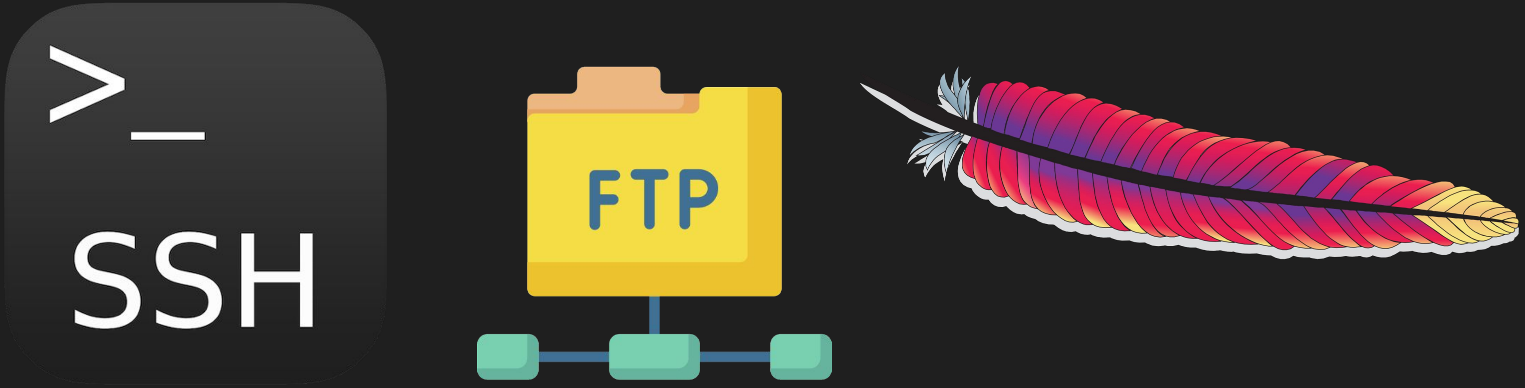
# Common Services

## CCDC Week 6



# whoami

Sara Downing | @ihasbunnyboo

2nd year Computer Science major

CCDC Alternate Member 2024-2025

# Weekly Schedule

| Date | CPTC (10AM-12PM) | CCDC (1PM-3PM) |
|---|---|---|
| ~~Jul 12~~ | ~~Cyber Bootcamp Kickoff!~~ | |
| Jul 19 | ~~Intro to Pen Testing~~ | ~~Business Week~~ |
| Jul 26 | ~~Hacking Web Apps~~ | ~~Introduction to Networking~~ |
| Aug 2 | ~~Hacking Linux~~ | ~~Securing Linux~~ |
| Aug 9 | ~~Hacking Windows~~ | ~~Securing Windows~~ |
| Aug 16 | ~~Consulting~~ | **Common Services** |
| Aug 23-24 | CPTC Tryouts (All day) | |
| Aug 30-Sep 13 | | CCDC Fall |
| Sep 20-21 | | CCDC Tryouts (1-5 PM) |

