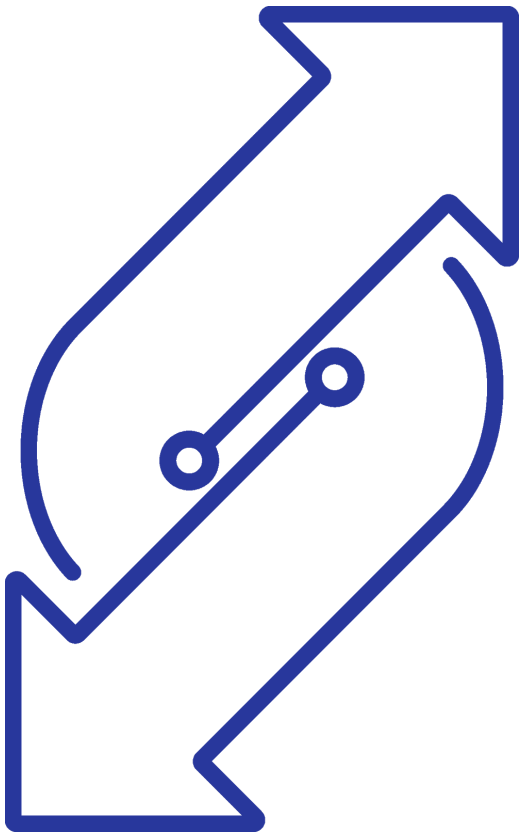


ISTS 2020

Blue Team Packet

Hosted by **RITSEC**

February 28th - March 1st, 2020

Table of Contents

Thanks to Our Sponsors

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

Scenario

Welcome to the dark world of black hat hacking!
You and four other ~~trusted~~ black hats have set out to corner the market on botnet installs. You've purchased a botnet framework called Jupiter from the Community of Cyber Children (an infamous hacking group that sells all things black hat). They manage access and hosting for the framework, all you have to worry about is getting those installs.

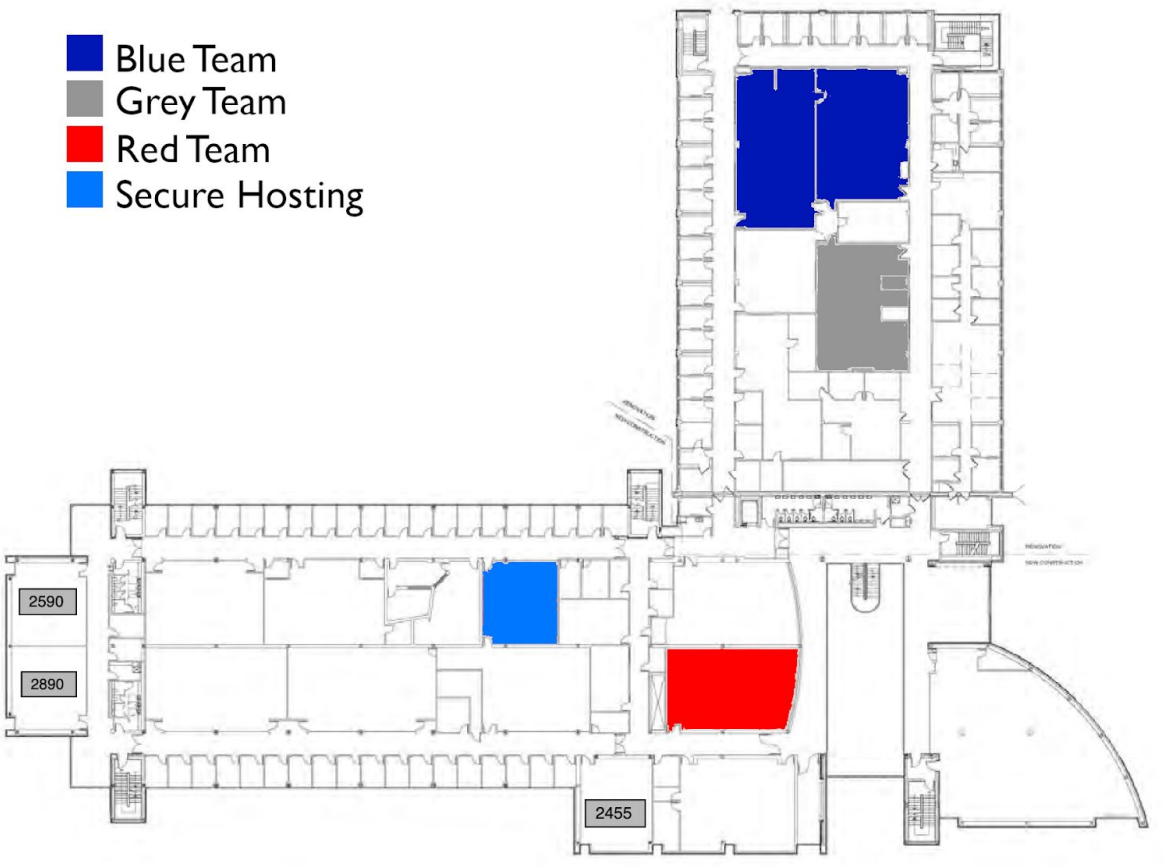
Since you don't have any money, they've agreed to accept a controlling share in your business in exchange for their services.

