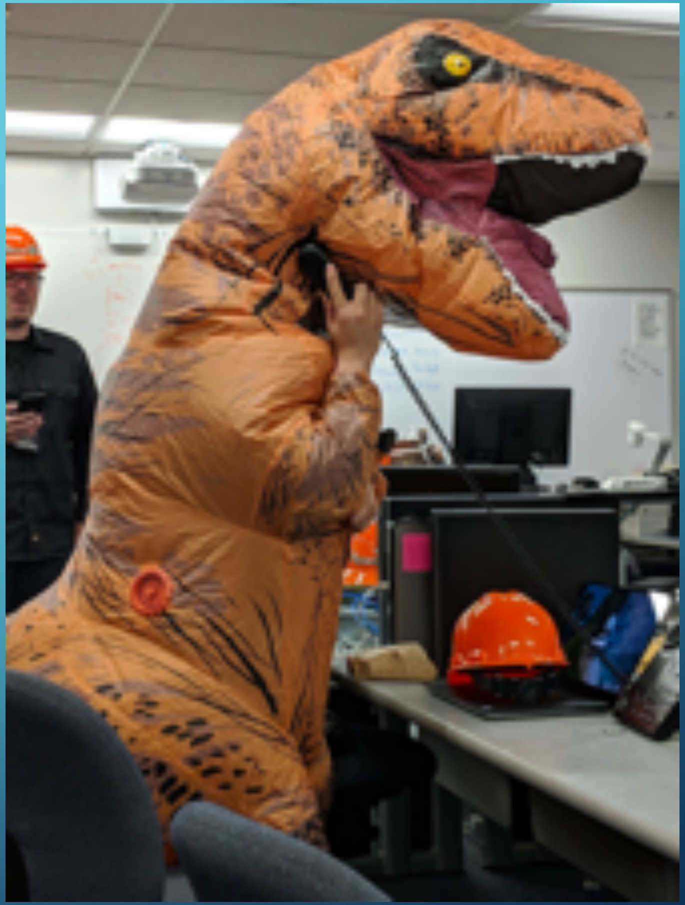
WRCCDC BLACK TEAM DEBRIEF

CONGRATULATIONS, WE WON!

WE ARE BLACK TEAM

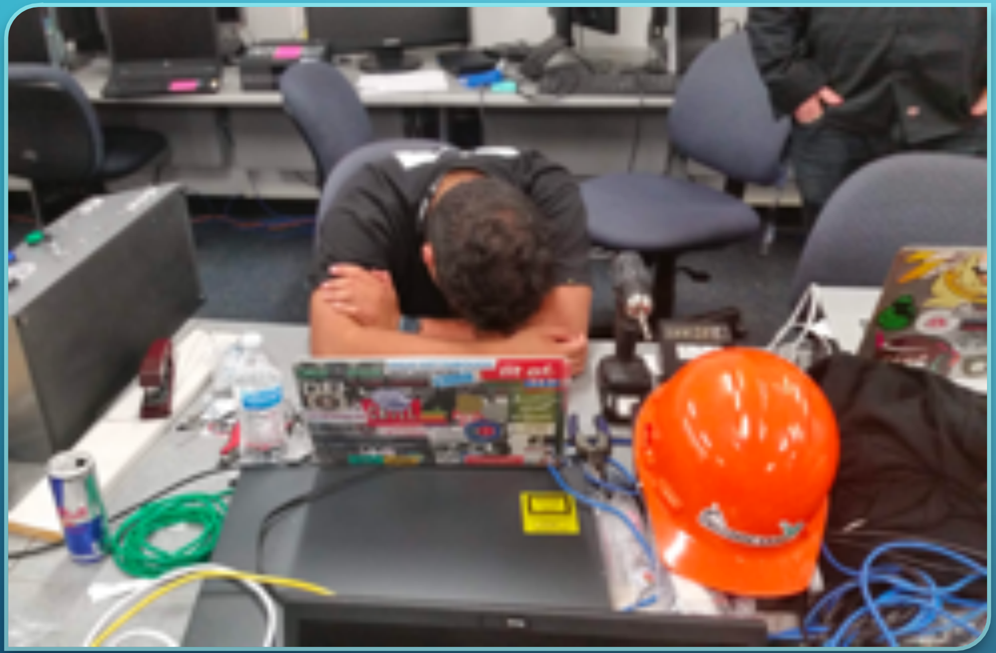
- Systems optimized for your convivence
- All systems worked
- Host naming was Xena Warrior Princess
- Daddy ‘Tops



THE TEAM

- Like to thank my core black teamers who helped every day to make sure this event happened
- Many new black teamers (6 in total!) and always happy to have more
- We are not your enemy. We are here to help you.
- Huge effort this year to integrate, test, and verify everything by all team members.
- We get paid in chuckles (still)!

MANY HOURS



- 7AM to 3AM
- Multiple days of all nighters

LESSONS LEARNED

NEGATIVES

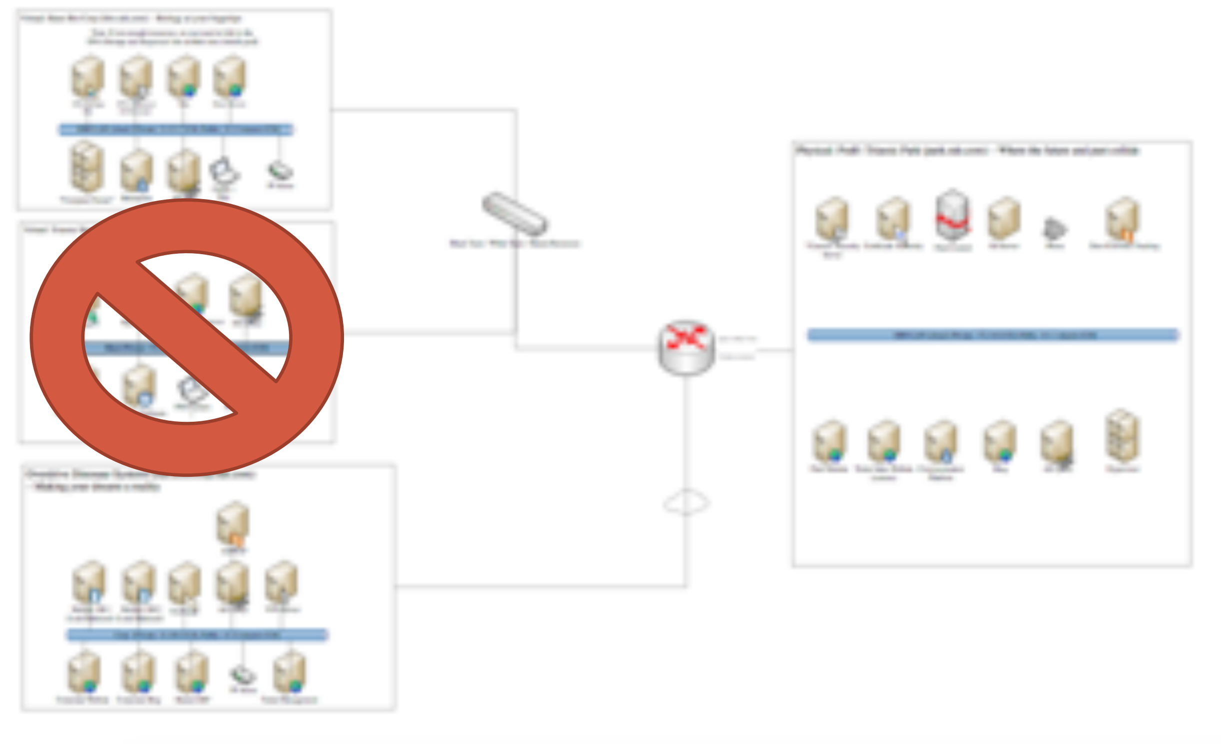
- Teams struggled with routers
- Windows Updates, *nix Updates not cached and were most of our bandwidth
- Could not serenade teams with wonderful music and memes
- Did not provide teams with access to snapshots (Oops)

