Lab 6: Perform Whois footprinting

**Lab Scenario**

During the footprinting process, gathering information on the target IP address and domain obtained during previous information gathering steps is important. As a professional ethical hacker or penetration tester, you should be able to perform Whois footprinting on the target; this method provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc. Using this information, you can create a map of the organization’s network, perform social engineering attacks, and obtain internal details of the network.

**Lab Objectives**

* Perform Whois lookup using DomainTools

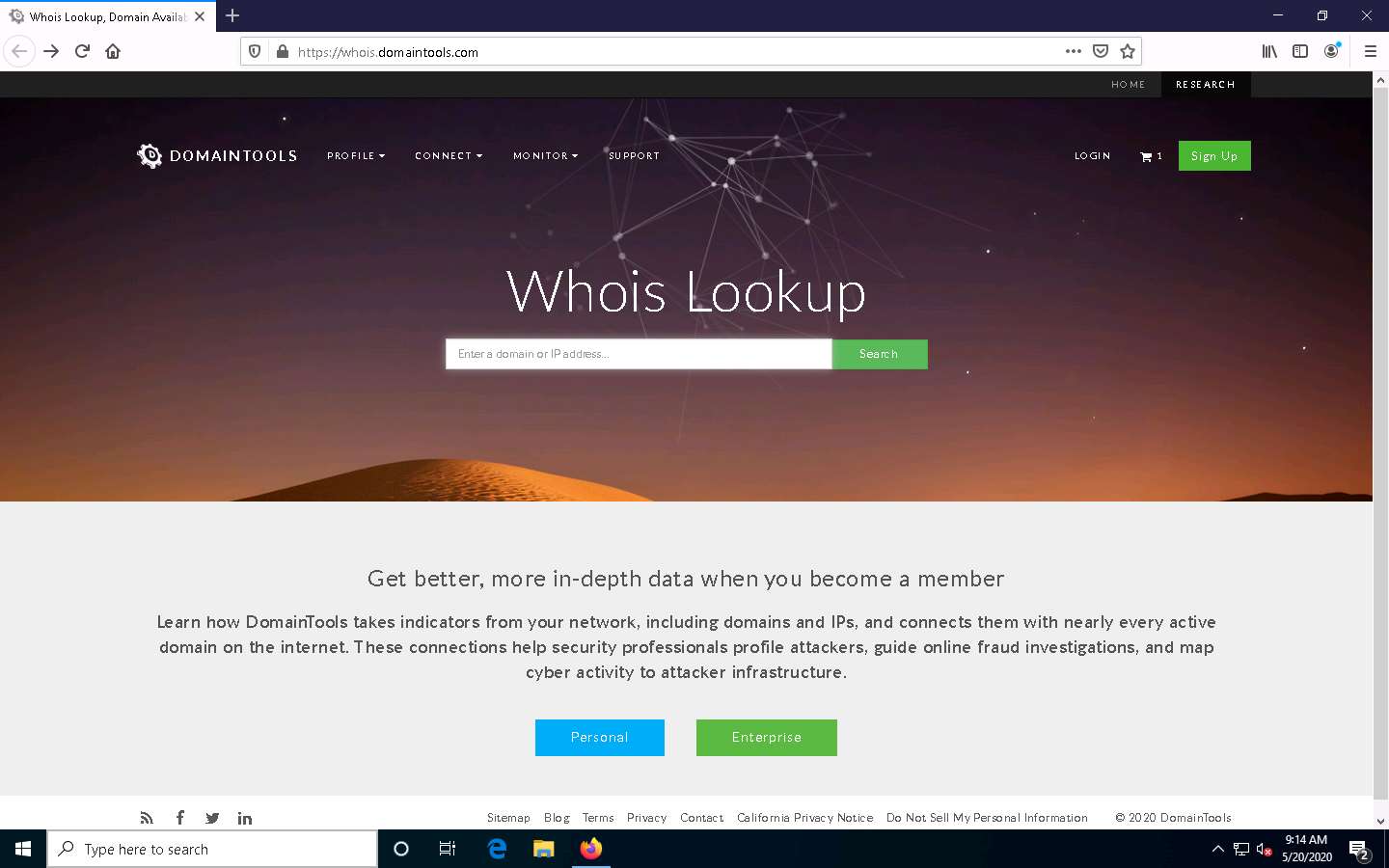
**Overview of Whois Footprinting**

This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

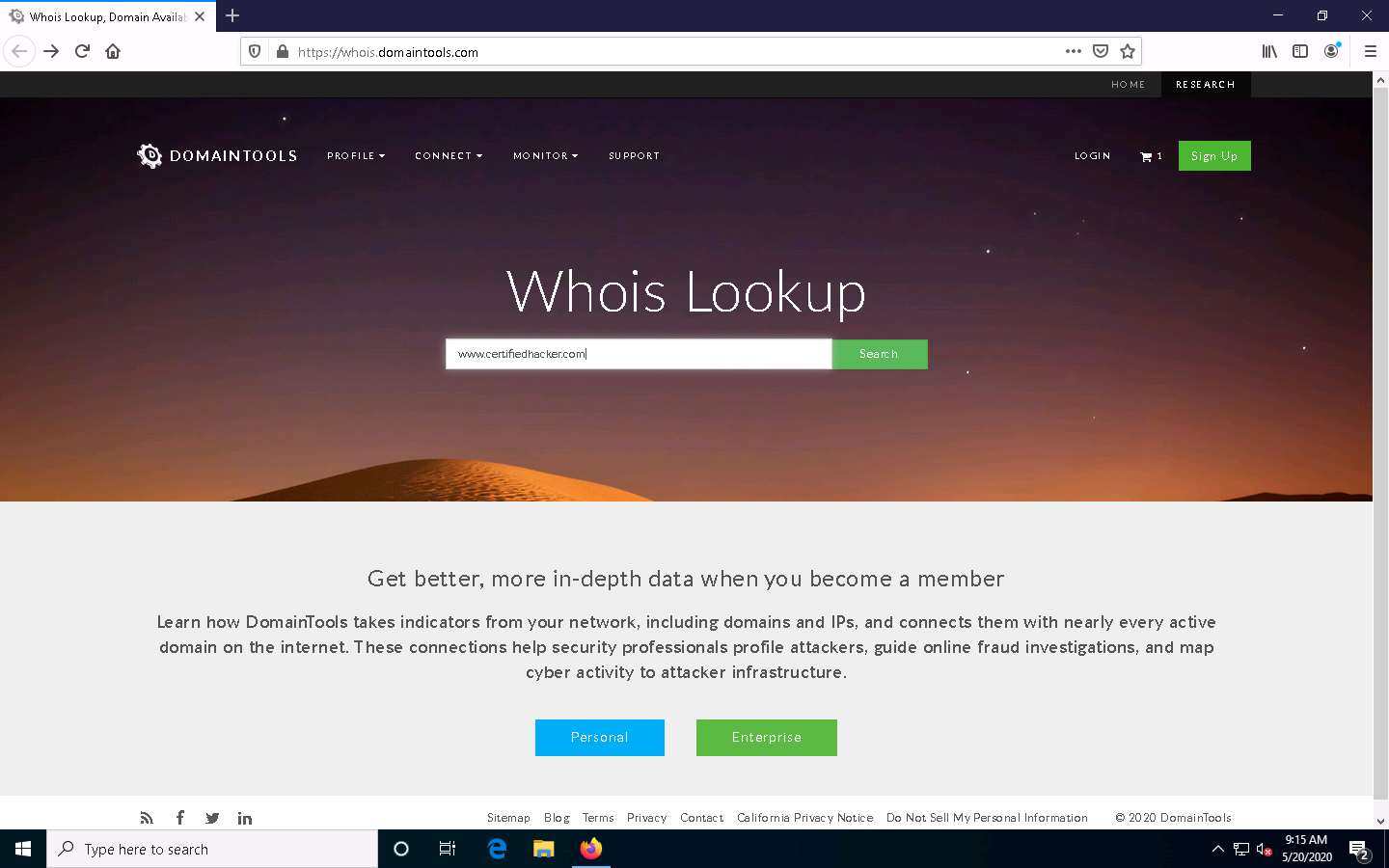
Task 1: Perform Whois Lookup using DomainTools

Here, we will gather target information by performing Whois lookup using DomainTools.

