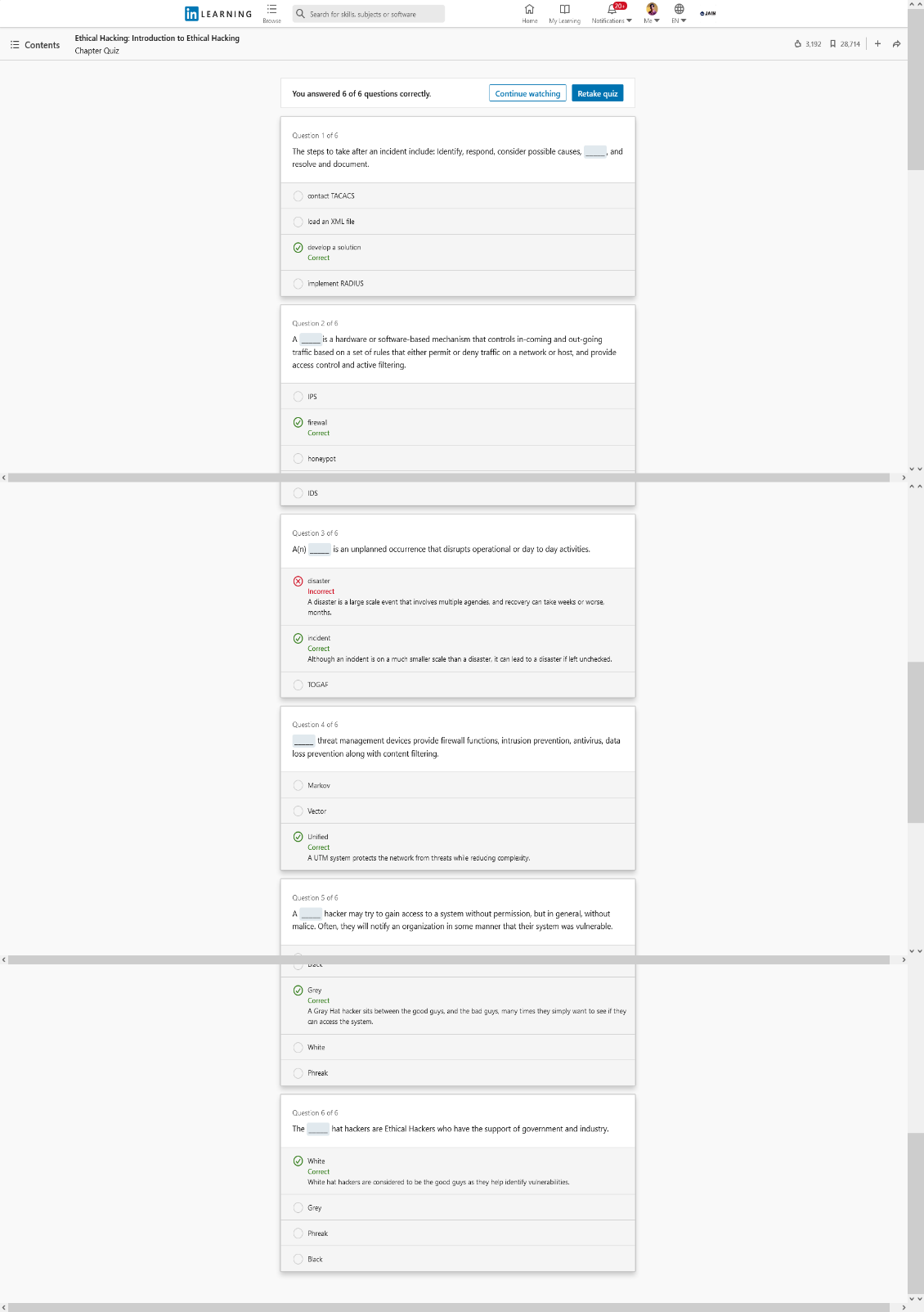
**Introduction to the Course**

In this course, we took a look at high and low-tech tools to scout our target. We first begun with a reconnaissance overview and then we saw how to use competitive intelligence. We examined search engines and look at Google hacking. We took a look at social media and the importance of tracking online reputation. We looked at email and website footprinting and how to mirror and monitor websites. We investigated email and email headers and we saw the power of open-source intelligence tools. We took a look at some of the reconnaissance tools that include footprinting network and examining ways to see how DNS can help us in our search. We looked at tools such as ping, tracert, nslookup, and dig. And then we looked at countermeasures for footprinting and reconnaissance and then pen testing reports which should be done at the end of every exercise. This course is part of the Ethical Hacking series.

**Learning objectives**

* Using competitive intelligence
* Hacking with search engines
* Using email for footprinting
* Getting social
* Mirroring websites
* Using Ping, Tracert, nslookup, and dig
* Taking footprinting countermeasures
* Pen testing for footprinting

