Student:	Email:
Isaiah Mosley	isaiahmosley80@gmail.com

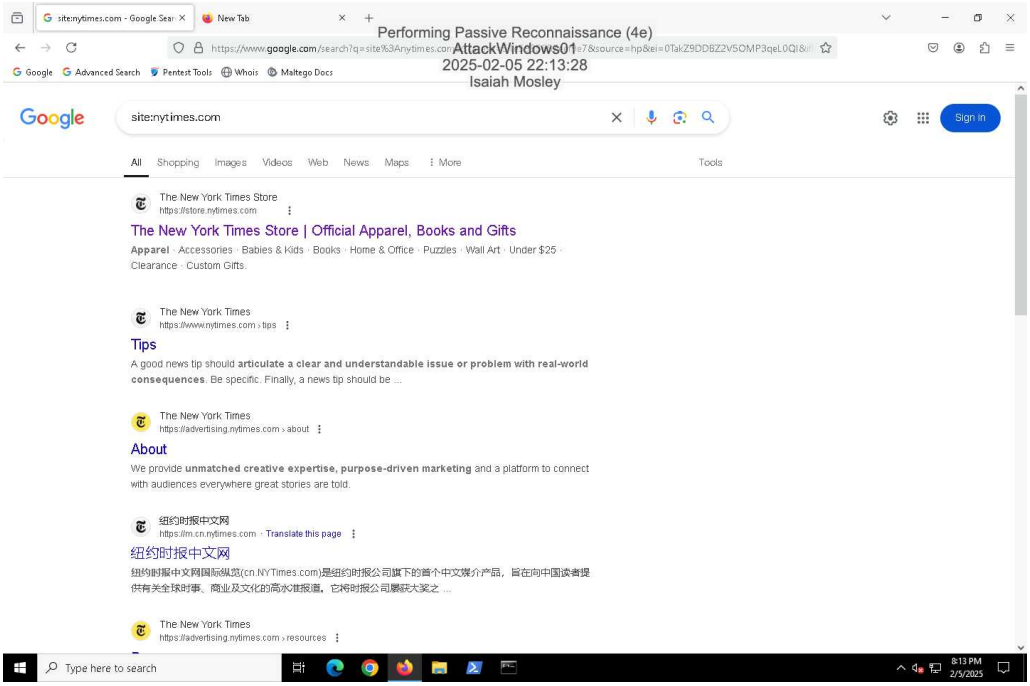
Time on Task:	Progress:
65 hours, 41 minutes	87%