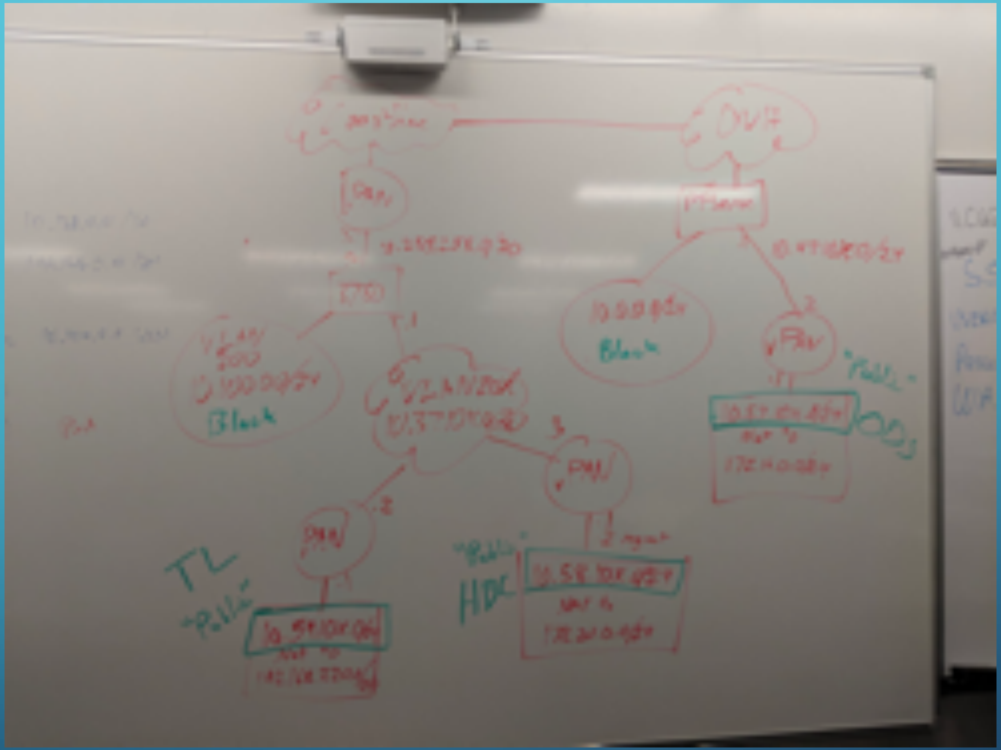
POSITIVES

- First year we have had multiple boxes with 12GB of RAM+ used/required
- Aged network to perfection for ~6 months
- Ticket system allows for teams to validate and audit issues
- Very good performance and connectivity

