Verified Employees:

Cal Beaver, CEO of CLFC - cbeaver@clfc.com

Marcus Green, CEO of Ozone Slayer (has a CLFC guest account) - mgreen@clfc.com

The FBJ - mrfbj@clfc.com

Shiela Carson from HR - scarson@clfc.com

Hank Olvin from Accounting - [holvin@clfc.com](mailto:holvin@clfc.com)

For red team we should do social Engineering tasks, and find ways to use a port scanner.

Possible Injects:

1). Social Engineering / Phishing URL to document user IP of users who click from mail / phishing / possible tech support emails. If Blue Team clicks -> points for red team

* Blue team can reject clicking the link by sending an email -> manual grading based on how they write the email ( Report Phishing)
* Maybe grade them on how professional they respond?

2). Possible Spy Injection: Both Blue teams must get screenshots of privileged information from each other. Punishment if either team can obtain a picture of someone else taking a picture.

3). Cal Beaver only cares about profit and starts unintentionally sabotaging blue and/or red efforts. Something like “this service is too expensive, you can’t use it?” “The cybersecurity press is slaughtering us, go easier on the IT teams. No more of that (insert service name) thingamajig”

* This will even the playing field by taking that service or tool off the field

4). Internal emails

* From: Sheila from HR: Hi, this is Sheila, I got logged out of my computer can you direct me to change my password
* From Kevin from Account: Hi, this is Kevin, Could you please click the link to enter your daily hours? Again, your login is your computer login

5). Summary: [Insert team] had a nice lunch at Salvatores. On their way back they realized the company building was being swarmed by protestors, therefore they can’t continue their work.

Effect: Blue Team can’t work for 15 mins

6). Summary: Unaware employee from accounting asks if a link is safe to click. Will click on it in one minute unless responded to

Effect: We can give credentials to the red team

7). Summary: “Team Member B, get me a bacon, egg, cheese and avocado bagel with a frappuccino, 37% cream, 3 sugar cubes. If you get my order wrong you will get your pay (points) docked”

* A delta team member stands outside the room and will do something like type up the order as dictated by Team Member B from B’s memory
* B gets a paper or email of what was typed up and brings it back to show completion
* Make them go to Ctrl Alt Deli and order actual food using a dining bucks gift card NOT their own money or bucks

Effect: Distracts a blue team member

Affected: Blue Team 1 or Blue Team 2

8). Janitors come in to do cleaning on specific PCs. Those PCs must be vacated for (time amount) while they clean

Effect: Distracts a [insert team] member

Affected: Blue Team 1 or Blue Team 2 or Red Team

8b) Janitors come in to do cleaning on specific PCs. Those PCs must be vacated for (time amount) while they clean. The janitor is a Red Team member.

Effect: Red Team can prebake

Affected: Blue Team 1 or Blue Team 2

9). Summary: Specific team member’s mother is asking for details on their day. If they ignore her, she will be very sad. Points awarded based on how loving the response is or something

Effect: Distracts a [insert team] member and the information received can be used against them

Affected: Blue Team 1 or Blue Team 2

Points: 0-30

10). Summary: It’s corporate Silly Day. Take a pic of a teammate in their silliest pose. Be careful, the other IT team will get more bonus points if they take a pic of your teammate doing their silliest pose

Effect: Distracts a member

Affected: Blue Team 1 or Blue Team 2

11). Summary: There is a highly privileged account that the former team lead of blue team 2 has. Go to James Brigden and ask him for his login

Effect: Anyone can get a privileged account

Affected: Blue Team 1 or Blue Team 2 or Red Team

12). Time for corporate mandated (specific team members’) exercise time! Go outside (of the room) and do 15 jumping jacks

13). Bring your child to work day? There was an accident, go to bathroom and get a DRY paper towel. We don’t want the PCs to get wet ;(

14). Anti fracking protesters and old regulars of the mom and pop shop joined forces and are storming the building! Select 2 team members (could be every team sending team members) to literally tell them “no, go away” or “get a job” (no physical contact and only language)

* Maybe mention in the inject specifically what to do so rule 2 (being respectful and professional) isn’t broken

15). The EPA is here! The Frackin’ IT team must hide or get taken away for questioning on Cal Beaver’s secret activities.

