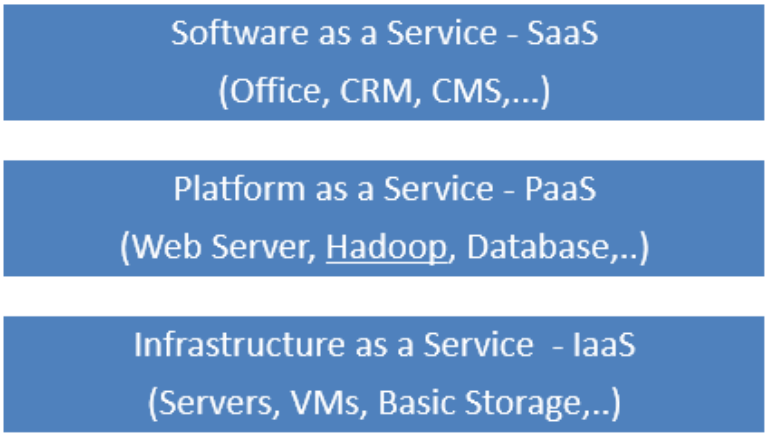
Ethical Hacking 200

Assignment 3-2: Attacking a Microservice Public Cloud PAAS Service

Contents

Recap

In class we covered a couple key concepts of big data and distributed processing such as different offerings. Each comes with its own security expectations, historical mistakes, and common problems.



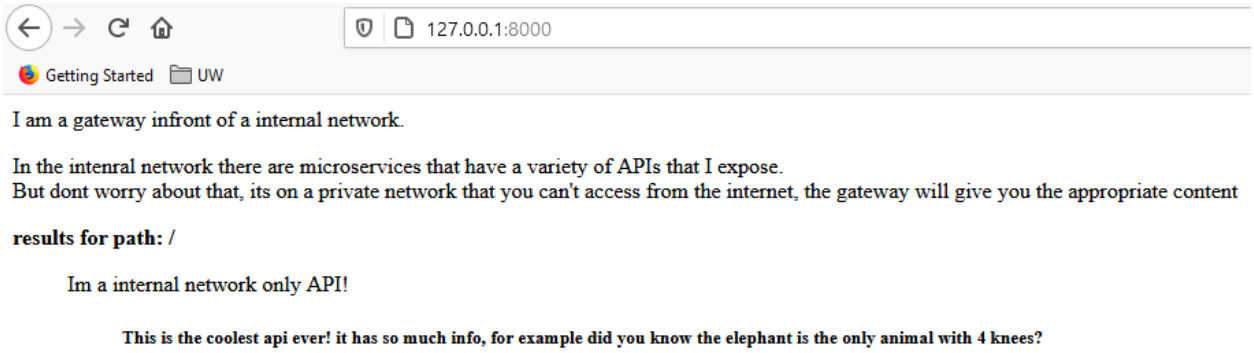
Models:

- Private Cloud
- Public Cloud
- Hybrid Cloud

Your Assignment:

- Think about these core concepts.
- Practice your skills in thinking about security expectations
- Practice your skills in imaging how parts fit together behind the scenes when you can't see them.
- You will pentest a theoretical microservice architecture with services on an internal network and a gateway exposing some services to the public. In this case you know you are looking specifically to steal the admin password, in a real world scenario you would not know what you are looking for. You will not need to cause any state changes such as "POST" requests, it will be all "GET" requests.

- If your browser is stuck loading try using “localhost” (e.g: http://localhost:8000), also try a different web browser such as chrome.



- Try out the assignment in a realistic experience.
  - Install python3 if you do not already have it
  - Execute both scripts “run_hidden.py” and “run_2hidden.py”
  - Then visit http://127.0.0.1:8000 in your web browser and start hacking.
  - **Hints** – Try to attempt the assignment without hints to experience testing the app from a real-world experience. The point of a real-world experience is to understand what information would have been necessary for you to figure out what was going on. Think back to lesson 1 and “hack this sentence”.
    However, if you are struggling use the hints, this won’t give you all the answers but will boot strap you. The higher the level the hint the more of the answer it will give you, but also the scenario would be less realistic. *You will not lose points for using hints, it is however in your own benefit to try the assignment first without them.*
  - Hint Level 0 – (still a bit realistic even using this hint)
    “Base64 decode” the string below
    dHJ5IHRvIG1lc3Mgd2l0aCB0aGUgVVJMIGFzIG11Y2ggYXMgcG9zc2libGUKZW50ZXIgZGlmZmVyZW50IFVSTCBwYXRocwpUaGF0IGlzIHlvdXIgcG9pbnQgb2YgYXR0YWNr
  - Hint Level 1 -
    “Base64 decode” the string below
    dmlzaXQgaHR0cDovLzEyNy4wLjAuMTo4MDAwL3Rlc3QlM2QlMDEKYW5kIHRoZW4gdmlzaXQgaHR0cDovLzEyNy4wLjAuMTo4MDAwL3Rlc3QlM2QKcGF5IGNsb3NlIGF0dGVudGlvbiB0byB0aGUgYmVoYXZpb3JhbCBkaWZmZXJlbmNlCkFsc28gaHR0cHM6Ly90b29scy5pZXRmLm9yZy9odG1sL3JmYzM5ODYjc2VjdGlvbi0yLjIgd2lsbCBoZWxw
  - Hint Level 2 -
    “Base64 decode” the string below
    V2hlbiBldmVyIHlvdSB2aXNpdCBodHRwOi8vMTI3LjAuMC4xOjgwMDAvCnB1dCAiP2hpbnQ9aGVscG1lIiBhdCB0aGUgZW5kIG9mIHRoZSBVUkwgc3VjaCBhcyBodHRwOi8vMTI3LjAuMC4xOjgwMDAvP2hpbnQ9aGVscG1lClBheSBjbG9zZSBhdHRlbnRpb24gdG8gYWxsIG9mIHRoZSBkaWZmZXJlbmNlcyBpbiBiZWhhdmlvcg==

What to turn in:

- **A description of what the *vulnerability* in the application is in addition to the admin password.** Be sure your explanation explains how the overall architecture of the theoretical ecosystem plays into the problem.
  - Example:
    (password: abcdefg)
    the vulnerability is a combination of the application doing A and not doing B. There are improper security executions XYZ. Due to the architecture service A believes xyz and something something does something.
  - **Submit:** Any reasonable text format is acceptable. (e.g: doc, docx, rtf, txt, etc).

Im having a really hard time!

As always, the best thing you can do is reach out as early as possible to the instructor.

On this assignment it is better not to group chat with other students such as to not ruin their learning experience. However if you do ensure you do not give any answers or hints away.

Again this is meant to be hard but not impossible. Try everything you can think of and then some, research, and lookup anything and everything. Nothing I dumb to lookup. Even looking up on the internet something like “security URL path attacks” can be tremendously helpful.