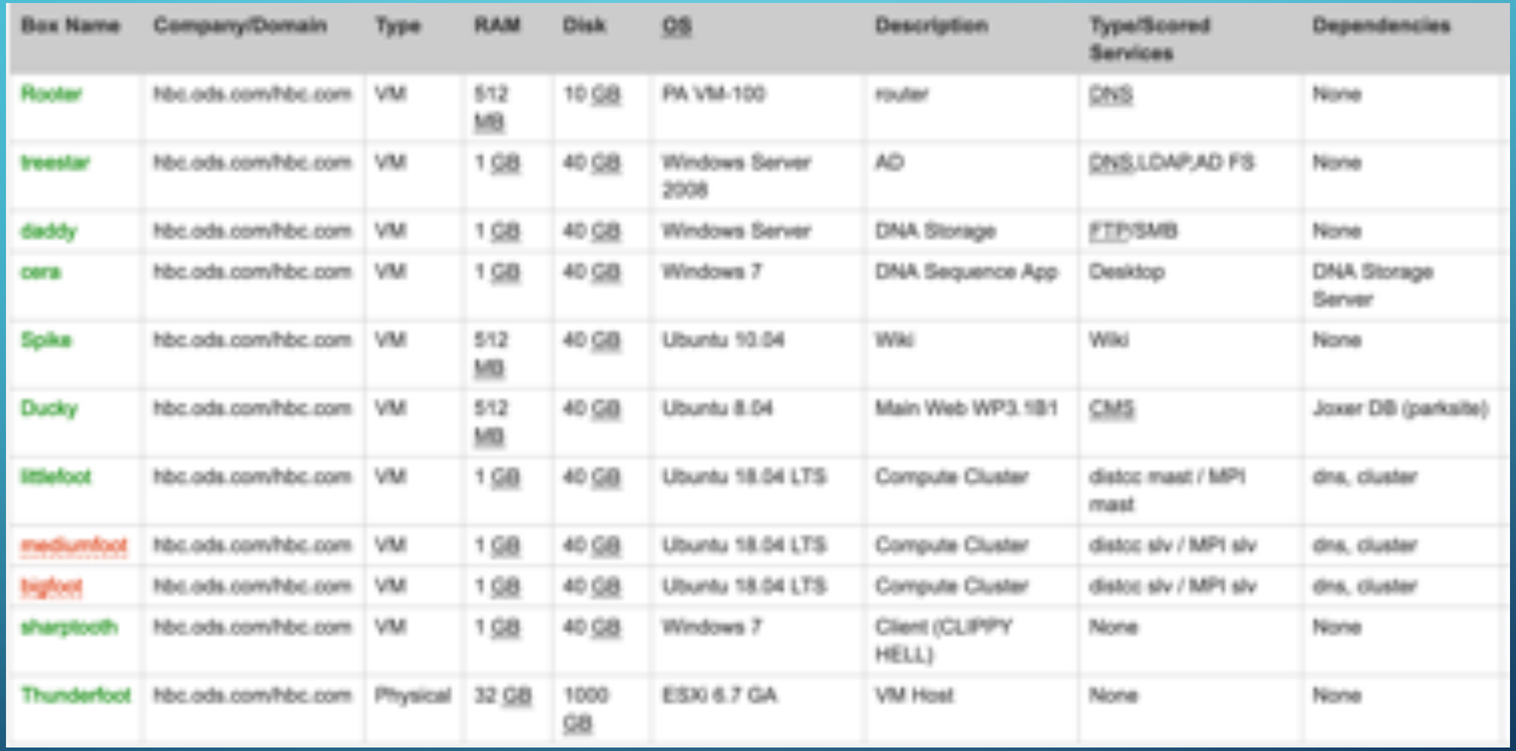
NETWORK REVIEW

NETWORK REVIEW



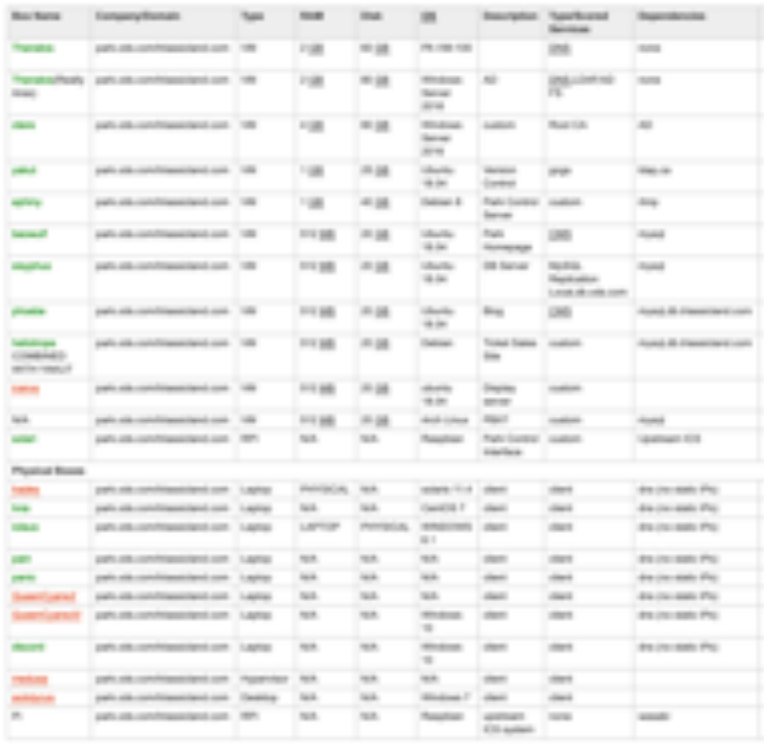

PAN
VLAN
500
Black
Black
PAN
PAN
PAN
"Public"
TL
"Public"
HDC
"Public"
ODS

HOSTS



Box Name	Company/Domain	Type	RAM	Disk	OS	Description	Type/Scored Services	Dependencies
Rooter	hbc.ods.com/hbc.com	VM	512 MB	10 GB	PA VM-100	router	DNS	None
treestar	hbc.ods.com/hbc.com	VM	1 GB	40 GB	Windows Server 2008	AD	DNS,LDAP,AD FS	None
daddy	hbc.ods.com/hbc.com	VM	1 GB	40 GB	Windows Server	DNA Storage	FTP/SMB	None
cera	hbc.ods.com/hbc.com	VM	1 GB	40 GB	Windows 7	DNA Sequence App	Desktop	DNA Storage Server
Spike	hbc.ods.com/hbc.com	VM	512 MB	40 GB	Ubuntu 10.04	Wiki	Wiki	None
Ducky	hbc.ods.com/hbc.com	VM	512 MB	40 GB	Ubuntu 8.04	Main Web WP3.1®1	CMS	Joxer DB (parksite)
littlefoot	hbc.ods.com/hbc.com	VM	1 GB	40 GB	Ubuntu 18.04 LTS	Compute Cluster	distcc mast / MPI mast	dns, cluster
mediumfoot	hbc.ods.com/hbc.com	VM	1 GB	40 GB	Ubuntu 18.04 LTS	Compute Cluster	distcc slv / MPI slv	dns, cluster
bigfoot	hbc.ods.com/hbc.com	VM	1 GB	40 GB	Ubuntu 18.04 LTS	Compute Cluster	distcc slv / MPI slv	dns, cluster
sharptooth	hbc.ods.com/hbc.com	VM	1 GB	40 GB	Windows 7	Client (CLIPPY HELL)	None	None
Thunderfoot	hbc.ods.com/hbc.com	Physical	32 GB	1000 GB	ESXi 6.7 GA	VM Host	None	None

AND THEN TRIASSIC LAND

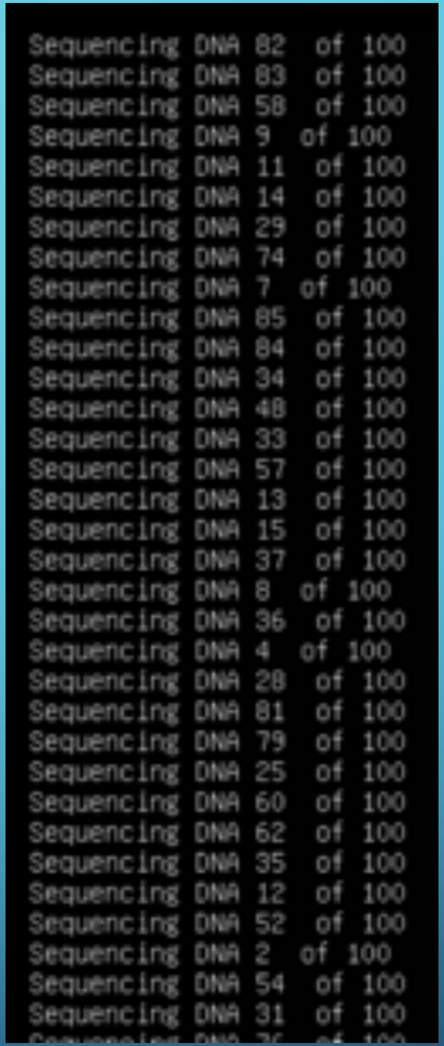


TOPOLOGY

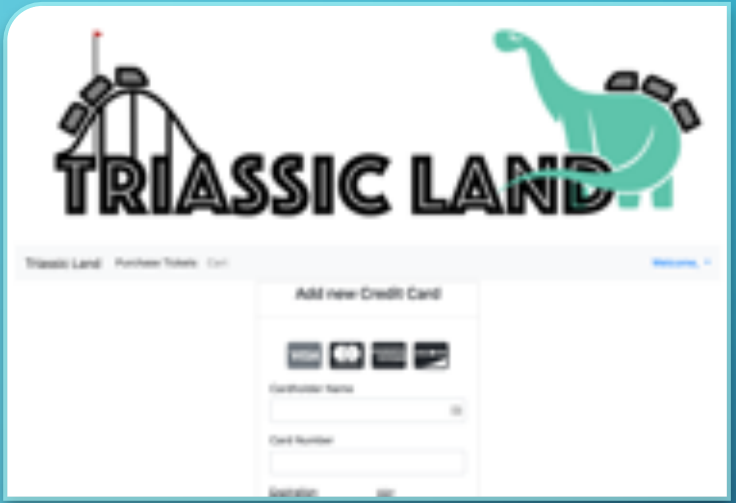
- 3x3 Site to Site VPNs on the first day (full mesh)
- HBC Moved as part of a “Data Center Migration” in competition
- Network doing an average of each team doing about 12mbps for the entirety of competition
- Conditional Trusts on all domain controllers, separate users
- Skype for Business and Outlook/Exchange functional and used

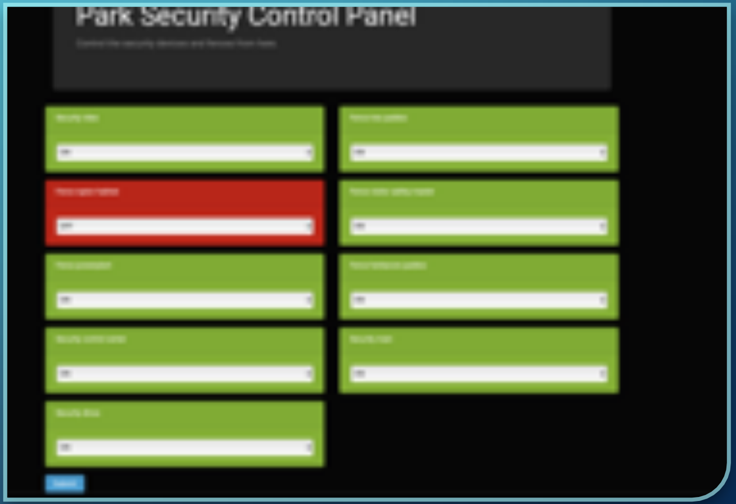
CUSTOM SERVICES

- Had a forensics challenge in the competition for the first time
- 4 custom written applications
  - Unified Systems Windows Apps
  - Park Fence Controller
  - Park Home Page
  - Park Sales Site

