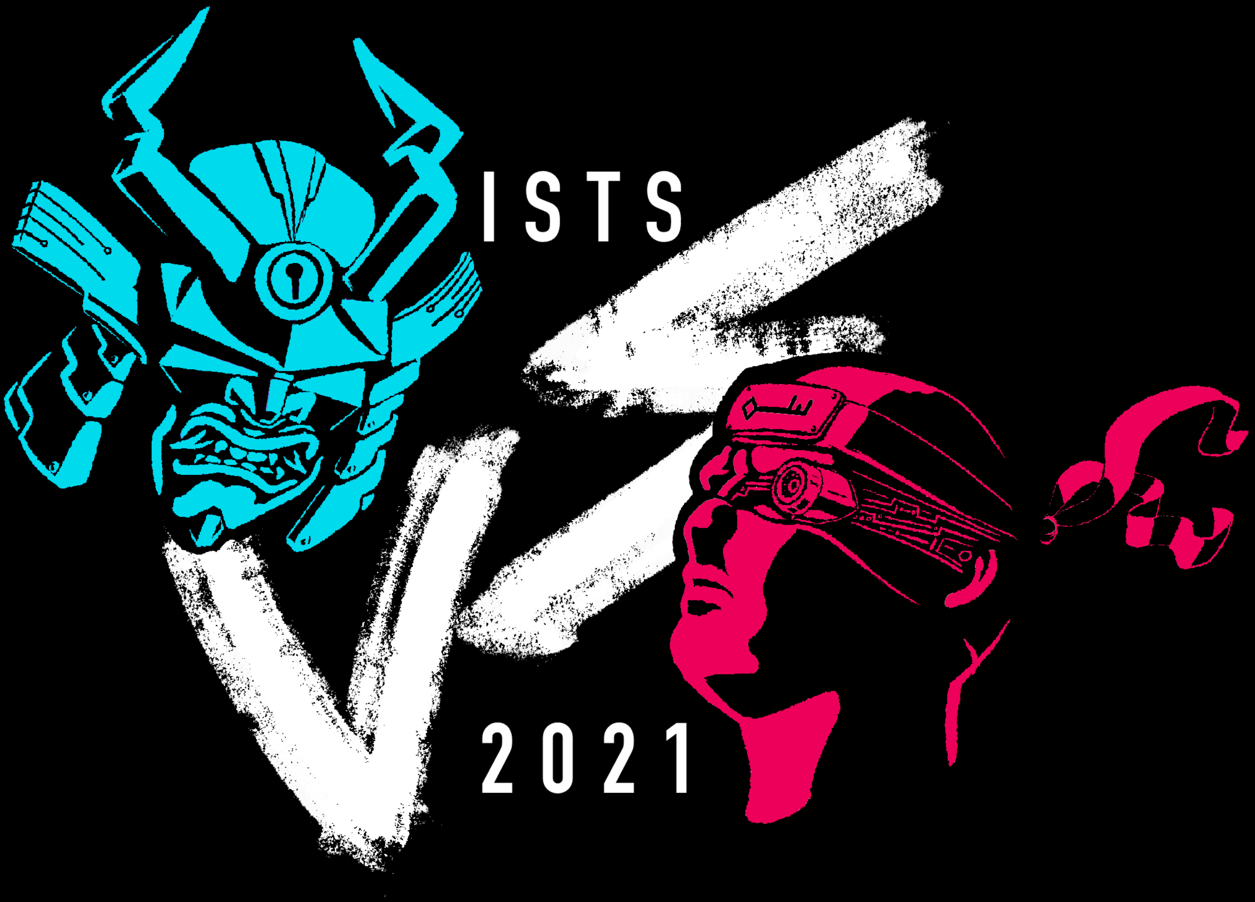


ISTS 2021

Enter the Cyber(punk)

