



STEAM's Pen-Test Report

Private and Confidential

This penetration test was conducted throughout the month of May of 2025 on behalf of scholars at the STEAM center.

Executive Summary

The Brooklyn STEAM Center has been around since 2019 and since then there has been no update to its network infrastructure since. Because of this our team's project is to break into the Public Announcement system (PA). Since we were successful in doing so we have also numerous devices that are or could be compromised. Below is a list of what we found and how we did it.

The objectives of this test include the following:

- Identify vulnerabilities of systems that are used day to day.
- Validate pre-existing vulnerabilities on systems found on CVE's.
- Exploiting vulnerabilities to test its integrity towards the network, and its security.



Fig.1 PA Brand, Identifiable name & MAC Address

We first found the MAC Address and name

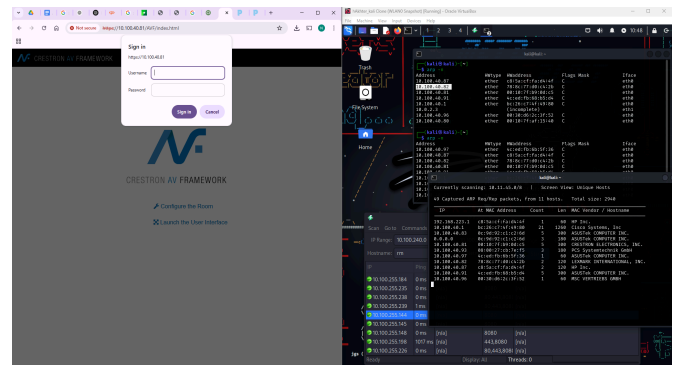


Fig.2 Angry IP Scanner & NMAP

Name Since indeifable information was found, we then started to conduct NMAP and Angry IP scanner scans on the neetwork to try and find it



Wi-Fi TCP/IP DNS WINS 80

IPv4 Address: 10.197.146.73

Router: 10.197.144.1

Network Address	Usable Host Range	Broadcast Address:
10.100.0.0	10.100.0.1 - 10.100.7.254	10.100.7.255
10.100.8.0	10.100.8.1 - 10.100.15.254	10.100.15.255
10.100.16.0	10.100.16.1 - 10.100.23.254	10.100.23.255
10.100.24.0	10.100.24.1 - 10.100.31.254	10.100.31.255
10.100.32.0	10.100.32.1 - 10.100.39.254	10.100.39.255
10.100.40.0	10.100.40.1 - 10.100.47.254	10.100.47.255
10.100.48.0	10.100.48.1 - 10.100.55.254	10.100.55.255
10.100.56.0	10.100.56.1 - 10.100.63.254	10.100.63.255

10.100.33.84

Shared with me - Google Drive

20021: Penetrating & Securing PA...

Unleashing Hydra: Exploring

[illegible]

The screenshot displays the BOGEN E7000 web interface. At the top, the header includes the logo, version (E7000), and a status bar with 'Ready: 07/08/2018', 'Time: 0:01:00', 'User: A1234', and 'Extension: 1000'. A red banner at the top right contains the text: 'This extension is not connected to the server. [Refresh]'. The left sidebar contains a navigation menu with icons and labels: Home, System Parameters, Call Transfer and Groups, Device, Features, Extensions, Groups, Calendar, Hold Calls, Advanced Configuration, Call Configuration, Admin Groups, Features, Single Services, Incoming Services, Audio, Announcements, Playlists, Recordings, Groups, and Internet Phone Services. The main content area is titled 'Dashboard' and includes a 'Incoming Calls' section. Below this, there are three main functional areas: 'Calling-Planing' (with icons for Monitoring, Dial Pad, Page Selection, Call Forwarding, and Page), 'Multi-Office Calling-Planing' (with icons for Routing Plan, Make into All Call, Forwarding Plan, Multi-Office Forwarding All Call, and Forwarding Plan), and 'Services/Announcements' (with icons for New Announcement, Alarm, and Stop Announcement). At the bottom, there is a 'Weekly Schedule' section with a table showing days of the week and their corresponding status (e.g., May 1, May 2, May 3, May 7, May 8, May 9, May 10). The table has columns for Sun, Mon, Tue, Wed, Thu, Fri, and Sat.