# Agenda

1

**Services**

Thats it lol

# Today's Objectives

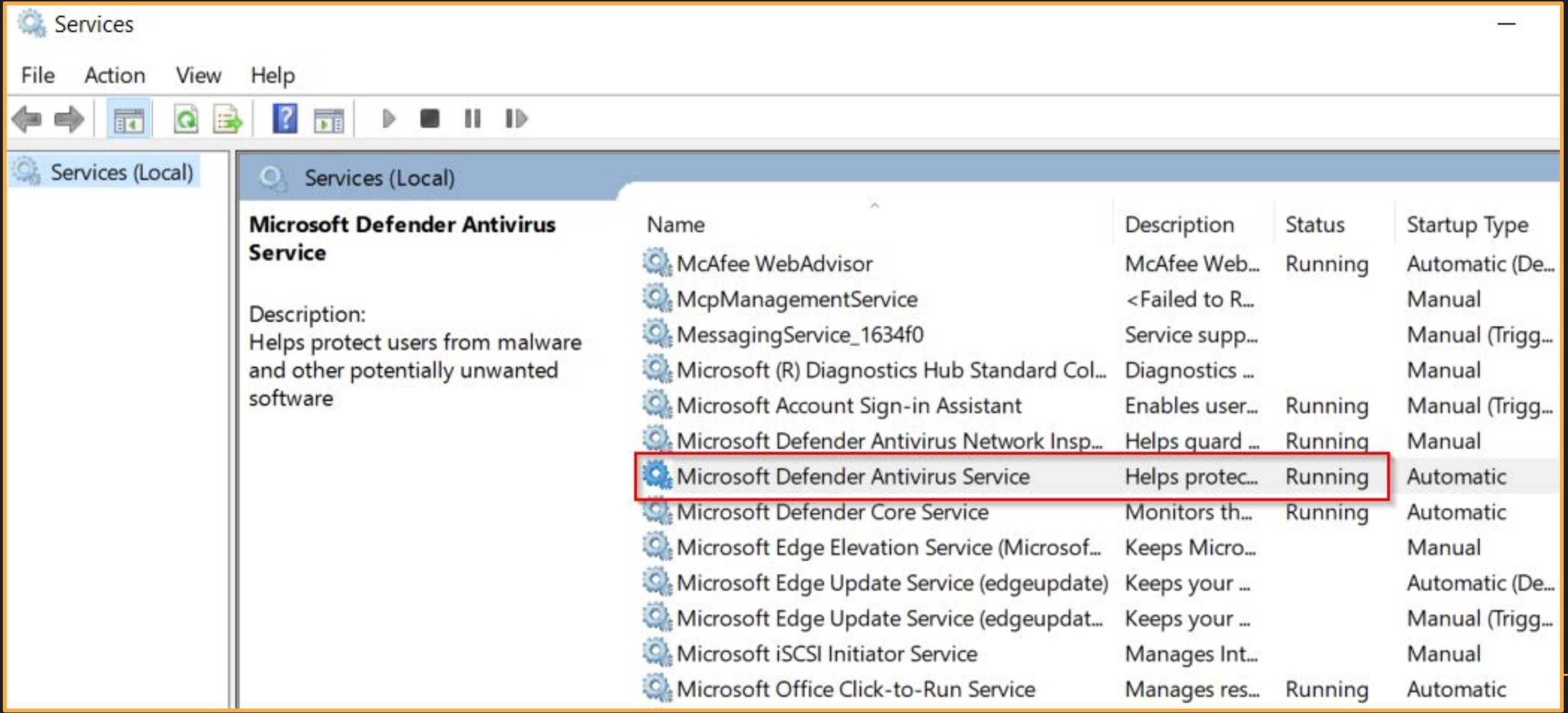
- ❏ Identify what a service is
  - ❏ Identify services present on a system
- ❏ Identify common CCDC services
- ❏ Understand service methodology
  - ❏ Install
  - ❏ Troubleshoot
- ❏ Understand service security
  - ❏ Configurations
  - ❏ Triaging

