IRSEC 2021

OCTOBER 2ND

RITSEC

Security Through Community

TABLE OF CONTENTS

THANK YOU TO OUR SPONSORS

IRSEC WOULD NOT BE POSSIBLE WITHOUT THEM!

DIAMOND

facebook

PLATINUM

CISCO

MITRE

SecurityRisk ADVISORS

GOLD

Miscreants®

SILVER

VINYL

INTRODUCTION

AFTER PROMETHEUS STOLE FIRE FROM ZEUS, THE KING OF THE GODS, A PLAN FOR VENGEANCE WAS EXACTED. PANDORA, THE FIRST MORTAL WOMAN, WAS MARRIED TO EPIMTHEUS, PROMETHEUS' BROTHER. AS A WEDDING GIFT, ZEUS PRESENTED AN ORNATE BOX WITH A SINGLE WARNING:

NEVER TO OPEN THE BOX.

AS THE YEARS WENT BY, PANDORA'S CURIOSITY GREW OUT OF CONTROL, AND SHE COULD NO LONGER HOLD BACK. ONE DAY, SHE TOOK THE BOX AND OPENED IT. ALL THE EVILS OF THE WORLD WERE RELEASED AT ONCE UPON HUMANKIND: WAR, FAMINE, DEATH, PAIN, AND REDTEAM.

BUT BEYOND ALL THESE TERRIBLE EVILS THAT WOULD TORMENT THE WORLD, ONE GOOD SPRUNG FROM THE BOX - HOPE. BY THE GODS, USE IT AS A LIGHT THAT SHINES THROUGH THE DARKNESS.

- A HUMBLE GUIDE

SCHEDULE

TIME	EVENT	HANDS-ON-KEYBOARD
8:00AM – 8:30AM	BLUE TEAM CHECK-IN	X
8:30AM – 9:30AM	WELCOME CEREMONY/KEYNOTE	X
9:30AM – 12:00PM	COMPETITION STARTS!	Y
12:00PM – 1:00PM	LUNCH / SPONSOR SOCIAL	X
1:00PM – 4:30PM	COMPETITION RESUMES!	Y
4:30PM – 5:30PM	IR REPORT TIME	Y
5:30 – 5:45PM	COMPETITION ENDS – BREAK	X
5:45PM – 6:15PM	RED TEAM DEBRIEF	X
6:15PM – 6:30PM	FINAL SCORES / PRIZES CEREMONY	X

COMPETITION TEAMS

BLUE TEAM (DEMI-GODS)

THIS IS YOU! YOUR PRIMARY OBJECTIVE IS TO DEFEND YOUR NETWORK TO MAINTAIN SERVICE UPTIME AND COMPLETE ASSIGNED INJECTS.

RED TEAM (GODS)

THE RIT RED TEAM HAS LAUNCHED AN OFFENSIVE AGAINST YOUR POSITION WITH THE ULTIMATE GOAL OF HELPING YOU LEARN MORE ABOUT THE SYSTEMS YOU DEFEND.

BLACK TEAM (UPPER PANTHEON)

THE BLACK TEAM ARE THE ORGANIZERS OF THE COMPETITION!

WHITE TEAM

THESE HARDWORKING VOLUNTEERS ARE THE GLUE THAT HOLDS THE COMPETITION TOGETHER. THEY ARE YOUR GO-TO FOR PRETTY MUCH EVERYTHING! THEY WILL HELP DURING THE COMPETITION BY ANSWERING QUESTIONS, GRADING INJECTS, MANAGING THE STORE, AND MUCH MORE.

E-BOARD

RITSEC E-BOARD MANAGES 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. "Hands Off" periods are subject to change pending an announcement by the Black Team
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 Quests must be completed by a registered member of **your** team.
    b. All interactions with the competition on behalf of **your** team must be performed by a registered member of **your** team.
    c. Spectators **may not** assist competitors in any way.
8. **Do not** share any point-earning information with **any** other team.
9. Injects **may** be written on your host machine.

