IRSeC 2022:
BLUE TEAM BRIEFING

November 5th

RITSEC
Security Through Community

Table of Contents

Sponsors

Titanium

Diamond

Platinum

Gold

Silver

Educational

Situation

MAIL FROM: <REDACTED>

RCPT TO: <REDACTED@CPA.AQ>>

SUBJECT: MISSION BRIEFING

HELLO,

YOU DO NOT KNOW WHO I AM, AND I INTEND TO KEEP IT THAT WAY. ALL THAT YOU DO NEED TO KNOW IS THAT WE HAVE A SHARED GOAL. UNDER THE GUISE OF A SHARED ORGANIZATION KNOWN ONLY AS THE SOUTHERN ENERGY ASSURANCE LEGION (SEAL), SEVERAL ENERGY CORPORATIONS HAVE TAKEN OVER THE ANTARCTIC COASTLINE FOR THE SOLE PURPOSE OF OIL EXPORTS. IN THE WAKE OF THIS ATROCITY, THE ENVIRONMENT HAS BEEN NOTHING BUT AN AFTERTHOUGHT. WALLS OF ICE ARE FALLING CONSTANTLY INTO THE OCEAN. FLOCKS OF ANIMALS HAVE HAD THEIR HABITATS DESTROYED. WE WILL NOT STAND FOR THIS MAYHEM.

WE HAVE ALREADY BEGUN OUR INITIAL ATTACK. TEAMS OF FIVE HAVE BEEN SPECIFICALLY CHOSEN BASED ON THEIR SKILLS TO INFILTRATE SEVERAL OIL RIGS AND DEFEND THEM UNTIL BACKUP ARRIVES. YOUR JOB IF YOU CHOOSE TO ACCEPT IT IS TO MAINTAIN THE OIL RIG INFRASTRUCTURE SO OUR PRESENCE SHALL REMAIN UNKNOWN. SEAL HAS INSTALLED SEVERAL COUNTERMEASURES, SO BE SURE TO KEEP WEARY SUCH THAT OUR ATTACK WILL REMAIN UNNOTICED. YOUR ASSISTANCE IS IMPERATIVE AND WE CANNOT HAVE A SINGLE TEAM FAIL.

YOUR TRIUMPH WILL BRING PEACE TO ANTARCTICA AND PUSH FOR ENVIRONMENTAL CHANGE WORLDWIDE. WE NO LONGER SIT IN PEACE AND WILL FIGHT FOR THE PROTECTION OF OUR WORLD.

REGARDS,

THE CIRCLE FOR THE PROTECTION OF ANTARCTICA (CPA)

Timeline

07:30-08:00 Check-in Begins
08:00-09:00 Welcome Ceremony/Keynote
09:00-09:30 Credentials Given
09:30-12:00 Competition First Leg
12:00-13:00 Lunch/Sponsor Interaction
13:00-17:00 Competition Second Leg
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/Prize Ceremony

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

Stakeholders

Blue Team

This is you! Your primary goal is to defend your network and maintain service uptime. However, don't forget about the injects. Injects will be assigned throughout the competition and it is in your best interest to complete them. At the end of the competition, you will also complete an incident response report on what you found on your network.

Red Team

These mercenaries for hire have been tasked with making your lives as tough as possible. Representing SEAL, they will find the cracks in your network and make every attempt to halt your operation. Make your best attempt at keeping these thugs off your boxes.

White Team

White team consists of a group of hardworking student volunteers who make sure the competition runs as smoothly as possible. They will be your go to for any help you may need during the day of the competition. This group will also be responsible for grading and collection of injects.

Black Team

The competition would not be possible without these amazing people. They have set up the competition infrastructure and wish you the best. Black Team has worked throughout the semester to implement this competition. If White Team cannot answer a question, they may escalate the issue to Black Team.

E-Board

RITSEC E-Board along with managing the club also helps with much of the administrative work with regards to the competition.

Sponsors

Our competitions would truly not be as great without the loving support of our sponsors. They have generously donated their resources and time. Please keep a look out for them throughout the competition.

**All teams will be identified by the color of their shirt

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 Injects 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 by the Wednesday before the competition (Nov 2nd)
    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	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 Scorestack (access to which is given below). Teams will have access to two dashboards within Scorestack. The first dashboard shows all teams and which services are still scoring (green). The second dashboard will show your individual teams score checks and will provide debugging information regarding why the service is not currently scoring. More information and a demo will be presented before the competition begins.

Access

During the competition you will have access to your team’s LAN environment via our new in-house tool Compsole. Before the competition begins you will be given credentials to access Compsole via. Along with Compsole you will also have access to Scorestack and the store via the following links:

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

Credentials for the above services will be given before the beginning of the competition. Service uptime will be determined by Scorestack 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 will be given below.

