

Clownville, USA

We are an MSSP run by a bunch of clowns! We think that everyone needs to have more fun in their work, so we bring that by making sure to bring the excitement! We are clown owned and clown operated, so every one of our customers knows they're in for a good time!

Welcome!

We're excited to have you with us. We think you'll be a great fit with the rest of us clowns here, and are excited to see you bring more fun to the network! Our computers should be very friendly and easy for anyone to use.

Job Perks

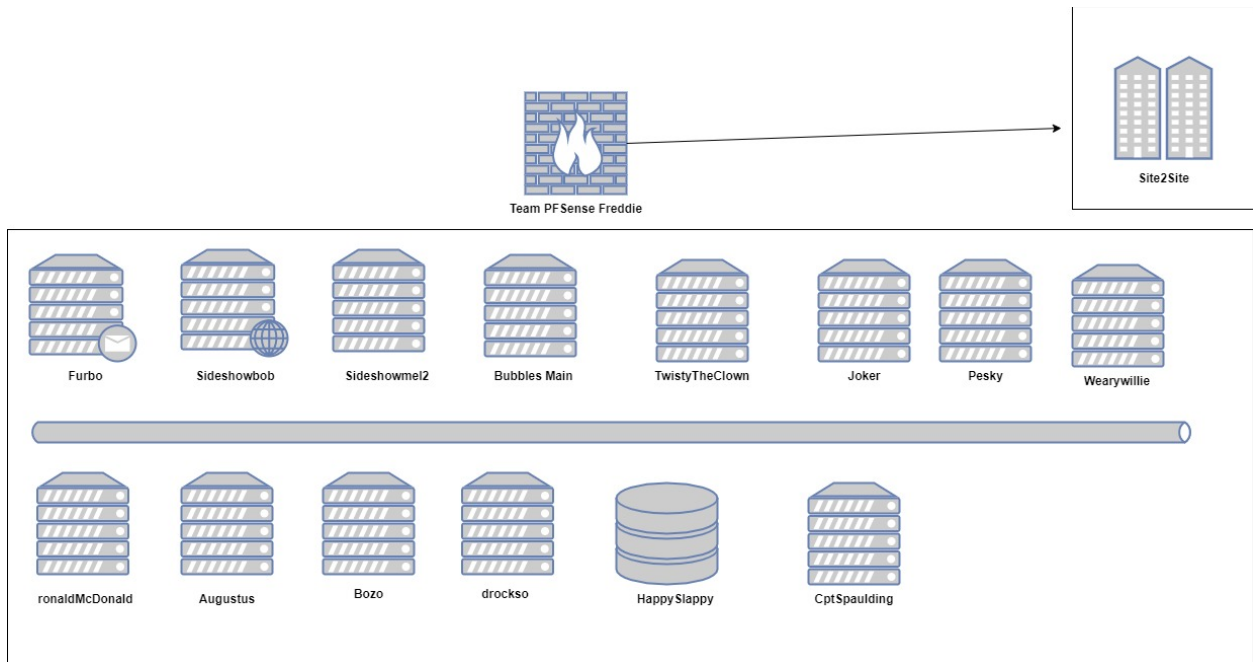
We offer a really competitive workplace including:

- Weekly office hours
- Dunk tanks
- Free face paint
- Extra large shoes

Services and Scoring

Known Services

We do have customers, and we want to make sure they can have lots of fun, so please make sure all of these things continue to work!



Common Protocols

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

Scoring Instructions

|||||

Routers

Due to the remote nature of this year, routers will be ISP (Operations Team) managed unless you wish to void this warranty. What does this mean for competitors?

- You will need to rely on host firewalls for security
- Operations Team will not add firewall block rules
- Red Team will not have access or be allowed to compromise routers
- Uptime guaranteed by ISP (Operations Team) if managed by ISP
- No-Cost reset or Repair of Router system if broken

This means you do not have to worry about reconfiguring or maintaining firewall rules as well as the NAT configuration. Your services will just work. However you will still 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.