# 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



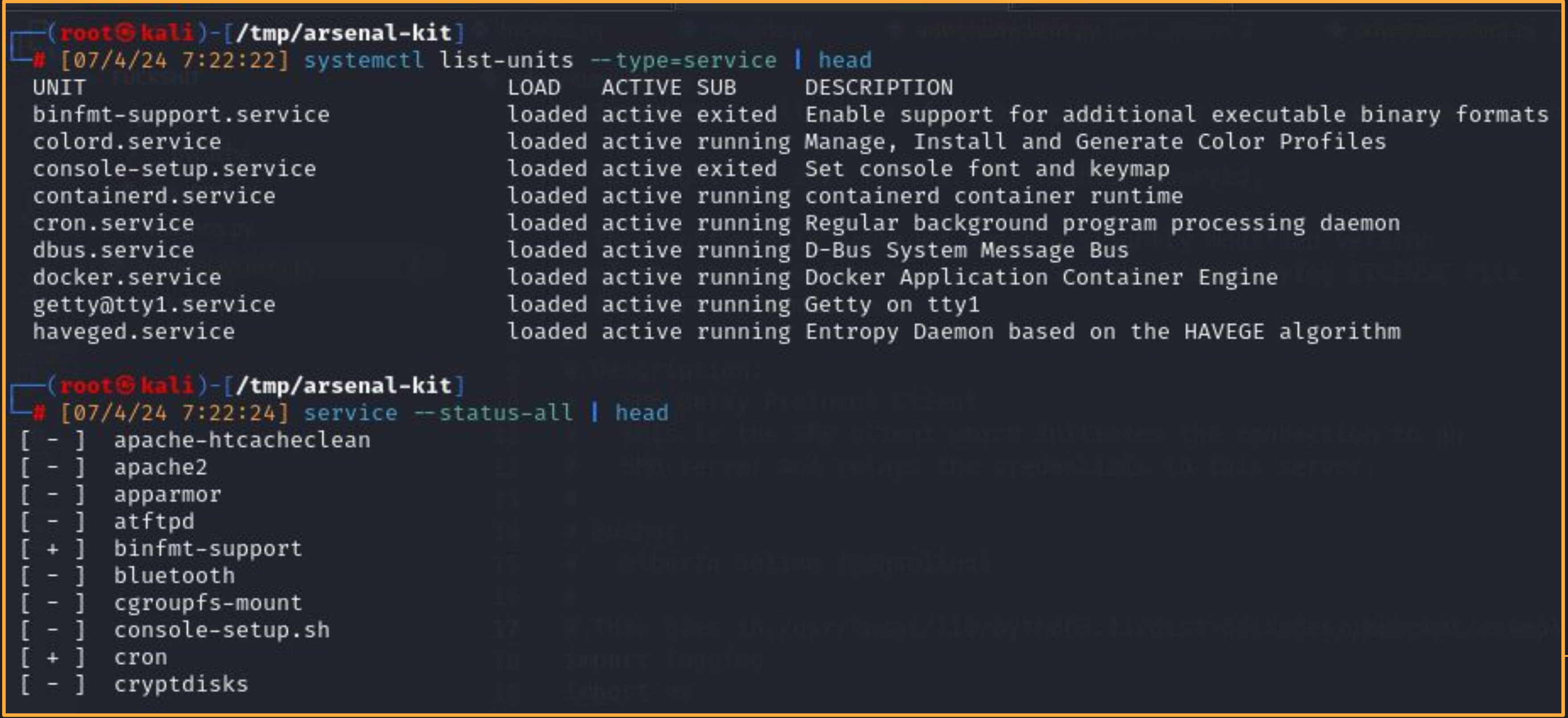
**Microsoft Defender Antivirus Service**

