



How to Win at CCDC



Tim MalcomVetter · Follow

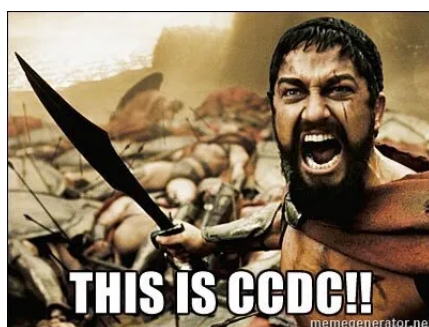
3 min read · Mar 26, 2018



26



1



Yesterday, during the wrap up just minutes before awards ceremony at the Southwest regional CCDC (Collegiate Cyber Defense Competition), I stated that the best performing teams did these 3 (okay ... four) things:

Number Zero: (yes, zero— this must happen first) The teams **got along with each other**. There was respect, order, positivity, and a lack of infighting. All technical things aside, the teams that get frustrated with each other don't win, because the conflict creates inefficiency and prevents productivity.

Now on to the technical things they did.

1. **Asset Inventory.** The best performing teams knew what was on their networks. They traced cables, inspected hypervisors for VMs, and scanned their networks from an attacker's perspective to discover hosts and listening services. They identified versions of software that were likely to be exploited. It all starts with inventory.
2. **Ingress/Egress Firewall Rules.** The best performing teams implemented good firewall policies for both incoming and outgoing traffic. Many SWCCDC red teamers this year discussed how it felt like several schools "didn't even have a firewall" this year, but we knew they did—they just didn't have restrictive policies. Some "bought" upgraded commercial firewalls while others kept the open source firewalls that were "free" in the game. Regardless of which product it was, the best teams implemented tight rules on whatever firewalls they ran—and that included for egress traffic, not just blocking traffic coming into anything that wasn't a "scored" service. When an attacker throws an exploit that binds a command/control (C2) shell to a port, and that port is not accessible via the ingress policy, the blue team prevails. Just as important: when an attacker throws an exploit that calls out to an endpoint the attacker controls and the egress firewall rules block the traffic, the blue team also prevails. In both real life and the game, the scenario where an exploitable vulnerability exists but a firewall policy drops the C2 traffic will slow the attacker down and cause them to do research. When the CCDC red team shares intel about a specifically exploitable vulnerability in the student networks, and it works on several of the student networks, but not yours because you have good ingress/egress filtering, then you just made it EXPENSIVE for the red team. It will cost them valuable time to troubleshoot why the C2 didn't work, which may possibly distract them from finding a different vulnerability that you haven't protected

yet. *[Also note: you can't do #2 if you don't do #1.]*

3. **Monitoring.** The best performing teams monitored their networks. They saw the firewall dropped packets and watched for the allowed packets to see if anything malicious was missed. They watched processes launching on hosts that were tied back to unexpected network traffic. Ideally, this would be done using centralized log management for better scalability, but some teams divided hosts up among team members and did okay at monitoring simply because the scale was small.

Not only will doing these three things make you a good CCDC competitor, but they will prepare you for real life in InfoSec as well.



Written by Tim MalcomVetter

1.4K Followers

Follow



Cybersecurity. I left my clever profile in my other social network:

<https://www.linkedin.com/in/malcomvetter>

More from Tim MalcomVetter



 Tim MalcomVetter

How to Create an Internal/Corporate Red Team

Congratulations! Your organization has approved the creation of an internal Red...

Jul 16, 2020  181  3



 Tim MalcomVetter

Safe Red Team Infrastructure

This is a quick follow-up to “Responsible Red Teams.” This walks at a high-level...

Feb 21, 2018  207

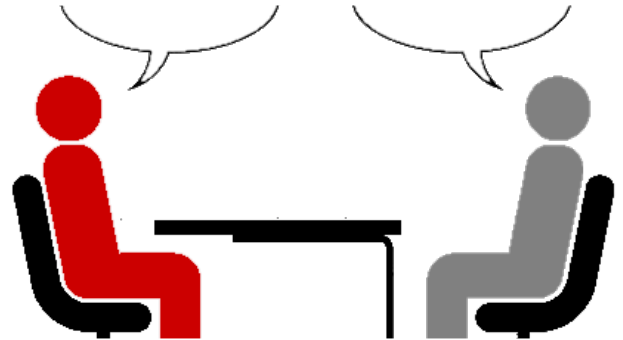


 Tim MalcomVetter

Simplifying Domain Fronting

Like many things in InfoSec, we complicate concepts with new terms and lingo, but th...