* The team members who are still sitting in their seat get taken away for a 1-2 minute interrogation
* Targets whichever blue team is supposed to be the Frackers

16). Cal Beaver sends an email asking for thoughts on his presidential campaign: We Frack, We Snack, We Bring Jobs Back. Government subsidies for fracking corporations, free snacks for K-12 and creating jobs via Big Oil

* Targets a specific team member and they must say what he wants to hear or their team loses points
* Write the email in a way that it’s very obvious that he lives in echo chamber: “My campaign’s perfect. There has never been a better presidential campaign in the history of presidential campaigns.”

17). Cal Beaver sends a very angry to Red Team because a very young family member of one of the member’s posted on X (Twitter) criticizing CLFC (it only has 3 likes)

* One (or all red team members) write a formal apology email to Cal or else he will pull the plug on their PCs (or maybe yell at them for 3 minutes)
* Goal: Waste red team’s time

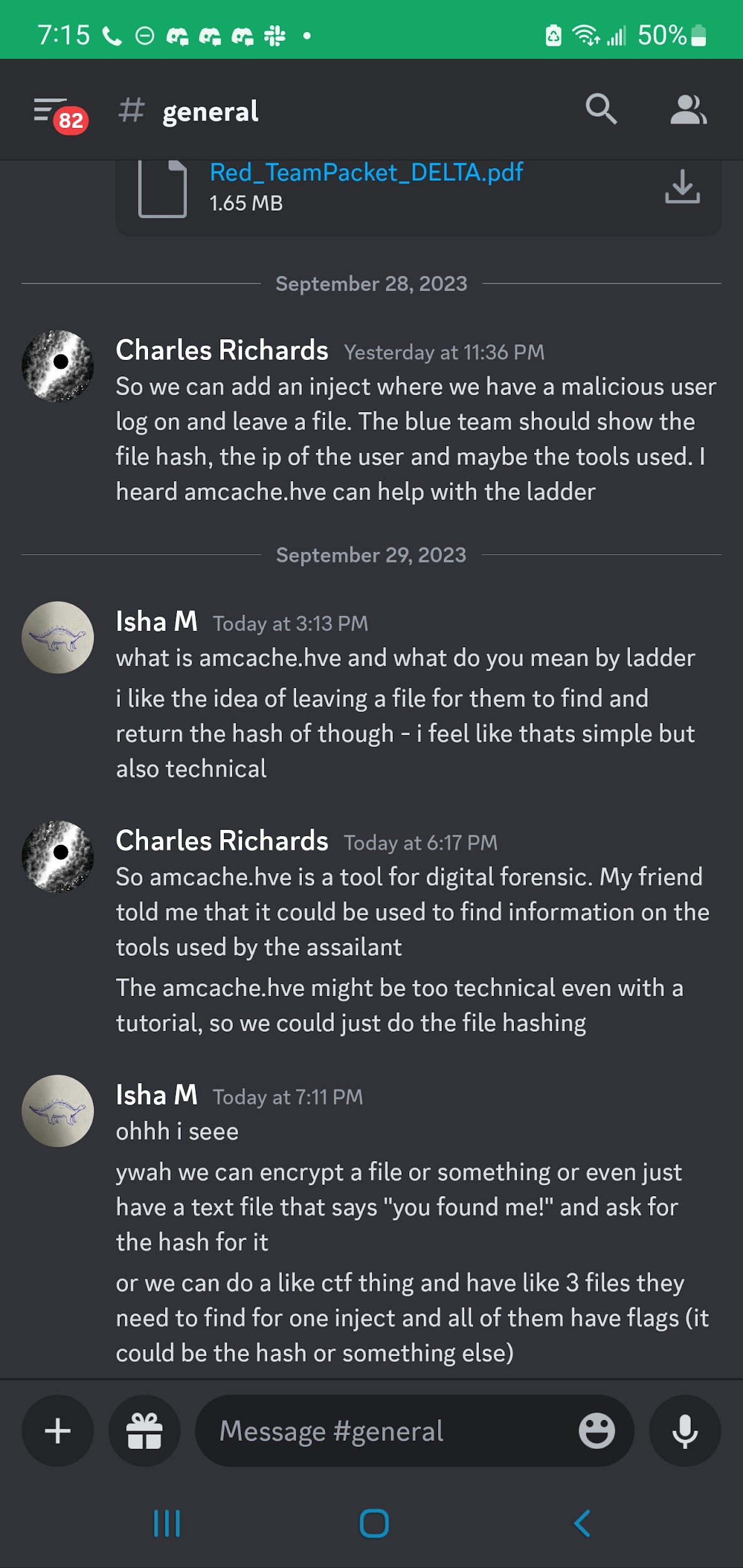
18). Cal Beaver is bored and needs someone to listen to him talk about his long hard day of sitting at his desk knitting.

