The Direction of STS

Jon C. Meyer, Kristopher K. Weeks

Scripps Institution of Oceanography

Shipboard Technical Support — Computing Resources

Ship's network is part of UCSD's network

- http://blink.ucsd.edu/go/networkstandards
- http://www-no.ucsd.edu/security/minstds/impl.guide.html
- http://blink.ucsd.edu/go/networkresources
- http://adminrecords.ucsd.edu/PPM/docs/135-3.pdf

Minimum UCSD security

- Software patch updates
- Anti-virus software
- Unnecessary services
- Host-based firewall software
- Passwords
- Minimize unencrypted authentication
- No unauthenticated email relays
- No unauthenticated proxy services
- Physical security

STS-CR: where we're at

- Cisco router is used for a firewall
- Managed Switches, VLANs
- Protocols typically allowed 24/7
  - IMAP, POP3, SMTP, select IM protocols
  - Special cases: video, special case Internet
- A few dedicated Internet access workstations
  - More, if Chief Scientist requests

STS-CR: lessons learned

- Weak passwords allow hacking
  - We've traced a hacking event to a weak password
- Patch systems before poking holes in firewall
  - We've had a system compromised because sshd was enabled before patching occurred

STS-CR: where we're going

- Better bandwidth management
  - Bandwidth monitoring
  - Allowances based on user privileges/class
- Better network segregation through VLANs
- Secure, but easier navigation in the shipboard network
  - Unified accounts (LDAP), with strong passwords
  - Network authentication (Kerberos)
- Shore-based administration, where possible
- Failover via clustering or failover-supporting protocols

Thanks!

Jon C. Meyer, Kristopher K. Weeks

Scripps Institution of Oceanography

Shipboard Technical Support — Computing Resources