ISTS 16

Blue Team Packet

Hosted by **SPARSA**

February 2nd - 4th, 2018

Table of Contents

Thank you to our Sponsors!

Gold

indeed®
How the world works.™

United Technologies
Climate | Controls | Security

PARSONS
CYBER

Silver

information security

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

twitch

BLACK HILLS
Information Security
CELEBRATING 10 YEARS
•2008-2018•

CS
CARVE SYSTEMS, LLC

COMPUTING
SECURITY

MITRE

B★G

Bronze

MWR
INFOSECURITY

FACTSET

Schedule

Friday - 2/2/2018

5:00 PM	Golisano Auditorium (1400)	Welcome and Introduction
5:15 PM	Golisano Auditorium (1400)	Keynote given by speaker David Merkel
6:15 PM	Golisano Auditorium (1400)	Speaker Q&A
6:30 PM	Golisano Auditorium (1400)	Competition Overview and Information

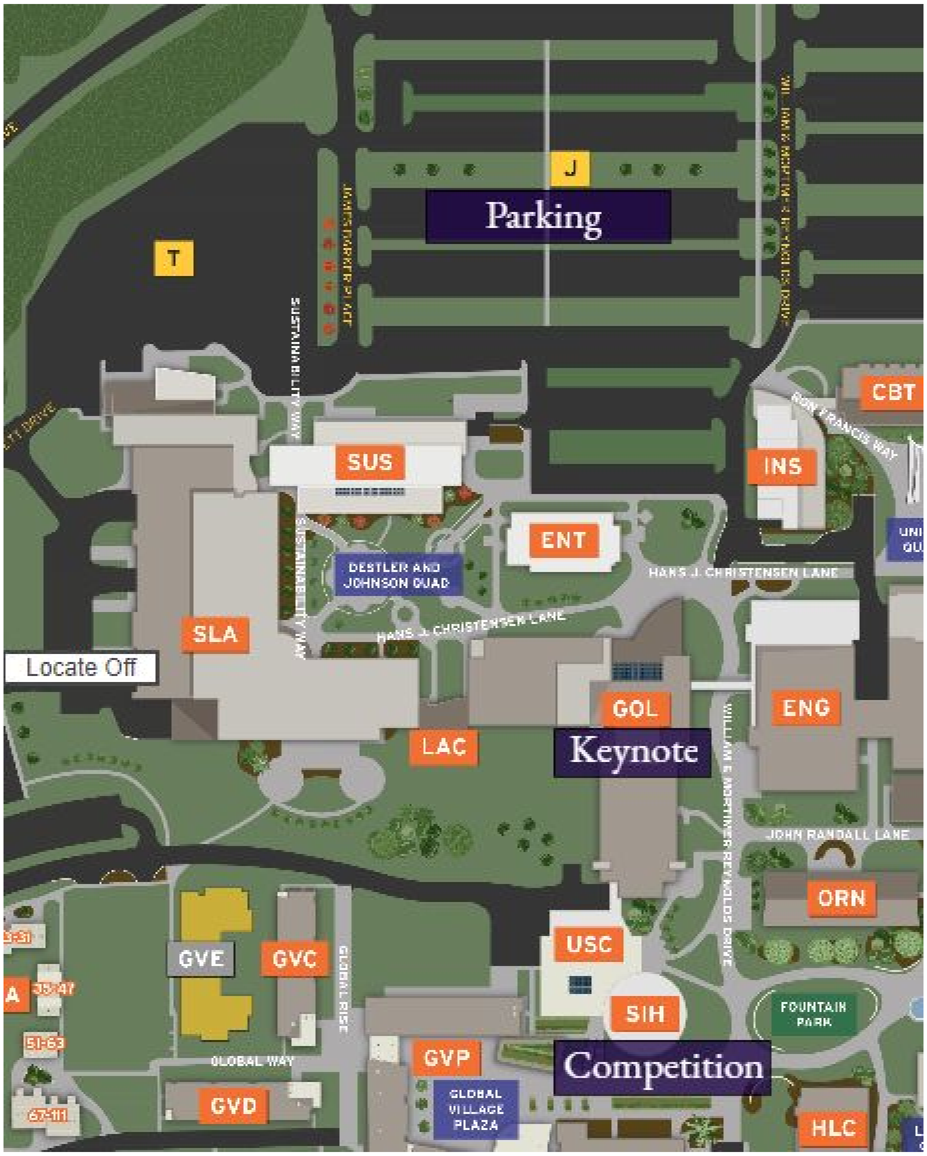
Saturday - 2/3/2018

8:00 AM	Student Innovation Hall	Breakfast
9:00 AM	Student Innovation Hall	Competition Start
12:00 PM	Student Innovation Hall	Catered Lunch
6:00 PM	Student Innovation Hall	Competition End
7:00 PM	Salsaritas	Mixer!

Sunday - 2/4/2018

8:00 AM	Student Innovation Hall	Breakfast
9:00 AM	Student Innovation Hall	Competition Start
12:00 PM	Student Innovation Hall	Catered Lunch
2:00 PM	Student Innovation Hall	Competition End, Score Calculation & Jeopardy
2:30 PM	Student Innovation Hall	Team Debriefs
3:00 PM	Student Innovation Hall	Final Ceremony

Location



The keynote presentation will take place in GOL-1400, which is the auditorium inside of the GOL atrium. The remainder of the competition will take place in the Innovation Hall, which is connected to the building, and can be reached by walking down the hall to the right of the auditorium. The mixer will take place at Salsaritas, which is located right outside of the Student Innovation Hall. Please check https://maps.rit.edu for more information on how to get around campus.

Team Identification

Blue Team

This is you and your team. You are responsible for defending the network you're given, completing business critical tasks (injects), and making sure that your services are always reachable. It is expected that you defend your services in a realistic way, and so occasionally manual checks may be conducted to verify that your systems are working as intended, and are not scoring without functioning.

Black Team

Black Team is composed of leadership roles that oversaw the creation and development of different areas of the competition. Each team lead is a subject matter expert in the area that they were assigned, and is responsible for a group of White Team volunteers. They are identified by the black shirts that they are wearing, which will indicate the competition area that they are responsible for. Red Team will under no circumstances impersonate a Black Team member.

