

Review: SANS SEC 617 - Surely You're Joking, Mr. Wright!

This review is long overdue. My apologies to EH-Net readers, SANS and especially Joshua Wright, developer and instructor of SEC 617 - Wireless Ethical Hacking, Penetration Testing, and Defenses. Its lateness is more due to my inability to comprehend exactly what I experienced than to a lack of desire to complete the task. I honestly sat down at the keyboard multiple times, but each time I felt I wasn't doing the course or Mr. Wright justice. OK… so like every other SANS course, it had quality courseware, the instructor was top-notch, and I walked away with much more knowledge than when I arrived. So I could simply state the above sentence, report on each and every day of the course offering endless details, recommend it to the masses and be done with my job. But even that felt like empty rhetoric.

As with the review of SANS 560 – Network Pen Testing and Ethical Hacking entitled "Ed Skoudis and the Pen Testing Factory," and many other articles, I felt the writer's need to have a theme. And it doesn't have to be a movie, but something that weaves a thread through the words to keep the reader engaged. Just the right connection or idea can make all the difference in the world. And as many do when faced with writer's block, I let it sit for a while knowing that inspiration would hit me when not looking. But even with pressure and anxiety to produce, it wasn't coming. Forcing it made for poor results. Suddenly during the minutia of daily life, a bright red spine from one of many bookshelves in my basement caught my eye. I had found my theme.

del.icio.us

Discuss in Forums {mos_smf_discuss:Editor-In-Chief}

SANS vLive! Security 617: Wireless Ethical Hacking, Penetration Testing, and Defenses

Tuesday, April 19, 2011 - Thursday, May 26, 2011

<https://www.sans.org/info/71593>

Get Free MetaGeek Wi-Spy DBx (\$599) with Code WISPY_EH

The red spine was from an audio CD Boxed Set from Nobel Prize winning physicist, Richard Feynman, entitled, "Six Easy Pieces: Essentials Of Physics By Its Most Brilliant Teacher," a tiny sampling of lectures from his acclaimed 2-year course, Lectures on Physics, delivered from 1961 to 1963 at the California Institute of Technology (And for you physics buffs out there, check out "Six Not-So-Easy Pieces"). Although he clearly excelled in his field, it was his irreverent teaching style and an unbridled ability to awaken a passion in his students that made him beloved. With his thick Long Island accent in full glory, Mr. Feynman found a particular joy in shaping the minds of those who might follow in his footsteps. In addition to opening the exciting world of physics to undergrad students, he also imparted the virtues of being a scientist and the wonder of doing research. After weeks of digesting my experience with Mr. Wright, there is no better comparison.

It all started out innocently enough. EH-Net had arranged with SANS to do reviews of their three course offerings in the ethical hacking space (560 mentioned above. Read Ryan Linn's Review of 542 - Web App Penetration Testing and Ethical Hacking). I had actually assigned this review to another columnist, but scheduling conflicts couldn't be avoided. With limited options, I had no choice but to accept the assignment myself. And why not? Spend a week in Florida playing around with some wireless toys with one of the best wireless hackers. No brainer.

The beginning of Day One, Wireless Architecture and Analysis, gently pulled us into the wireless world. Josh made his introductions to the course and himself. Knowing of Josh before the course and the teasers of what we were to do in this 6-day course, I started to get a little energized. He covered the basics of wireless threats and the misconceptions of many IT professionals and their management. He covered a few quick case studies such as TJX and what worse-case scenarios in the real-world truly look like. From the corporate world, we moved over to the home user, and how this can easily turn into serious privacy issues. It was a great entry-point into the class with some sexy teasers of what was to come.

After the energy build-up of the brief introductions and the eagerness by all of getting the SWAT Kits (wireless toys for the next four days of hands-on labs), we unfortunately moved into the foundational material. Before we get to the commentary, let's at least go over what was covered. First up was RF Fundamentals which included basic definitions, RF Math and types of antenna. Then we went into Physical Layer Transmission Technology with overviews of FHSS, DSSS, OFDM, MIMO, etc. Then we moved onto a huge section on Wireless LAN Organizations and Standards with information on the FCC, IETF, the Wi-Fi Alliance, OSI Model implications, standards such as WEP, WPA, WPA2, RADIUS, EAP and eventually through the alphabet soup which is 802.11.

