How i would hack you and attack you

Tags	checklist server
Property	

Introduction
Recon
- Social media hacking
- Port me like on of your french girls
- Tell the doctor where it hurts!
- Discovering an epic end

I've got some BeEF with you!
XSS the night away
SQLi me a slice of pie!
The only logical conclusion

Introduction

Whenever i am on a pentest, there are always several ways i approach my target. Please note how i mentioned penesting and no bug bounties as those are two totally different beasts. Pentesting makes it a lot easier in my opinion to find vulnerabililities but don't let that discourage you to do bug bounty hunting because while it might be true that pentesters find more issues, a lot of them are low priority or have less impact and as if that was not enough, een pentester needs to be pretty complete.

Recon

Recon recon recon, i can't stress enough how important this part of my hacking cycle is. To hack a target i need to have as much information as possible and for me this all starts with trying to map hidden attacke surface. A lot of people don't realise this but

social media accounts are a prime target for me so i will try to link data i have to existing social media accounts.

Social media hacking

I am telling you this because i think you need to be aware of the dangers of this kind of attack, not because i want you to go try it on your ex. This is not persé a real vulnerability on any websites part as their implementation will more than likely be correct however the creator of the current password system already stated that he regretted making the system so flawed from the start.

I really want to get into your social media account because that will contain a lot of information about you but how would i do this if I only have an email adress right? Well let's try the first thing that comes to mind, i'm just going to try and enter a random password. In this case it will prompt me to enter my password again OR it will allow me to click forgotten password and this is where the fun begins. Most people have their security questions enabled and they totally forgot which they set when creating their account. From here it's very simple to social engineer your answer to those security questions and take over account.

Moral of the story: Disable security questions and opt for a back-up adress instead such as alternative phone number and alternative email adress.

Port me like on of your french girls

Whenever i am dealing with a target, some hidden attack surface can always be found on the not-so-convential ports. Whenever we surf to a website for example, we might be communicating via port 80(http) or port 443(https) but those are just the default ports. There might be so much more webservers running on our target on a different port or VHost so that's why the first thing i will is:

- If broad scope, enumeration of subdomains
- If broad scope i will use masscan, The only problem i have with the tool is that i will need to specificy what ports to scan. To get around this, make a file that contains a list of common ports that you always scan for so that you can re-use that file.

```
masscan -p80,8000-8100 10.0.0.0/8 2603:3001:2d00:da00::/112
Scans port 80 and from 8000 to 8100 on network segment 10.0.0.0/8
```

- If i have a smaller scope or if I am done running my massive portscan i will try to focus a bit more with some more specfic commands to get both TCP and UDP ports and get nmap to scan the results from masscan.
- Id i know which ports are open, i will try to do some banner grabbing using nmap
    - nmap -sV -p80,443 thexssrat.com
- From the previous step note down all the information you can think of, webservers, versions of webservers, network topologie, etc...

Tell the doctor where it hurts!

While i have my nmap scans running, i'll in a dash of scripts to run on the known online ports by adding the "-sC" flag. Besides nmap i have many more vulnerability scanners in my toolbelt such as metasploit, xsshunter or burp suite pro scanner, i will try to run all of them on every entry point i see and even the entry points i do not see. I am pretty certain most happy paths work but i am looking for the extremities.

I'll run all the tools in my arsenal but prefer this order of importance:

- Any scans on authentication such as SQLMap
- Nikto to tell me more information about the webserver and it's possible vulnerabilities + burp suite pro scanner.
- Nuclei to tell me even more about the vulnerabilities
- Knoxss to find XSS as a browser plugin
- JS analysis with linkfinder and secretfinder

I will also look up all the port numbers, what the default applications are on there and how to hack them, keeping a special eye on version numbers of applications which i will litteraly google "how to hack x" or "exploit software 3.2.10". This will often lead me to exploit-db where i can also look at the google dorks to get some inspiration on how to hack your machine.

You have no idea how often I find entry into your HDD by using outdated software!(Hint: It's wayyyy too often.)

Discovering an epic end

Now that you are almost dead, im going to strike with looking for some content with tools like fuff or burp suites content discovery. I will especially be interested in custom login pages but of course i need to ensure my target allows me to use an automated scanner. I love search pages i am not supposed to see.

I've got some BeEF with you!

If you are smart enough to not click my links you are in luck but we both know I only need to get through one time while your defenses have to be picture perfect every time. This is where BeEF comes in, this amazing framework allows us to take control over a remote browser, even reading things like stored passwords if your victim stores your passwords in the browser.

XSS the night away

Now I'm going to try and pop you a new one with my XSS vector which you will never even see coming (This is why alert() is terrible yoooo! We don't want our targets to see that we are hacking them besides that, an alert is the most filtered word anyway). Right now i'm going to steal your data on the page, steal your session token, steal CSRF tokens or even just execute JS functions... so much we could do!

SQLi me a slice of pie!

I am always going to be testing for XSS and SQLi at the same time, just very passively! My real XSS and SQLi methodology consist of seeing where different values are reflected or if the values go into something like a prepared statement.

The only logical conclusion

When all else fails me, I know there are still business logic issues. I know how bad people are at logical reasoning and security by design is not one of our strong points. This is good though because it is not easy to automate these issues. Let's explore how to do this manually and automate like tomorrow will never come ...