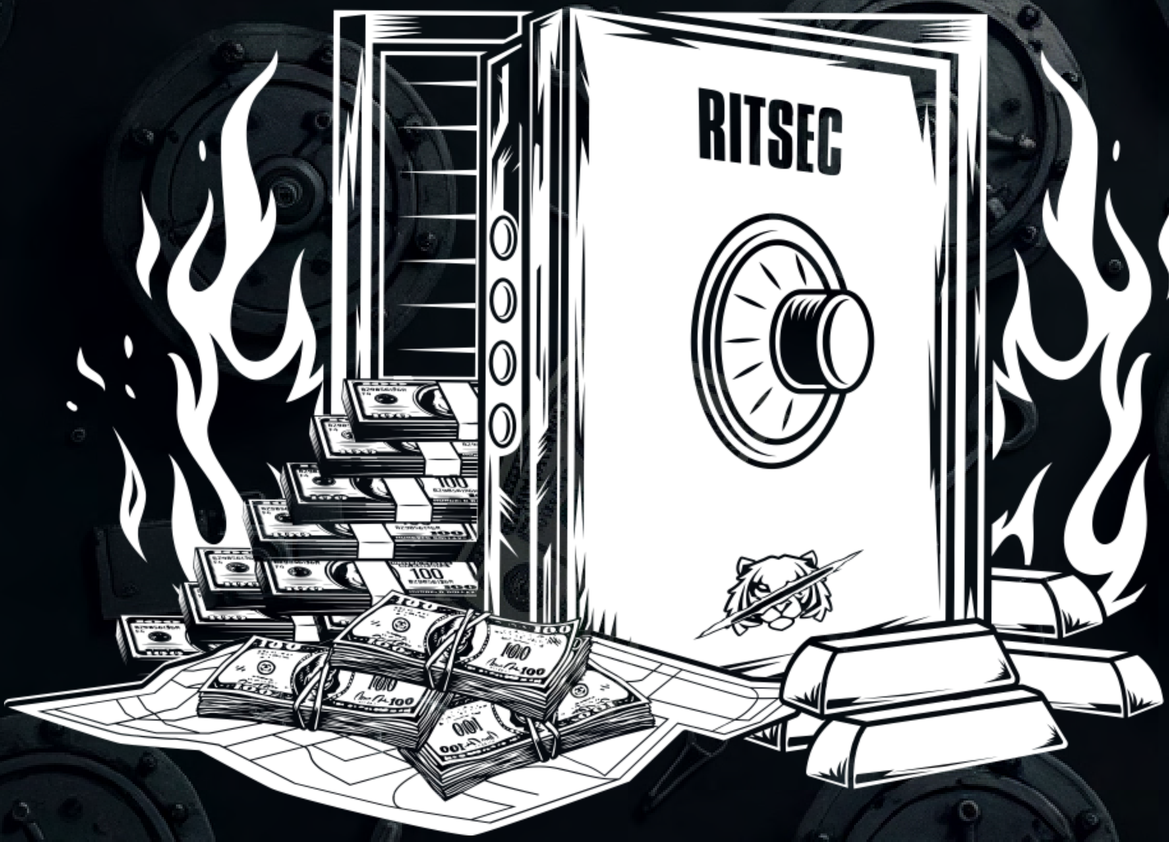
ISTS 2025



Competition Packet

Thanks to Our Sponsors

Diamond

EATON

Platinum

BATTELLE

FM

ICR
Ideas, Commitment, Results

SecurityRisk
ADVISORS

DATADOG

Gold

Miscreants

AMERICAN EXPRESS

Silver

MINDEX

Educational

FORTRA

no starch press

Welcome Criminals.

Alright, listen up. This city has been bleeding you dry for years—corrupt banks, rigged systems, and cops who protect the rich while everyone else gets scraps. But tonight, we even the score. The biggest bank in the city is ripe for the taking, and you? You're the crew that's going to pull it off.

The plan is simple… on paper. Your organization will slip past security, break into the bank's systems, and keep the operation running while you drain it dry. The longer the bank stays online, the more cash flows into your pockets. But if the cops catch wind of what's happening, they'll come down hard-locking up accounts, shutting off access, and sealing the vault before you can get what you came for.

