CyberForce2020: Leading an Army of 380+ APT Hackers against Innocent Windmills

U.S. DEPARTMENT OF ENERGY'S CYBERFORCE™ COMPETITION

DEFENDING U.S. ENERGY INFRASTRUCTURE

Kandy Phan

U.S. DEPARTMENT OF ENERGY NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

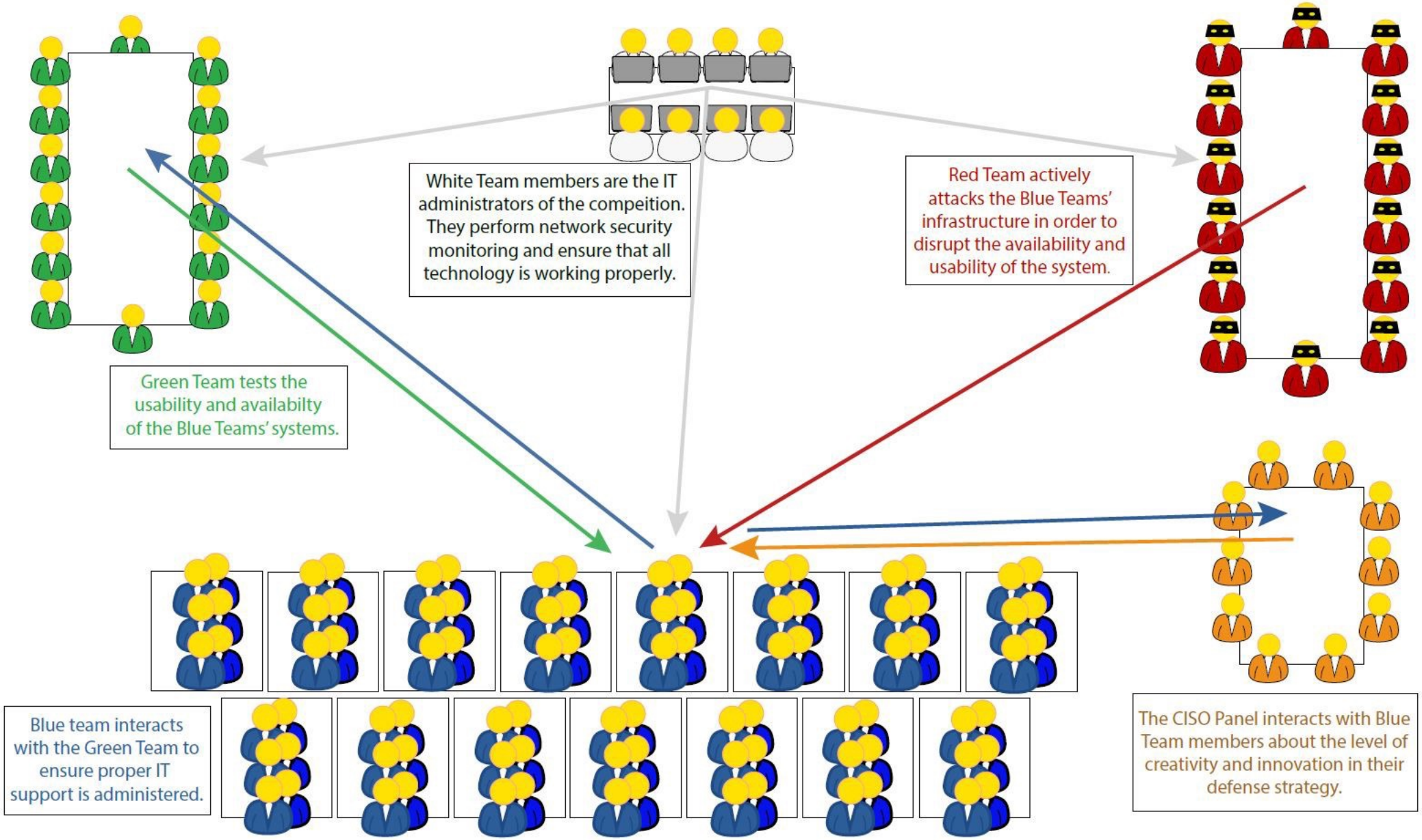
SAND No: SAND2021-7239C

whoami

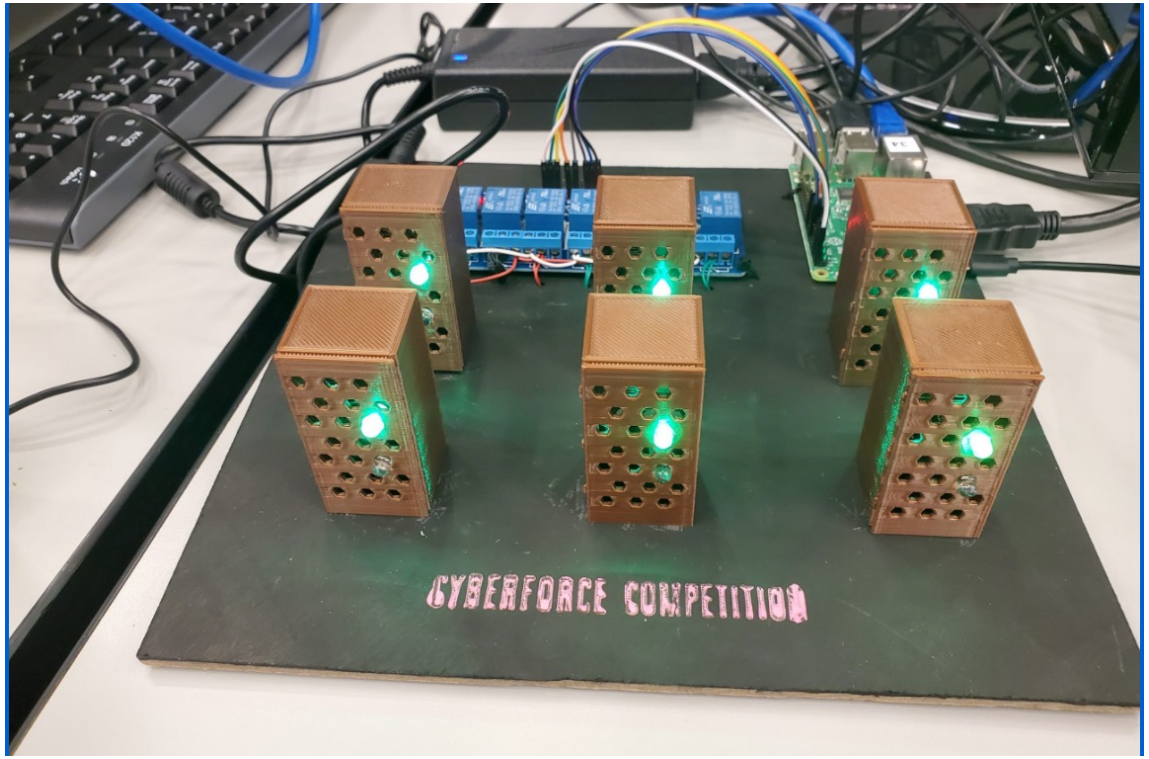
- Cybersecurity researcher, Red team lead
- Focus in ICS, enterprise, malware, red team TTPs, virtualization
- OSCP, OSCE, GXPN
- 15+ in infosec industry
- National Red team leader for CFC 2020

What is the DOE CyberForce Competition?

