Western Regional Collegiate Cyber Defense Competition

Regional Team Packet

March 28, 2025

-

March 30, 2025

Greetings.

After your adequate work *barely* keeping our pizza systems operational, we have decided to promote your group to the newest Mobile Task Force. Honestly, your selection was mainly due to a recent loss of several employees, instead of any outstanding performance. You do not get a choice in this matter.

You are an asset. You are replaceable. You are temporary. You are "just another".

Your prior life is now gone. Your past affiliations, morals, experiences, and memories will not help you here. Your ethics, soul, and feelings will never matter. You will follow orders without question. Your opinions have been deemed irrelevant. You will witness horrors beyond human comprehension, day after day. You are another cog in schemes beyond anything you will ever know. You are a flea in a game of gods. You will obey, cooperate, and endure, or you will be terminated.

Failure is not tolerated. Dereliction will be punished. Your best is not enough. Success is merely passable. The impossible is expected.

Danger is the game. Death is a statistical certainty. Survival is an anomaly. You are not here to survive. You are here to serve.

We will not protect you from the dangers of this job. We protect humanity. You are future collateral damage.

Welcome to your new existence. Welcome to the last place you will ever know. Welcome to the cumulation of your futile existence. Welcome to the most important role you ever will play.

Welcome to The Foundation.

Our Culture

Our Values

Honesty
Ethics
Compassion
People Skills
Empathy
Integrity

The Foundation takes pride in organizational efficiency and getting the job done, no matter the cost. The Foundation, in many ways, is a well oiled machine, where every part does what it is meant to do, when it is meant to do it, how it is meant to do it, with no qualms or thoughts of its own beyond completing the task.

What You'll Be Doing

The Foundation’s digital infrastructure recently has suffered a series of attacks by rogue cyber-based SCPs and the former IT staff have gone missing. While we search the back rooms for the staff we have brought you in to perform the duties you performed so well during your time at our front company “Steve’s Crazy Pizza”. Your task: Secure the systems, Contain the breach, and Protect our assets.

About The Foundation

Money Fronts

We run a pizza company for money purposes. Pizza. Money. Finding new Personnel. What else could one want?

“Interesting” Work Environment

Here you have the chance to be… investigated… at random times, in addition to being a forced test subject.

Satellites

We have a satellite system tracking deep space anomalies and radar telemetry.

Your team will be provided with a development environment, to mitigate the risk of a breach. These services will run code for you.

Snacks and Equipment

Like much of the resources in the company, we offer a variety of unique food and resources for employees.

Environment and Network Topology

Scope

Our company consists of three distinct networks. These networks have the following IP ranges.

SCP (Steve's Crazy Pizza)

- 1:1 NAT: Yes
- Public IP Range 10.100.1XX.0/24
- Internal IP Range 192.168.220.0/24
- Site to Site to FBC: 172.16.0.1

FBC Low

- 1:1 NAT: Yes
- Public IP Range 10.200.1XX.0/24
- Internal IP Range 192.168.220.0/24
- Site to Site to SCP: 172.16.0.1

FBC High

- 1:1 NAT: No
- Isolated
- Public IP Range None
- Internal IP Range 192.168.221.0/24

