

Forum:[Hack Forums](#)

Thread: [Tips, steps, and advices on targeted hacking mega thread !](#)

ch1kra - August 2, 2017, 5:09 am

Hello guys and welcom to my first thread on HF ?

- I'm a 22 YO gray hat hacker, I work as a white hat pentester (I'm nice and professional whit everything at work), but like everyone in this forum, I like to have fun with all kind of systems.

- In this post, I'm gonna present my main STEPS on hacking a target, hacking random people is easy, you take a random person, you try things, sometimes it works, sometimes it doesn't, but I don't really care about knowing that a random Bob is cheating on a random Alice, their problem, not mine.

- The main goal of this post, is gathering tips, and advices from all of you, I will keep on updating the main post, for the future ppl to see, I'm not an expert, I'm just putting my advices, and want to gather yours, I will not go into high details ^^.

===== Tips and Advices =====

- Avoid targeting, someone who knows that your passion is hacking, UNLESS, you're 100% sure, that this person will never find out about it.

- Avoid rushing into things, I hate people that just want to " hack " someone in 5 minutes, putting no tough behind it, specially if it's someone you know, hacking a target have some crucial steps, they may be boring for some of you, but they are CRUCIAL if you want to have more chance at succeeding !

- Be organized and methodic, I will present how I do this when i'll be in the main steps, but srsly guys, be methodic, 1 IP bit mistake and you could ruin all the process, and even get greater bad repercussions on your work.

- If the OSINT failes, I advise you to abort mission, you can continue at your own risk, but I like to have a good base befor goin in deep.

===== Steps =====

***** Step 1 : First layer informations scouting (OSINT and/or Doxing)

- I KNOW I KNOW, this step sucks for some of you, I actually like it, it gives you a comprehension about every thing you'll need to know for the next steps, in the first layer informations scouting I will be gathering most informations I'll need about the target, I usually prefer to do it mannualy, Facebook / instagram / google, are my friends, i'll create a power point, (I have my template, you should create your own, does not take time), with tables, forms, and a familly tree, I'll read all the pots on facebook, comments, liked pictures, pictures posted, pages they like, i'll open every page of someone having the same name familly, or someone that comments a lot on everything and seems

close to my target, then i'll go in google for the rest (TIP : don't forget to put the name between quotes on your google search, if you don't it may cause a problem, imagine for example you're searching for " Alice Badaboom", if you don't put quotes, it may provide you a juicy link to some private school informations list about student, you'll be happy, but you'll later find that in the list you'll have " Bob Badaboom, Alice Notttheonewewant " ==> that's a pretty bad ass family name) I'll spend a lot of time in google, searching for everything related to the name of our victim, i'll list everything on the ppt, so now I should have =>

- + A list of lot of informations (Full name, Age, birthday, Born city, high school.....) Even the most USELESS ONE ==> how many cats she/he had or i don't know, the thing she/he always eats when she/he goes to mcdonald's

- + A list of related friends and family, that I Will put on the "family" tree I use

- + Really nice informations I found, but I'm not sure about them being true or not, it seems like it's useless but it's REALLY important, cause sometimes when you link the dots, you'll find new crucial informations (I found a class picture of the victim when she/he were 10 Years old, but can't recognize it, and seems like you'll never need it, keep IT, maybe you'll confirm later that it is your victim, and you'll use it for your final step, and don't think something like < it's ok, i'll find it if i need it >, you should have been spending hours doing this, if you can find back every information in 30 seconds, it means you did a really really bad job)

- + Important events, everything that passed in your victims life, that can be important, graduation pictures, birthdays, first rave, someones death,

That's the organisation I use for step 1, go search for more specific OSINT / Doxing tutorials if you need help on how to do it.

***** Step 2 : Second layer informations scouting (OSINT and/or Doxing)

- This time, it's easier, but it takes time, you can ignore it, but it helps for the next step, when you did the OSINT on your main target, you had the relative facebook accounts and stuff in the family tree, it their time to go through the microscope, avoid doing all of them, would take a lot of time, try to get the close to mid-close ones.