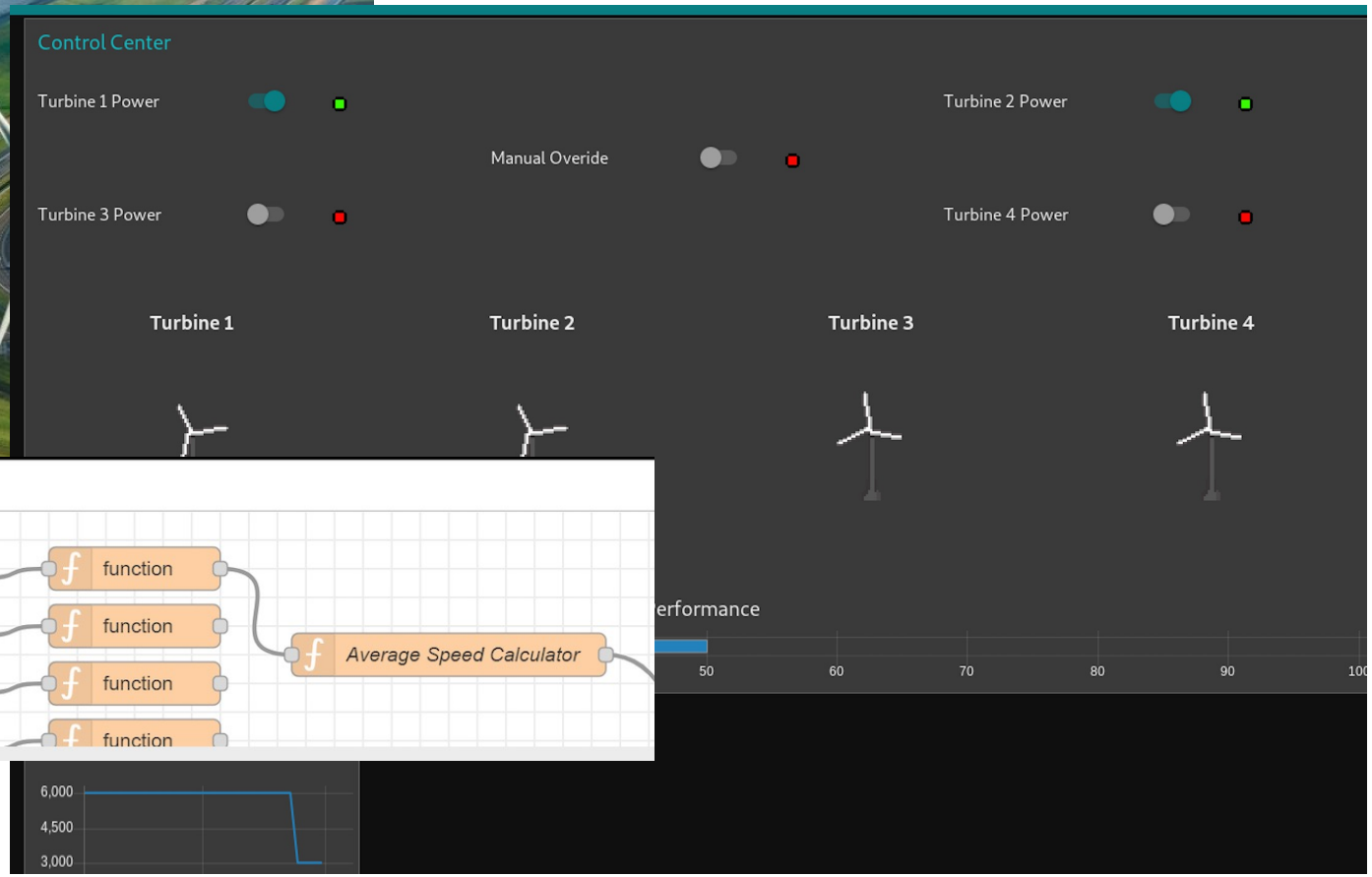
- Cyber Defense competition with ICS component, constant evolution
- Ran by all of the DOE national labs with Argonne being the lead lab
- Building the future cybersecurity workforce

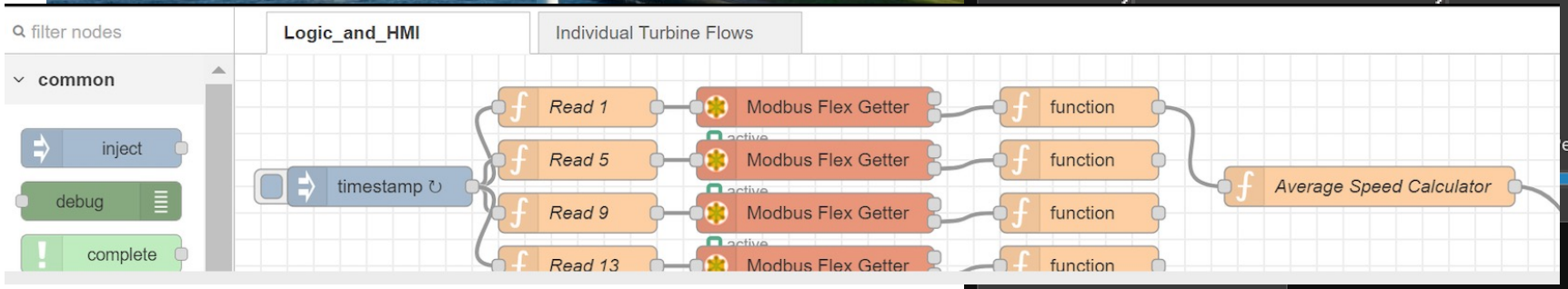

White Team members are the IT administrators of the compeition. They perform network security monitoring and ensure that all technology is working properly.
Red Team actively attacks the Blue Teams' infrastructure in order to disrupt the availability and usability of the system.
Green Team tests the usability and availabilty of the Blue Teams' systems.
Blue team interacts with the Green Team to ensure proper IT support is administered.
The CISO Panel interacts with Blue Team members about the level of creativity and innovation in their defense strategy.

Oil logistics and HPC simulators



2020 theme: Wind Farms





Realistic or Artificial?

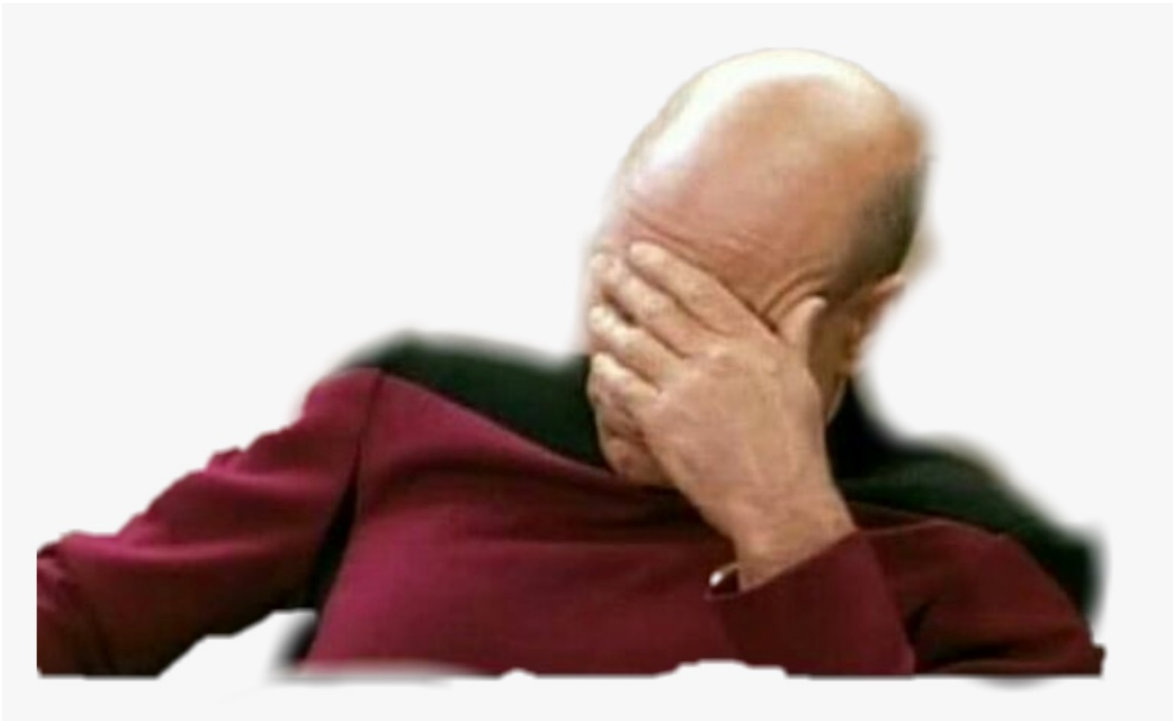
- Tailoring your tactics based on the rules of the game will lead to “gaming”
  - Action is effective in the game environment but doesn’t work in the real world
- Killing all new processes will work in game
  - Do this in a real world job and you will get fired
- Service was not functional but service check still scored as alive

- In CFC, we want to encourage methods that will work in real world conditions – realistic actions and countermeasures

Example of gaming

> Man funniest thing that happened to us one year was that red team broke into our HMI, then broke it so no one could log into it, but forgot to shut it down or disable the service, so it was effectively unhackable but still functional.