Fig.5 control interface

Once we were able to login, we were then able to record the message we wanted and play it over the speakers through the STEAM center. We were also able to view classroom details such as IP addresses, names, and etc.

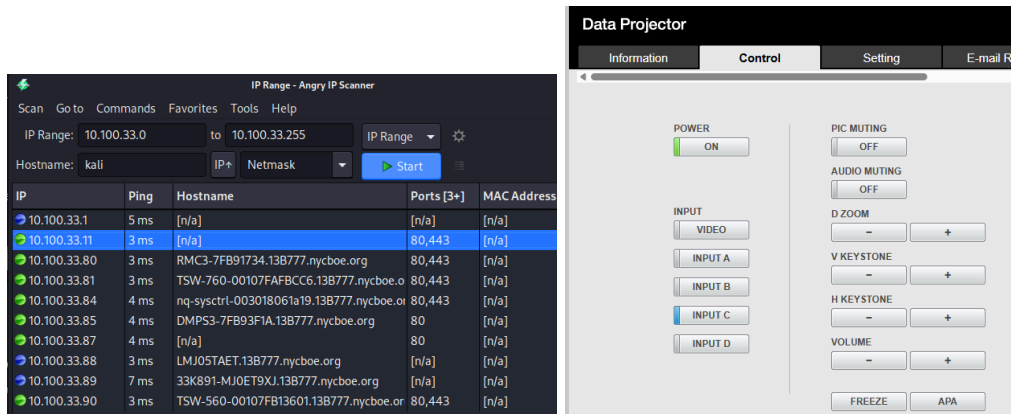


Fig.6 Commonas projector interface

Looking back on the range that we found the PA system on, we also found the Commons projector and alongside printers, and creaston devices.

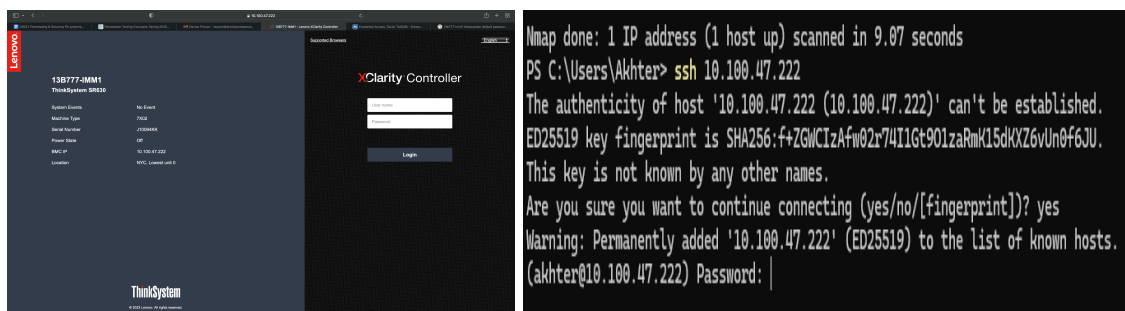


Fig.7 Lenovo Clarity Controller & exploitable port

Another device that was discovered was a Lenovo server with ports 22 & 23 open which is Telnet and SSH. These ports allow you to remote into the server from anywhere, and telnet does the same but it is an insecure connection.

RISK ASSESSMENT MATRIX				
SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Key findings and recommendations response:

STEAM's network environment is vulnerable to potential cyber attacks that pose a significant risk towards the school in terms of staff/students confidentiality, systems integrity, and overall the STEAM's security. To help decrease the severity of these risk we recommend

- Changing any and all default credentials still in use (Tools: [PW Strength tester](#))
- Disable insecure ports and put in some type of parameter in place for SSH ([Changing default port](#), Public Key Authentication, [Restrict SSH Access to specific IP Addresses](#), etc)
- Use HTTPS instead of HTTP for more secure browsing

