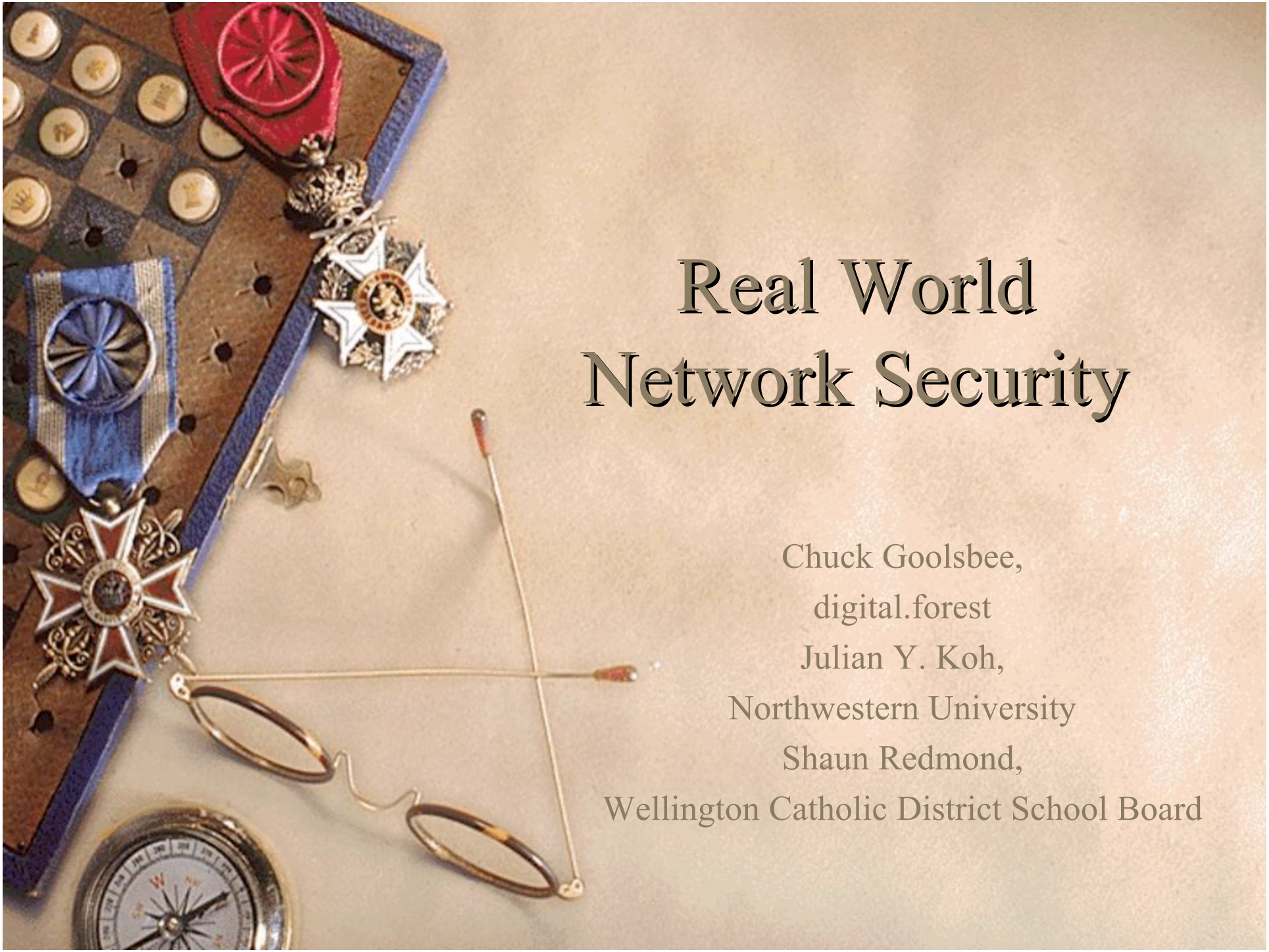


Real World Network Security

Chuck Goolsbee,
digital.forest
Julian Y. Koh,
Northwestern University
Shaun Redmond,
Wellington Catholic District School Board

Problems with Security Training

- Paranoid
- Hardly any Mac-specific info
- Really paranoid
- Lots of “what can the bad guys do” talk, little “what can you really do?” discussion
- Overly paranoid