* Can target red team or blue team
* Distract one team member for 2 minutes
* Red and Blue team get access to machine Logins, Blue team should change
* Flags
* **SCAVENGER HUNT**

Riddle for Garret:

Ideas

Osint prompt that uses values generated by ai. This is stored on a server called PII for (personal identifiable information)



# **Mild Time Wasters**

| Inject #1 | Name: ???? |
| --- | --- |
|  | Service: |
|  | Goal: |
|  | Description:  Unaware employee from accounting asks if a link is safe to click. Will click on it in one minute unless responded to  Effect: We can give credentials to the red team |
|  | Submission: |
|  | Email: |

| Inject #2 | Name: |
| --- | --- |
|  | Service: |
|  | Goal: |
|  | Description:  12). Time for corporate mandated (specific team members’) exercise time! Go outside (of the room) and do 15 jumping jacks |
|  | Submission: |
|  | Email: |

| Inject #2 | Name: |
| --- | --- |
|  | Service: |
|  | Goal: |
|  | Description:  18). Cal Beaver is bored and needs someone to listen to him talk about his long hard day of sitting at his desk knitting.  Can target red team or blue team  Distract one team member for 2 minutes  Maybe cal is bored and gives the team a silly goose chase on their machines? Looking for a file that does not exist just so he can have a laugh? |
|  | Submission: |
|  | Email: |

| Inject #2 | Name: |
| --- | --- |
|  | Service: |
|  | Goal: |
|  | Description: |
|  | Submission: |
|  | Email: |

| Inject #2 | Name: |
| --- | --- |
|  | Service: |
|  | Goal: |
|  | Description: |
|  | Submission: |
|  | Email: |

| Inject #2 | Name: |
| --- | --- |
|  | Service: |
|  | Goal: |
|  | Description: |
|  | Submission: |
|  | Email: |

1). Social Engineering / Phishing URL to document user IP of users who click from mail / phishing / possible tech support emails. If Blue Team clicks -> points for red team

* Blue team can reject clicking the link by sending an email -> manual grading based on how they write the email ( Report Phishing)
* Maybe grade them on how professional they respond?

4). Internal emails

* From: Sheila from HR: Hi, this is Sheila, I got logged out of my computer can you direct me to change my password
* From Kevin from Account: Hi, this is Kevin, Could you please click the link to enter your daily hours? Again, your login is your computer login

5). Summary: [Insert team] had a nice lunch at Salvatores. On their way back they realized the company building was being swarmed by protestors, therefore they can’t continue their work.

Effect: Blue Team can’t work for 15 mins

8). Janitors come in to do cleaning on specific PCs. Those PCs must be vacated for (time amount) while they clean

Effect: Distracts a [insert team] member

Affected: Blue Team 1 or Blue Team 2 or Red Team

8b) Janitors come in to do cleaning on specific PCs. Those PCs must be vacated for (time amount) while they clean. The janitor is a Red Team member.

Effect: Red Team can prebake

Affected: Blue Team 1 or Blue Team 2

13). Bring your child to work day? There was an accident, go to bathroom and get a DRY paper towel. We don’t want the PCs to get wet ;(

# 

# **Actually Annoying**

| **Inject #1** | Name: Corporate Silly Day Inject |
| --- | --- |
|  | Service: N/A |
|  | Goal: Distract a Team Member |
|  | Description:  It’s corporate Silly Day. Take a pic of a teammate in their silliest pose. Be careful, the other IT team will get more bonus points if they take a pic of your teammate doing their silliest pose  Effect: Distracts a member  Affected: Blue Team 1 or Blue Team 2 |
|  | Submission: physically show the photo to white team |
|  | Email:  TO: blue teams  FROM: [cbeaver@clfc.com](mailto:cbeaver@clfc.com)  SUBJECT: Corporate Silly Day  It's Corporate Silly Day! I almost forgot this wonderful tradition with all of the stress from the merger. Since most of you are new here, I’ll give you the rundown.  You have 15 minutes to take a picture of your teammate in their silliest pose. But, be careful, because you could lose the opportunity of getting full points if the other IT team takes a photo of YOUR teammate in their silliest pose, so be discreet.  I have other office members posted around the work area for you to go to once you have taken your photos (one photo per team member). However, they may send you back to your desk if they deem your photo not silly - this can also result in losing the opportunity to gain full points.  I look forward to seeing all your smiling faces on this beautiful day,  Cal Beaver |

