# Introduction

April 7, 2024

Welcome to Palmetto Crossing, a quaint town that prides itself on its "by citizens, for citizens" approach to utility offerings. The **Palmetto Crossing Department of Commerce (PCDC)** team works around the clock to ensure all citizens of Palmetto Crossing receive prompt, professional and excellent customer service from all utility providers within the city. Through its comprehensive services, PCDC works closely with local entrepreneurs, business leaders, and governmental agencies to ensure that the city remains a vibrant hub for innovation and opportunity. With a forward-thinking approach, the PCDC team is committed to making a positive impact on both the local and regional economies, ensuring long-term prosperity and stability for future generations. As part of its core mission, the department focuses on the strategic development and efficient delivery of utility services to ensure a thriving and sustainable community. The PCDC team is the reason Palmetto Crossing is able to maintain the quality and reliability of essential utilities such as water, electricity, and waste management. Through its efforts, PCDC plays a key role in supporting economic growth and fostering a high standard of living for all who reside within the area. With a strong commitment to customer satisfaction and sustainable practices, PCDC ensures that Palmetto Crossing remains a well-equipped, forward-thinking municipality where residents and businesses can thrive.

PCDC strives to continue offering consistent, affordable and reliable utility services to all citizens of Palmetto Crossing. Attentive customer service, friendly staff and attention to detail are what set the PCDC team apart from others. Enjoy your time in Palmetto Crossing!

**Palmetto Crossing Department of Commerce**

Empowering Growth and Building Futures

https://pcdc-sc.com

April 7, 2024

Blue Team,

Welcome to the Palmetto Crossing Department of Commerce! We are excited to have you on board as the new IT team, and we are confident that your expertise and fresh perspective will help drive our technology initiatives to new heights. As a key part of our organization, your role is vital in ensuring our systems, infrastructure, and digital services continue to run smoothly, efficiently, and securely.

The Department of Commerce plays a pivotal role in fostering economic growth, providing support to businesses, and driving the local economy. In today's rapidly evolving technological landscape, our department relies on cutting-edge solutions and seamless systems to achieve these goals. We need you to maintain and protect financial and customer databases, internal communication systems, API interfaces, and many other critical system functions, ensuring continuous service to our customers.

Your team must ensure Confidentiality, Integrity, and Availability is maintained using secured, encrypted data transmission protocols, firewalls, VPN tunneling for remote desktop support, and professional communication to multiple clients as needed on a day-to-day basis. Your team must also answer trouble calls from customers and special requests from various utility representatives. It is of the upmost importance that critical services remain available to ensure continued functionality of the city's infrastructure and necessary teams.

As the risk of data breaches, ransomware, phishing, and denial of service attacks continue to grow, it is paramount the security of our infrastructure be of the utmost importance to preserve our customer's satisfaction. PCDC has hired your team to ensure all databases are secured, company and customer information is protected, and professional service is always provided. Unfortunately, the previous team abruptly vacated their positions, so we cannot guarantee the current state of any service or accuracy of the network diagram.

PCDC is confident your team will help keep all the citizens of Palmetto Crossing satisfied. We are excited to have you as part of our exceptional team!

**Welcome to Palmetto Crossing Department of Commerce (PCDC)!**

Regards,

Roger Wakefield, CEO

# TABLE OF CONTENTS



# LIST OF APPENDICES

# 1.0 ACCOUNT INFORMATION

## 1.1 Initial Password List

At the start of the day, your team will be provided with your initial username and password information for all assigned assets.

## 1.2 Password Changes

Changes of domain user accounts need to be reported to the Gold Team. Please submit password changes to the Gold Team Ticketing service to lessen service check downtime. Failure to promptly report changes to domain user accounts can negatively impact service checks from the competition scoring engine. DO **NOT** CHANGE THE GOLD TEAM PASSWORD.

