WRCCDC – 2019-2020

CENTER FOR
CYBERSECURITY &
DIGITAL FORENSICS

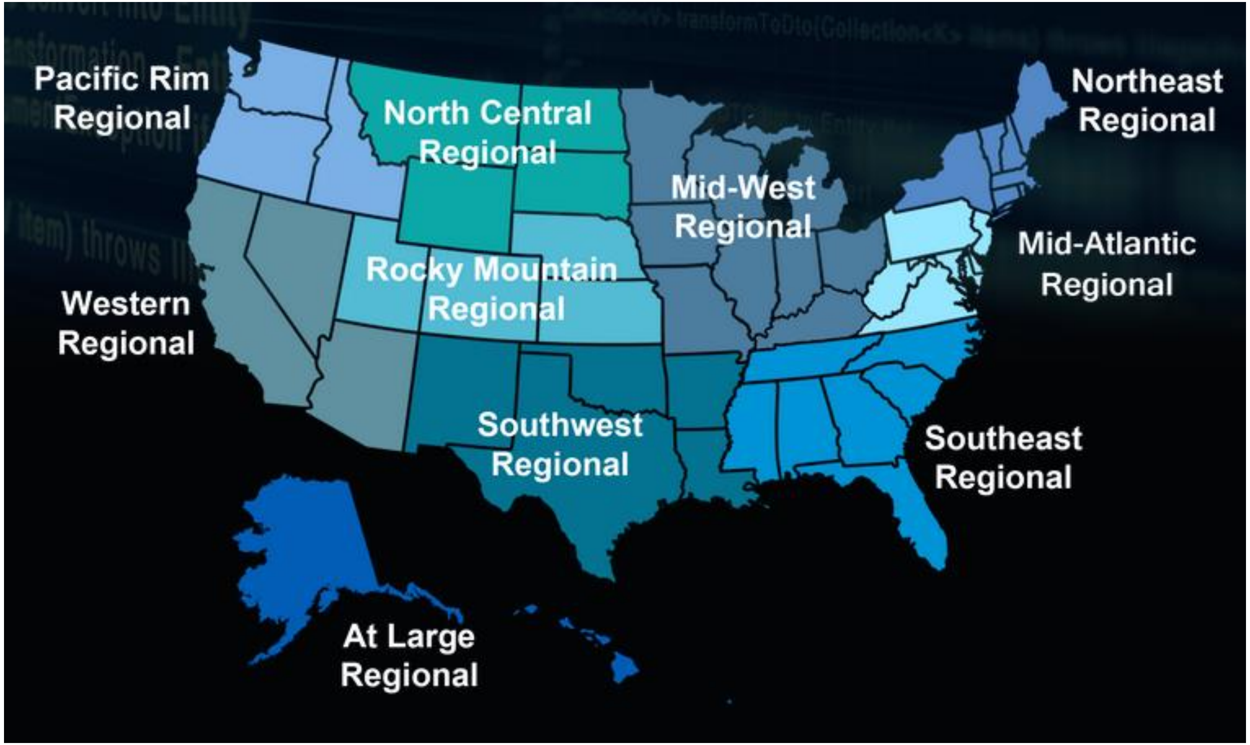
WESTERN
REGIONAL
COLLEGIATE
CYBER DEFENSE
COMPETITION

Ankur Chowdhary (achaud16@asu.edu)