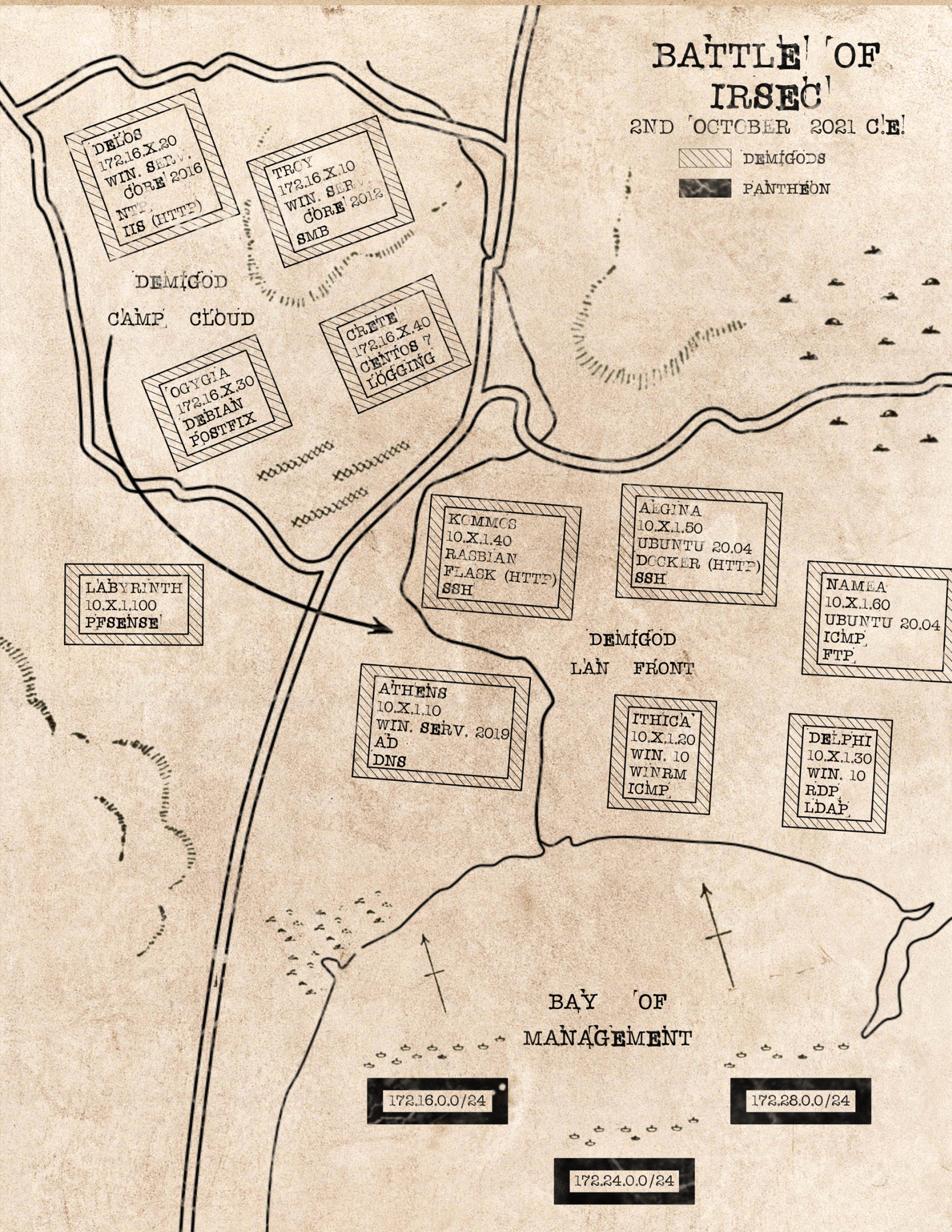
10. **Do not** change scored topology without written White Team approval.
    a. **Do not** change the underlying technology of scored services without written White Team approval.
    b. **Do not** change the machine that a scored service is on without written White Team approval.
11. Prestaging **is allowed** with both of these conditions:
    a. All scripts must be submitted to White Team through the Discord by the Wednesday before the competition (September 29th)
    b. All pre-staged tools must be publicly available
12. **Do not attack any team. This is an incident response-based competition. Any team found carrying out offensive attacks will be disqualified.**
13. **Do not** remove any artifacts from the competition environment.
    a. **Do not** upload artifacts to VirusTotal or similar sites.
14. Here is a quick list of technologies that are not allowed:
    a. Snapshots through Openstack are not allowed.
    b. The use of an Antivirus is not allowed.
15. Violation of **any** of the above rules will result in a penalty at the discretion of the White Team.

SCORING BREAKDOWN

COMPONENT	PERCENTAGE
UPTIME	35%
INJECTS	35%
INCIDENT RESPONSE REPORT	30%

HOW TO VIEW SCORING

Live scoring will be available at scoring.irsec.club throughout the competition. This score will reflect your current uptime score. This competition will utilize ScoreStack. There will be two dashboards to give you information about your score. The first will contain information about all the teams, and the second will showcase your team's score checks. There will be additional information displayed about the scoring checks on the team dashboard. There will be a quick ScoreStack demo before the competition begins!


BATTLE OF IRSEC
2ND OCTOBER 2021 CE
DEMIGODS
PANTHEON
DELOS
172.16.X.20
WIN. SERV. CORE 2016
NTP
IIS (HTTP)
TROY
172.16.X.10
WIN. SERV. CORE 2012
SMB
DEMIGOD
CAMP CLOUD
CRETE
172.16.X.40
CENTOS 7
LOGGING
OGYGIA
172.16.X.30
DEBIAN
POSTFIX
KOMMOS
10.X.1.40
RASBIAN
FLASK (HTTP)
SSH
AEGINA
10.X.1.50
UBUNTU 20.04
DOCKER (HTTP)
SSH
NAMEA
10.X.1.60
UBUNTU 20.04
ICMP
FTP
LABYRINTH
10.X.1.100
PFSENSE
DEMIGOD
LAN FRONT
ATHENS
10.X.1.10
WIN. SERV. 2019
AD
DNS
ITHICA
10.X.1.20
WIN. 10
WINRM
ICMP
DELPHI
10.X.1.30
WIN. 10
RDP
LDAP
BAY OF MANAGEMENT
172.16.0.0/24
172.28.0.0/24
172.24.0.0/24

