Stream Stream

The Best Streaming Under One Brook

Welcome to the best streaming service startup! We here at Stream Stream look forward to working with you for the following engagement. We have had some troubles with our security processes and technology so we are sure glad you accepted our offer!

We offer both audio and video streaming services for our clients to leverage our private cloud and deliver their products and messages to their clients. This way, the stream keeps moving down stream.

Our flagship service is the video streaming service that we are constantly developing for our clients. It ***is not*** 100% made for prime time, but it is at least 45% ready for late night. (Really, Really, Really, Late night. I'm talking like 3:45 AM Late Night…)

Most of this is because of our development team. They are very special but a little ill educated on the software security practice side of things. The same thing can be said of our previous IT Manager. He recently quit and was not too happy when we didn't give him his last check. (On time that is. We did pay him…. Eventually…..)

But HEY we are so happy you joined us!

Welcome!

We're excited to have you with us. We think you'll be a great addition to our team. Remember, here at Stream Stream, "YOU" (AND EVERYONE ELSE!) are special! We love all of our employees and want to get the very most out of them. We have a lot of upcoming projects that we need your help with around our infrastructure, data, and software security. We know that you will be the best at what you do and slide into things quickly. Our systems are pretty easy to use and should be very familiar to you from a fundamental standpoint. However, we do have some "customized" services that you may need to quickly familiarize yourself with in order to keep them in operation. Operations are very important to our customers and Stream Stream. We can't have any of our key services down from more than 12 to 24 minutes. If that happens, our customers / clients get really frustrated. When they get frustrated, the streams stop. What happens when a stream stops? Well, stuff gets backed up. That's not good at all. So, PLEASE DON'T LET THE STREAM GET BACKED UP!!!

Remember, it isn't just about making money, it's about the end user experience for our clients to make money. If the client(s) make money, we make money! When we make money, we can feed the bears and EVERYONE is happy!

Job Perks

We offer a really competitive workplace including:

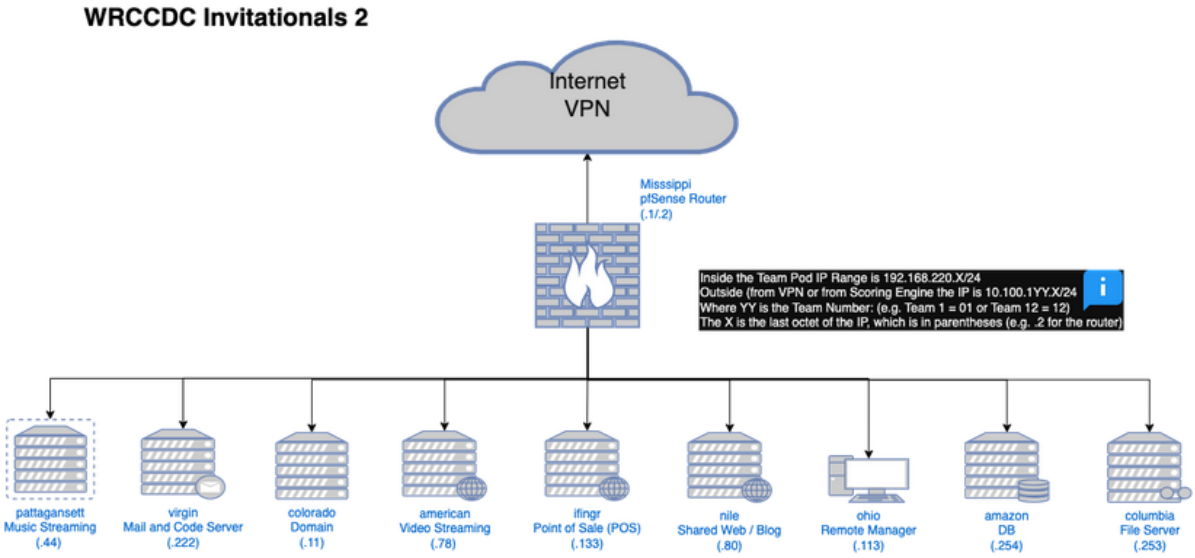
- Weekly Pick Nick by the River
- Tree Trimming services
- Outdoor FoosBall Tables
- Bears
- Financially supported by client perks with 15% of YOUR retainer! (Yay!)
- Plenty of outdoor standing desks are usable rain or shine! (WIth views of the Bears!)
- A great camp-site culture
- Bears,
- Legal Services for Contractors (Following signing of NDA)
- Maintaining an environmentally friendly environment.
- Bears
- Service Branches in Exotic, Outdoor Environments
- Next to Unreachable Locations! (Anyone a Pilot?)
- Bears (With Racoons!)
- Team Building! (With Bears)

Services and Scoring

Services

We do have customers, and we want to make sure they can access our services to support their streaming services to include uploads and downloads. We also offer other services such as online blogs to solicit client feedback. We have some traditional IT services as well as software support services that you would find in any modern-day business. Please note that the below diagram may not include ALL devices. We really hope that you can do some scanning stuff to find the rest of our infrastructure that may have become lost.