RITSEC

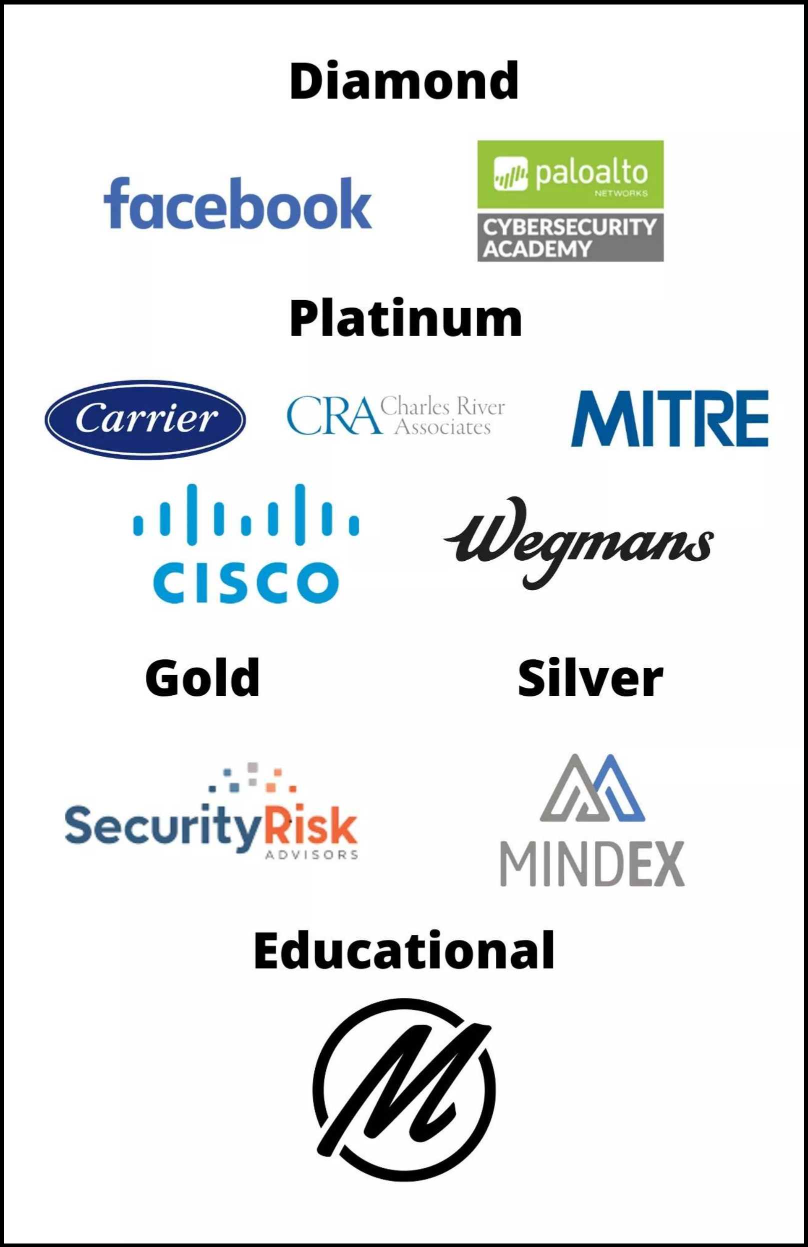
March 5 - March 7

Table of Contents

Thank you to our Sponsors

Without our generous sponsors, ISTS would not be possible.

Thank you for your contributions and support!



Scenario

Welcome to the future! Exciting, isn’t it?

Sort of? Good.

You have entered a future Japan, governed by corporations who have brought society back into the feudal period.

You will be taking on the role of samurai in the digital world. Hired by the ambitious Mr. Kumichō, a shogun in the new/old societal order with aspirations of leading his company, IkiruCorp, to its rightful place of glory as the most powerful corporate empire in the world. He will certainly keep you busy!

If that wasn’t challenging enough you have a formidable adversary who will sabotage and frustrate the efforts of IkiruCorp at every turn. The ninja are the resistance to the corporate overlords. They are crafty, and you have become their target. Hopefully you will fare better than their past victims…

Schedule

Time (EST)	Event	Hands-On-Keyboard?	Location
Friday - March 5th			
17:00 - 17:15	Opening Remarks	✖	Zoom
17:15 - 18:15	Keynote Speech	✖	Zoom
18:15 - 18:30	Keynote Q&A	✖	Zoom
18:30 - 19:00	Blue Team Briefing	✖	Zoom
Saturday - March 6th			
09:30 - 10:00	Blue Team Check In	✖	Discord
10:00 - 13:00	Competition Part 1	✔	Discord
13:00 - 14:00	Break for Lunch	✔	-
14:00 - 19:00	Competition Part 2	✔	Discord
19:00 - 19:15	End of Day Announcements	✖	Zoom
Sunday - March 7th			
09:45 - 10:00	Blue Team Check In	✖	Discord
10:00 - 13:00	Competition Part 3	✔	Discord
13:00 - 14:00	Break for Lunch	✔	-
14:00 - 16:00	Competition Part 4	✔	Discord
16:00 - 16:30	Final Scoring & Jeopardy	✖	Discord
16:30 - 17:00	Debriefing	✖	Zoom
17:00 - 17:30	Closing Ceremony	✖	Zoom

