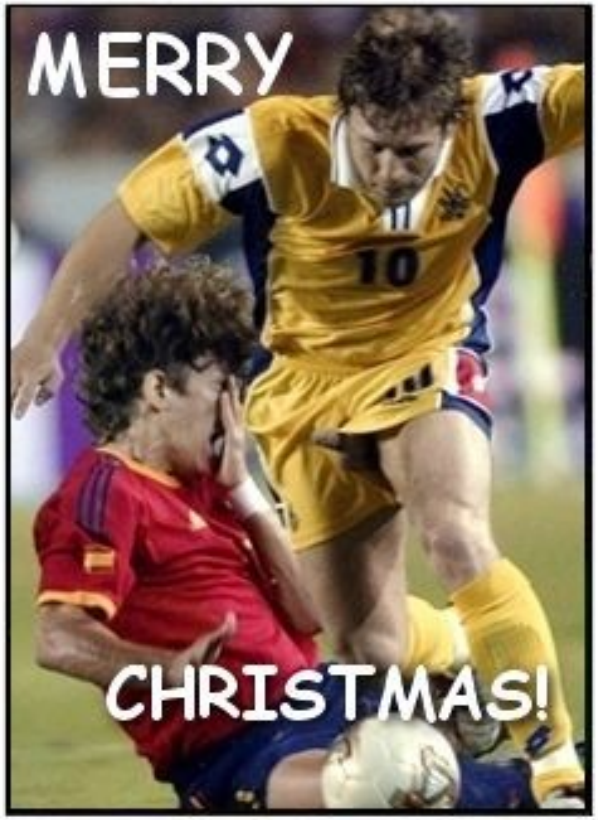
ZeCuRuZ Gl0balz, #cunce, #ruxcon, #blah, #straightmissionarysex, #d----

no names, just channels ☺

Questions?







pic unrelated