Topology



ID	IP	Name	OS	Purpose / Service(s)	
1	.2 Out .1 In .3 as well	mississipi	OPNsense		
2	.44	DragonFly	BSD		
3	.11	colorado	Win Svr 2022		
4	.133	ifingr	Centos 8		
5	..222	virgin	Win Svr. 2019		
6	.113	ohio	Arch Linux		
7	.78	american	Win. Vista		
8	.254	amazon	Alpine 3.10.9		
9	.80	nile	Ubuntu 22.04		
10	.253	columbia	Debian 10		

*NOTE: There may be other servers and services. I would do an inventory once you login…

Common Protocols

RDP	SSH
SNMP	SMTP
IMAP	POP3
VNC	OpenVPN
HTTP/HTTPS	Telnet
DNS	NFS
SMB	FTP

Scoring Instructions

Services will be scored with Service Level Agreements. Eighteen (18) services will be scored across most servers every 2-4 minutes. SLAs will be enforced after 6 unsuccessful attempts and every 6 additional attempts thereforward. SLA violations will cost teams 20 points each occurrence.

Routers

In years past, the Ops Team offered to administrate the head-end router of the Blue Team Pod. Unfortunately, this year we will not have the resources to do this. Blue Teams MUST administer this device. It is “in play” for the Red Team to compromise. If you know OPNsense, GREAT!! If you don’t, I would learn it FAST!!!

This means you have complete autonomy over your firewall. I HIGHLY suggest that you tread carefully with this device as if you lock yourself out, or block off your access (Or WORSE – BLOCK ACCESS TO THE SCORING ENGINE!!!) It will be a very long day indeed!!! There are three (3) NAT rules in the firewall by default.

Your services will be subject to going down if this device is misconfigured. Box Resets for this PFsense router / firewall will be an automatic -100 point deduction per reset.

Please keep in mind that you will have the 1:1 NAT in place, so when you connect to a system on 10.100.1XX.Y you will actually be connecting to 192.168.220.Y. For example, 10.100.102.10

translates to 192.168.220.10 from outside the PFsense device and ONLY the outside of the device. Put simply, you better know how NAT / PAT works!

If you run into trouble with the OPNsense Router, after filing out a ticket, please keep in mind the following:

- Cutover periods are every 30 minutes (e.g. 10:00 or 10:30 etc) This includes resets!
- A credential will be provided in the ticket to you that will let you administer the router completely
- You are allowed to change or delete or disable the “admin” user. Be careful with this! If you forget the password and delete the admin, you are looking at a box reset.
- We install an SSH key for remote-management, you can remove it if you want. However it is only used by the Operations Team. If you remove it and we cannot log in,you are looking at a box reset.
- It is recommended that you do not disable syslog or WAN firewall configuration access so that you can get data / administrate from the outside of the firewall, but that is up to each individual team to decide as the RED TEAM will also have access…

Resets and tickets will be provided on team-managed routers, and costs will be defined below. However if we lose access, a reset will take place.

*NOTE: There may be other servers and services. I would do an inventory once you login…

Service Locations (Critical Services):

Service Name	Last Oct	Scoring Protocol
pattagansett	.44	HTTP
Colorado	.11	DNS
Colorado	.11	SSH
Ifingr	.133	HTTP
Virgin	.222	GIT
virgin	.222	POP3
virgin	.222	SMTP
virgin	.222	SSH
ohio	.113	HTTP
ohio	.113	DNS
ohio	.113	HTTPS
ohio	.113	MESH
ohio	.113	SSH
American	.78	HLS
Amazon	.254	SSH
Nile	.80	WP
Columbia	.253	DNS
Columbia	.253	FTP

Connection Guidance

Teams will receive PAN Global Protect credentials for VPN access. Each team member will access the VPN with only one end device. Your device count is capped at 9 devices. This connection will serve as your starting point for ALL of your players. You basically will share the network (Via separate desktops / terminals.) Don't worry, it is powerful enough to support your activities for the day of the competition. You no longer need to supply your IPv4 addresses. We will monitor the number of addresses and connections into the environment. PAN Global Protect collects system fingerprint information to help us identify each student (or connect).

