P3 Team H: Internet Vulnerabilities in Educational Institutions

Brandon Sanders Natasha Levey Fareya Ikram

Abstract

With the dawn of the internet of things, a major spotlight has been placed on insecure networked systems and services. In this paper, we perform a survey of Massachusetts colleges to see how many of them use technologies that are discoverable on the open web, and how many of them use technologies that are regarded as insecure.

1. Introduction and Hypothesis

> ***Note:*** This paper is based on our originally submitted proposal for Project 3, and reuses the verbiage from that document.

In this paper, we hope to answer a single question: Are liberal arts colleges, which grow thought-leaders and philosophers, doing as much work as technical and engineering colleges in order to protect their institutional networks?

Our initial hypothesis is that liberal arts colleges are not adequately protecting their institutional networks, since they are generally less technoloy-oriented and thus have less of a focus on protecting their networks.

2. Methodology and Assumptions

To prove our hypothesis, we will analyze the following data:

1. The most frequently attacked (e.g., ***vulnerable***) network ports.
2. The colleges that have ***any*** publicly-discoverable network ports.
3. The colleges that have any ***vulnerable*** ports.
4. The percentage of these colleges that are strongly affiliated with the Liberal Arts.

We will limit our search to only the colleges in the state of Massachussetts in order to fit within the constraints of this study. For each college, we will determine if they are strongly affiliated with the Liberal Arts based on their website and matriculation data from the National Center for Education and Statistics (https://nces.ed.gov/collegenavigator/).

2.1 Vulnerability Criteria

We utilized Norse Corp's cyber attack thread map (http://map.norsecorp.com) to determine the most vulnerable network ports. After running their web application for several minutes, the following ports rose to the top of the attack list:

- 25 (SMTP)
- 23 (Telnet)
- 5900 (VNC)
- 8080 (HTTP)
- 445 (MS Active Directory)
- 3389 (MS Terminal Server)
- 50864 (XSAN FS?)
- 123 (Network Time Protocol)
- 53413 (XSAN FS?)
- 1433 (MS SQL)

In addiiton to these ports, we also included Port 22, which is used for the Secure Shell (SSH) protocol, and is commonly attacked by bad actors world-wide.

2.2 Vulnerability Data and Analysis

We used Shodan (https://www.shodan.io), an Internet of Things search engine, to obtain a list of publicly-discoverable web services belonging to all college-like organizations in the state of Massachussetts.

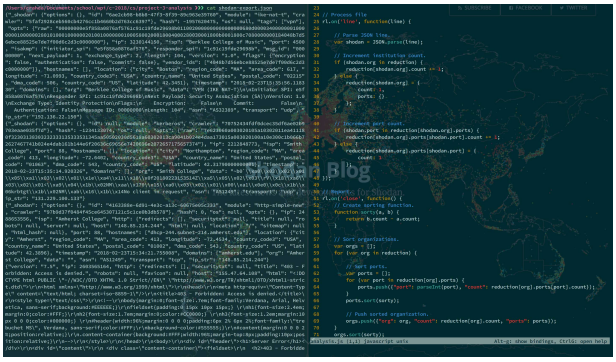

Figure 1: Left: Sample of raw JSON from Shodan.io, Right: Excerpt of Node.js map-reduction script

The raw JSON-formatted results of our Shodan search were too large for manual processing, so we developed a Node.js script to perform a map-reduction operation on the results to convert them to a parseable format (Fig. 1). We then utilized C3 (a wrapper library for the D3, https://d3js.org/) to graph these results for analysis (Fig. 2, Fig. 3).

3. Results

The top ten universities that appeared in our results (Fig. 2) identify themselves as liberal arts colleges. The top ten included:

- Smith
- Amherst
- Emerson
- Williams
- Boston
- Babson
- Simmons
- Mount Holyoke
- Hampshire

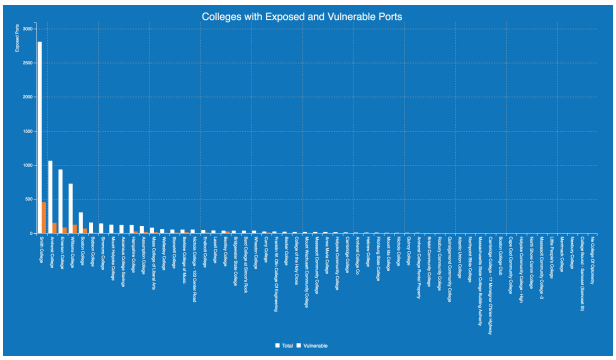

Figure 2: Graph of all ports in detected institutions

- Mass College of Liberal Arts
- Wellesley

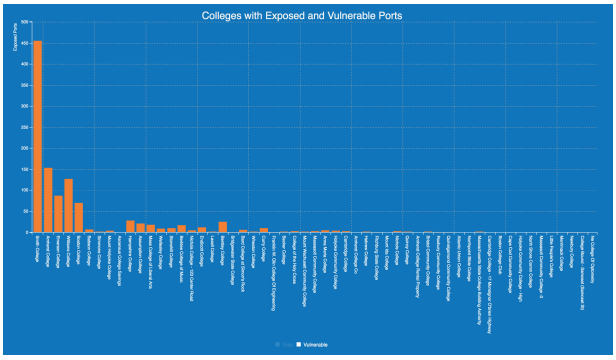

Figure 3: Graph of all vulnerable ports in detected institutions

Of these top ten universities, nine of them had one or more vulnerable ports (Fig. 3).

3.1 Conclusions and Future Work

These results support our hypothesis, demonstrating that liberal arts colleges in Massachusetts are more vulnerable to network attacks than non-liberal arts colleges. This may be because they do not focus on securing their network infrastructure or that they simply do not know that the ports that they are using are vulnerable.

To gain a deeper understanding of this problem in the future, we could extend our investigation to reach out to the IT departments of these colleges and ask them if they know if there ports are exposed and vulnerable. We could also extend this experiment beyond Massachusetts to see if this is truly a problem for colleges across the country, and gather data on which vulnerable ports are most common nationwide.

4. Sources Cited

This paper, the associated presentation, and all analysis scripts and data are publicly available on Git Hub (https://github.com/Mizumi/college-vulnerability-analysis). In addition, the presentation (http://quirky-murdock-e9a5b2.netlify.com/presentation) and D3 graphs (http://quirky-murdock-e9a5b2.netlify.com) may be viewed directly online.

- https://www.shodan.io
  - https://www.shodan.io/search?query=org%3Acollege+state%3AMA
  - https://maps.shodan.io/#42.12980284036179/-72.32025146484375/9/light/org:college%20state:MA
  - https://www.shodan.io/report/EPJF2Sy8
- http://map.norsecorp.com
- https://www.csoonline.com/article/3217944/security/8-top-cyber-attack-maps-and-how-to-use-them.html