Swiss Bank Xchange (SBX)

Introducing SBX, a digital financial institution providing innovative financial services and products for the modern investor. Our goal is to be the leader in new-world banking online and offer a comprehensive range of financial solutions. Whether you're in business, starting a business, or managing a business, SBX is your online financial hub.

Our suite of financial services includes cryptocurrency exchange with real-time rates, support for crypto wallets, blockchain solutions, and a recently launched NFT exchange for sales, support, and storage.

We aim to be at the forefront of the new wave in banking and investment, where traditional finance and digital assets seamlessly merge, giving you a personal metaverse to explore and invest in.

Welcome!

We’re excited to have you with us. We think you’ll be a great addition to our team. Remember, here at SBX “YOU” are special, loved, and appreciated! I will be your interface with the company as you take over our IT infrastructure and security operations. We know that you will fit right in with the rest of us here and are excited to see you bring more passion and vision to the network! Our systems should be very friendly and easy for anyone to use.

Remember, it isn’t just about making money here at SBX, it is about creating the market, space, and vision for the future!

Job Perks

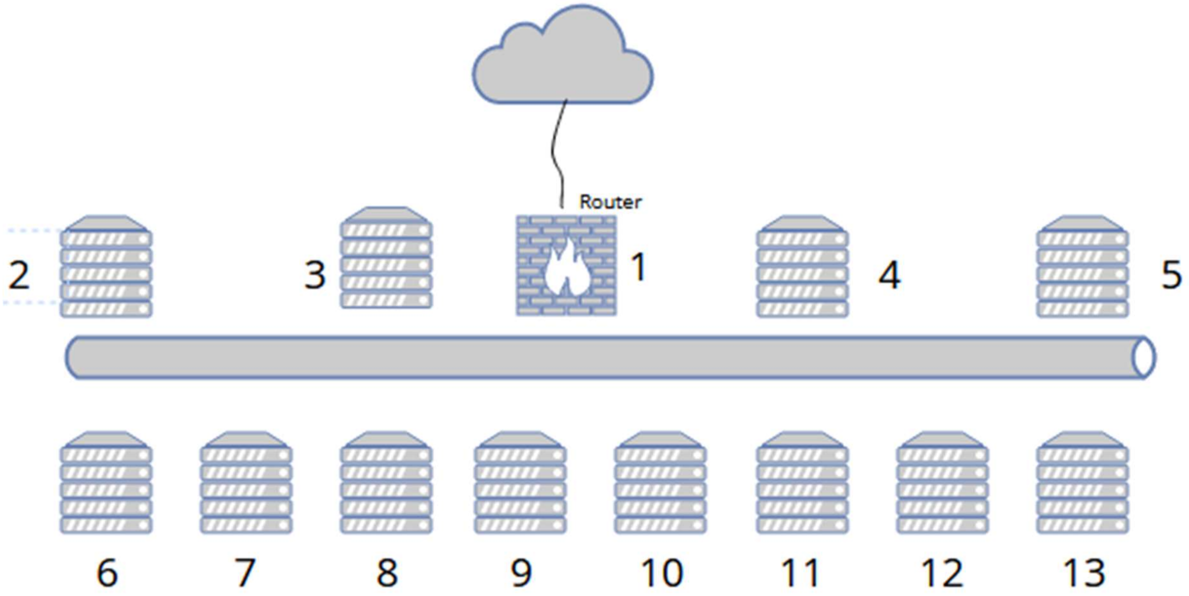
We offer a really competitive workplace including:

- Weekly off hour office hours
- Ping Pong Tables
- Financially supporting our charity with 10% of your salary
- Plenty of ergonomic financial products.
- A great can-do attitude
- Maintaining environment free of unionizing
- Refrigerators stocked full of NRG drinks
- Team Building!

Services and Scoring

Potential Services

We do have customers, and we want to make sure they can access our services to support their financial transactions and online exchange needs in the crypto banking world. We have some traditional banking services as well as IT services that you would find in any modern day business.



ID	Name	OS	Purpose / Service(s)
1	akkawi	PFSense	Router/Firewall
2	moliterno	Debian	Webserver
3	bluecheese	Windows Server	AD
4	Epoissesdebourgogne	Linux	Lots o’ Stuff…
5	milbenkase	Windows Server	File Server
6	casamartzu	Ubuntu	Wiki, KSMBD 🙂
7	havarti	Alpine	SMF
8	limburger	Debian	Collaboration Sheets
9	oaxaca	Ubuntu	Blog0, Files and Stuff

10	galbanino	Windows Server	Exchange 2019
11	kashkaval	Linux	DB Proxy
12	cheezwhiz	Rocky	Keycloak, DB
13	cottage	Debian	Docker, DB

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. Twenty (20) services will be scored across most servers every 2-4 minutes. If after 5 consecutive services checks a service is down, an SLA penalty will be assessed in the sum of -25 points.

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.

This means you do have to worry about reconfiguring or maintaining firewall rules as well as the NAT configuration. Your services will be subject to going down if this device is misconfigured.
Box Resets for this OPNsense router / firewall will by a -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 OPNsense device and ONLY the outside of the device. Put simply, you better know how NAT / PAT works!

