BLUE TEAM PACKET

BLUE TEAM PACKET

[redacted]

[redacted]

Thank You to Our Sponsors!!

Diamond

EATON

Platinum

BATTELLE

Amplify.

ICR
Ideas, Commitment, Results

SecurityRisk
ADVISORS

FM

Gold

Miscreants®

[redacted]

[redacted]

[redacted]

Silver

MINDEX

Educational

FORTRA™

no starch press

[redacted]

[redacted]

[redacted]

MEMORANDUM FOR: Delegates of Sovereign Nation

SUBJECT: Request to join Intelligent Response
and
Security Center

CONGRATULATIONS! You have been selected to be assisted by the Crisis Intervention Agency. This is a great honor!

Unfortunately, your Nation is under attack :(While we were secretly monitoring your network activity, we picked up on some suspicious activity which we have attributed to the Cyber Command and Control Party (CCCP). As you may already know, the CCCP operates under the belief that centralized control over all cyberspace is the only path to true stability. Their ultimate goal is to create a unified cyber empire, where they control all digital resources. The first step of their plan is to destabilize your network, allowing them to subsequently establish their authority.

We will not stand for this! We at the Crisis Intervention Agency have benefited greatly from using your private infrastructure as part of our botnet. We fear the actions of the CCCP would completely jeopardize our plans.

But all hope is not lost! We are currently attempting to break into their main control server via our state of the art HASH CRACKING CAPABLE RED TEAM COMPUTER. We anticipate we can shutdown their operations November 2nd, 17:00. Until then, it’s up to *you* to keep your services up. You are locked out at the moment, but we are working to provide you with access to your machines on November 2nd at 09:00.

READ THE REST OF THIS PACKET FOR IMPORTANT DETAILS!

[redacted]

[redacted]

[redacted]

[redacted]

Teams

Blue Team

This is you! Your primary goal is to defend your network and maintain service uptime. However, don't forget about the injects assigned to you throughout the competition by White Team.At the end of the competition, you will also complete an Incident Response Report on what you found in your network.

Red Team

These are the hackers of the CCCP that make your day as rough as possible. They will find cracks in your network and make every attempt to shut down your services. Make your best attempt at keeping them out!

White Team

These are the authorities that will help you throughout the competition! White Team consists of a group of hard-working student volunteers who make sure that the competition runs as smoothly as possible. They will be your go-to for any help that you may need during the day of the competition. This group will also be responsible for the grading of injects.

Black Team

Without Black Team, the competition would not be possible. They have set up the competition infrastructure and with you the best of luck during the competition! Black Team has worked throughout the semester to bring this competition to life. If White Team cannot answer a question, they may escalate the issue to Black Team.

[redacted]

[redacted]

[redacted]

Rules

These are the rules of IRSeC. Any breaking of the rules or intentional/deliberate attempts to skirt around or 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. 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.
7. Only registered blue team members may contribute to your team's work during the competition.
    a. Chaperones/Coaches are NOT permitted to coach, instruct, or guide your team in any way.
8. 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)

[redacted]

[redacted]

[redacted]

b. Out of Scope

i. 172.16.1.0/24- Management Network

ii. 172.29.2.0/23

iii. *.irsec.club

iv. *.ritsec.cloud

v. RITSEC or RIT Hardware (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, 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

9. DO NOT block subnets through Firewall rules or ACLs. Individual IP blocking is permitted.

a. Out of scope IP addresses may not be blocked.

10. Injects may be written and submitted on competition networks or on your physical host machine.

11. 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

12. 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.)

13. 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.

