

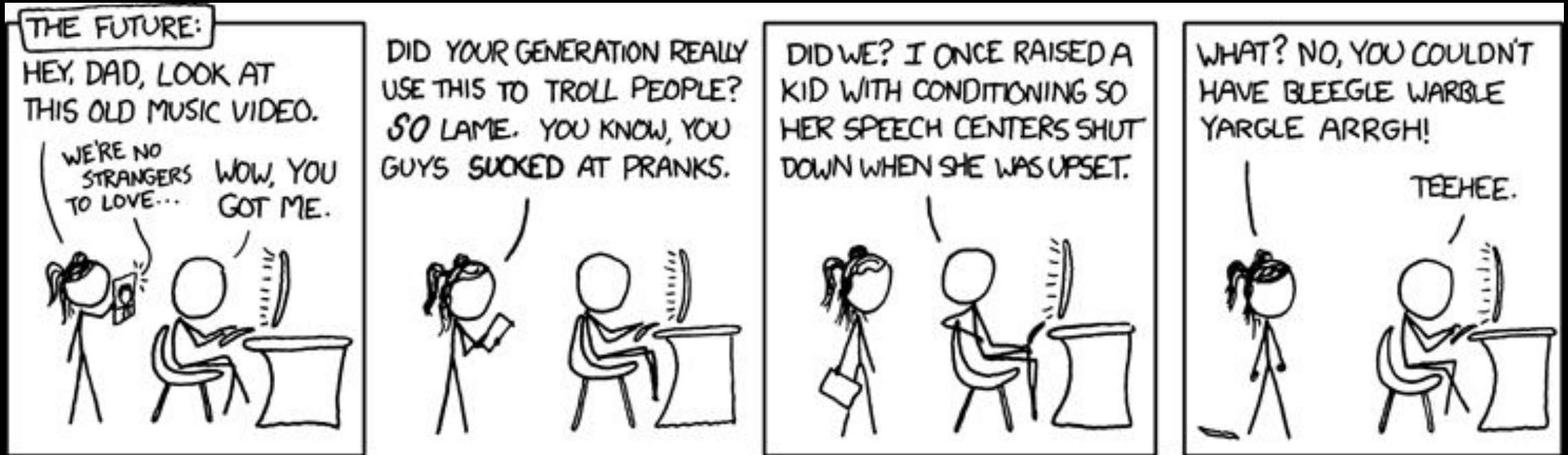
Week 08

The Big Rick

Minh Duong



sigpwny{dQw4w9WgXcQ}



Announcements

Fall CTF (HACK-athon) went great! In total 100+ (70 IRL) attended!

Details on Halloween Get Together



Disclaimer

Never ever do anything similar to what I did without permission



What is Rickrolling?

