**Crack-A-Lackin Frack’n Co.**

Information Technology Department Briefing

Fall 2023



**Table of Contents**

Table of contents ………………………………………………………………………………………… 1

Information Technology Department Briefing ……………………… 2

Schedule ………………………………………………………………………………………………………………… 3

Competitive Teams ………………………………………………………………………………………… 4

Rules ………………………………………………………………………………………………………………………… 5

Professional Conduct ………………………………………………………………………………… 7

Topology ………………………………………………………………………………………………………………… 8

Access ……………………………………………………………………………………………………………………… 9

Injects ………………………………………………………………………………………………………………… 10

Scoring Breakdown ……………………………………………………………………………………… 11

**Information Technology Department Briefing**

MAIL

FROM: [cbeaver@clfc.com](mailto:cbeaver@clfc.com)

TO: [it@clfc.com](mailto:it@clfc.com)

SUBJECT: Welcome and Good Luck

Welcome to Crack-A-Lackin Frack’n Co., or CLFC!

I am Cal Beaver, CEO of CLFC. As you might know, we recently celebrated the merging of Crack-A-Lackin Event Planning and Frack’n Co. We are happy to be working alongside each other and are excited to achieve our goals and much more during our future as one company together. You may be thinking, Cal, why does an oil company such as Frack’n Co. need the resources of a local event planning company? Well, I am here to say that you, as the Information Technology (IT) department, are not entitled to this information - please stop emailing HQ about it.

Anyways, the reason you are all getting this email is that we are now faced with an important decision. Both companies, before the merger, had their own IT department and team. Because we are not in need of a large IT team, we have taken the liberty of letting go of some members so only the five best members from each side are still employed. We did, unfortunately, have to let the team leader from Crack-A-Lackin’s IT team go - let this be your example of what happens when you ask me too many questions I don’t feel like answering.

After talking to the board, we have further decided to only keep five of you employed since we feel we don’t need an IT team of ten people. In order to determine this, we will give both IT teams a set of challenges to complete and the better team will be CLFC’s official new IT team! How exciting!

It also happens to be a complete coincidence that one of our rivals, Ozone Slayer, is currently trying to get into our systems. I have tried to reach out to their CEO, Marcus Green, but nothing has changed. It is up to you to secure our information, and therefore secure your employment.

Good luck and I will be in touch soon,

Cal Beaver

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Cal Beaver*

*CEO, Crack-A-Lackin Frack’n Co.*

*(248)434-5508*

**Schedule**

Monday 10/2: This is the day we set up the competition. Grey Team deploys the machines, the blue teams familiarize themselves with them and Red Team finalizes their tools.

Wednesday 10/4: Day 1, competition starts. Good luck, have fun! For the first 10 minutes, Red Team will have their hands off their keyboards, while the blue teams will use this time to set up their machines.

Wednesday 10/11: Day 2 of the competition. *A new, fun rule comes into play to spice up the game.* 🙂

Monday 10/16: Day 3 of the competition. No matter which team comes out on top, Cal Beaver wins either way! Have fun… 😈

Wednesday 10/18: Purple team day. Grey team deploys clean machines for the blue teams and Red Team to discuss their strategies and mindset to learn from each other. This is a good time to ask about any specific moments that might have surprised you or seemed unorthodox.

Monday 10/23: Recap, lessons and debrief. Congratulations, Competition 1 is over!