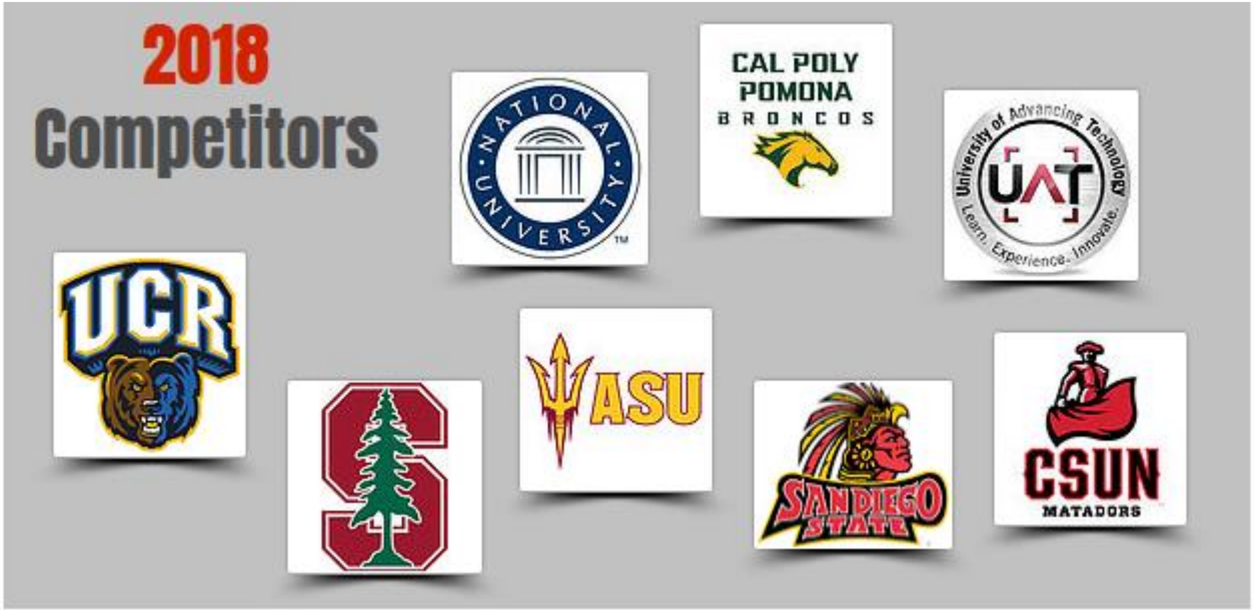
What is CCDC ?

- What you will do when you actually get attacked by some professional hackers?
- How will you ensure your customers don’t lose their business?
- Can you tell your boss why this attack happened in the first place, and how you ensured it won’t happen again?
- Can you work/coordinate as a team to protect your Company or Government Organization?
- Largest college level cyber defense competition.
- Focused on managing and protecting cyber infrastructure.
- Most competitions are focused on offensive aspect of cybersecurity, limited for defense.
- CCDC gives a unique opportunity to learn and respond to actual cyber attack.

NCCDC


Pacific Rim Regional
North Central Regional
Northeast Regional
Mid-West Regional
Mid-Atlantic Regional
Rocky Mountain Regional
Western Regional
Southwest Regional
Southeast Regional
At Large Regional

WRCCDC


2018
Competitors
NATIONAL UNIVERSITY
CAL POLY POMONA BRONCOS
University of Advancing Technology
UAT
Learn. Experience. Innovate.
UCR
ASU
SAN DIEGO STATE
CSUN
MATADORS

Timeline

Stage 1: Invitationals (Virtual)

- Sept 1 - Registration for Invitationals
- Oct 26 - Invitational 1
- November 23 - Invitational 2
- December 14 - Invitational 3
- December 20 - Team Roster Due (12 max, 2 grad students) - 8 will play

Stage 2 - Qualifiers (Virtual)

- Jan 25-26 – Primary Qualifiers (8 out of 17-20 teams go to next round)
- Jan 31 - Student Resumes due

Stage 3 - Regionals (In-Person)

- Final Team roster due
- March 24-26 - Cal Poly Pomona

Composition

- White Team - Hands out business injects
- Black Team - Sets up your network infrastructure
- Red Team - Attempts to penetrate your network
- Blue Team - Us (8 playing members), 4 - reserved (no substitutions during competitions)
- Orange Team - Customer who calls to check service status
- Gold Team - They are organizers, they send emails for logistics, conference calls to answer questions on rules, etc.