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*

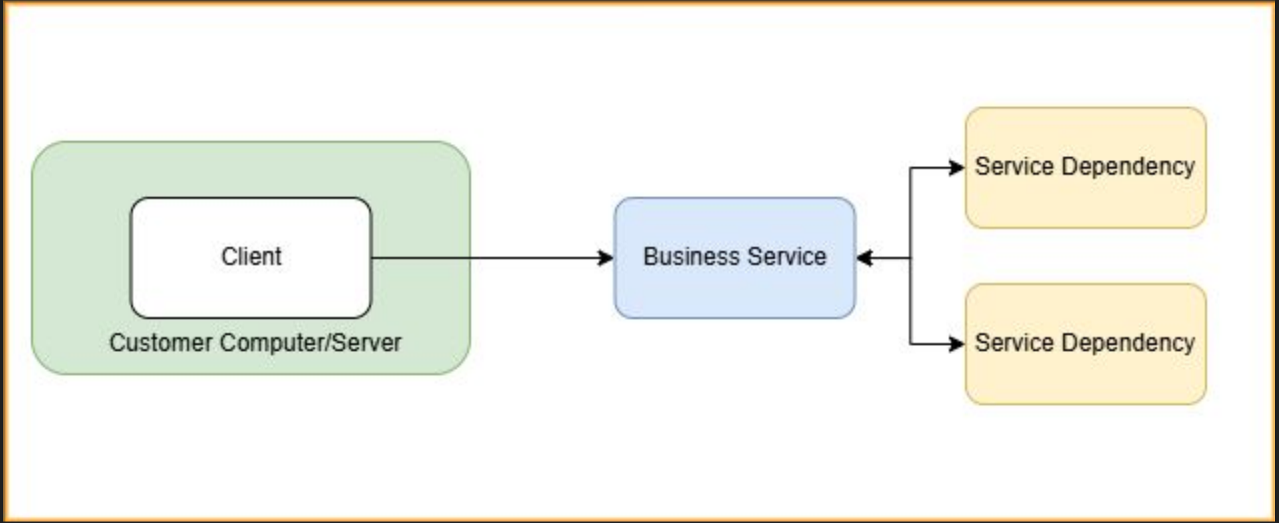
# Example: Host Service



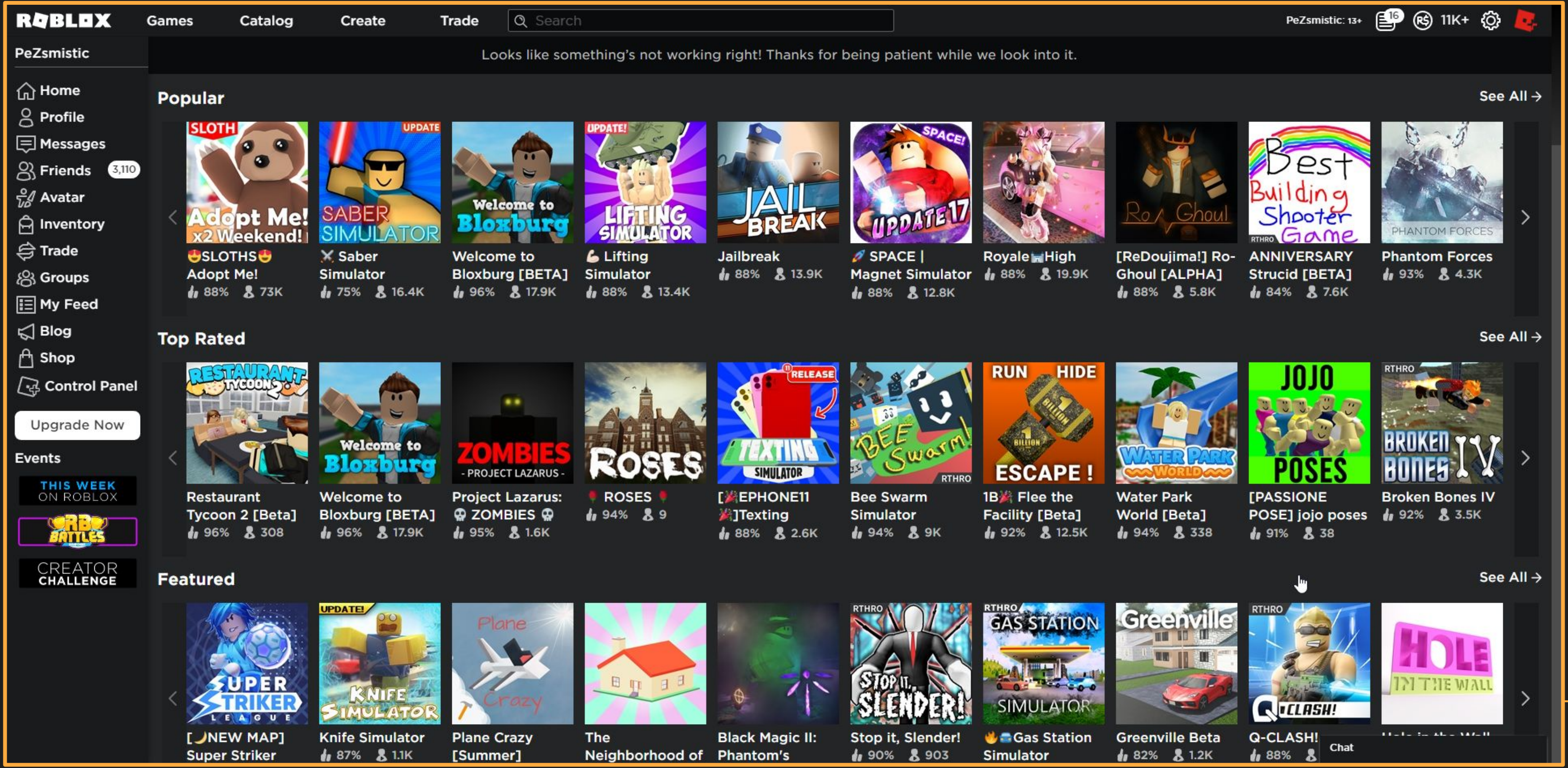
```
┌──(root㉿kali)-[/tmp/arsenal-kit]
└─# [07/4/24 7:22:22] systemctl list-units --type=service | head
  UNIT                                 LOAD   ACTIVE SUB     DESCRIPTION
  binfmt-support.service               loaded active exited  Enable support for additional executable binary formats
  colord.service                       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.

Popular

- SLOTHS Adopt Me! 88% 73K
- Saber Simulator 75% 16.4K
- Welcome to Bloxburg [BETA] 96% 17.9K
