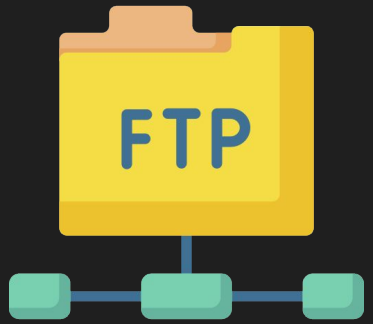
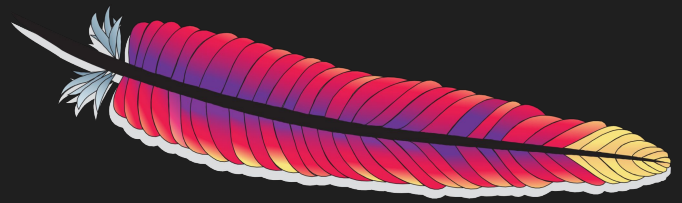
Common Services

CCDC Week 6





whoami

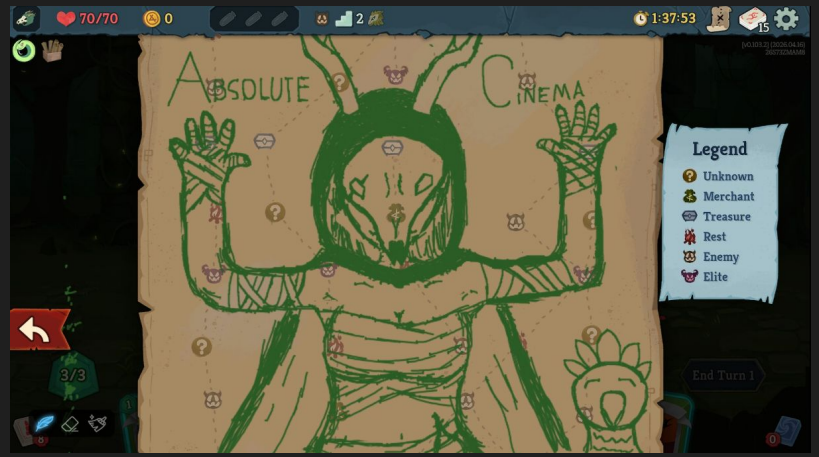
Adam Cheung | @adumb

IST Sysadmin Intern @ Esri

CCDC Co-Captain, Linux Lead 2026-2027
CCDC Linux Database 2025-2026

BS CS, Cyber Minor; MSIS 1st year
Sec+, Network+

slay da spire



whoami

Natalie Tran | @natworking

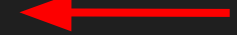
CD&E Intern

CCDC (Co-)Captain 2025-2026
CCDC Networking 2024-2025

4th year CS

geckos :D

Weekly Schedule

Date	CPTC (10AM-12PM)	CCDC (1PM-4PM)
~~Jul 11~~	~~Cyber Bootcamp Kickoff!~~	
~~Jul 18~~	~~Intro to Pen Testing~~	~~Business Week~~
~~Jul 25~~	~~Hacking Web Apps~~	~~Introduction to Networking~~
~~Aug 1~~	~~Hacking Linux~~	~~Securing Linux~~
~~Aug 8~~	~~Hacking Windows~~	~~Securing Windows~~
Aug 15	~~Consulting~~	**Common Services** 
Aug 22-23	CPTC Tryouts (All day)	
Aug 29-Sep 12		CCDC Fall
Sep 19-20		CCDC Tryouts (1-5 PM)