Now this is an area for which there is much debate among the SANS course developers and many of the students (and reviewers). In short, my contention is that for 500-level and 600-level courses (not just the wireless class), the inclusion of foundational material is a waste of a day or at least a portion of a day. But let's see both sides of the argument.

The course developers claim that one never knows who is going to be in the class and what their level of knowledge is. I'm sure SANS as well as many other training organizations have companies send people to training expecting them to learn everything there is to know about a particular topic. Time constraints by everyone at home and at work mean that most will not prepare in advance of taking intense multiple day courses. Also, if they don't make sure everyone is on the same page with the foundational material, then it might adversely affect the entire class's ability to comprehend the heavier material and progress properly through the course schedule. All valid arguments.

On the other side of the coin, some of us feel that it's not too much to ask for students to be expected to have a certain base of knowledge before attending a highly technical class, especially ones with the expertise that SANS offers. I can understand the argument if it was something like SEC 401 – Security Essentials, but for 500-level+ courses, one should teach to the highest level of the class and not the lowest. In talking to a number of people who have done training in the past, I'm not the only one who studies up on the topics to be covered without being asked by the training organization to do so. SANS could even make some money by offering Amazon links to suggested materials before the class. Even a simple link to the introductory slides, even if it's only a few days in advance, would allow the class to get to the meat of the course much more quickly. As an additional point, in these tough economic times when budgets for training and travel are cut if not eliminated, maybe cutting the class to 5 days would make SANS events more affordable and thus increase overall attendance.

Imagine how exciting Day One would have been to have the energetic intro and then move right into the visceral effect of having wireless hacking tools in the palms of your hands. That's what it was like during the last part of Day One, when we all couldn't wait to get back to the classroom to start playing with the SWAT Kit AKA SANS Wireless Auditing Toolkit. SWAT is a carefully compiled set of hardware and software that not only gives the students all of the tools needed for the hands-on portions of the course, but it is also completely plug-and-play with the custom version of BackTrack also included in the kit. The hardware included the AirPcap Tx USB adapter, a Zoom Bluetooth dongle, and the TripNav USB GPS device. The software as mentioned above was a customized version of BackTrack that includes all the drivers for the hardware pre-installed and all of the tools and lab files used in the course. There were also instructions given to move all of the contents of the bootable CD to your own USB drive for persistent sessions.

The rest of Day One was dedicated to getting the lab environment setup on your own laptops before the hard core sections of the next four days. To make sure the hardware was in working order given the variety of systems students may have, we completed the day by using the hardware during hands-on sniffing of wireless traffic. The lecture portion included the basics of sniffing and the tools to be used such as Tcpdump, Wireshark and Kismet. This was a good primer in how Josh would be conducting class. Intermixed in every lecture were hands-on demonstrations where the students got to play along on their own machines. There was also time dedicated to our own lab work after the lectures. This marks one of the brightest areas of the entire course. Not only did we have plenty of labs and time for hands-on work, but Josh was there before, during and after class to help with any issues or answer questions on the spot.

This is what makes the next four days, Hands On – Parts 1 – 4: Wireless Security Exposed, very easy to review. Lecture, real-world examples and exercises while lecturing, lab time, rinse & repeat. It was what everyone wanted in a class by the wireless expert Joshua Wright, and that's what they got… in spades. In fact, there is a 250+ Page Workbook with all lab exercises in addition to the six daily volumes normally given to SANS students. That alone shows how the hands-on portions are seminal to the philosophy of the past and ongoing development of the entire course. So let's just breeze by some of the topics covered in such detail and aplomb that even protocol authors would be envious (in no particular order):

- * Auditing Wireless Networks
- * Identifying, Locating and Defeating Rogue APs
- * Hotspot Networks
- * Cisco LEAP Networks
- * Wireless MAN Environments
- * Attacking Wireless Client Systems
- * Cracking WEP
- * WPA-PSK Networks
- * Assessing PEAP+WPA
- * Denial of Service Attacks
- * Fuzzing Attacks
- * Hacking Bluetooth
- * Other Wireless attacks including remotes, keyboards, baby monitors, cellular networks, etc.

