Performing Passive Reconnaissance (4e)

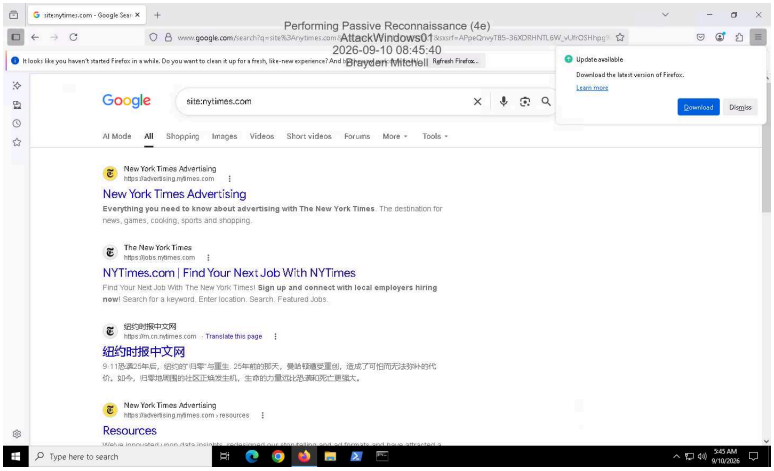
Ethical Hacking, Fourth Edition - Lab 01

Student: Brayden Mitchell
Email: brayden.m.mitchell@gmail.com
Time on Task: 1 hour, 55 minutes
Progress: 100%
Report Generated: Thursday, September 10, 2026 at 10:18 AM

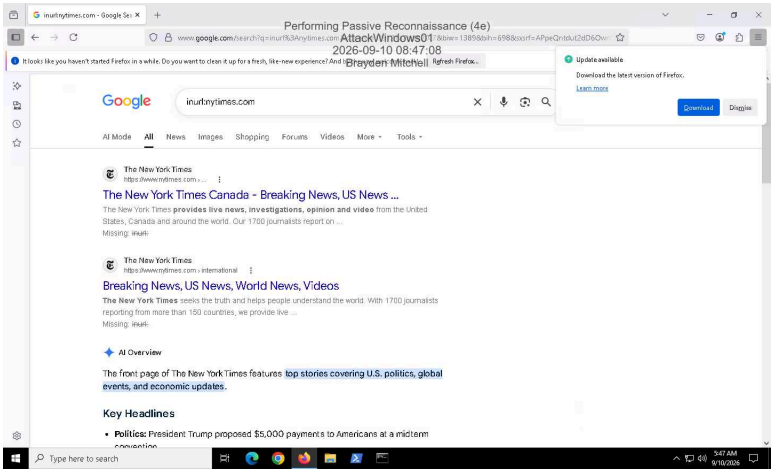
Section 1: Hands-On Demonstration

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.

You could map an organization's external/internet precense with related. During passive recon on a target company, "related:" can reveal sister companies,or partner organizations that might share infrastructure, credentials, or trust relationships which can then expand the attack surface understanding beyond the primary target.
You can identify trust relationships with link:. Finding who links to a target site can reveal other portals, vendor pages, or public pages where employees or partners discuss or share information about the organization which

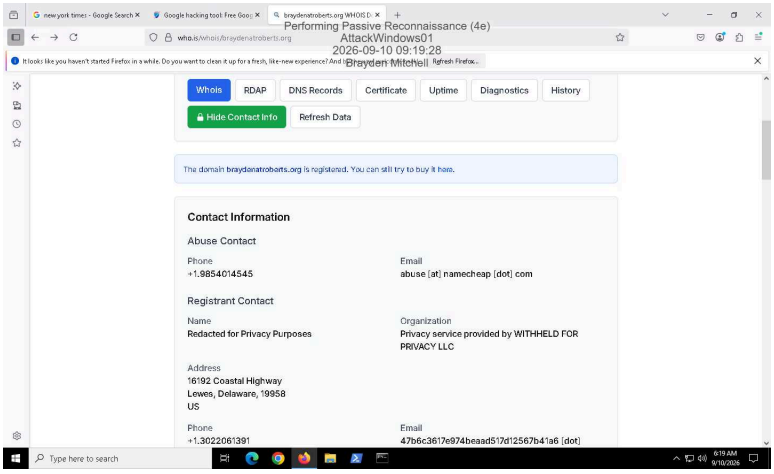
can be useful for social engineering.
You can assess cached content using info:. Checking Google's cached version of a page can reveal previously exposed content that may have since been removed or changed on the live site but still lingers in Google's cache.

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.

I didn't get any results but if I did, then it would provide me or the hacker a lot of information so that I wouldn't have to make a lot of guesses when starting my attack. There could be hidden credentials, open port logs, vulnerbility exposed in a database, and more which would allow me to have several immediate entry points to my attack on the organization.