Team Identification

Blue Team

This is you! Your primary objective is to defend your network to maintain **service uptime** and complete assigned **injects**. There are also **King of the Hill** and **CTF** challenges for you to compete in. All of this is factored into the **game** component of the competition. While this is all happening, you may also attack other teams' networks.

Red Team

This group of industry professionals attack your network with the ultimate goal of helping you learn more about the systems you defend. The Red Team will also participate in KotH, the CTF, and other parts of the competition, but they are not competing against you.

White Team

These hardworking volunteers are the glue that holds the competition together. Some of them assisted black team members in the lead up to the competition, and will help out during the competition by answering questions, grading injects, managing the store, and oh so much more.

Black Team

The Black Team is a subset of the White Team. They are the leaders who have overseen the creation of the various elements of the competition.

E-Board

RITSEC E-Board members manage the administrative side of the competition. Direct administrative questions towards them.

Sponsors

These individuals represent the organizations which have so generously donated the resources that make this event possible. They may assist you in your efforts and may also talk to you about opportunities with their organizations.

Rules

1. This competition exists for **fun** and **learning**.
   Do not break the spirit of the competition.

2. Be respectful towards **all** people involved with the competition.

3. The White Team exists to help you.
   Do not attempt to deceive or otherwise lie to the White Team.

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

5. **Do not** impersonate a Sponsor or a member of the White Team.

6. **Do not** perform any competition-related actions during periods designated as “Hands Off” on the schedule.

   a. **Do not** interact with any competition infrastructure.

   b. **Do not** attack any other team.

   c. “Hands Off” periods are subject to change pending an announcement by the Black Team

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

7. Anyone **not registered as a Blue Team member** may not contribute in any way to your team's efforts within the competition.

   a. All CTF challenges must be completed by a registered member of **your** team.

   b. All Quests must be completed by a registered member of **your** team.

   c. All interactions with the competition on behalf of **your** team must be performed by a registered member of **your** team.

   d. Spectators **may not** assist competitors in any way.

8. **Do not** share any point-earning information with **any** other team.

9. Quests **may** be written and submitted on your host machine.

10. **Do not** change scored topology without written White Team approval.

    a. **Do not** change the underlying technology of scored services without written White Team approval.
    b. **Do not** change the machine that a scored service is on without written White Team approval.

11. **Do not** attack out of scope infrastructure

    a. In Scope

    - i. 172.16.x.0/24 (x ≥ 1)
    - ii. 10.x.1.0/24 (x ≥ 1)
    - iii. 192.168.0.0/16 (KotH)

    b. Out of Scope

    - i. 172.16.0.0/24 (management network)
    - ii. 172.24.0.0/24 (management network)
    - iii. 172.28.0.0/24 (management network)
    - iv. 172.16.248.0/22 (Red Team/scoring network)
    - v. *.ists.io
    - vi. *.ritsec.cloud (including openstack accounts)
    - vii. RITSEC hardware
    - viii. network based denial of service attacks
    - ix. anything not listed as in scope

12. Black Team reserves the right to modify the definition of “scope” at any time.

13. Prestaging **is allowed**.

14. **Do not** use malware that is found online or in the wild

    a. You **may** use popular tools such as Metasploit.

    b. You **may** use custom malware if the source code can be provided and behaviour thoroughly explained.

    c. **Do not** download Malware from sites such as VirusTotal.

15. **Do not** remove any artifacts from the competition environment.

    a. **Do not** upload artifacts to VirusTotal or similar sites.