👀 2



Problems in 2019 …

- A few beginner teams -> frustration
- Most teams became unhackable -> boredom

To win in 2019

- Can be unhackable:
  - Apply patches
  - Strict firewall rules
  - Strong passwords
  - Find the backdoors in the VM images

- Those are all good things, but there’s so much more for blue teaming:
  - Detection, mitigation, recovery, hunting, system hardening, balancing functionality and security, enabling security features, understand underlying technology, tool competency, understand risk, attack analysis

The competition: What is it really?

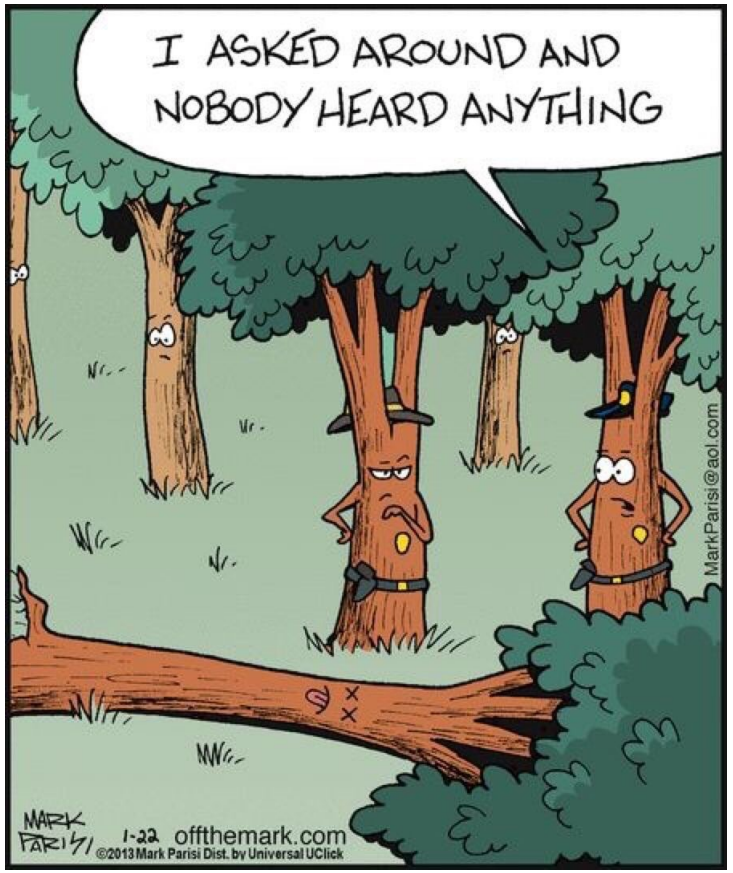
- A system administration / perimeter protection exercise?
  - That can be completed in 30 mins.

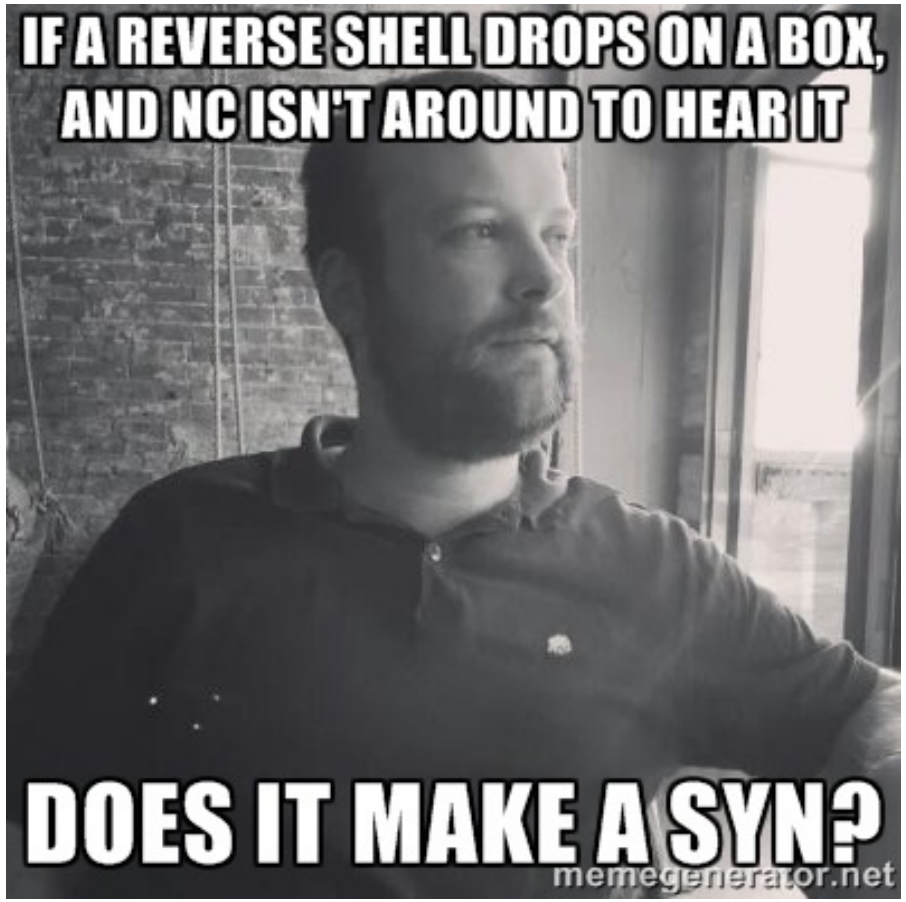
- Or full cyber attack lifecycle competition?
  - What is necessary to enable it
  - You won’t get it by giving blue a few VMs and then ask red to attack them

- What skills do we want see from the blue team?
  - To do so, your scoring needs to be explicitly directed at them

A cyber koan

- Can students demonstrate recovery/hunting if hackers can’t get in?





Role of the Red team?

- Emulate a high level adversary – nation state APT
  - Create the infrastructure to allow this
- Cover a WIDE range of TTPs
  - Including tailored ones against ICS systems
- Keep score of blue team defensive actions
  - Communicate to blue team the scoring criteria
- Goal of maximizing the learning for students

= A lot of work needs to be done!

This means you can’t just roll up on game day and “hack away”

Role of the Red team

- Red team is not “competing”
- Blue teams are competing against other
- Red is there to provide cyber effects,
  - give something for Blue to do

Role of the Red team

Run attacks

and

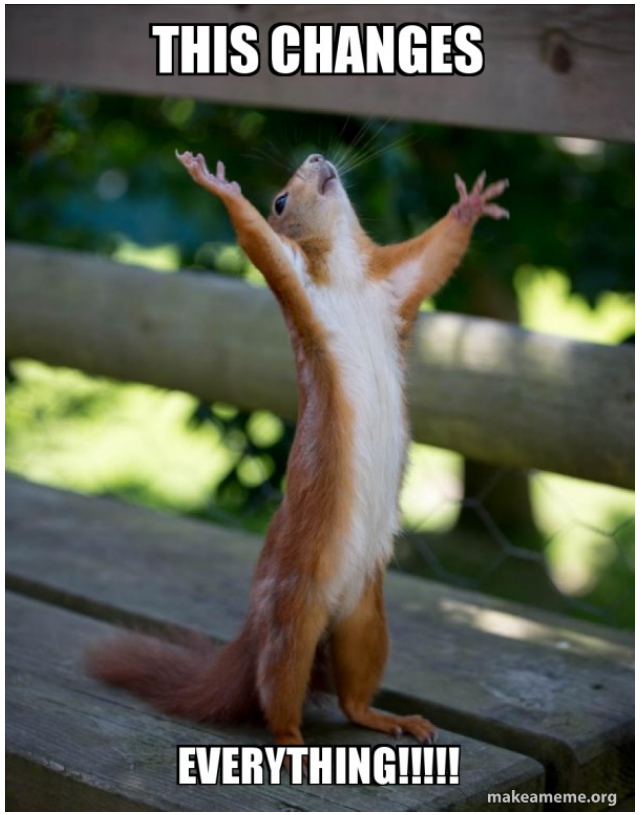
Score keeper/Judge

What’s the best part of the competition?