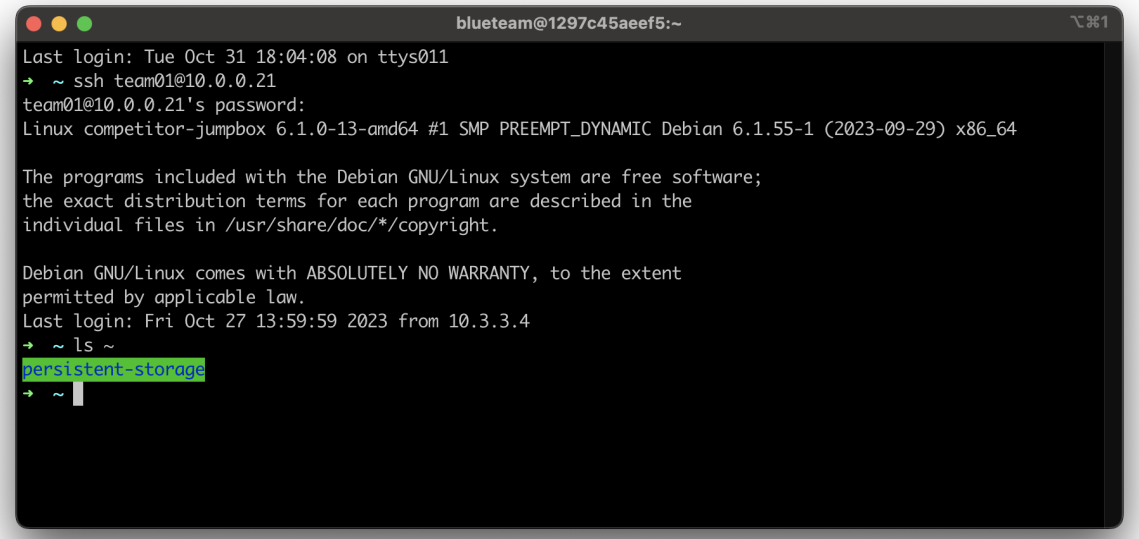
To help try to clarify, each competitor will have an account. ONLY one account can be used at a time. Each Team gets 9 accounts (8 Team Members and 1 Coach). Once in this network, they can reach their IP addresses relating to their pod via the connection. This will happen promptly at 9AM and you will have access onto the 192.168.220.0./ 24 network. This IP address range accepts credentials via SSH, VNC, Telnet, and Remote Desktop depending on device (See Table Above).

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)