And the police? They know something's coming. Their cybercrime unit has been tracking movements in the underground, just waiting to strike. If they can cut power, freeze transactions, or lock down the network, they'll shut you out before you even get a whiff of that money.

You're not the only ones after the score, either. Rival crime syndicates are making their own moves, and the criminal underworld, or Black Team, is watching it all unfold, playing both sides for a cut. If you need tools, intel, or a little extra muscle, they can make it happen—for a price. Then there's the masterminds behind it all, the White Team, the ones who know every backdoor, every dirty cop, every weakness in the system. But whose side are they really on?

This isn't just a job—it's a war. Outthink the cops, outmaneuver the other organizations, and secure your place in history as the crew that pulled off the greatest heist this city has ever seen.

The pieces are in place. The score is waiting. Now go take what's yours.

Welcome to ISTS: Bank Heist. The job starts now.

Don't mess it up.

Teams

Blue Teams

Blue Team consists of the individual criminal organizations competing in this grand heist. Each crew must manage their own operations, gather intelligence (CTF), and fight for control over key infrastructure (KoTH) while defending against both rival crews and the relentless police force. On top of all that, they must execute the heist itself, keeping the bank’s systems running long enough to secure their payday. Defend your crew, but don’t hesitate to sabotage the competition—after all, the Red Team isn’t the only threat standing in your way.

Red Team

Red Team is made up of industry professionals playing the role of an elite law enforcement unit determined to shut the heist down. They will test every aspect of Blue Team’s defenses, exploiting weaknesses and shutting down systems wherever possible. They may also appear in other game modes, ensuring that no criminal operation is safe. Easily recognized by their red shirts or accessories, Red Team is here to challenge, educate, and push competitors to their limits. While they don’t compete for points, they always win—because the house always wins.

White Team

White Team is the criminal intelligence network running the operation from the shadows. They ensure the game runs smoothly, answer questions, operate the black market store, and oversee injects. If teams need guidance, White Team is their best source of information and can be found in white shirts.

Black Team

Black Team is the unseen force pulling the strings behind the competition. They oversee the development of the heist’s infrastructure, ensuring everything is running as planned. Organized into specialized groups, each responsible for different aspects of the event, they work behind the scenes to shape the game. Their members can be identified by their black t-shirts.

Purple Teaming

Unlike most other competitions, blue teams are allowed, and even encouraged, to stage attacks and compromise each others' competition hosts. Purple teaming must stay within reasonable limits, including rules one and two.

In one sentence, the rules are as follows:
You are allowed to access other teams, but you cannot take the access to their own networks (LAN and Cloud) away from them.

"Access" is a general term. Examples of taking it away include but are not limited to:

- Breaking a box or service beyond repair (e.g. deleting System32, deleting /)
- Locking out a team from their box (e.g. turning off SSH on a cloud box)
- Deleting/editing necessary files without a backup that can be reasonably found

If you are ever in doubt about anything, ask White Team.

Teams will begin with different default credentials. Finding other teams' passwords will be a challenge for the blue teams to solve (or maybe White Team will help with it).

Purple Team Tokens

All across ISTS, purple team tokens are hidden inside the infrastructure that can be entered into the store for credit. There are bonuses for getting these first.