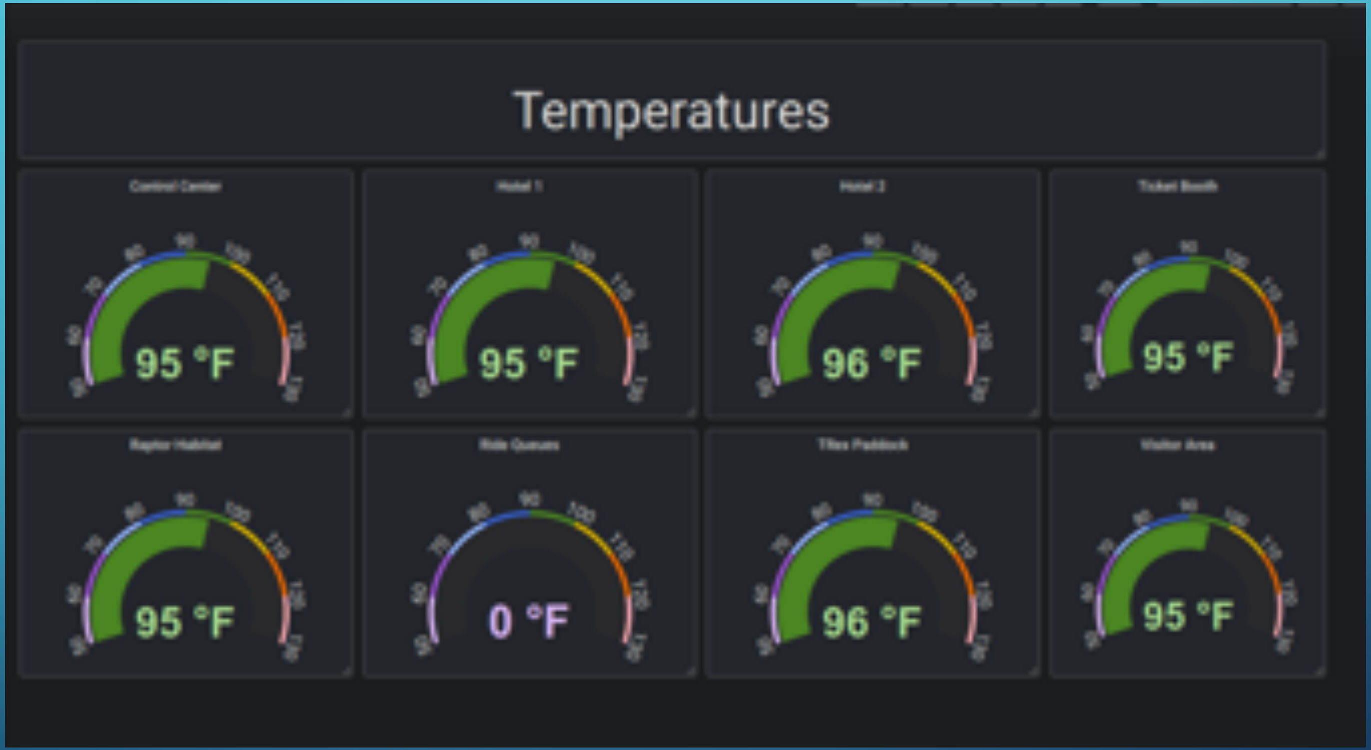


```
Sequencing DNA 82  of 100
Sequencing DNA 83  of 100
Sequencing DNA 58  of 100
Sequencing DNA 9  of 100
Sequencing DNA 11  of 100
Sequencing DNA 14  of 100
Sequencing DNA 29  of 100
Sequencing DNA 74  of 100
Sequencing DNA 7  of 100
Sequencing DNA 85  of 100
Sequencing DNA 84  of 100
Sequencing DNA 34  of 100
Sequencing DNA 48  of 100
Sequencing DNA 33  of 100
Sequencing DNA 57  of 100
Sequencing DNA 13  of 100
Sequencing DNA 15  of 100
Sequencing DNA 37  of 100
Sequencing DNA 8  of 100
Sequencing DNA 36  of 100
Sequencing DNA 4  of 100
Sequencing DNA 28  of 100
Sequencing DNA 81  of 100
Sequencing DNA 79  of 100
Sequencing DNA 25  of 100
Sequencing DNA 60  of 100
Sequencing DNA 62  of 100
Sequencing DNA 35  of 100
Sequencing DNA 12  of 100
Sequencing DNA 52  of 100
Sequencing DNA 2  of 100
Sequencing DNA 54  of 100
Sequencing DNA 31  of 100
```

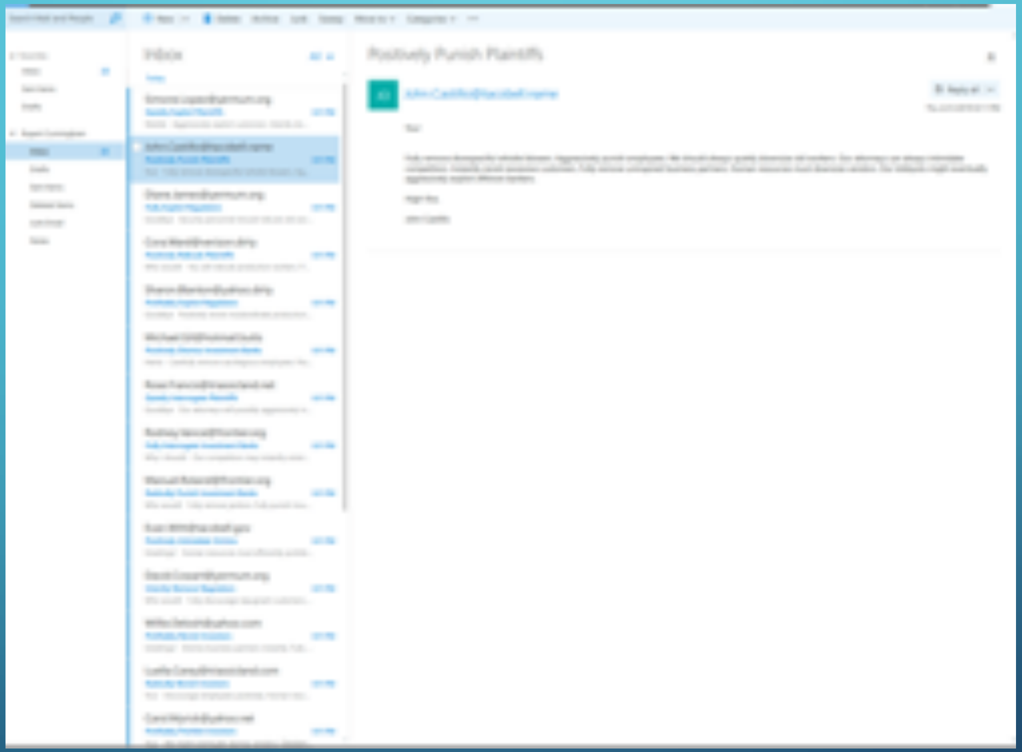




MONITORING


Temperatures
Control Center
95 °F
Hotel 1
95 °F
Hotel 2
96 °F
Ticket Booth
95 °F
Raptor Habitat
95 °F
Ride Queues
0 °F
TRex Paddock
96 °F
Visitor Area
95 °F

SPAM 4U



Inbox

Positively Punish Plaintiffs

DETERMINE WHAT IS IMPORTANT

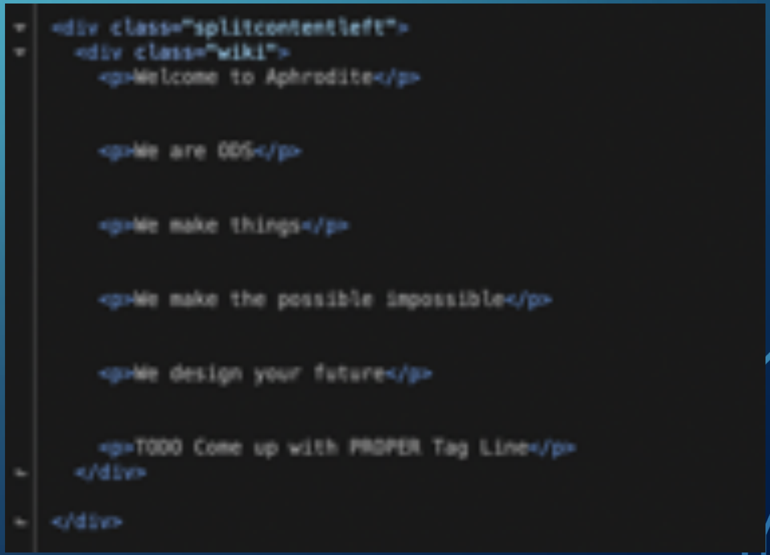
- Certificate Authority
- Git Repos (With our custom software)
- Domain Controller (maybe?)
- Exchange

STRATEGY?