- Lifting Simulator 88% 13.4K
- Jailbreak 88% 13.9K
- SPACE | Magnet Simulator 88% 12.8K
- Royale High 88% 19.9K
- [ReDoujima!] Ro-Ghoul [ALPHA] 88% 5.8K
- ANNIVERSARY Strucid [BETA] 84% 7.6K
- Phantom Forces 93% 4.3K

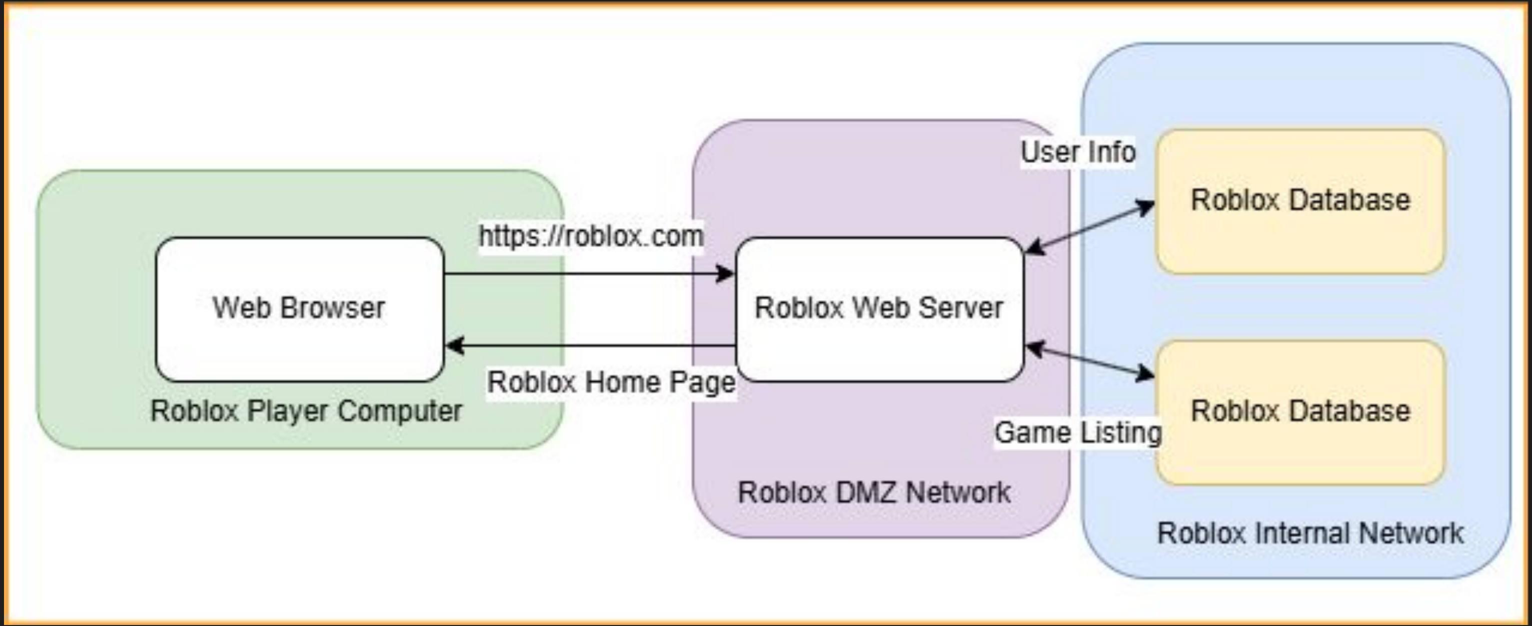
Top Rated

- Restaurant Tycoon 2 [Beta] 96% 308
- Welcome to Bloxburg [BETA] 96% 17.9K
- Project Lazarus: ZOMBIES 95% 1.6K
- ROSES 94% 9
- [EPHONE11 ]Texting 88% 2.6K
- Bee Swarm Simulator 94% 9K
- 1B Flee the Facility [Beta] 92% 12.5K
- Water Park World [Beta] 94% 338
- [PASSIONE POSE] jojo poses 91% 38
- Broken Bones IV 92% 3.5K

Featured

- [NEW MAP] Super Striker