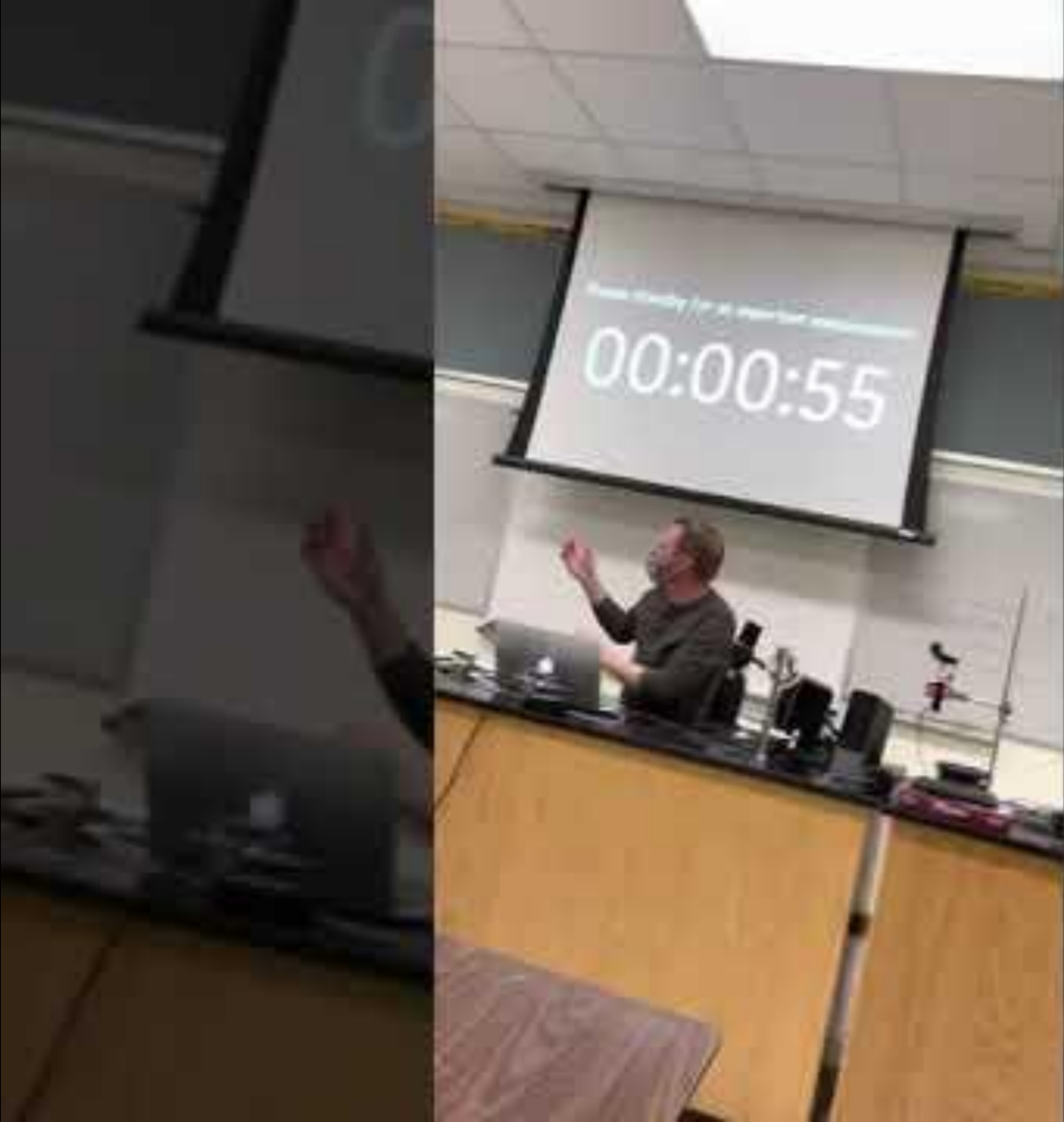
- The unexpected appearance of the music video for "Never Gonna Give You Up," performed by Rick Astley
 1. Bait-and-switch using a disguised hyperlink that leads to the music video
 2. Using the song's lyrics, or singing it, in unexpected contexts
- The song is from 1987, but rickrolling wasn't a meme until 2007



What is the Big Rick?

- A senior prank I organized which involved rickrolling my high school district using hacked Internet-of-Things (IoT) devices
 - Context: my high school district has 6 different high schools, each with about 2000 students





But how?

- In my freshman year (2017), I scanned the district network for devices running web servers (ports 80, 443, 8080)
 - Found printers, IP phones, security cameras, networked TV (IPTV) system exposed to student network



But how?

- In my freshman year (2017), I scanned the district network for devices running web servers (ports 80, 443, 8080)
 - Found printers, IP phones, security cameras, networked TV (IPTV) system exposed to student network
- In other words, my school district's security sucked



Security Cameras



Security Cameras




Avedia System (IPTVs)

- AvediaPlayer receivers act as an interface to control projectors and displays
- AvediaServers control AvediaPlayers and other Avedia products



Web Interface

AvediaPlayer Receiver



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

- ▶ 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



Controlling the Receivers

- Scripted local HTTP requests that would control projectors
 - Max volume
 - Power on
 - Switch input to custom stream
- Distributed the script to all the receivers
 - Execute the script via SSH from AvediaServer

No real command-and-control payload because of weird IoT architecture on the receivers + no time to learn how to code one