16. Violation of **any** of the above rules will result in a penalty at the discretion of the White Team.

Scoring

Breakdown

Component	Weight
Service Uptime	30%
Quests	30%
King of the Hill	15%
Capture The Flag	15%
Game	10%

Visibility

During the competition, you will be able to view your team's current scores for Service Uptime, King of the Hill, and Capture the Flag, and Game components through their corresponding web portals:

Uptime:	Scorestack	https://scoring.ists.io
KotH:	Scorestack	https://scoring.ists.io
CTF:	CTFd	https://ctf.ists.io
Game:	Game Webpage	https://game.kokka.jp

Sites on the ists.io domain are accessible outside of the competition environment, and may be accessed at any time.

Quests will be graded by the White Team and the scores will be returned 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.

Welcome

Welcome brave samurai,

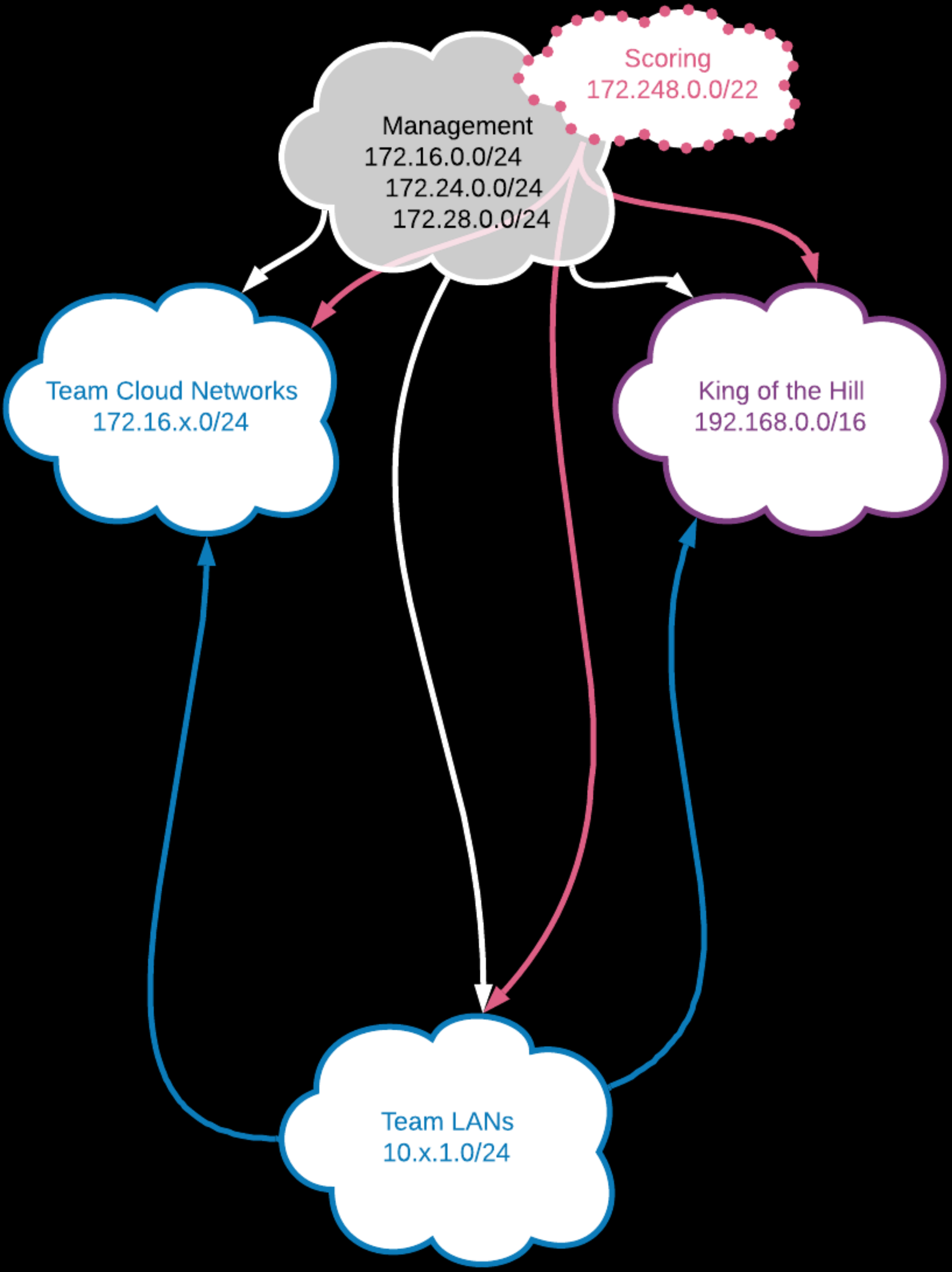
I have recruited you to defend my network from my rival shoguns and the meddlesome ninjas wreaking havoc on our networks, and to manage my assets. My daimyo and I have compiled a full description of each of your duties which you will find below. They are not small tasks, but I trust that you will be able to complete them diligently.