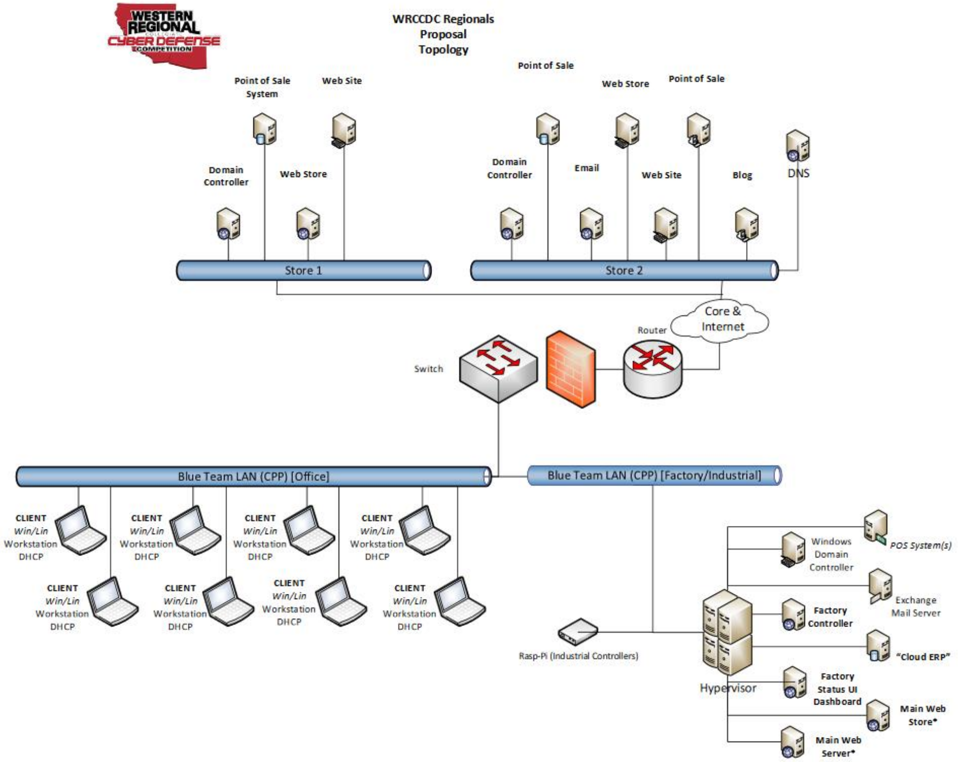
Roles and Responsibilities

- Windows Admin - 2003, XP, 2010, 2016, 2012-Server ?
- Linux Admin - Debian, Redhat, Arch Linux, Gentoo, Fedora, Ubuntu, Feratu ?
- Inject Admin - ?
- Firewall Admin 1&2 - ?
- Incident Response Admin - ?
- Log Analysis Admin - ?
- Database, Webapp Security Admin - ?
- Presentation and Orange Team Admin - ?

Environment

Qualifiers - 10 VMs - mix of Linux and Windows - 2,3 services on VMs, some VMs have no running services. Palo Alto Virtual Firewall.

Regionals - 8 physical machines, 20 virtual machines - 60% Linux, 40% Windows on VMWare esxi and other virtual infrastructure, Palo Alto Hardware Firewall, Cisco Switch.


WESTERN REGIONAL COLLEGIATE CYBER DEFENSE COMPETITION
WRCCDC Regionals Proposal Topology
Point of Sale System
Web Site
Domain Controller
Web Store
Store 1
Point of Sale
Web Store
Point of Sale
Domain Controller
Email
Web Site
Blog
DNS
Store 2
Core & Internet
Router
Switch
Blue Team LAN (CPP) [Office]
Blue Team LAN (CPP) [Factory/Industrial]
CLIENT Win/Lin Workstation DHCP
CLIENT Win/Lin Workstation DHCP
CLIENT Win/Lin Workstation DHCP
CLIENT Win/Lin Workstation DHCP
CLIENT Win/Lin Workstation DHCP
CLIENT Win/Lin Workstation DHCP
CLIENT Win/Lin Workstation DHCP
CLIENT Win/Lin Workstation DHCP
Rasp-Pi (Industrial Controllers)
Hypervisor
Windows Domain Controller
POS System(s)
Exchange Mail Server
Factory Controller
"Cloud ERP"
Factory Status UI Dashboard
Main Web Store*
Main Web Server*

WRCCDC - How we gain points ?