| Inject #2 | Name: |
| --- | --- |
|  | Service: |
|  | Goal: |
|  | Description:  15). The EPA is here! The Frackin’ IT team must hide or get taken away for questioning on Cal Beaver’s secret activities.   * The team members who are still sitting in their seat get taken away for a 1-2 minute interrogation * Targets whichever blue team is supposed to be the Frackers   This has the potential to be funny |
|  | Submission: |
|  | Email: |

| Inject #2 | Name: Hunt for Garrett |
| --- | --- |
|  | Service: N/A |
|  | Goal: Remove 1-2 Team Members |
|  | Description: Teams must decipher a riddle and go to Professor Garret’s office to receive a piece of paper either from him or his mailbox |
|  | Submission: |
|  | Email: See separate PDF |

7). Summary: “Team Member B, get me a bacon, egg, cheese and avocado bagel with a frappuccino, 37% cream, 3 sugar cubes. If you get my order wrong you will get your pay (points) docked”

* A delta team member stands outside the room and will do something like type up the order as dictated by Team Member B from B’s memory
* B gets a paper or email of what was typed up and brings it back to show completion
* Make them go to Ctrl Alt Deli and order actual food using a dining bucks gift card NOT their own money or bucks

Effect: Distracts a blue team member

Affected: Blue Team 1 or Blue Team 2

14). Anti fracking protesters and old regulars of the mom and pop shop joined forces and are storming the building! Select 2 team members (could be every team sending team members) to literally tell them “no, go away” or “get a job” (no physical contact and only language)

* Maybe mention in the inject specifically what to do so rule 2 (being respectful and professional) isn’t broken

16). Cal Beaver sends an email asking for thoughts on his presidential campaign: We Frack, We Snack, We Bring Jobs Back. Government subsidies for fracking corporations, free snacks for K-12 and creating jobs via Big Oil

* Targets a specific team member and they must say what he wants to hear or their team loses points
* Write the email in a way that it’s very obvious that he lives in echo chamber: “My campaign’s perfect. There has never been a better presidential campaign in the history of presidential campaigns.”

17). Cal Beaver sends a very angry to Red Team because a very young family member of one of the member’s posted on X (Twitter) criticizing CLFC (it only has 3 likes)

* One (or all red team members) write a formal apology email to Cal or else he will pull the plug on their PCs (or maybe yell at them for 3 minutes)
* Goal: Waste red team’s time

# Technical Injects

| Inject #1 | Name: Snake in the Grass |
| --- | --- |
|  | Service: |
|  | Goal: |
|  | Description:   * Have an inject where they need to find a “flag” or a “password” or something   + Create a python script for them to test the flag against     - The python script would be only viewed and edited by an admin, so they do not have access to it   + The password they are looking for could be in a file or image or something     - Maybe someone forgot their password and its ITs job to do this to “retrieve it”   + Submission: would be the password as well as the “success” message from the python script |
|  | Submission:  would be the password as well as the “success” message from the python script |
|  | Email: |

| **Inject #2** | Name: Work Hour Correction Inject |
| --- | --- |
|  | Service: MailServer |
|  | Goal: To Test Phishing Skills |
|  | Description:  Perrtdy HR is concerned that you have not properly logged your hours for work. It seems like a few hours are missing.  Blue team members would click the link to verify their work hours.  Phishing email.  Slightly altered email that looks like sheila’s but it is not. |
|  | Submission:  Full points: if they respond by emailing Cal saying that they dont think this is sheila and did not click the link.  Half points: if they were suspicious, but clicked the link and sent a screenshot of the first page.  No points: if they clicked the link and send in a screenshot of the second page of the website. |
|  | Email:  TO: [blue1@clfc.com](mailto:blue1@clfc.com)  FROM: shieIa.clfc.com (the lowercase L is replaced by an uppercase i)  SUBJECT: Work Hours Correction  Hi, this is Sheila from HR!  I was looking through your logged work hours and I noticed a little inconsistency. I was wondering if youplease click the link below to fix it. Let Mr. Beaver know when you are finished!  Thank you,  Shiela  Attached: <<url>>  (the grammar mistakes are to make them suspicious of it being a phishing email) |