- Knife Simulator 87% 1.1K
- Plane Crazy [Summer]
- The Neighborhood of
- Black Magic II: Phantom's
- Stop it, Slender! 90% 903
- Gas Station Simulator
- Greenville Beta 82% 1.2K
- Q-CLASH! 88%

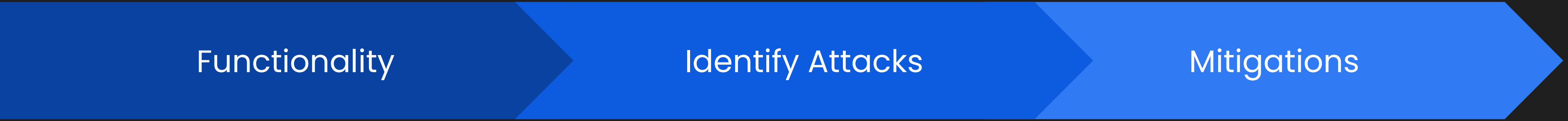
# Business Service



*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

Identify Attacks

Mitigations

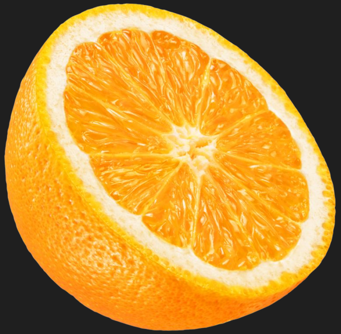
- What role does this service play in the business?
- How does this service work from a technical standpoint?
  - Ports?
  - Dependent services?

- 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?

- 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?

