# Common Services

**Sign-In:**
https://jessh.zip/ccdcw624

# whoami

Dylan Tran | @nigerald

CIS 2025

Ex Intern @ X-Force Red

**Linux @ CCDC (2021-2024)**

**Windows @ CPTC (2021-2024)**

# Agenda

1

**Services**

Thats it lol

# Today's Objectives

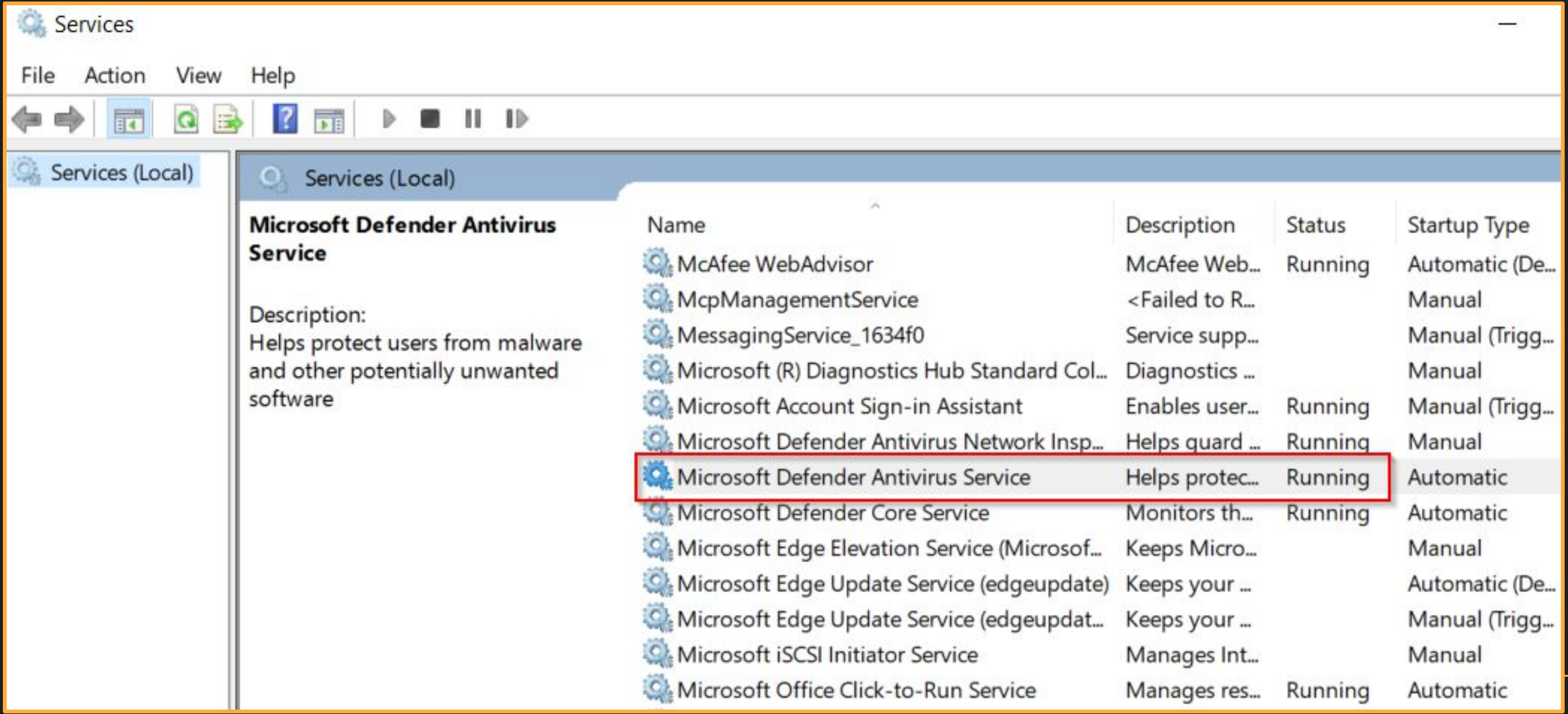
- ❏ Identify what a service is
  - ❏ Identify services present on a system
- ❏ Identify common CCDC services
- ❏ Understand service methodology
  - ❏ Install
  - ❏ Troubleshoot
- ❏ Understand service security
  - ❏ Configurations
  - ❏ Triaging