Network Topology Intel

MAIL FROM: <REDACTED>

RCPT TO: <REDACTED@CPA.AQ>

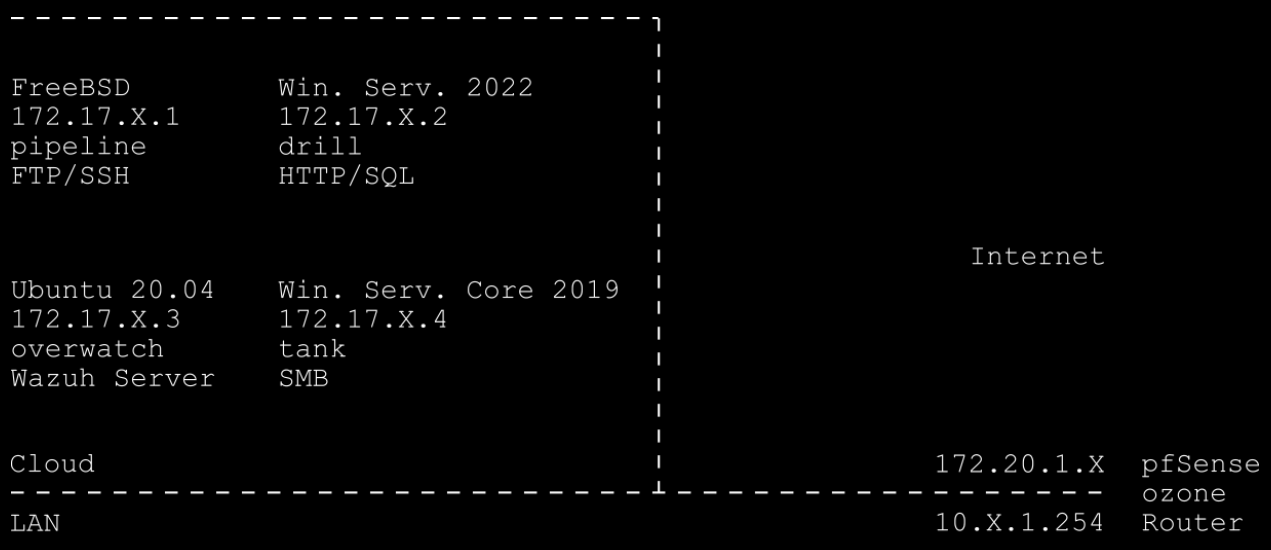
SUBJECT: INTEL REPORT

HELLO AGAIN,

ONE OF OUR OPERATIVES ON A PREVIOUS MISSION WAS ABLE TO RETRIEVE THIS NETWORK TOPOLOGY BEFORE RETREATING. USE THIS INFORMATION WISELY

REGARDS,

THE CIRCLE FOR THE PROTECTION OF ANTARCTICA (CPA)



Win. Serv. 2022	Windows 10	Windows 10
10.X.1.1	10.X.1.3	10.X.1.2
squid	sealion	penquin
AD/DNS	WinRM	ICMP

Arch Linux	Rocky Linux	Rasperry PI OS
10.X.1.4	10.X.1.5	10.X.1.6
albatross	orca	whale
SSH	IMAP/SMTP (MAIL)	ICMP

Scored Services

Hostname	IP Address	Operating System	Services	Scored
LAN				
ozone	10.X.1.254	pfSense	Routing	No
squid	10.X.1.1	Windows Server 2022	AD/DNS	Yes
penguin	10.X.1.2	Windows 10	ICMP	Yes
sealion	10.X.1.3	Windows 10	WinRM	Yes
albatross	10.X.1.4	Arch Linux	SSH	Yes
orca	10.X.1.5	Rocky Desktop	IMAP/SMTP	Yes
whale	10.X.1.6	Raspberry PI Desktop	ICMP	Yes
CLOUD				
pipeline	172.17.X.1	FreeBSD	FTP/SSH	Yes
drill	172.17.X.2	Windows Server 2022	HTTP/SQL	Yes
overwatch	172.17.X.3	Ubuntu 20.04	Wazuh Server	No
tank	172.17.X.4	Windows Server Core 2019	SMB	Yes

** The ‘X’ represents your team number.

Accounts

Domain Users

Administrators

- CharlesKoch
- HaroldHamm
- PhilipAnshcutz
- GeorgeKaiser

Users

- MichaelWirth
- BenVanBeurden
- DarrenWoods
- BernardLooney
- JosephKim
- JosephGorder
- AminNasser
- RyanLance
- CarlosJorda
- PatrickPouyanne
- ArmandHammer
- TengkuTaufik

Local Users

Administrators

- rigmanager
- derrickhand
- motorhand
- floorhand
- leasehand

Users

- driller
- steward
- custodian
- enzo
- emmanuel
- Bingus
- FireHazard

** All user credentials will be the exact same at the start of the competition. The credentials will be provided before the start of the competition.