Report Generated: Tuesday, December 2, 2025 at 1:21 PM

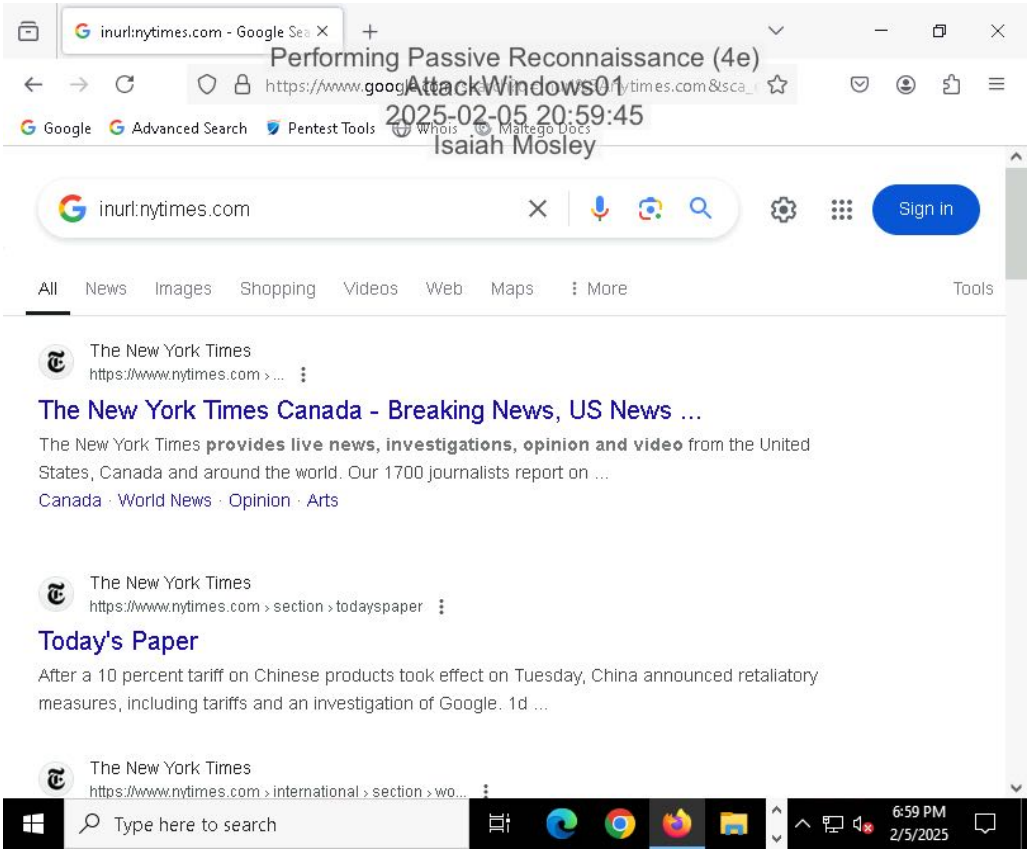
Section 1: Hands-On Demonstration

Part 1: Explore Google Hacking Techniques

5. **Make a screen capture** showing the **site:nytimes search results**.



7. **Make a screen capture** showing the **inurl:nytimes search results**.



9. **Briefly describe** the differences you noticed in the search results for each search operator and identify one or two scenarios in which any of these particular findings could be useful to the ethical hacker.

The "**link**" operator is used to search for specific domain or Url related what you're searching for.
The "**related**" operator searches for pages related to the website in the title tag.
The "**info**" searches for information related to a specific website or page.
Two Scenarios:**Link Operato**r: when the hacker is performing passive reconnaissance, they can utilize the link operator to search for websites that traces back to the target website. This can be helpful to identify possible sources of information, such as companies who are associated with the target.
Info Operator: If data is collected on the target website, a hacker can use the data given by the operator to swiftly get an overall observation of the website. For instance, a hacker can look at the cache versions and other pages associated with it. The information can help with breaking down how the website is structured and could potentially weak entry points

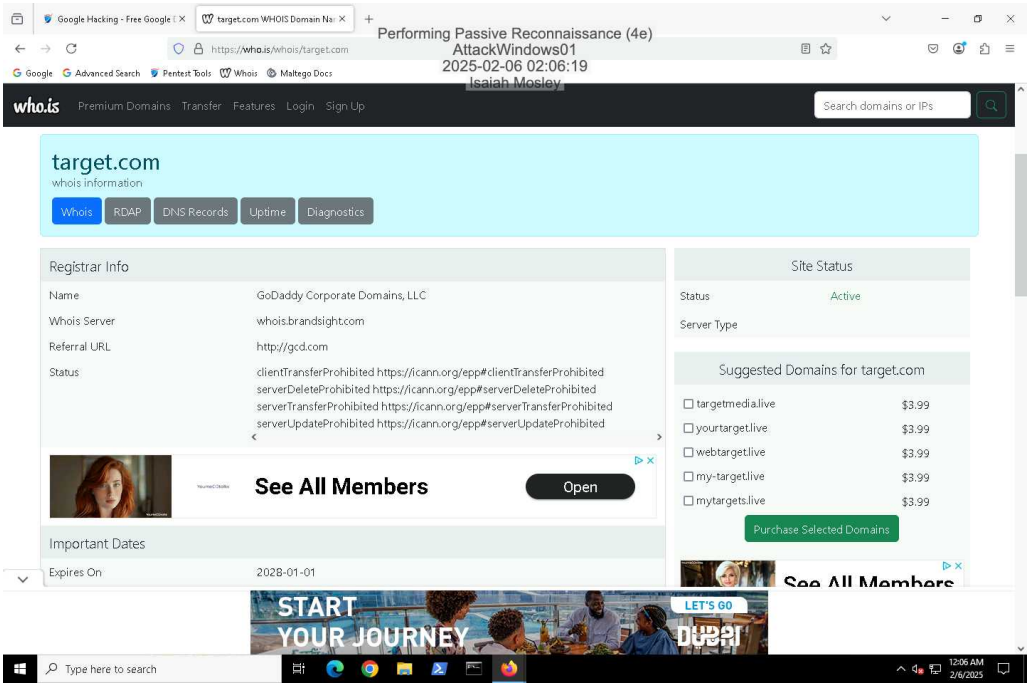
16. **Describe** any **search results** obtained in steps 14 and 15 that you think might provide a malicious hacker with information that could be used to target users or systems of your chosen organization.

