

Bringing the Unsexy Back: The Process of Selling SE Penetration Tests

By Chris Hadnagy

For the past few months, I've brought you articles on launching your career as a social engineer, the psychology and history behind hacking humans and even some scams you can pull on your clients for their own good. As wonderful as it is to talk about the methods, the tricks and the sexy stories of social engineering pwnage, we need to take a step back and discuss the business end of this spectrum.

Yes, I said it… business side. After all, most of us reading this article either are in IT/Security or want to be. So how can one sell SE penetration tests? How can you scope it? Price it? And what do you give the client at the end of the engagement? All of these are good questions for budding professional social engineers, and thus the topic of this month’s column, the process of selling and delivering a social engineering penetration test.

Discuss in Forums {mos_smf_discuss:Hadnagy}

Selling SE

In my career sitting in front of clients trying to sell these services, I have heard everything from, “That won’t work. Our people are smarter than that,” to, “It’s unfair ‘cause it will definitely work,” and just about everything in between. It is no secret that social engineering is not the easiest thing to sell. Why?

Social engineering is plagued by the same problems as standard pentesting. There are loads of people selling their version of social engineering pentests, which normally consists of a few unplanned phishing emails and maybe some very poorly planned calls. A weak report is generated, and, because they are getting success to some extent, companies are still buying this low-end form of social engineering.

Recently I had a chance to have dinner with Sharon Conheady, who in my opinion is one of the top female social engineers out there. We discussed this problem at length and determined we have the same problem. Interestingly enough, when I interviewed Kevin Mitnick on the Social-Engineer.Org Podcast, even he had the same problem. Convincing the client that getting a real, thorough and black box style SE pentest was not an easy task.

After discussing this with Sharon, I feel that the only solution is education. Clients need to be made aware of the threats out there but not by the use of fear mongering. Showing only the scary statistics of how many people get hacked is not really the only solution, but the client needs to hear and see the methods the bad guys are using. This means that the professional social engineering pentester needs to spend time educating themselves, so that they know these facts as well. Once they know these facts they can then relay this information in a professional manner to the client.

Of course this is much easier than it sounds, but the days of using fear to sell pentests should end, as it is not the type of motivation that works with clients. Smart companies will realize that this vector is the easiest and most successful method into their network and will want to hire the best to help them stay secure. In the end, it will simply make more business sense. As a provider of services, affecting their bottom line is a much more positive place to be.

Scoping & Pricing

So you are now armed with a headful of good facts, you know all the methods that the bad guys are using and you are prepared to help the client see the need. They listen to you, discuss their options and decide that they want to move forward. They request a quote. Now what?

The problem that most pentesters may have is just blurting out pricing without many facts. I recommend treating the quoting process like a pentest. 60% of your time should be spent gathering information you can use to truly help the client.

Ask a lot of questions, so you can most efficiently help them find out things like:

- How many people are you testing?
- Do they want just phishing, phone, onsite or a mix of all three?
- Do they have a budget set?
- What are the goals of the pentest for them?
- What is and is not allowed?
- How long do they want the pentest to last?

Understanding all of this can help in scoping out the pentest. After getting these details, what I still find is that most clients won't really know what they want. I find it a good idea to give them a few choices. Option 1 maybe is a very light pentest that will accomplish all their goals but be general. Whereas Option 2 may be more spear attacks mixed with the general options as well as some well-planned phone work. I think you get the picture.

In the end, the client should have a few choices that can help them determine the best way to create a secure environment for their employees.

Deliverables

This one seems obvious, but there is a lot of information that can go here. I will try to keep it as simple as possible. Primarily the report is the main deliverable. Too often, a pentest report is just a massive information dump. This is not only a disservice to our clients, but it doesn't help the client learn how to ward off attacks.

Instead a report should be a concise road map. What was found? How was it found? What worked? What did not? Provide examples of phish or phone scripts used. Screenshots or pictures of vectors that where used.

I always think it is a nice idea to provide audio recordings or video of things that were done. One major caution: in some states and countries it is illegal to do so with out all parties consent, so extreme caution and research is needed before including these.

In the end the client should have a clear picture of what was done, how it was done and what was the most successful method. In addition there should be a nice executive summary in the beginning preferably no longer than one page. Also

one of the most widely overlooked parts of the report is mitigation. We may be a 5-star pentester that has near 100% success ratios, but in the end the client doesn't really need to know all that. They need to know how to patch the holes.

Now Go Sell Something!

Social engineering is the biggest threat and as more and more companies begin to see it, realize it and yes, unfortunately, experience it, SE pentesting will become more readily used. Practice your skills, so you can be an effective and professional SE pentester.

Yes this will take some work and some time, but the rewards outweigh the work. The feeling of helping your clients to learn how to be secure and ward off an SE attack is very rewarding. Remember that true security can only be achieved through education – education of yourself as well as your clients. This is not a fast, overnight process, but it can happen. When it does, you'll be amazed at how well it works.

As usual, I am open to any discussion or suggestions on this topic.

Till next month!

If you have comments or questions – please feel free to reach out to me at logan@social-engineer.org

Chris Hadnagy, aka loganWHD, has been involved with computers and technology for over 14 years. Presently his focus is on the "human" aspect of technology such as social engineering and physical security. Chris has spent time in providing training in many topics around the globe and also has had many articles published in local, national and international magazines and journals. He is also the lead developer of Social-Engineer.Org as well as the author of the best-selling book, Social Engineering: The Art of Human Hacking.

He has launched a line of professional social engineering training and pen testing services at Social-Engineer.Com. His goal is to help companies remain secure by educating them on the methods the "bad guys" use. Analyzing, studying, dissecting then performing the very same attacks used by malicious hackers on some of the most recent attacks (i.e. Sony, HB Gary, LockHeed Martin, etc), Chris is able to help companies stay educated and secure. Chris can be found online at <http://www.social-engineer.org/>, <http://www.social-engineer.com/> and twitter as @humanhacker.