Agenda

1

Services

That's it lol

Today's Objectives

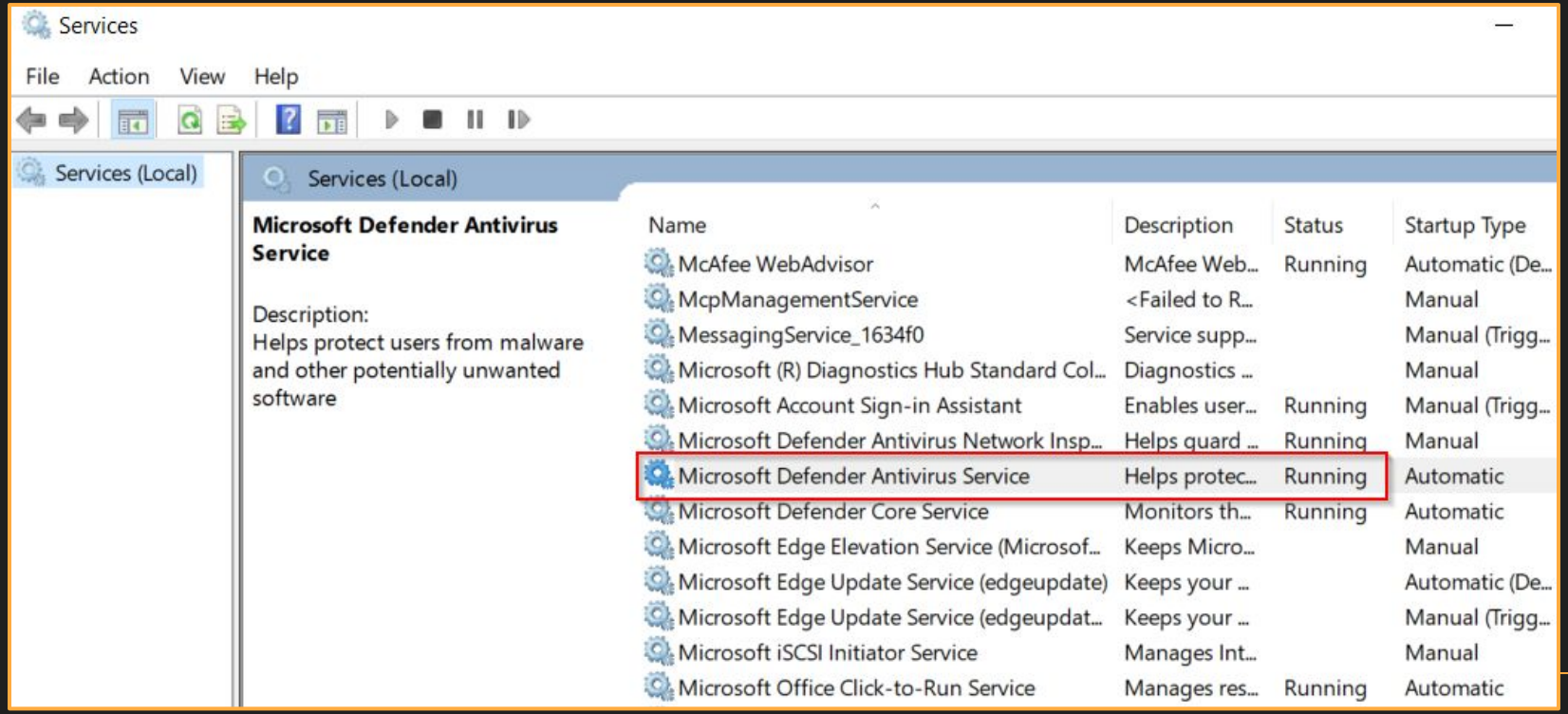
- Define what a service is
  - Identify services present on a system
- Identify common CCDC services
- Understand service methodology
  - Install
  - Troubleshoot
- Understand service security
  - Configurations
  - Triaging

What is a Service?