Network vs. Host Security

- Pedantic folk will always talk about the differences
  - Host security: “I wouldn’t have to worry about my hosts so much if those network people would set up the firewall”
  - Network security: “Firewalls are for people who can’t keep their machines secured - I just have to deliver the bits”
- Reality: the two are intertwined

Be Realistic

- Familiarize yourself with theoretical vulnerabilities
- Prioritize possibilities and assess practical risk
- Implement feasible defenses

Mac OS Host Security

- Good Old Days
  - No real worries
  - Mac OS 7-9 secure “by default” (accident?)
  - Primarily application-level issues
    - WebSTAR proxy on by default
    - Weak passwords on File Sharing accounts
  - Some OS-level problems
    - PMTU-D DOS possibilities
  - Small market share = poor hacking opportunity

Mac OS Host Security

- Good New Days
  - Mac OS X = FreeBSD Unix
  - Great availability of tools, both good and bad
  - Shared code --> shared vulnerabilities?
  - Apple doing pretty good job of proactive patching/updating
  - Short list of OS-level vulnerabilities
- Beware of complacency!

Secure Network Design

- What is your network used for?
- Balance wants/needs of your users/customers
  - Make them aware of tradeoffs
  - Beware the LCD
- Defense in depth
- Policies

Management <=> Security

- A well-managed network is well-watched
  - SNMP on everything
  - Network flow traffic monitoring
  - syslog analysis
  - Intrusion Detection System
    - Signature-based vs. Anomaly-based
- Learn what “normal” or baseline should look like
- Filter/correlate information gathered

Dealing with Threats

- Learn about attacks/vulnerabilities
  - CERT <http://www.cert.org/>
  - FIRST <http://www.first.org/>
  - SANS <http://www.sans.org/>
  - Internet Storm Center <http://isc.sans.org/>
  - NANOG <http://www.nanog.org/>
  - Team Cymru <http://www.cymru.com/>

Dealing with Threats

- Audit machines and devices
  - Simple: automate patches and AV updates
  - Medium: scan hosts for vulnerabilities
  - Complex: check password strength, patches of applications
- Get the most bang for your buck