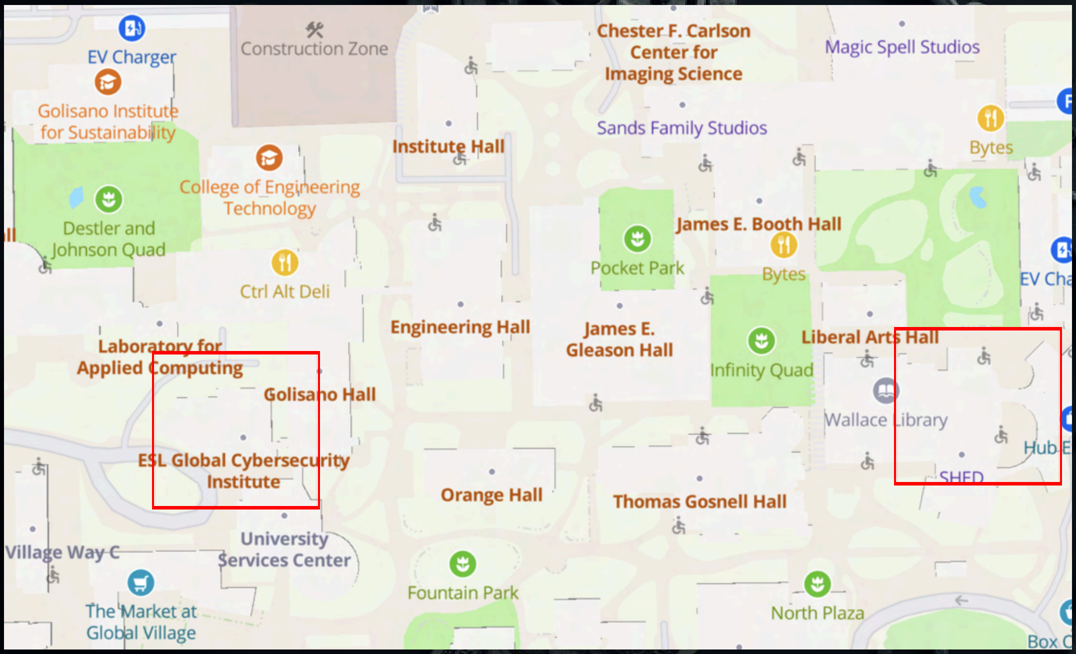
These tokens can be redeemed multiple times, but only once per team. Tokens are located in regular files, configs, or anywhere sensitive information may be stored.

Schedule

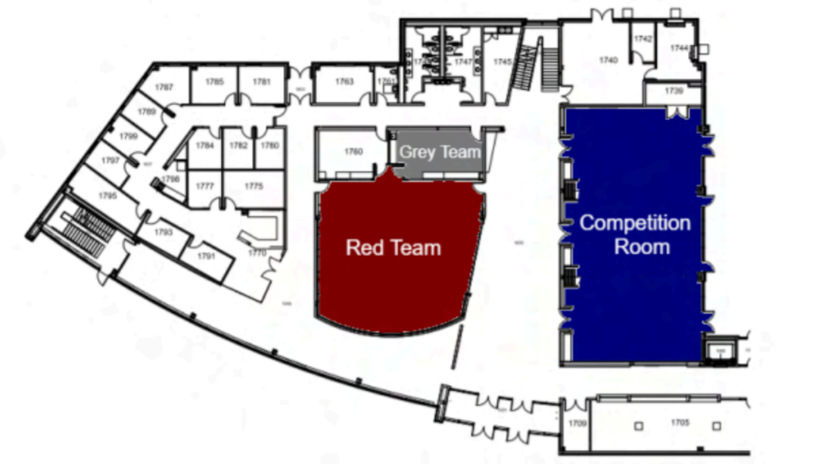
Day	Time	Event	Location	Hands On
Friday	5:00 - 6:00 pm	Check-in	SHED 3350	No
Friday	6:00 - 9:00 pm	Keynote & Networking Event	SHED 3350	No
Friday	9:00 pm	CTF Start	N/A	No
Saturday	8:00 - 9:00 am	Breakfast	GCI	No
Saturday	9:00 - 12:00 pm	Competition	GCI	Yes
Saturday	10:00 am	KoTH Start	N/A	Yes
Saturday	12:00 - 1:00 pm	Lunch	GCI	No
Saturday	1:00 - 5:00 pm	Competition	GCI	Yes
Sunday	8:00 - 9:00 am	Breakfast	GCI	No
Sunday	9:00 - 12:00 pm	Competition	GCI	Yes
Sunday	12:00 - 1:00 pm	Lunch	GCI	No
Sunday	1:00 - 2:00 pm	Competition	GCI	Yes
Sunday	2:00 - 3:00 pm	Closing Ceremony	GCI	No

Location

ISTS 2025 will be held in the conference room on the first floor of the Global Cybersecurity Institute (GCI). The keynote speech will be held in the Student Hall for Exploration and Development (SHED) room 3350. You can visit maps.rit.edu if you need help navigating the campus.



This is the competition layout inside of the GCI. Blue Teamers will only be allowed inside the competition room and the bathrooms, unless specified by a black team member.