1. Critical Services: Services are checked for functionality and availability throughout the competition – you gain points each time one of your services is “up” or functioning properly when it is checked. Scoring Engine ticks every ~5-10 mins.
2. Injects: Each team needs to perform business tasks and submit reports. Tasks range from simple password policy to complex - set up Sendmail server and create users for access by Orange Team, install IIS Server, set up DNS subdomains for websites. (0%- no submissions, 10% - something submitted, 25% - incorrect, 50% - didn’t follow instructions, 75% - correct but incomplete, 100% - nailed it)
3. Incident Response: Submit a successful and detailed root cause analysis report with proof (logs) to showcase you detected incident, how it can be prevented in future - Firewall, IDS, service logs.
4. Presentations and Orange Team (customer support) - 4 different presenters need to present to a panel.

WRCCDC - How we lose points

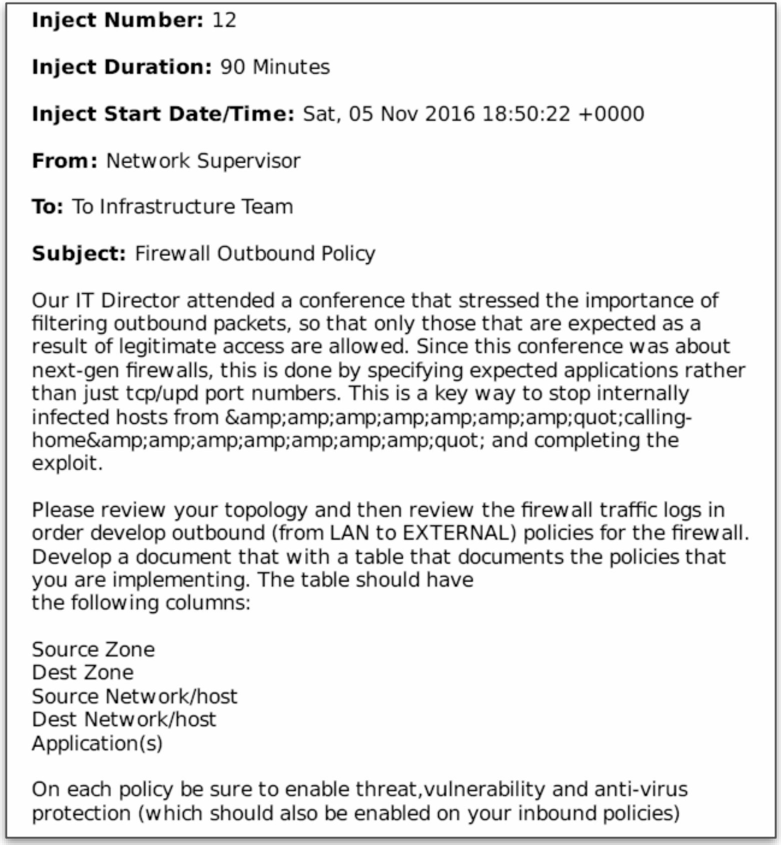
1. Red Team activities- Service goes down due to attack or misconfiguration on our part, scoring engine deducts points. User level access costs fewer points than root level access on VM/services.
2. Failed to submit business injects on time or incomplete business injects
3. Bad incident reports.
4. Bad presentations and Orange team operations.
5. Black Team helps you to debug networking issues that you can’t figure out.

Team which scores best on Service Points, Inject Points, Incidence Response points wins.

Critical Services

S.No.	Virtual Machine	Service
1.	192.168.1.13(morty)	dns
2.	192.168.1.16(nancy)	http, https
3.	192.168.1.19 (cyril)	https, ssh2, ftp
4.	192.168.1.21(frylock)	http, ssh2
5.	192.168.1.20(ethan)	pop3, smtp
6.	192.168.2.13(pam)	dns
7.	192.168.2.15(linda)	http, https
8.	192.168.2.17(shake)	https, ssh2
9.	192.168.2.21(lana)	pop3, smtp, https
10.	192.168.2.25(frylock)	https
11.	192.168.3.10(archer)	Http, https
12.	192.168.3.14(bob)	https
13.	192.168.3.15(meatwad)	ssh2
14.	192.168.3.18(lousie)	http