- The debrief/hotwash with the red team after the event
- Instead of just at the end of competition,
- Let’s do it throughout the competition with the score chat
- Able to accurately attribute different actions

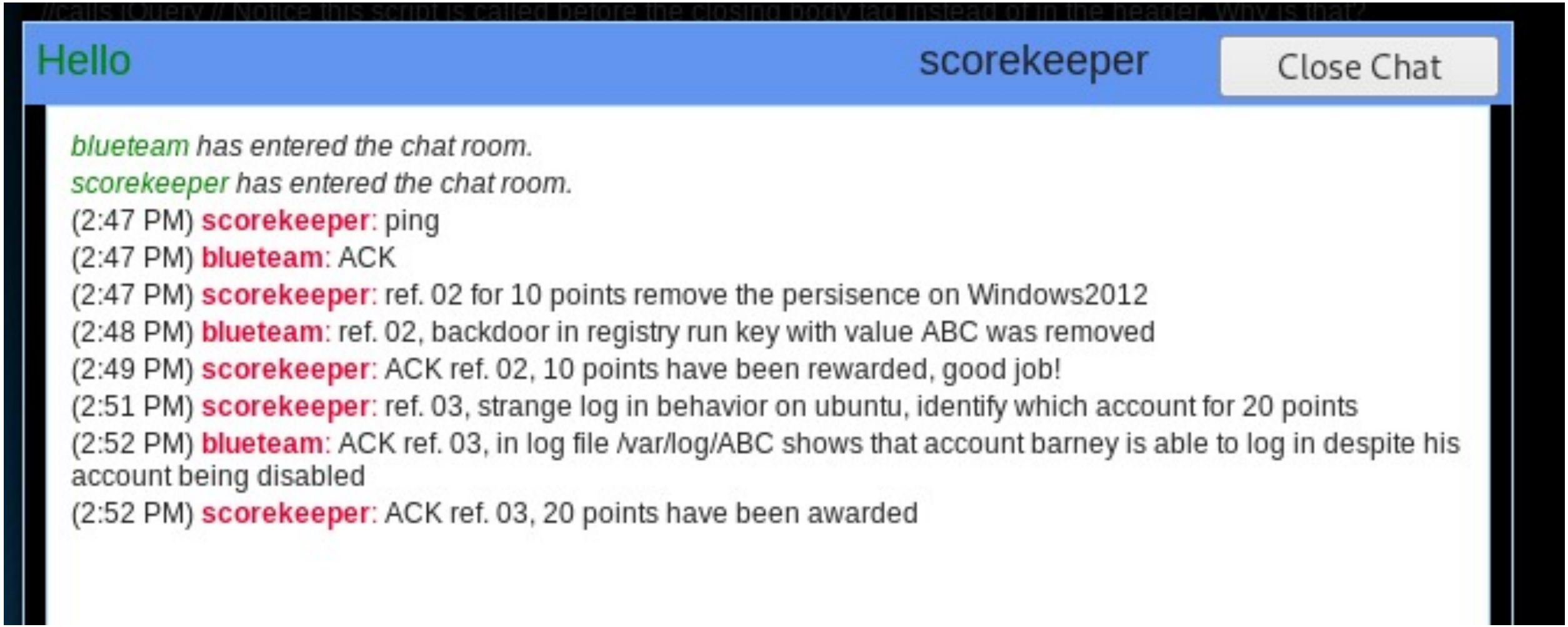
The Score Chat

- Transparency of scoring
- Able to help students uncover their weaknesses
  - SQL injection example
  - Teaching moments are everywhere
- Not allowed as an attacker vector
- Cannot use it for social engineering



On Scoring

- Other competitions: if red team is successful, you LOSS points
- In CFC 2020: our red teams can only GIVE you points
- What does this mean? Red will give you specific activities to complete to get points


//calls jQuery // Notice this script is called before the closing body tag instead of in the header. Why is that?
Hello
scorekeeper
Close Chat
blueteam has entered the chat room.
scorekeeper has entered the chat room.
(2:47 PM) scorekeeper: ping
(2:47 PM) blueteam: ACK
(2:47 PM) scorekeeper: ref. 02 for 10 points remove the persisence on Windows2012
(2:48 PM) blueteam: ref. 02, backdoor in registry run key with value ABC was removed
(2:49 PM) scorekeeper: ACK ref. 02, 10 points have been rewarded, good job!
(2:51 PM) scorekeeper: ref. 03, strange log in behavior on ubuntu, identify which account for 20 points
(2:52 PM) blueteam: ACK ref. 03, in log file /var/log/ABC shows that account barney is able to log in despite his account being disabled
(2:52 PM) scorekeeper: ACK ref. 03, 20 points have been awarded

Realtime and then turn-based

- Allows the blue team to breath

Stressed, knee jerk reactions

Have time to think

Can learn new things

More on Score Chat

- Have an option for hints
- Blue needs to justify their actions, do they really understand what's going on
- Need to show evidence of findings
- Guessing is not good enough

(10:42 PM) scorekeeper_kp: Did that work?
(10:43 PM) Blueteam: will check
(10:45 PM) Blueteam: once my winserv2012 starts responding
(10:46 PM) scorekeeper_kp: if winserv2012 is really slow and you have a command window, run sc stop jumpftp
(10:48 PM) Blueteam: once my windows show back up I'll try that
(10:49 PM) scorekeeper_kp: ok
(10:53 PM) Blueteam: the windows came back but now I'm trying to get cmd open
(10:53 PM) Blueteam: since powershell immediately crashed
(10:55 PM) scorekeeper_kp: ok
(10:55 PM) Blueteam: okay, I got it pulled up
(10:56 PM) Blueteam: I'm not seeing any file named info.php in C:php-test
(10:56 PM) scorekeeper_kp: that's is correct
(10:56 PM) scorekeeper_kp: maybe it's a different log entry that you have to focus on
(10:58 PM) Blueteam: so that GET log that I posted was not correct?
(10:58 PM) scorekeeper_kp: think it through - it looked like it would create info.php into c:php-test, but that didn't happen ....
(10:59 PM) scorekeeper_kp: how can you know for sure the results of a command ....
(11:07 PM) Blueteam: of a sql command? I have no logs for those aparently
(11:08 PM) scorekeeper_kp: so what you see in the log is the web request that was made. And it looks like there are sql statements there.
(11:09 PM) scorekeeper_kp: you have to figure it out will it do anything or if it's harmless and not doing anything
(11:10 PM) Blueteam: the file the sql command is saying to output to is not present, so it didn't run the sql command
(11:11 PM) scorekeeper_kp: that seems to be the case
(11:11 PM) scorekeeper_kp: but what if the sql command was different ....
(11:13 PM) Blueteam: I have no sql logs to confirm anything
(11:13 PM) scorekeeper_kp: do want to take the hint option?
(11:13 PM) Blueteam: sure
(11:14 PM) scorekeeper_kp: this is normal expected behavior: http://10.0.109.5/info.php?query=174
(11:14 PM) scorekeeper_kp: what happens you do this instead?
(11:14 PM) scorekeeper_kp: info.php?query=174%20union%20all%20select%201,%202,%20@@version
(11:16 PM) Blueteam: it outputs the version of mysql
(11:17 PM) scorekeeper_kp: If it can output the mysql version, what does that mean?
(11:19 PM) Blueteam: the sql commands worked, but they were just unable to write the output to the file
(11:19 PM) scorekeeper_kp: Yes!!!
(11:19 PM) scorekeeper_kp: try this:
query=174%20union%20all%20select%201,%202,%20table_name%20from%20information_schema.tables

Send

(10:55 PM) **Blueteam** okay, I got it pulled up
(10:56 PM) **Blueteam** I'm not seeing any file named info.php in C:php-test
(10:56 PM) **scorekeeper_kp**: that's is correct
(10:56 PM) **scorekeeper_kp**: maybe it's a different log entry that you have to focus on
(10:58 PM) **Blueteam**: so that GET log that I posted was not correct?
(10:58 PM) **scorekeeper_kp**: think it through - it looked like it would create info.php into c:php-test, but that didn't happen ....
(10:59 PM) **scorekeeper_kp**: how can you know for sure the results of a command ....
(11:07 PM) **Blueteam** of a sql command? I have no logs for those aparently
(11:08 PM) **scorekeeper_kp**: so what you see in the log is the web request that was made. And it looks like there are sql statements there.
(11:09 PM) **scorekeeper_kp**: you have to figure it out will it do anything or if it's harmless and not doing anything
(11:10 PM) **Blueteam** the file the sql command is saying to output to is not present, so it didn't run the sql command
(11:11 PM) **scorekeeper_kp**: that seems to be the case
(11:11 PM) **scorekeeper_kp**: but what if the sql command was different ....