**Competitive Teams**

* Blue Team 1
  + Background: As the former security team for Frack’n Co., your team was not happy with the merger. After all, you guys single-handedly took care of all the security issues Frack’n Co. has faced in the past and now your CEO thinks that you are, skillswise, on par with a mom-and-pop IT team. Show them you are in a completely different league.
  + Goals: Repair as many services that go down before Blue Team 2 can. Keep those services up for as long as possible. Do not leak confidential information… or at least do not get caught.
* Blue Team 2
  + Background: You were the former security company of Crack-A-Lackin Event Planning, a mom-and-pop business. Everything was nice until the merger. Your new coworkers treat your team poorly and have tried to sabotage your team in the past. This has led to the firing of your team leader. It is only a matter of time before they get rid of your team completely or make your team completely subservient to them. Your team has chosen to fight fire with fire.
  + Goals: Repair as many services that go down before Blue Team 1 can. Keep those services up for as long as possible. Do not leak confidential information… or at least do not get caught.
* Red Team
  + Background: Due to the recent merger of two competitive fracking companies, your team has been hired by Ozone Slayer to infiltrate their systems. Your team was the only group to accept such a job due to the recent uproar from climate activists surrounding the fracking industry. Your team is also aware of the schism within the company and wants to take advantage of that. The security teams of both merged companies want to show superiority over the other no matter what the cost. Ozone Slayer has authorized you on their behalf to pay good money for any information either IT team from Crack-A-Lackin Frack’n Co. is willing to give up on their competition.
  + Goals: Take as much sensitive information as possible. Take down services where possible.
  + Penalties: You may be arrested or sent to prison for violating rules or for causing too much chaos.