White Team

White Team is the backbone of the competition, and without their efforts the competition would not be possible. During the event, White Team members will be identified by the white shirts that they are wearing, however occasionally they might just be in casual clothing, so don't be too thrown off if this is the case. White Team should be your main point of contact for any questions or competition related issues. If you need to contact them, you may either call, or walk over to the service desk.

Red Team

Red Team is a band of industry professionals that are trying to help you learn and grow by attacking your infrastructure. Many refer to this style of competition as a Red vs. Blue competition, however you are not competing against Red Team. They just exist to facilitate an environment like no other, and to help you gain meaningful experience. Many of our Red Team members are sponsors who help us run the event, and so please feel free to talk with them.

Rules

1. The competition exists for fun and for learning, do not break the spirit of the competition.
2. Be respectful of all people involved with the competition.
3. Do not change the underlying technology that the services are scored on without written White Team approval.
4. Do not change the machine that a scored service is on without written White Team approval.
5. Do not attack infrastructure that is not operated by another Blue Team.
6. You may attack King of the Hill services and virtual machines.
7. Never attempt to impersonate a Competition Official or Sponsor.
8. All challenges must be completed by a registered member of your team.
9. Any interactions with the competition on behalf of your team must be performed by a registered member of your team.
10. You may not share point-earning information (CTF flags, etc.) with any other team.
11. Do not use malware that is found online or in the wild. Custom written malware, and popular tools such as Metasploit and Powershell Empire are allowed, however malware downloaded from sites similar to VirusTotal is prohibited. You should have the source code to the malware, or be able to describe in detail what it does.
12. Do not perform any competition related actions during "hands-off" time periods. This includes, but is not limited to:
    - ➢ Interacting with any competition infrastructure.
    - ➢ Attacking any other team (physical and technical attacks included).