For the company i chose to search for vulnerabilities that lead to information within the website directory, all of the google dork options didn't reveal any data leaks within areas of the website. Fortunately, i found 2 out of the 8 search options: Configuration files exposed and Login pages.
Configuration files exposed: The results of this search option lead to a domain that looks like a digital file storage locations. For instance, on the website it has a list of directories, such as "/admin" on "www.target.com/robots.txt" that could lead to access to the files containing tables and queries etc. that you can view, modify or delete only by having admin privileges.

Login pages: The results of this search revealed multiple login pages that shouldn't be exposed to the public. This could be used to gain unauthorized access to sensitive data. Also, i seen one of the target login websites using the unsecured version of HTTP, which could expose the if the PHP version is the latest. If not, a hacker can exploit vulnerabilities and gain unauthorized access, inject malicious code, or cause services to disrupt.

Part 2: Explore the WHOIS Database

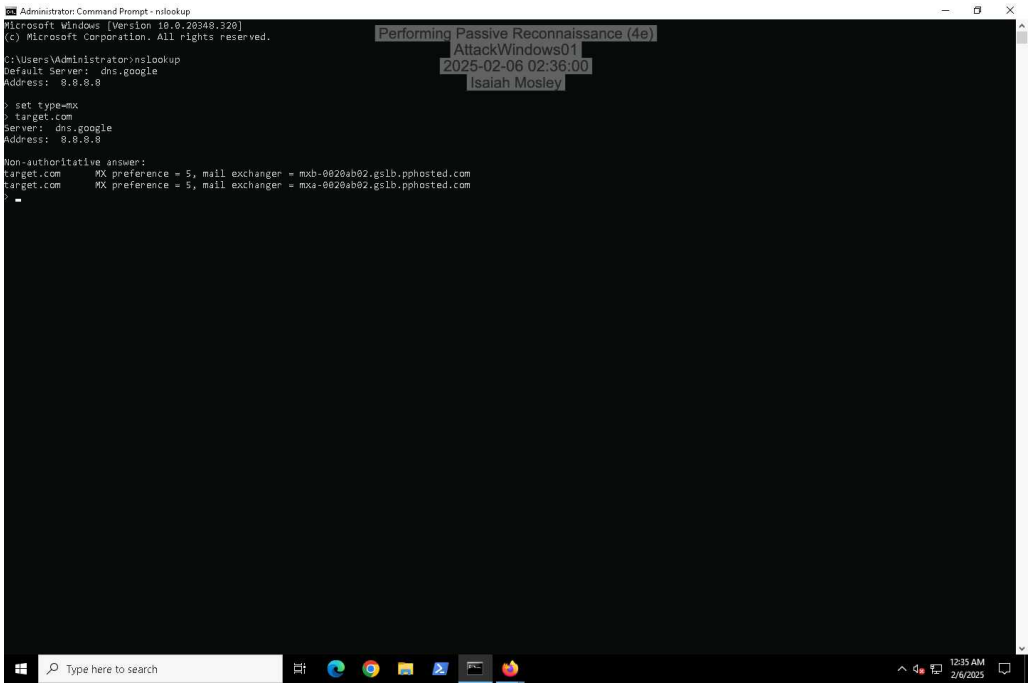
3. **Make a screen capture** showing the **results of the WHOIS search**.