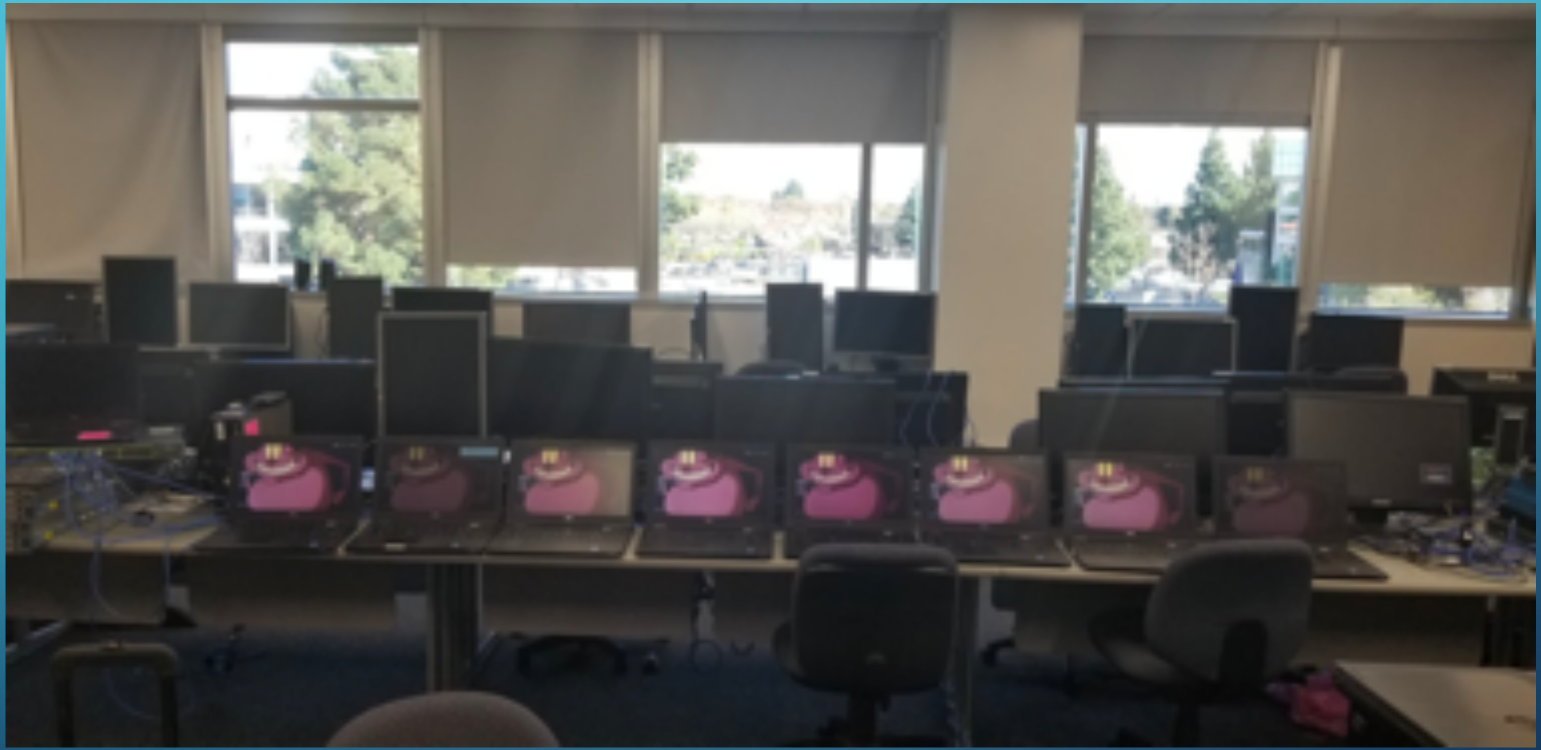
- Only 4 teams asked for scrubs
- We forgot flash drives… We didn't know till 2:30 PM on Saturday
- If black team suggests a consult… You probably should take us up on the offer.
- Data Center migration was there to help **you**

OPTIMAL HARDWARE

- Coco / The Router Guy
- Very very sketchy cameras
- Very good hypervisors



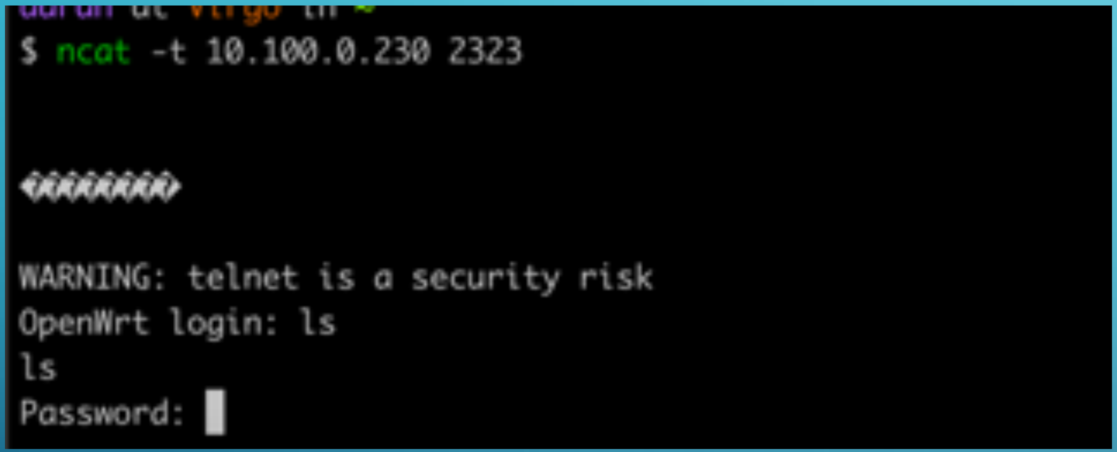
```
<div class="splitcontentleft">
  <div class="wiki">
    <p>Welcome to Aphrodite</p>


    <p>We are ODS</p>


    <p>We make things</p>


    <p>We make the possible impossible</p>


    <p>We design your future</p>


    <p>TODO Come up with PROPER Tag Line</p>
  </div>

</div>
```



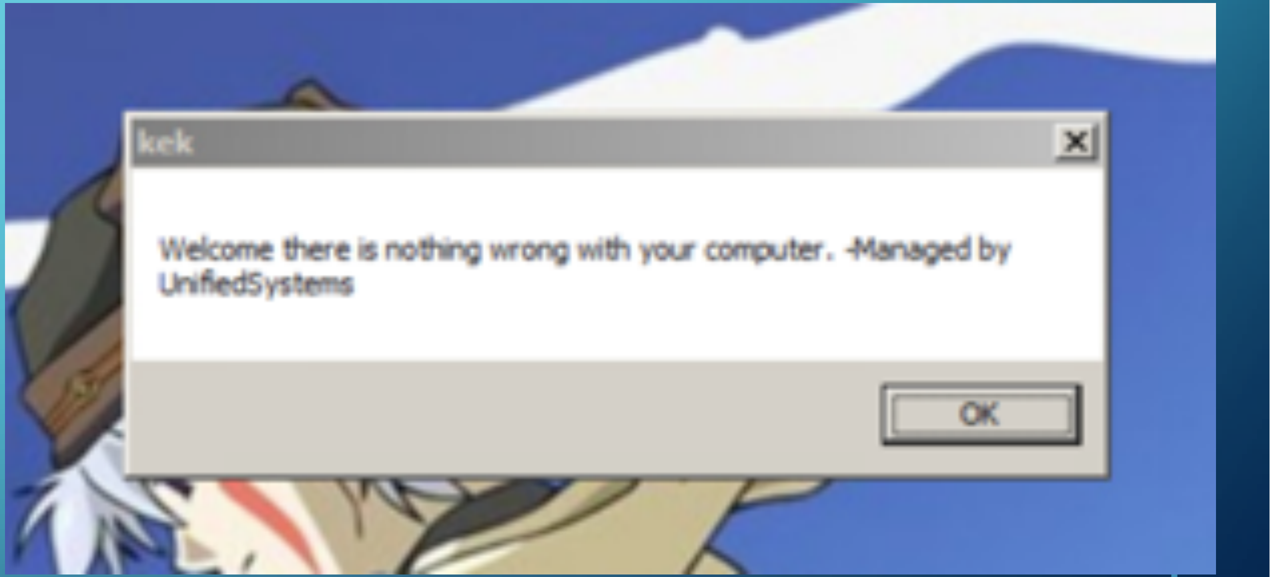
ACCESS

- Teams asked us to debug issues without access. Thankfully Red Team provided us with access to the teams
- Cameras were being monitored, some teams got creative about privacy