Together, we will elevate IkiruCorp to its rightful place at the top. I will claim my throne, and you will be well compensated.

Regards,

Mr. Kumichō,
Shogun, IkiruCorp

Competition Topology

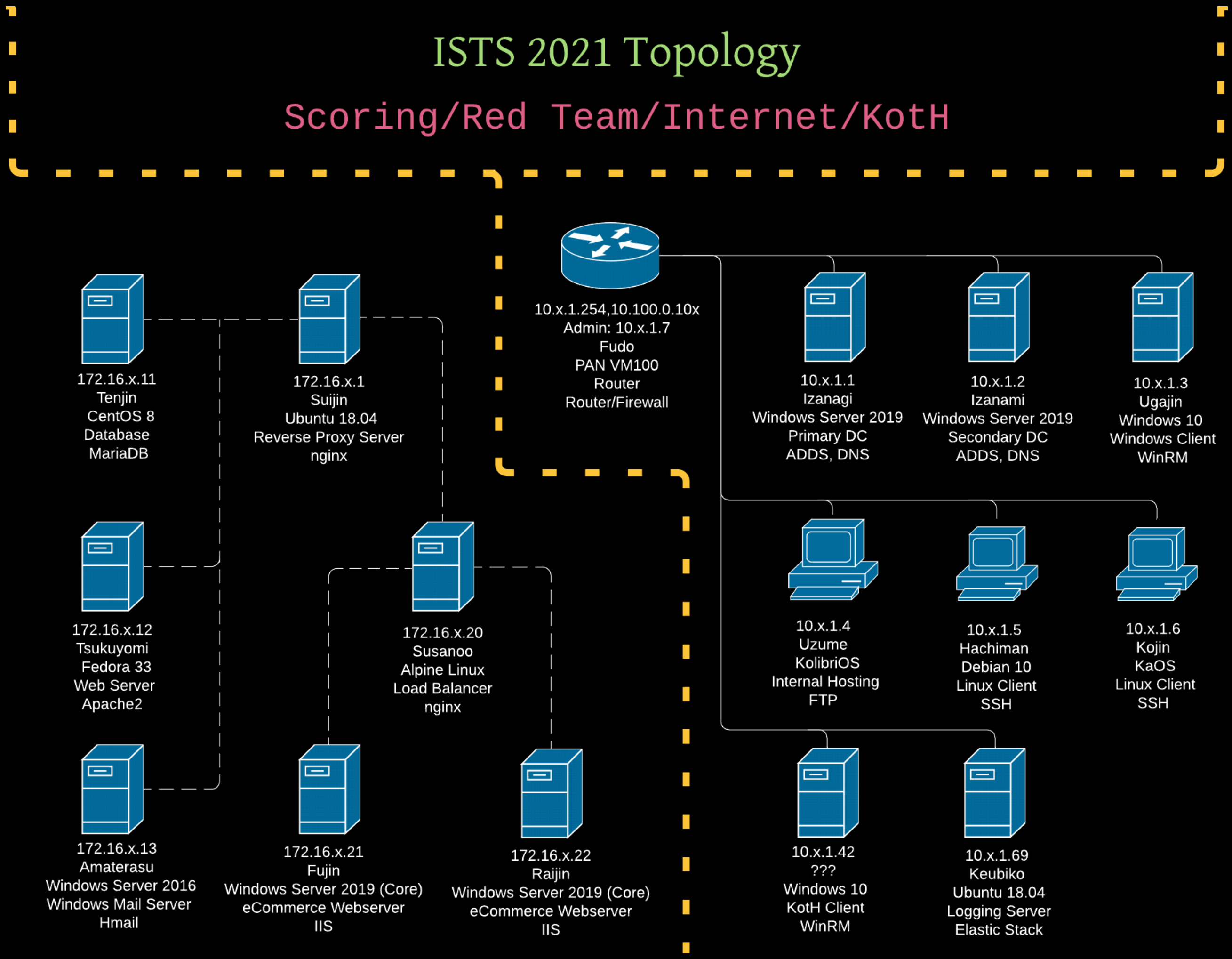


Network Topology

These are the two networks you will be defending and maintaining. The daimyos and I have carefully crafted this topology to be as comprehensive as possible.