# What is a Service?

1. Background process running on a host - "Host Services"
2. A functionality served by the business - "Business Services"
    - **Purpose**
        - To users -- public facing
            - SLAs
        - To business users -- internal

***Not 1:1***

# Example: Host Service



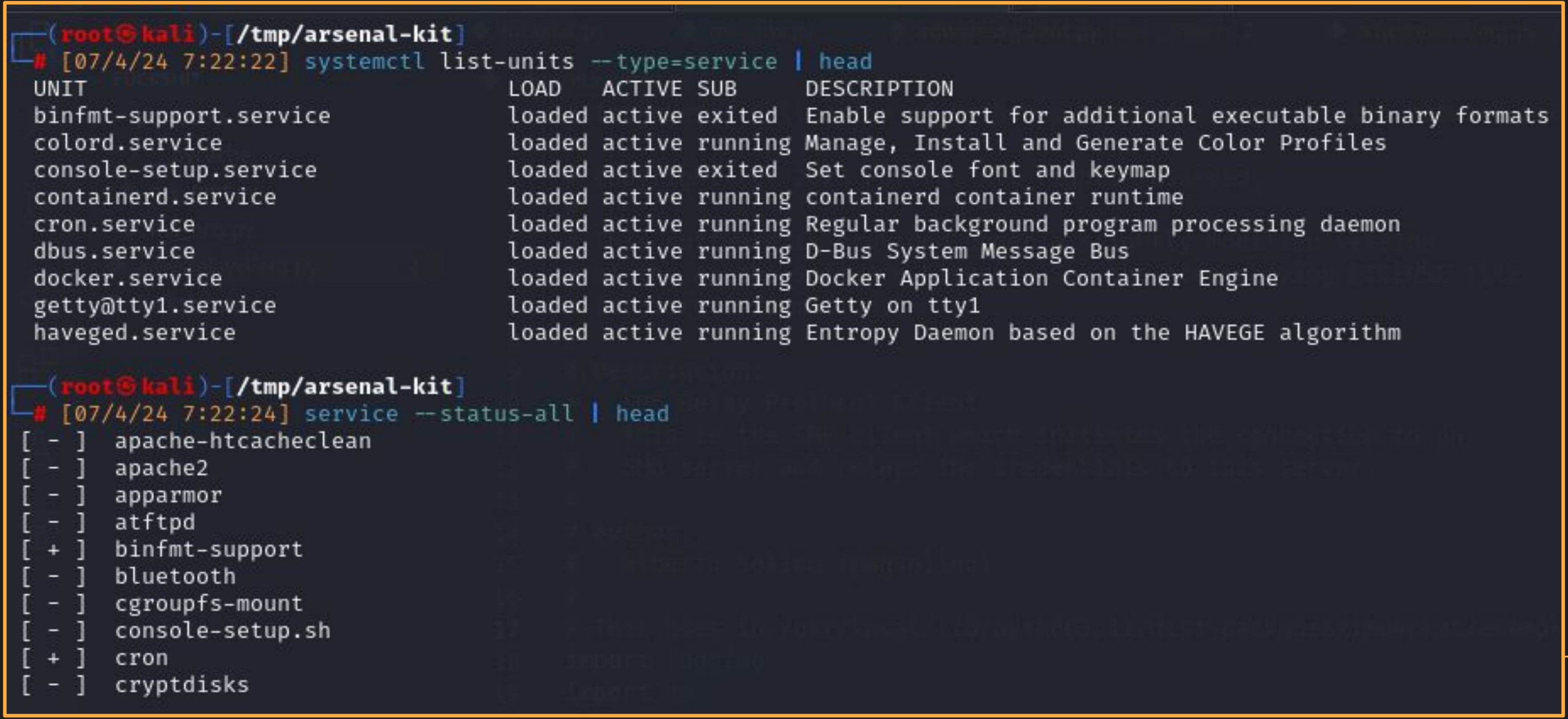
**Microsoft Defender Antivirus Service**