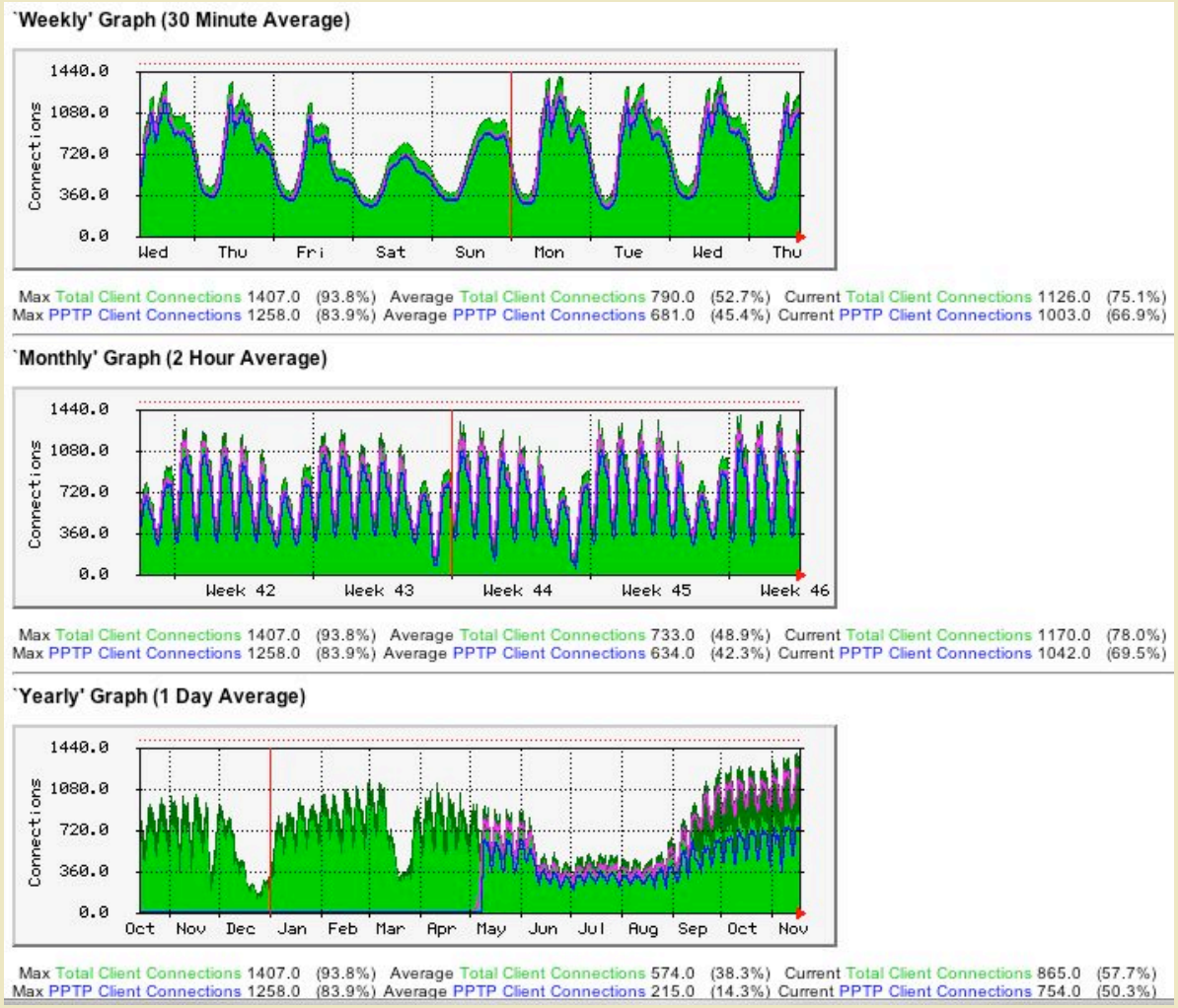
Dealing with Events/Incidents

- Security issues = operational issues
- Swift response can be key
- Clear presentation of data to response staff
- Make policies clear
- Beware retaliation

Examples - Northwestern

- All border flows exported
- PacketShaper bandwidth management
- All hubs & switches polled for MAC addresses of connected devices
- Dual Intrusion Detection Systems
- SNMP monitoring and statistics
- Central syslog collection and analysis
- NetPass Quarantine network for dorms