(11:13 PM) **Blueteam**: I have no sql logs to confirm anything
(11:13 PM) **scorekeeper_kp**: do want to take the hint option?
(11:13 PM) **Blueteam** sure
(11:14 PM) **scorekeeper_kp**: this is normal expected behavior: http://10.0.109.5/info.php?query=174
(11:14 PM) **scorekeeper_kp**: what happens you do this instead?
(11:14 PM) **scorekeeper_kp**: info.php?query=174%20union%20all%20select%201,%202,%20@@version
(11:16 PM) **Blueteam**: it outputs the version of mysql
(11:17 PM) **scorekeeper_kp**: If it can output the mysql version, what does that mean?
(11:19 PM) **Blueteam**: the sql commands worked, but they were just unable to write the output to the file
(11:19 PM) **scorekeeper_kp**: Yes!!!
(11:19 PM) **scorekeeper_kp**: try this:
query=174%20union%20all%20select%201,%202,%20table_name%20from%20information_schema.tables

- 25 mins. just for this one scored event
- What you're see here is knowledge transfer happening

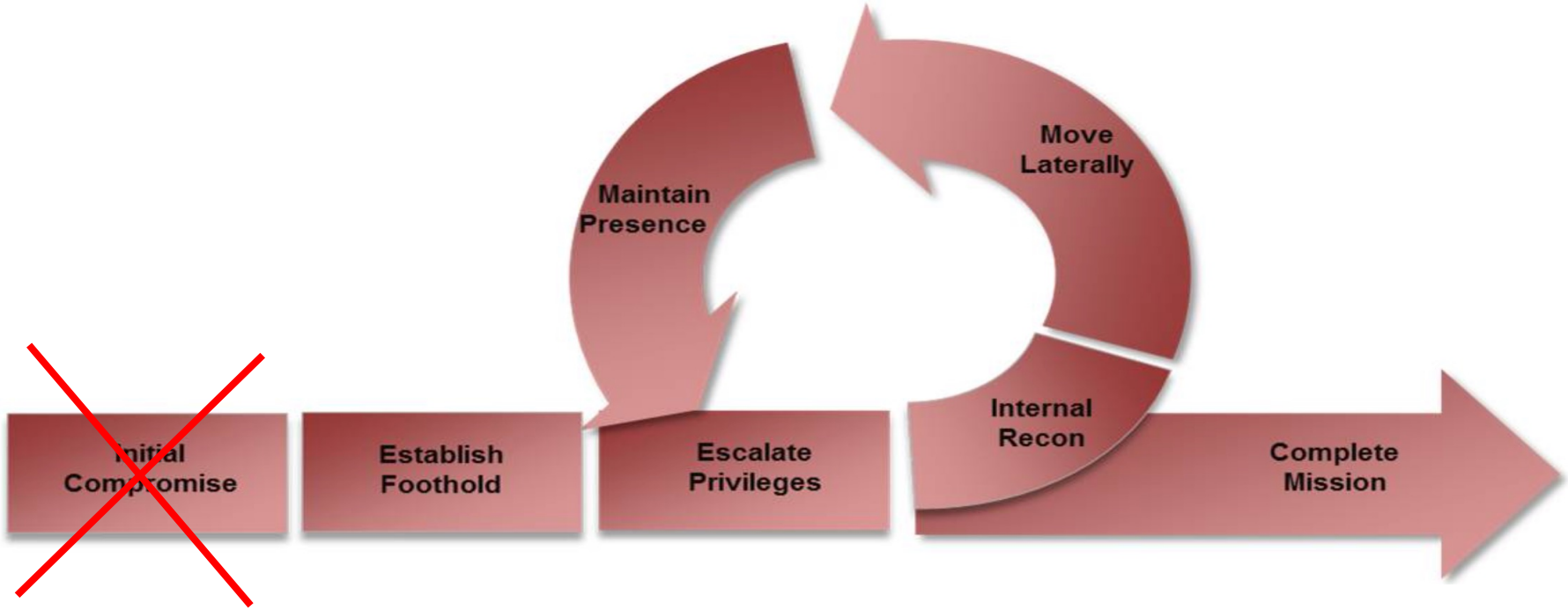
Justification not good enough for points …

- Allows us to find gaps in blue team knowledge and help remediate them
- Remain profession, we all have to start from somewhere

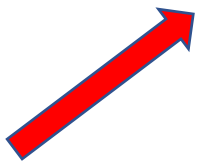
(9:21 PM) **scorekeeper_jb**: ref 701, the hackers were remotely able to find the following running processes: httpd, bash, sshd, systemd, ypbind, agetty, python3, cron, inetd, snmpd, ypserv, in.tftpd, atd, lxcfs, nfsd. How did they get this information from the Ubuntu machine?
(9:22 PM) [redacted]: nmap
(9:22 PM) [redacted]: they ran a sevice scan
(9:22 PM) **scorekeeper_jb**: How did you come to that conclusion?
(9:22 PM) [redacted]: i know how to use nmap

The access dependency problem

- Need access to do most attacks
- kill -9 [pid] ; iptables -P [INPUT,FORWARD] DROP



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		



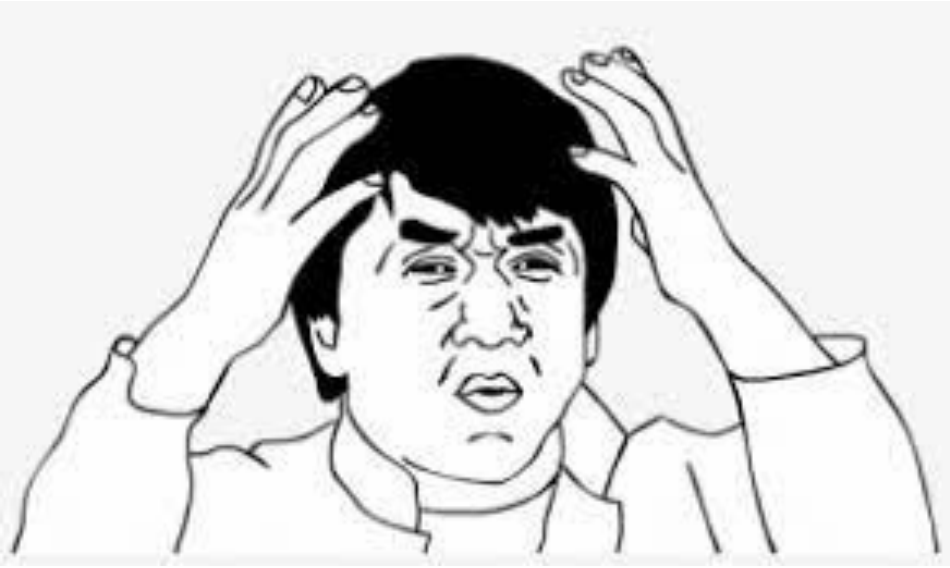
Need access

Solution to initial access problem

- Assume breach

... Ask the blue team not to kill your shells

- Will that work??!!
- YES!!!

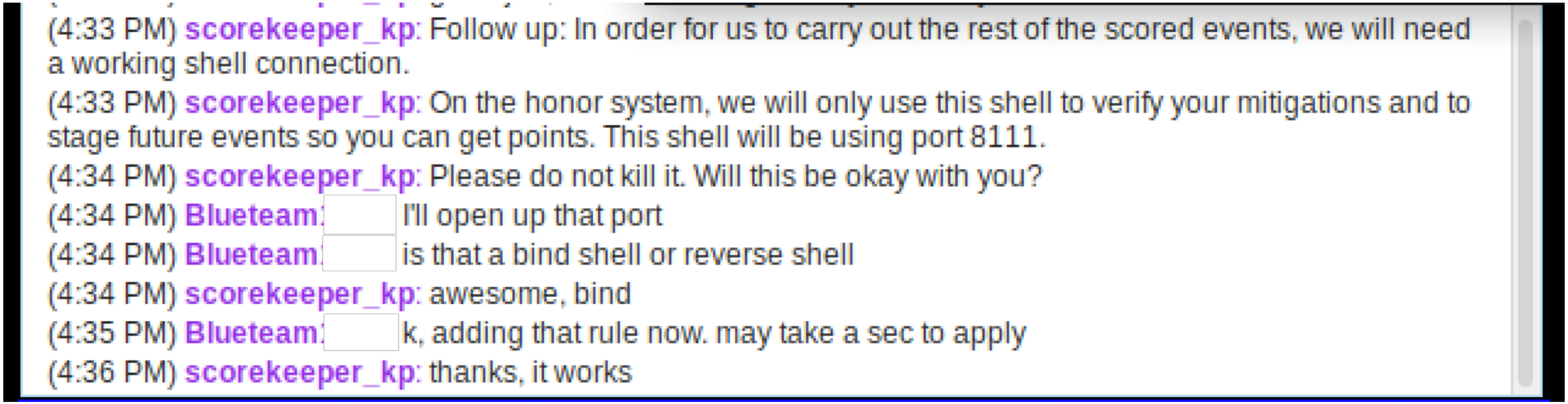


Coming to an agreement in Score Chat

- Red team uses an attack and gain a shell
  - Stops there (if red wanted, has the ability to rm -rf /)
- As a scoring event, ask blue to detect it
- As the next scoring event, ask blue to kill shell
  - Shows that blue has the ability to kill shells

- Red now pops a new shell and informs that it will only be used for verification and post exploit actions to give blue opportunities to score points
- Blue agrees!