**Screenshots**



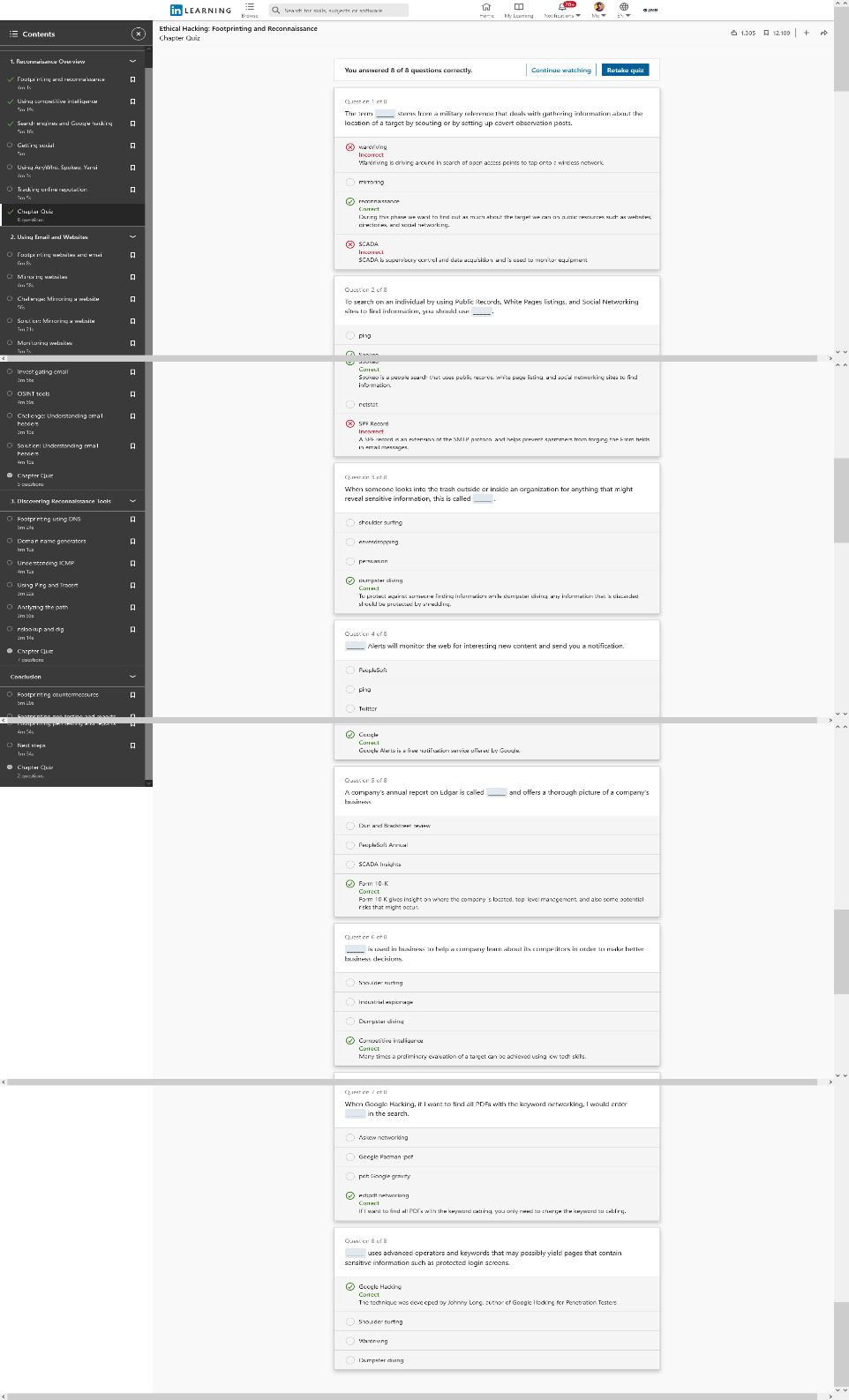


Figure: Section 01 – Reconnaince Overview Figure: Section 02- Information Security Control

