

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Hacking Methodologies: Why you need one \[INFLUENCE\]](#)

Dr. Gonzo - May 19, 2018, 5:01 pm

So perhaps you've learned how to exploit a few vulnerabilities. Maybe even quite a few. Its quite the feeling isn't it?

Particularly on here, I've noticed that many people go for a long time without even learning to hack pre-defined targets.

They know how to exploit various vulnerabilities based on scans and google dorking.

But their exploitation is limited to what exploits they know, and what methods they know of finding targets with very specific vulnerabilities.

In essence, HF hackers suck because we lack the crucial meta-discussion.

I come in this section and just see a bunch of disorganized tutorials.

You don't have to keep living your life this way.

Following a methodology will allow you to account for what you don't know. And more importantly It will give you better odds of hacking specific targets.

the following list is ONE methodology. It is by NO MEANS exhaustive or even detailed. It is merely an example I'm not going to go into detail on each step because that would defeat the purpose of this post, but I can make a separate one if its requested enough.

0. OpSec (anonymization)
1. (passive) Recon
2. Scanning (Active Recon)
3. Exploitation (gaining access)
4. Maintaining Access
5. Privilege Escalation
6. Cleaning up (covering tracks)

NOTE: Keep in mind that every hacker will have a different version of this.

for example, most whitehats/pentesters have limited to no need for OpSec.

Bug bounty hunters may not need or be allowed to maintain access of Privilege escalate (depending on the scope and rules of the bounty program) etc. You get the point.

Some may even have additional steps as well as Subcategories underneath the ones I've listed.

Sounds like a bunch of industry jargon/bullshit right?

Here's why this information actually helps you:

Hacking is an absurdly broad field and it becomes more convoluted every single day.

Having a set of steps will help you stay organized and simplify even the most complicated tasks by breaking them up into steps.

Additionally, Reconnaissance should be the step that takes you the MOST time out of anything.

This step gets completely overlooked because most people these days are used to hacking without a scope.

But in a real hack/pentest you don't get to just quit and move on to the next search result when Union based SQL injection doesn't work. You have to

FULLY MAP THAT TARGET

pretend you're a blind man trying to put together a puzzle because when hacking that is essentially what you are.

Do you just aimlessly put pieces down until something happens? No. It would take forever to get anywhere that way.

You feel the pieces until you understand what you're working with.

analogy aside, you have to understand every piece of relevant data about the target you possibly can.

What OS is it running, what version. What services are running, what versions? Is there a webserver? What's on it? What versions?

Are there any other sites hosted on the server? Is the server part of a network that is publicly exposed? Who/what owns the server? Can they be contacted?

Do they use any other websites? Do they reuse credentials? Pick at every single angle. And then once you have all the information organized. Start looking up the versions to see if they are vulnerable to anything. (this is not an exhaustive list of questions)

Your chance of success will be much greater than if you go around just seeing if the target is vulnerable to RCE and then giving up if it's not.

Resources:

<https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/>

<https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf>

<https://pastebin.com/QRkgip6q>

<https://github.com/xapax/oscp/blob/master/windows-template.md>

<https://gist.github.com/unfo/5ddc85671dcf39f877aaf5dce105fac3>

<https://github.com/xapax/oscp/blob/master/linux-template.md>

SilentkillerHF - May 20, 2018, 11:47 am

Great thread. This is all very much true. I am currently one of those skids trying my one way of SQLi and if it doesn't work I move on. I'm tired of that, I want to learn everything there is to learn about hacking. Currently I'm studying networking.

May I ask what your experience with hacking is? What's your "skill level", if you know what I mean?

- Silent

2xqz - May 21, 2018, 5:21 am

Great thread design my dude !

Condescend - May 21, 2018, 9:00 am

Very good thread. I agree with your opinion on the "click this to hack" ideology of some beginners.