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

Not 1:1

Example: Host Service

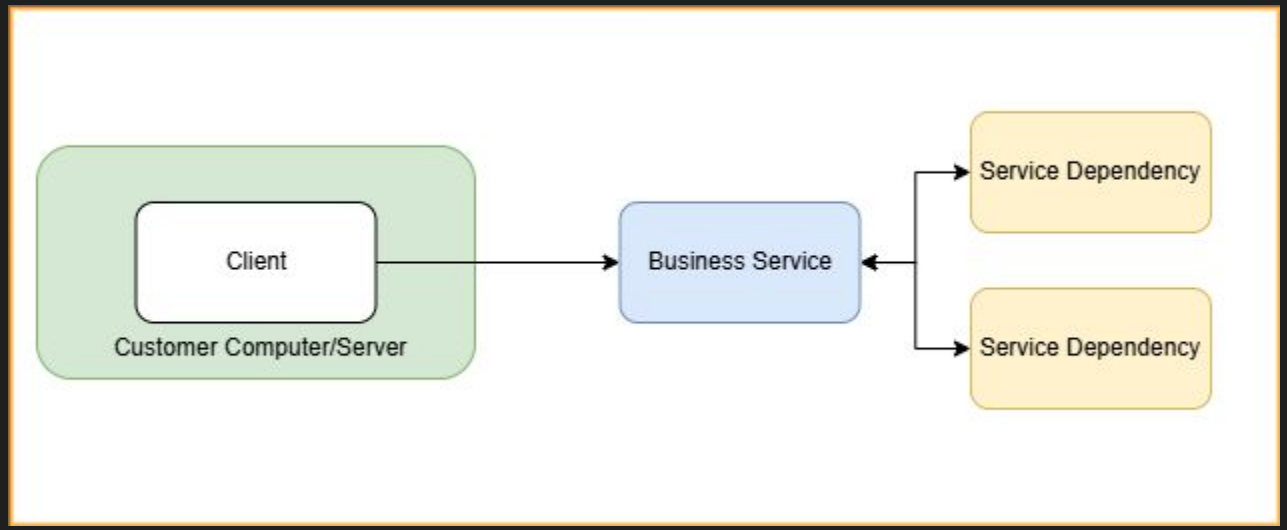


Windows Key + r ⇒ services.msc + enter

Example: Host Service

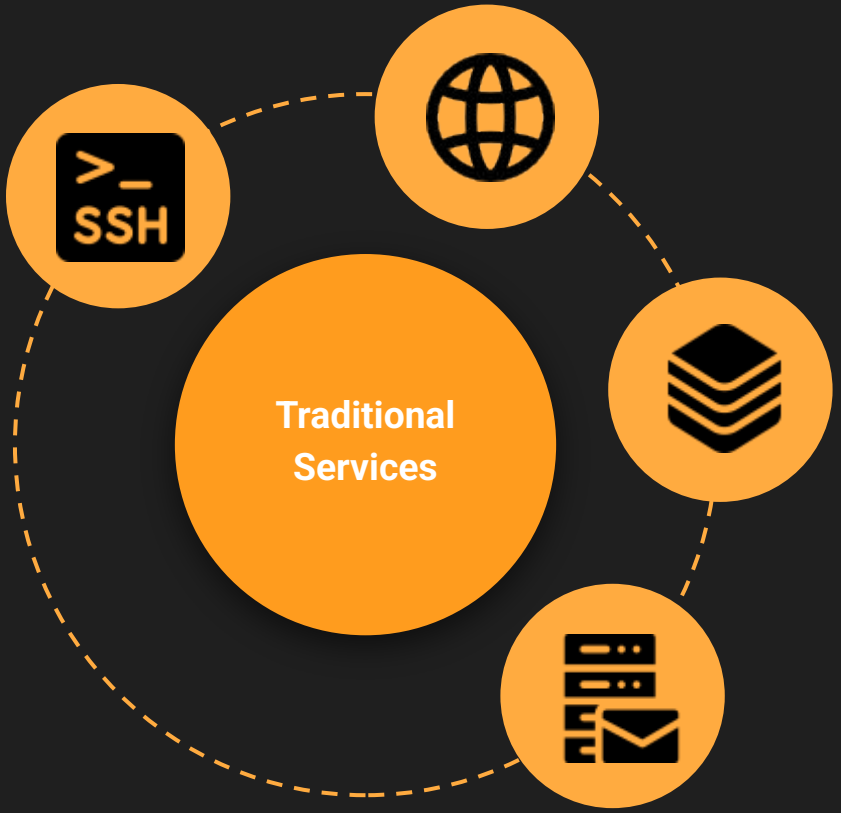
```
┌──(root㉿kali)-[/tmp/arsenal-kit]
└─# [07/4/24 7:22:22] systemctl list-units --type=service | head
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  binfmt-support.service              loaded active exited  Enable support for additional executable binary formats
  colord.service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



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**

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

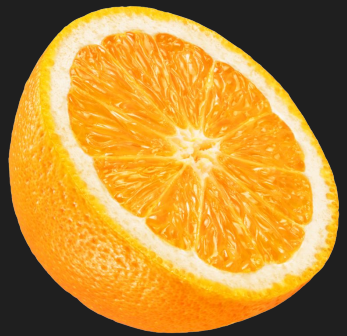
- What would impact the role of this service?
  - DOS?
  - Defacement?
- What impact does exploitation have to us?
  - Command Execution?
  - Information exposure?
- Requirements for the attack?
  - Network access?
  - (Un)authenticated?

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

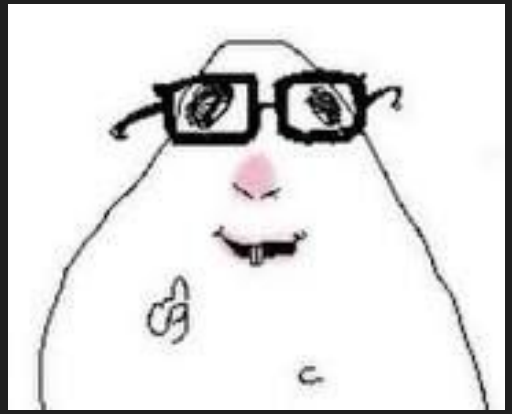


Example 1

- You've found that SSH is currently running on your machine
  - Your teammate says that only a website and file share are scored
- What should you do about SSH? (multiple may be correct)
  a. Drop SSH traffic with iptables
  b. Turn off SSH with systemctl stop + disable
  c. Nothing, you need SSH to remote in
  d. ? Check if file share is SFTP first!

Example 2

- Comp just started and you're currently completing your first 15
  - Your captain points out that your FTP service just went down
- What should you do about the FTP? (multiple may be correct)
  a. Drop everything to figure this out
  b. Finish inventory for the box and then get to it
  c. Run basic diagnostics of the FTP service
  d. ?



Basic Troubleshooting Workflow

1 **Service status**

systemctl / services.msc

2 **Network**

