Christopher Bazyani

CYB 552

Advanced Hacking Prevention

Lab 3

Data Gathering and Footprinting on a Targeted Web Site

**Section 1: Hands-On Demonstration**

Part 1: Technical Research

On the vWorkstation desktop, double-click the Sam Spade icon to open the Sam Spade application

Maximize the Sam Spade window

Sam Spade is a non-intrusive tool. While it provides quite a bit of information about a domain, it is merely combining publicly available information from a variety of sources

In the blank textbox under the Sam Spade menu, type the first domain that you wish to find information about: apple.com

As soon as text is entered into this field, the grey arrow to the right of the text box will turn purple

Click the purple arrow to start the WHOIS (Basics > Whois) query for this domain

Graphical user interface, text, application

Description automatically generated

From the Sam Spade menu, click File and select Save As

Graphical user interface, text, application

Description automatically generated

In the Save As dialog box, select Desktop from the Save in drop-down menu, then type whois domain in the File Name box, where domain is the name of the domain that you just investigated, and click Save to close the dialog box

Graphical user interface, application

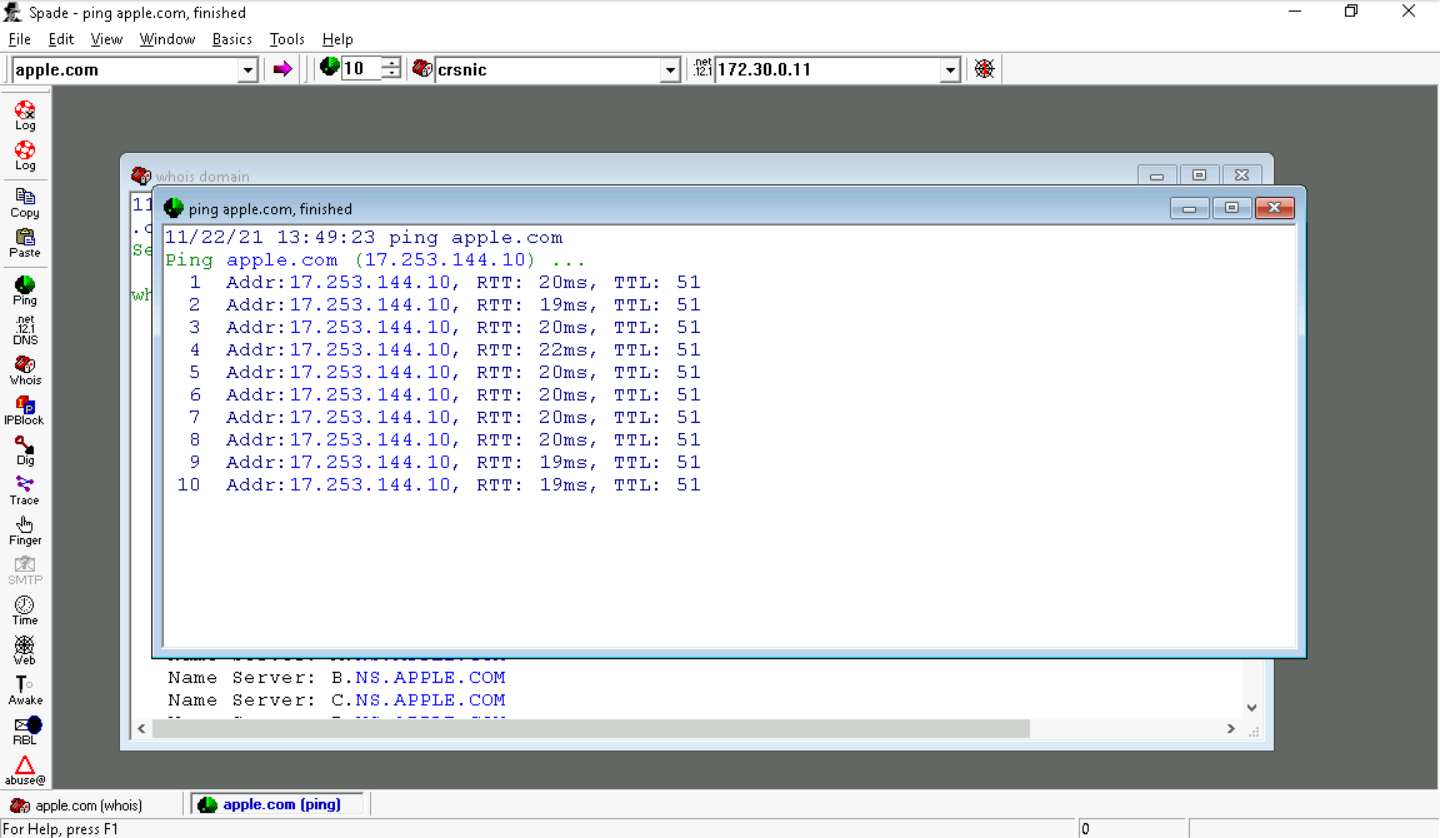
Description automatically generated

You will repeat these steps for additional domains, then use the information in these files to compile a report in Part 3 of this lab

From the Sam Spade menu, select Basics > Ping to initiate pinging the Apple.com server

Graphical user interface, text, application

Description automatically generated



Close the ping Apple.com, finished window

Close the whois Apple.com, finished window

Explore the other options in the Basics and the Tools menus

Repeat steps 3-12 for the following domains

Microsoft.com

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

Facebook.com

Text

Description automatically generated

Text

Description automatically generated

Close the Sam Spade window

From the Windows taskbar, right-click the Windows Start icon and select Run from the menu

In the Run window, type cmd and press Enter to open a command prompt

Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

In the command prompt window, type nslookup apple.com and press Enter to perform a DNS search on your target domain

Text

Description automatically generated

The nslookup tool is designed to perform DNS queries, allowing you to look up the DNS records associated with a given domain name

Make a screen capture showing the nslookup results and paste it into your Lab Report file

Repeat steps 17-18 for the following domains:

Microsoft.com

Text

Description automatically generated

Facebook.com

Text

Description automatically generated

At the command prompt, type tracert apple.com and press Enter to perform a trace route search on your target domain

Text

Description automatically generated

The traceroute tool is used to identify the network path that must be followed to reach one system from another. It provides the names and IP addresses of all intermediate systems and can be used to identify potential intermediate attack points. It may also be used to estimate the geographic location of a server