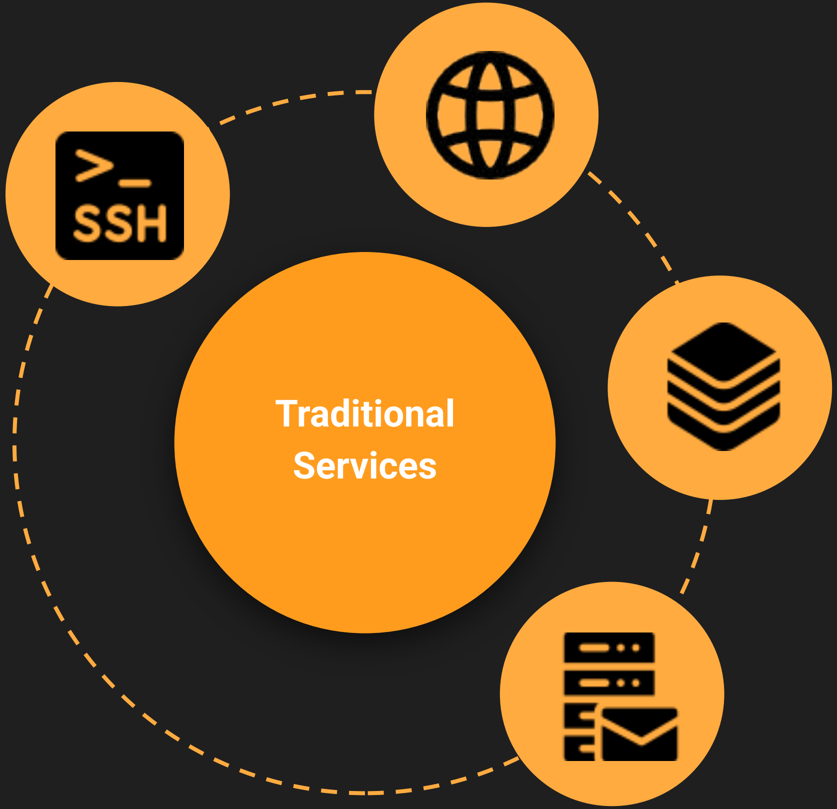
# Is the Juice Worth the Squeeze?

- 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

user/root:bruh
Administrator:CCDC2025!

# Remote Access

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

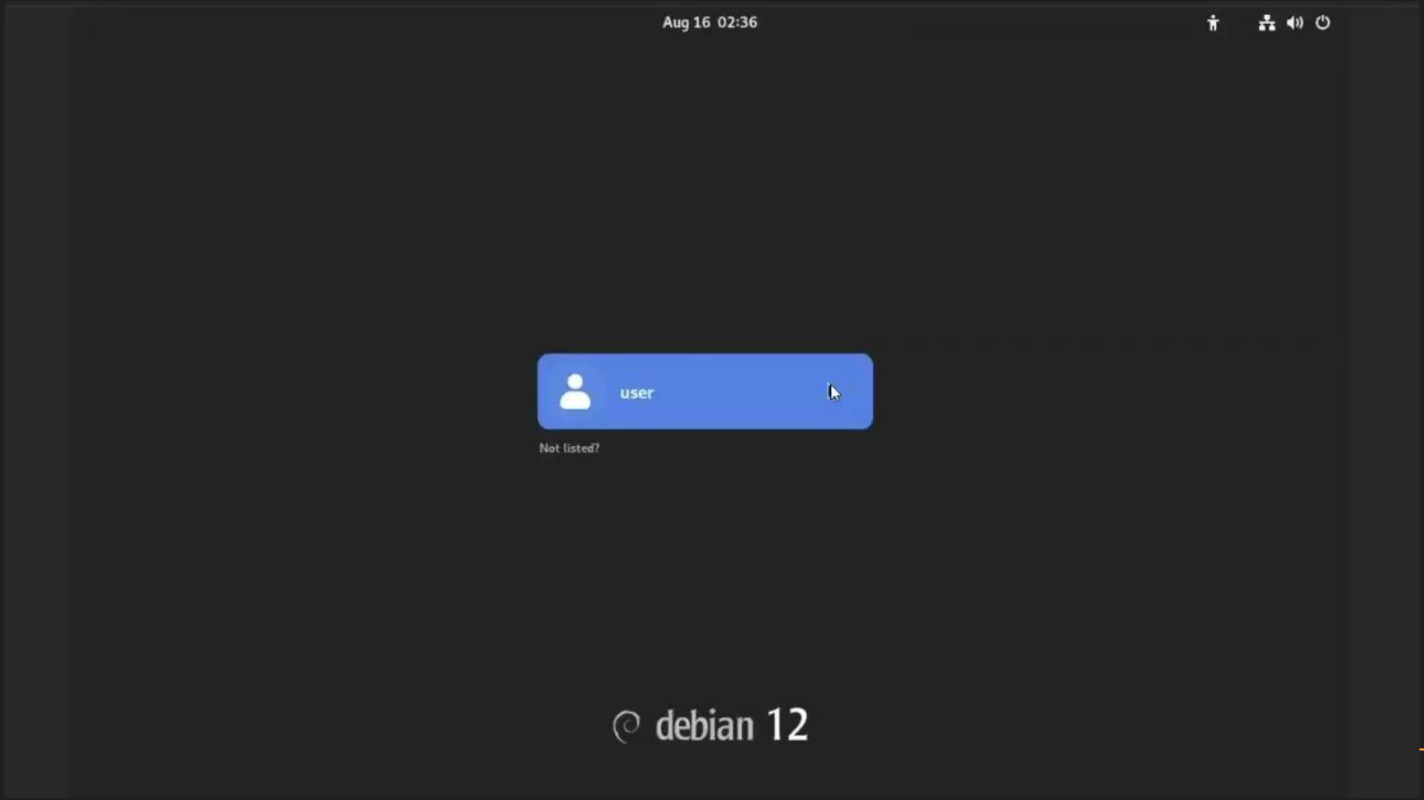
# Remote Access Lab

- 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. Figure out how to check the status of the service, then check it.

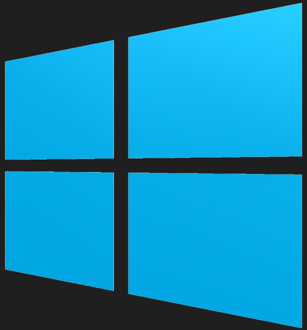
user/root:bruh
Administrator:CCDC2025!

# Remote Access Lab



# 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.

user/root:bruh
Administrator:CCDC2025!

# File Share Lab

