Campus Security

Essentials: L2 security mechanisms

Agenda

- In The News: Telnet sucks
- Lab Exam: group times are now posted in the BB gradebook!
- Complete last page, review Ch 7 – Network Management
- Start Ch 10 – Campus Security

Assigned Readings and Lab work

- Read FLG Ch 10 – Security due by Wed Mar 29
- Cisco **Ch 7** online test due before **Tue** Mar 28 @ 11:59pm
- Cisco **Ch 10** online test due before **Fri** Mar 31 @ 11:59pm
- Cisco **Ch 8** online test due before **Tue** Apr 4 @ 11:59pm
- Cisco online final due between Wed Apr 5 & **Fri** Apr 7 @ 11:59pm
- Pre-lab and post-labs as per the regular schedule
- Lab 11: Cisco v7 labs 8.1 – IP SLA and RSPAN

In The News

"Cisco Systems said that more than 300 models of switches it sells contain a critical vulnerability that allows the CIA to use a simple command to remotely execute malicious code that takes full control of the devices. There currently is no fix."

> "An attacker could exploit this vulnerability by sending malformed CMP-specific telnet options while establishing a telnet session with an affected Cisco device configured to accept telnet connections,"
> Mar 17, 2017

https://arstechnica.com/security/2017/03/a-simple-command-allows-the-cia-to-commandeer-318-models-of-cisco-switches/

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp

Major Security Concerns

4 categories of attacks that are covered:
– Device access attacks
– VLAN attacks
– MAC attacks
– Spoofing attacks (DHCP server, IP, MAC)

... and the counter-measures to protect and secure the network:
– port security
– storm control
– securing VLANs