14. Prestaging or pre-baking is allowed. IRSeC 2024 is an incident response competition.

[redacted]

15. 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.
16. 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.
17. 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.
18. 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

[redacted]

Scoring Breakdown

Component	Weight
Uptime	35%
Injects	35%
Incident Response Report	30%

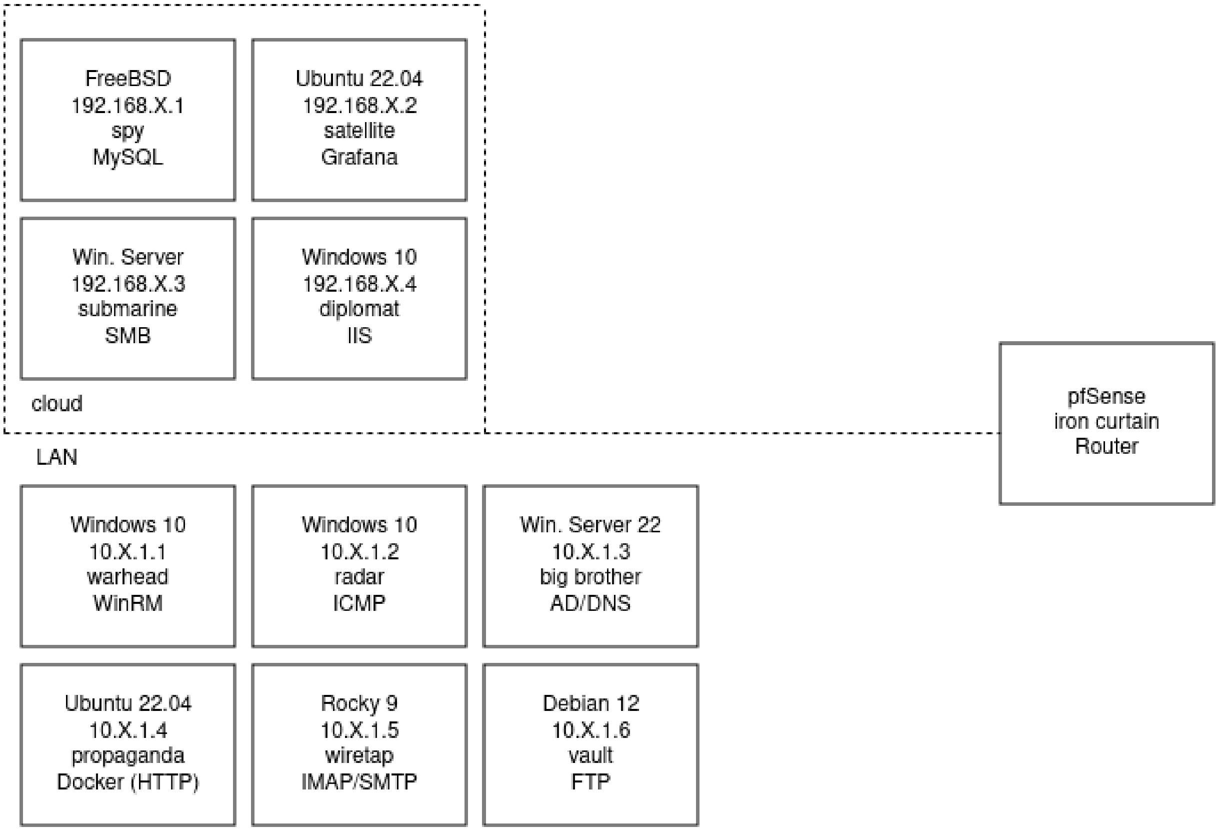
Live scoring will be available to you throughout the competition. Uptime scores will be provided by Scorify (access to which is detailed below). Teams will have access to two dashboards within Scorify. The first dashboard shows all teams and which services are still scoring (green). The second dashboard will show your individual team’s score checks and will provide debugging information regarding why the services are not currently scoring. More information and a demo will be presented before the competition begins.

[redacted]

[redacted]

[redacted]

Our network scans have identified this to be your network topology!