Description:
Helps protect users from malware and other potentially unwanted software

| Name | Description | Status | Startup Type |
|---|---|---|---|
| McAfee WebAdvisor | McAfee Web... | Running | Automatic (De... |
| McpManagementService | <Failed to R... | | Manual |
| MessagingService_1634f0 | Service supp... | | Manual (Trigg... |
| Microsoft (R) Diagnostics Hub Standard Col... | Diagnostics ... | | Manual |
| Microsoft Account Sign-in Assistant | Enables user... | Running | Manual (Trigg... |
| Microsoft Defender Antivirus Network Insp... | Helps guard ... | Running | Manual |
| Microsoft Defender Antivirus Service | Helps protec... | Running | Automatic |
| Microsoft Defender Core Service | Monitors th... | Running | Automatic |
| Microsoft Edge Elevation Service (Microsof... | Keeps Micro... | | Manual |
| Microsoft Edge Update Service (edgeupdate) | Keeps your ... | | Automatic (De... |
| Microsoft Edge Update Service (edgeupdat... | Keeps your ... | | Manual (Trigg... |
| Microsoft iSCSI Initiator Service | Manages Int... | | Manual |
| Microsoft Office Click-to-Run Service | Manages res... | Running | Automatic |

*Windows Key + r ⇒ services.msc + enter*

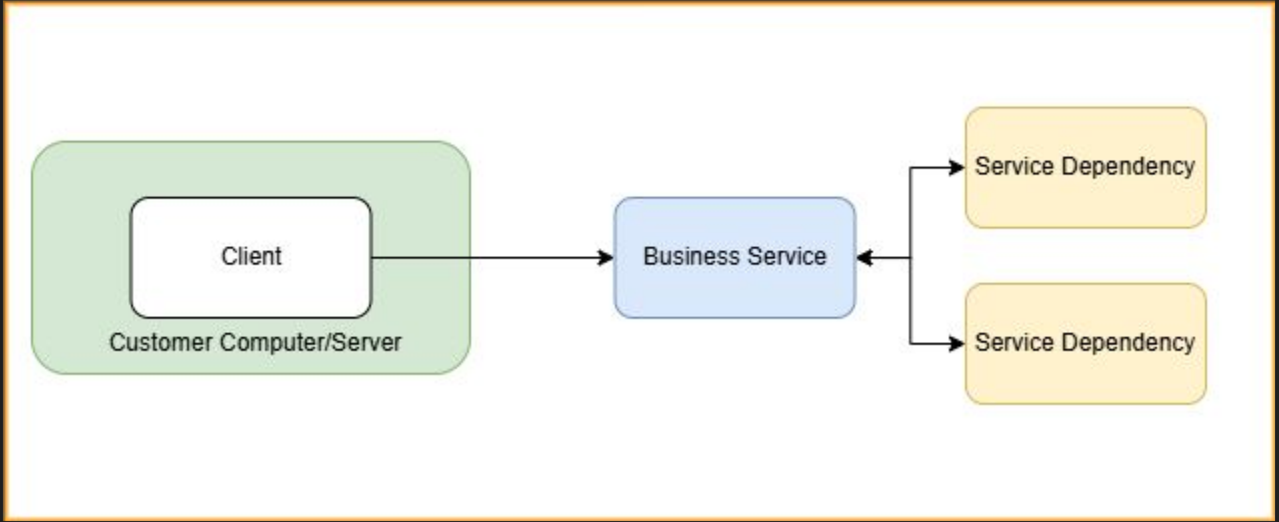
# Example: Host Service



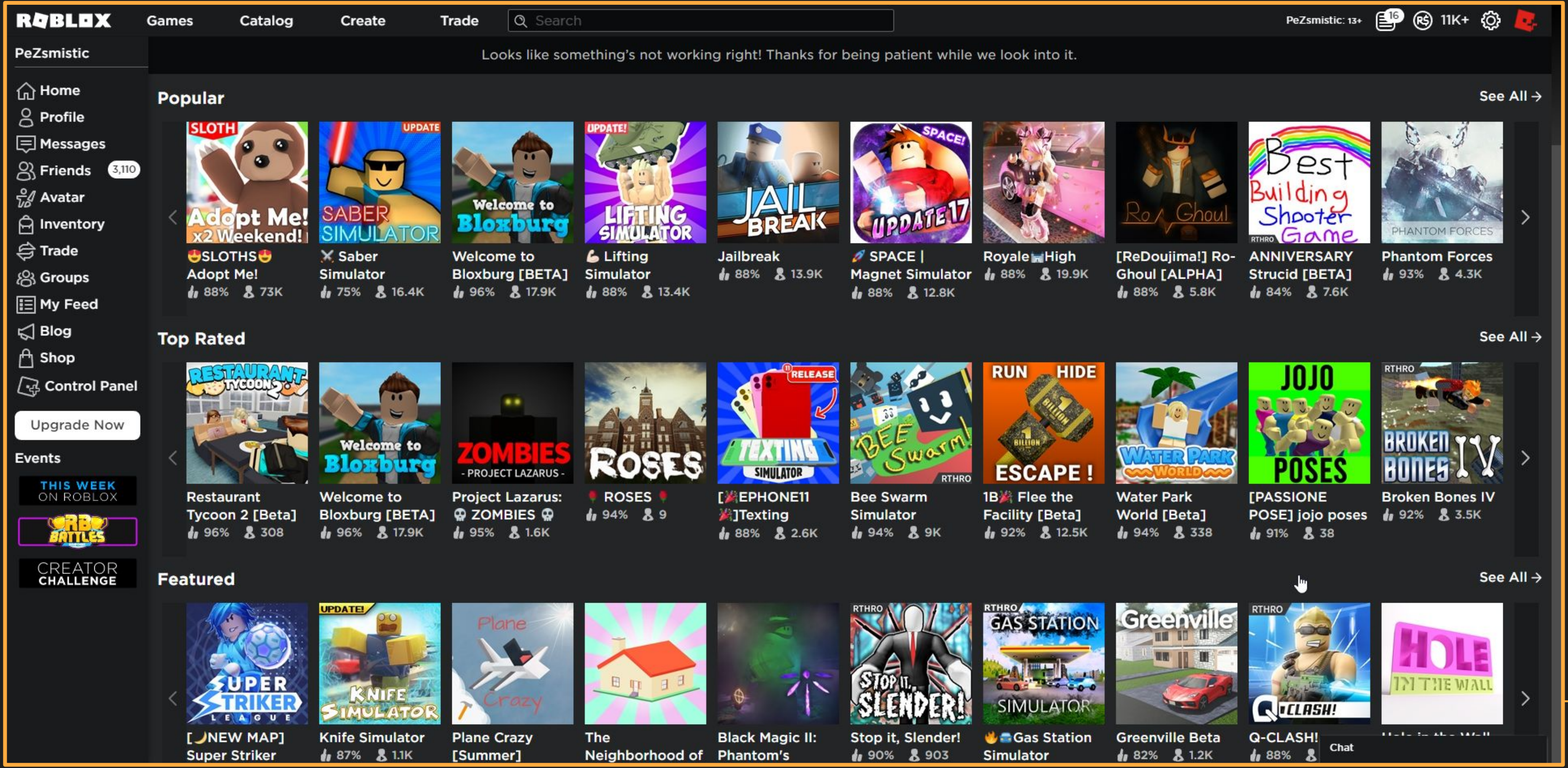
```
┌──(root㉿kali)-[/tmp/arsenal-kit]
└─# [07/4/24 7:22:22] systemctl list-units --type=service | head
  UNIT                               LOAD   ACTIVE SUB     DESCRIPTION
  binfmt-support.service             loaded active exited  Enable support for additional executable binary formats
  colord.service                     loaded active running Manage, Install and Generate Color Profiles
  console-setup.service              loaded active exited  Set console font and keymap
  containerd.service                 loaded active running containerd container runtime
  cron.service                       loaded active running Regular background program processing daemon
  dbus.service                       loaded active running D-Bus System Message Bus
  docker.service                     loaded active running Docker Application Container Engine
  getty@tty1.service                 loaded active running Getty on tty1
  haveged.service                    loaded active running Entropy Daemon based on the HAVEGE algorithm

┌──(root㉿kali)-[/tmp/arsenal-kit]
└─# [07/4/24 7:22:24] service --status-all | head
 [ - ]  apache-htcacheclean
 [ - ]  apache2
 [ - ]  apparmor
 [ - ]  atftpd
 [ + ]  binfmt-support
 [ - ]  bluetooth
 [ - ]  cgroupfs-mount
 [ - ]  console-setup.sh
 [ + ]  cron
 [ - ]  cryptdisks
```