    Predefined "hands off" time periods include:
    - ➢ Before the competition has started on any given day.
    - ➢ During the lunch period of the competition on any given day.
    - ➢ After the competition has stopped on any given day.
13. 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.

Scenario

In this year's competition, you will be defending *STARSA*, a space mining company. *STARSA* makes the majority of its profits from selling raw materials that it mines from distant planets. Occasionally, *STARSA* will need to escort a shipment of materials to one of its facilities, and so it also operates spaceship manufacturing plants, to help defend its shipments against competing miners and the space raiders. Without these spaceship manufacturing plants, *STARSA* has no way to protect its resources and wouldn't be able to make credits easily. Recently, the executive team from central command received reports of space raiders breaking into their facilities, attempting to steal both spaceships and credits from their stores. They insist that their use of the most modern technologies should make it easy for them to be secure, but they've hired you just to make sure. Your mission is to defend *STARSA* against space raiders and competitors, and to investigate recent incidents using the modern tooling that has already been configured.

Welcome

Subject: Welcome

Welcome!

We’re glad we were able to hire y'all so quickly, sure can be hard to find good talent all the way out here. Now I know the other execs tend to exaggerate sometimes, but I tell ya something dusty is going on out there. I was overseeing an escort mission last week, and I saw more space raiders than I’d ever seen in my life. They’re getting more organized, and must be stealing from our supplies. The dust is blowing on the far side of the galaxy, I can feel it. Once you’re settled in, let’s talk.

Signed,

Thomas Sherman

Chief of Mining Operations (CMO), *STARSA*

Initial Credentials

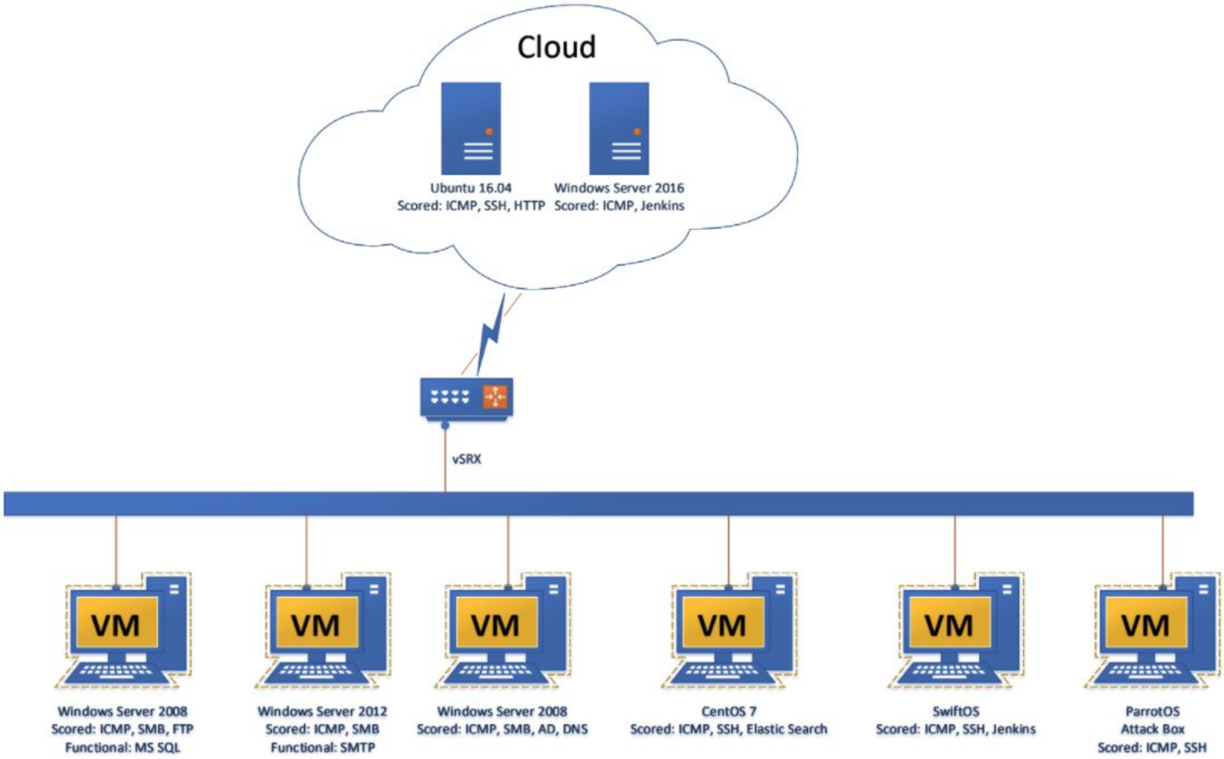
VCenter	teamX@whiteteam.ists	**Handed out at start of competition.**
Linux Machines	root	Changeme-2018
Windows Machines	Administrator	Changeme-2018
Web Applications	admin	Changeme-2018
Databases	root	Changeme-2018
When in doubt	root / admin / Administrator	Changeme-2018