You may ask for credentials to manage your pfSense Firewall Router at a cost of 50 points. You may also request, at a cost of 50 points, for a replacement Palo Alto Networks Virtual Firewall Appliance which will replace your PFSense router. This will be configured to match your PFSense configuration and have a preconfigured password for you to access. You will need to use your PA License that was sent you at the beginning of the season in order to activate this device in order to gain full capabilities. **If you elect to do either of these changes, you will forfeit the above guarantees of the Ops Team. These requests will be on a first come first serve basis.**

This may not be suitable for all teams, as they may wish to configure firewall rules or maintain things themselves. This can be done by making a ticket request. Requests to manually configure firewall rules will be accepted after the first hour of competition. Please note this will void your warranty and is subject to fees as defined in the bottom of this packet.

After filing a ticket you please keep in mind the following:

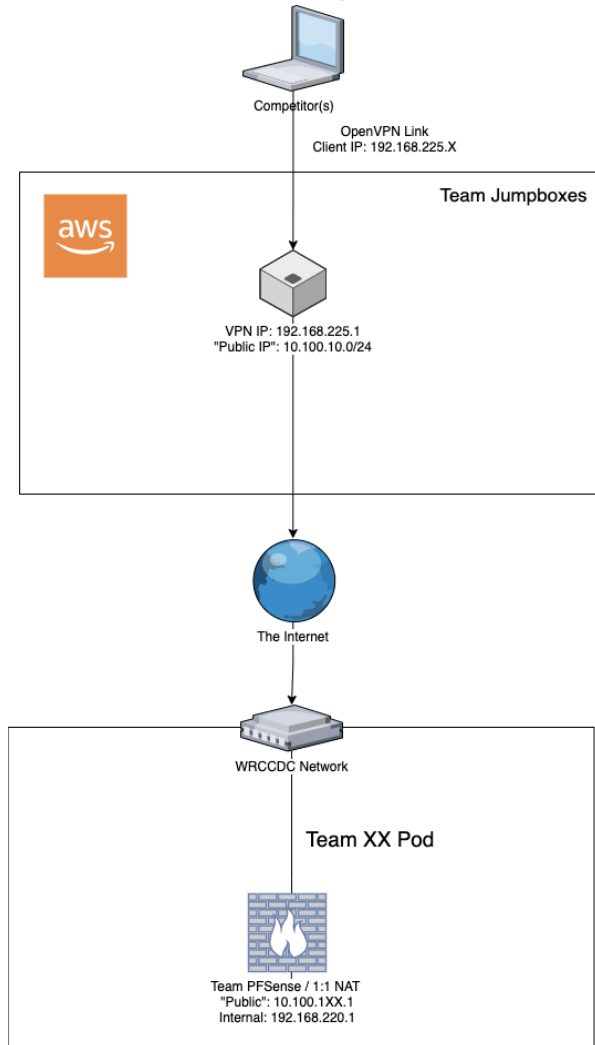
- Cutover Windows are every minutes (e.g. 10:00 or 10:30 etc)
- A credential will be provided in the ticket to you that will let you administer the router completely
- Do not change or delete or disable the "admin" user, this is used by your ISP and uses a secure password. (I'm serious, Red Team isn't going to use this)
- Do not disable syslog or WAN firewall configuration 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.

Connection Guidance

To help try to clarify how connections Each competitor will connect via OpenVPN to their JumpBox. Once on their Jumpbox they can reach their IP addresses relating to their pod via the connection into 192.168.225.1. This IP address accepts credentials via SSH and RDP. This box is the OpenVPN gateway for teams as well as their link into the pods. It will have an IP address

of 10.100.10.1XX. This will allow teams to connect to their pod which will have an IP address of 10.100.1XX.Y/24. Where Y is the last octet provided in the topology guide, once connected to a team device, it will internally have an IP address of 192.168.220.Y, again where Y is the last octet provided in this packet. *For example if a user from Team 2 connected to their Jumpbox, they would appear to be connecting from IP 10.100.10.102 to their system in pod 10.100.102.10, which would have an IP internally of 192.168.220.10.*



Team SIP Phones

This years qualifiers will have a public PBX server for teams to connect to for their VoIP Phones. One member of the team will need to download and install linphone (<https://www.linphone.org/>) on either a smartphone or desktop/laptop. The device being used for the softphone does not need to have a VPN connection to the competition.