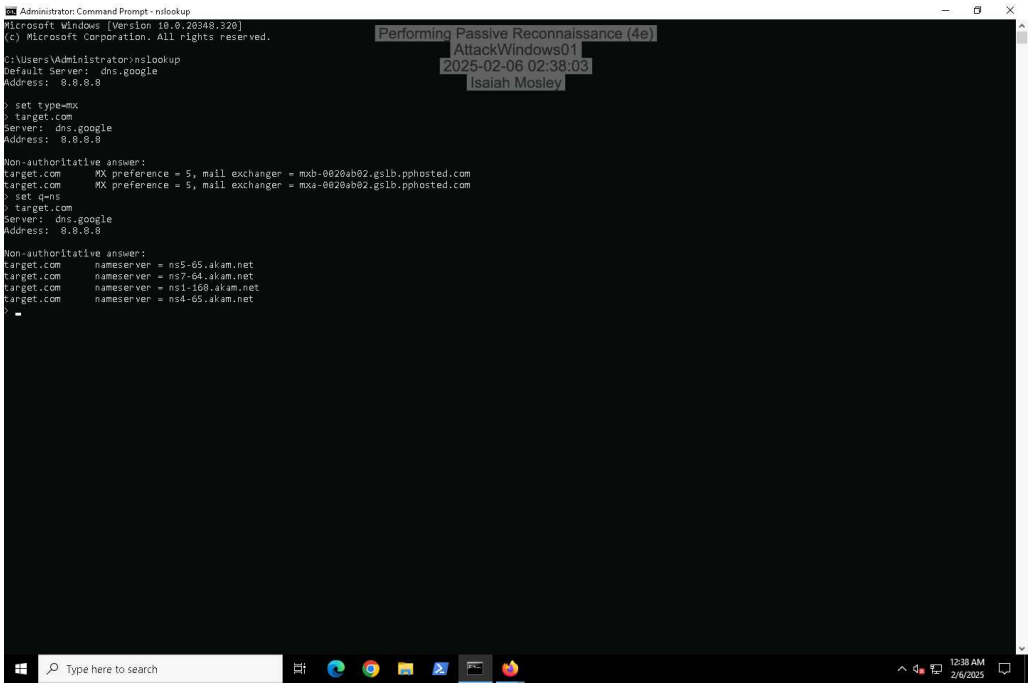
4. **Document** the **date of the most recent update** to the domain record.

2025-01-11

11. **Make a screen capture** showing the **results of the MX query**.