## 1.3 Email Access

Blue Teams will access their web-based email through the following web address: **https://mail.blueXX.pcdc.local** which is in scope. Any email from @pcdc.local is out of scope from the Red Team, however, that does not mean all emails from @pcdc.local are credible. All emails should be evaluated properly, and any suspicious activity should be reported immediately. Roger Wakefield (roger.wakefield@blueXX.pcdc.local) is the Chief Executive Officer for Palmetto Crossing Department of Commerce and will be receiving various messages throughout the day. You are required to monitor this account at all times.

# 2.0 NETWORK OVERVIEW

Your assigned network consists of virtual machines that are accessed via standard remote access protocols (RDP and SSH) from the assigned laptops. Usernames and passwords for all assets will be provided in the Initial Password List at the start of competition. An old network diagram was found and is located in Appendix A. Your network will consist of a mix of Windows and Linux operating systems.

## 2.1 Backups and Recovery

Teams do not have access to create backups of VMs, nor to recover a VM. Recovery requests can be submitted via a ticket to the Gold Team Help Desk. Select ***Request*** as the ticket category and use the following format:

**SUBJECT:** Recovery Request
**BODY:**
Team #: _____
Request: _____
Justification: _____

If you do not use the correct request format, your recovery request will not be completed by Gold Team. A detailed justification is required. Please note that recovery comes with a **substantial cost** and reverts the machine to its initial operating condition.

### 2.2 Active Defense

While this term is still being defined in industry (some say it includes offensive capabilities and others say it does not), we are referring to Defending Forward – countering or preventing a perceived cyber-attack by taking the fight to your adversary with the goal of taking away their ability to perform offensive cyber operations against you. This is **not permitted under any circumstances**. Teams should keep their actions within their own assigned assets.

### 2.3 Incident Reporting

Accurate incident reports that can be verified will net your team a modest number of points in the end-of-day team assessment. Incident reports must contain a description of how and what occurred (including source and destination IP addresses, timelines of activity, passwords cracked, access obtained, damage done, etc), a discussion of what was affected, and a remediation plan. Overly inaccurate Incident Reports, especially abuse of Incident Reports, will net no points and may result in a loss of points.

Written reports must be coherent, detailed and professional. Should you recognize that an incident has occurred, you may escalate an incident response report by submitting a ticket to the Gold Team Help Desk. Select ***Incident*** as the ticket category and use the following format:

**SUBJECT:** Incident Reporting
**BODY:**
Team #: _____
Time(s) of Incident: _____
Asset(s) Affected: _____
Source (IP Address) of Attack: _____
Description of Attack/Incident: _____
Remediation/Plan to Resolve: _____

## 2.4 Firewall Requests

The perimeter firewall will be managed by the PCDC Gold Team. All requests to modify the perimeter firewall must be submitted to the Gold Team via the Help Desk Ticketing system by selecting the ticket category ***Request*** and submitting a detailed request, including IP addresses and a defined justification. Host based firewalls may be managed by the Blue Teams.

## 2.5 Laptop Information

Certain programs and applications have been setup on the laptop for use during the competition. They include but are not limited to:

- puTTY (SSH)
- Remmina (RDP)
- Chrome
- KeePass

## 2.6 Out of Band Information

The below items are out of band. Please pay careful attention to this section.

- The laptops are out of band and are fully out of scope from the Red Team.
- The account "goldteam" on all physical machines, virtual machines and network devices is out of band and off limits for all Blue Teams and the Red Team.
- All traffic and devices on the 192.168.40.0/24 network are out of band for the Red Team. Blue Teams are **not authorized** to block traffic from this network.
- Edge routers are off limits and out of band for all Blue Teams and the Red Team.
- Blue Teams are **not authorized** to block traffic from 192.168.20.10.