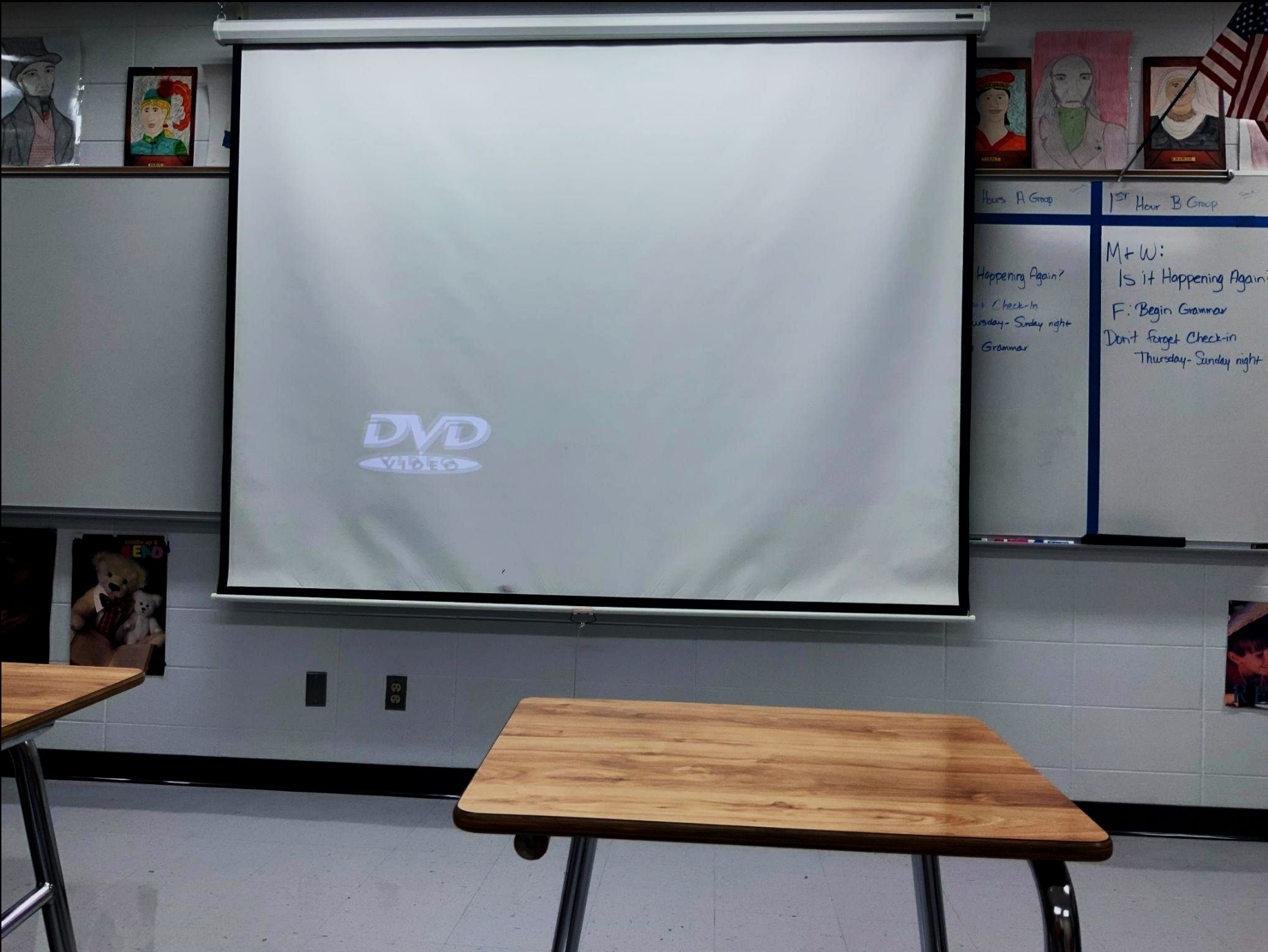


Testing the Stream

- Most stream tests were at night by using webcams in computer lab pointed at the projector
- Final stream tests were done with students at each school confirming they worked
- I lived right across the street from my high school and could watch the projectors from my house through the windows







Hours A Group

1st Hour B Group

Happening Again?

Check-in
Thursday-Sunday night
Grammar

M+W:

Is it Happening Again?