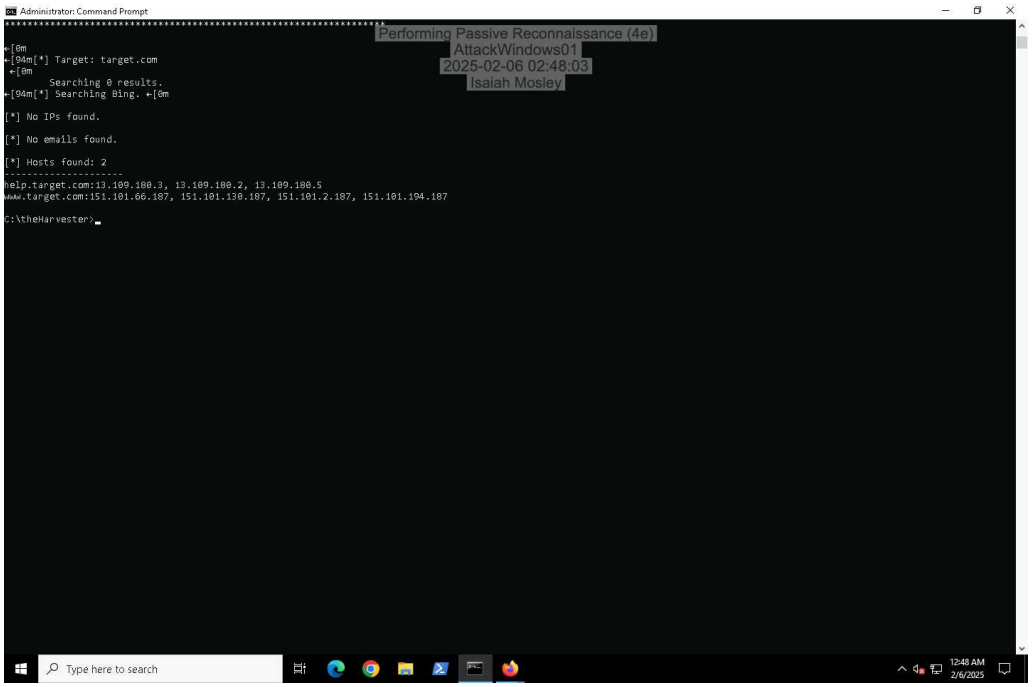
14. **Make a screen capture** showing the **results of the NS query**.



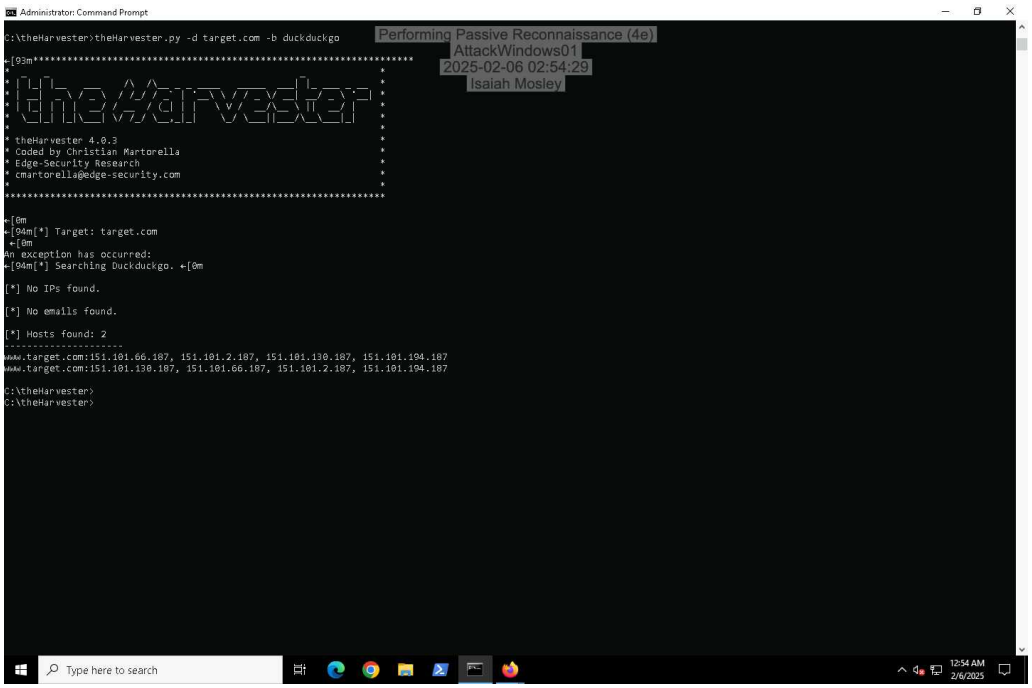
Section 2: Applied Learning

Part 1: Collect Information with TheHarvester

Make a screen capture showing the **search results from theHarvester using Bing**.

