

Forum:[Hack Forums](#)

Thread: [How do I practice Social Engineering?](#)

StinkButt420 - August 31, 2024, 4:36 pm

Right, we all know about TryHackMe, HackTheBox, the actual practice machines we like to do. But one aspect I see discussed a lot, is Social Engineering.

Social Engineering (to my knowledge) is the act of an attacker convincing someone to give sensitive information, such as login credentials, to themselves, in order to further their attack. But it might also be a pet's first name, a common security question for a login. Or maybe your mother's maiden name.

I've heard lots of interesting stories of such method. Such as what Kevin Mitnick did in the 1980s to Motorola. Kevin Mitnick was at one point looking for the source code to the operating system of a Motorola phone he owned. So he decided to take it. He called up Motorola pretending to be an engineer, and actually secured a copy of the source code. Because he was able to convince the low level employee that he was who he said he was.

He even convinced the receptionist to FTP it to him, and taught her how right then and there. I might be getting some things wrong, but that's the long and short of it.

My question is, HOW are we supposed to practice this? You can't just call Microsoft and say "hey can I practice committing a crime against your corporation?" That's the biggest reason HTB and THM has the boxes they do, it's a legal way to ethically practice, and learn CS. But there's no way for a pen tester to really practice SE.

DramaKing - August 31, 2024, 5:09 pm

(Aug 31, 2024 04:36 PM)StinkButt420 Wrote: [\[CITE\]](#) Right, we all know about TryHackMe, HackTheBox, the actual practice machines we like to do. But one aspect I see discussed a lot, is Social Engineering.

Social Engineering (to my knowledge) is the act of an attacker convincing someone to give sensitive information, such as login credentials, to themselves, in order to further their attack. But it might also be a pet's first name, a common security question for a login. Or maybe your mother's maiden name.

I've heard lots of interesting stories of such method. Such as what Kevin Mitnick did in the 1980s to Motorola. Kevin Mitnick was at one point looking for the source code to the operating system of a Motorola phone he owned. So he decided to take it. He called up Motorola pretending to be an engineer, and actually secured a copy of the source code. Because he was able to convince the low level employee that he was who he said he was.

He even convinced the receptionist to FTP it to him, and taught her how right then and there. I might be getting some things wrong, but that's the long and short of it.

My question is, HOW are we supposed to practice this? You can't just call Microsoft and say "hey can I practice committing a crime against your corporation?" That's the biggest reason HTB and

THM has the boxes they do, it's a legal way to ethically practice, and learn CS. But there's no way for a pen tester to really practice SE.

All you can do is learn the theory and see how others have done it.

whisperedone - *August 31, 2024, 8:03 pm*

The best legal way is probably to do customer service or sales work. In sales, you're SE'ing someone into buying a product. In customer service you're doing it to get them to like you and be agreeable. I get tons of practice on the help desk when angry people call in.