

Social Engineering as a Technical Tool

By Chris Hadnagy

When we speak about social engineering the normal conversation steers away from the technical and more to the psychological. This month we are going to change it up a bit and steer head on into the technical arena for a discussion about penetration testing.

There seems to always be a debate online about pentesting, what it is and what it isn't. How to do it right, how to do it "real world," how to do it hardcore and even l33t. But at the end of the day what each and every pentester wants (or should want) is to uncover the holes in the clients network, so they can be mitigated before the bad guys use those very same holes for malicious purposes.

That desire should drive each "real world" pentester to use every tool - technical or not - at his disposal for the benefit of his clients. This is where our discussion about how to use social engineering as a technical tool or as a tool to get technical details.

Discuss in Forums {mos_smf_discuss:Hadnagy}

Social Engineering in a Pentest

Social Engineering is used in a pentest in a few different ways. First way is as the main part of a pentest either through phishing/web attacks, phone elicitation attacks or in-person/onsite attacks. Each has its own level of difficulty as well as its own layers of social engineering skill involved. Secondly social engineering can be used to facilitate further attacks such as tailgating to get inside a secure area, getting close enough to drop USB keys or using phone elicitation skills to find out details about vendors that is then used to perform phishing or onsite attacks.

But lets focus on another method that social engineering can be used in a pentest: Information Gathering. For privacy sake I cannot disclose who the target was, but I can say that this phase of an attack was discussed by some hacktivist groups. The victim company denied the nature of the attacks, as it would affect their security posture in the market. But lets imagine that this group wanted to attack CompanyA and this company had a SQL database that might be vulnerable to injection. Sure, the hacker could attack the database until it caved or try every SQL statement until they found one that worked. Better yet, they could simply place a call into the database support administrators posing as fellow programmers and working on SQL statements for a new database connection tool.

Each call that was placed used the information from the previous calls to further their knowledge. After six phone calls to multiple different database administrators, the hackers had enough details to create a statement that granted them access to the data they wanted. Result - Compromise!

This is a devastating form of social engineering, one that is not just about gaining access or going in "for the kill" with the first shot. This one utilizes social engineering skills to build upon the attackers knowledge of the inner workings of an organization's IT infrastructure, in effect making the attacker able to appear knowledgeable to a deeper and more knowledgeable crowd. This makes the attacks harder to spot and more devastating when successful.

How to Use This Method on a Pentest

This method should be included on pentests where data is very important. Why not set up a team to have what might be considered public knowledge of certain database protocols or connection statements? From there, see if they can utilize social engineering skills to build upon that knowledge. Once a good base is built, see if they can use that knowledge to launch a full scale attack giving them access to the data that would make the pentester successful.

This means that the pentester would need a diverse team, one that is able to understand, speak and use technical jargon and terms. A team that can speak in the language needed, but also a team that has a skilled social engineer or two on it to know what to ask, how to ask and where to find the numbers and data to make the calls realistic.

Why Go Through the Hassle?

That is a valid question. But why... why go through the trouble of setting up these elaborate kind of pentests? One simple answer - the bad guys are doing it.

In the last 6-10 months with attacks from Anonymous and groups like UGNazi, we are seeing that social engineering is not being used to gain physical access to buildings but to collect data. Data collected is then used to further attacks and make them more successful and quicker without chance of failure.

If the bad guys are spending the time to utilize these attacks, a company that is serious about security should spend the time and money to test, patch and educate on this type of attack. Sure it is easy for me to say this, but I clearly understand that this is not easy to implement. It is hard, expensive, time consuming and maybe even scary. But what are the alternatives?

Really there are two:

1) Hide your head in the sand, pray you never get attacked and if you do then mitigate.

2) Prepare properly (still pray you never get attacked), and know that the proactive steps taken can save the headache and embarrassment of a breach.

Free will is a funny thing, and I am not able to answer for you which option is preferable. I can tell you that I think the answer is obvious.

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.