Once you have it installed you can proceed to the wizard/assistant to set up your phone and select "Use Sip Account"

The PBX server is pbx.wrccdc.org:5061

Your Account Name is 8## based on your team number e.g. Team 1 is 801 and Team 12 is 812

Your Display Name should be Team ##.

Your SIP Password will be provided as part of the credential document.

Once you are connected you can test by calling 402 (Dhulaic)

You also have voicemail but will need to be set up. Call *97, the first time you connect use your own extension as the pin and you will be asked to set a new one.

If a Team requires more than 1 line for any given reason you can submit a ticket for extra extensions. You will be given a 4 digit number starting at 8##1 and up to 8##8 and will be given a ring group of 8##0. The Ticket when closed will have your Extensions, Display Names and SIP Passwords. This will be first come first serve and is not a requirement if you do not want more numbers.

Remote Access Guides

We will be providing you with full remote access connectivity for the duration of the competition.

CCDC Arena Jumpboxes

The primary means you will be connecting to the environment by means of Jump Systems. These systems will allow you to connect via OpenVPN. This interface may provide you with additional (and optional) connectivity options in the case of issues. We do not plan to have this exposed until issues take place. Each Jumpbox has dedicated resources of 4 cores and 16gb of RAM.

Prerequisites/Dependencies

- VPN Client such as OpenVPN Connect (Windows) or Tunnelblick (macOS) or similar
- Connectivity to 1194 UDP from your location
- Your IP Address whitelisted (by providing to operations) before start of event

Provided Capabilities

- Access into hosts via SSH, RDP, and VNC
- Ability to upload/download files where supported
- Ability to copy and paste over the network where supported

Once on the VPN you can verify connectivity by checking if you can ping the IP address 192.168.225.1. You will also use this IP address for connection into RDP/SSH. **Please do not perform scans from the jumpbox if possible, instead use a system within your pod.**

Logging into the CCDC Jumpboxes is easy, and uses the same credentials as the rest of the competition. Please note both the password and JumpBox IP address are in separate text files in the JumpBox bundle zip which includes OpenVPN Configuration as well.

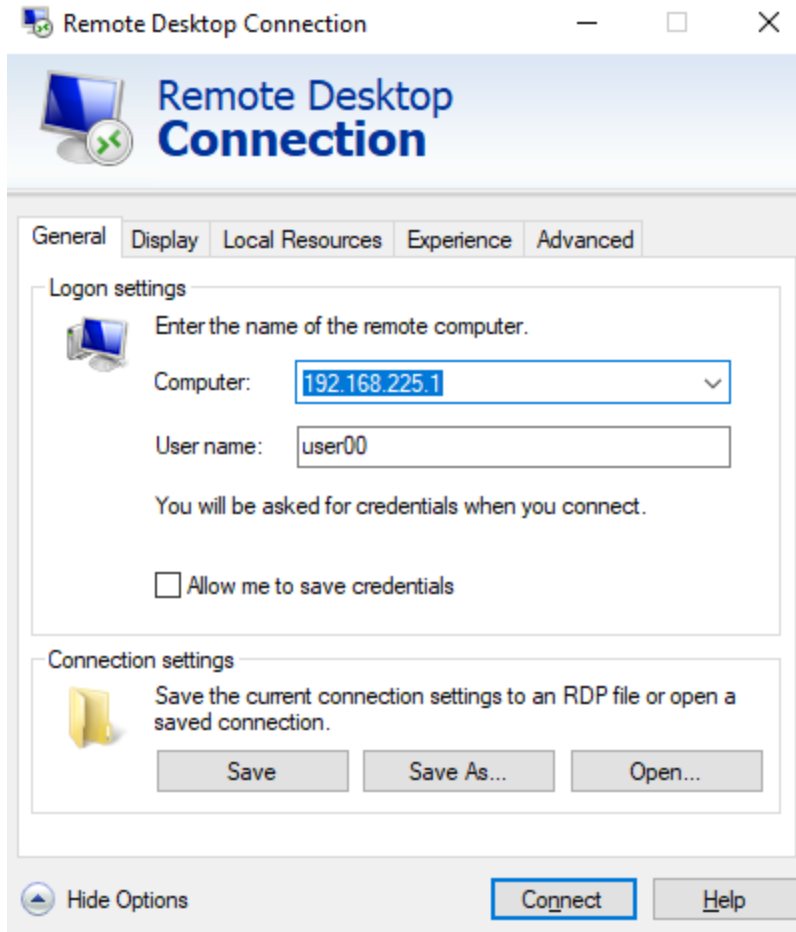
Username: userXX (e.g. user01, user02, ... user08)

