

Forum:[Hack Forums](#)

Thread: [What do you think is the ultimate *almost guaranteed* way to hack on average.](#)

Mr. Robot - April 28, 2019, 7:25 am

So i've had this discussion in the past, mid tier individually owned companies/websites - I believe are 'almost' always "hackable".

The process I have used in the past for security testing and whatever works and is the following. I would like to hear what you would change or possibly do differently that could be better.

>>Find who owns website/company/service.

>>Hack their home WiFi/Exploit family member who lives there who has access from down the road. Even easier if they have WPS - like hack it every time and most people have it.

>>Escalate privileges and gain access through attacks like MiTM and network escalation.

Now there are other options such as posing as a religious person or if you have information on the target - try gain access to their house with their permission and see if you can record/gain enough time to control a device. Computer technician in some cases.

You could also B&E - lockpick or whatever. That's getting down an entirely different route.

Silent Uprising - April 28, 2019, 7:37 am

MITM attacks on home network always seems like an OP method.

I remember speaking about this with my high school computer security teacher and I told him wouldn't it be possible for anyone to change grades by literally just cracking that teachers house wifi and when they are logging in there account from there house to start updating grades mitm you have their password and can go update it yourself.

Obviously this was a just for fun topic I had with him but it always seemed like really over powered method to me.

IniGo - April 28, 2019, 7:46 am

Getting access to the home network and work from there will be one of the best methods to use, but not always required

Most companies have secretary, who deals with a huge ammount of pdf, doc, xml and so on. A high quality forged document, a business offer for example, or an invoice from one of there partners with a silent exploit is also working very well. There pc will often have access to alot of critical data aswell as a possible line to the ftps, or private networks.

All depends on the company and the situration tho

Mr. Robot - April 28, 2019, 8:05 am

(Apr 28, 2019 07:37 AM)Silent Uprising Wrote: [\[CITE\]](#) MITM attacks on home network always seems like an OP method.

I remember speaking about this with my high school computer security teacher and I told him wouldn't it be possible for anyone to change grades by literally just cracking that teachers house wifi

and when they are logging in there account from there house to start updating grades mitm you have their password and can go update it yourself.

Obviously this was a just for fun topic I had with him but it always seemed like really over powered method to me.

Because most networks have WPS it makes it just that much easier. Once you have access anyway you can always just inject code into their browser on requests and escalate into a shell into a proxy.

(Apr 28, 2019 07:46 AM)IniGo Wrote: [CITE](#) Getting access to the home network and work from there will be one of the best methods to use, but not always required

Most companies have secretary, who deals with a huge ammount of pdf, doc, xml and so on. A high quality forged document, a business offer for example, or an invoice from one of there partners with a silent exploit is also working very well. There pc will often have access to alot of critical data aswell as a possible line to the ftps, or private networks.

All depends on the company and the situration tho

This is also pretty powerful however I would say targeting that employee for their phones wifi network in most cases will be pretty broken.

Psychedelic. - April 28, 2019, 11:51 am

Social engineering, obviously