Part 2: Explore the WHOIS Database

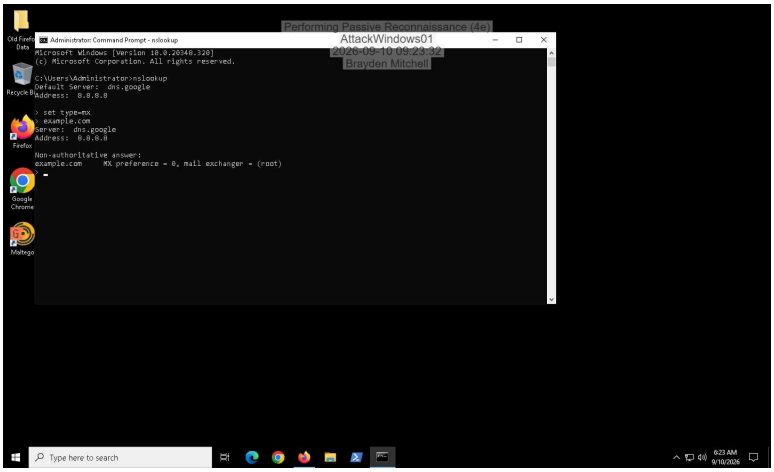
3. **Make a screen capture** showing the **results of the WHOIS search**.



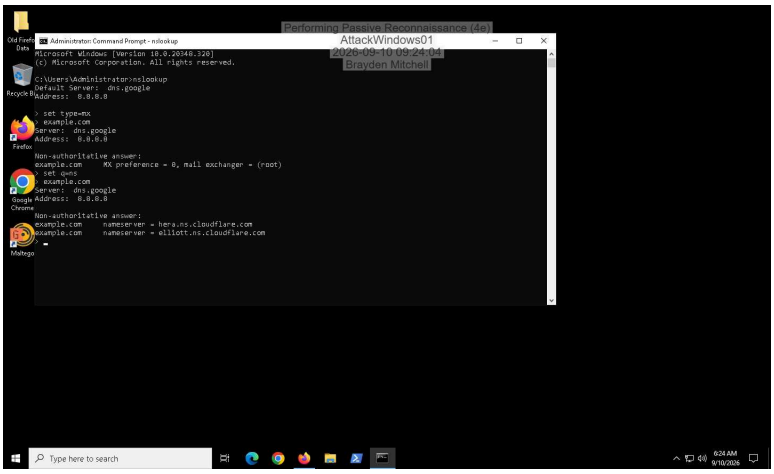
4. **Document** the **date of the most recent update** to the domain record.

September 9.2026 I actually just renewed this domain name yesterday

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



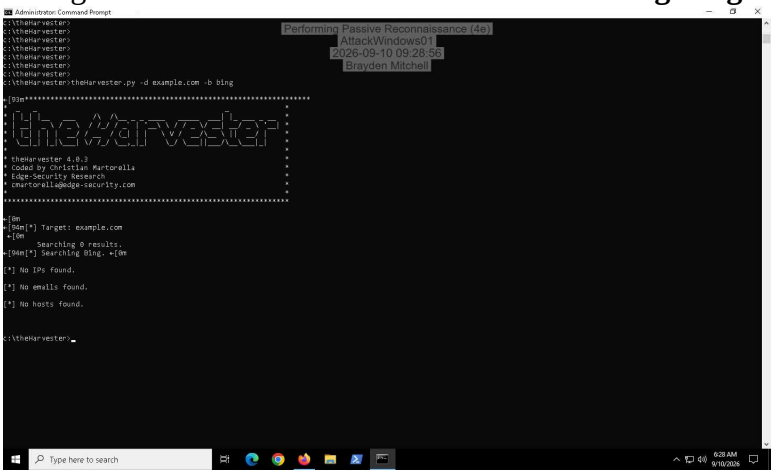
14. **Make a screen capture** showing the **results of the NS query**.