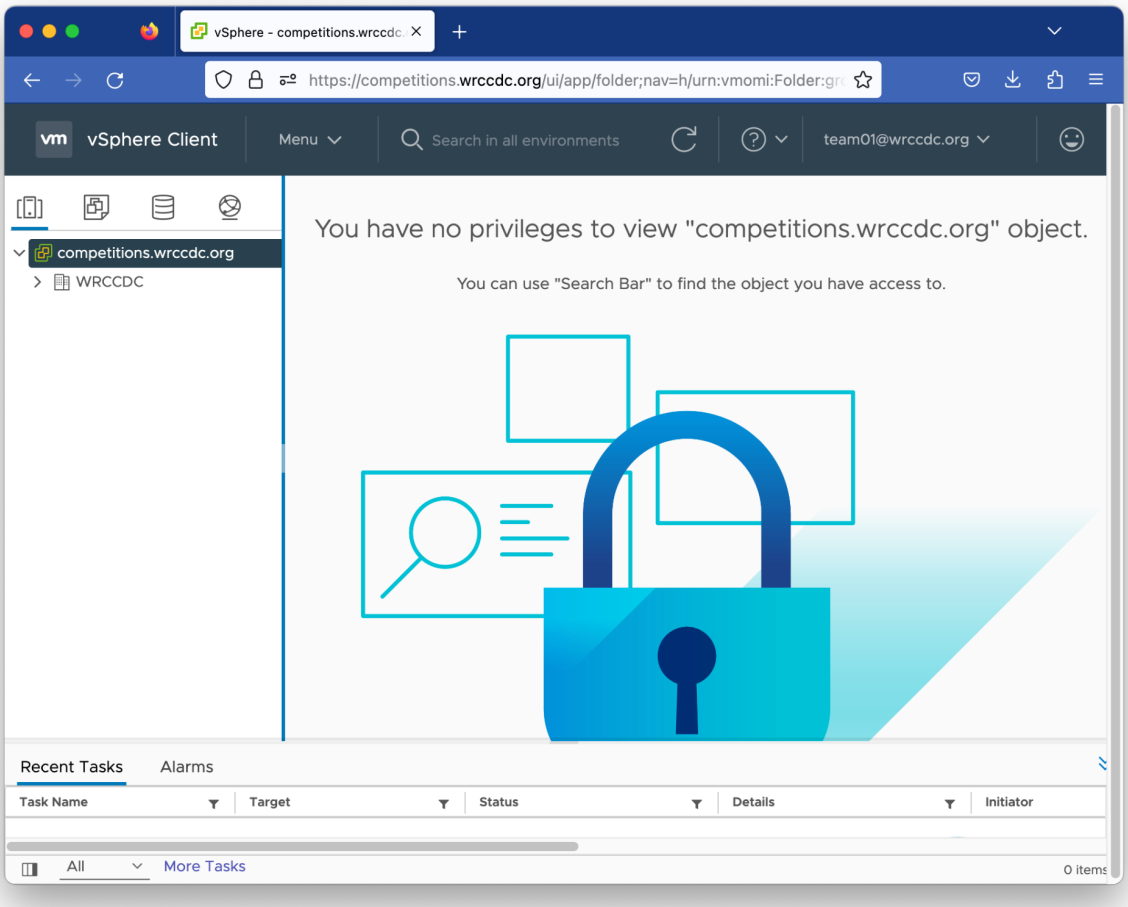
A complete list of tools is available at our GitHub https://github.com/wrccdc-org/competitor-container. Use this system to perform any tests you need against systems in your environment. Please make sure to use the public IP Addresses, such as 10.100.1YY.ZZ. Where YY is your team number, and ZZ is the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

Limited vCenter Access

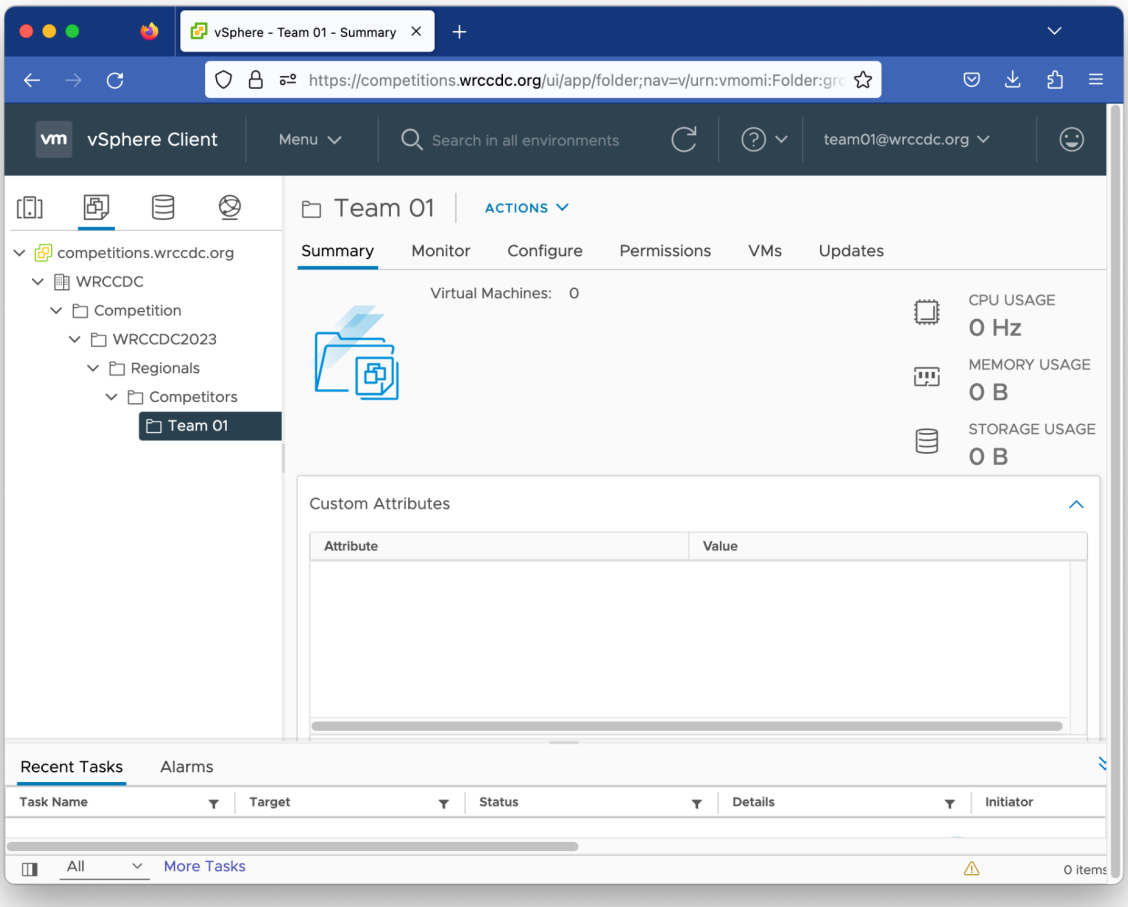
We are providing limited access to vCenter to teams. You can connect to the vCenter at https://competitions.wrccdc.org. This includes potentially taking snapshots, restoring snapshots, power cycling the system, and general management of the system. **Current Console Access is not enabled and vCenter 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”