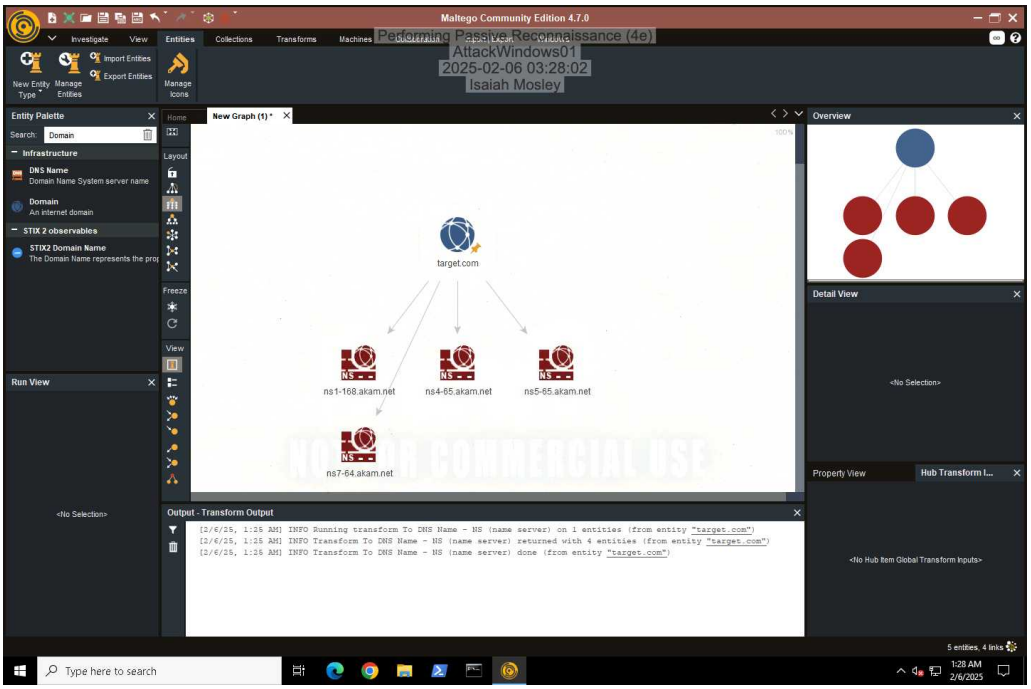


7. **Make a screen capture** showing the **search results from theHarvester using DuckDuckGo**.