## 2.7 Out of Band Email

Blue teams will be given an Amazon WorkMail account that will be used for email and Gold Team Help Desk access. This account is out of scope for the Red Team. This account will be used for inject distribution, submitting injects and access to the Gold Team Help Desk. Please verify access to this email at the start of the competition, and let White Team or Gold Team know if there are any issues with the account. The Amazon WorkMail site can be reached at:

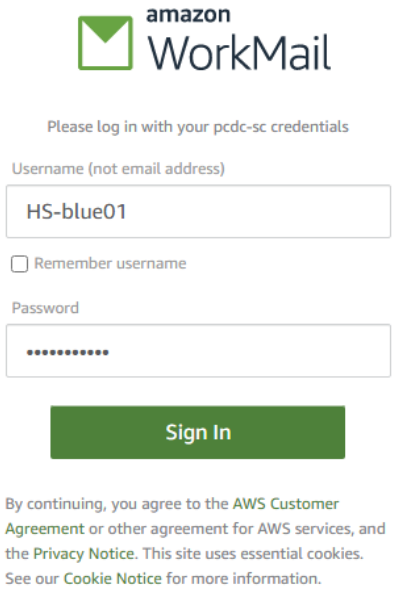
https://pcdc-sc.awsapps.com/mail

Account format is:

HS-blueXX@pcdc-sc.org
COL-blueXX@pcdc-sc.org
PRO-blueXX@pcdc-sc.org

Passwords will be provided the day of competition.

Pay close attention to the login page – you are to use your username only, NOT your full email address, as shown below.



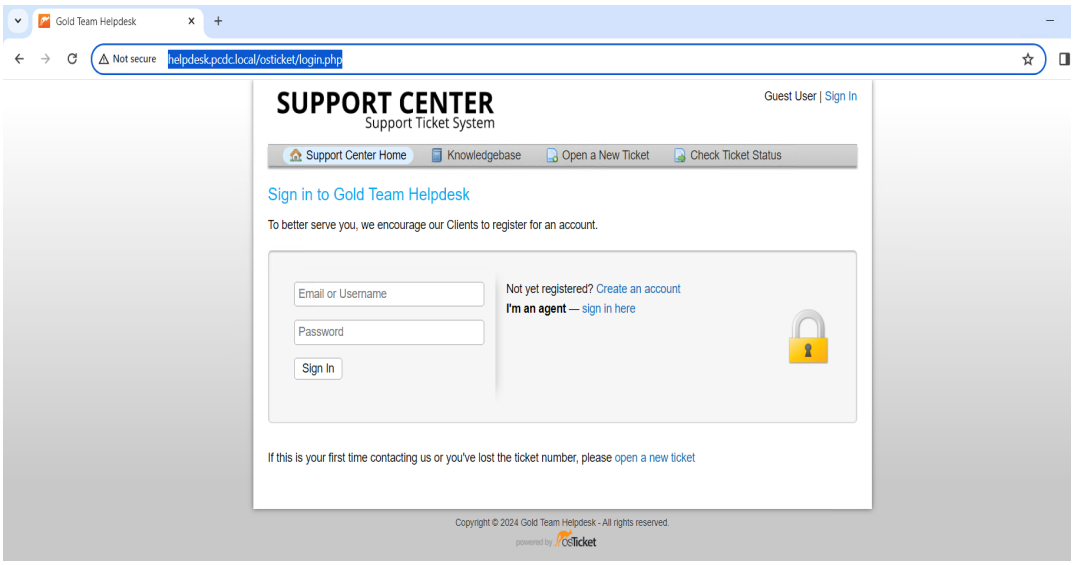

As a reminder, communication with other teams or any person(s) not a part of your respective Blue Team is **strictly prohibited.**

## 2.8 Gold Team Help Desk

There will be an online Help Desk system provided for teams to request assistance from the Gold Team. The Help Desk can be reached at:

http://helpdesk.pcdc.local/osticket/login.php.

The Gold Team Help Desk will respond as soon as possible to your ticket. The Help Desk chat function will also be available to use as needed.




## 2.9 Physical Table Components

The 2025 competition will include physical boxes on the competitor tables as part of the scenario. These boxes contain proprietary microcontrollers and various electrical components to simulate critical and non-critical utility services on the board. The microcontrollers and other items within the box are logically **in scope** for Red Team and should be secured as part of the network. However, the boxes themselves and everything in them, are **not to be touched** by any member of a Blue Team or Red Team, unless given explicit permission from a Gold Team Lead.