And the list just went on and on, and even included blended attacks some of which can be seen in Josh's webcast series, The Pen Testing Perfect Storm, with the other two ethical hacking instructors from SANS, Ed Skoudis and Kevin Johnson.

The general process of going through each wireless technology was that Josh would introduce the topic, go through the protocol specs literally bit-by-bit (and all from memory I might add), point out weaknesses, introduce tools to get the job done (often written by Josh himself), and end with hands-on exercises for students to do what he just discussed. And it was in these four days where Josh truly shined. He got so excited about the material he couldn't contain himself. He often got loud, animated, bumped into the tables and the projector, turned off the microphone recording the course to share secrets, and had stories of his own experiences to punctuate each area of the course. Again I'm reminded of our wily physicist in his famous tome, "Surely You're Joking, Mr. Feynman!", where he recounts his life not in a linear fashion, but rather illustrating who he is as a person by sharing his experiences with selected stories from an accomplished life. As Josh waxed on, he was like a kid during the holidays not able to wait to show off all of his toys to his friends. But it was even better than that, because he actually took the time to figure out what the toys could do before telling the masses. That way everyone could do the cool things he could do as well. That's part of the fun of a Josh course.

Speaking of some interesting asides when attending a Josh course, there are a couple of extra-curricular events. The first one was the Rogue AP Hunt. Now this is actually part of the standard class. Based on what was learned on Day 2 utilizing the SWAT, students on their own or in teams were sent on a quest to find three APs hidden somewhere on the grounds of the sprawling Dolphin Hotel. My family was also in town, and it just so happened that was the night I had scheduled to be with them. Luckily it was an optional task. I did however try to hunt down one of the APs using a tool introduced to me in the class. WiFiFoFum2 is a Windows Mobile application that seeks out APs and plots them on a makeshift radar screen. Since it only goes by signal strength, it clearly can't make a directional guess as to the

location of the AP. It nonetheless looks cool. So while waiting to be picked up in front of the hotel, I turned on my phone, popped up WiFiFum, and lo and behold, one of the hidden APs blipped onto my screen. I had a few minutes, so I decided to take a stroll. I eventually found what I thought was a perfect hiding place – a trash can next to an outdoor power outlet in a landscaped island in the middle of the parking lot. Bingo!! I walked over to it, poked my head into the can, and was promptly greeted by rats who looked up at me as to say, “Hey. You mind? I’m trying to have some dinner over here.”

Another evening activity (this one presumably reserved for the annual SANS 20xx event), was Full Contact Mini-Golf. Now we’re a bunch of geeks, so it’s not really full contact with each other, but rather full contact with the golf ball. Here’s an example. As long as the ball is still moving, additional taps with the putter are not counted as extra strokes. Golf balls in water traps are encouraged, because most of the fun is in the retrieval of said ball. And my personal favorite is the use of the putter as a pool cue. One extra-curricular activity for educational purposes, the other for comradery; both just added to the many layers of 617.

Before skipping ahead to the final day, there is one set of comments that needs to be made, and I’m not sure where to put. So this is just as good a place as any. The tool that was easily the most used in this course is Wireshark (NOTE: Although v1.x was used in class, v1.2 was released on June 15, 2009). Although Josh’s ease with of a number of tools was evident, it was his abilities with Wireshark that left me thinking that I was also attending a master class on the popular network protocol analyzer. Not only is it an invaluable tool for analyzing wireless packets for pen testing purposes, but it can reveal the underworld of the wired network world, too. Truly impressive and incredibly useful for all aspects of network administration and security. He even went the extra mile in creating a Cheat Sheet for the students not only with the most commonly used filters in Wireshark but also helpful hints and command line reminders for most of the tools used in the class. Thanks Josh.

So here it is, the final day, Wireless Security Strategies and Implementation. This was unfortunately another day that was a little disappointing to me. It started off strong with Wireless IDS Technology. Josh adequately covered what it is, how it is done, the major players in the space and evasion techniques. He also included some sample cases with packet captures to see if we could identify attacks from legitimate traffic. This was great from a cumulative standpoint, as we had to take a bunch of what we learned throughout the week and spot the hack. This was almost like a philosophical Capture the Flag (CtF) exercise. The lack of a real CtF as the other Ethical Hacking courses from SANS have on their last day was disappointing. However I completely understand the difficulty in creating an effective CtF without interfering with legitimate wireless devices at the host hotel, other classrooms, hotel guests and students. Josh and I joked about a huge, travelling Faraday Cage that would make a CtF possible. He’s a smart guy, I’m sure he’ll figure something out.