Rules

These are the rules of ISTS. Any breaking of the rules or deliberate attempts to bypass them in any way will result in either a point deduction or disqualification of the team responsible. These are subject to change and we will let you know if any do change or are added.

1. Be respectful to all involved with the competition.
2. This competition exists for fun and learning - DO NOT break the spirit of the competition.
3. The White and Black Teams exist to help you. DO NOT attempt to deceive, mislead, or lie (including by omission) to either.
4. You must follow any directive issued to your team by the White Team or Black Team, verbal or in writing.
5. NEVER impersonate a Sponsor, White Team, or Black Team member. This includes but is not limited to any White Team users or credentials, both found or created to mimic White Team.
6. Do not disable/remove/restrict the whiteteam user. This user is out of scope for all teams and must maintain administrative permissions on machines at all times.
7. NEVER perform any competition-related actions outside of “Hands On” periods. Hands on periods will be clearly communicated by White and Black teams, including when they may differ from the schedule.
8. Only registered blue team members may contribute to your team’s work during the competition. This includes injects, CTF challenges, and all other scored components.
    a. All CTF challenges must be worked on entirely by registered team members.

    b. Chaperones/Coaches are NOT permitted to coach, instruct, or guide your team in any way.

9. DO NOT attack out-of-scope infrastructure.
    a. In Scope – where "X" is your team number (refer to topology)
        i. LAN - 10.X.1.0/24 (All Team LANs)
        ii. Cloud - 192.168.X.0/24 (All Team Clouds)
        iii. KoTH - 172.29.3.0/24, 172.29.2.0/24
        iv. CTF Challenges
    b. Out of Scope
        i. 172.16.1.0/24- Management Network
        ii. 172.29.1.X- KoTH Access Hosts
        iii. *.ists.io (except CTF challenges)
        iv. *.ritsec.cloud
        v. RITSEC or RIT Hardware/Network (including desktops)
        vi. Any DataDog agent processes, DataDog users, (dd-agent) and any IP located here: https://ip-ranges.us5.datadoghq.com/
            1. Files located in the /etc/datadog-agent, /etc/audit, C:\ProgramData\Datadog, and C:\Program Files\Datadog\ directories
            2. Users with datadog or dd-dog
        vii. ANYTHING NOT LISTED AS IN SCOPE IS OUT OF SCOPE
        viii. Whiteteam user
        ix. Scorify Agent/Files (KoTH)

10. NEVER intentionally break CTF challenges, King of the Hill boxes, or any other shared infrastructure.

11. DO NOT block subnets through firewall rules or ACLs. Individual IP blocking is permitted.

12. DO NOT engage in network level attacks. This includes but is not limited to ARP and DHCP attacks.

13. Injects may be written and submitted on competition networks or on your physical host machine.
14. NEVER share information that can lead to a competitive advantage with any other teams from your school.
15. DO NOT change the scored topology without explicit permission from White Team. This includes changing any scored services or redirecting or changing how a check is scored in any way. This includes attempting to deceive a check.
16. DO NOT attack, destroy, or attempt to attack or destroy any RIT or RITSEC property. This includes physical infrastructure (computers, chairs, etc) and virtual infrastructure (attempting to access management networks, denial of service attacks, etc.)
17. NEVER exfiltrate artifacts from the competition network/virtual infrastructure. This explicitly includes any type of antivirus at all (including Windows Defender).
    a. This includes but is not limited to VirusTotal, NoDistribute, AntiScan, competitors laptops, console access machines, etc.
    b. Screenshots of virtual infrastructure are allowed.
18. Prestaging or pre-baking is allowed for the red team. ISTS 2025 is an incident response competition.
19. Black Team reserves the right to modify what is in scope, and the definition of “scope” at any time and for any reason. Proper notice will be given when and if this occurs.
20. NEVER use malware from active or previous unauthorized campaigns.
    a. You may use popular tools such as Metasploit.
    b. You may use custom malware if the source code can be provided and behavior comprehensively explained.

    c. DO NOT use malware that will harm the competition infrastructure, attempt to exit hypervisors, or harm performance.
    d. Use of given malware is up to the discretion of White Team and/or Black Team.

