Server Security Essentials

Protecting a Lone Network from the Wild, Great Wide Open

By Hansen Wu

Opening the Floodgates

- Sheltered and protected behind your router
- Port forwarding
- Firewall
  - Router blocks most things

Bandits At The Door

- Starts the moment of exposure
- SSH Brute Forcing
- nmap examples

Protecting your Lonely Network

- PASSWORD
  - NEVER NEVER NEVER USE A DEFAULT OR OBVIOUSLY WEAK PASSWORD
- Ports
  - Non-default: obfuscation at best
  - Allow access only to the services you need
- Web Server
  - Require index files

Protecting your Lonely Network Cont

- SSH
  - Botnet ssh brute forcing
    - root login, dictionary attack
  - Command line remote access
  - Disallow root login
  - fail2ban
    - Observes logs and blocks connections using iptables
    - Configuration file
  - Visual ECDSA Fingerprint
    - Hash of server public key
    - Client side setting