# Business Service

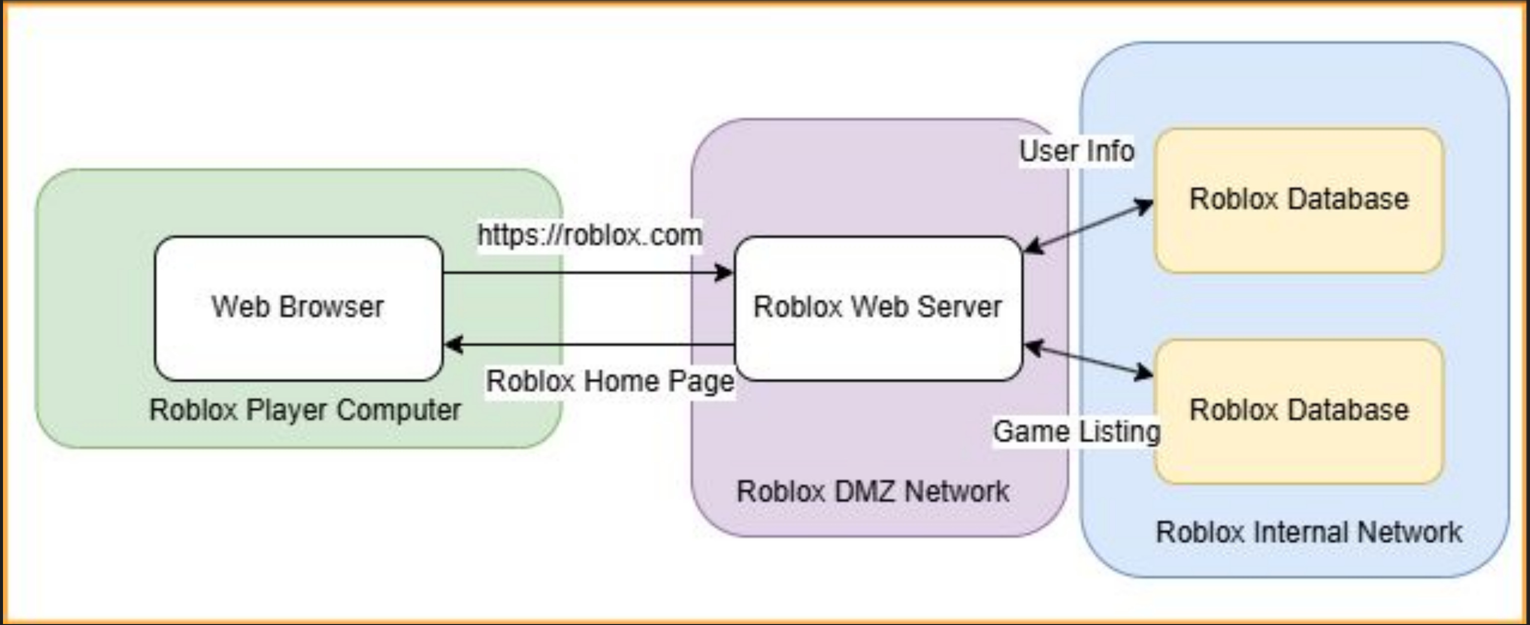


# Example: Business Service



Looks like something's not working right! Thanks for being patient while we look into it.

