Section 2: Applied Learning

Note: SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will also conduct further investigation on one of the target web sites and expand on your Section 1 Research Report.

Please confirm with your instructor that you have been assigned Section 2 before proceeding.

1. On your local computer, **create** the **Lab Report file**.
   Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. If you already completed Section 1 of this lab, you will need to reset the virtual environment before beginning Section To reset the virtual environment, complete one of the following options.
   a. **Click Options > Reset Lab** to restore all virtual machines to their base state. This will take several minutes to complete. If you do not see the vWorkstation desktop after five minutes, **click Options > Reload Lab** to reload your lab connection.

   b. **Click Disconnect**, then **select Discard Changes** to end your lab session without creating a StateSave. If you previously created a StateSave, delete the StateSave at the launch page, then start a new lab session.

3. **Proceed** with **Part 1**.

Part 1: Technical Research

Note: In this part of the lab, you will use Sam Spade to further explore the domains you researched in Section 1 of this lab. This data-gathering process is important in the first phase of hacking.

When gathering information on a person or a digital footprint of a company, it is important to gather as much information as possible. You will be performing several different methods in extracting information. You will be responsible for determining what to document throughout this part of the lab to complete the research report in Part 3 of this lab.

1. From the vWorkstation, **launch** the **Sam Spade application**, then **search** for the target organization you selected in Section 1.

   If you were not assigned Section 1 of this lab, refer to Part 2 of this section for information about the requirements for the target organization. You will need to select an organization to research in order to complete the deliverable in Part 3 of this lab.

2. From the Sam Spade menu, **select Basics > Whois** to perform a WHOIS search on the target e-commerce organization you chose in Section 1, then **save the results** to the vWorkstation desktop as whois_*target*, replacing *target* with the name of the targeted organization you chose to research.

3. From the vWorkstation taskbar, **launch** a **command prompt window**.

4. At the command prompt, **execute** `whois domain.ext`, replacing *domain.ext* with the domain name and extension (for example, amazon.com) for the target organization you chose to research, to use the command line to generate a WHOIS search.

5. **Resize and move** the command prompt window and the Sam Spade window as necessary, then **compare** the **data generated** by both tools.

Note: The WHOIS registry service provides a wide variety of information about the registration of a domain, including the name of the domain owner, contact information for individuals responsible for the domain, and the identities of responsible nameservers. It is primarily used to verify whether the domain name is available or whether it has been registered.

By its nature, WHOIS information must be publicly available. Some companies may wish to disguise their ownership of a domain for a variety of reasons. Companies wishing to do so may choose to register domains through an agent. The agent’s contact information will then appear in the WHOIS results, concealing the actual owner of the domain.

6. From the Sam Spade menu, **select Tools > Fast traceroute** to perform a fast traceroute

search on the target e-commerce organization you chose in Section 1, then **save the results** to the vWorkstation desktop as traceroute_*target*, replacing *target* with the name of the targeted organization you elected to research.

7. In the command prompt window, **execute** `tracert domain.ext`, replacing *domain.ext* with the domain name and extension (for example, amazon.com) for the target organization you chose to research, to use the command line to generate a traceroute report.

8. **Resize and move** the command prompt window and the Sam Spade window as necessary, then **compare** the **data generated** by both tools.

Note: Traceroute shows the path a data packet traverses to get to a specific IP address. Traceroute, which is one of the easiest ways to identify the path to a targeted website, displays the list of routers on a path to a network destination by using time-to-live (TTL) time-outs and Internet control message protocol (IMCP) error messages. The program is available on both UNIX and Windows operating systems. In Windows operating systems, the command is known as *tracert*. In UNIX, the *traceroute* command is used.

9. From the Sam Spade menu bar, **select Basics > Dig** to perform a DIG (Domain Internet Groper) DNS query on the target e-commerce organization you chose in Section 1, then **save the results** to the vWorkstation desktop as dig_*target*, replacing *target* with the name of the targeted organization you elected to research.

10. In the command prompt window, **execute** `nslookup` to start the nslookup tool.

11. At the command prompt, **execute** `set type=any` to instruct the tool to return any information it uncovers for subsequent searches.

12. At the command prompt, **execute** `domain.ext`, replacing *domain.ext* with the domain name and extension (for example, amazon.com) for the target organization you chose to research, to use the command line to perform the query.

13. At the command prompt, **execute** `IPaddress`, replacing *IPaddress* with the IP address that you discovered in step 12 to use the command line to perform a reverse DNS query.

14. **Resize and move** the command prompt window and the Sam Spade window as necessary to

compare the **data generated** by both tools.

Note: Nslookup is a program that queries Internet domain name servers (DNS). The nslookup utility will use the system's primary DNS IP. Running the nslookup command from your local computer system will yield the same results, but use a different default DNS.

