CHAPPELL UNIVERSITY

Insider Tips

Wireshark in Cybersecurity Training

Laura Chappell, Founder, Chappell University, WCNA Certification Program, Author, Speaker

Please connect to me on LinkedIn. -Laura


https://www.linkedin.com/in/chappelllaura/


https://twitter.com/laurachappell


https://www.facebook.com/laurachappell

Laura Chappell, Wireshark guru and leading cybercrime instructor shares numerous tips focused on using Wireshark to detect network breaches and provide students with exercises to learn network forensics. Laura will also give a sneak preview of the upcoming CORE-IT free training event that provides interactive cybersecurity training for faculty, students, and professionals.

Notes from THE ICT EDUCATOR WEBINAR SERIES (February 7, 2020) https://ictdmsector.org/educator-webinars/

1. Wireshark is considered a top tool for cybersecurity work. (https://wireshark.org) For coding students, you can browse the code on Github [Develop | Browse the Code > epan > dissectors]
2. Students need to know the protocols well. What is normal? [Demo: Chrome and google.com behavior] One of the biggest problems these days is that most traffic is encrypted (we will get to that in #6!].
   Free TCP Protocol Poster is available at:
   https://www.chappell-university.com/post/free-tcp-analysis-poster
3. Grab my trace files ("sec-*" are security-related files)
   Access to trace files:
   a. FTP Access – wiresharktraces.com [look for annotations]
      Username: traces@wiresharktraces.com
      Password: wireshark2020
   b. https://www.netresec.com/?page=PcapFiles
   c. https://pcapr.net/home
4. Annotate your trace files for your students! [Demo: sec-getsplendid.pcapng]

5. To show all elements of behavior, clear cache before capturing (arp -d, ipconfig /flushdns, browser flush cache)
6. Decrypt SSL/TLS traffic (using the client pre-master secret key) (RSA/Diffie-Hellman)
   [Demo: Windows sslkeylog file setup and use]
   Great Links with Environment Variable Setup Instructions:
   https://support.f5.com/csp/article/K50557518#OnMac
   https://support.f5.com/csp/article/K50557518#OnLinux
   https://support.f5.com/csp/article/K50557518#OnWindows
7. Decrypt SSL/TLS traffic (using the RSA key), Extract Session Key, Embed Session Key
   Step-by-step instructions on applying an RSA key in Wireshark are available on the *Network Forensics Cheat Sheet* which is available at:
   https://www.chappell-university.com/post/network-forensics-cheat-sheet
8. Access to scenarios.
   a. https://www.malware-traffic-analysis.net/ - Brad Duncan
      Palo Alto Networks – Unit 42 [password: infected]
   b. https://digitalcorpora.org/corpora/scenarios
      Solutions are only available to faculty at accredited institutions and to trainers within the US Government. [Demo: Windows Nitroba Harassment Case]
      Solutions Request Form: https://digitalcorpora.org/contact
9. Other tools of interest
   a. Nmap (https://nmap.org) - scanner
   b. NetScanTools (https://www.netscantools.com/) – scanner/online investigation
   c. Autopsy (https://www.sleuthkit.org/) – host forensic analyzer
   d. TraceWrangler (https://www.tracewrangler.com) – trace file sanitizer
   e. Security Onion (https://securityonion.net) – collection of tools
   f. Tor (https://www.torproject.org) – anonymizing browser
   g. Zeek (https://www.zeek.org) – network security monitor
   h. Kismet (https://www.kismetwireless.net) – WLAN detector/sniffer

Invitation to CORE-IT (Free Virtual Conference)

Please accept my invitation to join me and many of my industry friends online March 24-30th at CORE-IT.

CORE-IT is a **free** virtual conference that will bring together existing and next-generation industry talent with top-level training, trainers, mentors, companies, products, and opportunities. On March 24th, speakers and mentors will be online during the sessions. All sessions will be available on demand through March 30th.

March 24-30th: Register today at https://engagez.net/coreit1

Access to free training on the tools, protocols, and sessions covering best-practices.

Speakers
Laura Chappell, Founder of Chappell University
Sake Blok, Wireshark Core Developer
Andrew Lewman, Co-Creator of Tor
Mike Kershaw, Creator of Kismet
Doug Burks, Creator of Security Onion
Tony Fortunato, Network Analyst with NATO Top Secret Clearance
Jasper Bongertz, Creator of TraceWrangler
Kirk Thomas, Creator of NetScanTools
Betty DuBois, Wireshark Instructor/Analyst
Mike Pennacchi, Analyst/Instructor/Performance Testing
Terry Cutler, Pen Tester, Cyology Labs CEO
… and more

Thirty sessions focused on core tools, protocols, and best practices. Visit the vendors in the Exhibit Hall (including the High Technology Crime Investigation Association), take quizzes to achieve Open Badges, and network with speakers, mentors, professionals, and peers in the Chat Lounge.