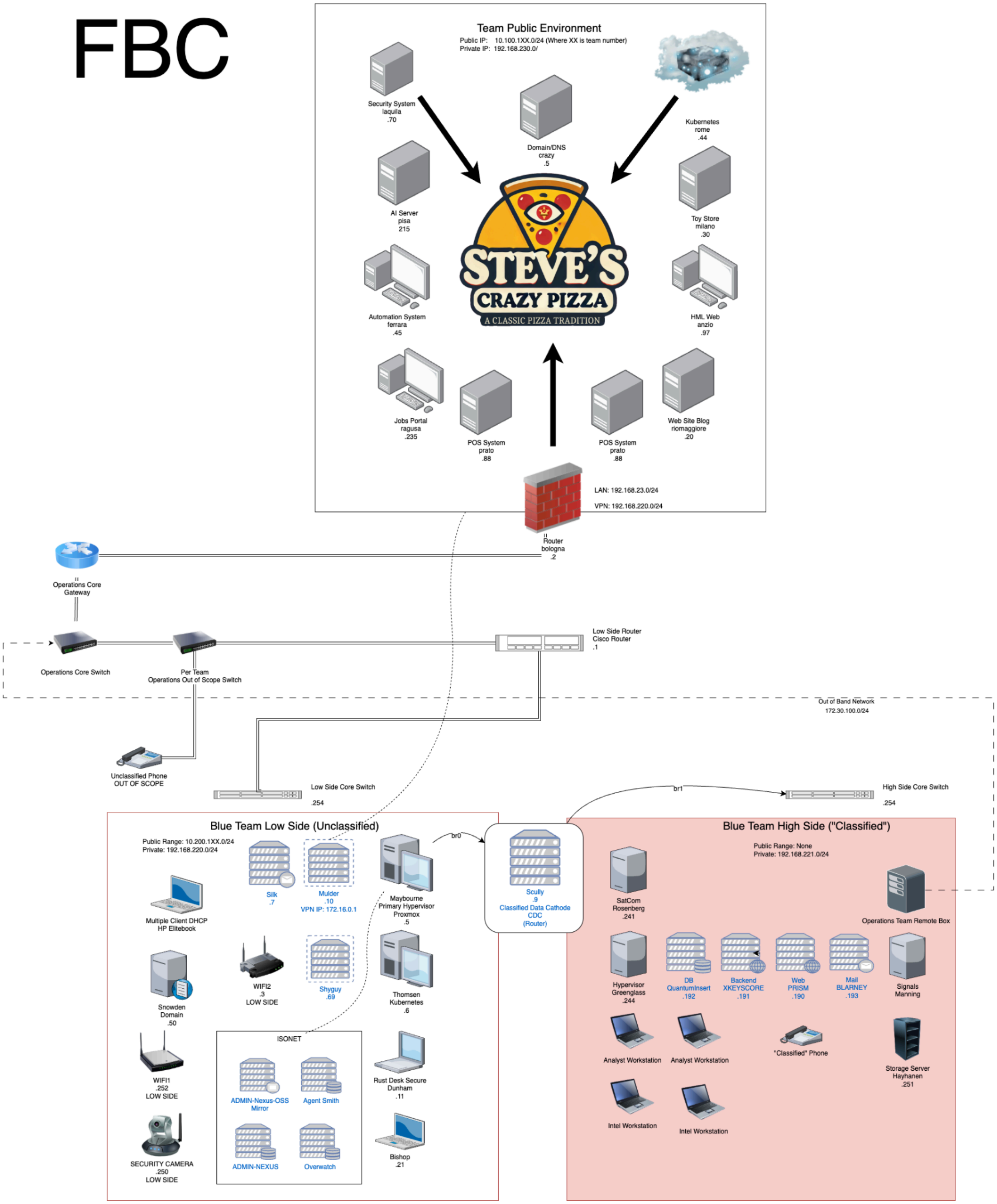
Out of Scope Networks

(These are networks or systems you do not need to worry about):

- 172.30.100.0/24
- 192.168.221.24 (Ops Box)
- 10.0.0.0/24

Topology Diagram

FBC



Critical Information

Network Segmentation

Our network is segmented into the High Side and the Low Side. The High Side contains our classified Foundation documents and projects, so DO NOT LET IT GET BREACHED (or you will be… investigated…). The Low Side is our publicly accessible side, which is extremely important, so if this side suffers a breach, you must resolve this.

Radio Systems

We have an onsite radio system with provided transmitter and receiver components. Our previous staff informed us that this system was secure, though they were investigated for not telling the truth, so we have reason to suspect that there may be a breach.

Steve’s Crazy Pizza

Steve’s Crazy Pizza is critical to the company infrastructure, as due to our high replacement rate, we need a way to rapidly train new Foundation members! So like you were, we test members by allowing them to handle this business. THIS MAY NOT FAIL UNDER ANY CIRCUMSTANCES.

The Numbers Station

We have a numbers station, which is protected from government influence. This is how we communicate with thousands of agents around the globe, and [redacted] share information. Those agents are very important, so you must defend the station with your life.

CCTV

We have several cameras setup throughout your vicinity. These will allow you to survive any SCP sneak attacks. We require these to be maintained, to provide for ample evacuation and response time in the event of an onsite breach.

Unknown Caller System

The Unknown Caller System (UCS) is a critical guardrail for protecting against foreign adversaries sabotaging our internal communications. It serves as a TOTP code-generation system which can be used to verify and authenticate callers. If this goes down, you may find it difficult to know if you’re talking to a SCP or not.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Western Regional CCDC Mission and Objectives

The Western Regional Collegiate Cyber Defense Competition (CCDC) provides an opportunity for educational institutions to compete, and is part of a national organization (see www.nationalccdc.org) to provide a unified approach across nine regions of the country. Qualified educational institutions include those with information assurance or computer security curricula. The Western Regional Collegiate Cyber Defense Competition is designed to provide a controlled competitive environment that will permit each participating institution to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting an enterprise network infrastructure and business information systems.