Business Injects



Inject Number: 12

Inject Duration: 90 Minutes

Inject Start Date/Time: Sat, 05 Nov 2016 18:50:22 +0000

From: Network Supervisor

To: To Infrastructure Team

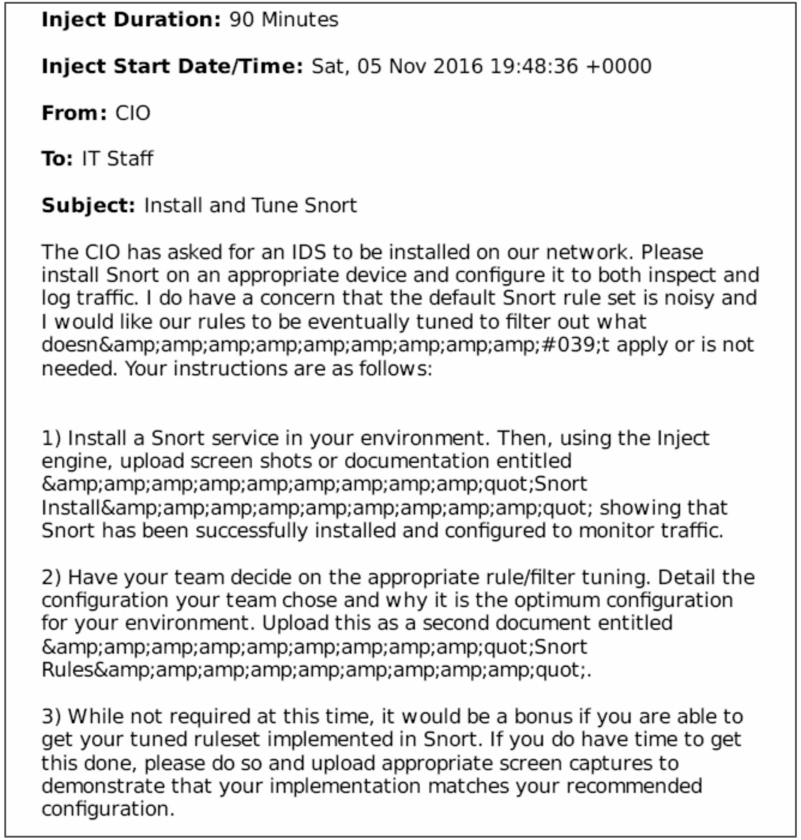
Subject: Firewall Outbound Policy

Our IT Director attended a conference that stressed the importance of filtering outbound packets, so that only those that are expected as a result of legitimate access are allowed. Since this conference was about next-gen firewalls, this is done by specifying expected applications rather than just tcp/upd port numbers. This is a key way to stop internally infected hosts from &amp;amp;amp;amp;amp;amp;quot;calling-home&amp;amp;amp;amp;amp;amp;quot; and completing the exploit.

Please review your topology and then review the firewall traffic logs in order develop outbound (from LAN to EXTERNAL) policies for the firewall. Develop a document that with a table that documents the policies that you are implementing. The table should have
the following columns:

Source Zone
Dest Zone
Source Network/host
Dest Network/host
Application(s)

On each policy be sure to enable threat,vulnerability and anti-virus protection (which should also be enabled on your inbound policies)