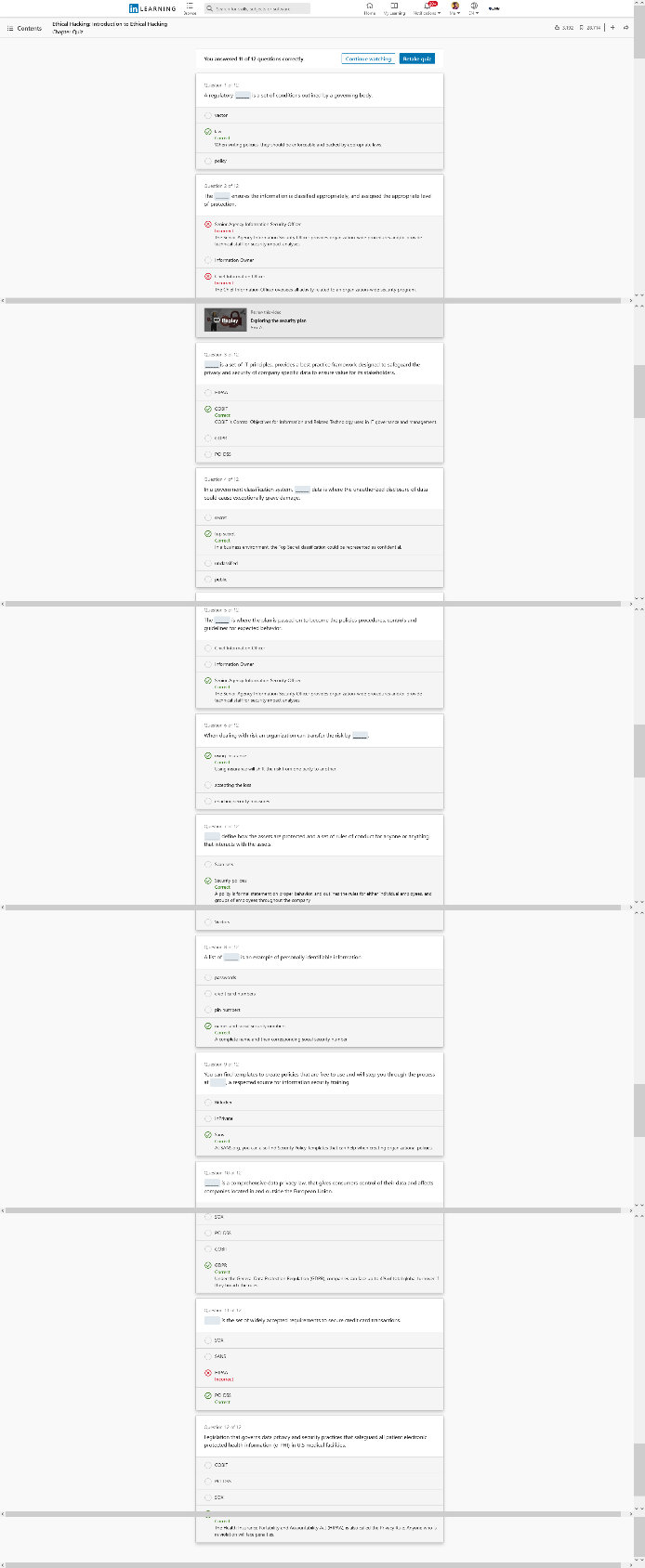
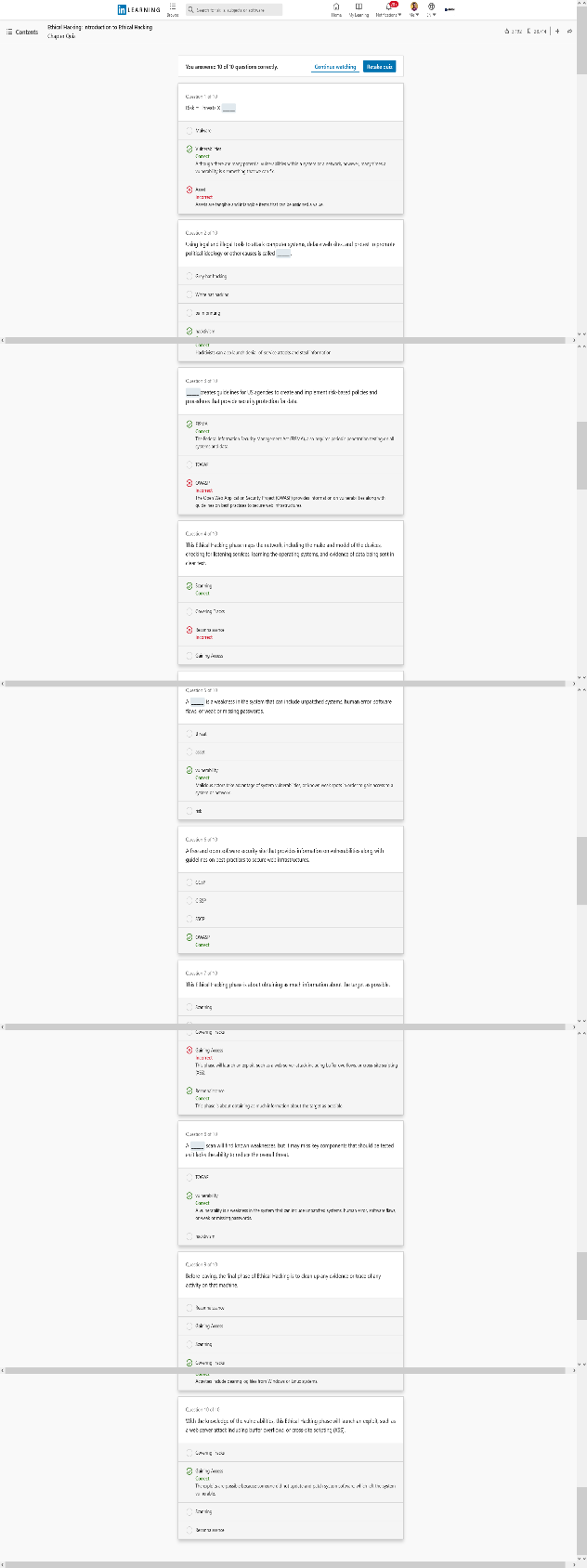
****

Figure: Section 03 – Data Proyection in a Digital World Figure: Section 04- Support Ethical Hacking

**Conclusion**

In this course, we took a look at today's threat landscape, current attacks, and attack vectors. I covered the cyber kill chain and the importance of adhering to standards and regulations. We looked at policy creation along with the concept of ethical hacking as it relates to organizational security. I learnt about different organizations like: COBIT, OWSAP, SANS, CISA etc. and their functions. I learnt about different hacking prevention measures too.

**Certificate**

****