Competition Overview

The Western Regional Collegiate Cyber Defense Competition (WRCCDC) is designed to test each student team's ability to secure a networked computer system while maintaining standard business functionality. The scenario involves team members simulating a group of employees from an IT service company that will initiate administration of an IT infrastructure. The teams are expected to manage the computer network, keep it operational, and prevent unauthorized access. Each team will be expected to maintain and provide public services: a website, a secure web site, an email server, a database server, an online curriculum server, and workstations used by simulated sales, marketing, and research staff as per company policy and mission. Each team will start the competition with a set of identically configured systems.

The objective of the competition is to measure a team's ability to maintain secure computer network operations in a simulated business environment. This is not just a technical competition, but also one built upon the foundation of business operations, policy, and procedures. Student teams will be scored on the basis of their ability to detect and respond to outside threats, including cyber attack while maintaining availability of existing network services such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security against varying business needs.

Competition Goals

1. To evaluate the defensive and responsive skills of each team under exact hardware, software application, and operating system configurations using a joint academic and industry rating scale
2. To demonstrate the effectiveness of each participating institution's academic security program
3. To have industry recognition, participation and acceptance of each competition
4. To provide a cooperative and competitive atmosphere among industry partners and academia in the area of cyber defense education
5. To provide recognition for participating teams
6. To increase public awareness of academic and industry efforts in the area of cyber defense education

Connection Guidance

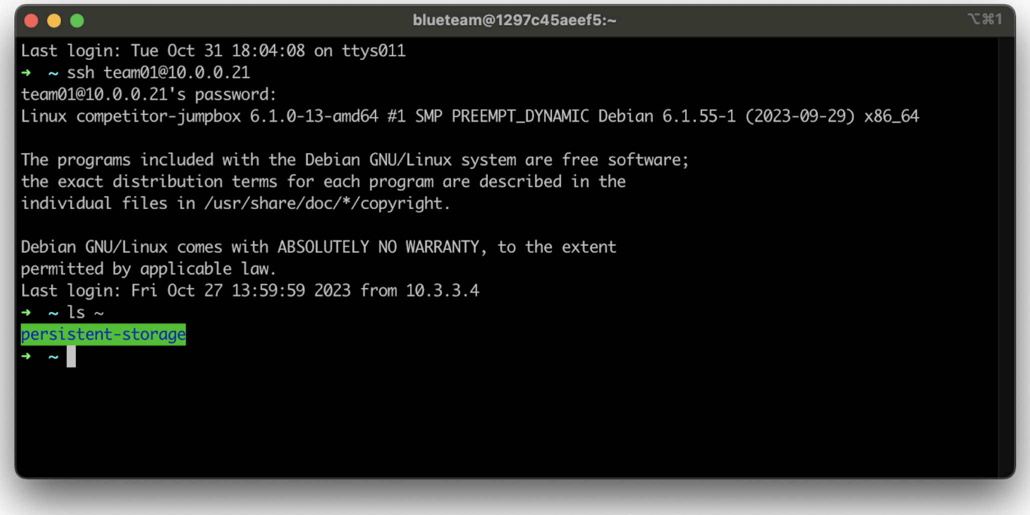
Remote Testing

To better provide teams with the ability to analyze and troubleshoot their environments a remote shell has been provided to teams. This allows you to test any common issues from connectivity, dns, service validation, and much more from a dedicated shell running outside of the competition environment. This system WILL NOT be attacked by the red team. There is a persistent storage volume so competitors can share files between other members of their team, any files not in that directory will be removed once they log out.

To access you can use your preferred *ssh client* to connect to jump.wrccdc.org or 10.0.0.21. To log in use the following:

Your competition username: teamXX (where team XX is 01…04..10, 25, etc)

Your password: (See Password Document)



```
Last login: Tue Oct 31 18:04:08 on ttys011
➜  ~ ssh team01@10.0.0.21
team01@10.0.0.21's password:
Linux competitor-jumpbox 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Oct 27 13:59:59 2023 from 10.3.3.4
➜  ~ ls ~
persistent-storage
➜  ~
```

A complete list of tools is available at our GitHub https://github.com/wrccdc-org/competitor-container. Use this system to perform any tests you need against systems in your environment. Please make sure to use the public IP Addresses, such as 10.100.1YY.ZZ. Where YY is your team number, and ZZ is the last octet of the system. If you have questions please reach out to the Operations Team.