Inject Duration: 90 Minutes

Inject Start Date/Time: Sat, 05 Nov 2016 19:48:36 +0000

From: CIO

To: IT Staff

Subject: Install and Tune Snort

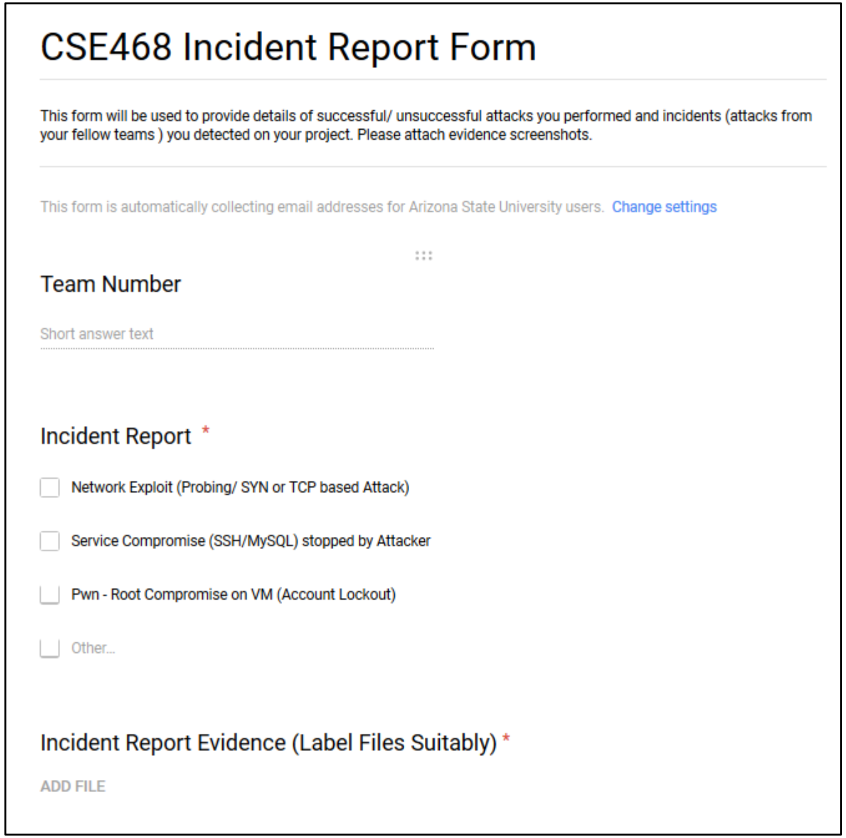
The CIO has asked for an IDS to be installed on our network. Please install Snort on an appropriate device and configure it to both inspect and log traffic. I do have a concern that the default Snort rule set is noisy and I would like our rules to be eventually tuned to filter out what doesn&amp;amp;amp;amp;amp;amp;amp;amp;#039;t apply or is not needed. Your instructions are as follows:

1) Install a Snort service in your environment. Then, using the Inject engine, upload screen shots or documentation entitled &amp;amp;amp;amp;amp;amp;amp;amp;quot;Snort Install&amp;amp;amp;amp;amp;amp;amp;amp;quot; showing that Snort has been successfully installed and configured to monitor traffic.

2) Have your team decide on the appropriate rule/filter tuning. Detail the configuration your team chose and why it is the optimum configuration for your environment. Upload this as a second document entitled &amp;amp;amp;amp;amp;amp;amp;amp;quot;Snort Rules&amp;amp;amp;amp;amp;amp;amp;amp;quot;.

3) While not required at this time, it would be a bonus if you are able to get your tuned ruleset implemented in Snort. If you do have time to get this done, please do so and upload appropriate screen captures to demonstrate that your implementation matches your recommended configuration.

Incidence Response



CSE468 Incident Report Form

This form will be used to provide details of successful/ unsuccessful attacks you performed and incidents (attacks from your fellow teams) you detected on your project. Please attach evidence screenshots.

This form is automatically collecting email addresses for Arizona State University users. Change settings

Team Number

Short answer text

Incident Report *

□ Network Exploit (Probing/ SYN or TCP based Attack)

□ Service Compromise (SSH/MySQL) stopped by Attacker

□ Pwn - Root Compromise on VM (Account Lockout)

□ Other...

Incident Report Evidence (Label Files Suitably) *

ADD FILE

Time Commitment

- August-September 3-4 hours every week + meeting
- October-December - 5-6 hours/week
- Qualifier - January ~ 8-10 hours/week
- Feb - March End ~ 8-10 hours/week

FAQs?

Can I compete if I graduate this semester?

Yes. If you are registered in current team, they allow you to compete this season.

I don’t have that much experience in Cybersecurity, will I be a good fit?

We have talked to competing team members from other schools with Biotech and Electrical Engg. majors, as long as you are dedicated you can be good fit.

When does Red Team starts to attack/ begin?

Same time as you login

FAQs?

What tools Red Team uses?

Cobalt Strike, metasploit, etc.

What is strength of Red Team?

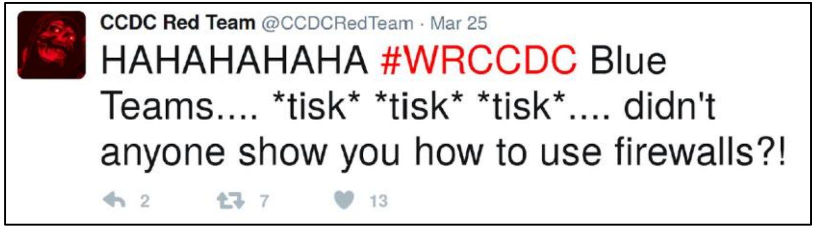
Regionals have 15 members with ~5-10 years of industrial experience.

