Summary:

While working for Network Associates (now McAfee/Intel/NetScout) as a Senior Systems Engineer, Aaron Janssen facilitated a series of Red Team workshops, social engineering presentations and 'rogue' 802.11 AP demonstrations that ultimately led Sandia National Laboratories (DoE) to purchase a $6 million Sniffer Pro license covering the entire top-secret facility.

Background:

Sandia National Labs is one of the most technically sophisticated customers in the entire world, as a primary Department of Energy facility they have been involved in everything from developing nuclear weapons, homeland security surveillance and even researching Star Wars systems.

Their Red Team wanted to understand what security risks were associated with the development and introduction of 802.11 technologies inside and in proximity to the lab's boundaries. The Red Team needed to articulate these threats to their management, who would in turn disseminate this information to the wider DoD, national intelligence and allied military audiences. Red Team technical approval was essential to authorizing the purchase of any network monitoring or security appliances.

Strategy:

Working with internal SNL coaches and champions, I developed a comprehensive campaign approach that combined hacker role playing, real-world WEP demonstrations and detailed design solutions of cutting edge beta gear. I brought in Product Line Managers for NPO, Visualizer, proto-Infinistream plus the first 10 GB analyzer in history (Sniffer Book Ultra). Ultimately, I created an overlapping universal distributed coverage solution that protected SNL's perimeter from unauthorized Wi-Fi and equipped the guards to be able to monitor the parking lots and exterior public areas for mobile rouge access points.

Tactics:

I had countless round table discussions, whiteboard sessions and escalating presentations leading to a single combined event where I explained the entire integrated system to senior DoE decision makers. Sniffer Pro Wireless version 4.7 had not been released but I was able to successfully demonstrate how I could combine existing and beta products together to provide the security Sandia National Labs needed.

- Social engineering role playing consisted of a tool belt, hard hat and other gear to simulate a 'telco' worker's successful penetration of an adjacent multi-story building's MDF. I showed how to install Omni and uni-directional antennas to stationary rogue APs I had hidden in my toolbox.
- The next step was presenting how to conduct a traditional backpack attack, in addition I used an attaché case with an 802.11 AP, honeypot laptop and battery pack. I also cut a small hole in the case which allowed me to extend the power supply and long black Ethernet cable, this non-descript dark briefcase was completely overlooked until I triangulated its position later.
- My talk and collaboration seminar with the dozens of threat engineers / managers of NSA, DoE, DoD and other classified customers was an in-depth WEP related discussion. We covered the ability to detect rogue wireless NICs, MAC spoofing APs and a variety of other topics.
- I then showed the attendees how to use the laptop's RF signal strength meter to provide rudimentary hot / cold, single axis detection to the stationary 802.11 access points I had set up

previously. I then explained how switching to non-standard Wi-Fi channels and detecting non broadcasting SSID could allow two Sniffer Pro wireless laptops to provide triangulation to the previously unknown hostile backpack and briefcase. The excitement kept building in the room.

- At the time PDAs were new and the Compaq iPAQ was being developed/alpha tested as a lower layer analyzer called Sniffer Wireless Portable Analyzer (SWPA). I obtained several iPAQs with SWPA, earlier I had fully trained my champions and during the show, we provided previously identified key VIP decision makers the chance to hunt down their own 'rogue' Access Points.
- This was the precise moment when the entire room got even more energized! I had also used Velcro tape to mount 10 micro Access Points with small battery packs under the tables and around the room with the names of the division / leaders in the SSID or labeled on the hardware. It became a race for each team to find the other intruder and defend their side.
- I provided the critical third axis of detection, some of the APs were deployed high up and the attendees could see how if they equipped their guard and recon teams with SWPA they could have complete coverage. They instantly started formulating plans on how to accomplish goals.

Outcome:

As a direct result, Sandia National Laboratories purchased a complete site license of Sniffer Pro, millions of dollars in Distributed Sniffer equipment and hundreds of thousands of dollars in professional services. The total of the entire deal as well over $6,000,000, however it was worth far more to the company because I cemented Network Associates/McAfee product lines into SNL's future. The combined revenue generated over the years (this was 2001) with the integration of PGP, McAfee, Infinistream and other related solutions is easily in the tens of millions of dollars.

I later used my Sandia National Labs presentation slide deck as inspiration when I was honored to win the McAfee Sales Engineering presentation contest.

Notable:

The largest audience I have spoken to was estimated at over 1500 attendees, I was the primary presenter at a global computer science teachers' convention in Monterey, Mexico. In 1994, I designed the Wide Area Network for Albuquerque Public Schools and pioneered video conferencing education via a program called CU-See-Me. The IEAERN conference was sponsored by the Mexican telecommunications industry so we had dozens of schools participating from all over the world.

On 3 massive 30' auditorium projector screens I facilitated a multi-lingual (with translation help) discussion on how internet technology would forever change the path of education and future society.

Conclusion:

I'm able to easily explain detailed technical issues, be clearly understood within all management levels of an organization and by the entire diversity of company personnel. I'm experienced and persuasive with customers, skilled at delivering the product message with depth and genuine enthusiasm!