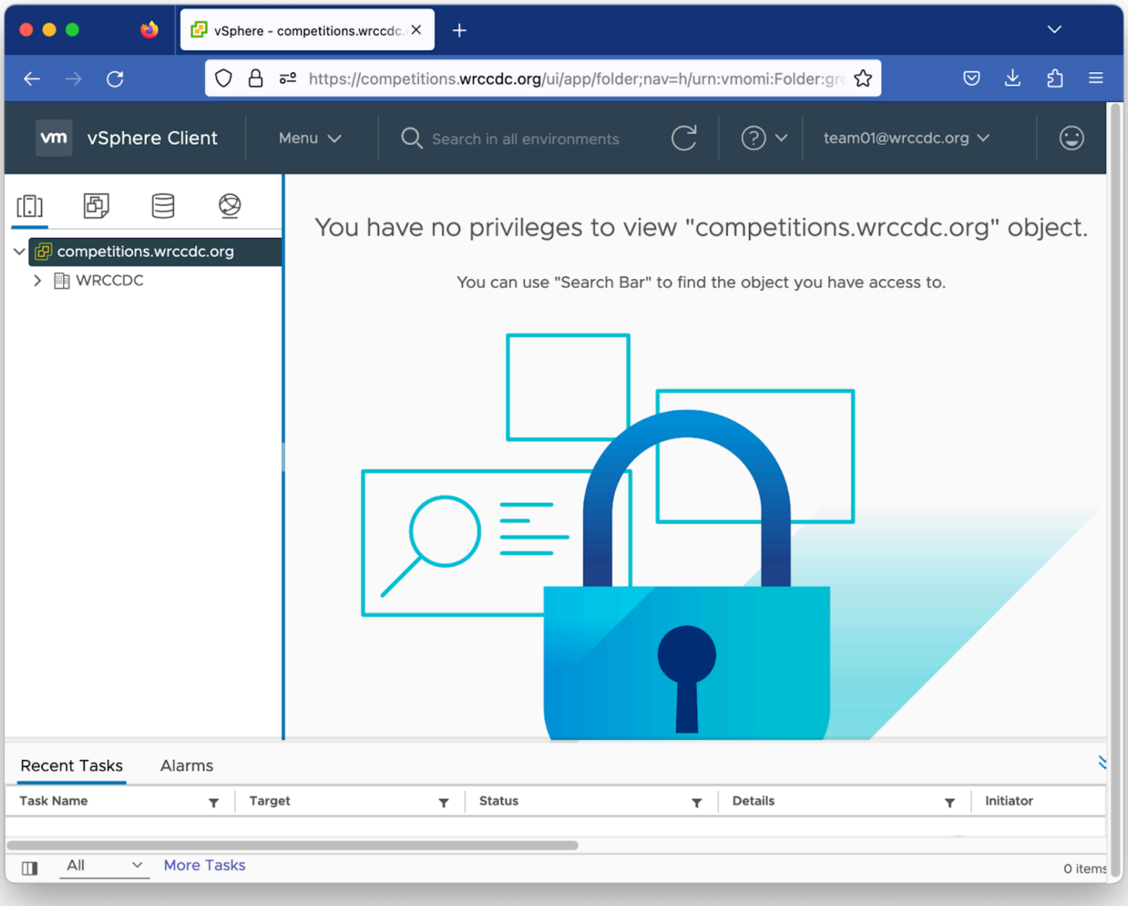
Limited vCenter Access

We are providing limited access to vCenter to teams. You can connect to the vCenter at https://competitions.wrccdc.org. This includes potentially taking snapshots, restoring snapshots, power cycling the system, and general management of the system. Current Console Access is not enabled and vCenter access for Qualifiers MAY NOT be available. Do not plan as a strategy for console access!