```
user@debian12:~$
```

# Web Servers & Applications

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

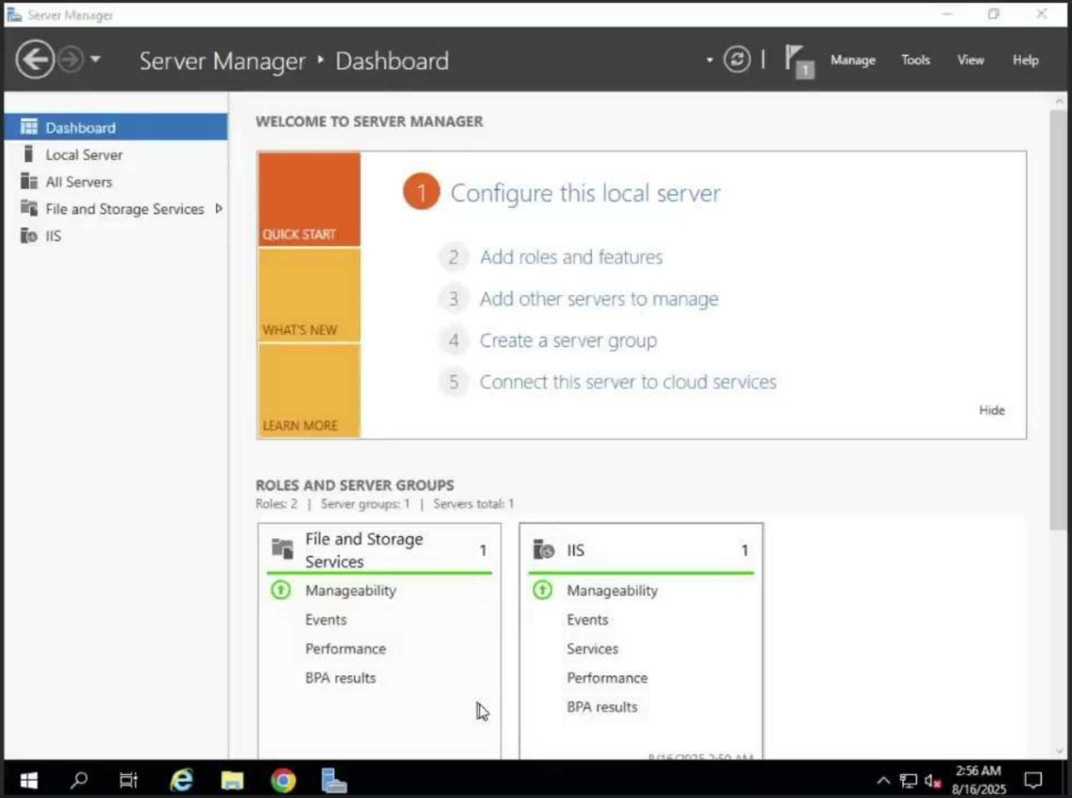
# Web Lab

- 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.

user/root:bruh
Administrator:CCDC2025!

# Web Lab



WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1

File and Storage Services 1
Manageability
Events
Performance
BPA results

IIS 1
Manageability
Events
Services
Performance
BPA results

# Databases

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

# 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
- **<u>INVENTORY</u>**

# No CCDC HW this week

Feel free to continue working on the labs!