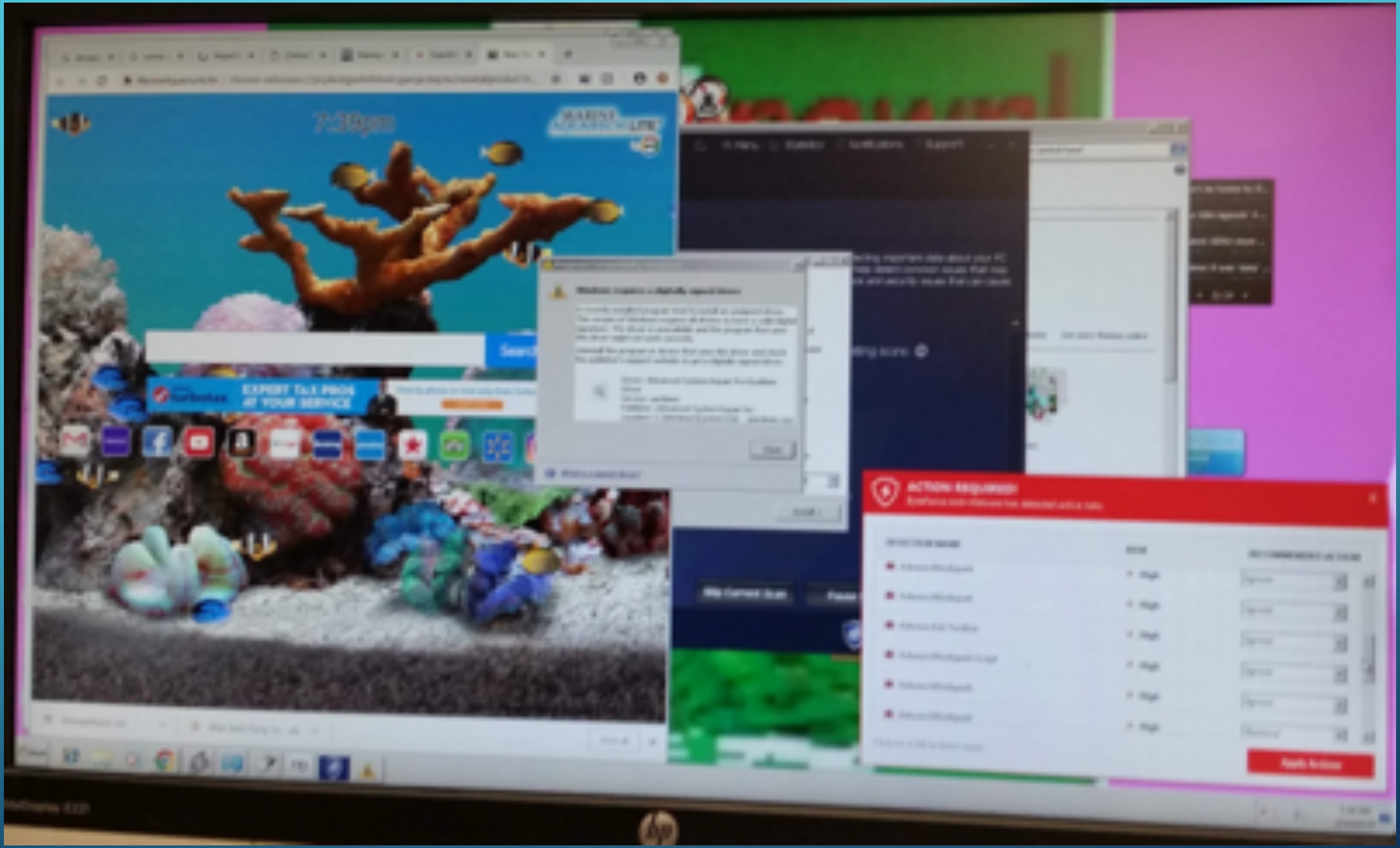
OPTIMAL SYSTEMS



```
aaron at virgo in ~
$ ncat -t 10.100.0.230 2323


�������

WARNING: telnet is a security risk
OpenWrt login: ls
ls
Password: █
```



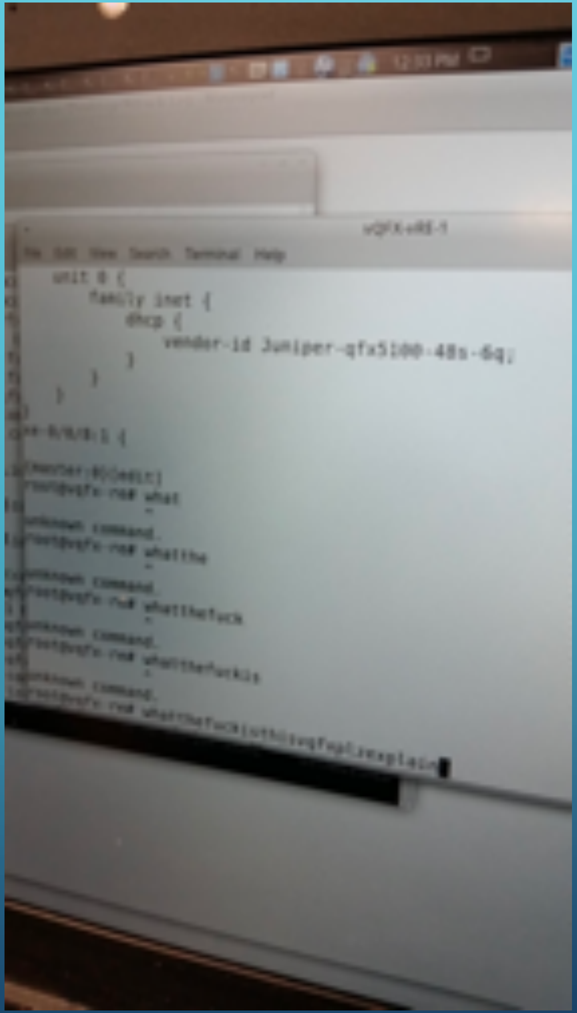
Welcome there is nothing wrong with your computer. -Managed by UnifiedSystems


7:39pm
MARINE AQUARIUM LITE
EXPERT TAX PROS AT YOUR SERVICE
ACTION REQUIRED!
High
High
High
High
High
High
Apply Actions