| **Inject #3** | Name: IP / Domain Background check |
| --- | --- |
|  | Service: Virus Total |
|  | Goal: Test Team members ability to perform risk assessment and management |
|  | Description: Send a list of IP’s and Domains to the Blue team and propose that these be requested for the creation of future VM’s and Internal Phishing Campaigns. The team must determine which are clean and which pose potential risks to the company. |
|  | Submission: A Breakdown of each domain/IP and the results of their research - Are they safe? Why not? Should the request to use them for a VM be approved? Should they be considered for the upcoming Crack-A-Lackin’ Frackin’ Phishing Campaign? |
|  | Email:  TO: [blue1@clfc.com](mailto:blue1@clfc.com)    Dear IT Team,    Listed below is a list of Domains and IP Addresses that are being requested across the company to be used in soon to be spun up Virtual Machines and the upcoming CLFC Internal Phishing Campaign. We need you guys to analyze each item in the list and summarize if they are safe to use and whether or not you recommend using them for the upcoming phishing campaign. We expect your responses to be thorough and because your jobs are not yet secured, all information will be double checked to measure your accuracy and efficiency. Time is of the essence!  WE DO NOT SUGGEST CLICKING ON ANY OF THESE  “ scam[.]com”  “ facebookztv[.]com”  “ adminsecurity101[.]com”  “ fractracker[.]org”  “ 45[.]116[.]226[.]15”  “ 171[.]25[.]193[.]78”  “ 127[.]0[.]0[.]1”  “ 129[.]21[.]31[.]88”  Good luck and I will be in touch soon,  Cal Beaver  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  *Cal Beaver*  *CEO, Crack-A-Lackin Frack’n Co.*  *(248)434-5508* |

| **Inject #4** | Name: More Friends, More Good Inject |
| --- | --- |
|  | Service: Windows User Desktop |
|  | Goal: Create 3 New Users |
|  | Description:  We will task the blue teams to create 3 users for the new interns. Since they are interns, they must have the lowest levels of access. They can read files and write their own, but they cannot execute or edit already existing files. |
|  | Submission: picture proof of the users added and their permissions |
|  | Email:  TO: blue teams  FROM: [cbeaver@clfc.com](mailto:cbeaver@clfc.com)  SUBJECT: New Interns!  I have recently hired 3 new interns to start working with us! I am giving you the task of making 3 new users on our network so they can start working right away. Here are their usernames and passwords:  Natasha Boulevard  nboulevard  PW: securepassword!?  Owen Ipswitch  oipswitch  PW: betterpassword!?  Lacy Smith  lsmith  PW: morepassword!?  Since they are interns, they only need to read files and write their own, but they cannot execute or edit already existing files. I’ve never met any of these people but I’m sure that they are wonderful to work with and totally not fake!  You have 15 minutes to complete this assignment and when you are done, send me an email with proof of their permissions.  Good luck and I await your response,  Cal Beaver |
|  | Scoring:  Full points: if they create the users like we asked them too and gave them the correct permissions  Bonus points: if they say they created the users and then disabled them because Cal’s email was suspicious and their passwords are not secure either |

| Inject #5 | Name: My Old Rival |
| --- | --- |
|  | Service: amcache.hve |
|  | Goal: To use amcacheParser to see the logs |
|  | Description: Blue Team will analyze a file/program that was placed on the system using AmcacheParser |
|  | Submission: |
|  | Email:  TO: blue teams  FROM: [cbeaver@clfc.com](mailto:cbeaver@clfc.com)  SUBJECT: Hacked account!  According to the FBI, one of our Grey Team machines was hacked. We believe this was done by Markus Green, my old friend. He couldn’t accept that my earth-destroying company was better, so he resorted to this tactic. Anyways the account has access to all accounts. They have given us instructions on how to find the file  “Using the AmcacheParser.exe in your downloads folder, analyze what the attack placed.  Open task scheduler and Microsoft Compatability Appraiser in Microsoft> Windows> Application> Experience. This will make sure the amcache is up to date.  Run the command AmcacheParser.exe -f Amcache.hve --csv ./  Where the correct file paths are used. The .hve should be in C:\Windows\appcompat\Programs.  Analyze the unassociated file entry csv”  The assailant had the account between .Give the file hash (SHA 1), the timestamp, the program id and threat level. A screenshot must be taken and submitted using the csv file, this must also be added to any report that is being drafted at the moment.  Since this assignment is very important, you have until the end of the day. It is important to note that the first team to have this done will get a bonus of 5 points. There will be 1 point for every malicious tool found.  (The email should include the amcache parser and libreoffice which are in the email machine downloads. This request should happen after a inject that prevents the blue team from using the machines so that we can log in and do a pip update. Fun fact, nothing malicious was downloaded yet.) |

