ZD Net fighting back against Anonymous, LulzSec and the global cyber insurgency (6.20.12)

One of the system administrators had come to me to show me that there was someone in one of our new servers. We had just returned from the first Linux conference in North Carolina and had installed a new distribution of Linux on one of our systems.

It was the late ‘90s. Like many small firms of the day we were excited to try something new, but did not have a sandbox. I recall pulling the network cable and then going to work to ensure that none of the other systems had been compromised. We were lucky, they only had access to the one machine.

We did a reverse look up and found the domain from which the attacking IP had originated, and crossed our fingers that they had not gone through an anonymizer. Again we got lucky and were able to track the IP address to an ISP in Croatia.

The sysadmins at the Croatian ISP did not want to give me the user’s name, understandably. But the intruder was in our system and I told them I just wanted to speak to him; though, honestly, I was not sure what I was going to say, other than, “Stay the hell out of our systems.”

I never did get a hold of the guy, maybe he had caller ID, who knows. We had been attacked through a fairly well-known exploit. It was our bad for not plugging the hole.

The book We Are Anonymous, Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency, by Parmy Olsen reminded me of this as I was reading it over the weekend, a father’s day gift from my eldest.

The way that the online community has assembled itself, organized loosely and opportunistically to hack into various systems — most through exploitation of well-known issues, and other times through social engineering brought back the memories of that attack so long ago.

The majority of the attacks detailed in the books followed a basic pattern of research, identification of the vulnerability, gaining access, discovery, data download, covering tracks, then announcing the exploit on Twitter and making the data available to all through pastebin.com or some other channel.

The book was full of interesting personalities who you rooted for but knew would be caught. It was interesting to read about mob psychology amplified by the anonymity that could be found online.

The best approach to securing systems is the same today as it was back in the day, when Kevin Mitnick, at the age of 12 socially engineered his way on to the LA bus system by dumpster diving for transfers and punching his own tickets.

Social engineering is the art of manipulation to gain access to things you ought not have access to. In the book it seemed that many had the art of social manipulation and intimidation down to a science while being technical newbies.

Another basic ploy employed by the hackers was to uncover a password (some which were quite strong) either through social engineering or hacking but once discovered could be used to gain access to many accounts.

So, the hackers would end up ‘owning’ the person: having access to their bank, gaming and social media accounts. Often they would trash the person’s reputation through any number of ways that I’ll let you read about yourself.

The lesson here is that a strong password is not enough: you also need to have different passwords for all of your online accounts. The recent LinkedIn breach is a good case for this, many experienced a breach of several accounts as a result of the LinkedIn hack.

Lastly, I was amazed in reading the book that there were so many high profile sites that were so easily breached through well-known vulnerabilities. A preferred method was SQL Injection, where a hacker passes SQL statements directly to the server instead of a search string, for example, and gains access to the server and everything on it.

The lesson here is this: patch your servers and be diligent in the monitoring of your systems! It is not enough to install the tools. Make certain that they are configured properly and employed correctly.

Be diligent, and remember: they are Anonymous. They are Legion. They do not forgive. Expect them!