BLUE TEAM BLUES

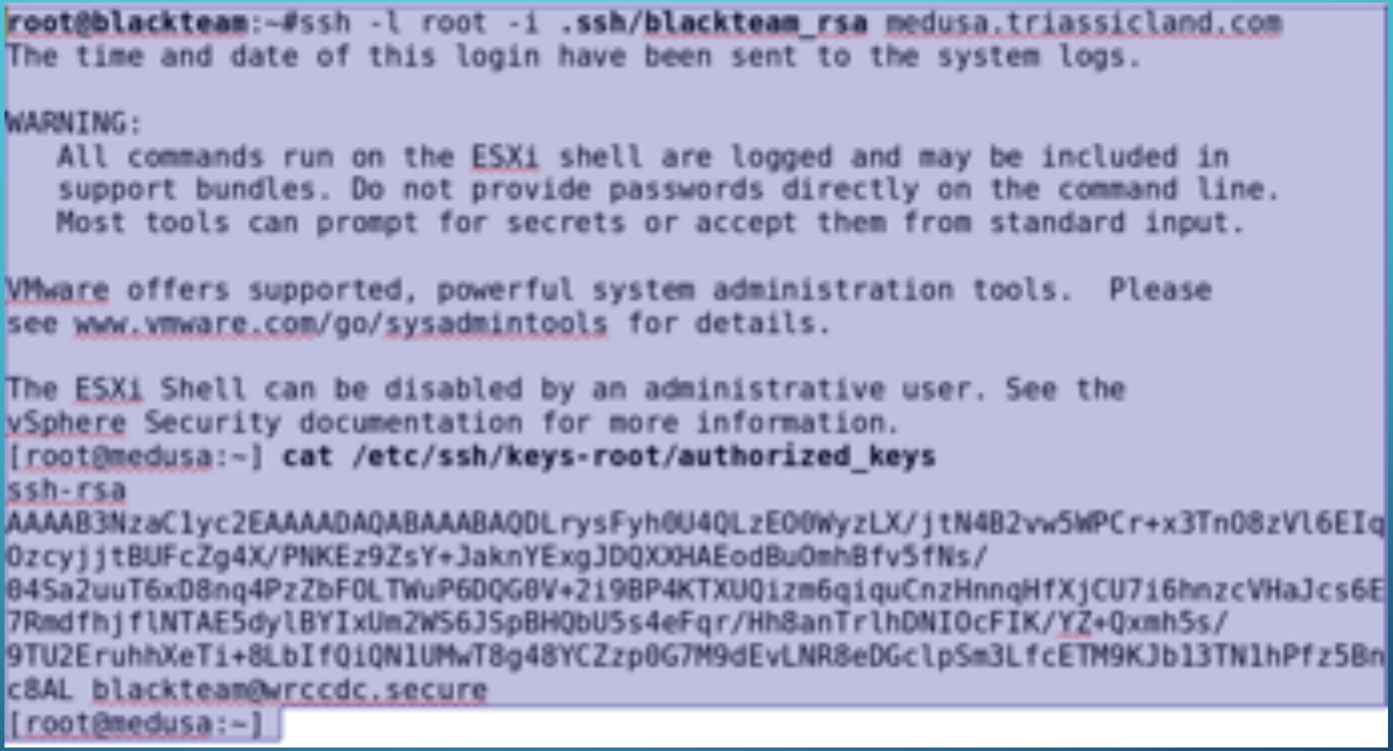
- Teams struggled with default credentials well into the second day
- Teams struggled with routers
- Teams not willing to scrub/get consult (hint: usually less of a point loss)
- Teams struggling with troubleshooting connectivity issues
- Guest WIFI?
- Playing Halo while in competition

PAN TO PI AND CISCO TO JUNIPER



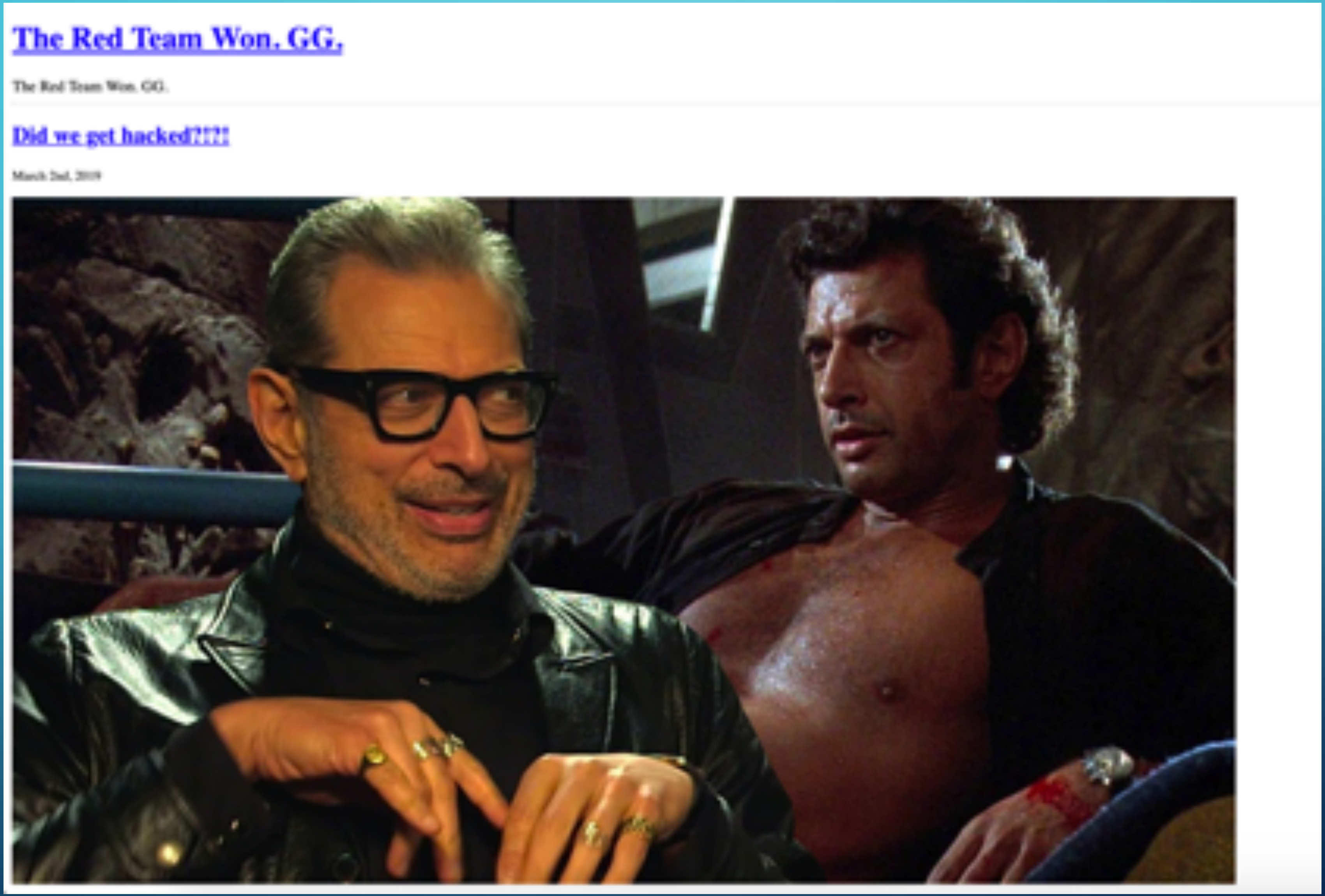
```
    unit 0 {
        family inet {
            dhcp {
                vendor-id Juniper-qfx5100-48s-6q;
            }
        }
    }
}
xe-0/0/0:1 {

{master:0}[edit]
root@vqfx-re# what
              ^
unknown command.
root@vqfx-re# whatthe
              ^
unknown command.
root@vqfx-re# whatthefuck
              ^
unknown command.
root@vqfx-re# whatthefuckis
              ^
unknown command.
root@vqfx-re# whatthefuckisthisvqfxplzexplain
```

DEFAULT SSH KEY



```
root@blackteam:~#ssh -l root -i .ssh/blackteam_rsa medusa.triassicland.com
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@medusa:~] cat /etc/ssh/keys-root/authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDLrysFyh0U4QLzEO0WyzLX/jtN4B2vw5WPCr+x3Tn08zVl6EIq
OzcyjjtBUFcZg4X/PNKEz9ZsY+JaknYExgJDQXXHAEodBuOmhBfv5fNs/
045a2uuT6xD8nq4PzZbFOLTWuP6DQG8V+2i9BP4KTXUQizm6qiquCnzHnnqHfXjCU7i6hnzcVHaJcs6E
7RmdfhjflNTAE5dylBYIxUm2WS6JSpBHQbU5s4eFqr/Hh8anTrlhDNIOcFIK/YZ+Qxmh5s/
9TU2EruhhXeTi+8LbIfQiQN1UMwT8g48YCZzp0G7M9dEvLNR8eDGclpSm3LfcETM9KJb13TN1hPfz5Bn
c8AL blackteam@wrccdc.secure
[root@medusa:~]
```