Your LAN contains the internal services such as Active Directory, a logging host, a network firewall, and client hosts. The hosts on this network will be accessible via the Openstack console.

Your WAN contains public facing sites and can only be accessed remotely via SSH, WinRM, etc.



Scoring Service Uptime

Services

Hostname	IP Addresses	Operating System	Services	Scored
LAN				
Izanagi	10.x.1.1	Windows Server 2019	WinRM, LDAP, DNS	✔
Izanami	10.x.1.2	Windows Server 2019	WinRM, LDAP, DNS	✔
Ugajin	10.x.1.3	Windows 10	WinRM	✔
Uzume	10.X.1.4	Kolibri OS	FTP, ICMP	✔
Hachiman	10.x.1.5	Debian 10	SSH	✔
Kojin	10.x.1.6	KaOS	SSH	✔
Fudo	10.x.1.7 10.x.1.254 10.100.0.100 + x	PANOS	Routing	✖
???	10.x.1.42	Windows 10	WinRM	✖
Keubiko	10.x.1.69	Ubuntu 18.04	Logging	✖
Cloud				
Suijin	172.16.x.1	Ubuntu 18.04	HTTP	✔*
Tenjin	172.16.x.11	CentOS 8	MariaDB	✔
Tsukuyomi	172.16.x.12	Fedora 33	HTTP	✖*
Amaterasu	172.16.x.13	Windows Server 2016	Mail	✔
Susanoo	172.16.x.20	Alpine	HTTP	✖*
Fujin	172.16.x.21	Windows Server 2019 Core	HTTP	✖*
Raijin	172.16.x.22	Windows Server 2019 Core	HTTP	✖*

* Fujin and Raijin are “load balanced” by Susanoo, which is reverse proxied by Suijin, as is Tsukuyomi. Scoring checks for HTTP will only be sent to Suijin, but all HTTP hosts must function properly for all checks to pass.

Access

As mentioned above, the only hosts you will have direct console access to are those in your team’s LAN. This access will be through our Openstack cloud console, hosted at https://stack.ritsec.cloud.

The credentials needed to access different components of the infrastructure, along with the rest of your team’s passwords needed to access and interact with the various components of the competition, will be placed into your team’s *#team-xx-safe* channel at minute 0 of the competition. All users on your network will use your team infrastructure password by default.

Scoring

Service uptime will be determined using the automated scoring engine *Scorestack* (https://github.com/scorestack/). You 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.). You will be able to see a live scoreboard of each teams’ scores, as well as view logs detailing the reasons a service check failed. *Scorestack* will be hosted at https://scoring.ists.io.

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.

Users

DOMAIN USERS:

Administrators

TokugawaIemitsu
HojoSadatoki
AshikagaTakauji
MinamotoNoSanetomo

Users

TokugawaHideyoshi
WatanabeKazan
EraFusahide
NagaoHarukage
TokiYorinari
YamauchiKazutoyo
TaigenSessai
WadaShinsuke
EnomotoTakeaki
NaoeKagetsuna
TakedaShingen
YamadaArinobu

LINUX USERS:

Administrators

jimmu
suizei
annei
itoku

Users

kinmei
bidatsu
yomei
sushun
suiko
jomei
kogyoku
kotoku
saimei
tenji
kobun
jito
monmu
geme

Service Users

Wordpress:

wordpressuser and host superusers

Nopcommerce:

Admin

Database

wordpress
nopcommerce

Quests (Injects)

While defending our network is a time consuming and important task, it is not, of course, your only duty — we are trying to build an empire after all. The daimyo and I will periodically task you to perform administrative tasks integral to the stability of our services.

Receiving and Submitting

Quests will be released in the *#white-team-quests* channel on the ISTS 2021 Discord server.

Quest submissions will be made via your *#team-xx-quests* channel unless otherwise stated.

General questions about quests should be asked in the *#white-team-questions* channel. Questions that contain scoring concerns or sensitive information should be asked in your *#team-xx-general* or *#team-xx-safe* channels.