Repeat steps 20-21 for the following domains:

Microsoft.com

Text

Description automatically generated

Facebook.com

Text

Description automatically generated

At the command prompt, type exit and press Enter to close the command prompt window

Part 2: Public Domain Research

On the vWorkstation taskbar, click the Internet Explorer icon to open a new browser window

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

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

In the browser’s address box, type google.com to open the Google search tool

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

Outlook

* Domain name and extension (domain.ext) for the target organization (for example, amazon.com)

outlook.com

* URLs for the e-commerce website and any social networking sites

https://outlook.live.com/owa/

* Physical address of the main headquarters location used by the target company; use Google Maps to locate the building

One Microsoft Way, Redmond, WA, USA

Zip Code: 98052

* Names of officers (for example, CEO, president, and CIO) at the organization

Satya Nadella, CEO

Brad Smith, President

Jim DuBois, CIO

* Number of employees at each major physical location

181,000

* Business partners or clients of the organization

10th Magnitude, Azure, Central Chicago, Ill

6th Street Consulting, SharePoint, Cloud West, Redondo Beach, CA

A.B. Computer Systems Inc., Dynamics, East Melville, N.Y

**Section 2: Applied Learning**

Part 1: Technical Research

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

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

Graphical user interface, text

Description automatically generated

From the vWorkstation taskbar, launch a command prompt window

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

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

From the vWorkstation taskbar, launch a command prompt window

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

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

Graphical user interface, text

Description automatically generated

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

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

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

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

Text

Description automatically generated

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

Graphical user interface

Description automatically generated

A screenshot of a computer

Description automatically generated

In the command prompt window, execute nslookup to start the nslookup tool

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

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

Text

Description automatically generated

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

Resize and move the command prompt window and the Sam Spade window as necessary to compare the data generated by both tools

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

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

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

Text

Description automatically generated

Close the command prompt window