About using CloudGoat, Pacu, and ChatGPT


Christophe August 27, 2023

Disclaimer

This course teaches techniques that can cause damage and harm to AWS accounts and resources. What we will demonstrate is perfectly safe, legal, and conformant to AWS terms of service, so long as you stick to our instructions, scenarios, our labs, and/or your own lab environments. **Do NOT use these tactics against production accounts/resources while you are learning, and do not use them against organizations that have not provided you with explicit written permission.** I will provide further instructions for this as we get started with the course so that you can safely create a separate AWS account to ensure isolation from production resources, but I want to make it very clear that this course is strictly for white hats and ethical hacking.

About the tools we're going to use

As the title of this course implies, we're going to be using 4 primary tools:

- CloudGoat
- Pacu
- ChatGPT
- AWS CLI

In order to pentest various types of vulnerable AWS environments.

But how exactly are we going to use these tools? And if you're not already familiar with them, what are they used for? Let's take a look.

CloudGoat

CloudGoat is a vulnerable-by-design AWS deployment tool that can be used to create and configure intentionally vulnerable AWS environments. It's a learning tool that provides a safe and legal sandbox for conducting security research, penetration testing, and assessment of your AWS environment's security. This is a great tool to practice identifying and exploiting various types of security vulnerabilities in AWS environments.

The environments created by CloudGoat are vulnerable by design, and they contain security weaknesses that can be exploited to simulate real-world attacks. This enables you to learn about different types of security vulnerabilities and how they can be exploited in a controlled environment.

Examples of scenarios we can generate include:

- Misconfigured S3 buckets
- Compromised AWS credentials
- Misconfigured cloud instances
- Misconfigured containers
- Etc...

We'll be using CloudGoat modules in this course — one per section — to provide a hands-on AWS security learning experience. Yup, that means *you* will be going through these scenarios step-by-step instead of just watching me do it.

You'll learn how to identify and exploit different types of security vulnerabilities in AWS environments which is a skill you can then directly apply on the job. That means the next time you see a vulnerable IAM policy, you can not only detect it, but you can also create a proof of concept for the rest of your team and upper management.

To build these skills and to find these vulnerabilities, we'll make use of two other tools, one of which is called Pacu.

Pacu

Pacu is an open-source AWS exploitation framework that helps pentesters and security researchers assess the security of their AWS environments.

Pacu is highly modular and extensible, means that we can even create our own custom modules to extend its capabilities if we need to. Don't let that intimidate you, though, because it includes many pre-built modules that can be used to perform a variety of attacks that we will use throughout this course, like:

- Enumeration
- Privilege escalation
- Data exfiltration
- Etc...

In this course, we'll be using Pacu to perform a number of different types of attacks against vulnerable AWS environments.

With that said, we won't just be using Pacu. Sometimes it's easier and more practical to just use the AWS CLI, so we'll be combining both approaches to switch back and forth and to show you that there are multiple approaches we can use.

ChatGPT

I highly doubt this is the first time you've heard of ChatGPT, so I'll focus more on *how* we'll be using it in this course.

ChatGPT is an amazingly useful AI tool that can help us when we get stuck. It's generative AI, which means that the responses I get could be different from the responses *you* get. Sometimes *completely different*. The point, then, is not to use it so that you can copy/paste the results that I get into your terminal, but instead, the point is to teach you how you can use ChatGPT with the AWS CLI, Pacu, and CloudGoat to troubleshoot, and craft commands.

That way, once you're done with the course, you can take those new ChatGPT skills and the types of prompts that I'll show you to take it further and continue your learning.

Conclusion

That's it for this lesson, I just wanted to give a quick overview of what you'll be learning and using in this course. Now, let's complete this lesson, and let's move on to the next.