

Forum:[Hack Forums](#)

Thread: [Social Engineering vs Vulnerabilities?](#)

pokego709 - July 23, 2017, 4:20 pm

For those of you who do pentesting for a living (or even as a hobby), do you find the most common vulnerabilities are the people or the systems? And if it's the systems is there a usual suspect (software that is always vulnerable)?

The-hunter22 - July 23, 2017, 11:21 pm

From my experience, I find the most vulnerabilities in the software. Here in the Netherlands people are very aware, sometimes they can't handle my charisma but often they just misconfigure a firewall or don't patch their software. That is the most common, in my experience. Once you have a client who is good protected and has good policies for their digital security, then they are so focused on the digital side, that they forget the human side. They don't have strict policies for uncommon things, and you can abuse that during a pentest.

That doesn't mean software isn't getting more secure, it is just that not every company uses the resources to secure itself. They just simply don't patch it, or do it in a wrong way. When they do it right, then the human side is the most vulnerable side.

jamdoughnut - July 24, 2017, 3:10 am

I mainly do work in the UK and I haven't had a Spear Phishing engagement (yet) that didn't come out with at least a 30% success rate. I have had a couple of external tests that haven't resulted in a compromise however almost all internal tests result in some sort of compromise.

Statistically, from my experience, I would have to say that people are more exploitable than software.

JammyD

IIIIII - July 24, 2017, 4:32 am

This all depends on how good you are as a penetration tester, no system is hack proof, and no human is hack proof. They are still finding vulnerable points during fuzzing and large companies and organisations are still getting hacked through social engineering, like NSA or CIA. One big proof in how social engineering is a great method is by thinking like this, how did they get the IP to CIA's office? because someone did a huge mistake, or insider job.

But systems are usually more vulnerable than the people behind the service in my opinion, websites that are done before 2008 are more likely to be vulnerable than websites that were done after 2013 since they didn't think about updating everything in their server

Voget - July 24, 2017, 4:38 am

Can be considered both as: Code can be written poorly == Code written by people. (Code/Software can be designed poorly, but programmers sometimes don't program to the language's full capacity... if you know what I mean).

easy_win - July 25, 2017, 9:31 pm

It depends on what you are trying to do. Larger organizations provide you with a larger number of potential SE targets; increasing your likelihood of success. However, they also have more

money and resources for security teams, appliances and other mitigations. Smaller organizations are more likely to have vulnerable/unpatched software, but might still have limited forward facing infrastructure to attack. Their SE footprint will also be smaller, but provide you more possible avenues (maybe just easier avenues; i.e older or un-administered system) of attack.

Mr_Sploiter - July 26, 2017, 4:02 pm

A Biggest hacks is due to a simple error, it can be human, or from system side .

example: when an update is launched, and a system is not patched, or take some delay to get updated, a hacker can be exploited before it's get patched .

It's a matter of time .

HUMAN side 'SE' is the king of hacking techniques .

SQLInjekt - July 27, 2017, 6:16 pm

almost all attacks are carried out by some form of social engineering. it's a very essential technique to have in your toolbox.

Bouzazi - August 2, 2017, 3:42 am

People often represent the weakest link in the security chain.. -- Bruce Schneier

LegitGuy - August 21, 2017, 10:44 am

A good dev / programmer has to be a good SEngineer, otherwise it will be very hard for any jobs later. When you did a perfect exploit but this one is only detected by one AV, so you'll have to SE your victim, imagine that he or she has the one AV that detects it. It will be very dangerous to try any attack. So you'd better SE to see what AV she or he has, or simply do your job. If SE is too hard for you, try drama lessons ?

Abellaandrew128 - August 22, 2017, 10:20 am

Please, I need a good social engineering . Somebody should Please help me with one.