**Penetration Testing (3): Social Engineering**

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this series of three articles, Mark Fischer <mailto:Mark.Fischer@SecurityGuild.com>, a student in the first cohort of the Norwich University MSIA (Master of Science in Information Assurance) program, has very kindly consented to share one of his essays with readers of this newsletter. The topic in that particular week was penetration tests, and Mr Fischer continues this time with how he and his colleague used social engineering on their client’s personnel.

***

The last part of the pen test was to use social engineering against the employees and IT staff. We had two goals: to social engineer the password from users and to social engineer user passwords from the Help Desk.

* Password From Users *

To get the passwords from the users we took our company phone list to a vacant conference room and began “dialing for dollars.” We spoke to five people, including the CEO’s secretary and the head of the legal department. We said we were consultants working with the Help Desk to rebuild the user database and needed to confirm their user information. The typical conversation went like this:

Us: “Your name is Jane Smith”
Them: “Yes”

Us: “You are on the fifth floor north in the accounting group”
Them: “Yes”

Us: “Your phone extension is 4365”
Them: “Yes”

Us: “Your username is Jsmith and your password is ‘aligator27’”
Them: “No, my password is ‘HappyBunny’”

Us: “Thanks, that must be part of the database that was messed up. Have a good day”

We were able to collect passwords from four of the five people we spoke with. The only exception was a lady, Agnes (her real name!), who said “I have worked here for 27 years and I don’t know you and I’m not going to talk to you on the phone. If you want to talk to me, come to my desk where I can see you” and then hung up the phone. We later learned that she then called Corporate Security to report the incident.

* Passwords From Help Desk *
Our last task was to social engineer user passwords from the Help Desk. To do this we went to a conference room at 4:50 pm. We selected a mid-level manager from the phone list and locked his account by entering three wrong passwords. I called the help desk person who unlocked the password. We deliberately locked the account again and called back. There was a frantic tone in my voice and explained that I still couldn’t get on the system and important people were going to be in the conference room in about three minutes to see my presentation that I could not do because the stupid computer wouldn’t let me in. I know I was typing the right password, but it wasn’t working. The Help Desk person suggested that he could set the password to “password” but I would have to change it as soon as I could. I thanked him and hung up with a grin my face.

* Conclusions and Postscript *

This was an interesting pen test that demonstrates how interlocking good security is. They had good passwords on the domain but we were able to gain access by “daisychaining” from the TESTW2K server. From there we could have gone after the mainframe.

The story of our social engineering was printed in the next employee newsletter and was included as parts of future security training for employees.

The head of IT security later moved to another company and called me up from there to do pen testing and a good deal of other security work for them as well.

We saw Agnes in the restaurant the next day at lunch and sent over a large chocolate sundae to reward her for doing the right thing.

* * *

Mark Fischer < mailto:Mark.Fischer@SecurityGuild.com > is the founder and Managing Director of Security Guild, LLC, an information security consulting company. He is a Certified Information Systems Security Professional (CISSP) and a graduate of the Rochester Institute of Technology. He has been building and breaking systems and networks for more than 15 years.

* * *

For further reading:


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.
