



IT Security - UNAM

Rubén Aquino Luna
raquno@seguridad.unam.mx



IT Security at UNAM

- Large network (132.248.X.X, 132.247.X.X)
- A lot of problems (several kind of problems)



IT security challenges

- Over 200 units (faculties, institutes, administrative, etc)
- Permissive perimeter (everything allows, a few things forbidden)
- Very general computer and network use policies



IT threads

- Automated attacks (virus, worms, DDoS, Brute Force attacks, bots)
- Scams
- Computer and network resources misuse
- Information theft (administrative, research)



Risks

- Infrastructure failure
- Information leakage
- Frauds against community members
- Infrastructure misuse



How do we minimize risk

- Promote prevention
 - All levels (manager, IT admin, users)
- Improve monitoring
 - IDS, darknet, malware sensors
 - Deploy detection devices
- Incident Response: UNAM-CERT
- Best practices



Lessons learned so far

- It is difficult to have restricted policies for all university
- Focus on prevention at different levels
- It is difficult to persuade people
- Focus on implementing best practices



Universidad Nacional
Autónoma de México



Rubén Aquino Luna
raquino@seguridad.unam.mx