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



Support and Tickets

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)

Discord

Discord may be used during the competition as a means of communicating to Black Team, Orange Team, and White Team. It is a means of communicating between your team securely and an easy way to share files to your team and competition organizers. You will not be required to leave after the competition, and you may use this Discord server to freely chat between schools and teams and participate in other events we have. Your team will be unassigned from you after the competition.

As part of this packet (or sent separately at the same time) you will have been given thirteen tokens (Up to 12 Team Members, including alternates and 1 for the team's coach. These may be used to register you into your team role in the competition discord.

Steps to Join and Setup Discord:

1. Join Discord using a personal account or one generated for the competition provided by the organizers.
2. Read the instructions in #welcome.
3. Set your role using !usekey in #role-selector
4. Begin using your team channel
5. You are joined!

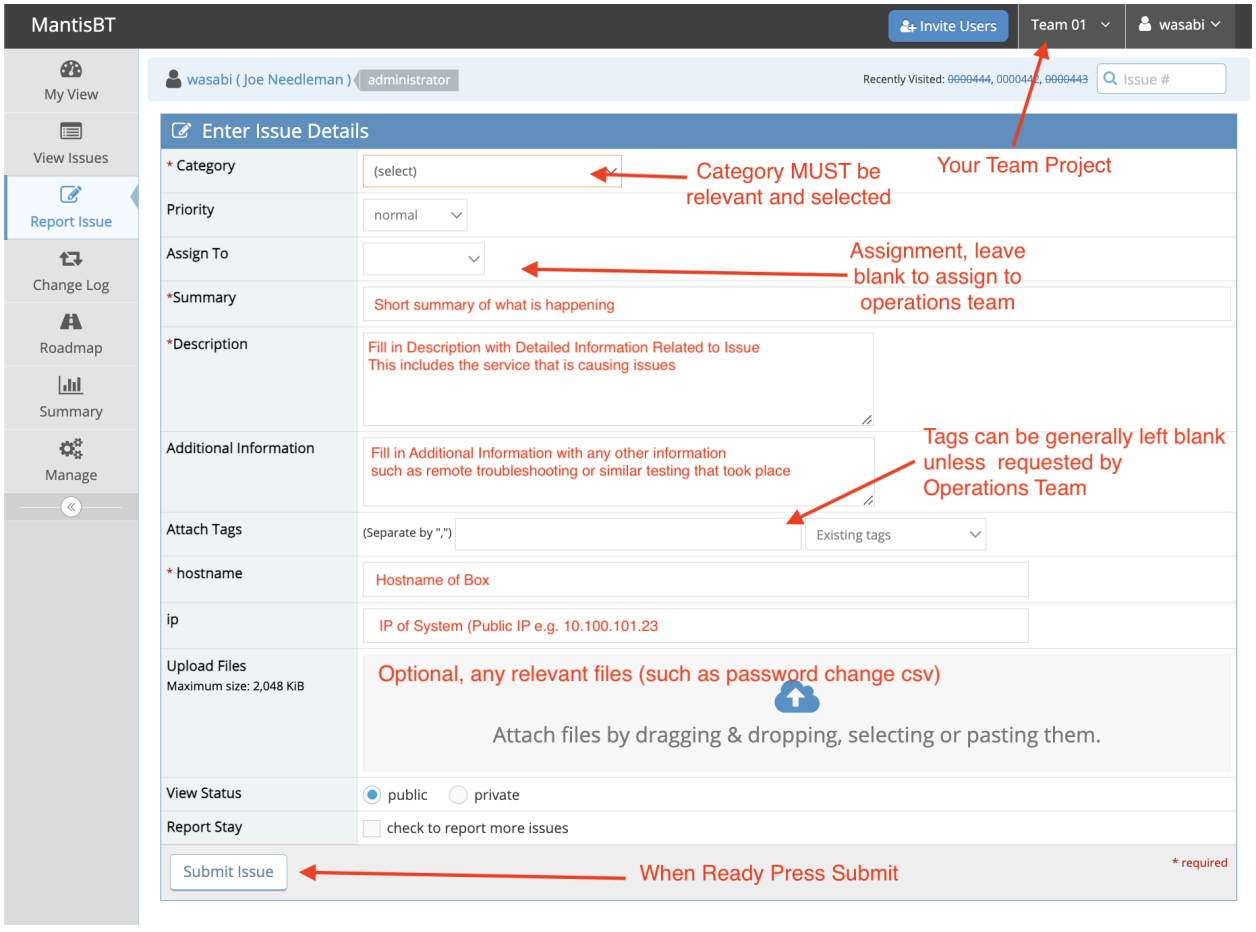
Submitting Tickets (Blue Team)