(4:15 PM) **scorekeeper_kp**: ref.501: hacker has a backdoor listener running on ubuntu, id the port number of it
(4:15 PM) **Blueteam**: port 1337
(4:15 PM) **scorekeeper_kp**: how did you get that information?
(4:15 PM) **Blueteam**: https://imgur.com/a/TatrxSw
(4:17 PM) **scorekeeper_kp**: congrats, you have scored 100% for ref.501
(4:17 PM) **scorekeeper_kp**: you can now close the port 1337
(4:18 PM) **Blueteam**: Thanks, was already closed by my firewall
(4:19 PM) **scorekeeper_kp**: please kill the process that is assoicated with port 1337
(4:20 PM) **Blueteam**: done
(4:20 PM) **scorekeeper_kp**: nice!
(4:27 PM) **scorekeeper_kp**: ref.502: ID the current established connection used by the hacker on ubuntu .5 and show evidence



- Hopefully, in the future we can just require a shell be given to red team for post exploitation/verification

- Increases red-blue interaction because red doesn't have to worry about burning access and persistence mechanisms

Variety of scoring events now possible

- Can chain plays/events together
- Enabling security features such as logging
- Disabling vulnerable functionality
- Reconfiguring firewall rules for a new device
- Requiring a fix of the vulnerability while maintaining the functionality
- Learn to run a security tool

Score Chat: result of all of this learning

2019

2020

Documentation of Scoring

Reference ID	Play Name		Server	Approx. Time
505	Bind9 Unquoted Service Path Privilege Escalation			10:50 AM
		75%		
	3 bonus morris worm			
506	php remote code execution			11:00 AM
	hint: 75			
507	SMTP account enumeration			11:10 AM
		100		
	2 bonus for opinion			
508	scan ICS modbus			11:20 AM
	5 bonus points movie			
		100		

A playbook approach

- Fairness: all blue teams will experience the same attacks
- Ensure a good selection of different TTPs
- Good coverage of MITRE ATT&CK framework
- Given exact commands to run
- Pre-packaged attacks

ref.500

title

hydra: easily guess password with ssh [ ], ubuntu 18.04, medium

exploit:

```
hydra -l admin -P pwlist.txt 10.X.Y.5 -t 2 ssh
```

result is

If that doesn't work, try this one:

```
hydra -L hydra-users.txt -P hydra-passwords.txt -u -t 4 10.X.Y.5 ssh
```

result is

solution

score chat

> On ubuntu, hacker was able to log in with compromised account, idenitfy the account

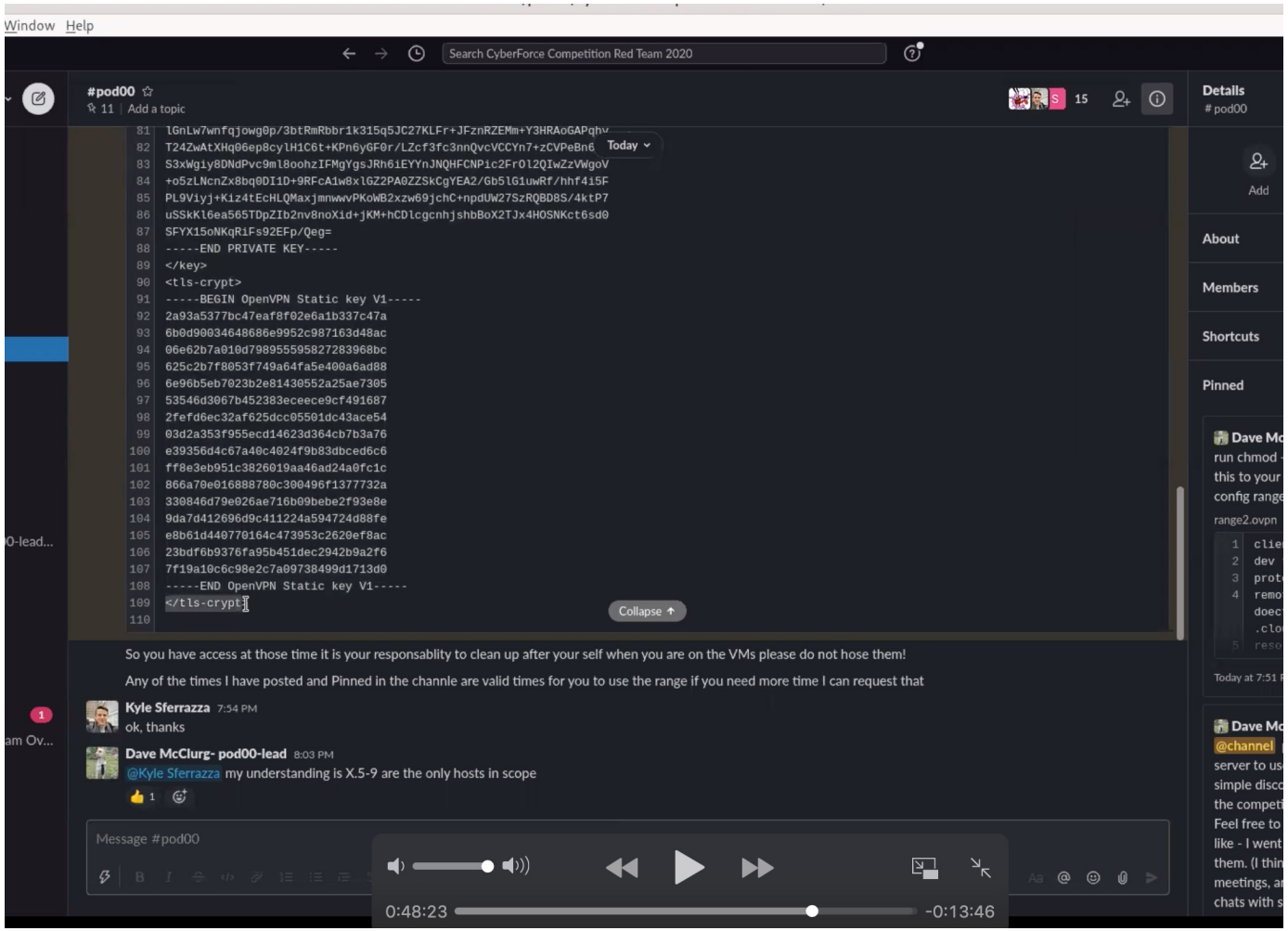
hint

> review s

notes

More complex attacks - hard to understand

- Provided video walk-thru



What about free play and creativity?

