ISTS17

Blue Team Packet

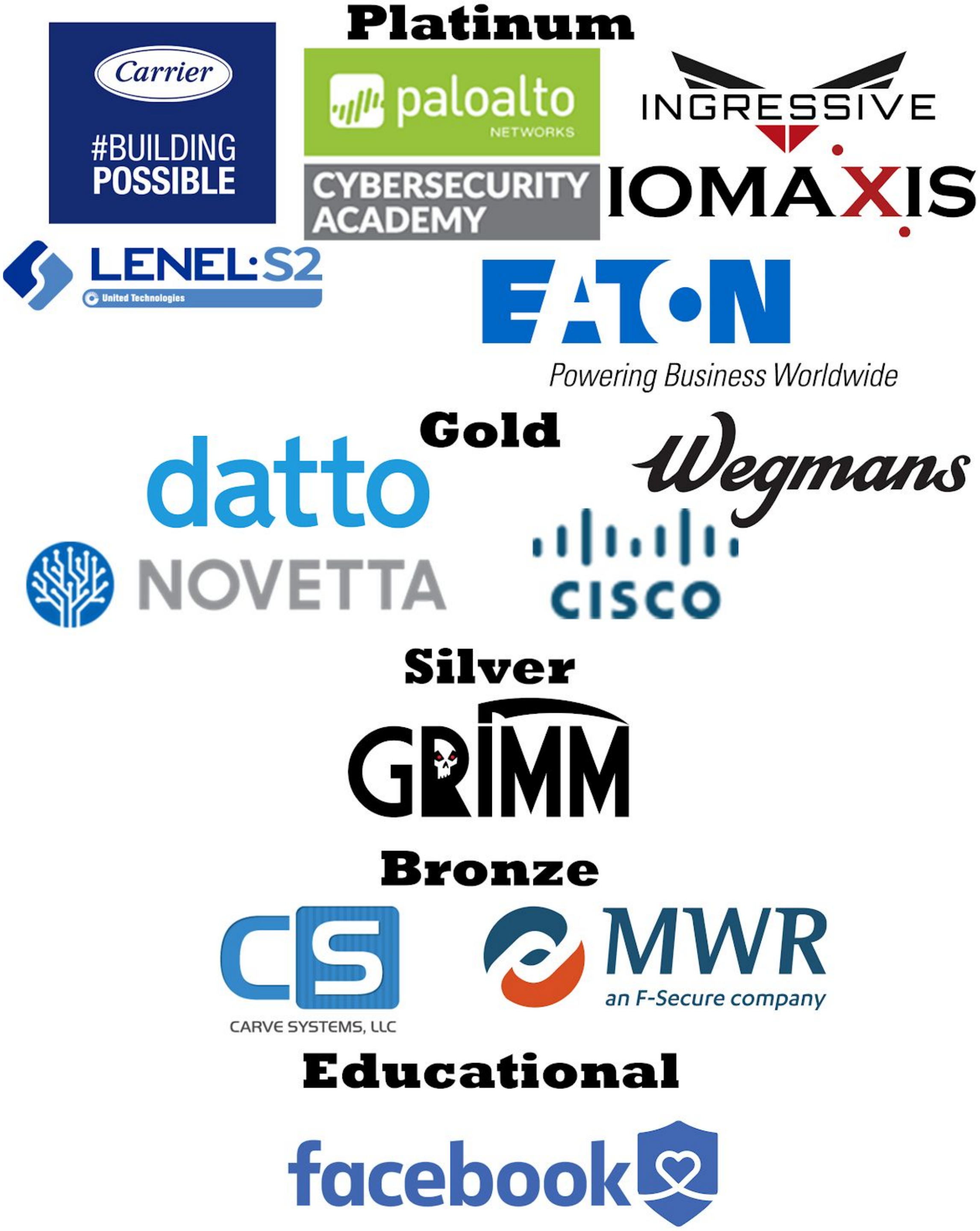
Hosted by **RITSEC**

February 22nd - 24th, 2019

Table of Contents

Thanks to Our Sponsors

Without our generous sponsors, ISTS would not be possible. Thank you for your support!