15. At the command prompt, **execute** `set type=soa` to specify the start of authority (SOA) for the nslookup query.

Note: The SOA record for a domain stores information about the server. The following list describes some common results provided by an nslookup query. Use this information to interpret the results of your own queries.

Server: FQDN (Fully Qualified Domain Name)
Address: IP Address of the FQDN (DNS)

Non-authoritative answer: A non-authoritative name server is one that does not contain the records for the zone being queried
domain.ext

- **primary name server** = The Name Record Server FQDN
- **responsible mail addr** = If there is a MX (Mail Exchange) record present, oftentimes, this is left with *namehost.DomainExample.com*
- **serial** = The revision number of this zone file. Increment this number each time the zone file is changed so that the changes will be distributed to any secondary DNS servers.
- **refresh** = The amount of time in seconds that a secondary name server should wait to check for a new copy of a DNS zone from the domain's primary name server. If a zone file has changed then the secondary DNS server will update its copy of the zone to match the primary DNS server's zone.
- **retry** = The amount of time in seconds that a domain's primary name server (or servers) should wait if an attempt to refresh by a secondary name server failed before attempting to refresh a domain's zone with that secondary name server again.

- **expire** = The amount of time in seconds that a secondary name server (or servers) will hold a zone before it is no longer considered authoritative.

- **minimum** = The amount of time in seconds that a domain's resource records are valid. This is also known as a minimum TTL, and can be overridden by an individual resource record's TTL.

- **default TTL (time to live)** = The number of seconds a domain name is cached locally before expiration and return to authoritative nameservers for updated information.

DNS and web servers may live anywhere in the world with internet, and a single domain may not necessarily have these servers in the same location.

16. At the command prompt, **execute** ***`domain.ext`***, replacing *domain.ext* with the domain name and extension (for example, amazon.com) for the target organization you chose to research, to use the command line to perform the query.

17. In your Lab Report, **record** any useful technical information you gathered for your target domain in this part.

18. **Close** the **command prompt window**.

Part 2: Public Domain Research

Note: Search engines allow data gatherers to find a large amount of information about a company, using not only the officially released information but also information in publications and other websites. In the next steps, you will use Google.com from your local computer to capture data about a targeted company that might be useful in performing a potential attack on that company's corporate website.

In the next part of this lab, you will create a report of your research findings as if you were an ethical hacker gathering information for a client. You will be responsible for determining what to document throughout this part of the lab to complete this report.

If you completed **SECTION 1** of this lab, skip to Part 3 of this Section.

1. From the vWorkstation, **launch Internet Explorer** to open a new browser window.

   If you prefer, you can complete Parts 2 and 3 of the lab from your local computer instead.

2. **Select** a **target organization** with an e-commerce website, such as Target or Amazon. You can target an organization with which you are already familiar, or use the browser's search tool to identify a potential target organization.

3. In your browser's address box, **type** `google.com` to open the Google search tool.

4. Using Google as your search engine, **locate** the following information about your target organization and **record** it in your Lab Report file. Use screen captures in your Lab Report file where necessary to illustrate your findings.

   - Name of the target organization
   - Domain name and extension (*domain.ext*) for the target organization (for example, amazon.com)
   - URLs for the e-commerce website and any social networking sites
   - Physical address of the main headquarters location used by the target company; use Google Maps to locate the building.
   - Names of officers (for example, CEO, president, and CIO) at the organization
   - Number of employees at each major physical location
   - Business partners or clients of the organization

Part 3: Research Report

Note: In the next steps, you will write a narrative research report that includes specific information about the results of the research you conducted earlier in this lab.

If you completed Section 1, use the Hacking Research Report you created in that portion of the lab as a draft and update it with the research you conducted in Section 2 of this lab. Your final report from Section 2 will be the required deliverable file from this lab.

1. On your local computer, **create** a new document called **Hacking Research Report** that includes the following sections:

   - **Executive Summary:** Write a 2-3 paragraph summary of the information you uncovered in Parts 1 and 2 of this lab and how an attacker might be able to exploit this information. It may be helpful to write the Executive Summary *last*, after you have completed your analysis in the other sections of the research report.

- **Methodology:** Describe the tools and techniques that you used to conduct both the technical research and public domain research in this report.
- **Technical Research Results:** Summarize the results of your technical research into Apple.com, Microsoft.com, and Facebook.com from Part 1 of the lab.
- **Public Domain Research Results:** Summarize the results of your public domain research into the targeted company from Part 2 of the lab.
- **Findings and Conclusions:** Present your detailed conclusions about each of the four companies (Apple.com, Microsoft.com, Facebook.com, and the company you chose in Part 2).
- **Avenues of Further Research:** Describe what additional research you might conduct to learn more about the four companies. If you were planning a hacking attack, what questions might you try to answer?

Note: This completes Section 2 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

2. On the vWorkstation desktop, **drag** the deliverable files into the File Transfer folder to complete the download to your local computer.

   - whois_*target*
   - traceroute_*target*
   - dig_*target*