

Laura Chappell TechEd US Speaking Schedule

Tues 6/10	Wed 6/11	Thurs 6/12	Fri 6/13
4:45 – 6:00p SEC356 Questionable	1:00-2:15 SEC351 NetForensics	10:15a-11:30a SEC364 Case Studies	12:00p-12:45 LUN60 (lunch presso) 2:45-4:00 SEC363 Top 10 Skills
6:00p - ? At some party	6:00p - ? At another party	6:00p - ? At a party she won't remember	6:00p - ? At a party with people she doesn't know after missing her flight home

Hangout Area – the Security Cabana

When Laura is not presenting, she will be hanging out at the Security Cabana. Come visit Laura and her assistant, the infamous Brenda! Make sure you get your Laura's Lab Kit v9 from this area of the show floor as well.

Schedule Changes

We have absolutely no control over the conference (and are still a bit amazed to see Laura even there). Sessions may be moved around to different times or locations. Check the conference schedule and onsite updates regularly.

Heads Up!

This year Laura will be spending a bit more time in the wireless world and demonstrating some of the hottest tools for network forensics, reconnaissance and traceback, network tapping, traffic visualization and reporting!

Session Codes, Titles, Scheduled Times and Abstracts*

LUN60	<p>Hot Tools 2008: Security and Troubleshooting Session Day/Time: 6/13/2008 12:00PM-12:45PM <i>In this session, Laura Chappell lists a variety of tools that every IT professional should consider having in their toolbox. The tools include a decoy and deception honeypot, Bluetooth scanner, wireless scanners, reconnaissance and traceback multifunction tools, penetration testers, host and network forensic examination tools, password crackers, network mappers and more. In this fast-paced presentation, Laura demonstrates many of these tools to highlight their unique capabilities.</i></p>
SEC356	<p>Analyzing Questionable Network Applications Session Day/Time: 6/10/2008 4:45PM-6:00PM <i>So... you are supporting a network filled with users who have their own idea of the purpose of that network, eh? They exchange data using peer-to-peer applications, they talk to their best friends in numerous countries throughout the day and they play addictive MMORP (massive multiplayer online role playing) games. In this session, Laura Chappell examines the various 'special' applications that plague networks today. In addition, Ms. Chappell examines the possible methods to block this type of traffic, if possible. An entertaining and educational session that covers many fascinating topics prompted by our unique blend of network users.</i></p>
SEC363	<p>Top Ten Analysis Skills for Troubleshooting and Securing Your Network Session Day/Time: 6/13/2008 2:45PM-4:00PM <i>troubleshoot and secure their network. It covers wired and wireless tap-in methods, usage of the "not my MAC" filter for application baselining and analysis, advanced display filtering techniques, data reassembly and decryption methods, unattended capture configurations, command-line capture and trace file manipulation, expert analysis and code reviews and advanced graphing. In this session, Laura Chappell demonstrates many of the hottest techniques for identifying network faults and security breaches.</i></p>
SEC351	<p>Network Forensics: Reconnaissance and Attack Traffic Patterns Session Day/Time: 6/11/2008 1:00PM-2:15PM <i>After providing a brief example of host forensics using the infamous BTK serial murderer case, Laura Chappell uses all new evidence files to perform network forensics on reconnaissance processes as an attacker identifies target systems and target resources. In addition, Laura peruses through trace files from compromised systems to identify the signature of the attacks and breaches, and she provides signature resources for other types of attacks and reconnaissance processes.</i></p>
SEC364	<p>Case Studies: Identifying Compromised Hosts Session Day/Time: 6/12/2008 10:15AM-11:30AM <i>In this session, Laura Chappell examines network traffic patterns that indicate possible problems—including phone-home application traffic, IRC backchannels over standard and non-standard ports, tftp data transfers, excessive connection attempts, unusual protocols, and illegal packet structures. In this session, Laura defines normal network traffic patterns and explains what this suspicious traffic may indicate—a compromised system, reconnaissance, attack, or other abnormal situation.</i></p>

* Check the conference guides and onsite updates to locate rooms and verify presentation times.