iptables / WDF

3 **Logs**

wtf happened

4 **Authentication**

Changed pw? PCRs?

Service Deployment

Lab time!

Lab Goals (For each service)

Management

Functionally, examples

Security

Installation & Configuration

Threat Model

What is it?

user/root:bruh
Administrator:Password123

Remote Access

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

Remote Access Lab

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

1. SSH into Debian from Windows
2. RDP into Windows from Debian
3. Check the status of each service

user/root:bruh
Administrator:Password123

Remote Access Demo

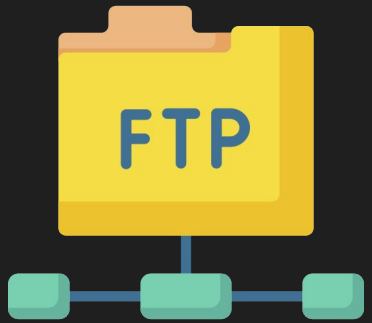
Remote Access Security

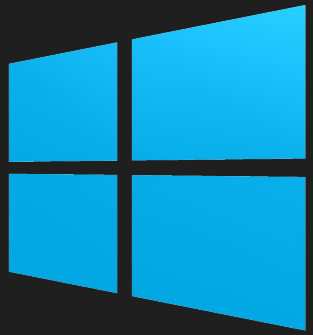
- Questions to ask:
  - Is SSH/RDP needed?
    - Stop + Disable if not needed
    - Make proper firewall rules
  - Who should be able to use remote access?
    - User + group management

user/root:bruh
Administrator:Password123

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. Check the status of each service

user/root:bruh
Administrator:Password123

File Share Demo

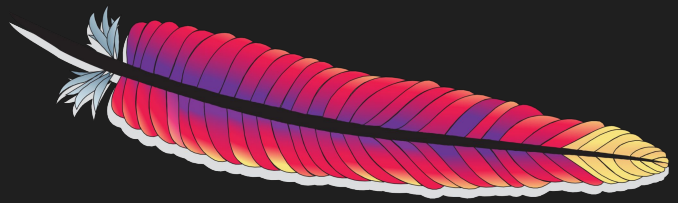
File Share Security

- Questions to ask:
  - What is in the file share?
    - PII = bad
  - Who should be able to access the file share?
    - User + group management
    - Firewall

user/root:bruh
Administrator:Password123

Web Servers & Applications

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



Microsoft
IIS

Web Lab

- Debian: Install nginx
- Windows: XAMPP (already installed)

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:Password123

Web Demo

Web Security

- Questions to ask:
  - Does the site have file upload?
    - File upload almost always = web shell
  - Does the site require login?
    - SQL Injection
    - User + group management (LDAP?)
  - What port does the site run on?
    - Firewall

user/root:bruh
Administrator:Password123

Databases