Should your VCenter credentials not work, please contact a White Team member to assist you.

Competition credentials may be changed since you receive this packet, so an updated credentials sheet will be provided for you at the start of the competition.

Should any other credentials not work, please figure it out and protect our network!

Topology


Cloud
Ubuntu 16.04
Scored: ICMP, SSH, HTTP
Windows Server 2016
Scored: ICMP, Jenkins
vSRX
VM
Windows Server 2008
Scored: ICMP, SMB, FTP
Functional: MS SQL
VM
Windows Server 2012
Scored: ICMP, SMB
Functional: SMTP
VM
Windows Server 2008
Scored: ICMP, SMB, AD, DNS
VM
CentOS 7
Scored: ICMP, SSH, Elastic Search
VM
SwiftOS
Scored: ICMP, SSH, Jenkins
VM
ParrotOS
Attack Box
Scored: ICMP, SSH

Specifications

System	IP Address	Scored Services
SwiftOS	10.2.X.10	ICMP, SSH, Jenkins
Windows FTP	10.2.X.20	ICMP, SMB, FTP
Windows 2012	10.2.X.30	ICMP, SMB Mail used for injects
Windows AD	10.2.X.40	ICMP, SMB, AD, DNS
CentOS 7	10.2.X.50	ICMP, SSH, ElasticSearch
Parrot OS	10.2.X.60	ICMP, SSH
☹◆■♋	♒❍✍	⌖♏♌ 🌢♍♋●♏
Ubuntu 16	10.3.X.10	ICMP, SSH, HTTP
Windows 2016	10.3.X.20	ICMP, Jenkins
vSRX	10.2.X.254 10.3.X.254	N/A

Subject to Change

Injects

Overview

This year we are taking a different approach to injects at ISTS. We wanted to avoid giving injects that instruct teams to configure tools or services for an inject, and then have them turn it off immediately afterwards. We're aiming to provide you with meaningful security-focused injects that have you utilize tools that have already been configured.

Important Technologies

The infrastructure is a bit more advanced than it has been in the past. We are therefore providing a non-complete list of technologies that teams should have an understanding of before competing this year:

- OSQuery
- Zentral & ElasticSearch
- OSSec
- Tripwire
- Active Directory & Kerberos Authentication
- Configuration management tools like Ansible or Puppet
- Continuous Integration tools like Jenkins
- Docker

Questlines

Injects will be given out in our new "Questline" format. Throughout the competition, White Team will provide you with "Baseline" injects that will have a time limit associated with them. After the Baseline inject is completed, teams will then receive additional related injects that build off of the Baseline inject. These additional or "Questline" injects have no deadline, and should be completed by the end of the competition. If a Team fails to complete a Baseline inject, they may still attempt to complete additional Questline injects, however many of the Questline injects may require the Baseline inject to be completed successfully. This means that teams will likely need to complete the Baseline inject before being able to pursue additional Questline Injects.