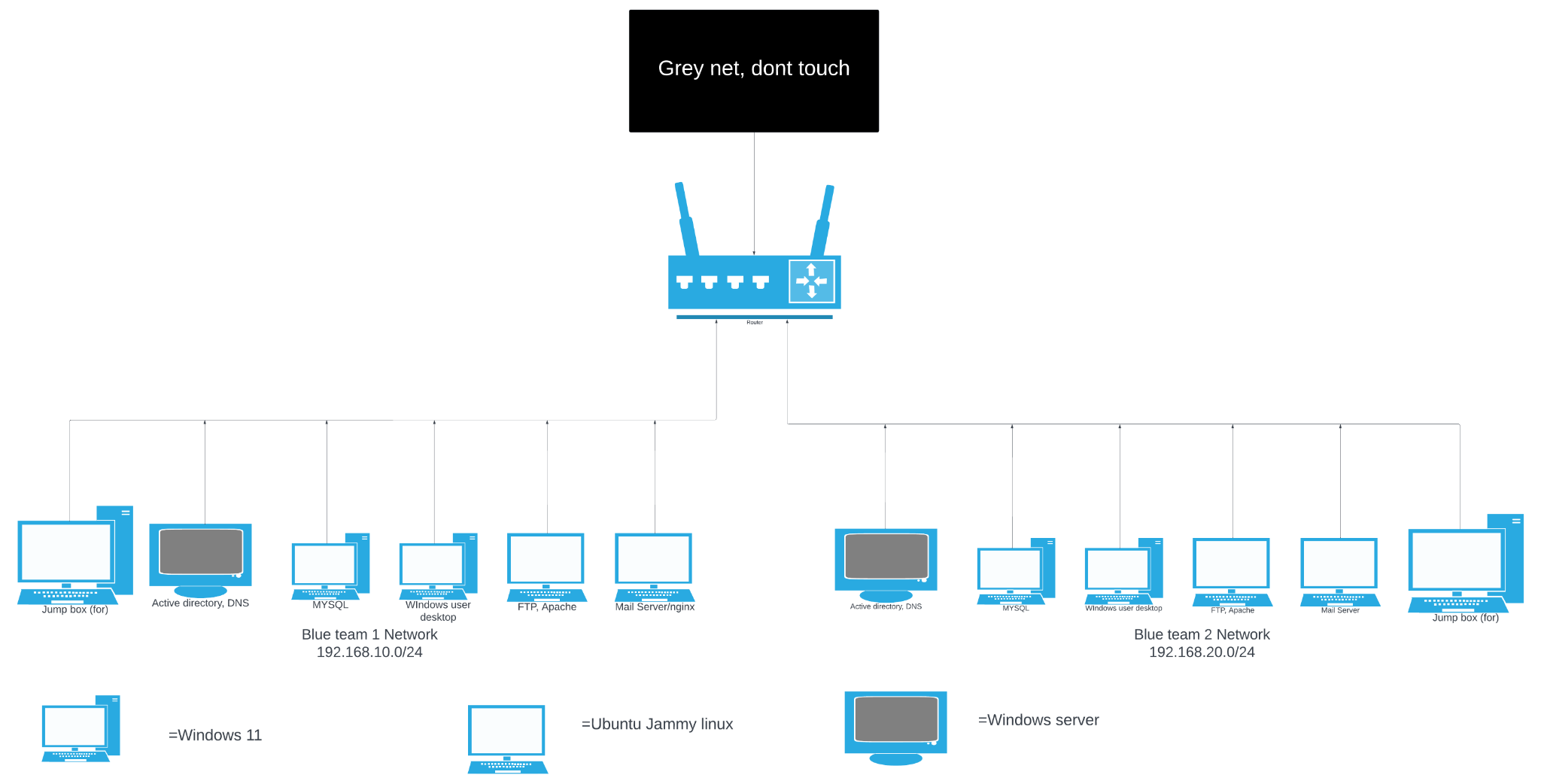
**Rules**

1. This competition is for *fun* and *learning*. Do not break the spirit of competition.
2. Be *respectful* and *professional* to everyone.
3. No attacks on any of the **Grey** Team accounts are allowed.
4. No interference of any kind on port 80 is allowed.
5. Do not alter the scoreboard, including the manual scoring page.
6. No spoofing of the HTTP requests used for the scoring.
7. No spoofing Injects.
8. No one is allowed to change any Blue Team machine’s IP addresses.
9. Red team is not being scored, the blue teams are.
10. If anyone bricks a machine, their team will lose points
11. Timeout will take place outside the room to prevent eavesdropping.
12. Red team rules
    1. Red team cannot lock out either of the blue teams from their own boxes.
    2. Red team can use pre-staged tools if they share it with everyone and can explain what it does.
    3. No denial of service attacks of any kind.
    4. Red team cannot log in as Grey Team, but they can impersonate them.
       1. Red team cannot spoof the “notouchaccount,” as it is called a No Touch Account for a reason.
13. Blue teams rules
    1. The blue teams cannot attack the Red Team in any way, including taking pictures.
    2. The blue teams cannot use an antivirus of any kind.
    3. The blue teams cannot directly attack or sabotage the other blue team in any way. (Unless otherwise stated)
    4. The blue teams cannot impersonate anyone.
    5. Blue Team is not allowed to block the IP range for Red Team, but they can block individual IP addresses.
14. Mail server rules
    1. The mail server cannot be altered or attacked in any way.
    2. Red Team can get in.
    3. The blue teams can get in.
    4. Each Blue Team member has their own email.
    5. Red Team cannot lock anyone out.
    6. Blue team can block the Red Team from having access.
    7. ***Do not lock out Grey Team!***
    8. If the mail server is taken down once by a blue team, the offending team will lose points. This applies to all blue teams.
    9. If the mail server is taken down twice by the same team, the offending team will miss out on injects, lose points, and possibly be told to sit out. This applies to all blue teams.
    10. If the mail server is taken down by Red Team, the involved parties will be forced to sit out for a certain amount of time determined by Grey Team based on the severity of the situation.
15. Phones and laptops are allowed during the competition.
    1. Picture takers can be caught in the act by having their attempt reported to the Grey Team. If a competitor is caught, the picture must be deleted and the player MAY be timed out. The reporter must add this incident to their report.
    2. Pictures must be clear to earn points.
    3. No videos are allowed.
16. A blue team that uses their pictures to tell the other blue team to improve their security will gain *2 points.*
17. The blue teams are allowed to sell information from each other to Red Team for points starting on Day 2.
    1. The blue team that sold the information will receive *a certain amount of points (Determined by the Red Team).*
    2. The Red Team will have a predetermined amount of points to spend.
    3. The blue teams can sell fake information.
    4. Red Team must verify the information on their own.
    5. If anyone gets scammed, it is their problem.
18. All teams must write *everything* down in their report during the competition which includes pictures and transactions. Any disputes will be settled with both teams’ reports.
19. Violations of any of the above rules will result in penalties at the discretion of Grey Team.
20. New rules can be added during competition and will be announced to everyone before they are put into effect.