# 3.0 TEAM ASSESSMENT

Employee performance is assessed at the end of each day. A single score is given to each team of employees.

## 3.1 Scoring

Scoring is based on keeping required services up, controlling/preventing unauthorized access, completing business tasks (a.k.a. injects) from colleagues, supervisors, and other departments throughout the day, and continuing to provide critical business products/services. Teams accumulate points by successfully completing these injects and maintaining services. Teams lose points by violating service level agreements, usage of recovery services, and successful penetrations by hackers, a.k.a. the Red Team.

Any team action that interrupts the scoring system is exclusively the responsibility of that team and will result in a lower score. Any team member that modifies a competition system or system component, with or without intent, in order to mislead the scoring engine into assessing a system or service as operational, when in fact it is not, may be suspended or fired. **Validation of this act will come with a significant points penalty** as it gives the Blue Team an unfair points advantage for a service that is not actually up.

### 3.2 Injects

If a business task (a.k.a. inject) requires multiple files for fulfillment, please compress the files into a single file in .zip format. This ensures that each inject has only one upload. Please name inject emails/files in the following format:

**<teamNumber>_<injectNumber>_<injectTitle>**

**Injects and services are weighted evenly; it is disadvantageous to ignore injects.**

There will be no partial credit for late injects, so make a point to fulfill injects on-time. Inject responses that are submitted on-time will be allowed at least partial credit. Gold Team and PCDC Leadership/Judges reserve the right to change this policy as needed, and will notify all teams at the same time of any changes.

If an inject is directed to be submitted to the Gold Team Help Desk, select the ticket category ***Inject*** when creating the ticket.

## 4.0 ADDITIONAL INFORMATION

### 4.1 Blue Team Tools and Supplies

At the start of competition there will be supplies provided that could include notepads, pens, mouse pads, dry erase board markers and erases, folders, and network cable tools. Please be sure to leave these on the team tables at the end of the day.

### 4.2 Scripting

Scripting during the competition is allowed, and teams are encouraged to write their own scripts. All team written scripts should be submitted to the Gold Team Help Desk for review and approval prior to use. Any resources or tools pulled down from the internet to assist with scripting shall be **publicly available and free of cost.** The use of scripts or tools not created by the team should be submitted to Gold Team by opening a Help Desk ticket, **including the citation** for the tool or resource used if applicable. Failure to notify Gold Team of script or tool usage that was not provided by the Gold Team, or the use of non-public resources **may incur a penalty.**