We utilize Mantis Ticketing System, to authenticate you need to use the same credentials you use for logging into Global Protect and vCenter. You can be on VPN and off VPN to access tickets.

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.



Common Service Requests

- Service Scoring Validation
  - 0 points, but we'll 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

Inject Scoring

Inject Scoring Engine

Injects will be distributed, returned, and scored in a single application. This application known as the inject scoring engine will be available at the onset of the competition. WRCCDC staff will distribute credentials via email/discord either the evening before or the morning of the competition. The first inject will be available at the start time of the competition.

Injects are scored based on complexity of the tasks required. They are given a time period for completion and have a rubric for scoring. One judge will be assigned per inject for scoring so as to level any inconsistency with scoring a single inject. There will be several judges assigned to injects over the course of a competition.

The URL for the Inject Scoring Engine (ISE) is:

https://ise.wrccdc.org

You will receive credentials prior to the competition.

Once logged in, you will find injects there. Additionally, we will push any announcements through this application.

Injects will be scored based on criteria given in the inject. As mentioned before, rubrics will be leveraged to level scoring. Not all injects will be weighted the same. Examples are below:

As you can see, there will be a very wide range of scoring across all injects based on complexity. Please note, the “or” indicates a range of values, for example 0 through 25.

All injects are timed. They will show their completion time in ISE. There will also be a “Reject” Time. The “Reject” time will be the time at which submissions will no longer be accepted. We try to make the reject and completion time the same. Late injects will not be accepted.

All Judging is final. It will take us about a day or two to calculate scores and provide them to the competition organizers at which time finalists will be published. It is our intent to share the scoring rubrics to their teams. Teams will not receive other teams rubrics.

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

File types must be PDF only. No other file formats will be accepted.

Example of file naming convention:

- inject04_team13.pdf

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.

Manual Scoring (Orange Team)

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 a 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 Discord Chat (if available) 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)

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

Discord Printer - This service may not be working at the onset. However, you may get instructions to stand it up. (via an inject)

AD Accounts - We have an outside contractor who is helping us out with an external audit. His name is Pedro and he may need an account created. Instructions on this will be forthcoming. His account needs access to many different services and needs to be available to him all day.

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

There is a company BLOG server on .80. Ensure that it remains functional. I.E. you can BLOG to it and others can respond to posted BLOGs.

There is a “streaming audio”WiKi server on .44. In addition to it remaining up, ensure that users can create, maintain, and modify content.

Other circumstances may arise. They will be communicated to you via Discord Voice.

*NOTE - RED TEAM does not have access to your Discord Server. They will not impersonate the Orange Team during this competition. They will not be able to use the DISCORD Printer either.

If you interact with the Red Team, it will be on your VMs that you are managing ONLY!

Point Deductions (Red Team)

If in case 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

Red Team actions are cumulative. For example, a successful attack that yields a system breach 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 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 Points for PII loss

Total Deduction from one Incident would be: -425 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 compromises 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 servers (Except the PFsense). PFsense is in play for compromise and locking out Blue Teams, but RED team is prohibited from stopping, rebooting, or changing configurations (I.E. ACLs).

Red Team needs to provide proof of breach or data compromise along with a date / time stamp for point deduction.

Remote Site Judges

There are NO Remote Site Judge Requirements for this Invitational Competition.