mrtg SNMP Collection



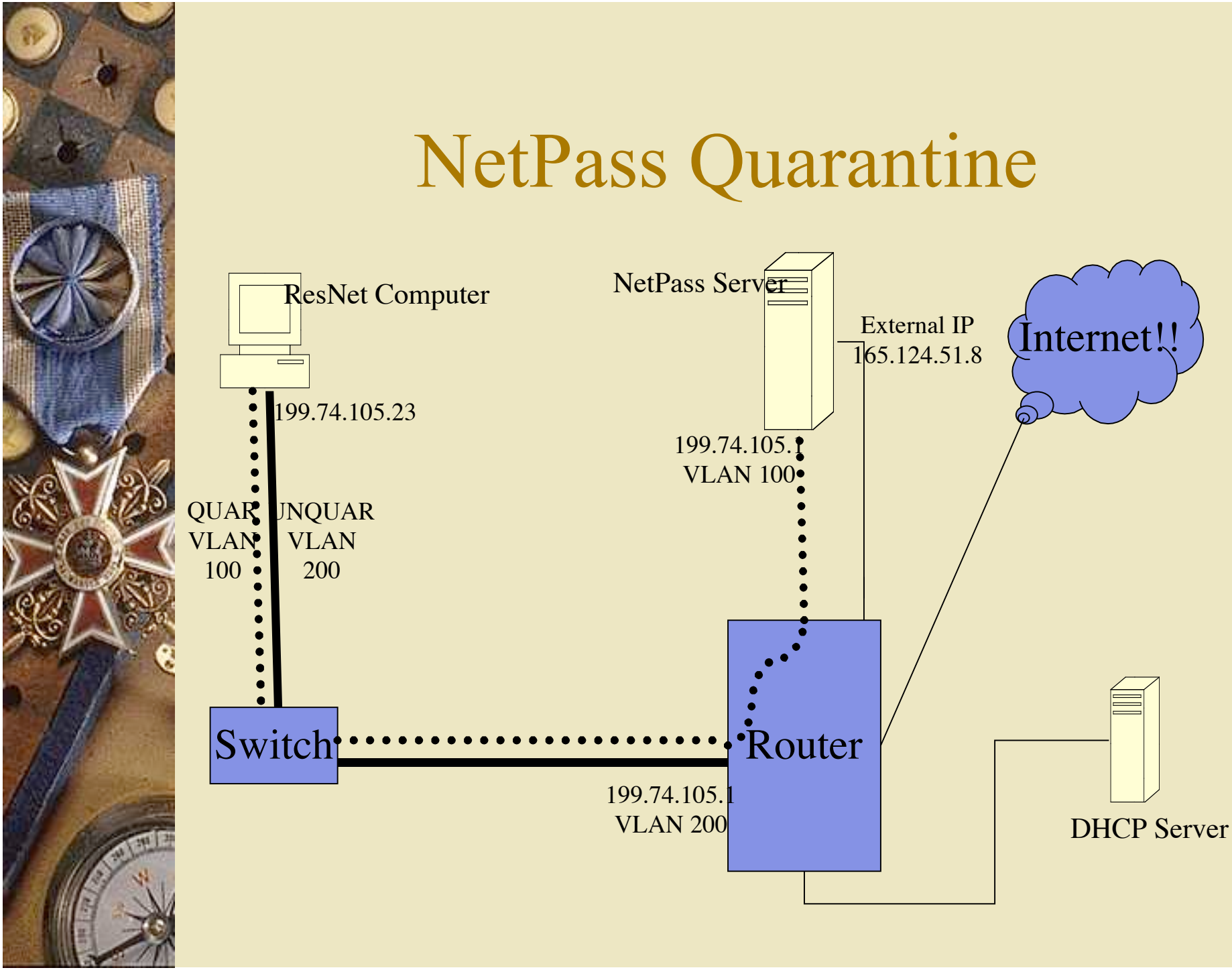
NetVigil Statistics

Test Summary
vpn-public.vpn - 129.105.253.246
Select a test name below to view a graphical test history.
Events for the last 24 hours
Device performance for the last 24 hours
Turn Display Filter On

page 1 of 1 GO
enter regexp SEARCH

STATUS	TEST	VALUE	WARN/CRIT	TEST TIME	DURATION	MODIFY	HELP
ok	CPU Utilization	77 %	93/98	4:13 PM	00:00		
ok	Remote Access Users	1205 Users	1300/1400	4:14 PM	1d 00:26		
ok	PPTP Users	1075 Users	1200/1300	4:14 PM	1d 00:40		
ok	Round Trip Time	1 ms	500/1500	4:13 PM	15d 07:17		
ok	DEC 21143A Traffic In	14709 kb/s	75000/90000	4:09 PM	15d 17:24		
ok	DEC 21143A Traffic Out	5 kb/s	75000/90000	4:13 PM	15d 17:31		
ok	DEC 21143A #2 Traffic Out	16889 kb/s	75000/90000	4:13 PM	15d 17:31		
ok	DEC 21143A #2 Traffic In	4849 kb/s	75000/90000	4:13 PM	15d 17:31		
ok	Packet Loss	0 %	40/60	4:14 PM	15d 17:32		

NetPass Quarantine



Secure Wireless Networking

- Don’t assume the threat is on the outside
- The same Network vs Host Security applies
- Use common sense to guide your strategy
- Be careful of what you wish for
- Monitor, Baseline and Respond

Network vs. Host Security

- It is the same yin yang as wired security
  - Host security Don't assume that just because you are using a TLA (WEP …) that you can rest on your laurels and have loose host security
  - Network security: Just because you have tight security on hosts don't be too lax on the network access/encryption side
- Reality: You have to be cognizant of both

Be Realistic

- Understand where YOU may have vulnerabilities
- Rank the vulnerabilities as to the probability of exploitation
- Determine how much is involved in implementing different aspects of security

Ounce of Prevention?

- Make changes that integrate with the workflow of your organization.
- Don't turn it in to a make work Project!
- Don't make it too painful on yourself or your users as a network that is too hard for the average user to use isn't much good. Balance the "wants" versus "needs"

Evolutionary Security

- Monitor your network!
  - Soft Tools (APMU, MRTG, Stumbler, intermapper, LanSurveyor….)
  - Hard Tools (Yellowjacket, Hornet!, Beetle… from Berkley Varitronics)
- Baseline
  - So you can discern business as usual from problem situations.
- Determine how will you respond ahead of time
  - More than just tactics it involves communicating with your clientele

Questions?

- goolsbee@forest.net
- kohster@northwestern.edu
- sredmond@wellingtoncssb.edu.on.ca