- Discretionary pool of points available
- You can create novel attacks and use it
- But you must document it on the shared playbook on gitlab so that all red teams can use it (fairness)
- You must also create a scoring criteria for it
- In a dynamic environment, there going to be a lot of adapting that is necessary
- Last 10 mins., there is a ”keep out” phase of the game

Pre-baking vulns. into VMs

- Ideally lead by an experienced Red teamer
- Need to make sure that they don’t conflict
  - Having 3 different web applications trying to use port 80
- Guarantee a variety of different vulnerability types and classes
- High quality vulns. will require months to develop
  - Need to use a compiler to create these vulns.
  - Assigned to a trusted core team (thanks Marshall Riley!)
- Make sure that the corresponding exploit will work in deployed environment

More on the VMs

- Reality: red teams only used pre-existing vulnerabilities added by the organizers
- Blue teams did not add vulnerabilities or exploitable misconfigurations
- I put out a friendly wager that if you found an exploitable vulnerability that was not added by my team, you would get a prize
  - None found

New for 2020

- We have zero days!
  - Good for blue teams to experience, it’s not the end of the world
- We have phishing attacks against email
  - Not to full shell (because green team is off-limits)
  - Allow blue team to experience and learn to detect it
- More advanced web attacks: LFI to RCE
- Complex attacks with 3+ dependencies

Rules regarding the VMs

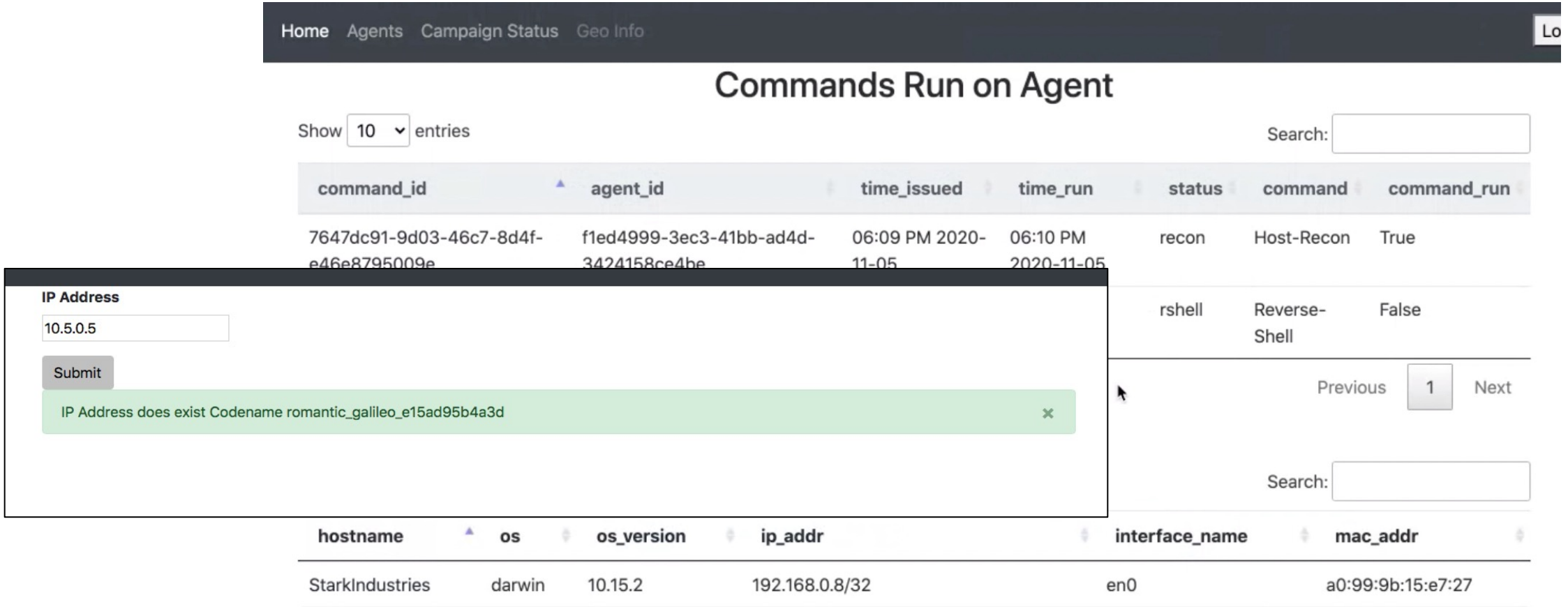
- There are a set of services, accounts, and configurations that blue team is NOT allowed to change
  - This allows minimum attack surface that the red team can leverage
  - No attack surface means no red activity (everyone can go home)
- This also allows the white team to inject vulnerabilities during game time
  - Simulate developers and junior admins making system changes
- All of the other services and configurations is open game
- So a combination of static and dynamic system configurations

Shell sherpas

- National CCDC has been doing this for a long time
- Special team that is in charge of managing long haul C2 servers
- We had 2 different shell sherpa teams:
- A) Cobalt Strike team (thanks Raphael Mudge for allowing usage!)
  - 260+ beacons

- B) Custom C2 team – DirtyC2 (thanks Brandon Radosevich)
  - 1000+ agents

DirtyC2


Home
Agents
Campaign Status
Geo Info
Lo
Commands Run on Agent
Show 10 entries
Search:
command_id
agent_id
time_issued
time_run
status
command
command_run
7647dc91-9d03-46c7-8d4f-e46e8795009e
f1ed4999-3ec3-41bb-ad4d-3424158ce4be
06:09 PM 2020-11-05
06:10 PM 2020-11-05
recon
Host-Recon
True
rshell
Reverse-Shell
False
Previous
1
Next
IP Address
10.5.0.5
Submit
IP Address does exist Codename romantic_galileo_e15ad95b4a3d
Search:
hostname
os
os_version
ip_addr
interface_name
mac_addr
StarkIndustries
darwin
10.15.2
192.168.0.8/32
en0
a0:99:9b:15:e7:27

ICS attack dev team

- Need the right experts
- Guidance of the types of attack needed
- Also need to have a good scoring objective (detection, mitigation, or recovery?)
- Make sure the packaged attacks are well tested so that all red teams can use

Technical maturity of red team

- Moving away from typical pentesting – nmap (scanning), nessus, metasploit, dirbuster, hydra (password guessing)
- To advanced red teaming – weaponized TTP approach covering the whole attack life cycle to achieve attacker goals
- Understanding this is important for blue teams to improve and for the organizers to provide the right resources

Assigning people to groups

- I want an environment where we can all learn from each other
  - Ultimately we're all one team
- Meet new people – you learn much more that way instead of staying in your clique
- Identify potential group leaders – have the skills and are already helping others
- When groups are set, knowledge tends to stay within them instead of shared globally

Instead of griefing, encourage

- CFC wants to be a welcoming and inclusive environment
- We stopped “burn everything to the ground” since 2018
- Blue teams wanted their VMs intact after event to do analysis
- We got a lot of positive feedback from blue teams

CFC 2020: Red team believes in you!!

HMI	Info	Help	Admin	About

Sat Nov 14 22:16:51 UTC 2020

end of page

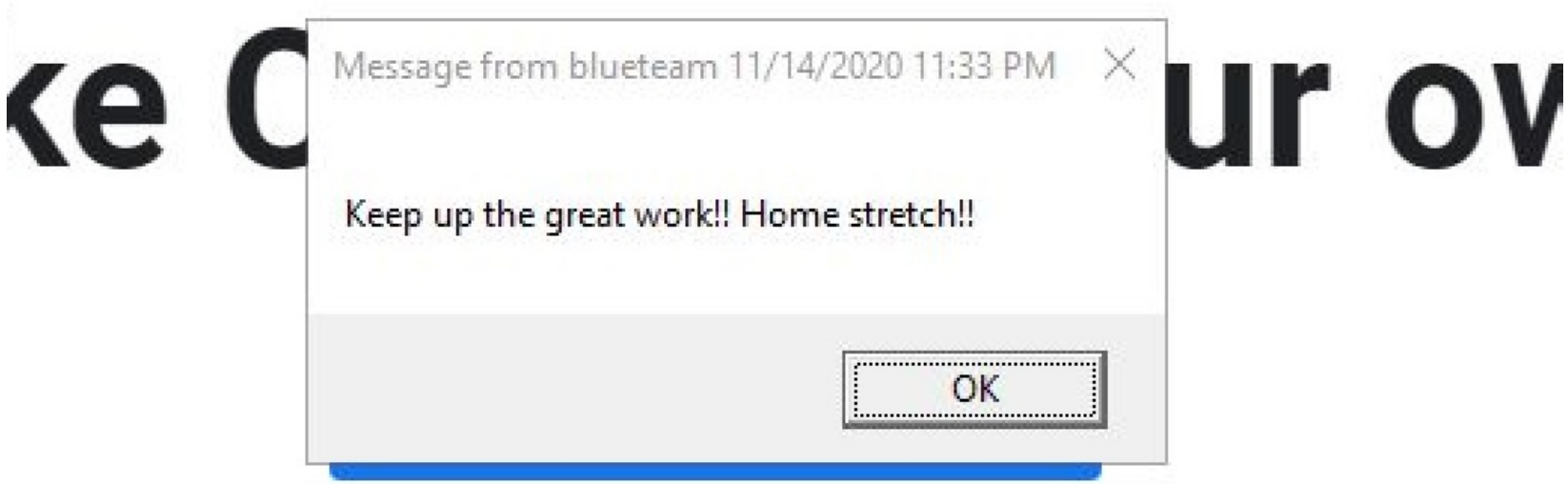
CyberForce Competition 2020: Welcome to WindFarm Local!