**Professional Conduct**

All competitors (Red and Blue Team) will conduct themselves in a professional manner. This includes refraining from excessive profanity, unsportsmanlike conduct, disregarding the directions of the Grey Team or the Cyber Range staff, misusing RIT equipment, and any other behavior that the Grey Team deems to be unprofessional. Competitors should use common sense when determining what behavior is acceptable. Any competitors who are found to be behaving unprofessionally risk point deduction, temporary/permanent removal from the competition, or disqualification of their team. All disciplinary action will be enforced at the discretion of the Grey Team based on the severity of the infraction. Any person can lodge a complaint to the Grey Team, who will investigate the allegations and determine the outcome.

**Topology**



The image provided depicts the network topology created to test your skills in the field. Designated as the “Red Team Jumpbox”, the offensive team from Ozone Slayer will connect to the network with their already created boxes filled with tools to test who truly deserves their jobs with the Crack-A-Lackin Frackin’ Co.

**192.168.10.0 - Blue Team 1**

**192.168.20.0 - Blue Team 2**

**192.168.50.0 - Grey Team DO NOT TOUCH**

**Access**

| Crack-A-Lackin (Team 2) | Username | Password |
| --- | --- | --- |
| Renzhong Huang | rhuang | Password1! |
| Wesley Weng | wweng | Password1! |
| Matthew Faulkner | mfaulkner | Password1! |
| David Kumar | dkumar | Password1! |
| Ben Wright | bwright | Password1! |
| Active Directory Admin | ADAdmin | Password1! |
| Blue Default Local | blue\_admin | Password1! |

**DO NOT TOUCH THESE ACCOUNTS:**

grey\_admin

notouchaccount

**Injects**

During this competition, there will be a series of challenges, or Injects, to complete within a matter of time. Each Inject will be given out through the **mail server** and they will be given out randomly. The Inject will specify how much time is allotted for completion as it will not be the same for every Inject handed out. Every Inject is also worth a different amount of points to add to your overall score, and can even turn the competition around.

Submission

Complete the Injects to the best of your ability, and even if the Inject itself is not completed, a lack of any submission before the time is up will result in 0 points. This will not reflect negatively on your overall score, but some partial points may be given out if a submission is made for an incomplete Inject. Submission must be through the mail server.

Example Submission

MAIL

FROM: <<EMAIL>>

TO: [cbeaver@clfc.com](mailto:cbeaver@clfc.com)

SUBJECT: <<INJECT NUMBER>> <<TEAM NAME>>

<<DAY>>

<<TIME>>

Hello Sir,

Here are our findings for Inject #1. This is what we did. This is what we didn’t do.

Thank you!

Blue Team

**Scoring Breakdown**

Service Scores: General points are awarded based on how long a service is up, this will be automatically checked periodically. Points can be received for Injects and at the discretion of Grey Team.

| **Service** | **Points** |
| --- | --- |
| FTP | 1 per 5 minutes |
| DNS | 1 per 5 minutes |
| Apache | 1 per 5 minutes |
| MySQL | 1 per 5 minutes |
| Active Directory | 1 per 5 minutes |
| Injects | \*changes based on the Inject\* |
| Discretionary Points | \*not a set amount depends on the situation\* |

Additional Ways to Gain Points: Starting on ***Day 2*** of the competition, Blue Team members will be allowed to take pictures of sensitive information that belongs to the other blue team. If a blue team member gives the information to Red Team, then they will have a chance to gain however many points Red Team gives out added to their overall score. It is up to Red Team to determine whether or not the information given to them is correct. In order for the blue team to get the points, a Red Team member must come up to Grey Team and they will manually add points to the blue team’s score. If the blue team chooses to warn the other blue team of their leaked information, then they will receive 2 points added to their overall score. A team member of the warned blue team must come up to Grey Team to give the other blue team their points.