Mini-project 2: Network Auditing

Goal: The goal of this project is to learn how to perform an audit on a network with the intention to discover interesting characteristics and phenomena. The project is mostly open-ended (that is, there is no specific correct answer, and I do not have a working "solution."). In doing so, you will be required to be creative and learn new tools. Students will turn in project reports that describe both their findings and techniques used to determine the findings. Any custom scripts or tools built for the project will also be submitted.

Collaboration: Students may work in teams of 1 or 2 students. No other collaboration is allowed.

Dataset: For this assignment, you must create a censys.io account. Once you have an account you will perform an audit on NC State's networks using the IPv4 Hosts Search. **Note:** *do not use tools that perform active scans on the NCSU networks*, **you must use censys.io**, unless noted otherwise.

Responsible Disclosure: As a result of this project, you may find a security issue within the NCSU network. We ask that you do not publicly disclose (Tweets, Snapchat, Blog Posts, etc.) any information about your findings for 90 days after the homework is due. This will allow us to report the findings to Security and Compliance and give them time to address the issue. However, you may discuss your findings with the instructor staff or students in the class after the assignment is due.

Grading

Project 2 is worth 100 points, as specified in Table [tbl:breakdown]. All figures and tables in the project report must have a caption with a label of Figure X. or Table X. These labels are really helpful to use during discussion as a reference. **Note:** figure captions are generally placed under the figure, and table captions are generally placed above the table.

Table 1: Point value for each section.

Section	**Points**
Question 1	20
Question 2	40
Question 3	30
Question 4	10

Question 1: Network Address Identification {20 points}

Before performing an audit you should always be sure the network addresses you plan to analyze belong to the organization agreeing to be audited. The goal of this question is to familiarize the student with doing necessary reconnaissance and background research before performing an audit.

NC State owns multiple IPv4 network blocks. Identify *at least* 2 IPv4 blocks. For each block you identify, list the CIDR block, Network Name, Autonomous System Number (ASN), and Autonomous System Name. Additionally, describe your process for how you found this information, including screenshots as needed. You must start your search using censys.io, but may include information from links provided in the censys.io results. **Reminder:** *Do not use any tools that perform an active scan on the NCSU Network.*

Question 2: Network Summary {40 points}

Once you have a list of target IP addresses (Question 1 above). The next step is to identify hosts on the network. The goal of this question is to familiarize the student with gathering information about the network and organizing the information into a report that helps triage potential security issues.

Using censys.io perform an IPv4 Hosts Search on the network blocks identified in Question 1. Visualize the results of the search using tables or charts (e.g., bar graph). Include a discussion that interprets your visualizations, justifies why your visualizations are useful, and describes how you obtained the data. Note: it may be easier to get familiar with the search functionality using the web interface, but I highly recommend using the API and writing Python scripts to save the results locally and then processing it with offline tools. This reduces the number of queries you will have to perform. **Reminder:** *Do not use any tools that perform an active scan on the NCSU Network.*

You must appropriately visualize and discuss the following information to receive 30/40 points: (1) hosts by operating system, (2) hosts by web server (Apache, Nginx, IIS, etc.), and (3) hosts by protocol. **To receive the other 10 points you must be creative and go beyond the bare minimum described above.**

To build your charts you may use any software you like, below are some suggested tools:

- Gnuplot is a command line graphing utility.
- Spreadsheets such as Microsoft Excel, LibreOffice Calc, or Google Sheets all have the capability to create charts.
- Plotly may be particularly useful for those using the Censys Python API to perform queries. After retrieving the data from Censys, you can easily output a Plotly chart from your script.

Figure 1 shows an example bar chart made with Plotly. You should use this as inspiration to create a chart using real data in your solution.

Question 3: Interesting Security Findings {30 points}

The final step of an audit is to find and report security issues on the network. The goal of this question is to familiarize the student with identifying security issues in a network.

Starting from the data you collected from censys.io, document an interesting security-related finding. Discuss why you found it interesting, background information about the finding, recommendations on how to address what you found, and a description on how you discovered the security issue. Hint: you may create an account on shodan.io and use the Shodan API to identify security issues. The free version of Shodan limits the number of queries you can do per month, but we can use our censys.io information to more efficiently use Shodan.