Quest Rubric

On-Time	25%	Submit by the due time. Quests will be accepted after the due time, but no points will be awarded for this criteria. If you cannot complete a quest you must inform the Quests Division or request an extension (within reason, including an explanation).
Professionalism	25%	Follow the competition lore, address the daimyo and I properly, and make your deliverables easy to understand.
Technical Details	50%	Respond with the requested items in the format specified. A breakdown of expected items may be provided.

A more comprehensive quests guide will be released shortly before the beginning of the competition.

King of the Hill (KotH)

The King of the Hill network (192.168.0.0/16) is your chance to prove yourselves as the superior fighters in the kingdom. All of your cunning and skill will be needed to infiltrate and control the network. Each team will be given a host on their LAN with special relationships to the KotH network, however the KotH network is accessible from anywhere in the competition.

Scoring

All King of the Hill boxes will have two scored services (HTTP). The scoring engine will perform regular checks to verify that the scored service is operating properly and to check ownership of the box. Your team will receive a KotH token in your *#team-xx-safe* channel alongside your credentials. This token string will be used to claim ownership of KotH hosts checks.

Ownership

For your team to own a host (and get points for owning that box), you must place your team's KotH token in the specified location for that host. The service must continue to operate properly in order for your team to earn points from the host.

HTTP

Replace the token in the **ownership.html** file with your team's KotH token to claim ownership of the host.

Capture the Flag (CTF)

These challenges are an opportunity for you to demonstrate your skill as capable warriors. While they may not be directly related to your duties, they will help you curry favor with the nobles and win over the people’s hearts.

Do not let these challenges distract you from your other responsibilities; you have a network to defend!

Access

Your team will be given credentials to log into the CTFd instance hosted at https://ctf.ists.io.

Categories

The CTF will have four 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 web service related challenges
- Crypto: all things cryptography
- BinEx: binary exploitation - make the program give you your flag
- Forensics/Reversing: trace back the steps and solve the mystery

Game

The digital world is not the only front that needs defending, we also must defend our assets in the physical world. You are the commanders of my – now our – army. You must build up our army to defend our interests and gain the power needed to place IkiruCorp at the forefront. In order to build the strongest army possible, you will need to acquire funds through the other components of the competition. I trust that you will take good care of our Soldiers.

Components

The game website will be hosted at https://game.kokka.jp. It has a market and a map component, through which you will control the various aspects of the game once you have authenticated.

You will receive credentials to log into your game account at the beginning of the competition.

Market

The market is the competition storefront. It is here that you will be able to hire mercenaries and purchase other services to aid you in the competition. These services relate to the infrastructure, red team, or can serve as a fun diversion. The market is also the place where you can redeem the tokens you acquire from the other parts of the competition for the in game currency. If you are feeling generous or want to pool resources with another team, there is also the option to share funds through the marketplace. The amount of money in the economy is not infinite, so manage our funds wisely.

Map

The map is where you can control troop movements. Each team (including the Red Team) will have a territory on the map and there is one special territory owned by the Emperor. During each round of the game, battles will take place in all territories that were attacked.

Rules

Economy

Currency

The currency in the game is called BitRyo. It is the only form of payment accepted in the market. You will start with 10000 BitRyo, and there are four ways to obtain additional BitRyo:

1. Taxes during the upkeep phase of each round
2. Pillaging another territory after winning a battle as an attacker
3. Redeeming a token acquired from the competition environment
4. Receiving a gift from another team

Tokens

Tokens are earned through participation in various aspects of the competition. Once your team has acquired the token it can be redeemed on the market page of the game site. There are four types of token, each with different methods of acquisition and different values.

CTF Tokens are obtained by solving CTF challenges. They are the flag which you submit to CTFd. CTF Tokens are redeemable **once per team**.

Value: 20,000 BitRyo

Purple Team Tokens are hexadecimal strings which are hidden in files with dubious names on each host in each Blue Team network (except the router). You will not be able to redeem your own purple team tokens until the second day of competition, so if you find them, keep them safe. Purple Team Tokens are redeemable **once for the whole competition.**

Value: 25,000 BitRyo

Sponsor Tokens are held by our wonderful sponsors! Go talk to them and they might just share their tokens with you! Sponsor tokens are redeemable **once per team**.

