



# Demo Day Presentation

By Robert Ajegbo



# Introduction:

- My name is Robert Ajegbo and I am an aspiring Cyber Security Analyst with a background in Physiology and Pharmacology
- I made the decision to shift away from health sciences and pursue a career within the technology industry because I have always had a passion for tech, and I feel like this is the exact time to join this evolving sector
- Cyber Security felt like the best option due to what interested me and the flexibility for future opportunities



# Presentation Focus

- In my project, I have chose to give a brief background on the scenario and the main vulnerability that led to the cyber incident
- I will then shift focus to a summary of security recommendations that I listed as far as reactive measures to deal with the incident at hand and proactive measures to prevent future incidents from occurring

# Project Background

From: 4C484C@qq.com

To: support@premiumhouselights.com

Hello,

We will go right to the point. We are in possession of your database files, which include sensitive in

You wouldn't want this information to be out on the internet, would you? We will release this informat

1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid

by Monday at 10:00AM UTC.

To demonstrate to you that we aren't just playing games, here is a snippet of your customer database t

contactFirstName	contactLastName	phone
Carine	Schmitt	40.32.2555
Jean	King	7025551838
Peter	Ferguson	03 9520 4555
Janine	Labrune	40.67.8555
Jonas	Bergulfsen	07-98 9555

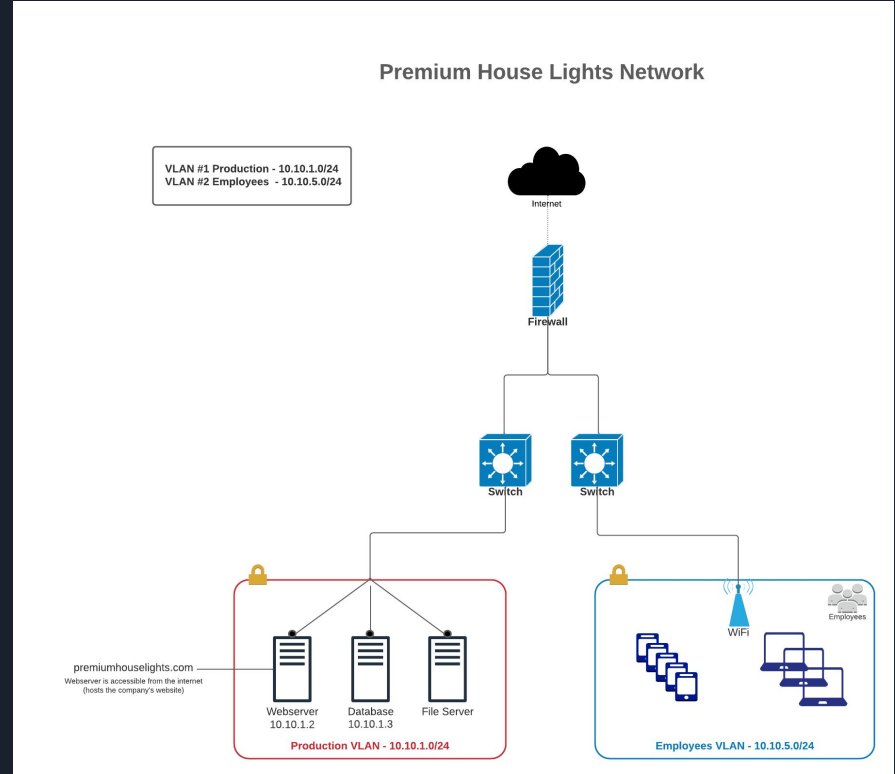
Now the ball is in your court to make the right decision and take action. There will be no negotiation

// The 4C484C Group

- Premium House Lights Inc. is a mid-sized company based in Ontario, Canada and they have just suffered a major data breach
- The primary victims of the the attack were their customers as the hacker group copied and stole a customer database, which revealed all of the personally identifiable information of their clients
- There were multiple contributing factors to this incident but the main vulnerability was within their network layout

# Primary Vulnerability

- The main contributing vulnerability to this breach was a lack of network segmentation within the network layout
- Network segmentation is the process of isolating critical systems away from less secure areas on the network
- In this example, the attackers breached the web server through the internet using brute force techniques and then they were able to move laterally to the database simply



# Key Recommendations

Recommendations include but are not limited to:

- Patch systems
- Multi-Factor Authentication
- Network Segmentation
- Data Encryption and Access Control



Thank You for listening!