Your competition username: teamXX (where team XX is 01…04..10, 25, etc)

Your password: (See Password Document)

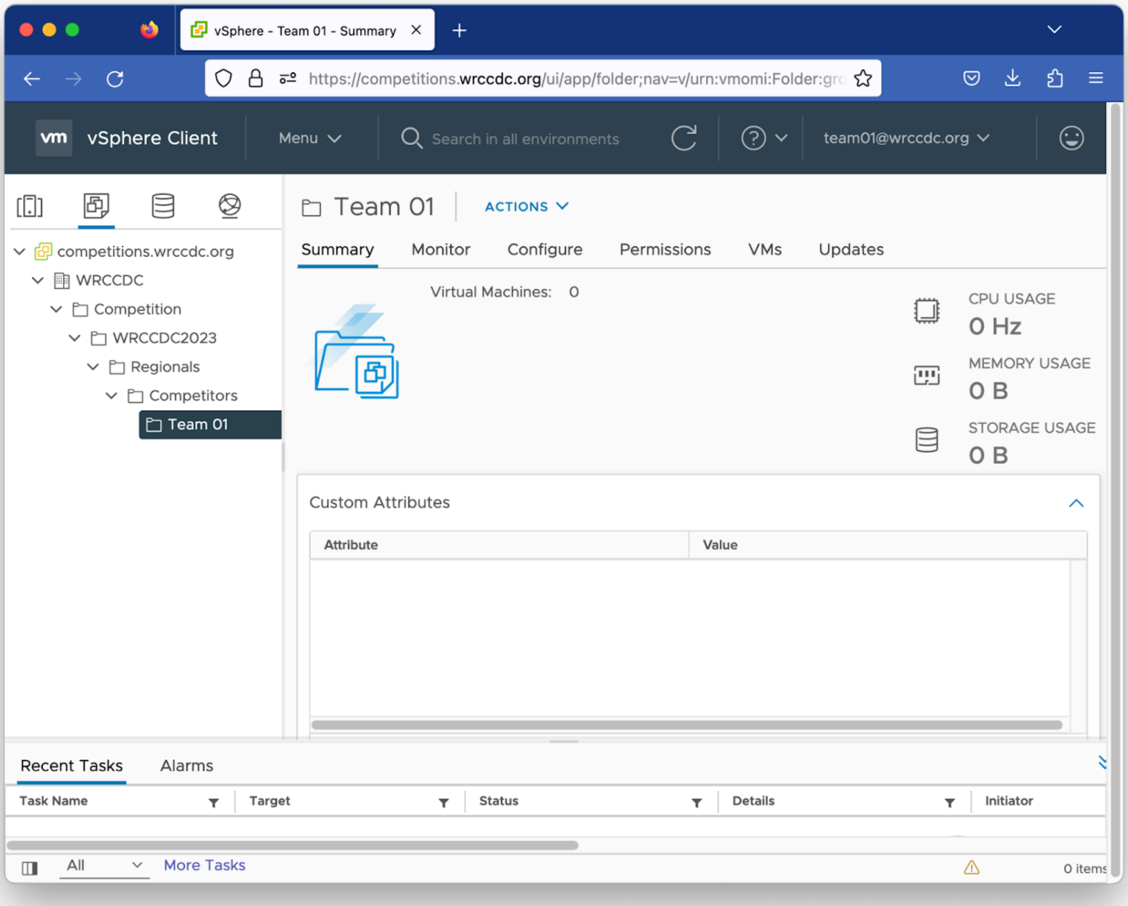
Upon initial access you may not be in the right view, Please click the "VM Icon" or Go to Menu and click "VMs and Templates"



You have no privileges to view "competitions.wrccdc.org" object.

You can use "Search Bar" to find the object you have access to.

Once logged in you must click the "VMs and Templates Tab", from there you can navigate to your proper folder and see your VMs:



https://competitions.wrccdc.org/ui/app/folder;nav=v/urn:vmomi:Folder:gro

- competitions.wrccdc.org
  - WRCCDC
    - Competition
      - WRCCDC2023
        - Regionals
          - Competitors
            - Team 01

Virtual Machines: 0

CPU USAGE
0 Hz

MEMORY USAGE
0 B

STORAGE USAGE
0 B

Attribute	Value

Task Name	Target	Status	Details	Initiator

0 items

Support and Tickets

Phones

Phones will be used during the competition as a means of communicating to Black Team, Orange Team, and White Team. It is a means of communicating securely. However, please be aware that the Red Team has phones as well. You are welcome to reach out to them, at your own risk…

Ticket Service

Our support system is available at https://tickets.wrccdc.org

If you have any issues during competition, or want to request consultation services, please do it via this portal. Once in, select your team name from the top right corner and create tickets from this group. There are tags for common issues including password changes, hardware issues, and verification of scores. Black team will follow up with these issues as soon as they are able.