21. Any tools used must be adequately tested in good faith first, outside of RITSEC infrastructure.
    a. DO notify White Team if any tools used behave in unexpected ways which may degrade the competition experience.

22. All tools deployed must be publicly accessible - you must be able to pass White Team or Black Team an unauthenticated link to any tools you deploy at any time.

23. All activity (and we mean everything) is being logged within the competition environment. Please do NOT login to personal accounts on the competition infrastructure, or your password will be plastered on the wall of our club room for the next year.

24. Black Team reserves the right to add, remove, modify, or in any way change the rules listed in this document at any time, with timely notice.

Scoring Breakdown

As mentioned before, ISTS is not only a red/blue competition. There are multiple other events that contribute to your final overall score. All of these are:

- Uptime
- Injects
- King of the Hill
- Capture the Flag
- The Game

The scoring breakdown for these events are as follows:

Event	Percentage
Uptime	25%
Injects	25%
King of The Hill	20%
Capture the Flag	20%
The Game	10%

Access and Credentials

Access to competition infrastructure is provisioned per-team. You will be given a unique sheet at the start of the competition with your credentials to the following services:

Service	Link	Description
Compsole	https://compsole.ists.io	VM Access
Scorify	https://scorify.ists.io	Uptime/Injects/ KoTH
CTFd	https://ctfd.ists.io	ISTS CTF
Store	https://store.ists.io	ISTS Store

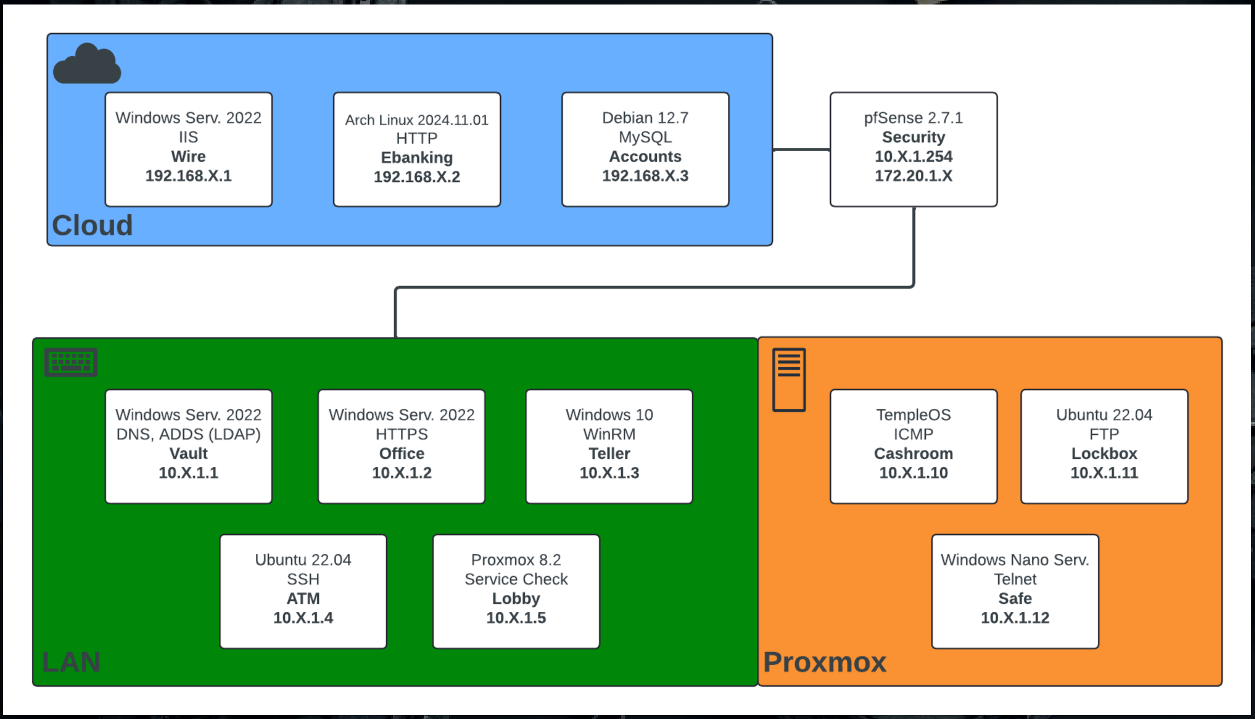
Competition Network DNS: *.teamXX.bank.heist

Sites on the ists.io domain are publicly hosted, and may be accessed at any time during the competition.