Can we initially shut ourselves from external network and bring services up once we have secured everything - take some penalty at beginning and be safer in long run ?

They know you will try that - scoring engine penalty is twice as high initially

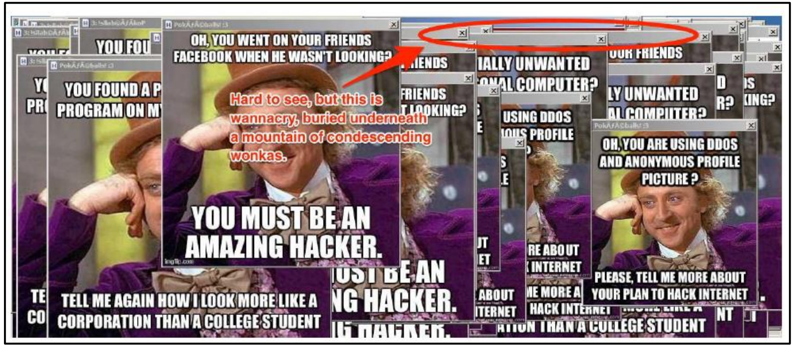
How do I know we have been hacked and it’s not a misconfiguration?

You will definitely know….!!!!



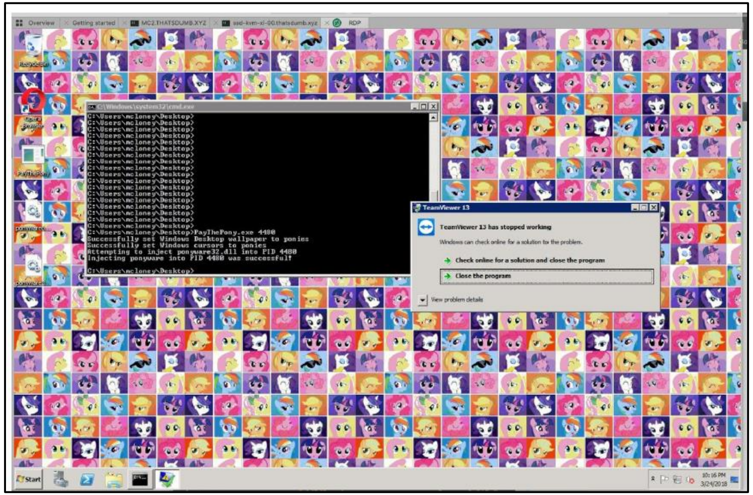
CCDC Red Team @CCDCRedTeam · Mar 25

HAHAHAHAHA #WRCCDC Blue Teams.... *tisk* *tisk* *tisk*.... didn't anyone show you how to use firewalls?!



OH, YOU WENT ON YOUR FRIENDS FACEBOOK WHEN HE WASN'T LOOKING?
YOU MUST BE AN AMAZING HACKER.
YOU FOUND A P… PROGRAM ON M…
TELL ME AGAIN HOW I LOOK MORE LIKE A CORPORATION THAN A COLLEGE STUDENT
OH, YOU ARE USING DDOS AND ANONYMOUS PROFILE PICTURE ?
PLEASE, TELL ME MORE ABOUT YOUR PLAN TO HACK INTERNET
…IALLY UNWANTED …ONAL COMPUTER?
imgflip.com

Hard to see, but this is wannacry, buried underneath a mountain of condescending wonkas.



```
C:\Windows\system32\cmd.exe
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>
C:\Users\mcloney\Desktop>PayThePony.exe 4480
Successfully set Windows Desktop wallpaper to ponies
Successfully set Windows cursors to ponies
Attempting to inject ponyware32.dll into PID 4480
Injecting ponyware into PID 4480 was successful!

C:\Users\mcloney\Desktop>
```