Receiving & Submission

Injects should be submitted to **injects@whiteteam.ists**
Injects will be sent to your mail server at **injects@tauri.teamX.ists**
If your mail server is not functional, you will need to contact White Team directly for injects, and will receive a small penalty for doing so.

King of the Hill

Overview

King of the Hill is a new component that we're adding to ISTS this year, that will have a strong focus on evaluating a team's ability to break into systems. As servers come online, teams will need to break into them and overwrite a file on the system with their team identifier. The flags will be checked by a King of the Hill scoring engine, and points will be awarded to the dominating team. Each server will be available for approximately an hour, but the duration is subject to change. We encourage teams to be creative with their defense of the machines once compromised.

Scenario Information

Each King of the Hill server is a new planet that has been discovered by *STARSA*, and the executives from Central Command would like you to defend the new mining sites they set up. The longer you can defend the sites, the more points your team will earn.

Capture the Flag

Overview

The CTF this year will be hosted in DigitalOcean, and you may work on the challenges at any point after the competition starts, until the competition ends. However, you will not be able to complete "Attack Challenges" outside of the competition hours, as this requires access to the competition infrastructure. Teams are ***not*** allowed to complete Attack Challenges during "hands-off" periods as defined in the rules above.

Categories

Attack Challenges

Note: You will receive these flags from a White Team judge after successful completion.

Web

Reversing

Cryptography

Misc

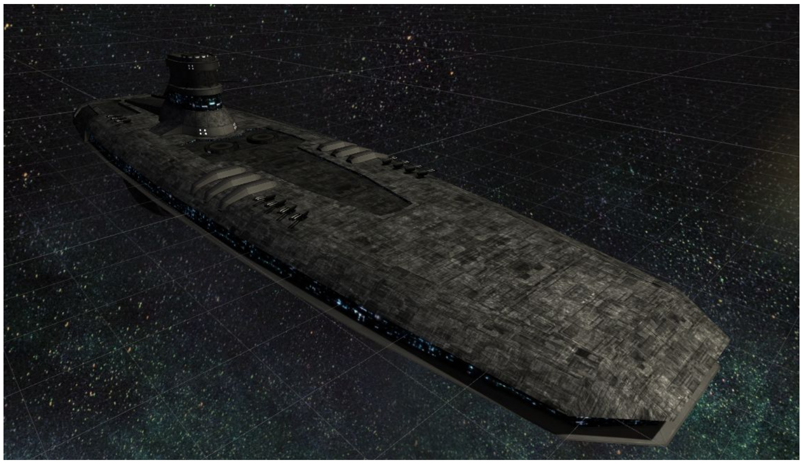
Space Escorts

Overview

Occasionally, STARSA will need to defend shipments of materials that are being transported back from distant planets. STARSA has two main ship building factories, located at Wolf and at Vega. As their builds complete, teams will be awarded with spaceships that may be used to defend their frigates that are transporting materials, and to attack other team frigates. These ships are completely expended during each Space Escort mission, and none will carry over into the next round. Space Escort missions will occur periodically throughout the competition, and are a chance for teams to earn more credits. The amount of credits that frigate's carry during a given round is left to the discretion of White Team. During an Escort mission, each team will also be able to choose one other team to attack.

Ships

Frigate



The frigate is the main way STARSA is able to transport materials. Teams will receive credits based on the amount of health a Frigate has left at the end of a mission.

Health	200,000	**Speed**	0
Team Limit	1 ship	**Turn Speed**	0
Damage	1000	**Acceleration**	0
Fire Rate	3.5 shots per min	**Range**	750

Bomber

The Bomber is a primary offensive ship for STARSA, used to attack enemy Frigates. The Bomber will fly to be in range of a Frigate, and then proceed to attack it with devastating lasers until it is destroyed. Each team may choose a single team to attack, and the Bomber will attack that team’s Frigate.