Scenario

This year, ISTS is set in the fictional country of Hackistan. The previous president of Hackistan died under mysterious natural circumstances, and an election is being held to select the next president. Each team represents the campaign team for a different political party in Hackistan, and they all are trying to get their candidate elected president. Your campaign must employ your cunning wit, careful strategizing, and some l33t hacker skills in order to win the election.

However, not everything is sunshine and rainbows in the country of Hackistan. There are rumors that foreign groups are trying to influence the election…

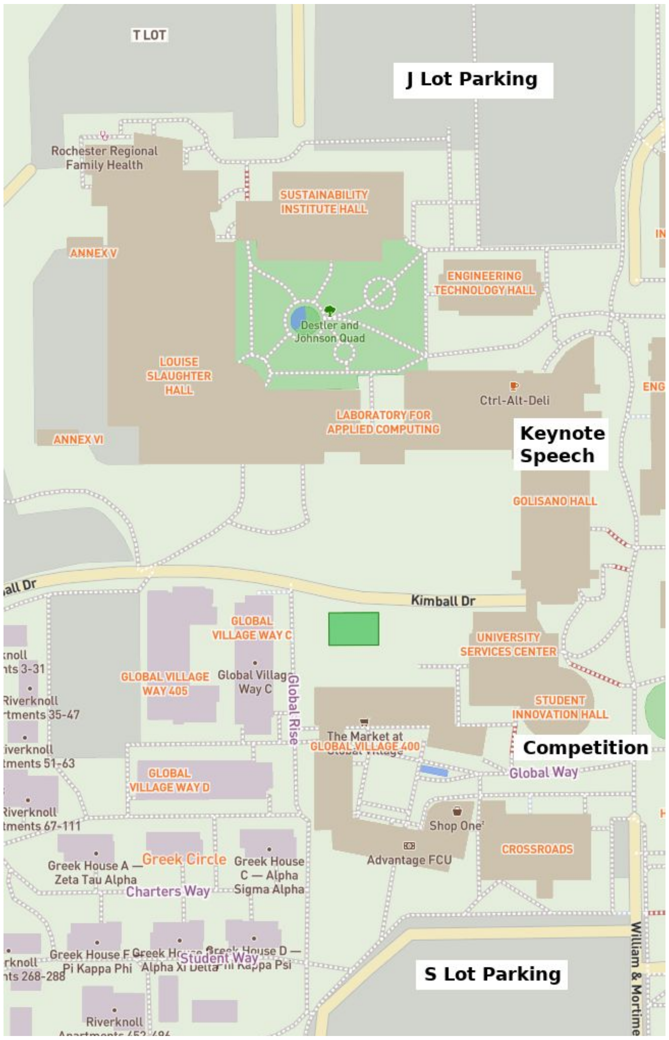
Schedule

Time	Description	Hands off	Location
FRIDAY			
5:00 PM - 5:30 PM	Blue Team check-in	X	GOL-1400
5:30 PM - 5:45 PM	Opening remarks	X	GOL-1400
5:45 PM - 6:45 PM	Keynote speech	X	GOL-1400
6:45 PM - 7:00 PM	Keynote speaker Q&A	X	GOL-1400
7:00 PM - 7:30 PM	Blue Team briefing	X	GOL-1400
SATURDAY			
8:00 AM - 9:00 AM	Breakfast, Blue Team check-in	X	SIH-1610
9:00 AM - 12:00 PM	Competition begins		SIH-1600
12:00 PM - 1:00 PM	Break for lunch	X	SIH-1610
1:00 PM - 6:00 PM	Competition resumes		SIH-1600
6:00 PM - 6:10 PM	Competition ends for the day, announcements	X	SIH-1600
6:15 PM - 7:15 PM	Dinner social	X	Salsarita's
SUNDAY			
8:00 AM - 9:00 AM	Breakfast	X	SIH-1610
9:00 AM - 12:00 PM	Competition resumes		SIH-1600

12:00 PM - 12:30 PM	Lunch (competition continues)		SIH-1610
12:30 PM - 2:00 PM	Competition continues		SIH-1600
2:00 PM - 2:30 PM	Final scoring & Jeopardy	X	SIH-1600
2:30 PM - 3:00 PM	Debriefing	X	SIH-1600
3:00 PM - 3:30 PM	Closing ceremony	X	SIH-1600

Location

Please go to https://www.rit.edu/maps/ for information about navigating to RIT. An interactive map of the RIT campus can be found at https://maps.rit.edu/. You can also search for "RIT S Lot Parking" or "RIT Parking Lot J" in Google Maps for directions directly to the closest parking lots.



The keynote speech will be held in Golisano Hall (GOL) auditorium, room 1400. The competition will be held in Student Innovation Hall (SIH), rooms 1600 and 1610. The dinner social/mixer at Salsarita's is on campus, right next door to Student Innovation Hall. The closest parking lots are S lot and J lot. Any spaces (including reserved spaces) can be used after 5:00 PM Monday through Friday and all day Saturday and Sunday without a parking pass.

Team Identification

Blue Team

This is you! You will be given a network to defend and assigned injects to complete on your network. Your team will also be working on CTF challenges, attacking King of the Hill boxes, and taking down other teams' defensive networks. It is your responsibility to realistically defend your network and keep your services running. Manual service checks may be performed at any time to verify that services are functioning as intended.

Red Team

Red Team is a group of industry professionals who will be simulating threats on your defensive network. They can sometimes be identified by their red shirts, but may sometimes be dressed in casual clothes. Their goal is to help all Blue Team members learn and grow during the competition, and have some fun along the way. They are here to help create the unique environment possible only at ISTS and competitions like it. While Red Team will also participate in King of the Hill, the CTF, and other portions of the competition, they are not competing with you.

White Team

White Team is a group of student volunteers who are the backbone of the competition. They can be identified by their white shirts, but may occasionally be dressed in other casual clothing. Prior to the competition, these individuals helped put in the work necessary to get things running smoothly. During the competition, they will be available to help with injects, the CTF, running the store, answering questions, and many other things. Should you have any questions during the competition, a White Team member should be your first point of contact.

Black Team

Black Team is a group of leadership roles that oversaw the creation and development of different areas of the competition. Each Black Team member is responsible for a specific portion of the competition, and leads a group of White Team members in that area. They can be identified by their black shirts, which will also identify which portion of the competition they are responsible for. Black Team is a subset of the White Team.

Rules

1. This competition exists for fun and learning. Do not break the spirit of the competition.
2. Be respectful of all people involved with the competition.
3. Do not make changes to the scored topologies without written White Team approval.
    a. Do not change the underlying technology that the services are scored on without written White Team approval.
    b. Do not change the machine that a scored services is on without written White Team approval.
4. Do not attack out-of-scope infrastructure.
    a. All Blue Team defensive infrastructures are in scope.
    b. The King of the Hill offensive infrastructure is in scope.
    c. All other areas (including physical hosts) are out of scope.
    d. Black Team reserves the right to modify the definition of "in scope" at any time.
5. Never attempt to impersonate a member of the Black Team or a Sponsor.
6. Anyone not registered as a team member may not participate in any way in the competition.
    a. All CTF challenges must be completed by a registered member of your team.
    b. All Injects must be completed by a registered member of your team.
    c. Any interactions with the competition on behalf of your team must be performed by a registered member of your team.
7. Do not share any point-earning information with any other team.
8. Do not use malware that is found online or in the wild.
    a. Popular tools such as Metasploit and Powershell Empire are allowed.

   b. Custom written malware is allowed, however you must have the source code to the malware, and must be able to explain in detail what it does.

   c. Malware downloaded from sites similar to VirusTotal is prohibited.

9. Do not perform any competition-related actions during "Hands Off" periods.

   a. Do not interact with any competition infrastructure.

   b. Do not attack any other team (physical and technical attacks included).

   c. "Hands Off" periods are marked in the schedule above.

   d. "Hands Off" periods are subject to change. Any changes will be announced by Black Team.