F: Begin Grammar

Don't forget Check-in
Thursday-Sunday night



Preparing the Rickroll Stream

- Took a while to figure out correct transport stream format (MPEG-TS) and use ffmpeg
- Streamed from AvediaServer
 - Included 1 hour countdown + rickroll + message text
 - **Comic Sans** :)

Please standby for an important announcement

00:13:37



Preparing the Rickroll Stream



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

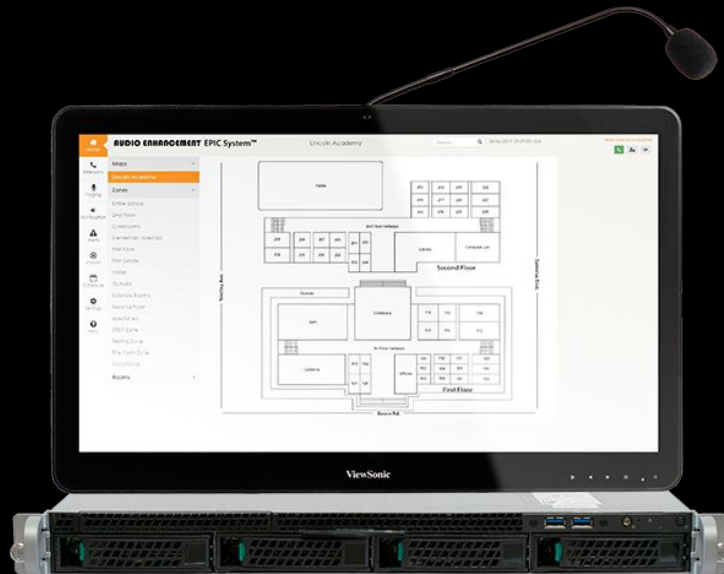
Good luck on AP and final exams!
Congrats to the Class of 2021!

#D214RickRoll

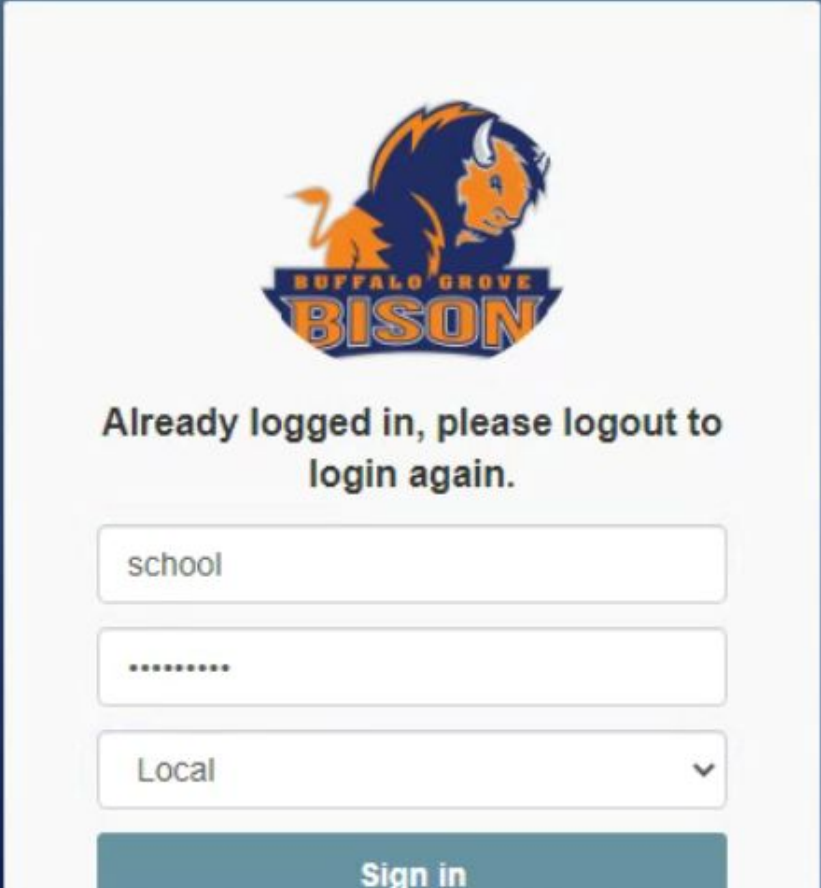
The TV will reset momentarily. Please be patient.