Health	1,500	**Speed**	10 m/s
Team Limit	50 ships	**Turn Speed**	1
Damage	100	**Acceleration**	1 m/s^2
Fire Rate	30 shots per min	**Range**	200

Guardian

The Guardian is the only ship that stands in the way of enemy companies and the raiders. Designed for the sole purpose of protecting the frigate, this ship will patrol the Frigate looking for enemy ships to attack.

Guardian Specialty: +10% Health to all ships for each Guardian owned.

Health	1250	**Speed**	20 m/s
Team Limit	50 ships	**Turn Speed**	1.4
Damage	50	**Acceleration**	3 m/s^2
Fire Rate	200 shots per min	**Range**	50

Striker

The Striker is an offensive mercenary ship used by *STARSA* to protect their Bombers. It will follow a team's Bombers into battle, and assist by attacking enemy Guardians and Raiders. A Striker's goal is to buy time for it's Bombers, as it does not have the weaponry to pierce through a Frigate's shields. These ships are not built by *STARSA* and can only be obtained through the White Team store.

Striker Specialty: +5% Damage to all ships for each Striker owned.

Health	750	**Speed**	15 m/s
Team Limit	50 ships	**Turn Speed**	1
Damage	50	**Acceleration**	2 m/s^2
Fire Rate	120 shots per min	**Range**	50

Raider

The Raider is a ship constructed by Red Team, that attempts to destroy a team's guardians. Scientists know very little about this ship, as they are uncommon. However, there have been an increasing number of sightings in recent years...

Raider Specialty: ???

Health	????	**Speed**	?? m/s
Team Limit	??? ships	**Turn Speed**	??
Damage	????	**Acceleration**	?? m/s^2
Fire Rate	??? shots per min	**Range**	??

Ship Factories

STARSA operates two main ship building factories (Jenkins servers). Each time a Jenkins check passes, teams will be awarded with a spaceship. Wolf will produce “Bomber” type ships, and Vega will produce “Guardian” type ships. A third type of ship, “Striker”, will only be obtainable by purchasing it from the White Team store.

Additional Details

- Each round will have a maximum time limit.
- A round ends when all Frigates have been destroyed, or the time limit has been reached.
- Teams will only be awarded Credits if their Frigate survives.
- When a Team’s frigate is destroyed, so are the rest of their ships (Bombers, Strikers, etc.)
- Boosts and Sabotages will be purchasable from the White Team store.
    - Boosts will allow you to increase your ship Health, Damage, or Speed.
    - Sabotages will allow you to hinder an enemy team.
- White Team reserves the right to retry, modify, or nullify the simulation whenever necessary.
- To be clear, you earn ***Credits*** from Space Escort missions, ***not*** points.

Economy

Income

Your team has two sources of income this year. The first being the E-Commerce website that your team hosts. White Team will attempt to buy resources from your team, and if the transaction is successful you will earn some credits. The second source of income is from Space Escort missions, and as mentioned above the amount of credits earned is based on the remaining health of your Frigate.

White Team Store

The White Team store is the place for you to spend all the credits you've earned. You interface with this app through your ecommerce site. If your site is down, you may make purchases at the physical White Team service desk using the mag-stripe card provided to your team. Prices for items are subject to change at any time, based on availability and demand.

Bucket List

As always, the Bucket List is back again for teams looking to earn a little extra cash. Stop by the White Team service desk to ask what you might be able to do to earn some credits. Usually this would involve something like crab walking around the competition area, or singing the Canadian National anthem with the rest of your team.

Scoring

Breakdown

CTF	15%
King of the Hill	15%
Service Uptime	35%
Injects	35%

Methodology

This year’s competition will be using stateful checks to ensure services are online. For instance, we may write data to a database, or create a file somewhere on a server. The check will then verify that the state has been maintained, and pass or fail accordingly. This is in an attempt to stop scoring engine gamification by teams, as we feel it is deeply against the spirit of the competition. If the precautions we have taken are not able to fully prevent this sort of behavior, there will be point deductions based on the White Team’s judgement. Manual checks may be issued at any time by White Team to ensure that a service is functioning as intended if it is marked as scoring, and any discrepancies may result in a point deduction.

Thanks, and good luck!