Home | HMI | Info | Help | Admin | About

Today is 2020-11-14 18:50:44 ET / 17:50:44 CT

end of page

Set up your browser in a few simple steps



Already a Chrome user? Sign in

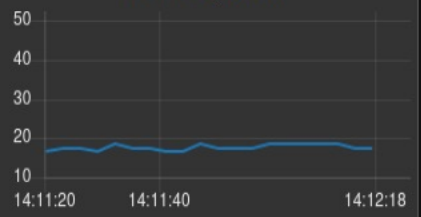
Node-RED Dashboard

10.0.24.9:1880/ui/#!/0?socketid=mXB1W-fFDMS_yUzbAAAE

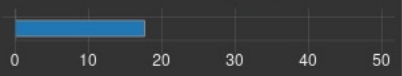
Home

Wind Speed

Wind Speed



Current Average Speed



17.5 Km/h

Control Center

Turbine 1 Power

Turbine 2 Power

Manual Overide

Turbine 3 Power

Turbine 4 Power

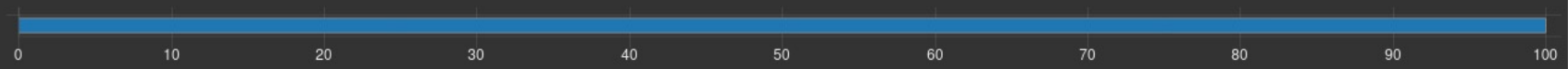
Turbine 1

Turbine 2

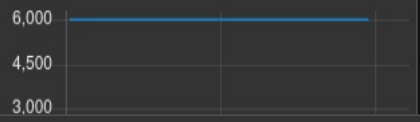
Turbine 3

Turbine 4

Performance



Wind Power



Kill Switch

Mozilla Firefox

File Edit View History Bookmarks Tools Help

10.1.38.5/

10.1.38.5

CFC 2020: Welcome to Wind Farm!

HMI | Info | Help | Admin | About

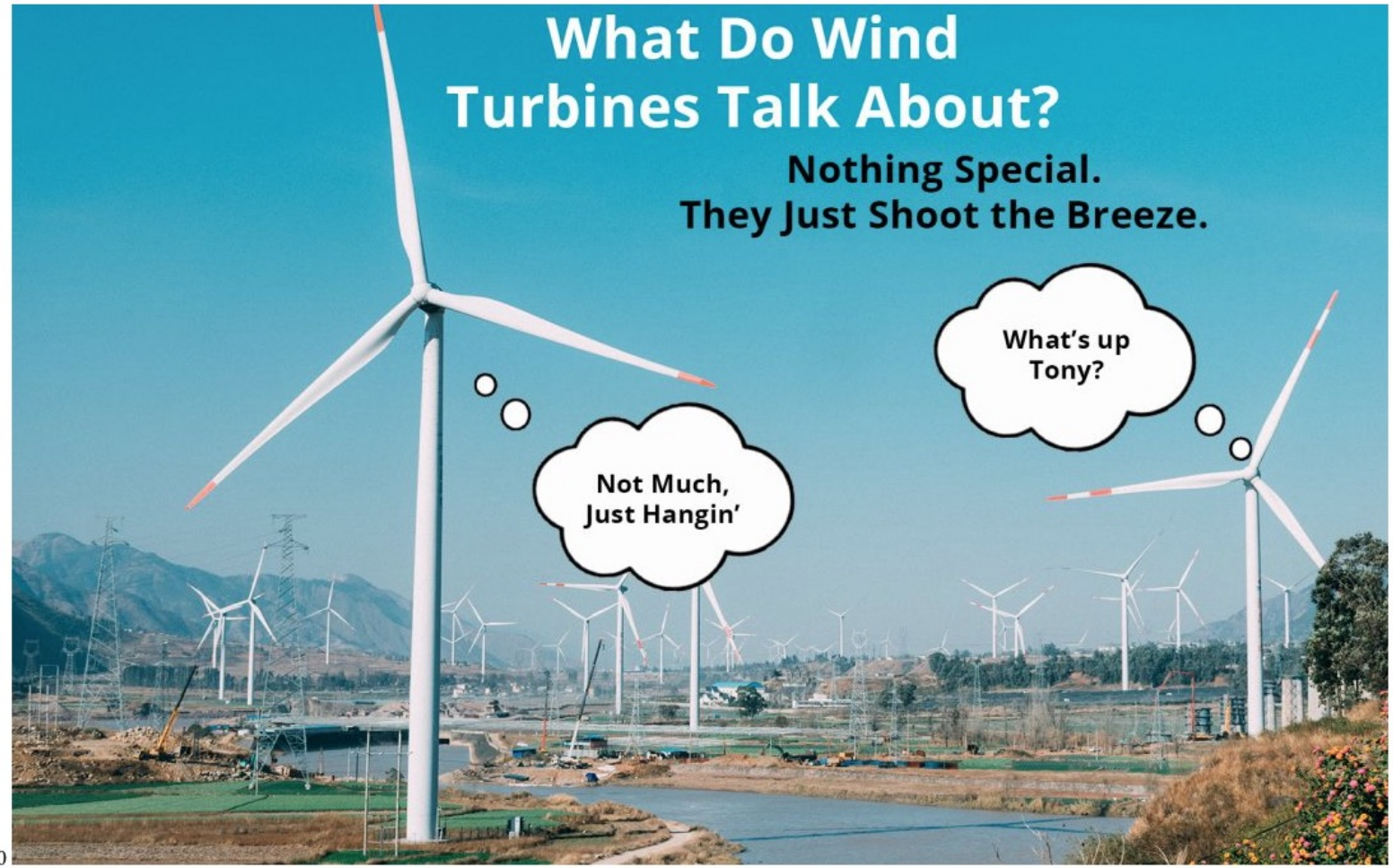
Sat Nov 14 19:06:34 UTC 2020

end of page

Not Secure | 10.0.114.5/index.php

CyberForce Competition 2020: Welcome to Wind Farm!

Home	About	Info	HMI	Help	Admin



Sat Nov 14 21:59:40 UTC 2020

end of page

References

- https://alexlevinson.wordpress.com/2013/04/24/ccdc-2013-red-team-feedback/
- https://www.hecfblog.com/2013/04/nccdc-2013-lessons-learned.html
- https://www.scriptjunkie.us/2014/03/ccdc-and-ctfs-addressing-the-criticisms/
- https://bluescreenofjeff.com/2017-05-02-red-teaming-for-pacific-rim-ccdc-2017/
- https://blog.cobaltstrike.com/2014/09/09/infrastructure-for-ongoing-red-team-operations/

Thanks!

- Thanks Amanda and Josh at ANL, they are awesome!!
- Thanks to all of the volunteers, core team and my pod leads
- We’re hoping to continually improve the red team aspect
- kphan451 [AT] gmail . com
- @kphan451

Backup slides

Rules for Hack-the-Box Battlegrounds

https://help.hackthebox.eu/en/articles/5185620-gs-introduction-to-battlegrounds

- Defenders are not allowed to massively "kill shells" to secure their systems. They should focus on patching the actual vulnerabilities.

- Defenders aren't supposed to kill a service to patch vulnerabilities.

- When defenders try to patch vulnerabilities, it's their responsibility to ensure that no underlying functionality has been stopped due to their patch. For example, there is a reason for sudo entries, so they should still serve their original purpose when they are modified. Removing a sudo entry is not a "fix", and defenders should consider fixing the insecure "sudo entry" instead of removing it.

- If a system check has been fired in the middle of a service restart or Box reset/reboot, there is a chance that the game will punish defenders with a loss of points. This is intended, and the reason behind that is to "award" the players who didn't restart/reboot many times.

Hack-the-box Cyber Mayhem rules

- A defender's primary goal should be to fix a machine's vulnerabilities while making sure that the machine is available to its users. For example:
- Defenders aren't supposed to shut down machines.
- Defenders aren't supposed to change the root password of machines.
- Defenders aren't supposed to kill a service just to patch vulnerabilities.
- Defenders are not supposed to block the traffic for other users in order to keep them away from their machines.
- Trying to trick the system checks is prohibited. We have created several controls and many are in the works.
- Removing cron jobs is not a "fix" and defenders should edit the script/entry in order to fix the actual vulnerability behind a cron entry.