Aug 3, 2017  263  4



 Tim MalcomVetter

How to Pass a Red Team Interview

I get the question “What makes a good Red Teamer?” or “What do you look for in a Re...

Oct 20, 2017  415



See all from Tim MalcomVetter

Recommended from Medium

AMAZON.COM

Seattle, WA

Software Development Engineer

Mar. 2020 – May 2021

- Developed Amazon checkout and payment services to handle traffic of 10 Million daily global transactions
- Integrated Iframes for credit cards and bank accounts to secure 80% of all consumer traffic and prevent CSRF, cross-site scripting, and cookie-jacking
- Led Your Transactions implementation for JavaScript front-end framework to showcase consumer transactions and reduce call center costs by \$25 Million
- Recovered Saudi Arabia checkout failure impacting 4000+ customers due to incorrect GET form redirection

Projects


NinjaPrep.io (React)

- Platform to offer coding problem practice with built in code editor and written + video solutions in React
- Utilized Nginx to reverse proxy IP address on Digital Ocean hosts
- Developed using Styled-Components for 95% CSS styling to ensure proper CSS scoping
- Implemented Docker with Seccomp to safely run user submitted code with < 2.2s runtime

HeatMap (JavaScript)

- Visualized Google Takeout location data of location history using Google Maps API and Google Maps heatmap code with React
- Included local file system storage to reliably handle 5mb of location history data
- Implemented Express to include routing between pages and jQuery to parse Google Map and implement heatmap overlay



 Alexander Nguyen in Level Up Coding

The resume that got a software engineer a \$300,000 job at...

1-page. Well-formatted.

 Jun 1  23K  451 

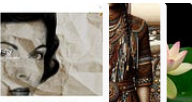
 Kris Gage

How to *really* know you're in love

Because most of “the signs” they tell you are garbage

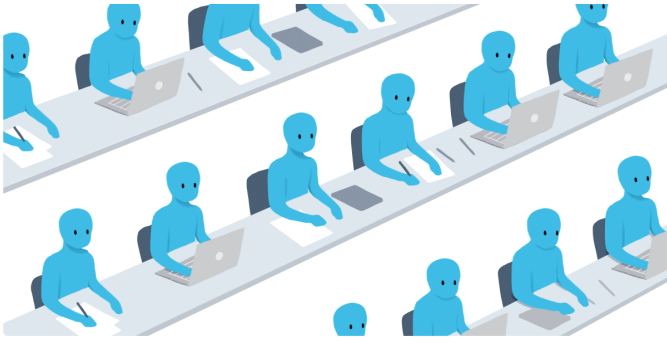
 Aug 3, 2017  141K  899 

Lists



Medium's Huge List of Publications Accepting...

334 stories · 3632 saves



 Devon Price  in Human Parts

Laziness Does Not Exist

Psychological research is clear: when people procrastinate, there's usually a good...


★ Mar 23, 2018  326K  1683 

Kim! Kardashian, 40, reveals how she failed her First Year Law Student exam by scoring 474 but needing 560 to pass despite 'studying 10-12 hours a day for six weeks straight'

Kim didn't pass the baby bar, also known as the First Year Law Student exam

Kim Kardashian failed twice before passing!

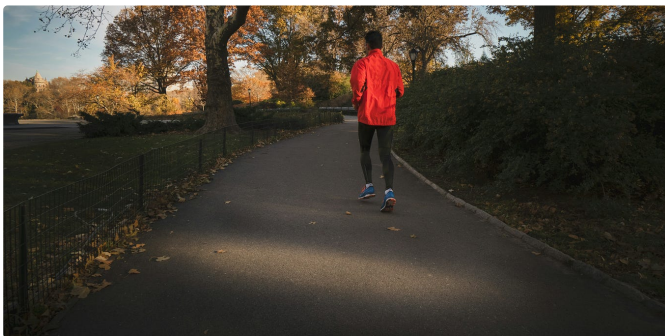


 Tessa Schlesinger Global Atheist... in Tessa's W...

How Do You Recognize Someone Truly Intelligent?

There is only one characteristic that separates them from others.

★ Apr 20  11.9K  265 



 Rebecca  in ILLUMINATION

I Started Waking up at 4:30 a.m. Daily— This Is What Happened

For 21 days, I wake up at 4:30. The results were CRAZY.

★ Apr 9  10.3K  260 



 John Gorman

Stop Wasting Your Time

A Simple Framework for Making Better Decisions

★ Jun 4  19K  348 

See more recommendations