SCORED SERVICES

X = YOUR TEAM NUMBER

HOSTNAME	IP ADDRESSES	OPERATION SYSTEM	SERVICES	SCORED
LAN				
Athens	10.x.1.10	Windows Server 2019	AD/DNS	Y
Ithaca	10.x.1.20	Windows 10	WinRM, ICMP	Y
Delphi	10.x.1.30	Windows 10	RDP, LDAP	Y
Kommos	10.X.1.40	Raspberry Pi	SSH, Flask(HTTP)	Y
Aegina	10.x.1.50	Ubuntu 20.04	SSH, Docker(HTTP)	Y
Namea	10.x.1.60	Ubuntu 20.04	ICMP, FTP	Y
Labyrinth	10.x.1.254 10.100.0.100 + x	pfSense	Routing	X
CLOUD				
Troy	10.x.1.10	Windows Server 2016	SMB	Y
Delos	10.x.1.20	Windows server 2016	NTP, IIS(HTTP)	Y
Ogygia	10.X.1.30	Debian	Postfix	Y
Crete	10.x.1.40	Centos 7	ELK	Y

ACCESSING THE INFRASTRUCTURE

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 distributed to your team via a messenger at the start of the competition. All users on your network will use the same 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.irsec.club/

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.

ACCOUNTS

DOMAIN USERS:

ADMINISTRATORS

ACHILLES
OEDIPUS
ODYESSEUS
PARIS

USERS

ACETAEON
DAEDALUS
CLYTEMNESTRA
DIOMEDES
HIPPOTHOON

LOCAL USERS:

ADMINISTRATORS

AENEAS
HERACLES
PERSEUS
THESEUS

USERS

ICARUS
PHEOBE
EURYBARUS
ZAREX
ACADEMUS

INJECTS

THE TWELVE LABORS (INJECTS)

The Great Hero Heracles, the Son of Zeus and Alcmena, was punished by the jealous Hera for Zeus' infidelity. He was driven insane, and, in his craziness, he slaughtered his wife and children. Once he awoke from his state, he sought guidance from Apollo, who urged him to repent by spending 12 years in service to the Mycenaean King Eurystheus. The King gave Heracles 12 Labors to complete. The Labors given to Heracles were tasks deemed to be impossible, but the 12 Labors that you will complete will not be. Throughout the competition, you will be given administrative tasks that will bolster your defensive posture.

RECEIVING AND SUBMITTING

The Twelve Labors will be released in two locations:

a. On paper, distributed to each team

b. in the #white-team-quests channel on the IRSeC 2021 Discord server.

Reports of Completion will be made via a flash drive to the Oracle. The Oracle will be in the lobby, through an obstacle course. To submit your inject, you must go through the obstacle course. If you try to go around the obstacle course, you must visit Chiron before attempting to cross the obstacle course again

General questions about injects should be directed towards White Team. Questions that contain scoring concerns or sensitive information should be asked privately.

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 consul 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.

INCIDENT RESPONSE REPORT

At the end of the competition, your team will be given the opportunity to recount your adventures. You can write down your trials and tribulations against the Gods and your adventures in the Great Battle. Make sure to submit reports as you find artifacts of the battle so that the historian can write it all down.

THE AGORA

While we are at the precipice of the Great Battle, you still have time to stock up. No army travels without a few merchants and vendors to liven up the troops. Check out the Agora for goods and services to help you and your team during the competition!

HOW YOU GET MONEY

You will receive money for the following actions:

- Score Checks
  - Every thirty minutes, you will receive 100 Drachma for every score check you have up
  - You will lose 25 for every score check you have down
- Injects
  - You will receive 10 drachma per point you receive for your injects. If you get a 100/100, you will receive 1000 drachma. If you get a 50/100 you will receive 500 drachma
- Games
  - If you successfully complete challenges given to you by white team, red team, or black team, you will be rewarded with drachma

HOW TO SPEND MONEY

The Agora will be located in the corner of the room! You will be able to enter the agora and trade your drachma with the merchant(s)!

SERVICES PROVIDED

You will find that there are a wide variety of services and goods available to buy! Some will help your team in your endeavors:

- Divine Messenger
  - Get help from the Black Team
- Titanic blessing
  - Get help from the red team
- The oracle's whispering
  - Get the ramblings of the oracle
- Storyline reset
  - Revert a Box
- Quest Assistance
  - Get help or an extension on an inject
- And More

Of course, some merchants will register their goods will the Consul in the morning of the competition

GOOD LUCK AND HAVE FUN!