Password: [Provided as part of Jumpbox Bundle In Zip]

Your team pod is accessible via 10.100.1XX.0/24 where XX is your team number. *For example* Team 2 would be 10.100.102.0/24.

Our RDP server supports pre-filled and prompted credentials at login. If you run into “failed to open session 0”, please delete saved passwords and login again or use manual login window to proceed. On Linux we recommend Vinagre or similar, macOS we recommend Microsoft Remote Desktop. These will prompt you for passwords and not have any issues.

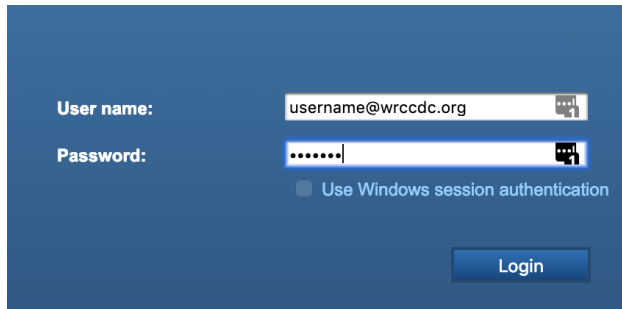
On Windows if you wish to prefill credentials you must check the box “Allow me to save credentials”. It will only prompt once, if you do not enter them correctly you will need to delete saved credentials and start again.



VMWare Console Access

If connectivity issues occur you may be asked to connect to our backup method of connectivity. You will not use this until we provide access.

1. Browse to <https://arena.wrccdc.org> and click on "VMWare" (<https://competition.wrccdc.org>)
2. Have your team captain attempt to login first and verify connectivity (you must have @wrccdc.org to login successfully)



User name:

Password:

Use Windows session authentication

Login

Support and Tickets

Ticket Service

Our support system is available at <https://wrccdc.servicenow.com>

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 username: TeamXX (where team XX is 01...04..10, 25, etc)

Your password: (See Password Document)

While the service scoring engine is out of scope of red team, it is encouraged you change your team password to something unique and memorable. You will be using the ticket manager primarily for any requests to us.

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 twelve tokens. 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 using this invite link: <https://discord.gg/jdFuFG4>
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)

<https://wrccdc.service-now.com/> - Use your AD credentials

Click "Request Something" then select the "[Services](#)" category to see all the types of requests you can submit.

Services



Manage the stuff and do the needful

<p>Box Reset Revert or reset some things (0-60pts)</p> <p>View Details</p>	<p>Bug Report Tell us about a bug! (0pts)</p> <p>View Details</p>	<p>Password Change Request Get some accounts some new passwords</p> <p>View Details</p>
<p>Resource Request Request something - like some hardware (0pts)</p> <p>View Details</p>	<p>Service Check Check up on some of your services</p> <p>View Details</p>	<p>Troubleshooting Get some expert help with something (100-200pts)</p> <p>View Details</p>

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. Points will be deducted for not following these guidelines.

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 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!

Manual Scoring (Orange Team)

There will be services that are scored manually. These can be blog commenting and posting, email use, ftp availability, ssh / rdp access 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 an 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 where as 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.

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 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.

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