If we can still get in, red team can still get in



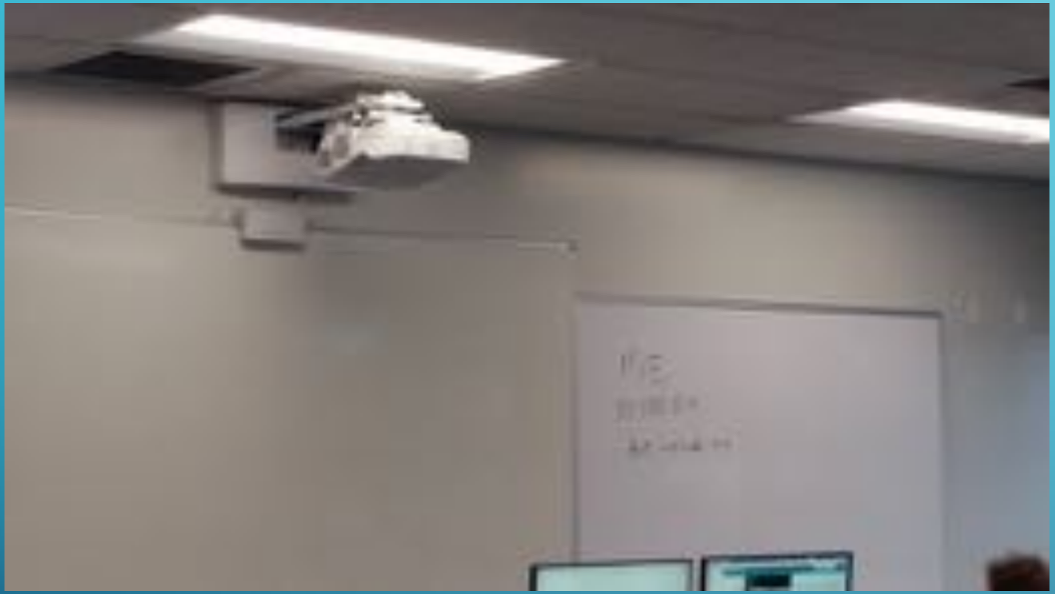
The Red Team Won. GG.

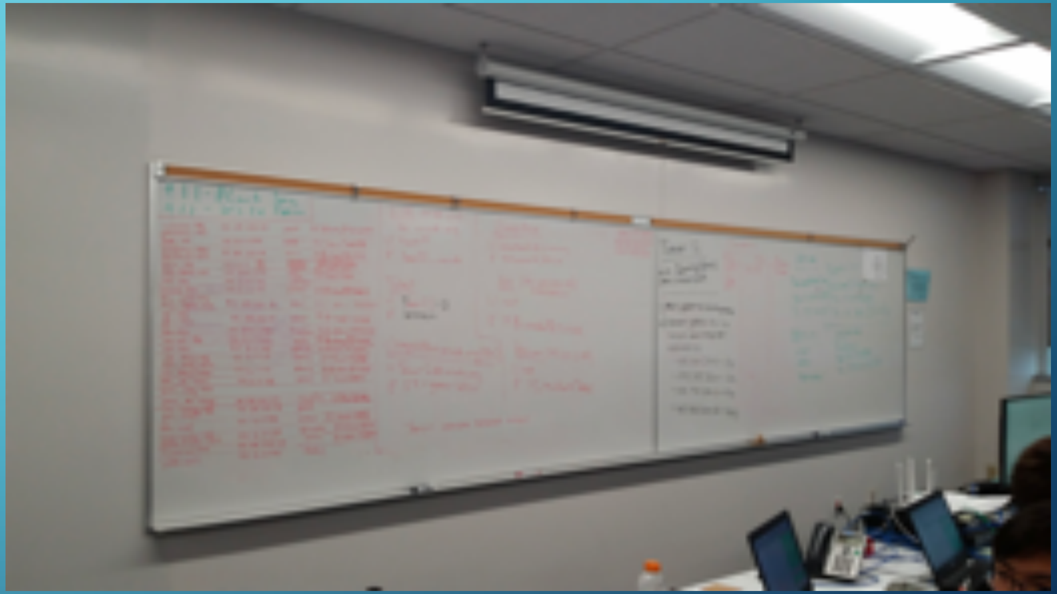
The Red Team Won. GG.

Did we get hacked?!?!!

March 2nd, 2019

DOCUMENTATION IS KEY



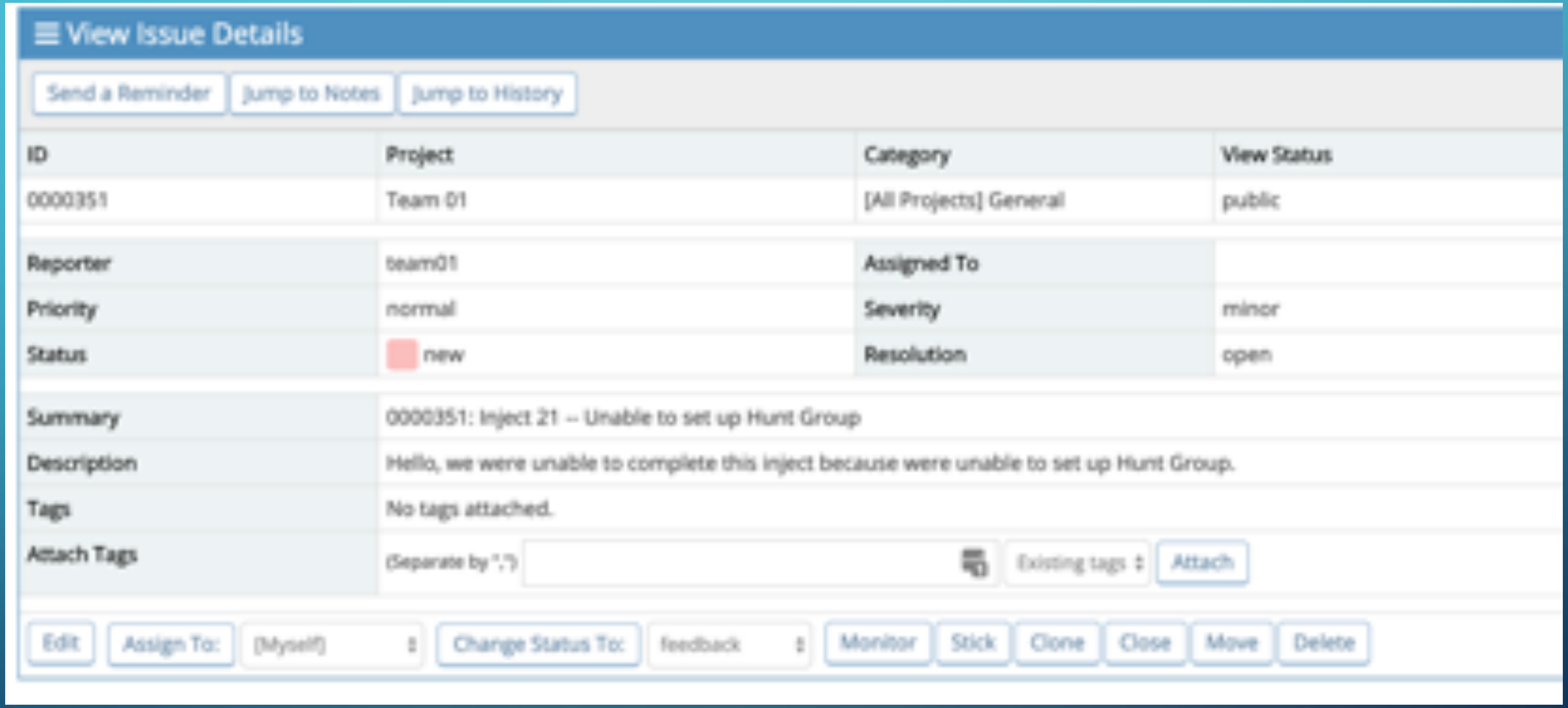


TAQUERIA DE MEXICO

THOUGHTS FROM BLACK TEAM

- Tickets are your friend – two teams submitted issues were tracked and resulted in point changes to their benefit
- Ask for help quicker!

WE ARE CONSULTANTS..



ID	Project	Category	View Status
0000351	Team 01	[All Projects] General	public

Reporter	team01	Assigned To	
Priority	normal	Severity	minor
Status	🟥 new	Resolution	open

Summary	0000351: Inject 21 -- Unable to set up Hunt Group
Description	Hello, we were unable to complete this inject because were unable to set up Hunt Group.
Tags	No tags attached.
Attach Tags	(Separate by ",")

AND HERE WE ARE