TeamViewer 13

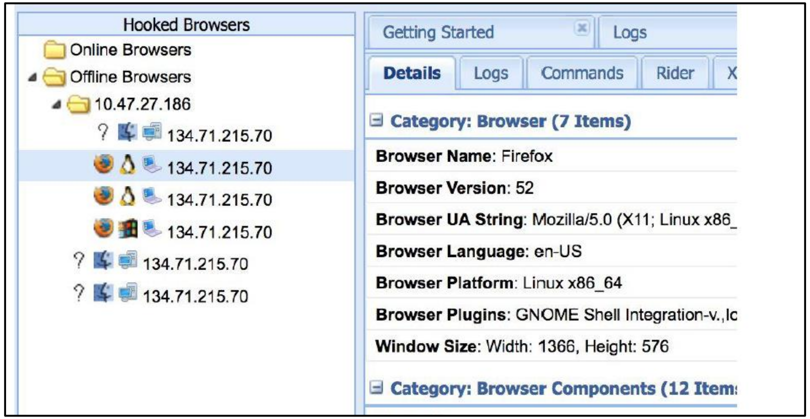
TeamViewer 13 has stopped working

Windows can check online for a solution to the problem.

→ Check online for a solution and close the program

→ Close the program

View problem details



Hooked Browsers

- Online Browsers
- Offline Browsers
  - 10.47.27.186
    - 134.71.215.70
    - 134.71.215.70
    - 134.71.215.70
    - 134.71.215.70
  - 134.71.215.70
  - 134.71.215.70

Category: Browser (7 Items)

Browser Name: Firefox

Browser Version: 52

Browser UA String: Mozilla/5.0 (X11; Linux x86_

Browser Language: en-US

Browser Platform: Linux x86_64

Browser Plugins: GNOME Shell Integration-v.,lc

Window Size: Width: 1366, Height: 576

Category: Browser Components (12 Item

Perks

- Chance to network with renowned industry professionals working as Red Team members, pen-testers in the Industry.
- Chance to interact with recruiters for Cybersecurity positions.
- Real world Blue teaming practice enhances your preparedness to respond to actual cyberattacks.
- WRCCDC trip is sponsored by ASU Center for Cybersecurity and Digital Forensics (CDF).
- Add CCDC experience to your Resume. Past team members found good positions in Cybersecurity Industry.

Raytheon
workday.
NSA
WHERE INTELLIGENCE GOES TO WORK
IntelligenceCareers.gov/NSA
CWW
cyberwatch west
paloalto NETWORKS
ISACA
Los Angeles Chapter
W
UNIVERSITY of WASHINGTON | BOTHELL
MASTER OF SCIENCE IN CYBER SECURITY ENGINEERING
COBALT STRIKE
IBM
AIR FORCE
CIVILIAN
SERVICE

Perks

WRCCDC 2018 Team

WRCCDC 2017 Team

WRCCDC ASU Alumni

2018 - Team

- Vaibhav Dixit - Software Engineer (Comcast) - Grad
- Chase Lybbert - Cybersecurity Analyst (McKesson) - Undergrad
- Jeffrey Moore - Security Engineer (McKesson) - Undergrad
- Michael O’Loughlin – Security Engineer (Honeywell) - Undergrad
- Jacob Loden - Sr. Pen Tester (Honeywell) - Undergrad

2017 - Team

- Tejas Khairnar - Security Engineer (Intuit) - Grad
- Emanuel Boderash - Security Application Engineer (AMEX) - Undergrad
- John Shaller - (Accenture) - Undergrad
- Nicholas Ton - Network Consulting Engineer (Cisco) - Undergrad
- Wil Gibbs - ASU Student, President: pwddevils - Undergrad
- Ngoc Nguyen - ?
- Daniel Martin - ?

Joining Requirements

- Meeting every Friday 4:15-5:15 pm in BYAC 110.
- Create an account on ThothLab: https://www.thothlab.com/
- Discord Channel : https://discord.gg/JFq44mJ.
- Bring your laptop.
- We are also starting a WRCCDC Capstone this fall, make a team, ask Capstone mentor about this, tell your friends…!!

References and Previous Documents

http://www.wrccdc.org/competition-overview

https://archive.wrccdc.org/

https://www.nationalccdc.org/

https://www.scribd.com/document/318192735/wrccdc-security-policy

http://nccdc.org/files/CCDCteamprepguide.pdf

https://en.wikipedia.org/wiki/National_Collegiate_Cyber_Defense_Competition