EPIC System (Bells)

- Education Paging and Intercom Communications
- Networked speakers in halls and classrooms
- Controlled by EPIC server



Hacking Bell System in 3 Days





Already logged in, please logout to login again.

school

Local

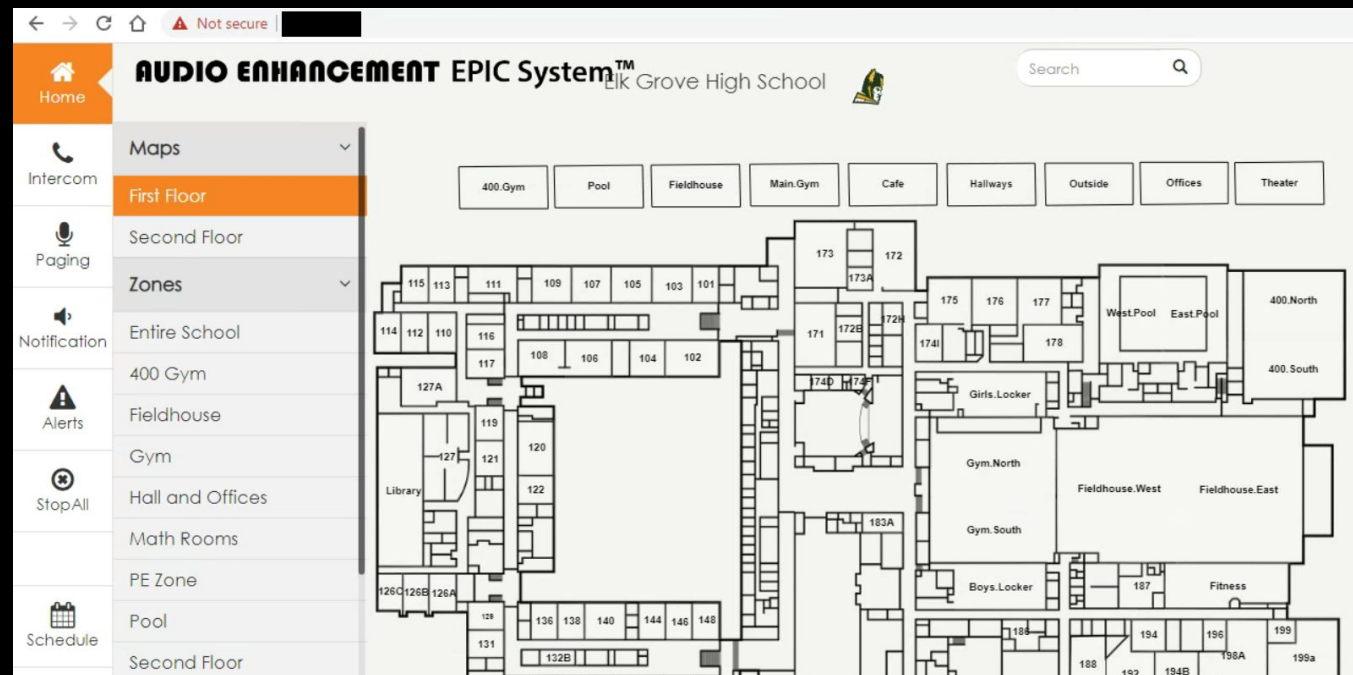
Sign in

- We found a bunch of other IoT devices after a scan
 - They were ceiling speakers in the halls and classrooms used for announcements and bells
 - Each speaker was linked to an EPIC server



Hacking Bell System in 3 Days

- A single EPIC server had default admin credentials, allowing us to modify the bell tones/schedule for that school
- The other EPIC servers/schools did not have default credentials



Hacking Bell System in 3 Days

- The backup system used a file server with the default creds
- What if the other EPIC backup servers also use default creds?

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

Frequency *

Backup Location *
Example: //127.0.0.1/Backup

User Name*

Password*

Hacking Bell System in 3 Days

- Information that was backed up to file servers included an SQL dump file containing password hashes!
- Found admin account across all servers and cracked the password

| Name | Date modified | Type | Size |
|---------------------|-------------------|-----------------|----------|
| config | 4/29/2021 3:17 PM | File folder | |
| public | 4/29/2021 3:17 PM | File folder | |
| config.txt | 4/29/2021 3:17 PM | Text Document | 10 KB |
| config_template.txt | 4/29/2021 3:17 PM | Text Document | 10 KB |
| device-sip.txt | 4/29/2021 3:17 PM | Text Document | 27 KB |
| epicsystemdump.sql | 4/29/2021 3:17 PM | SQL Source File | 2,269 KB |
| extconfig.txt | 4/29/2021 3:17 PM | Text Document | 1 KB |
| extensions.txt | 4/29/2021 3:17 PM | Text Document | 2 KB |
| http.txt | 4/29/2021 3:17 PM | Text Document | 1 KB |