# Business Service



**This is not representative of Roblox's infrastructure at all, just a hypothetical diagram as an example*

# How can you secure a service?

# Threat Modelling

## Functionality

- What role does this service play in the business?
- How does this service work from a technical standpoint?
  - Ports?
  - Dependent services?

## Identify Attacks

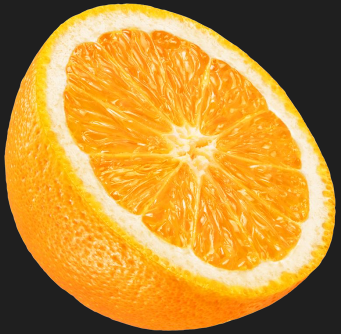
- What would impact the role of this service?
  - DOS?
  - Defacement?
- What impact does exploitation have to us?
  - Command Execution?
  - Information exposure?
- Requirements for the attack?
  - Network access?
  - (Un)authenticated?

## Mitigations

- Is there a configuration or patch that affects the attack's requirements?
- How can I cut the attacker's access?
  - Host level?
  - Network level?
- Can I isolate the impact?

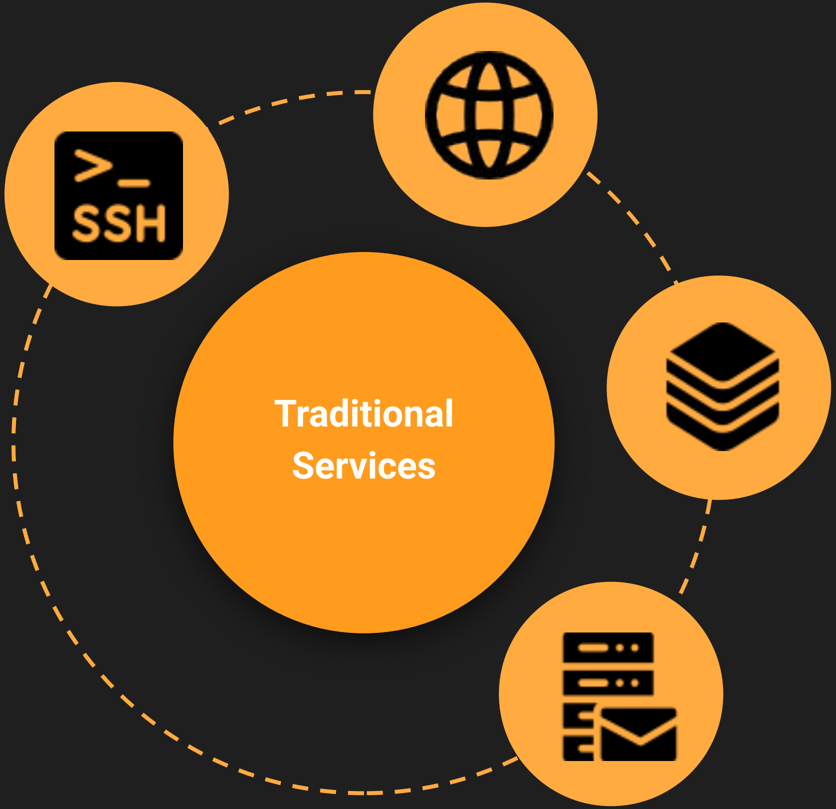
# Is the Juice Worth the Squeeze?

- We want the most impact for the least effort
- We are on a time crunch
- Example:
    - You have a remotely accessible database server with an unknown amount of databases and users
        - Option A: Audit the database, apply principle of least privilege
        - Option B: Restrict ingress to a subnet



# What Services Exist?

- Traditional
    - Remote Access (SSH/RDP)
    - Web Server
    - Databases
    - LDAP
    - Mail Servers
    - File Servers
- "Other stuff"
    - SAAS - Software as a Service
    - PAAS - Platform as a Service
    - Cloud Computing
    - etc.