It's not easy being a black hat, you'll need to work hard to maintain your client facing services while hiding your identity from the FBI.

Schedule

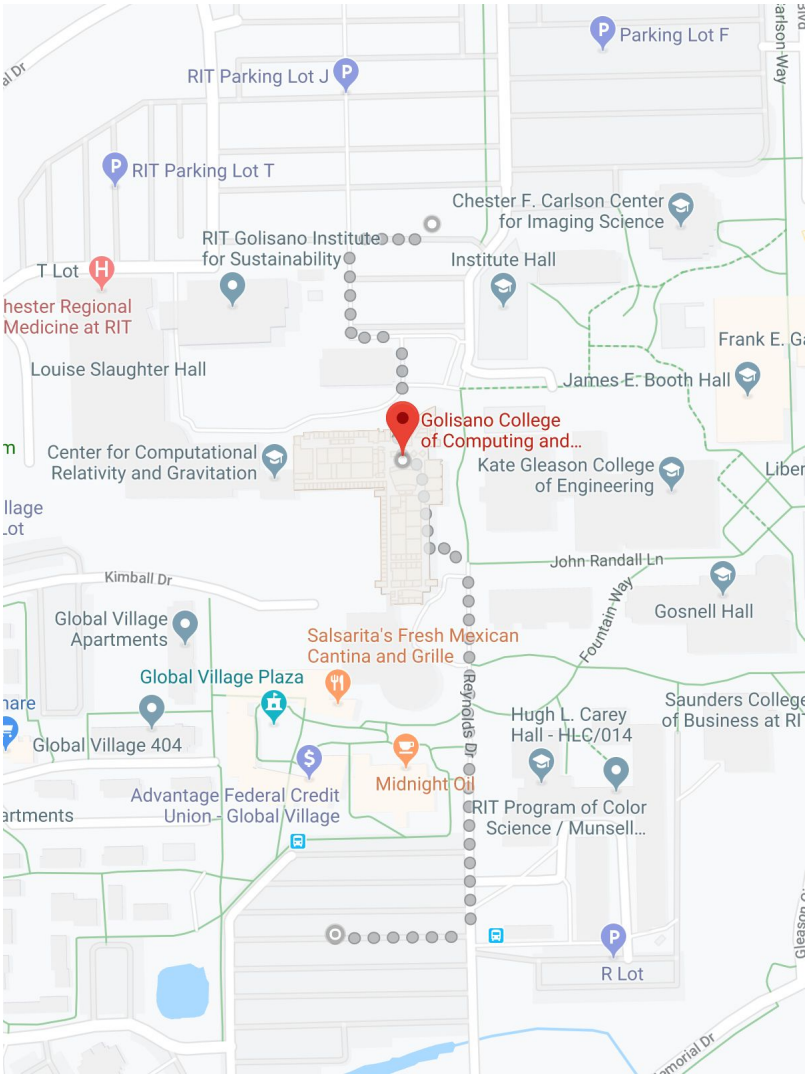
Time	Description	Hands on	Location
FRIDAY			
5:00 PM - 5:30 PM	Blue Team check-in	🚫	GOL-1400
5:30 PM - 5:45 PM	Opening remarks	🚫	GOL-1400
5:45 PM - 6:45 PM	Keynote speech	🚫	GOL-1400
6:45 PM - 7:00 PM	Keynote speaker Q&A	🚫	GOL-1400
7:00 PM - 7:30 PM	Blue Team briefing	🚫	GOL-1400
SATURDAY			
8:00 AM - 9:00 AM	Breakfast, Blue Team check-in	🚫	GOL-2400
9:00 AM - 12:00 PM	Competition begins	✔️	GOL-2320 GOL-2160
12:00 PM - 1:00 PM	Break for lunch	🚫	GOL-2400
1:00 PM - 6:00 PM	Competition resumes	✔️	GOL-2320 GOL-2160
6:00 PM - 6:10 PM	Competition ends for the day, announcements	🚫	GOL-2310
6:15 PM - 7:15 PM	Dinner social	🚫	Salsarita's
SUNDAY			
8:00 AM - 9:00 AM	Breakfast	🚫	GOL-2400

