Society of Payment Security Professionals - Payment Security Blog

Secure Payments, PCI DSS, Regulatory Compliance Blog

You can hate 'em…but you better respect 'em…

September 22nd, 2009 by cmark Posted in PCI DSS

Long ago...

During my time in the military I learned a few things that have served me will in my position as a business owner, a payment card security practitioner, and a person. One of the things I learned early on is that you may not like the enemy or adversary but it is short sighted to not respect their skills and ability. Respect for skills is not the same as acceptance of their position, morals, or ethics. The US military, and many of our NATO friends are arguably some of the most most powerful militaries the world has known. Regardless, a single motivated individual from an underdeveloped country with a bolt-action rifle has demonstrated an ability to inflict a lot of damage and deserves our respect. We have learned this lesson time and again in places like Vietnam, Somalia, Iraq, and, the Belgian Congo, Afghanistan (both the Russians and the US) and even the American Revolutionary War. Discounting the abilities of a seemingly unsophisticated, under equipped, bumbling foe has resulted in many powerful nations learning very hard lessons. Unfortunately these lessons are counted in the number of soldiers killed. This lesson repeats over and over throughout life.

In much the same vein it is important to not discount the skills and abilities of the data thieves that are currently preying on our industry. We may not like their tactics or their motives, and may abhor their lack of

morals but it is important to acknowledge their expertise and respect their skills. Without an acknowledgement of their expertise, we cannot adequately prepare to defend our environments from these individuals. It is certainly short sighted to discount their abilities or think of them in the abstract. We must understand their mindset, motivations, and tactics. Too often I read articles that are dismissive of the skills and talents of data thieves. Make no mistake, I do not like what they do. But I do respect their skills. I recently read an article in which the author stated definitively that PCI compliance could have prevented Albert Gonzalez from stealing data. Really? Are we to think that Albert Gonzalez can be deterred by a firewall and IDS? It is this type of ignorance and arrogance that will result in companies continuing to be breached.

Recently I have begun focussing on learning more skills in penetration testing and hacking. The deeper I get into the subject, the more I find my self drawing parallels between what a hacker does and my previous role as a sniper. While the tools, and area of operation (AO) are different, the mindset and tactics are oddly similar. My experience also serves as a good example of the need for respect to which I was referring.

Along with the Brits, the Israelis, and a few others the US Marines are arguably some of the most highly trained snipers in the world. The selection process is rigorous and the training is intense. US Marine Scout/Snipers are trained to operate autonomously, in small groups for extended periods of time.

During my time as a sniper, I spent my life crawling through swamps, hills, and woodlands most often at night. I have been bitten by ticks, leeches, spiders and every other type of creepy crawly imaginable. I prayed for cold, rainy nights. While stamina is important, some of the most important lessons I learned were to observe human behavior and look for weaknesses and mistakes. It is invariably the human element that will fail, not the technology. Consider a situation in which my team was tasked with observing a platoon moving through a certain area of operation. By evaluating the terrain on a map, we could determine the 'natural lines of drift' with some accuracy. Many people may not know this but Humans drift toward the path of least resistance. Humans traveling would naturally drift toward these lines. By understanding these drift lines, you can determine where a patrol will move, get ahead of them and intercept their movement. If needing to move through an area in which an observation post is located when is the best time to move? I liked to move at about 4am. Why 4am? Simple. Most soldiers would stay awake for most of the night anticipating something. By 4am, however, they have been awake for hours and the inevitable doubt creeps into their mind. They are getting tired and the cold is setting into their bones. The sun is up in a couple of hours and they are thinking: "If nothing has happened yet, it isn't going to happen and I can get a couple hours of sleep." Bad mistake on their part. All I needed was one small moment of weakness and I was through.