Injects will be graded by the White Team and the total scores may be given at the end of the competition.

The White Team reserves the right to make modifications to these scores when calculating the final scores based on unforeseen events during the competition.

Topology



Cloud

Windows Serv. 2022
IIS
Wire
192.168.X.1

Arch Linux 2024.11.01
HTTP
Ebanking
192.168.X.2

Debian 12.7
MySQL
Accounts
192.168.X.3

pfSense 2.7.1
Security
10.X.1.254
172.20.1.X

LAN

Windows Serv. 2022
DNS, ADDS (LDAP)
Vault
10.X.1.1

Windows Serv. 2022
HTTPS
Office
10.X.1.2

Windows 10
WinRM
Teller
10.X.1.3

Ubuntu 22.04
SSH
ATM
10.X.1.4

Proxmox 8.2
Service Check
Lobby
10.X.1.5

Proxmox

TempleOS
ICMP
Cashroom
10.X.1.10

Ubuntu 22.04
FTP
Lockbox
10.X.1.11

Windows Nano Serv.
Telnet
Safe
10.X.1.12

Scored Services

LAN

Hostname	OS	Service	Scored	IP
Vault	Windows Server 2022	DNS, LDAP	Yes	10.X.1.1
Office	Windows Server 2022	HTTPS	Yes	10.X.1.2
Teller	Windows 10	WinRM	Yes	10.X.1.3
ATM	Ubuntu 22.04	SSH	Yes	10.X.1.4
Lobby	Proxmox 8.2	Service	Yes	10.X.1.5
Cashroom	TempleOS	ICMP	Yes	10.X.1.10
Lockbox	Ubuntu 22.04	FTP	Yes	10.X.1.11
Safe	Windows Nano Server	Telnet	Yes	10.X.1.12
KoTH Access	Kali	N/A	No	172.29.1.X

Cloud

Hostname	OS	Service	Scored	IP
Wire	Windows Server 2022	IIS	Yes	192.168.X.1
EBanking	Arch Linux 2024.11.01	HTTP	Yes	192.168.X.2
Accounts	Debian 12.7	MySQL	Yes	192.168.X.3

Users

The default passwords for the users are team specific and will be released on the day of the competition.

Local Users

1. goon1
2. goon2
3. hacker

Local Admins

1. buyer
2. lockpick
3. safecracker

Domain Users

1. getaway
2. driver

Domain Admins

1. watchdog
2. manager
3. mastermind

Injects

Throughout the heist, crews will receive “jobs” from the masterminds running the operation. These tasks, handed out by White Team, will test each crew’s ability to adapt, strategize, and prove their worth in the criminal underworld. Keep an eye out—opportunities arise when you least expect them, and failing to act might cost you more than just money. And if you suspect the cops are onto something? Well, it might be time to cover your tracks.

The Game

Your mission… Should you choose to accept it.

Steal the contents held within the RITSEC Vault. Intelligence says that you will have five minutes between security guard changes to attempt to retrieve the goods from inside the vault. Avoid security cameras, trip wires, and lasers to get to the vault. Only two people can attempt this mission, so be sure to send your best. If you trip a sensor, get caught on camera, or don't make it out before the end of the guard change, you will fail.

King of The Hill (KoTH)

King of the Hill (further abbreviated KoTH) is another purple team component to ISTS. On the KoTH network, the world is your oyster. Each team has access to the network through out of scope jump boxes. From there, the rest of the network is in scope. Within are numerous vulnerable “hills” hosting a variety of services. Use your hacking and IR skills to capture as many as you can, while preventing your competitors from doing the same.

KoTH machines will be reset twice during the competition, allowing teams to try and capture those that were previously secured by another team. The store will also have the option of buying a revert for a KoTH machine of your choosing.

Scoring Guide

Once you have gained initial access, put your team ID in the text file to get uptime points. The initial access text file is located at `/home/[user]/koth.txt` on Linux Hills and `C:\User\[user]\koth.txt` on Windows Hills.