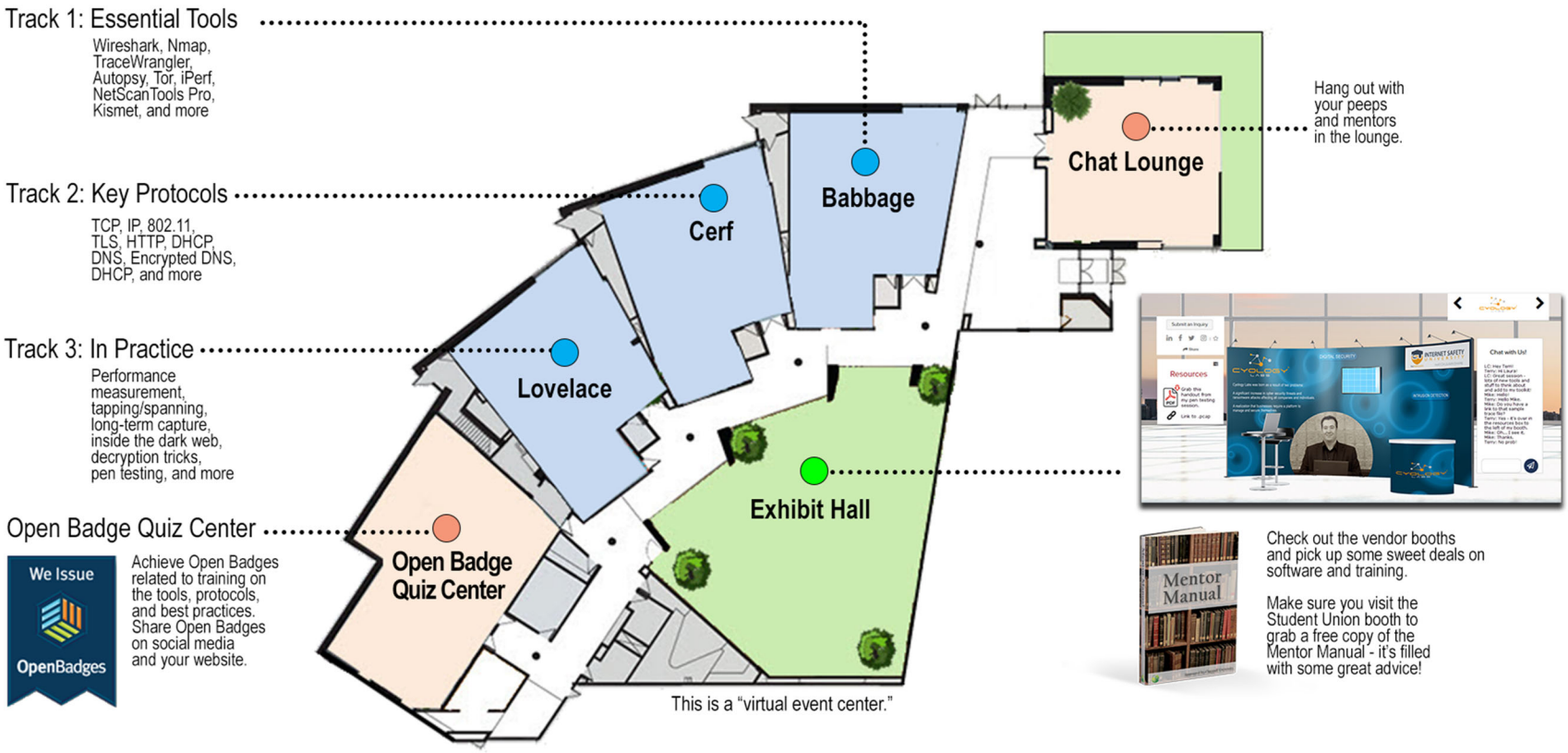
Please forward this invitation along to your students and any faculty members who may be interested in joining us.

Questions? Feel free to reach me at laura@chappellU.com.

Cheers!

CORE-IT VIRTUAL EVENT CENTER

Register for free at engagez.net/coreit1



FREE Virtual Conference covering core tools, protocols, and practices for IT/cyber specialists.

Thirty sessions focused on core tools, protocols, and best practices. Visit the vendors in the Exhibit Hall (including the High Technology Crime Investigation Association), take quizzes to achieve Open Badges, and network with speakers, mentors, professionals, and peers in the Chat Lounge.

March 24-30th: Register today at https://engagez.net/coreit1