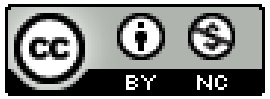
Systems & Network Security

Jonathan Brewer
Network Startup Resource Center
jon@nsrc.org



What do we mean by security?

- A good definition:
  - "[...]*processes and mechanisms by which compu 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
  - DDoS
  - Data Breach / theft of customer databases – (Sony, Citigroup)
  - Defacement or Vandalism
  - Malware, viruses, malicious PDF, Flash, Java
- Motivations
  - Political / Ideological
  - Commercial
  - Gaming
  - Vandalism
  - Personal / Social networking related
  - Revenge / disputes between groups
  - Extortion