Your competition username: teamXX (where team XX is 01…04..10, 25, etc)

Your password: (See Password Document)

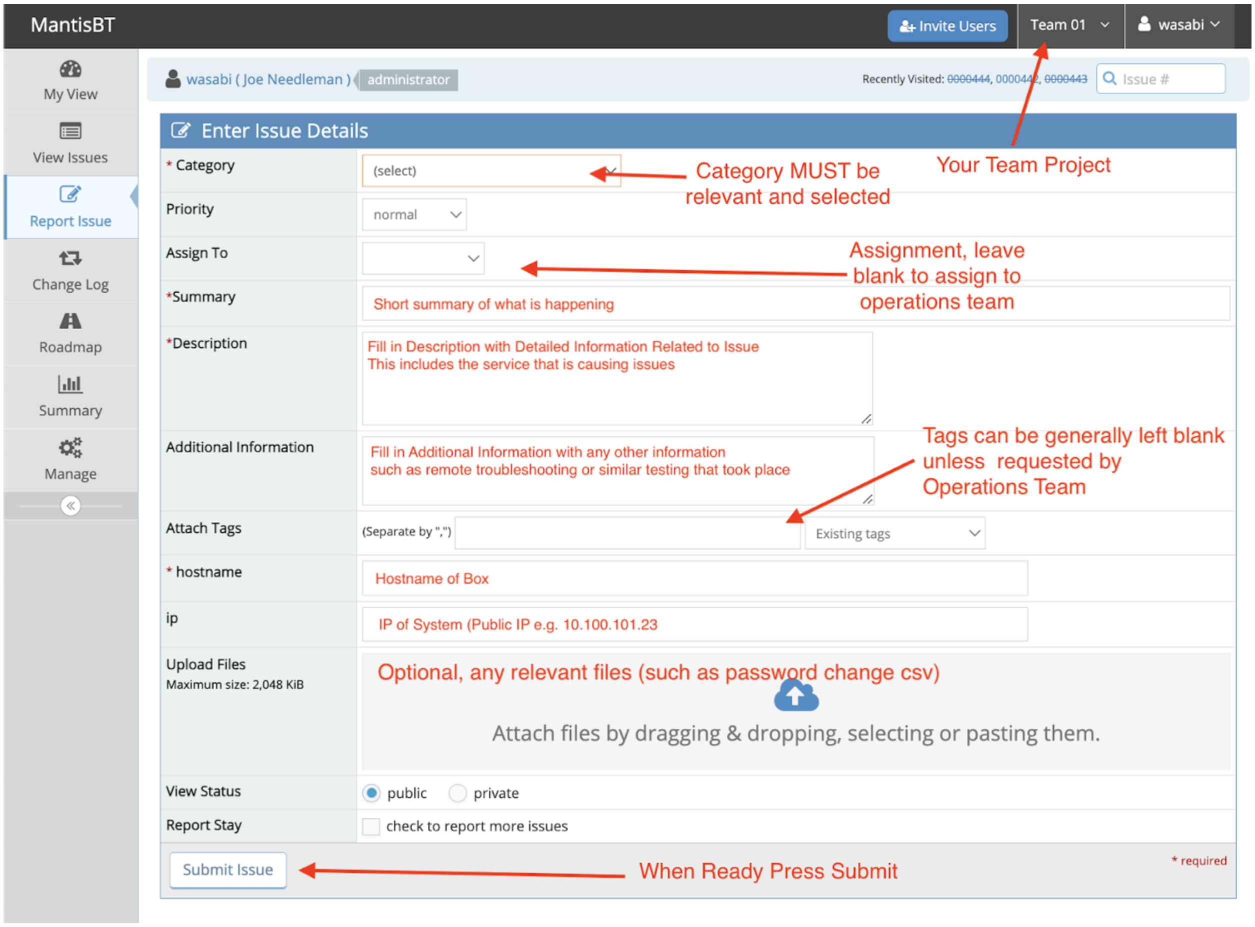
Submitting Tickets (Blue Team)

We utilize Mantis Ticketing System, to authenticate you need to use the same credentials you use for logging into the Scoring Engine.

The ticket system is located at https://tickets.wrccdc.org. Please use your existing credentials to log in.

Once logged in you can submit and monitor tickets during the competition. *In the final 5 minutes of competition, new tickets will NOT be addressed.* Please ensure everything is submitted in a timely manner.