Injects

MAIL FROM: <REDACTED>

RCPT TO: <REDACTED@CPA.AQ>

SUBJECT: SPECIAL OPERATIONS

HELLO AGAIN,

I HAVE ALREADY ASKED MUCH OF YOU. HOWEVER, IF OUR MISSION IS TO BE TRULY SUCCESSFUL, I MUST ASK MORE FROM YOU. WHILE INFILTRATING THE COMPOUND YOU WILL BE TASKED WITH OPERATIONS THAT ARE IMPERATIVE TO THE SUCCESS OF THE MISSION. WITH YOUR SUPPORT WE WILL BE ABLE TO ABLE TO TAKE DOWN THIS HEINOUS ORGANIZATION ONCE AND FOR ALL WHILE SENDING A MESSAGE TO ALL WHO PLAN TO HURT THIS VERY PLANET WE LIVE ON. BE ON THE LOOKOUT FOR FUTURE INFORMATION.

REGARDS,

THE CIRCLE FOR THE PROTECTION OF ANTARCTICA (CPA)

Submission

With the infiltration task at hand, you will be given several operations to commit to. All injects will be released via paper from white team at various points in the competition. You will be given two flash drives. All inject submissions will be given to white team by the deadline on said flash drive. You have two such that while one inject is being graded you will still be able to submit upcoming injects. These flash drives are your lifeline. Do not lose them.

Any questions should be directed towards white team or our inject lead.

Inject Rubric

On-time	25%	Submissions must be completed by the due-time. While late submissions will be accepted, no points will be awarded for this category If you cannot complete an inject you must inform the Underground or request an extension (within reason, including an explanation).
Professionalism	25%	Follow the competition lore, address the CPA 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

MAIL FROM: <REDACTED>

RCPT TO: <REDACTED@CPA.AQ>

SUBJECT: A FRIENDLY REMINDER

MY FINAL REQUEST,

BEFORE WE CAN RETRIEVE YOUR TEAM, WE MUST ASK THAT YOU RECORD ALL ASPECTS OF THIS INFILTRATION. THIS TASK IS IMPERATIVE SO THAT WE CAN CONFIRM THAT OUR OPERATION RAN SMOOTHLY WITH NO INVESTIGATIONS. WE MUST DOCUMENT THE ATROCITIES COMMITTED HERE. DOCUMENT EVERYTHING YOU CAN FIND ABOUT SEAL, WITH SPECIFIC EVIDENCE, IMPACT, AND DETAIL.

REGARDS,

THE CIRCLE FOR THE PROTECTION OF ANTARCTICA (CPA)

** At the end of the competition you will be asked to compile a report of all obstacles you encountered. Make sure to keep an eye out for anomalous activity within your network as this means the mercenaries have successfully detected our intrusion. Take note of anything you think may have blown our cover.

Store

MAIL FROM: <REDACTED>

RCPT TO: <REDACTED@CPA.AQ>

SUBJECT: SUPPORT

DON'T WORRY,

WE ARE NOT HANGING YOU OUT TO DRY. WHILE YOU ARE INFILTRATING THE COMPOUND, WE WILL BE WORKING HARD ON OUR END TO GET YOU ANY ASSISTANCE YOU MAY NEED. FURTHER INFORMATION IS PROVIDED IN THE ATTACHMENT BELOW.

REGARDS,

THE CIRCLE FOR THE PROTECTION OF ANTARCTICA (CPA)

Receiving Money

The following actions will supply you with money:

- Score Checks
  - You will receive credits based on the increase of your total score
- Injects
  - You will receive 10 credits per point you receive for your injects. If you get a 100/100, you will receive 1000 credits. If you get a 50/100 you will receive 500 credits.

Services Provided

The CPA has an entire site dedicated to getting the resources you need to best accomplish your mission. Please make sure to locate the store at store.irsec.club and spend your credits wisely.

MAIL FROM: <REDACTED>

RCPT TO: <REDACTED@CPA.AQ>

SUBJECT: MY FINAL MESSAGE

THESE ARE TRYING TIMES. ALL THAT I ASK IS THAT YOU KEEP THE PRIMARY MISSION AT MIND. AND PLEASE, GOOD LUCK AND HAVE FUN!

BEST WISHES,

THE CIRCLE FOR THE PROTECTION OF ANTARCTICA (CPA)