

Students in our advanced courses are required to do field testing of the techniques they are learning and are continually surprised at the results. Here's what some of them found

Social Engineering

I decided to take my social engineering assignment and combine it with a trip to the mall. The only targets I chose while there were the cell phone kiosks. The simple request to see the manuals for various phones allowed me to appear to browse the material while actually paying attention to the other customers at the counter.

At one kiosk, a young lady approached the sales rep with questions about her service. I struck up a conversation and asked her what she thought of the model phone she had, and especially the quality of the photos it took. She was very helpful and while extolling the virtues of all the whistles and bells on her phone, promptly opened the phone and entered her unlock code, explaining she had to keep the phone locked in order to prevent her pre-school daughter from making random calls on the phone. Of course I was eagle eyed enough to see the unlock code as she entered it.

I mentioned I would never be able to keep my phone locked because with all the passwords I have to remember, I would have brain overload trying to remember another password. She told me she had experienced the same problem, but had solved it by setting all her passwords to the same thing on all her accounts. I told her that was a good idea, but we have to change our passwords at work monthly. She then told me she worked for an insurance company (she actually told me the name and the office location) and they had to change theirs every month also, but she used the simple expedient of using her first name followed by the digits for the month and year. I thanked her for her advice on the phone and walked away knowing the following information:

1. The password she used on her personal accounts
(her cell phone password)
2. Her first name.
3. Where she worked.
4. The password she used for her work system.

*All of this information was obtained from only a student!!
Just how much more information could have been
acquired if this was a professional thief with the intention of
using the information obtained for malicious purposes!!*

Remote Access

Today, with the beautiful weather we had, I sat on my front porch and was looking to see if I could locate any wireless signals around my house. Lo and behold I found two of them. The SSID on one of them was LINKSYS and the other was NETGEAR. I was able to log onto the LINKSYS network without a problem. They had the SSID broadcasting and the IP address on the router was the default 192.168.1.1. They didn't even bother to change the configuration password from admin. Once inside the configuration page I looked through some of the settings. (Yes, I know that was bad of me but I wanted to prove they did nothing more than hook it up right out of the box.)

I saw they had an e-mail address listed and no security options whatsoever in place. They had no MAC address filtering and had it configured for open access. I also took a look at the activity logs and was able to see that they had recently been on DirecTV.com

There are only two of my neighbors that have DirecTV dishes on their house and are only two houses away, one is across the street.

I was unable to connect to the NETGEAR connection because the signal was too weak. I have a good idea who has the other network because they called me a few months ago and asked me my opinion of the DSL service in the area.

I figured that was enough snooping to see what's out there. I didn't even need to go any further than my front porch to find something.

White Hat Hacking

When I first tried the packet sniffer at work I got about 200 different entrees (no joke) in 32sec. It's funny now to find out that I have been trying to pick out my IP info from the entire network. Not a good thing to know that that much information is broadcast to every computer in the network. Thinking back to the beginning of the class; if you happened upon a business network that someone set up themselves to save money and they didn't bother to change any default password. Well you could give your self a network address and gust set up shop on all the info that's sent back and forth. Not a good thought. I thought hacking into networks would be a lot harder.

(This student acquired permission from his place of employment to do a security audit for this assignment.)