BRIITE-NESS
September 2004
Seattle

OVERVIEW

The next BRIITE will be held in Seattle, WA September 22th – 24th. The Networking, E-mail, Security, and Storage Special Interest Group (BRIITE-NESS SIG), catering to attendees with hands-on responsibilities in these areas, will host sessions in parallel with the main conference.

If you live within OSI Layers 0-7, then BRIITE-NESS is your forum. Like last year, we offer a mix of focused (Security, Network Management Tools) and free-form (Physical Layer Tour and Current Challenges) sessions.

SCHEDULE

Day	Date	Time	Location	Topic
0	Wednesday 9/22/04	9:00am - 10:30am	J3-102	Security at Layers 1-3
0	Wednesday 9/22/04	11:00am - 12:00pm	J3-102	Security at Layers 4-7
0	Wednesday 9/22/04	1:30pm - 3:00pm	J3-102	Physical Layer Tour
0	Wednesday 9/22/04	3:30pm - 5:00pm	J3-102	Network Management Tools
1	Thursday 9/23/04	1:30pm - 3:30pm	J3-102	Physical Layer Tour
1	Thursday 9/23/04	4:00pm - 5:30pm	J3-102	Current Challenges
2	Friday 9/24/04	8:30am – 10:00am	J3-102	Current Challenges
2	Friday 9/24/04	10:00am – 1:00pm	J4-102	Network Analysis Coaching

TOPICS

Security at Layers 1-3

In the age of the worm, compare and contrast strategies for identifying and characterizing what exists on our networks, scanning for vulnerabilities, and disabling the ethernet ports feeding infected machines. How do you find owners for orphaned machines? What steps are you taking toward access control at the port level: authenticating users before they are allowed to connect to the internal network: MAC-based port security, 802.1x, creative use of VLANs? How do you parse the firewall logs; how do you produce reports?

Security at Layers 4-7

How do you handle patching desktops and servers? What steps are you taking to filter malware at the edge (spam handling and virus-scanning on the mail relays, virus and spyware detection at the firewall)? What do you do when users employ Web browsers to read their Hotmail accounts … and thus bypass virus-scanning on your mail relays and post offices? Have you tackled intrusion detection and intrusion prevention? What do you do for incident response?

Physical Layer Tour

Compare notes on network and server installation and management strategies in a hands-on fashion, while touring sample IDFs, MDFs, meet-me rooms, and server rooms. Compare and contrast strategies for organizing and documenting copper and fiber cable plants, rack layouts, cooling, and power distribution. Stare at boxes-with-blinking-lights … and correlate them against FHCRC's Layer 2-3 Network Map. These tours function as a jumping off point for

discussing current challenges in network design, device management, facilities operations, firedrills, wireless deployment, and redundancy testing.

Network Management Tools

FHCRC uses a mix of open source products and in-house Perl scripts to manage our Layer 0 - 3 infrastructure (UPSes, switches, routers), to trend patterns, and to identify both service disruptions and security vulnerabilities. We post many of our in-house tools to http://netops.sourceforge.net – Perl code for monitoring the health of UPSes, for modifying config files & operating systems on switches & routers, for building MRTG config files, for identifying unused Ethernet ports, for analyzing IP space usage. Come see a demo, show off yours, and then brainstorm what comes next. We will show-case Soma, our in-house product which scans our network every few hours, analyzing each station and recording information like location (Ethernet switch/port), guess at OS (from nmap), list of known vulnerabilities (from nessus) … dumps the results into a database … and provides a Web-based reporting front-end. BYOL (Bring Your Own Laptop). [Once you are inside FHCRC's network, point your browser at http://www.fhcrc.org/admin/it/itprof/ and http://www.fhcrc.org/admin/it/vox/itprof for pages illustrating the use of these tools.]

Current Challenges Roundtable

WiFi. Security. VoIP. Managing Internet bandwidth usage, disaster recovery, firedrills, remote access. Storage consolidation: NAS and SAN, Fibre Channel and iSCSI. During the first ten minutes of each session, we'll poll the crowd, brainstorm topics, prioritize them, and then roll.

Network Analysis Coaching

Tired of talking? Tired of theory? Want to get your hands dirty with bits & bytes? Take a break from the rest of BRIITE and get seriously geeky. Twice a month, the Voice/Data Operations group within FHCRC IT hires Mike Pennachi of Network Protocol Specialists (http://www.networkprotocolspecialists.com/) to run a coaching session on trouble-shooting problems in a networked environment. See 'IP VTC Event' and 'Wincati Event' at http://www.skendric.com/packet/ for write-ups on past sessions. During these sessions, hands-on staff from around the Center will plug in their laptops, fire up copies of free utilities (Ethereal, iPerf, QCheck …) and commercial utilities (Sniffer, Surveyor, AppVantage …) and analyze whatever issues are currently hot, diverging as needed to white-board discussions of Ethernet, TCP-IP, and client/server performance issues. Mike teaches workshops at Interop: Troubleshooting Ethernet and Switched Networks (http://www.interop.com/lasvegas2004/conferences/index.php?s=tutorial_detail_fm&sessionid=4309 and Analyzing Application Performance (http://www.interop.com/lasvegas2004/conferences/index.php?s=tutorial_detail_fm&sessionid=4310). BYOL.

LOGISTICS

Mailing List

To stay in touch with the rest of the BRIITE-NESS community, comment on preliminary agendas, and receive late-breaking news, send e-mail to briiteness-request@lists.fhcrc.org, with a blank subject line and a body containing the word "subscribe".

Directions

Consult the following map http://www.fhcrc.org/visitor/maps/slu.html for the layout of our Day Campus (aka South East Lake Union campus). Most locations are in the J Building, also called the Yale Building, and designated as "5" on the above map, though the plenary session is in the Thomas Building (D Building), and the rest of the main conference is in the PHS Building (M Building).

Places to Work, Places to Talk

FHCRC IT offices are on J4 – feel free to drop by and yak with our staff from Desktop Services, Server Operations, and Voice/Data Operations between sessions. An office, a cubicle, and a conference room are available to you throughout your stay as a place where you can jack in, pull out your cell phone, and stay in touch with home.

Office: J4-118
Cubicle: J4-125
Conference Room: J3-506

Questions

For BRIITE-NESS SIG issues:

Stuart Kendrick
J4-120
206-667-6974 voice
206-541-2717 pager
skendric@fhcrc.org

For general BRIITE issues:

Cindy Blattman
206-667-1761 voice
cblattma@fhcrc.org