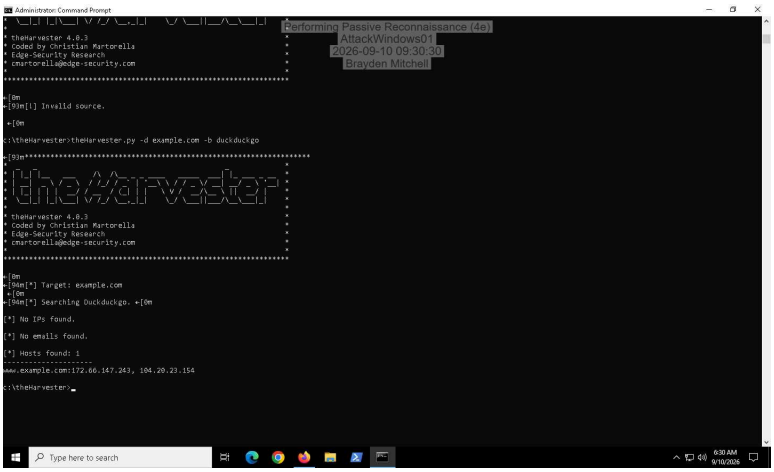
Section 2: Applied Learning

Part 1: Collect Information with TheHarvester

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

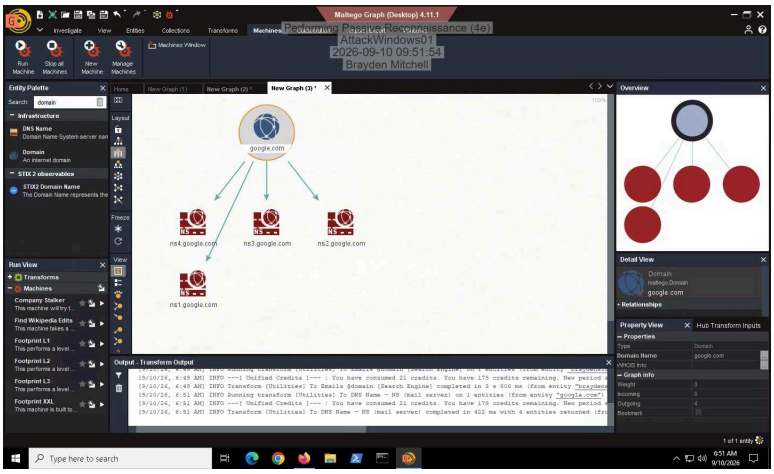


7. **Make a screen capture** showing the **search results from theHarvester using DuckDuckGo**.

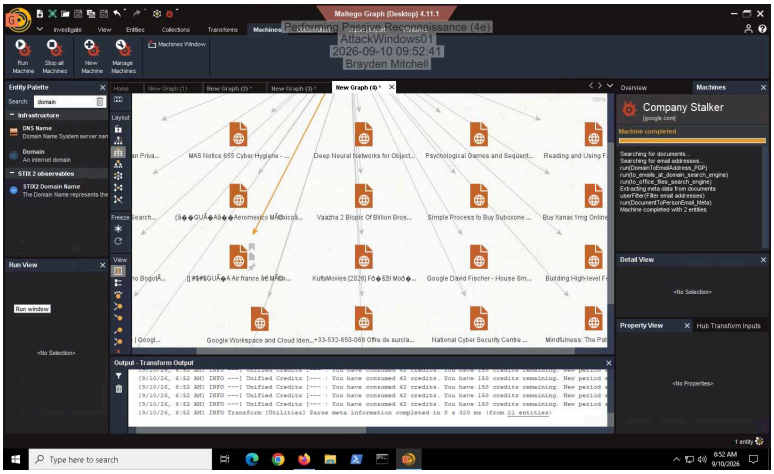


Part 2: Collect Information with Maltego

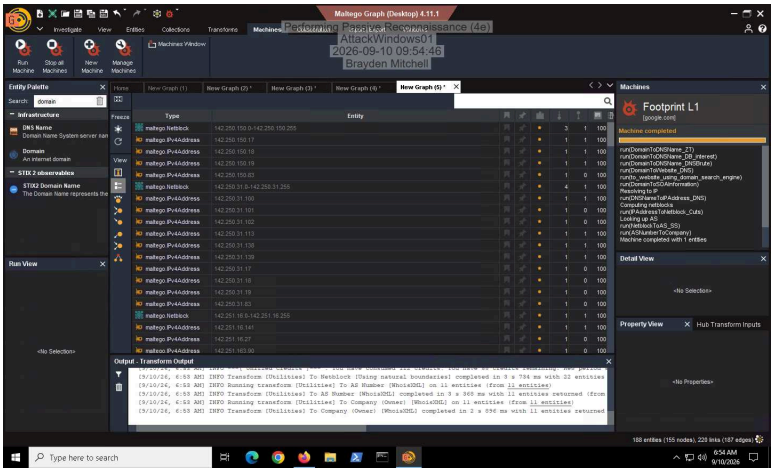
20. **Make a screen capture** showing the **graph of the NS Records for the target domain**.



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.

1. Amazon2. Amazon.com3. amazon.com4. 410 Terry Ave N, Seattle, WA 98109
5. Andy Jassy President & Chief Executive Officer (CEO) Oversees all of Amazon's global business segments

and operations
Jeff Bezos Executive Chair Founder and former CEO; remains active as the head of the Board of Directors
Brian T. Olsavsky Senior VP & Chief Financial Officer (CFO) Leads global financial strategy, budgeting, and investor relations.
Matt Garman CEO, Amazon Web Services (AWS) Runs Amazon's multi-billion dollar cloud computing and AI division.
Douglas J. Herrington CEO, Worldwide Amazon Stores Manages global e-commerce retail storefronts, physical stores, and fulfillment networks.
David A. Zapolsky Senior VP, Chief Global Affairs & Legal Officer Serves as general counsel, managing all legal, regulatory, and public policy affairs.
Shelley L. Reynolds VP, Worldwide Controller Serves as the principal accounting officer managing global accounting function
6. 5,000 + employees at each location, can reach up to 60,000 employees at a single location
7. AI, tech, manufacturers, and shipping companies all make deals with amazon to better their relationship, they are not exclusive in the slightest.

Part 2: Analyze Reconnaissance Results

Describe one or two possible scenarios in which these findings could be used in further ethical hacking endeavors.
Executives, have power. Just knowing their names and role is great information for a social engineering attack. Knowing the physical address and locations would be enough information for you to try and perform a physical penetration test. These 2 scenarios alone open tons of opportunities and all you need is 1 weak spot to get in. I would start with a phising attack from a spoofed executive email.