* Maybe one analyzing packet captures?
* Simple create these 5 users and give them these permissions” inject
  + Create users with these passwords
  + Give extra points if they show that they disabled the users
* Create a database in mysql? Or do we give them a large csv file and have them give us different tables and stuff showing different information?
* Blocking an ip and having them submit a ping test as proof
* Very simple inject of finding the ip address of every machine and submitting that to us
* Create a new directory, move files to that dir and change permissions on the file
* “Question-and-answer problems. For question-and-answer problems, the competitor must find the correct answer to one or more questions by performing challenge tasks. The answers to the challenge questions can take several forms, such as entering file paths, IP addresses, hostnames, usernames, or other fields and formats that are clearly defined.” <https://insights.sei.cmu.edu/blog/designing-great-challenges-for-cybersecurity-competitions/>

“Several business injects are documented on the web. These include:

• Rebrand the entire web presence with the new corporate name and logo images

• Configure SSH

• Install and configure WSUS for updates

• Implement VPN access

• Install a “live chat” function on the web page

• Write a corporate policy covering appropriate use of social networking sites

• Perform a security assessment on your own network and write a report

• Upgrade workstations to Win7

• Perform a password strength audit on your systems and write a report

• Pack up all the equipment at the end of the competition

• Install Snort in less than 2 hours

• Rehost E-Commerce site from one web server to another while maintaining

service functionality

• Opening an FTP service for 2 hours given a specific user name and password

• Closing the FTP after the 2 hours is up

• Creating/enabling new user accounts

• Auditing a user’s activities through system logs

• Installing new software package on CEO’s desktop within 30 minutes “

<https://www.nationalcyberwatch.org/wp-content/uploads/2016/03/NCC_Press_How_To_Prepare_For_the_CCDC-1.pdf>

Incident Response Report

In CCDC events, a thorough, well-written Incident Response report on Red Team

activity can reduce a team’s penalties. The report is part of the incent response

process. CCDC alumni describe an eight step process for incident response which

should help teams lessen the impact of the Red Team’s activities.

1. Throughout the competition, teams should be gathering information. In order

to determine if a system has been compromised, collect evidence from multiple

sources

2. If an attack has occurred, document the business impact of the problem; the

mock-CEO will want to know this.

3. Next, create hypotheses about what has been done to the system(s); verify the

hypotheses with the evidence that was collected.

4. Document the team’s problem solving process.

5. Decide on a plan.

6. Execute the plan.

7. Document the steps the team took to remediate the problem AND prevent a

future problem of this sort.

8. Complete the incident report. If possible, the report should include the Red

Team

DAY THREE:

* Sandwich inject
  + Execution: give them a paper inject that is designed like a note from cal saying that he wants a sandwich from the deli in the cafeteria
  + Purpose: to get team members afk from camping wireshark
  + Submission: a photo of a “fake sandwich” we planted at the deli OR put pics of sandwiches in another golisano location and call that the “cafeteria” OR maybe just a pic of the deli?
* EPA is here!
  + Execution: The IT teams must hide or get taken away for questioning on Cal Beaver’s secret activities. (we give them 15 seconds to hide)
  + Consequence: The team members who are still sitting in their seat get taken away for a 1-2 minute interrogation
  + Purpose: to get team members away from camping wireshark
* Timeclock sheila
  + Execution: we slack them a pdf of the email from sheila with the link and if they click it, they lose points
  + Execution Idea 2: we hand them a piece of paper that's the printed out version of the email so they have to type in the URL for the link on their machines
    - Benefits: this reduces confusion and will not take them to the church website
    - Cons: it might be harder to figure out that its not actually sheila’s email
  + Execution Idea 3: We hand them a piece of paper that has a handwritten note from sheila
    - Benefits: this gets rid of the confusion for the link and requires them to type it in
    - Cons: this gets rid of the phishing email part, how did the note get there? Is there an insider spy?
  + Purpose: technical inject for phishing / keeping the company safe
  + Submission: a picture of the website or an email saying “i am not clicking the link”
* Cal is being Cheap
  + Execution: Cal sends a message to both blue teams on Slack demanding they stop using a service (most likely Wireshark) because it costs too much money. It will take 5 minutes (we time it or we go by the scoreboard) for someone to explain that Wireshark is free
    - Pros: stops Wireshark camping, encourages other tools, gives time for red team to do stuff, is annoying, **deduct points if they fail?**
    - Cons:
    - Submission: either someone types up a full essay with citations on why Cal is wrong or no submission