9:00 AM - 12:00 PM	Competition resumes	✔	GOL-2320 GOL-2160
12:00 PM - 12:30 PM	Lunch (competition continues)	✔	GOL-2400
12:30 PM - 2:00 PM	Competition continues	✔	GOL-2320 GOL-2160
2:00 PM - 2:30 PM	Final scoring & Jeopardy	🚫	GOL-2400
2:30 PM - 3:00 PM	Debriefing	🚫	GOL-2400
3:00 PM - 3:30 PM	Closing ceremony	🚫	GOL-2400



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 to the closest parking lots.



The keynote speech will be held in **Golisano Hall (GOL) auditorium, room 1400.** The competition will be held in **GOL-2160 & GOL-2320**. The dinner social/mixer is at Salsarita's on campus, right next door to the 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 as well as 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 simulating threats on your defensive network. They can sometimes be identified by their red shirts, but can also 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. While the 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 students in a leadership position that supervised 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 state their positions. 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 service is on without written White Team approval.
4. SLAs
5. Prestaging is allowed
6. Do not attack out-of-scope infrastructure.
    a. All Blue Team defensive infrastructure is in scope.
    b. The King of the Hill offensive infrastructure is in scope.
    c. Network based denial of service attacks
    d. Blue team openstack accounts are out of scope.
    e. White team infrastructure, networking, and web applications are out of scope. This includes but is not limited to:
        i. *.ackforums.com
        ii. the scoring engine
        iii. whiteteam store
    f. physical security scope
        i. Physically damaging anything is out of scope.
        ii. If you are caught you will be "arrested" by the FBI
        iii. You may not remove the boot drive for the ESXi servers.
        iv. If you're asked to leave a team's space you must leave.
        v. Blue team badges are in scope.

    g. Black Team reserves the right to modify the definition of "in scope" at any time.

7. Secure hosting procedures
    a. All participants must badge in to the facility.
    b. All participants must have their badge present at all times while in the facility.
    c. Participants may only interact with the systems that they have a badge for.
    d. If asked to leave by White Team you must do so promptly.
    e. Only one member of a team is allowed in the secure hosting facility at a time.
8. Never attempt to impersonate a member of the Black Team or a Sponsor.
9. 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.
10. Do not share any point-earning information with any other team.
11. You may write and submit injects from you host machine
12. 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.
13. 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.

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

14. White Team exists to help you. Do not try to deceive or otherwise lie to White Team.
15. You must follow any directive issued to your team by White Team. This may be written or verbal.
16. 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	33%
King of the Hill	20%
Capture the Flag	14%

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

Hello team,

While our arrangement to host your infrastructure in exchange for 51% of your business is unusual I am none the less happy that you chose Community of Cyber Children to manage your infrastructure.

In your purchase request you said that you want to "pop b0xes and pwn n00bs." We understand that this can be difficult, especially for a new team and in order to help you we've prepared some documentation to help get you started!

I'll be checking in on you periodically to make sure you're on the right track.