But after the IDS portion, the rest of Day 6 left me feeling like this was a course with an identity crisis, or at least one in transition. The reason for this comment is that the next lecture was a lengthy one on Deploying a Certificate Authority. The topic could have been covered by simply stating the benefits of a CA and then pitching the SEC 505 - Securing Windows class by SANS. I just didn’t feel it was necessary for Josh to go through the entire process from installation to implementation of a Windows Server 2003 CA. In all fairness, he did cover OpenSSL on Linux. And in true Josh style, he performed all of the steps live, so we could see it on the big screen. Although I truly understand the importance of such an architecture in today’s enterprise, especially when it comes to wireless security, it just seemed out of place after days of hacking.

We completed the day and thus the course with Configuring and Auditing Access Points. Seems like a great place to end, with recommendations on how to at least attempt to avoid the attacks so impressively shown by Josh in Days 2 – 5. I say ‘attempt’ because I feel that Josh’s strengths are greater in the attack phase. Or at least his enthusiasm for teaching attacking was greater. Either way, it just ended there, and therefore seemed to lack an exclamation mark on the course and thus felt almost anti-climactic.

And this is how I left the class. Questioning its identity. I understand that the title has changed to fit in with the other 2 new courses by SANS dealing with ethical hacking, but has that lent itself more to its identity crisis? Let's look again at its current title for some clues, "SEC 617 - Wireless Ethical Hacking, Penetration Testing, and Defenses." Is it a pen testing class? If so, then we definitely didn't need the last day. Is it a 600-level class? The middle 4 days sure felt like it, but the other 2 not so much. Is it a course on defenses? We covered methods of defending against each attack performed on Days 2 - 5, but did having the word in the title itself make them feel like they should keep Day 6? Would splitting it up like the network pen testing side into Incident Handling for one class and then another completely separate class for pen testing be the answer? Is there a large enough wireless audience to fill two classes?

Maybe this was one of the reasons I had a hard time compiling my thoughts into an article with a single thread, because this class has multiple threads. Wireless technologies are not like the wired world with only one dominant set of protocols, TCP/IP. Wireless has a multitude of protocols, all seemingly memorized by Mr. Wright. Or is it simply that even with the small issues I had with portions of two days, I am grabbed by the wonder of a wave and how it can transmit data? Josh's ability to visualize that wave and how it can be bent to his will? His need to look at each specification and ask, "What if?" His drive to take that "what if" and turn it into idea and eventually a tool that he freely shares with the community? The simple answer is yes to all of them. This is a strange course in that the farther away it gets, the more I realize how much of it stuck with me. Ever since leaving Orlando, I simply can't help myself from popping up Kismet just to see what's out there, or peaking underneath wireless devices to see what gems the manufacturer or even the user left for me. I even hear Josh's voice in my head with his New England accent guiding me on what to do next. That is the sign of a truly unique class and a talented instructor.

So in the final analysis, the cost of this wireless course is worth every penny. Suffice it to say that any criticism of some of the small details throughout the course are completely outweighed by the four days of "Wireless Security Exposed," and exposed they were. From Wi-Fi to cellular, encryption to proprietary protocols, popular tools to pure research, this course had it all. It's an eye-opening week into just how pervasive, inherently insecure and ultimately scary our wireless world is, especially through the eyes of Wright the Wireless Wizard.

Wireless is everywhere. And industry powerhouses make sure that this is so by basically encouraging deployment in almost any scenario with every type of wireless technology available today. They also do their best to make it "easy" for everyone, including click-happy grandmothers. This is where the vast knowledge of Joshua Wright comes into play. Where systems, especially wireless, tip too far toward the "easy" side of the equation, security issues inevitably increase. Like Mr. Feynman in the area of physics, Mr. Wright brings vast knowledge of everything wireless, passion for the topic, and irreverence in teaching to SANS 617. That combination awoke a passion in this humble reviewer, one I didn't even know was there. I'm confident it can do the same for you.

Donald C. Donzal

Editor-In-Chief

The Ethical Hacker Network