# In CCDC

- 10-30 Services
- 40% of Scoring

## Relevant Services

- **Web Servers & Applications**
- **File Shares**
- Mail
- **Remote Access**
- **Databases**
- DNS
- Docker

# Lab Goals (For each service)

## What is it?

Functionally, examples

## Management

Installation & Configuration

## Security

Threat Model each service

root/Administrator:bruh

# Remote Access

- SSH, RDP, VNC, WinRM
- Remote Access.. (crazy)
- TCP: 22, 3389, 5900, 5985/6

# Remote Access Lab

- Debian: Install openssh-server and xfreerdp
- Windows: Install Remote Desktop Protocol server

1. SSH into Debian from Windows
2. RDP into Windows from Debian
3. Add another user "user" to both systems
   a. Add this user to the Remote Desktop Users group on Windows
4. Access each system using the user you added
   a. Delete the user. Can you still use them to access the systems?
5. Figure out how to check the status of the service, then check it.

# File Shares

- Share files (crazy x2)
- FTP, SMB*
- TCP: 21, 445

# File Share Lab

- Debian: Install vsftpd
- Windows: Install ftp

1. Configure Guest authentication for both FTP servers
2. Create a file in the FTP root of both servers
3. Access both FTP servers from the other machine
4. Figure out how to check the status of the service, then check it.

# Web Servers & Applications

- Web Servers
  - IIS, Apache2, Nginx
- Applications
  - XAMPP, Flask, etc.
- Other Uses
  - Reverse Proxies, Load Balancers
- TCP: 80, 443

Microsoft
IIS

NGINX

# Web Lab

- Debian: Install apache2
- Windows: XAMPP

1. What is a webroot? Try adding files to it and browse to them
    a. Linux: /var/www/html
    b. Windows: c:\xampp\htdocs
2. Figure out how to check the status of the service, then check it.
3. Add this file (shell.php) to the webroots on both systems
    a. Access both web servers and hit "/shell.php?cmd=whoami"
    b. Does it work? What do you think happened?

# Databases

- Store data (crazy x3)
- MySQL, MariaDB, PostgreSQL, MSSQL, Mongo, Cockroach
  - Yeah there's a lot
  - SQL is typically TCP:3306, except MSSQL