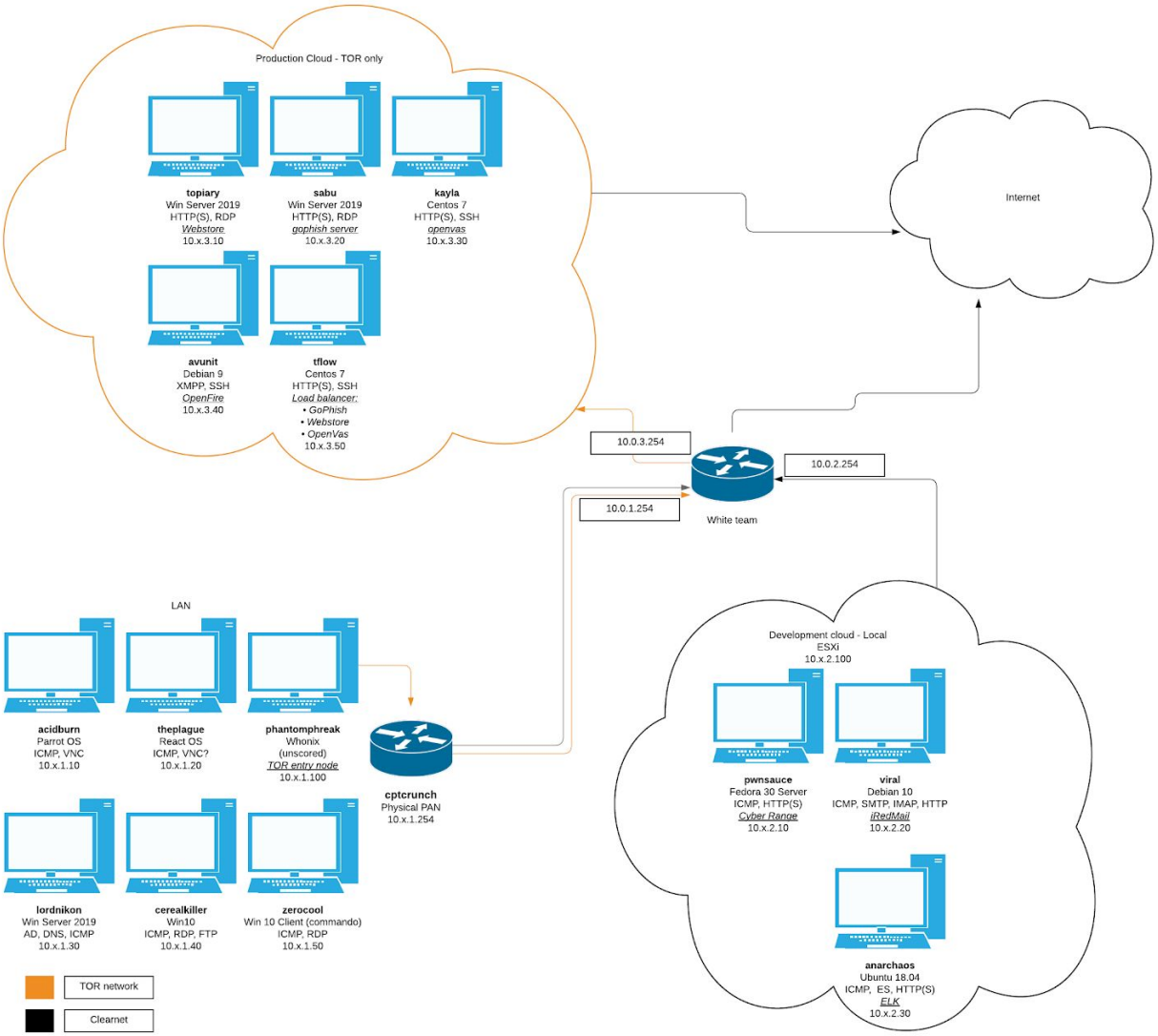
Good luck on your venture!

Sincerely,
Hulto
CCC CEO

Defensive Topology

Here's what your networks looks like! We've done our best to make it as comprehensive as possible.
We've built you three networks, a LAN that you'll be able to console into, a development cloud that will allow you to test your "products", and a production cloud that is only accessible over our private anonymous network called 'new-tor'. Each of the services in the production cloud is a TOR hidden service that is connected to 'new-tor'
The LAN will be accessible through a web console or via remote viewing tools that we will manage for you. We've setup your development cloud in our secure hosting site "steel hill", in order to access this site you'll need to badge in and pass a rigorous security screening.