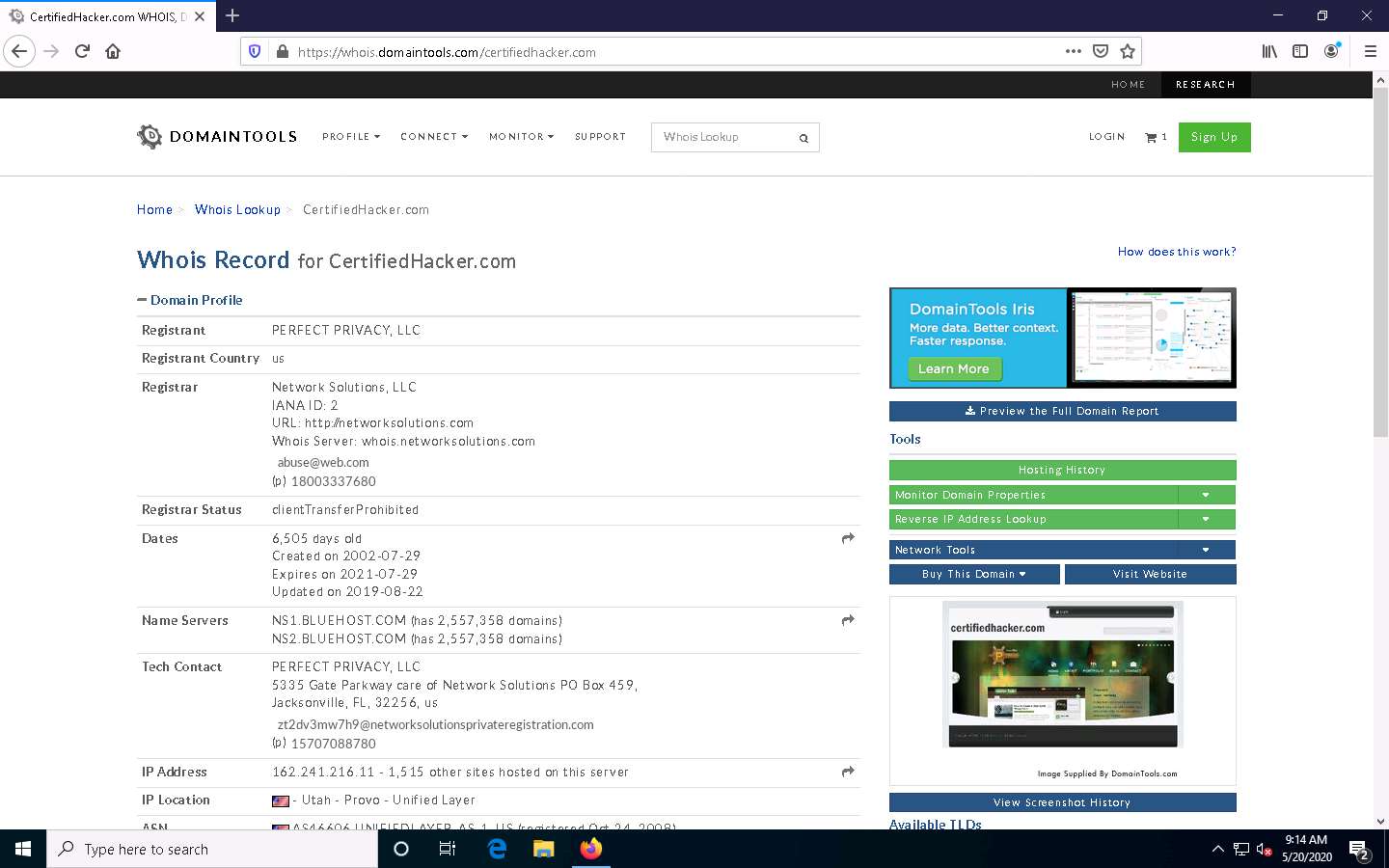
1. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, click http://whois.domaintools.com and press **Enter**. The Whois Lookup website appears, as shown in the screenshot.

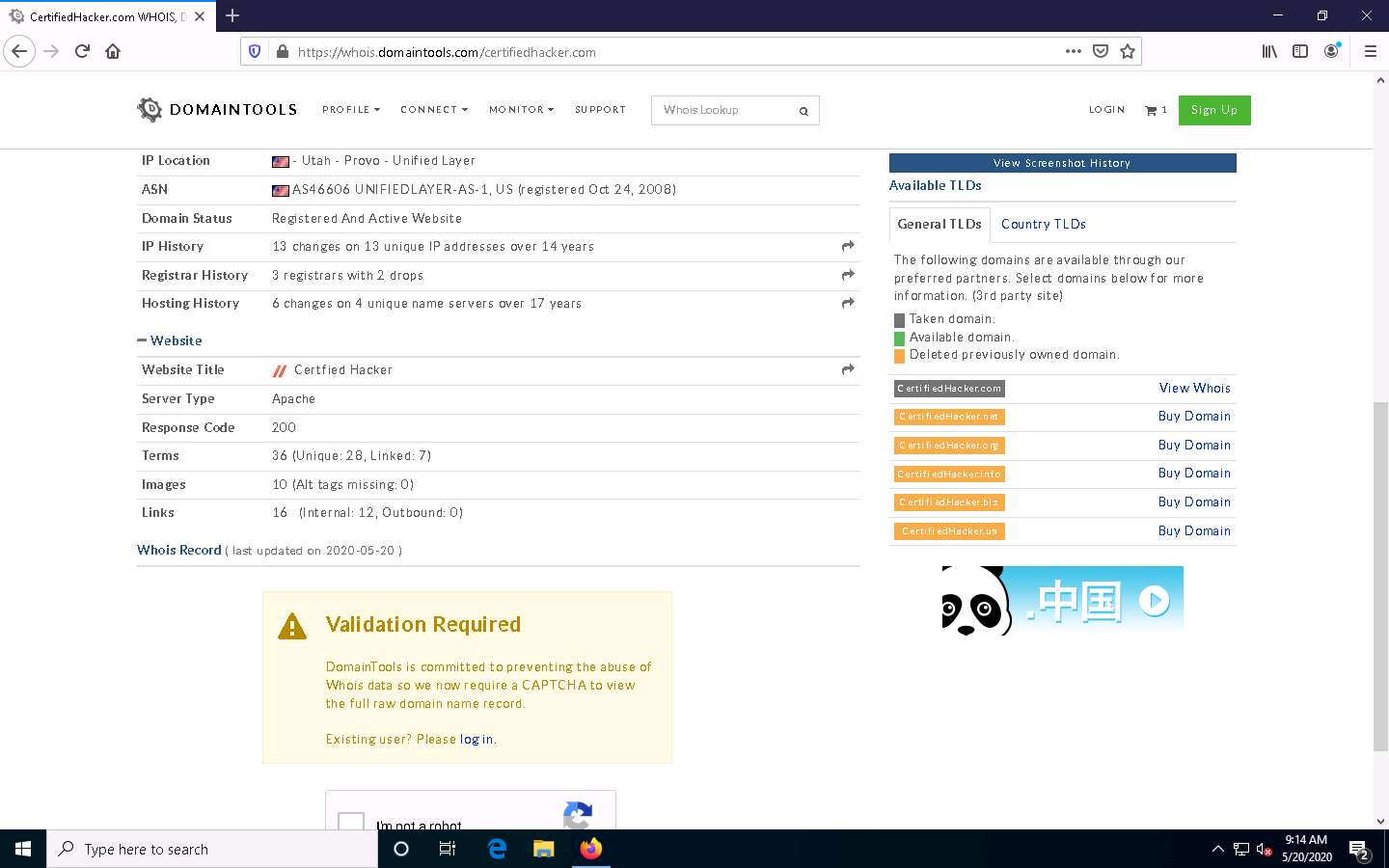


1. Now, in the **Enter a domain or IP address…** search bar, type **www.certifiedhacker.com** and click **Search**.



1. This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.





1. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
2. You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.
3. Close all open windows and document all the acquired information.