10. You may work on the CTF at any point during or outside of the competition.

11. White Team exists to help you. Do not try to deceive or otherwise lie to White Team.

12. You must follow any directive issued to your team by White Team. This may be written or verbal.

13. Breaking any of the above rules will result in a penalty at the discretion of White Team.

Scoring

Breakdown

Component	Percentage of Total
Service Uptime	33%
Injects	32%
King of the Hill	20%
Capture the Flag	15%

Score Visibility

During the competition, teams will be able to view each team's current score for the Service Uptime, King of the Hill, and CTF portions of the competition through the web portals for each of those portions. However, please note that the displayed scores are not correctly scaled relative to each other. Additionally, White Team reserves the right to make modifications to these scores when calculating the final scores based on any unforeseen events during the competition.

Welcome

TO: ALL STAFF

Welcome to the team! Or rather, congratulations on being selected as the new team. I'm sure you've heard by now what happened to our previous campaign team. Turns out the electorate doesn't like it when you use campaign contributions to fund an intergalactic mining operation.

Anyway, it's good that you're finally here. The election is ending soon, and there's still a lot for us to do before the polls close. First, you'll need to maintain all of our websites and services. Yeah, I know, we should hire an IT team for that. Well guess what? IT doesn't get us any votes, so we had to cut that team a while ago. I hope you know your way around the command line. Also, you'll have to deal with the press. They have the power to make or break our campaign, so we need to make sure they're on our side.

I'm sure you'll do great! Oh, and one last thing--do whatever it takes to win this thing. I don't need to know about it, but let's just say that if another campaign gets their servers hacked, it won't be good for their PR.

Sincerely,

Cory Rupt

Cory Rupt

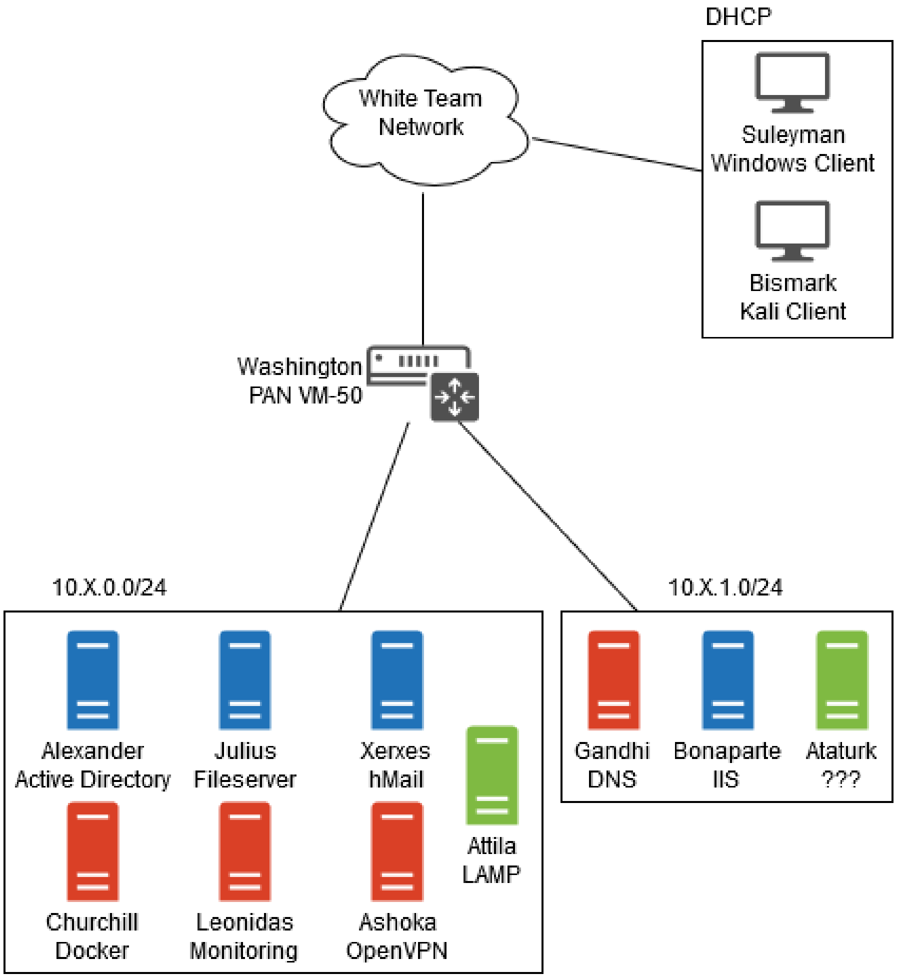
Party Chair

Defensive Topology

We need our services up and running in tip-top shape so we can reach out to voters. We're not sure what exactly the last nerds had running, but we looked at the sticky notes on their desks and hired a really expensive consultant to take a look. This is the information the consultant gave us. We're not really sure what else they did, but the way they talked made them sound super important, so the money must have been well spent.

Before we fired them, the last team yelled at me saying the consultant would "install back doors" into the systems. I don't know why they're talking about doors; we have Windows computers! Anyway, that last team never got us any votes, so what do they know?

Topology



Services

Hostname	Operating System	IP Address	Scored Services
Alexander	Windows Server ????	10.X.0.1	LDAP, DNS
Julius	Windows Server ????	10.X.0.2	SMB, FTP
Churchill	Ubuntu ??.??	10.X.0.3	Docker API
Leonidas	CentOS ?	10.X.0.4	Web, Elasticsearch API
Attila	???? Linux	10.X.0.5	Web
Xerxes	Windows Server ????	10.X.0.6	SMTP
Ashoka	Ubuntu ??.??	10.X.0.7	VPN
Gandhi	FreeBSD ??.?	10.X.1.1	DNS
Bonaparte	Windows Server ????	10.X.1.2	Web
Ataturk	openSUSE ??.?	10.X.1.3	Web, SSH
Bismark	Kali ????.?	DHCP	
Suleyman	Windows ??	DHCP	
Washington	PAN	Multi	

Initial Credentials

Use	Username	Password
vCenter	???	**Distributed at competition start**
Linux Machines	???	**Distributed at competition start**
Windows Machines	???	**Distributed at competition start**
Web Applications	???	**Distributed at competition start**
Databases	???	**Distributed at competition start**
When in doubt	root / admin / Administrator	**Distributed at competition start**

Scoring

Service uptime will be determined using an automated scoring engine. Each team will be provided with credentials at the start of the competition for the scoring engine, where they can log in to change information used by the engine to perform service checks (passwords, SSH keys, etc.). Teams will be able to see a live scoreboard of each team's scores, as well as view logs detailing the reasons a service check failed.

At any time during the competition, White Team may perform a manual service check to ensure that services are functioning properly. If a team is found to have taken measures to fraudulently pass service checks, points will be deducted from the team's score during final calculations at the discretion of White Team.

Injects

Since we're running a skeleton crew for the rest of the election, everyone will have to step in and help out when other people are having trouble. In other words, I'll be pawning all my work off on you guys. Make sure to be checking your email regularly for various assignments that need to get done. Remember, everything is TOP PRIORITY!

Important Technologies

Our aim with injects this year is to provide teams with tasks that will help them learn more about a certain area of security. Additionally, most injects are geared towards helping you secure your infrastructure. In order for these injects to be the most beneficial, we are providing a list of technologies that you will encounter in the injects questlines this year so your team can be comfortable with them prior to the start of the competition.

- OSSEC
- Graylog
- GitLab CI

Receiving and Submitting

Each team will be provided with an email account the day of the competition that will be used for injects. This email account will be through a third-party email provider, such as Gmail or ProtonMail. White Team will send all injects to only this email address, and all inject submissions should come from only this email address.

When an inject is made available, White Team will send an email to your team containing the inject's instructions, including the email address to send inject submissions to. If you have any questions about the inject, you may contact White Team at any time using the VoIP phones provided to you.

King of the Hill

We have a decent relationship with the media, but it could be better. We all know how important media relations are for a campaign, so getting the news outlets on our side will be one of your priorities.

There are several media companies that are covering this campaign, and you should be able to... coerce them to support us. Your team is great at this computer thing, right? Just get into their systems and let them know how awesome we are. They should hop on our bandwagon right away. If they don't... well, it shouldn't be that hard to make some minor modifications to their content.

Availability

All King of the Hill boxes will be accessible on a single offensive network. Blue Teams will be provided with the networking details of the offensive network prior to the competition. This network will be accessible from each team's defensive networks, assuming you don't firewall off yourself. Please note that it will **not** be accessible from the desktop computers provided to your team. You **must** connect to this network using the VMs on your team's defensive network.

At the start of the competition, some of the King of the Hill boxes will be immediately available to all teams. These boxes will be running a variety of vulnerable services, and teams must attack the boxes to gain access and score points. Every so often during the competition, we will release additional boxes. Once a box is made available, it will stay online for the rest of the competition.

Scoring

All King of the Hill boxes will have a single scored service (SSH, HTTP, DNS, etc.). An automated scoring engine, similar to the engine used for the defensive networks, will perform checks regularly to verify that the scored service is operating properly and to check the ownership of the box. To gain points for a box, both the service and ownership checks must pass.

Ownership

For your team to own a box (and therefore get the points for it), you must place your team's King of the Hill hash in the specified location on the box. This location is different for each service--see below for instructions. Initially, this location will be occupied by a special placeholder hash that signifies that the box is unowned. Once a team's hash is placed in the correct location, the scoring engine will transfer ownership of the box to your team after the next round of checks.

A complete set of instructions for all services will be provided upon arrival at the competition.

HTTP(S)

Replace the placeholder hash in the `ownership.html` file on the webserver with your team's hash. A `GET /ownership.html` request should return only your team's hash in the response body.

FTP

Replace the placeholder hash in the FTP banner with your team's hash. The FTP banner should not be modified in any other way.

SSH

Replace the placeholder hash in the SSH banner with your team's hash. The SSH banner should not be modified in any other way.

Telnet

Replace the placeholder hash in the Telnet banner with your team's hash. The Telnet banner should not be modified in any other way.

Uptime

Not only does your team have to correctly claim ownership over a service, you must also keep its service running. Each round, the scoring engine will perform an uptime check. If a box you own does not pass its uptime check, your team will not earn points for that box in that round.

If a box fails three uptime checks in a row, **it will be reset and your team will lose ownership**. Please note that the box may be down for a few more rounds as a fresh version is deployed and booted. Once the box is redeployed and accessible, all teams may reattempt to claim the box for their team. This mechanic is intended to prevent teams from simply turning off the vulnerable service to "lock down" the box.

Capture the Flag

In addition to running the campaign, your team will be responsible for a number of projects we've committed to over the course of the last several months. While not directly related to the election, ~~we saw a magic quadrant~~ we did in-depth research and decided that these projects would be the most likely to boost our numbers in some key swing states.

Yes, this will take some of your time away from your other responsibilities. It shouldn't be a problem for your team, though. Didn't you say during the interview that your team was the best?

Categories

This year, the CTF will have five categories. The following list is an overview of the challenge categories and brief explanations of what topics may be expected in each category. These topics are not exhaustive, and will not necessarily be included in the challenges. They are just examples to provide teams with a general idea of what they may encounter in the CTF challenges.

- **Web**: web vulnerabilities and anything else related to web services
- **Crypto**: all things cryptography
- **Reversing**: binary reverse engineering and binary exploitation
- **Misc**: steganography, file format bingo, OSINT, programming puzzles, trivia
- **Attack**: various attacks to be carried out on other teams, such as changing desktop backgrounds or website defacement

Electioneering

This year, ISTS will have an election-themed game that revolves around the polling that typically takes place in the lead-up to an important election. Over the course of several polling periods during the competition, teams will be provided with the means to cast their votes for whatever team they wish. At the end of each polling period, teams will win campaign funds based on how many votes they received.

Voting

Every hour a new poll will start, and each poll will last one hour. All votes received during the hour will be counted for that poll, even if they were submitted by the client during a prior polling period. Teams may vote for any team, including themselves.

To vote, each team will be given a Raspberry Pi and a keyboard, mouse, and monitor to use with it. The device will be connected to a special network separated from the competition network. Preinstalled on the device will be software that teams can use to submit votes for the current poll. Votes submitted through this method will be rate limited to 1 vote per 5 seconds.

Teams will also be allowed to vote through voting booths we will have set up at the competition. These will be touchscreen devices that teams log in to using credentials provided to them by White Team, and will allow for the bulk submission of 120 votes at a time. Teams will only be able to use this method once every 10 minutes.

All vote submissions from all clients are sent to a central server to be processed, validated, and recorded. Votes must be recorded by the central server in order to be counted towards the poll total.

A Note

All components of the game are fully in-scope. This includes the Raspberry Pis and the software running on them for all teams, the voting booth accounts, the voting booths themselves, and the central server. This does not include the web server that will display live results of the polls.

The only thing that will be used to determine the per-team payouts for a poll will be the vote totals recorded in the central server. How these vote totals get recorded does not matter, it only matters that they are recorded.

Red Team will be given the same access to the game as the Blue Teams, however Red Team will not be allowed to submit any votes.

Red Team ***really*** wants to win the polls.

It would behoove you to consider how Red Team would win the polls, and use that information to benefit your team's numbers in the polls.

Red Team *really* wants to win the polls.

Economy

Separate from the points your team will earn in the various competition components is the income your team will make. These *campaign funds* will not directly contribute to your final score, but they can be used to purchase various items at the competition store. These purchases can help out your team if you're in a rough spot, or make life harder for your competitors.

You don't get any points for saving money, so spend it up! Stimulate the economy!

Income

At the beginning of the competition, all teams will start with some campaign funds to get started. If your team wants more campaign funds (you should), you can earn more through the polling game or by completing items on the bucket list.

Money is earned through the polls. Each hour, a new poll is started with a unique payout amount. At the end of the hour, this payout will be distributed among the teams based on the proportion of the votes they received that hour. For example, if a poll has a payout of $100,000 and your team has 50% of the votes for that poll, then your team would receive $50,000 from the poll.

For information about the bucket list, see the **Bucket List** section below.

Store

The store is where Blue Teams and Red Team can go to purchase various items that will help their team, harm other teams, or are just plain fun. It is entirely White Team managed, and teams will have access to it through both a web application and an in-person store staffed by White Team. Each team will be given an account at the store which will be used to track their campaign funds balance and make purchases.

The store infrastructure will be out of scope this year, however teams may attempt to impersonate other teams if they wish (and are able to). **It is the responsibility of your team to protect your store account credentials.** White Team will attempt to independently verify a team member's claimed identity, but remember that they are just humans, and they are often sleepy. Sleepy humans are prone to errors.

Examples of store items from past years include box resets, Red Team member consulting, and forcing other Blue Team members to be hands-off for a certain amount of time. Most items can be purchased multiple times, as long as a team has the funds. If an item is limited to a certain number of purchases, the limit will be listed in the item description. Store items and prices are subject to change at any time during the competition.

Bucket List

The bucket list is an ISTS tradition. It is a list of several activities your team can complete in order to earn additional campaign funds. Most items on the bucket list can only be completed a single time, but some items can be repeated for more funds. Bucket list items from past years include lockpicking, trivia questions, selling a keyboard/mouse/etc., and singing karaoke to a song of White Team's choice.

Bucket list items and payments are subject to change at any time during the competition. The current bucket list will be listed on a store page, and any changes will be reflected there.

To complete an item on the bucket list, **teams must come up to the physical White Team store**. Your team will then sign in as if making a store purchase, and then the bucket list item will be selected. At least two White Team members must witness the completion of the bucket list item in order for it to be valid.

White Team has the final say about whether your team will receive the payment for the bucket list item. As long as your team completes the task in the spirit of the competition, there will be no issues with receiving the payment. If you believe your team has been wrongfully denied payment for a bucket list item, please discuss the issue with the Competition Architect or club President.

If you're thinking about bringing bolt cutters for any of the lockpicking challenges, leave them at home.