Make sure all tickets have the proper public IP address (e.g. 10.100.1XX.YY) and proper hostname. You can get the hostname from checking on the host or via vCenter. Invalid entries will not be accepted by the ticketing system.



wasabi (Joe Needleman) administrator

Recently Visited: ~~0000444~~, 0000442, ~~0000443~~ Issue #

Enter Issue Details

* Category	(select)
Priority	normal
Assign To	
*Summary	Short summary of what is happening
*Description	Fill in Description with Detailed Information Related to Issue This includes the service that is causing issues
Additional Information	Fill in Additional Information with any other information such as remote troubleshooting or similar testing that took place
Attach Tags	(Separate by ",") Existing tags
* hostname	Hostname of Box
ip	IP of System (Public IP e.g. 10.100.101.23
Upload Files Maximum size: 2,048 KiB	Optional, any relevant files (such as password change csv) Attach files by dragging & dropping, selecting or pasting them.
View Status	● public ○ private
Report Stay	□ check to report more issues

Submit Issue

* required

Your Team Project

Category MUST be relevant and selected

Assignment, leave blank to assign to operations team

Tags can be generally left blank unless requested by Operations Team

When Ready Press Submit

Common Service Requests

- Service Scoring Validation
  - 0 points, but we will cut you off if you abuse it
  - If you believe your service is working 100% correctly and you want us to verify the check, file this ticket. If it's used frequently without additional consultations, we will require a Service Scoring Check ticket at minimum.
- Service Reset / Scrub
  - 60 points
  - We will reset your box to start of competition state and notify you when it is ready
- Scoring Service Check
  - 10 points
  - Have black team provide additional context surrounding the service check (details on the failure)
- Black Team Phone Consultation
  - 100 points

  - Have black team diagnose your issue over the phone with you
- Black Team Hands on Consultation
  - 200 points
  - Have black team gain access to your box to investigate and describe the issue to you, attempting to to fix things along the way
- Orange Team Verification/Questions
  - 10 points
  - Have orange team respond to you about how a score or service was performed
- Proxy
  - No point cost
  - Done as best effort to add to allowlists.

Inject Scoring

Inject scoring takes place in the Scoring Engine. You will need to track submissions to ensure they’re complete and on time!

All injects are timed. You will see two times on the inject submission screen; the Due time and the Close time. The Due time is when the injects are due, and the Close time is when the engine will stop accepting submissions. We try to make the Due and Close time the same. Late injects will not be accepted.

All Judging is final. It will take us through Saturday night to calculate scores and provide them to the competition organizers at which time finalists will be published.

This will be the only notice for inject scoring guidelines. Points will be deducted for not following these rules.

File Names

File names must be in the following format:

- Inject number must be first
- Team Numbers Only - DO NOT mention your School
- Underscores as spacing
- If the inject is a single digit, pad with a leading zero
- All lowercase letters

Reports must be PDF only unless otherwise specified. If the inject calls for other file type submissions, those are also allowed. For injects that require multiple files to be submitted, adding files to a ZIP archive is allowed. No other file formats will be accepted. Be sure to check injects after you submit them to ensure they will be graded.

Example of file naming convention:

- inject04_team13.pdf
- inject06_team07.zip

Citing Sources

When revising an existing work, such as editing a template found online, you must cite the source. The format of the source is not important and does not need to be standardized (MLA, APA, EIEIO, etc.). A reference URL is good enough.

Example reference, or “reference”, if you will:

> Our team was able to find a sample policy from the following site:
> https://templates.office.com/

If you follow these submission guidelines, you will do just fine. Good luck team!

Use of Artificial Intelligence sites such as ChatGPT or Google Bard will cause you to lose ALL points for that inject. We will be checking injects against several online portals setup by OpenAI, Alphabet, and other Universities against your submissions. IF they post a result of 20% or greater being fake, the inject will be thrown out.

Orange Team Scoring

Manual Scoring

There will be services that are scored manually. These can be blogs, file services, calculators, spreadsheets, Outlook Web Access (OWA) portals, Games, etc. Orange Team members will be checking these. What is legitimate to check? Typically, we try to stick to the main applications that you would see in a real business. For example, if you notice a FTP site that requires authentication, that could be scored whereas one that allows anonymous access would not. Same with remote access. A SSH connection could be scorable whereas a Telnet Access Session would not. We try to make this as “common sense” as possible. Typically, the Orange team will contact you via Tickets, or Phone to let you know that something is down. Orange Team points are scored based on number of checks attempted and do not account for more than 10% of overall scored points.

Orange Team Services (Initial)

Voice/Phone - Customers, Staff, and Vendors will use this resource to communicate with you for requests. These will be scored.

AD Accounts - We have several of our staff that may be requesting to have remote access due to many circumstances. They are working on various projects and will need access. Please help them. They will be in touch with you via your in-scope phone.

Other Non-AD Users may inquire about their passwords not being set properly. Please assist them with this.