Value: 50,000 BitRyo

KotH Tokens are hexadecimal strings which are hidden in files with dubious names on each KotH host. Each of the 15 KotH Tokens is redeemable only **once for the whole competition**.

Value: 75,000 BitRyo

Army

Our army is a fine one, but nowhere near powerful enough to rule the world. You will start the game with control over 5000 troops. Troops can either attack or defend a location. Any troops remaining in our territory when combat begins will defend it.

Rounds

A round lasts for one hour of real world time and consists of three phases: an upkeep phase, a preparation phase, and a battle phase.

Upkeep Phase

This phase will happen almost instantaneously at the beginning of the round. During this phase you will collect a tax of 10,000 BitRyo from our territory, half of which will be ruthlessly taken by the Emperor. This will leave you with 5,000 BitRyo, and the emperor with 5,000 BitRyo **for every team in the competition**.

Preparation Phase

The preparation phase lasts for the duration of the round. During the preparation phase, you may take the following actions:

- Redeem tokens for BitRyo at the market
- Purchase market items using your BitRyo
- Transfer funds to another team
- Send troops to attack another territory
- Send troops to defend another territory

Note that there is no movement time for units, this is the future after all, and we are not as limited by the bounds of space and time as you may be used to. Your troops can be deployed to any territory on the map, and will warp there to take part in combat.

Battle Phase

The battle phase will happen almost instantaneously at the end of the round. All troops that are not sent to another territory will defend your territory. The results of the battle in each territory of the map will be calculated, and the resulting changes to funds and army losses will be applied. Once this is done, the next round will begin.

Emperor's Palace

The Emperor's Palace is a special territory which is not controlled by a team. It accrues a large sum of money each round as the Emperor collects taxes from each team.

The Emperor's Palace has a formidable army of 200,000 Soldiers protecting it. It will be some time before you are able to challenge his might, but when you can, it will certainly be worth it! After each battle, the Emperor will replenish his army.

Battle System

Each round, you will have the ability to send your armies to invade other territories on the map. At the end of the round, a battle will take place; to the victor go the spoils.

There are three possible outcomes to a battle:

Attacker Troops > Defender Troops → Attacker Victory
Attacker Troops < Defender Troops → Defender Victory
Attacker Troops = Defender Troops → Draw (Both Lose)

The winner of a battle will lose 10% of the troops they sent into battle unless the opposing force is less than 10% of the victor, in which case the winner will lose one unit per unit the loser sent to battle. If the winner attacked the loser, they will pillage 10% of the loser's BitRyo. In the event that multiple attackers successfully defeat a defender, the rewards will be split between the attackers proportionally to their contribution to the attacking force.

The loser of a battle will lose 15% of the troops they sent into battle. If the loser was the defender, they would lose a total of 15% of their BitRyo as a result of the loss.

For example, given a defender with 2,020 BitRyo and 100 troops defending, and two attackers sending 51 and 50 troops respectively, the attackers would win since their 101 troops outnumber the 100 troops of the defender. The attackers would pillage 202 BitRyo from the defender, 102 of which would go to the first attacker, and the remaining 100 to the second attacker. The defender would lose an additional 101 BitRyo, totalling 303 BitRyo in losses, and ending with a total of 1,717 BitRyo. The defender would lose 15% of their troops, leaving them with 85 troops remaining. The attackers would lose 10% of their troops, resulting in 46 troops returning to attacker 1, and 45 troops returning to attacker 2.

See the table below for a more succinct breakdown of this example battle.

Defender Troops	Defender Funds	Attacker Troops		Attacker Funds	
Before Battle					
100	2020 BR	51	50	0 BR	0 BR
After Battle					
85	1717 BR	46	45	102 BR	100 BR

Scoring

Scoring for the game will be based on 2 factors: our army's strength compared to the Emperor's army, and our army's strength compared to those of the other teams.

If our army is superior to the Emperor's army, your team will receive 5 points.

The remaining 5 points are based on where our army ranks compared to other armies. Armies in the 25th percentile will receive 1 point each, the 50th percentile will receive 2 points each, the 75th percentile will receive 3 points each, and the top 25% will receive 4 points each. The team with the strongest army will receive one additional point, putting them at 5 points.

These two criteria will be combined for a maximum of 10 points.

“

It's not DNS

There's no way it's DNS

It was DNS

-SSBroski

”