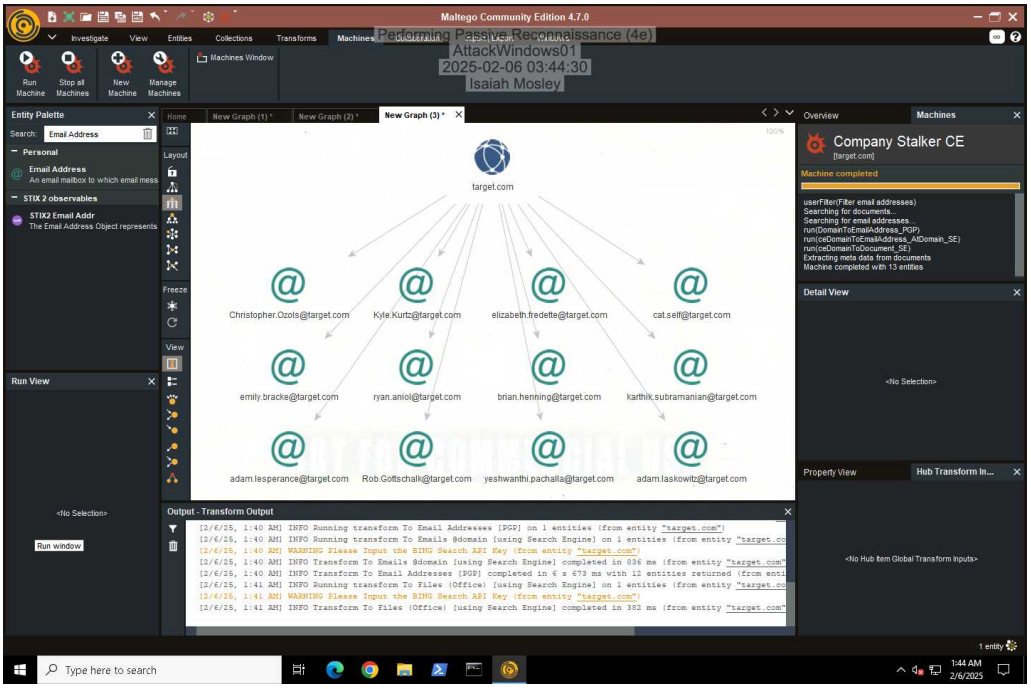


Part 2: Collect Information with Maltego

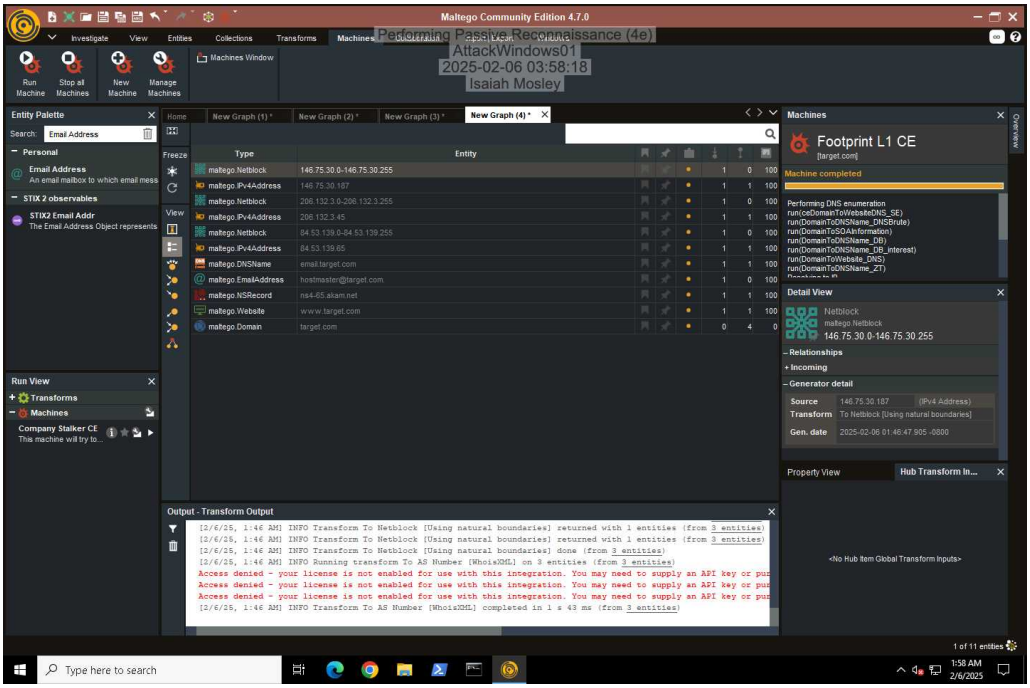
20. **Make a screen capture** showing the **graph of the NS Records for the target domain**.



28. **Make a screen capture** showing **the graph of the email addresses for the target domain**.



35. **Make a screen capture** showing the **first page of the IP addresses and domain names for the target domain**.



Section 3: Challenge and Analysis

Part 1: Perform Reconnaissance on a Chosen Target

Document the above details you discovered for your selected organization.

Incomplete

Part 2: Analyze Reconnaissance Results

Describe one or two possible scenarios in which these findings could be used in further ethical hacking endeavors.

Incomplete