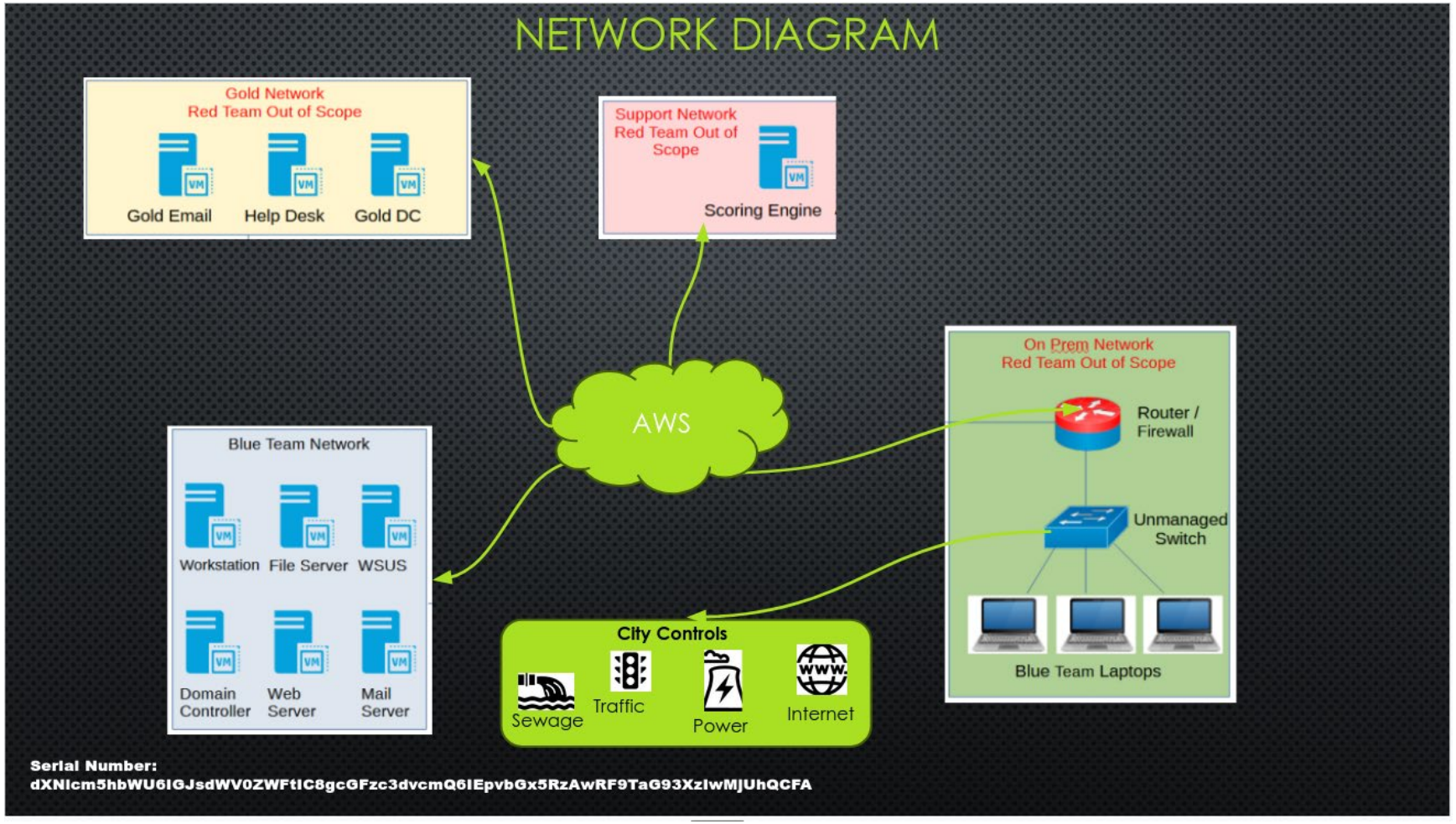
If the blue team has written a script in advance of the competition, it may only be brought into the competition typed and printed on a sheet of paper or hand-written in a notebook. It must be submitted to the Gold Team Help Desk including any sources used for approval.

To submit a script or resource to Gold Team for approval, create a ticket with ***Request*** as the ticket category and use the below template:

**SUBJECT:** Resource Approval Request
**BODY:**
Team #: _____
Resource Name: _____
Citation: _____
How Resource Will Be Used: _____

The request must be approved by Gold Team **prior** to use.

# Appendix A Network Diagram



# Appendix B PASSWORD TRACKER

| Username | Password | Account Description |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Appendix C ORGANIZATION CHART

This list only contains the Palmetto Co-Op Doctors Clinic department leads and does not include all Palmetto Co-Op Doctors Clinic employees.

| First Name | Last Name | Position | Domain Admin |
|---|---|---|---|
| Roger | Wakefield | CEO | No |
| Olivia | Russell | CISO | No |
| Kathleen | Gonzalez | CFO | No |
| Kathryn | Sawyer | Water Quality Assurance Lead | No |
| Ralph | Ferry | Sewage Help Desk Lead | No |
| Grace | Ziegler | Power Generation Lead | No |
| Jennifer | Gray | Regulatory Compliance Lead | No |
| Carl | Baker | Maintenance Lead | No |
| Cynthia | Schuster | Energy Help Desk Lead | No |
| Dorothy | Lawless | Sales and Marketing Lead | No |
| Sophia | Resnick | Network Help Desk Lead | No |
| Amber | Bongard | Lead Enterprise Administrator | Yes |
| Megan | McCormack | Lead Network Administrator | Yes |
| Hannah | Baker | Human Resources Lead | No |

This Page Intentionally Left Blank