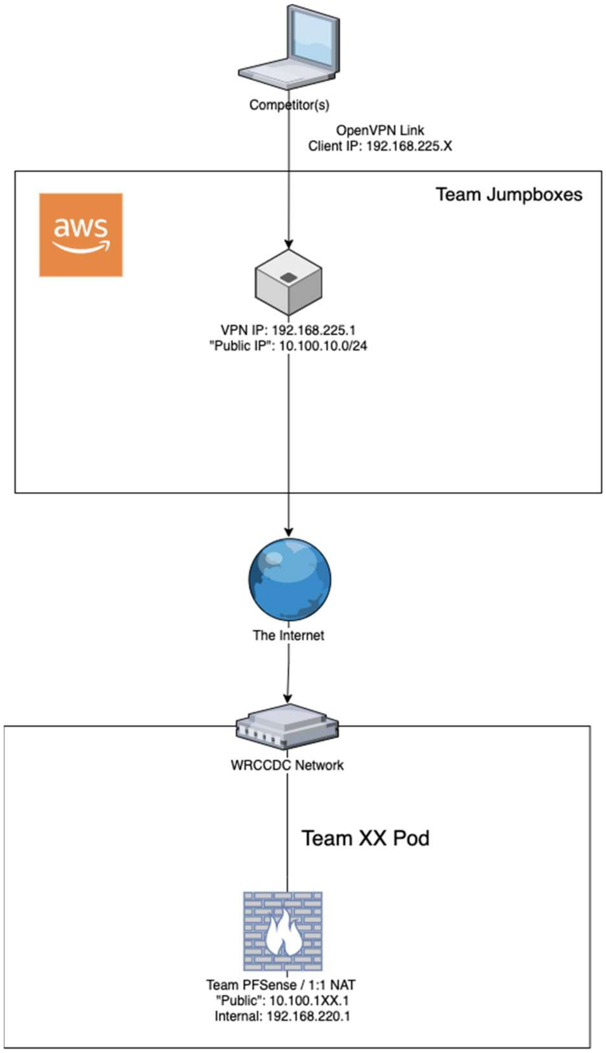
If you run into trouble with the PFsense Router, after filing out a ticket, please keep in mind the following:

- Cutover Windows 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.
- 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.

Connection Guidance

Teams will receive an OpenVPN key for VPN access. Each team member will access the VPN with only one end device. Your device count is capped at 8 devices. This connection will serve as your starting point for ALL of your players. You basically will share the machine (Via separate desktops / terminals.) Don’t worry, it is beefy enough to support your activities for the day of the competition. You will need to provide your team’s IPv4 address(s) / Network Scope to Dr. Brown. If you have not, it may delay you in starting the competition. If that happens, there will be no grace period for inject turn in or Red Team Start against your infrastructure. From this Jumpbox, you can ssh / RDP to your machines. Info on the machines will be provided tomorrow in DISCORD.
To help try to clarify how connections Each competitor will connect via OpenVPN to this single OpenVPN JumpBox. 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 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. (where XX is your team number). 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.*



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.

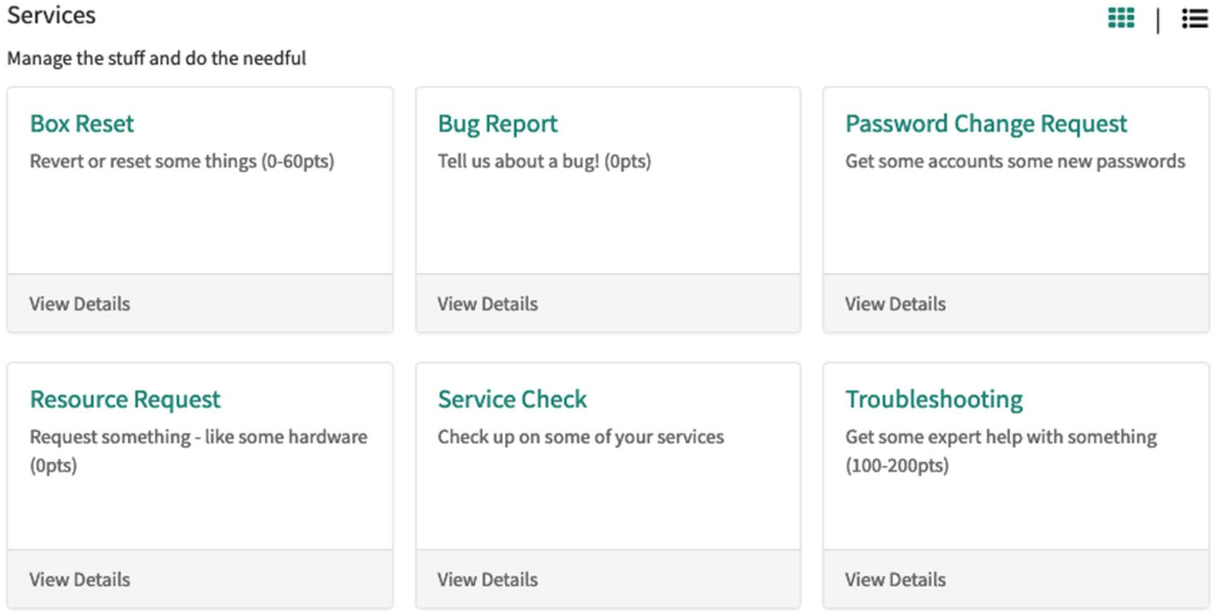
As part of this packet (or sent separately at the same time) you will have been given twelve tokens. These may be used to register you into your team role in the competition discord.

Steps to Join and Setup Discord:

1. Join Discord using a personal account or one generated for the competition 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)

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

Box Reset
Revert or reset some things (0-60pts)
View Details

Bug Report
Tell us about a bug! (0pts)
View Details

Password Change Request
Get some accounts some new passwords
View Details

Resource Request
Request something - like some hardware (0pts)
View Details

Service Check
Check up on some of your services
View Details

Troubleshooting
Get some expert help with something (100-200pts)
View Details

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 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 FTPsite 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 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

Your remote site judge will need to email Director Brown (brandon.brown@wrccdc.org OR bbrown118@coastline.edu) prior to the start of the competition stating that they have verified all player't IDs.