In our battalion the commanding officer would give a 4 day pass to any platoon that caught a sniper team during exercises. While snipers did get caught on occasion, we were successful the vast majority of the time. Why? Obviously training was one aspect, but more importantly was the mental aspect and the discipline. I loved being a sniper and thrived on the visceral thrill and excitement of being able to move undetected among the larger, more well-armed adversary. While the average Marine grunt was focused on his weekend pass or getting hot chow, I had a single, all consuming objective. I was driven and focused on the objective and knew enough about human nature that I could operate effectively without being caught. There is nothing quite like moving within meters of a platoon of Marines undetected and being able to move and operate with near impunity. I was skilled, well trained, and arrogant in my abilities. I felt I was nearly untouchable by the average solider, or Marine. Was I the best sniper in the unit? Absolutely not. In fact, many of my friends have moved on to Tier 1 units, and various government jobs. The point here is that I had better training than the average Marine or Soldier, I was not bound by the Standard Operating Procedures (SOP) of the average infantry unit, and I had greater motivation than the average Marine or Soldier. As importantly, I knew and understood the SOP of the standard infantry unit and could tell you how their observation posts were established, where crew served weapons (machine guns) would be employed, and where patrols would be moving.

As a sniper, I only need one small mistake. I would wait and watch until a unit made a mistake or exposed a vulnerability. To protect against me, a unit had to be nearly perfect. They had to cover all vulnerabilities and make no mistakes. (does this sound familiar?)

Consider someone like Albert Gonzalez or any hacker (white hat or black hat) you may know. Take a visit to Black Hat, Defcon or any other hacker convention. Watch and talk to the people there. You will likely notice the same arrogance and air of superiority I just described. These people share many of the same aspects of the sniper. They operate in small groups or alone. They rely upon stealth and capitalize on mistakes and vulnerabilities. They are more attuned to human behavior than may be immediately apparent. They possess technical skills that are often far superior to those that we have in our own companies. In much the same way that I thrived on the visceral thrill of operating as a sniper, many hackers and data thieves appear to have the same obsession. They are able to operate undetected against a larger, more well-funded adversary. In short, they are more motivated, and skilled than the average security professional. They understand our SOPs and our tactics. To make their job easier, we publish the PCI DSS.

Like the sniper, a good hacker only has to find one vulnerability or wait for one mistake while our companies have to operate nearly perfectly. We have to ensure we have addressed all vulnerabilities and made no mistakes.

So what is the best defense against snipers or hackers? Quit simply, other snipers or hackers. US sniper doctrine states that the best defense against a sniper is another sniper. They possess the same skills, and mentality and can counter the snipers' actions and operations.

I would argue that the best defense against the type of data thief and hacker we are dealing with today is not a static standard similar to the SOP described above, rather it is another skilled hacker that understands the mindset, tactics, and tools of the adversarial data thieves. Only by understanding and respecting the adversary can we develop tactics, and techniques to protect our own environment.

I would encourage all security professionals to learn more about penetration testing and hacking. If you really want to have a humbling experience, hire a good white hat hacker to conduct a penetration test on your network. I can say that I have had a chance to see DJ Vogel from 403Labs in action and it is truly a humbling experience to have your own work ripped to shreds in a penetration test. While painful at the time, it makes you a better security professional if you learn from the experience.

Do not mistake my post for admiration of data thieves. I do not like or support what data thieves and black hat hackers stand for or the methods they employ. I do, however, have respect for their skills and capabilities.

Sorry, comments for this entry are closed at this time.

- Infosec Podcast
- IT Security in Europe
- Michael Santarcangelo
- Network Security Blog
- Payment Card Security & IT Controls Explained
- PCI Podcasts
- Security Convergence Blog
- Society of Payment Security Professionals (SPSP)
- Zen Dzign

Forums

- Certification
- Facebook Group
- Forum
- PCI Podcasts
- Society of Payment Security Professionals (SPSP)

Categories

- Approved Scanning Vendor
- Asia-Pacific
- ATM
- Audit log
- Banking
- Card Brands
- Chip PIN
- Compensating Controls
- Compliance
- Conferences
- Contactless
- Credit Card Fraud
- Database
- Encryption
- Europe
- Government
- Legislation
- Merchant
- pa-dss
- Payment Applications
- PCI DIY
- PCI DSS
- PCI PIN
- PCI SSC
- Podcast
- Point of Sale
- QSA
- Service Provider
- Society of Payment Security Professionals
- SPSP

- Third-Parties
- Uncategorized
- Vendors
- Web Applications
- Wireless

- **Society of Payment Security Professionals - Payment Security Blog**

  - No Future Posts