Hacking Bell System in 3 Days

- That's how we went from one system with default credentials to compromising all the EPIC servers

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 |

Preparing Bell System Rickroll

Show entries

| Name | Type |
|--|------|
| All Clear | bell |
| Bell chime | bell |
| Bell ding | bell |
| Bell mechanical | bell |
| Bell tone | bell |
| commissioningPing | sip |
| D214_Lockdown_with_Alert_tone_Repeated | bell |
| Fire urgent | bell |
| Gym_Bell | bell |
| Lightning | bell |
| Lockdown | bell |

- Uploaded custom audio .wav file of "Never Gonna Give You Up" to bell tone list
 - Named similarly to legitimate bell tones
 - "Musical scale" - actual bell
 - "Musical scale" - rickroll bell



Preparing Bell System Rickroll










- Created new bell schedules containing the rickroll tones
- Named discreetly with a very similar color to the real schedule

Rickroll bell schedule



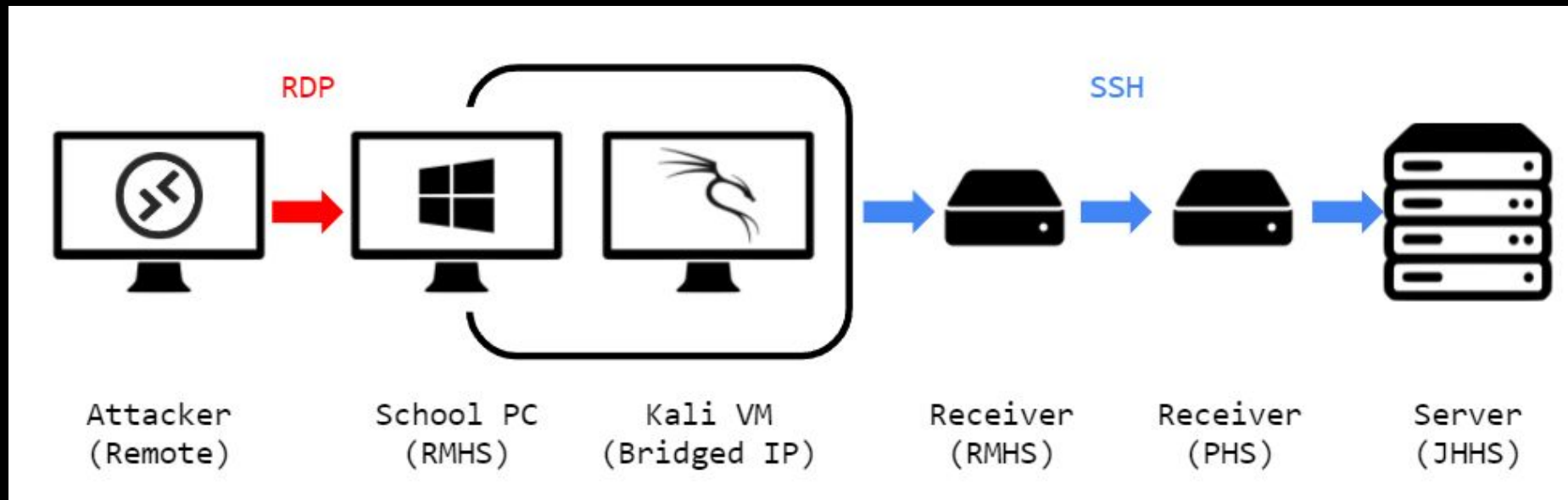
Real bell schedule



| | | |
|------------------------------|---|---|
| No Student Day |  | |
| Block Days |  |  |
| Block Days W Better Music |  |  |
| Block Days w Exclusions |  |  |
| Block Days W Music |  |  |

Operational Security

- Pivoting through receivers
- Limited traffic bandwidth and number of requests
- Encrypted communications (Signal + Element Matrix client)
- Cleaning metadata from prepared materials
- Wiping school PCs when finished



Report Writing

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 |

- We documented everything in a 26-page penetration test report
- Email with the report was automatically sent to the technical supervisors after the prank was finished



Hot Water

- Right after the bell system hack, the dean called my brother down to his office
 - At this point, the report was just sent and they did not see it yet
 - Asked why he was recording the video in the first place
 - The dean knew that I was into cybersecurity and asked my brother if I was involved or knew anything about it
 - When my brother told me about this, that's how I knew the administration was already suspicious of me