***** Step 3 : What's the best door to chose, and what vehicle ?

- Take your pop corn, shit is getting real, you did the scouting, it's time to do the strategy, it's not a hacking tuto, it's more of an organisation tuto, so i'm not gonna go on details about a way of hacking or something, but you need to chose the best way, so you don't do something stupid that would alert your victim, and make him/her harder to get, you have thousands of ways, thousands of doors thousands of vehicles, most of the doors can't be open, and sometimes, when you try to open one that is closed, your mission can get killed and you'll need to abort, and some vehicles are louder then others, so be carreful on choosing, it's simple as it is, if someone ges the feeling that someones is trying to get hes/her account, he/she would change password to a harder one, and he/she'll be really carreful for sometime, and if he/she knows you're a hacker, and you have a purpose in hacking him/her, he or she would get suspicious of you, so be carreful on choosing the way and the entry.

Door : The way, the entry, the exploit (are you gonna talk to him directly with your account ? a fake account ? email her with a fake account ? physicaly do it ? talk to her friend ? her mom ? send a package at her home with an infected USB ? (I really want to try this one ^^ it should work, someone who don't understand shit, receives a random USB in a nice package, with a mistery love message,

he or she would automatically plug it in))

Vehicle : The weapon, the virus, the payload (RAT ? Meterpreter ? phishing ? Brute force ?)

So here are some tips to chose your best way :

- Consider the level of knowledge of your victim, if the OSINT was good you should know what kind of things your victim likes, per example a hard gamer would certainly some basics about hacking.
- Consider using a weak link, if her brother is 13 years old, he's an easy target, he's curious and just wants some money to get any game he wants, I like taking the weak link path, even if he understand you want to hack him, he'll never link you to the victims friend.
- Consider doing basic " I'M SUCH A HACKER I CRACKED WINZIP LULULULUL HAHAHA " things. Like seriously, REMEMBER THAT PEOPLE ARE DUMB, I had a friend, I tried her full name with her birthday on apple cloud, it worked, went to notes, had all her password list AND HER BEST FRIEND PASSWORD LIST.

- For the vehicle, you need to fully understand how the thing you're going to attack works, per example if you want to hack a facebook, create one, and try everything you can think off, forget password, change password, change email, change phone number, delete email, reput email, desactivate the notifications etc etc, you need to understand the behavior off all the things, [per example, I know that the person can activate security notification whenever someone connects to the acocunt from a new place, so i would never connect until I know the person is assleep, and i will delet the notificaiton cause I know she have the iphone, and that the iphone would delete the notification from the locked screen once I open it and delete it in facebook.] Then depending on your door, choose the best vehicle ?

***** Step 4 : Ready, set, HACK

- You have all the informations you need, You have a good anonymous strategy, it's time to hack, just be organized, write down the infromations you'll use, write down the steps you did on a paper, go slowly and surely don't rush into things, be sure about what you are typing and what you are saying, be methodic, be proffesional, don't be a kid playing with a weapon he don't understand. (it'll go faster and faster with experience).

PS : Avoid harming people for no reason in the process, the best black hats are humble, get in fast, get what you want, delete your presence, (you can leave a backdoor), and get out. don't destroy, it's dumb to hack for revenge (or harm someone in any way just for revenge)

EXAMPLE :

[let take the 13 years old little brother example, I know he plays LoL from the OSINT (Ewww, go play dota 2), I know he uses he's sister PC, she had a picture on instagram with her MAC PRO LMAO XDA879DZA87DA97DZA (I hate macs common guys stop buying them ffs , he posted a picture with a screen shot of a score he did in LoL, I create a LoL account, I play ... yeah .. I'll play LoL > < .. get some levels, add him, he'll accept me, he's 13 years old, he'll accept anyone, i'll E-whore him, tell him I want to learn and want him to show me cause he is SOOOO good, he's at my mercy, would just need to chose a MAC exploit, find a way to send him, ==> basic thing would be to e-whore and tell him he'll have a sext, get a meterpreter in there, keylogg it, take the facebook, desactivate the security notification, connect, delete my connexion history on facebook, reactivate security, get off, you can even let a backdoor on the facebook account, she could find it, but it's not that likely]

I'm sorry for the bad english and the mistakes, not a native english speaker, i'll complete the post tonight I have some work right now can't finish it.

Now let's hear from you guys !!!! I'll add any good advice on the POST so we could have mega thread about how do you organise !!!

idkausername1234 - *August 2, 2017, 5:48 am*

Thank you for making this massive thread, agree with everything and didn't know about the google thing (no wonder I get irrelevant results when looking up names). Cheers :)

PLAY3R_0N3 - *August 2, 2017, 6:01 am*

Awesome thread! Alot of info:-)