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

Databases Lab

- Since we've already installed and added data to MariaDB on Linux... let's try it on Windows!

1. Install MySQL Server
    - Be sure to install Workbench if you want to get the GUI experience!

2. Create a database and a table
    - At least 3 rows and 3 columns of data
    - You can put anything you want :D

user/root:bruh
Administrator:Password123

Database Demo

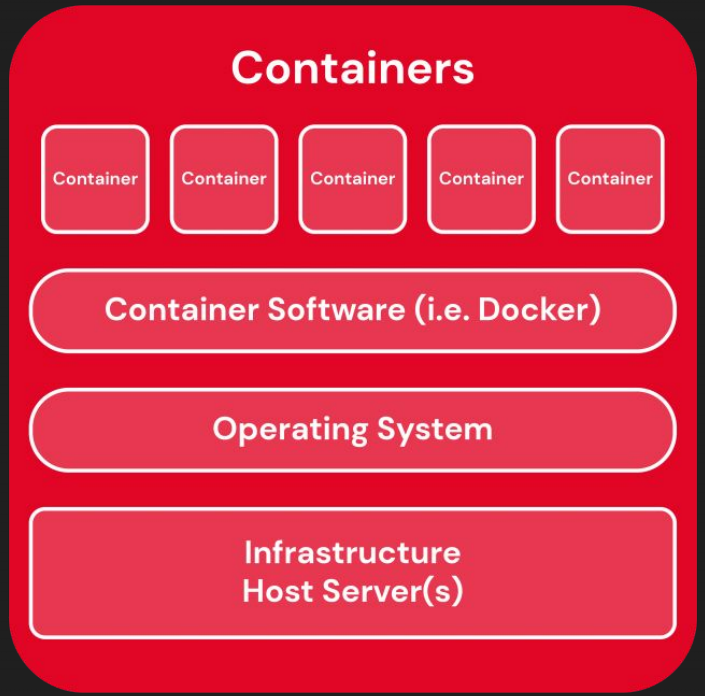
Database Security

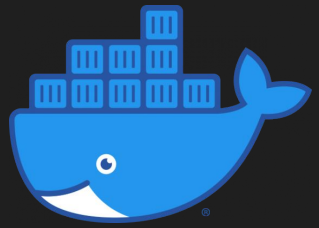
- Questions to ask:
  - What should be able to access the database?
    - Web (Wordpress, App, etc.) accounts
  - What privileges should each database account have?
    - Hosts, privileges, etc.
- Backups
  - mysqldump

user/root:bruh
Administrator:Password123

Containers

- Packaged applications built for portability and ease of use
- Docker: deploy and create containers
- Kubernetes: deploy and orchestrate containers

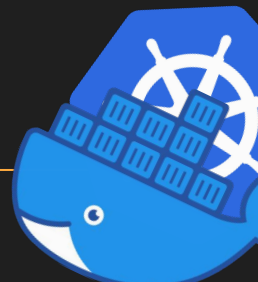




Containers Lab

- Deploy a Portainer docker container using docker compose

1. On Debian, install Docker
2. Create a docker compose file
    a. Do not configure the container in the command line!
3. Bring the container up
4. Check for the exposed Portainer website



Containers Demo

Container Security

- Questions to ask:
  - What ports are exposed on the container(s)?
    - Are ports mapped 1:1?
  - What directories are mounted?
    - Config files, database files, etc.
  - Where is the docker compose file?
    - docker-compose.yml
  - Are the containers privileged?
    - Inspect containers

user/root:bruh
Administrator:Password123

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**

No CCDC HW this week

Feel free to continue working on the labs!

Please delete your pods by August 21st

Thanks!

Any questions? Please ask questions; we are available to help :D