Aftermath

- A few days after the report was sent, we received an email
- District administration was so impressed by the report, they decided not to pursue discipline
- Instead, they thanked us and wanted us to debrief the hack

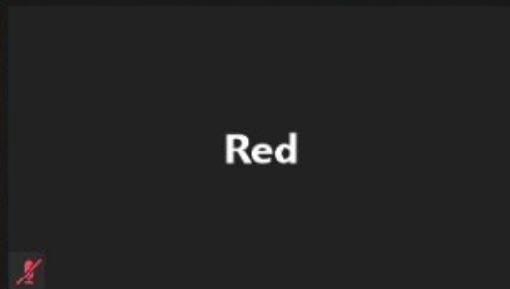
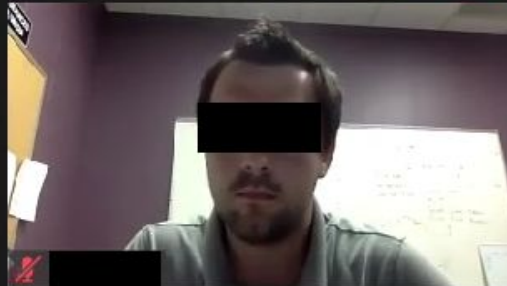
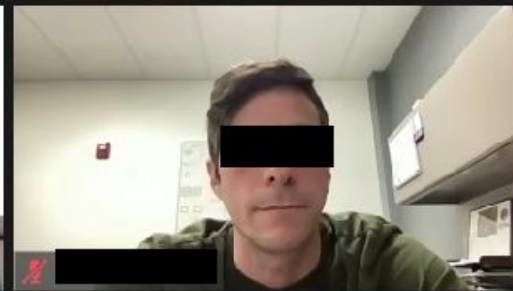




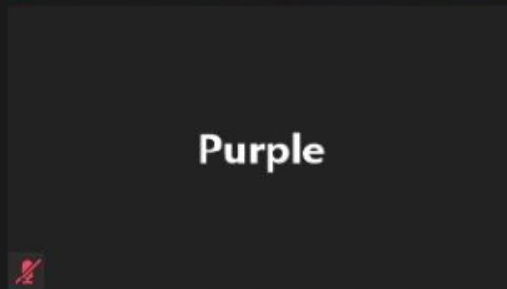
View



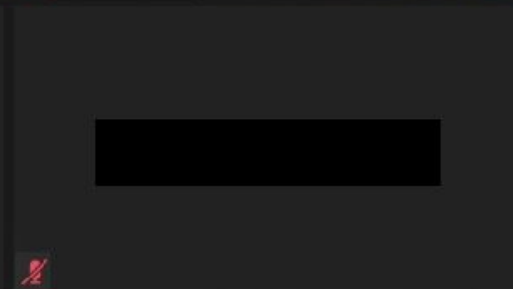
Minh Duong



Red



Purple



Unmute

Start Video

Participants 12

Chat

Share Screen

Record

Reactions

Leave

An Edge Case in Modern Times

- I was very lucky
- I didn't get a slap on the wrist... not even told off!
- Doing something like this without getting in trouble is almost impossible today
 - e.g. Governor of Missouri on the inspect element "hack"
- The Computer Fraud and Abuse Act (CFAA)
 - Unauthorized computer entry: 1-5 years of prison
 - Trafficking in passwords: 1-2 years of prison



The Ethics Dilemma

- Was the prank "right" or "ethical"?
- Was the district right to not press charges against us?
- Was publishing my blog post a good idea?
- Why step forward and reveal my own identity during the debrief?
 - Risking my peers' identities and their futures



Blog Post

- Published just a few weeks ago
- Goes over a lot of what I said plus extra



WhiteHoodHacker

[/home](#)

[/posts](#)

[/contact](#)



[← .. /](#)

IoT Hacking and Rickrolling My High School District

October 04, 2021 · 8 min read



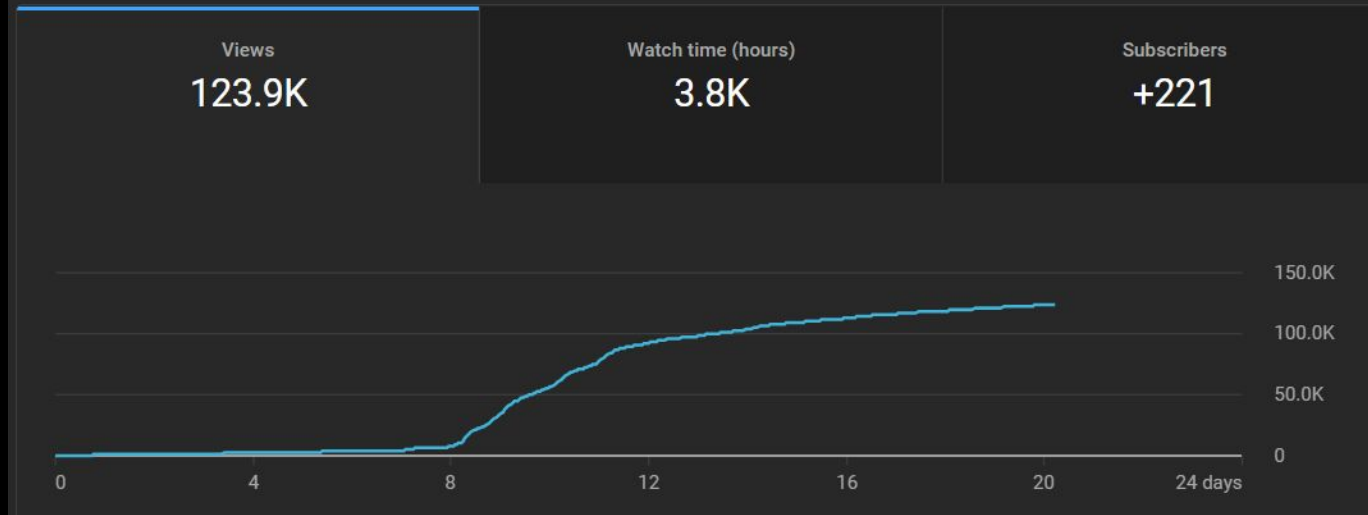
Feedback

  **r/nextfuckinglevel** · Posted by u/Merz_Nation 12 days ago

115k  2  3  147  153  144  134  2  6 

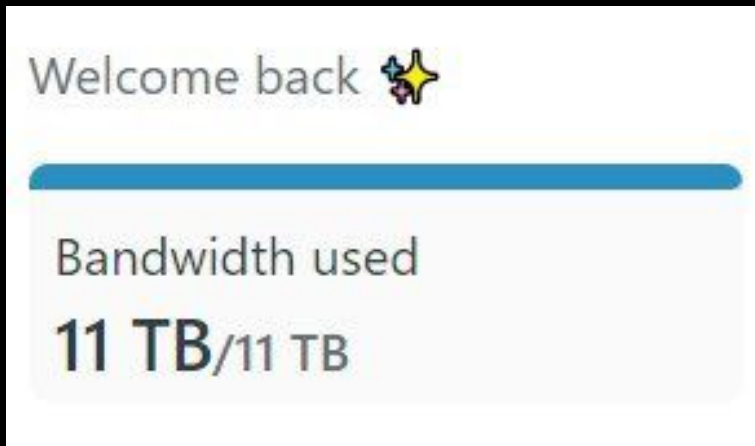
 **High schooler rickrolled entire school by hacking into IoT system**

This video has gotten **123,881 views** since it was published



Website Attacked

- Someone tried to DDoS my site
 - My site didn't go down, but all the requests made counted towards bandwidth limits for my web hosting
 - \$2,240 bandwidth charge! (reverted by support)



| | |
|--------------------------|---|
| Starter team plan | |
| Effective from Jun 13 | |
| 11 TB / 100 GB bandwidth | |
| 3 / 300 build minutes | |
| \$0.00 | |
| Bandwidth | ▼ |
| \$2,240.00 | |



Thank you!

Any questions?



Next Meetings

Next Thursday: Forensics

- How to find hidden information
- How to retrieve and analyze data from systems

Sunday Seminar: Halloween Spooky Get-Together

- Quick get together at 2PM @ the CIF (30 minutes)
- Invite your families if you want to (I am going to run a quick funny meeting on what SIGPwny is that way they know what you are talking about).
- Costumes optional, but encouraged.



RICK ASTLEY

NEVER GONNA
GIVE YOU UP