Topology



Services

Hostname	Operating System	IP Address	Scored Services
acidburn	Parrot OS	10.x.1.10	ICMP, VNC

theplauge		10.x.1.20	ICMP, VNC
phantomphreak	Whonix	10.x.1.100	
lordnikon	Win Serv 2019	10.x.1.30	ICMP, AD, DNS
cerealkiller	Windows 10	10.x.1.40	ICMP, RDP, FTP
zerocool	Windows 10	10.x.1.50	ICMP, RDP
cptcrunch	PAN OS	10.x.1.254	
pwnsauce	Fedora 30	10.x.2.10	ICMP, HTTP, HTTPS
viral	Debian 10	10.x.2.20	ICMP, SMTP, IMAP, HTTP, HTTPS
anarchaos	Ubuntu 18.04	10.x.2.30	ICMP, Elastic Search, HTTP, HTTPS
topiary	Win Serv 2019	10.x.3.10	RDP, HTTP, HTTPS
sabu	Win Serv 2019	10.x.3.20	RDP HTTP, HTTPS
kayla	Centos 7	10.x.3.30	SSH, HTTP, HTTPS
avunit	Debian 9	10.x.3.40	SSH, XMPP
tflow	Centos 7	10.x.3.50	SSH, HTTP, HTTPS

Initial Credentials

Use	Username	Password
Scoring Engine	???	**Distributed at competition start**
ackforums.com	???	**Distributed at competition start**
Openstack	???	**Distributed at competition start**
Linux Machines	hannibal	N3xtGenH@ck3r101
Windows Machines	hannibal	N3xtGenH@ck3r101
Web Applications	???	**Distributed at competition start**
Databases	???	**Distributed at competition start**
VNC	-	password
ReactOS	Admin / VNC	N3xtGenH
When in doubt	root / admin / Administrator	**Distributed at competition start**

Web apps

Use	Username	Password
Greenbone	admin	admin
GoPhish	admin	gophish

Webstore	shopadmin	velvet_admin
Kolide	admin@teamX.ists.io	admin

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

I'll be reaching out to you over the hacking forum ackforums.com with tasks to help you improve my.... I mean your business. Make sure you do them, I am running your infrastructure for you after all. 😉

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. Make sure your team can be comfortable with them prior to the start of the competition.

- TOR
- Offensive security frameworks
- Incident response & logging
- Sandboxing and virtualization

Receiving and Submitting

The day of the competition, each team will be provided with an ackforums.com forum account that will be used for injects. White Team will send all injects to you through ackforums.com, and all inject submissions should be submitted through ackforums.com, unless told otherwise.

When an inject is made available, White Team will make a post on the forum containing the inject's instructions, including the username to send your inject submission to. At any time, if you have any questions about the inject, you may contact White Team using the VoIP phones provided to you.

King of the Hill

The saying goes, there's a lot of fish in the sea. That's not the case here. We've managed to get you access to the dev network of a startup incubator with a few apps setup inside it. If you can get access to their dev network we're sure to have access once they go public!

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 scored service(s) (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.

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 a black hat company, your team will have to maintain their reputation in the hacking community. These challenges may not be directly related to your company, but I feel it's important for you to maintain your reputation.

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 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

Botnet game

This year, ISTS will have a botnet themed game that revolves around the installation of bots. A windows and linux bot will be provided to each team at the start, however the API is also available and a team can write their own bots. At the end of each polling period, teams will win crypto coins based on how many boxes they have compromised.

Callbacks

Every hour a new poll will start, and each poll will last 30 minutes. Teams will earn points based on what percentage of **all** systems they have compromised, not the frequency, or number of callbacks. Each bot will callback to the white team C2 server, request a command to run, and send back a response.

In order to score points your bot will have to callback to the C2 server within the 30 minute period.

If two teams have compromised a system then the team with the most recent call back at the time of polling will receive the points for it.

Economy

The income your team will make is separate from the points your team will earn in the various competition components. These *crypto coins* 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 crypto coins to get started. If your team wants more crypto coins (you should), you can earn more through the botnet game or by completing items on the bucket list.

Money is earned through botnet installs. 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 bot installs they received that hour. For example, if a poll has a payout of $100,000 and your team has 50% of the installs 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, 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 crypto coins, 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 coins. 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 crypto coins. Most items on the bucket list can only be completed a single time, but some items can be repeated for more coins. 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.