Systems & Network Security

Introduction

What do we mean by security

- A good definition:
  - "[…] *processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction*"
  - ***"Computer security also includes protection from unplanned events and natural disasters"***

Source: https://en.wikipedia.org/wiki/Computer_security

What are we trying to protect

- Infrastructure
  - Routers, switches, and associated data
- Hosts, services
  - Mail, DNS, …
- Data
  - Files, databases, …
- Users
  - Passwords, privileged accesses

In other words…

- Host security
  - Remember, everything is a host
  - Protect the infrastructure as well as the hosts running services
- Data security
  - Mitigating what “they” have access to, once they’re inside
- Intrusion Detection
  - Try and detect malicious behaviour

Our approach

1. Prevent and protect
2. Detect
3. Mitigate

Security threats and trends

- Threats

  [excerpts from Arbor Network's yearly security report]
- Some clear threats emerge:
  - DDoS - http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet
  - Data Breach / theft of customer databases – (SONY, Citigroup, RSA, Evernote,)
    - More and more reports every month of compromised companies
  - Defacement (usually harmless, but poor image)
  - Malware (infected software, viruses, malicious documents – PDF, Flash, Java)
- Motivations for DDoS (upwards of 100 Gbps is not unheard of nowadays)
  - Political / Ideological
  - Gaming (!)
  - Vandalism
  - Social networking related
  - Revenge / disputes between groups
  - Extortion (less than people think)

http://www.arbornetworks.com/research/infrastructure-security-report

Questions

?