For example, you may find a vulnerable host on the network. Give information about the vulnerable host, what the vulnerability is (cite a CVE if possible), and a description of how you found the vulnerable host on the network. A vulnerable host is not the only kind of security-related result, be creative. **Reminder:** *Do not use any tools that perform an active scan or probe on the NCSU Network.*

If you are unable to find anything interesting, describe your thought process for partial credit. Please be as verbose as possible, describing what you tried and why you tried it. Also any partial successes and possible reasons to why you think your approach was not successful.

Bonus (5 Points): We will try to report all findings to Security and Compliance at NCSU. If they confirm your findings are an issue, we will give additional bonus points. Note, it may take time to get a response so bonus points may be awarded after receiving your initial grade.

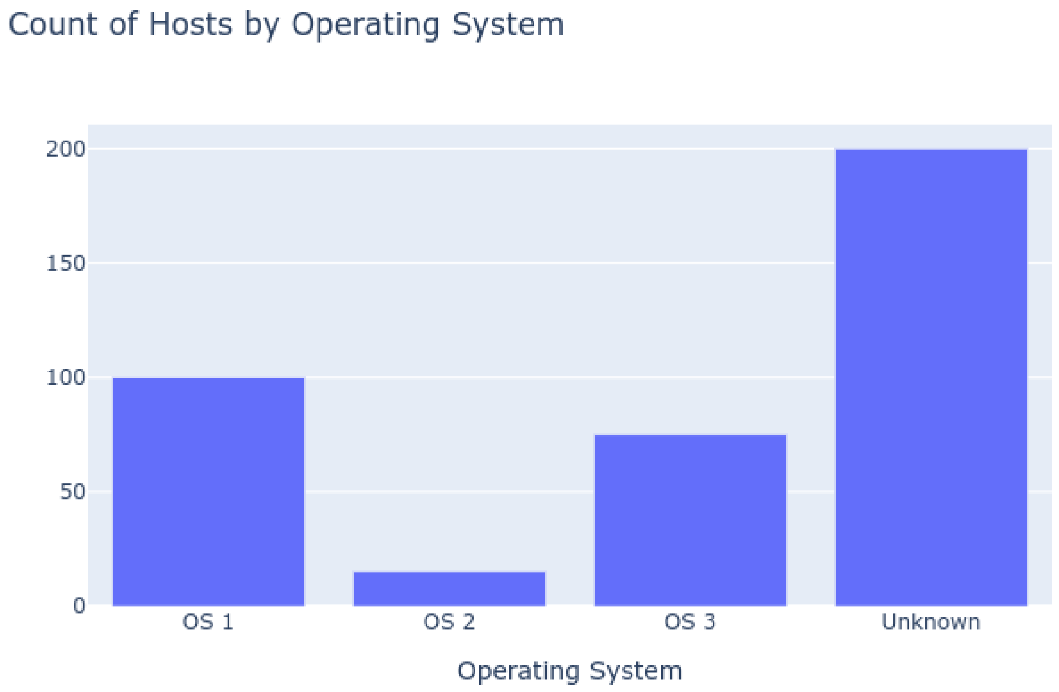

Figure 1: Sample figure showing bar chart for a limited number of Operating Systems.

Question 4: Impact of IPv6 {10 points}

Censys and Shodan continuously scan the Internet to build their host databases. Discuss how IPv6, which use 128 bit addresses rather than 32 bit addresses, may impact the effectiveness of these tools. Scanning the IPv6 Internet: Towards a Comprehensive Hitlist may be a good place to begin your research. Remember to cite any sources you use.

Submission Instructions

Submit your solution as two separate files using WolfWare (one .pdf, one .tar.gz or .zip). To upload your assignment, navigate to the CSC574 course. Use the “Project 2” assignment under “Mini-Projects.”

The first file should be a single PDF document with your report. **Writeups submitted in Word, PowerPoint, Corel, RTF, Pages, and other non-PDF or ASCII formats will not be accepted.** Consider using LaTeX to format your homework solutions. (For a good primer on LaTeX, see the Not So Short Introduction to LATEX.) The second file should be a tarball (`.tar.gz`) or Zip (`.zip`) of any custom tools that are relevant to your report.

Please post questions (especially requests for clarification) about this homework to Piazza.