Who this course is for

Christophe September 4, 2023

In short: this course is for individuals who want to perform security assessments of AWS environments and resources, or who want to learn what to do once they've gained access to a set of limited AWS credentials or access.

This course includes a mixture of learning how to gain initial access and how to escalate privileges from existing access. There are more scenarios that lean on the privilege escalation path rather than gaining initial access, meaning that it is primarily about finding weaknesses and misconfigurations in AWS cloud environments that enable privilege escalation from limited credentials or from misconfigured services.

It is designed for those who want to test their own organization's cloud security posture, or that of a client. That client or your organization has given you access to limited accounts or services that aren't supposed to have elevated privileges, but you are going to exploit multiple different kinds of services and weaknesses to escalate privileges.

While there is one or two scenarios we'll go through that show you how to exploit and gain access to credentials through misconfigurations, that's not going to be the primary objective of this course and so if that's what you're expecting, then this is probably not for you. (We do plan on having a separate course that focuses more on gaining initial access since I know that's an interest for many)

This course will teach you how to navigate the inner workings of AWS by exploiting multiple different services. It will teach you how to find weaknesses and misconfigurations in IAM through multiple different AWS services such as EC2, Lambda, ECS, etc... services commonly used by large and small companies around the world.

Many organizations quickly throw together IAM policies, run a couple of quick tests, and then think they're good to go. This will show you why that's not sufficient, and how badly written IAM policies or badly configured cloud instances and containers can be exploited to gain admin-level privileges through seemingly harmless configurations.

If this sounds interesting to you, then I'll see you in the course!