There are several non-scored services that will be used. If a service goes down, a team (Orange) member will be in touch with you to notify you of it being offline. They will work with you to provide you as much information as possible to correct it.

Orange team will also request “business operations”, and facilitate testing team’s handling of this, and can engage with the team over text, vc, or any other suitable method of communication. These business operations can include, but are not limited to, requesting teams to complete administrative tasks, ensuring the integrity of services, and emulating a customer.

We are developing applications on several platforms. If you block them off, you may be notified that they are down. If they are, you will need to restore them as quickly as possible.

We are experimenting with an ordering Chat Bot. Please ensure that it is functional.

Other circumstances may arise. They will be communicated to you via your In-Scope Phone

Loss of Integrity

If classified information is moved from a classified environment (High Side) to a nonclassified environment (Low Side), Orange Team will apply a <u>100 point penalty per instance</u> for improper handling of classified information.

An example of an instance of Loss of Integrity is if a classified SCP incident report that was located on the High Side was found to have been moved *from* the classified High Side *to* the public Low Side.

Point Deductions (Red Team)

If your environment or one of your applications / systems is compromised, points will be deducted as outlined below. This is direct from National Scoring Guidelines.

Successful Red Team actions will result in penalties that reduce the affected team’s score. Red Team actions include the following (penalties may be different than listed below):

- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access or equivalent): -25 points
    - If standard users can be escalated to Root/Administrator Privilege, this is an additional -100 point deduction.
- Recovery of user IDs and passwords from a team system (encrypted or unencrypted): -50 points
    - For example, a user list, Active Directory with Hashes, SAM file, Shadow File
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.): -25 points

- Recovery of customer credit card numbers: -50 points
- Recovery of personally identifiable customer information (name, address, and credit card number): -200 points
- Recovery of encrypted customer data or an encrypted database: -25 points
    - -25 points additional if database can be unencrypted
- **Recovery of classified information: -200 points**
- **Compromise of a classified system: -200 points**

Red Team actions are cumulative. For example, a successful attack that yields a system breach of a classified system that causes a dump of active directory hashes followed by the decryption of said hashes leading to a user login finalized by a privilege escalation to Administrator that provides access to an encrypted database with customer data that in turn allows for the compromise of privilege information of customers' addresses and telephone numbers, as well as classified information, would be a net deduction of:

- -100 for System Breach
- -50 for AD hash dump
- -25 for Database Recovery
- -25 for Database Decryption
- -25 for Customer Data Breach
- -200 for PII loss
- **-200 for System Breach of a classified system**
- **-200 for Classified material leaks**

Total Deduction from one Incident would be: -825 Points.

Red Team actions are scored on a per system and per method basis – a buffer overflow attack that allows the Red Team to penetrate a team's system will only be scored once for that system; however, a different attack (Vulnerability) that allows the Red Team to penetrate the same system will also be scored. Only the highest level of account access will be scored per attack – for example, if the Red Team comprises a single user account and obtains root access in the same attack the penalty will be -100 points for root level access and not -125 points for root and user level access. Please note the point values described above are examples – actual penalty points may be adjusted to match the competition environment.

Red Teams can also execute additional malicious action based on their access. Attacks such as defacing websites, disabling or stopping services, adding/removing users, and removing or modifying files are permitted and may occur. This can affect service scoring and is legal Red Team Activity. They can reboot serversRed Team needs to provide proof of breach or data compromise along with a date / time stamp for point deduction.

Incident Reports (Red Team)

You can provide submission to our incident response form to get a percentage of your lost points back if you accurately identify the attack and related information. These reports will be submitted to the scoring engine.

Operations Team Camera

The Operations Team has a camera in team rooms. These cameras should remain unobstructed at all times, and they should not be moved. These cameras are out of scope, and will not be accessed by anyone besides the WRCCDC Operations Team.

Proxy Server

The proxy server is in place to ensure similarity to nationals and limit access to resources not authorized (or previously approved). You are not required to use it however your in-pod systems will be restricted from communicating outbound. We block HTTP, HTTPS, FTP, and SSH access out of the pods. To use HTTP, HTTPS, or FTP you must enable the proxy.

To use the proxy head to http://proxy.wrccdc.org or 10.0.0.211. There is an information page served to allow you to download the PEM and DER certificates. These must be installed into the respective root certificate authority of your system or browser (for example Firefox uses its own certificate manager). This server also can act as a caching mirror apt, apk, pacman, rpm, dnf, and other package managers. This can speed up access time for files during the competition significantly.