# Database Lab

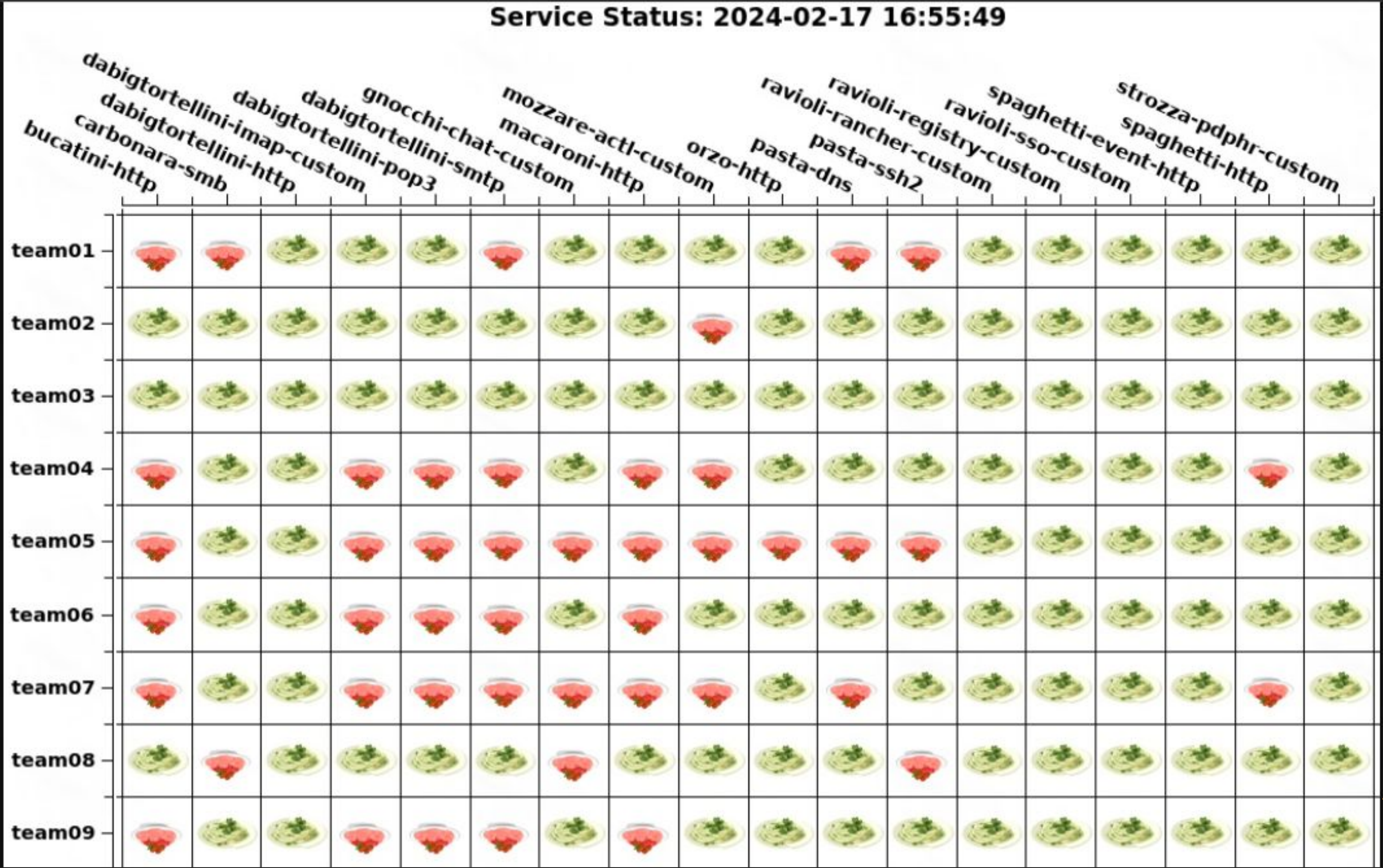
- Debian: Install mariadb-server

1. Database management
    a. Create a user "xampp" with password "xampp" on the database
    b. This user should only be able to log in from 192.168.1.10
2. Add [this file]() (db.php) to the XAMPP webroot and browse to it.
    a. Is it working? Did we forget something?
        i. If it isn't, try fixing the issue!
3. Figure out how to check the status of the service, then check it.

# Application to CCDC

# Operating in CCDC

- "An IT competition, with some focus on security" - someone probably
- We know how to set up & manage a service? What next?
    - Know the threat model for each service
    - Is the juice worth the squeeze?
        - Configure a password policy vs. changing passwords
        - Configure HTTPS vs. changing application admin's password
        - Is it even scored?
            - Block remote access ports
            - Change all database passwords vs. firewalling it
- **INVENTORY**



## Service Status: 2024-02-17 16:55:49

| | bucatini-http | carbonara-smb | dabigtortellini-http | dabigtortellini-imap-custom | dabigtortellini-pop3 | dabigtortellini-smtp | gnocchi-chat-custom | macaroni-http | mozzare-actl-custom | orzo-http | pasta-dns | pasta-ssh2 | ravioli-rancher-custom | ravioli-registry-custom | ravioli-sso-custom | spaghetti-event-http | spaghetti-http | strozza-pdphr-custom |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| team01 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| team02 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| team03 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| team04 | 🟥 | 🟩 | 🟩 | 🟥 | 🟥 | 🟥 | 🟩 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 |
| team05 | 🟥 | 🟩 | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| team06 | 🟥 | 🟩 | 🟩 | 🟥 | 🟥 | 🟥 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| team07 | 🟥 | 🟩 | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 |
| team08 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| team09 | 🟥 | 🟩 | 🟩 | 🟥 | 🟥 | 🟥 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |