Lab 4: 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

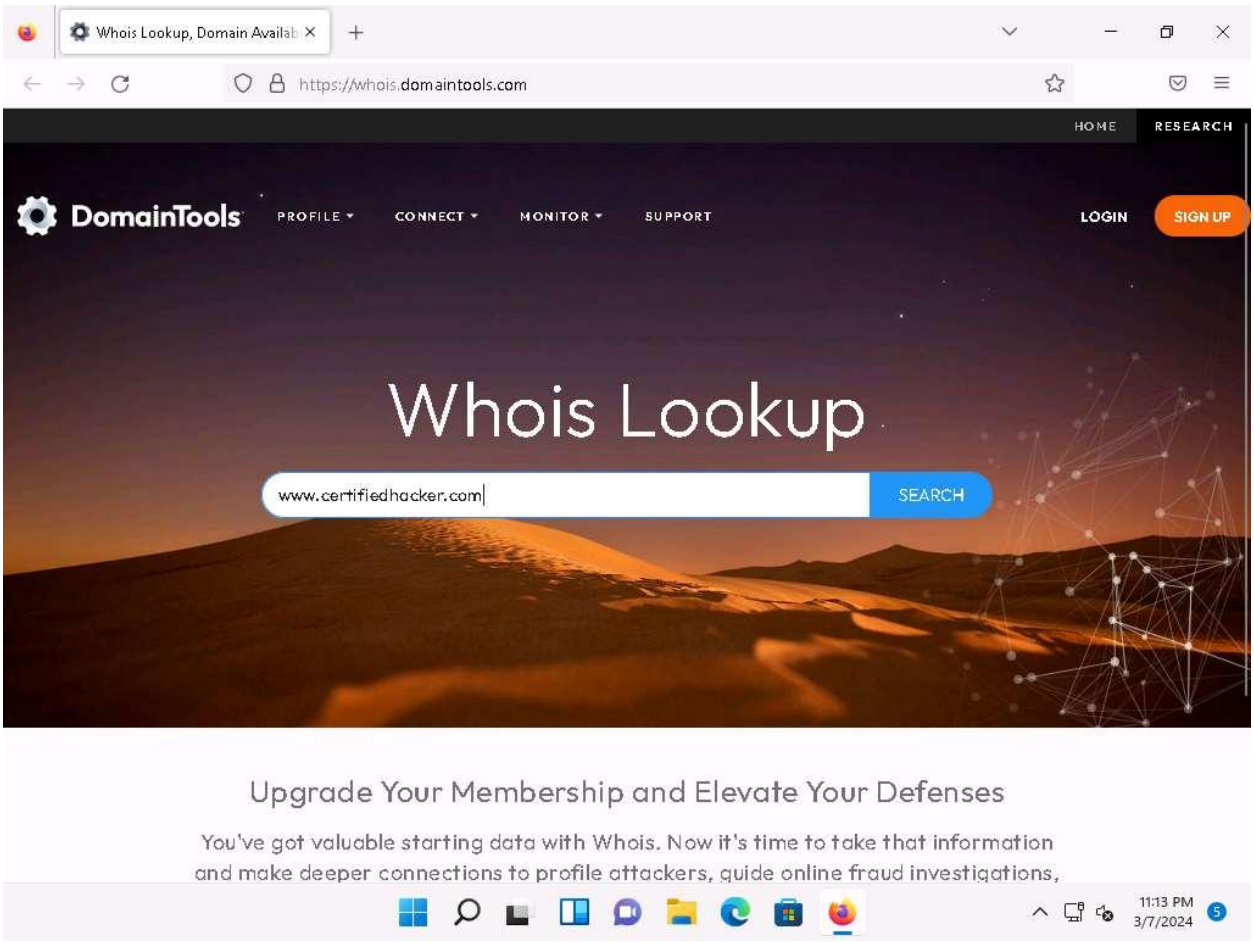
Overview of Whois Footprinting

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).

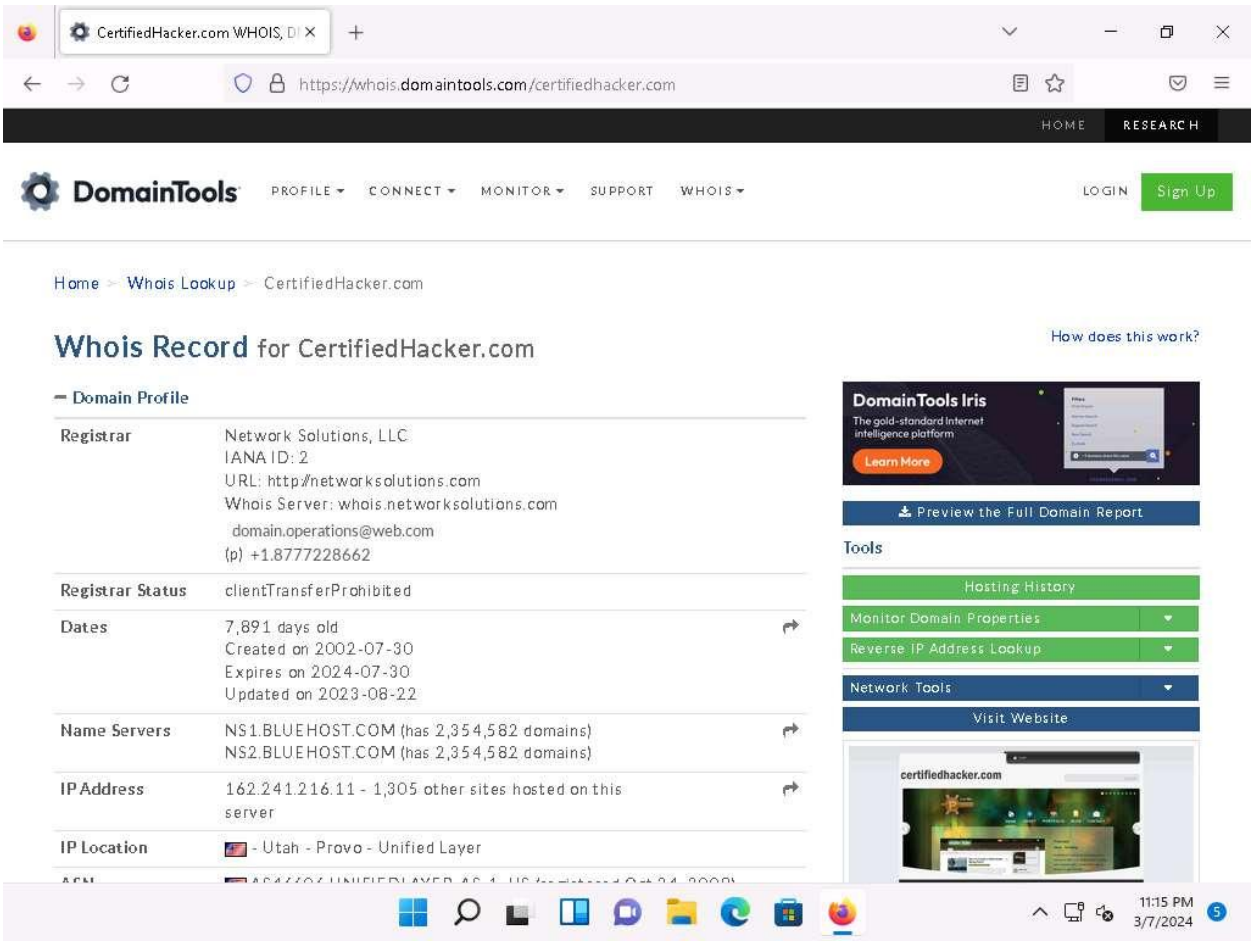
Task 1: Perform Whois Lookup using DomainTools

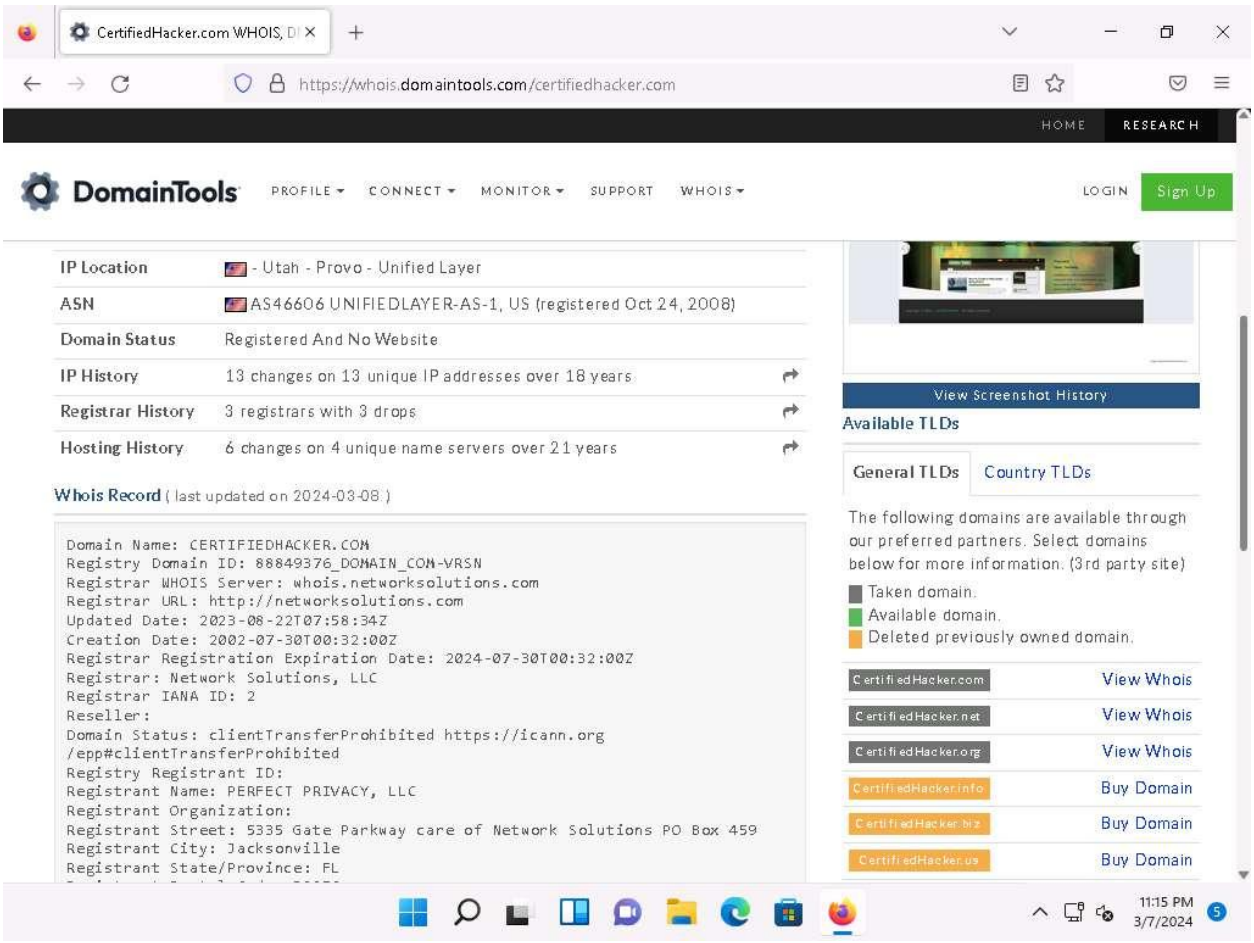
Here, we will gather target information by performing Whois lookup using DomainTools.

1. Click Windows 11 to switch to the **Windows 11** machine, open any web browser, and go to **https://whois.domaintools.com** (here, we are using **Mozilla Firefox**).
2. The Whois Lookup website appears, as shown in the screenshot. Now, in the search bar, search for **www.certifiedhacker.com**.



3. 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.


CertifiedHacker.com WHOIS, D
https://whois.domaintools.com/certifiedhacker.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
WHOIS
LOGIN
Sign Up
Home > Whois Lookup > CertifiedHacker.com
Whois Record for CertifiedHacker.com
How does this work?
Domain Profile
Registrar
Network Solutions, LLC
IANA ID: 2
URL: http://networksolutions.com
Whois Server: whois.networksolutions.com
domain.operations@web.com
(p) +1.8777228662
Registrar Status
clientTransferProhibited
Dates
7,891 days old
Created on 2002-07-30
Expires on 2024-07-30
Updated on 2023-08-22
Name Servers
NS1.BLUEHOST.COM (has 2,354,582 domains)
NS2.BLUEHOST.COM (has 2,354,582 domains)
IP Address
162.241.216.11 - 1,305 other sites hosted on this server
IP Location
- Utah - Provo - Unified Layer
DomainTools Iris
The gold-standard Internet intelligence platform
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Visit Website
certifiedhacker.com
11:15 PM
3/7/2024



4. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
5. Using this information, an attacker can create a map of the organization's network and further mislead domain owners with social engineering, and obtain internal details of the network.
6. 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.
7. Close all open windows and document all the acquired information.