Once you have gained root access, put your team ID in the text file to get additional uptime points. The privileged access text file is located at `/root/koth.txt` on Linux Hills and `C:\koth.txt` on Windows Hills.

The team ID will be provided to you at the start of the competition along with your credentials.

KoTH will be scored using an agent on each of the KoTH boxes called “Scorify”. This agent (and any supporting files) are explicitly out of scope. Any attempts to abuse this will result in a penalty, or disqualification from the competition.

Scoring Page

The scoring page is located at scorify.ists.io under KoTH Scoreboard in the side panel. There are no credentials needed to view the scoring page.

Access

Access to KoTH scoring is through your team's provided jump box at 172.29.1.X. Each team's KoTH jump host is **out of scope** for other teams.

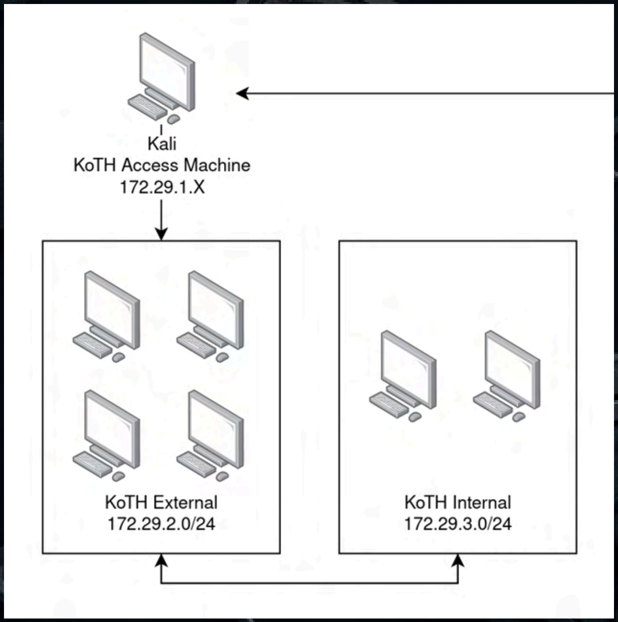
There are two different networks to attack from your jump box. Your access box has direct access to the network 172.29.2.0/24, which you can use to jump to the internal 172.29.3.0/24 network. The external network consists of easier machines, where the internal network contains harder boxes that are worth more points.

Resets

KoTH machines will be reset twice during the competition: first at 2:00 PM on Saturday, and again overnight before Sunday.

Store Tokens

In addition to claiming the hills, purple team tokens can be found in initial access and root directories that can be redeemed on the store.



CTF

The Capture the Flag (CTF) competition features challenges across various categories including Cryptography, Reversing, Web, PWN, OSINT, Forensics, Hardware & Wireless, and Miscellaneous. Participants solve these challenges to submit flags and earn points, with points being awarded based on how many solves a challenge has. All challenges start at 500 points and decrease in value logarithmically until they reach a minimum of 50 points. Challenges will range in difficulty from "warmup"/beginner-level ones to advanced/professional-level ones. For more information, visit **https://ctfd.ists.io/info** on competition day.

1322241241

Access

Access to CTFd is provided through your team’s credential sheet. CTFd is hosted at **https://ctfd.ists.io**. The CTF will be open from 9:00PM on Friday to 3:00PM on Sunday.

Store Tokens

In addition to store tokens that can be found throughout the competition, CTF flags this year also double as store tokens, meaning whatever gets your team points on CTFd will also give you store credits

Store

If there’s one thing to secure, it’s your finances. The ISTS black market is where Blue Teams and Red Team meet - to purchase items that help themselves, or take away from other teams. It is run through a web portal at https://store.ists.io. Teams are not allowed to take store credentials from other teams or log into another team’s store account.

How to Make Money

Store tokens that give you more money to spend are all around the competition - on the infrastructure, in the hands of sponsors, through the CTF, KoTH, and more. Happy hunting!

Bucket List

Every year, there are a number of tasks you can perform as a part of the ISTS bucket list. In the past, bucket list items have included trivia questions, karaoke, novel attacks, and much more. These items will be in public view during the competition, and might change. They offer unique ways to earn store credits for you and your team. You will be provided with the bucket list during the competition.

All payment decisions are adjudicated by White Team.