FreeBSD
192.168.X.1
spy
MySQL

Ubuntu 22.04
192.168.X.2
satellite
Grafana

Win. Server
192.168.X.3
submarine
SMB

Windows 10
192.168.X.4
diplomat
IIS

cloud

pfSense
iron curtain
Router

LAN

Windows 10
10.X.1.1
warhead
WinRM

Windows 10
10.X.1.2
radar
ICMP

Win. Server 22
10.X.1.3
big brother
AD/DNS

Ubuntu 22.04
10.X.1.4
propaganda
Docker (HTTP)

Rocky 9
10.X.1.5
wiretap
IMAP/SMTP

Debian 12
10.X.1.6
vault
FTP

[redacted]

Scored services:

Hostname	IP Address	Operating System	Services	Scored
ironcurtain	10.X.1.254	pfSense	Routing	No
warhead	10.X.1.1	Windows 10	WinRM	Yes
radar	10.X.1.2	Windows 10	ICMP	Yes
bigbrother	10.X.1.3	Win. Serv. 22	AD/DNS	Yes
propaganda	10.X.1.4	Ubuntu 22.04	Docker (HTTP)	Yes
wiretap	10.X.1.5	Rocky 9	IMAP/SMTP	Yes
vault	10.X.1.6	Debian 12	FTP	Yes
spy	192.168.X.1	FreeBSD	MySQL	Yes
satellite	192.168.X.2	Ubuntu 22.04	Grafana	No
submarine	192.168.X.3	Win. Server 22	SMB	Yes
diplomat	192.168.X.4	Windows 10	IIS	Yes

[redacted]

Timeline

07:30 - 08:00	Check-in in the Atrium
08:00 - 09:00	Keynote in GOL-1400
09:00 - 09:30	Initial Access (Credentials Given)
09:30 - 12:00	First Half of the Competition
12:00 - 13:00	Lunch
13:00 - 17:00	Second Half of the Competition
17:00 - 18:00	Incident Response Report
18:00 - 18:30	Break
18:30 - 19:00	Red Team Debrief
19:00 - 19:15	Final Scores and Prize Ceremony

** You will be notified by the CA when you are able to access the competition infrastructure

[redacted]

[redacted]

[redacted]

We've recovered the following accounts from your systems:

Domain Users

Administrators

- representative
- senator
- attache
- ambassador

Local

- foreignaffairs
- intelofficer
- delegate
- advisor
- lobbyist
- aidworker

Local Users

Administrators

- president
- vicepresident
- defenseminister
- secretary

Local

- general
- admiral
- judge
- bodyguard
- cabinetofficial
- treasurer

[redacted]

Competition Access

During the competition, you will have access to your team's LAN environment via our in-house tool, Compsole. Before the competition begins, you will be given credentials to access Compsole. Along with Compsole, you will also have access to Scorify, the store, and the inject submission site with the following links:

Compsole: compsole.ritsec.cloud
Scorestack: scoring.irsec.club
Store: store.irsec.club
Inject Submissions: injects.irsec.club

Credentials for the services listed above will be given before the beginning of the competition. Service uptime will be determined by Scorify automatically. 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. More information regarding the store is given below.

[redacted]

Injects and The Final Incident Response Report

Injects

While your network is under attack, you will be given several tasks to complete. All injects will be released via sheets of paper handed out by our Injects Lead, who is on Black Team at various points in the competition. Each inject will have its submission deadline, task, and grading rubric/weight on it.

Incident Response Report

At the end of the competition, you will be asked to compile a report of all the obstacles that you have encountered. Make sure to keep an eye out for anomalous activity within your network as this means that the CCCP’s hackers have successfully intruded your infrastructure. Take note of anything that you believe is evidence of an intrusion.

Submissions

In order to submit an inject or the Incident Response Report for grading by White Team, you must upload a pdf file to injects.irsec.club before the deadline. To submit, select your team number on the website and log in with your credentials.

Store

Receiving Credits

The following actions will supply you with credits to spend at the store:

- Injects
- Challenges

[redacted]