Common Services + Q&A

CCDC Fall Bootcamp Week 3

Sign-in:
jessh.zip/2026ccdcfallweek3

whoami

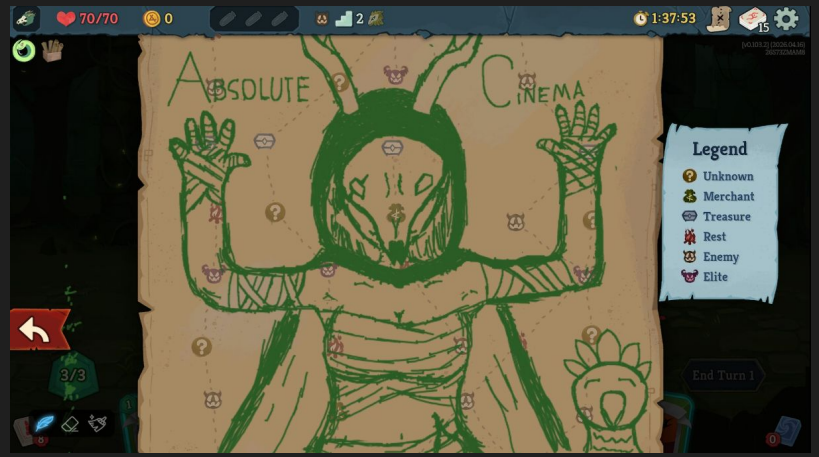
Adam Cheung | @adumb

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 Captain 2025-2026
CCDC Networking 2024-2025

4th year CS

geckos :D

Weekly Schedule

Date	CCDC (1PM-4PM)
Aug 29	Intro, Business, and Networking
Sep 5	Securing Linux and Windows
Sep 12	Common services + Q&A
Sep 19-20	CCDC Tryouts (1-5 PM)

Agenda

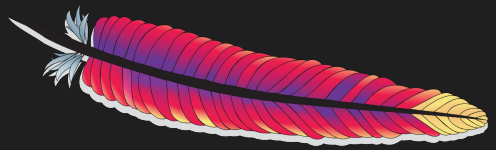
1 **Services**

Most of troubleshooting tbh

2 **Tryouts Info**

Date + Do's & Don'ts

Common Services



Today's Objectives

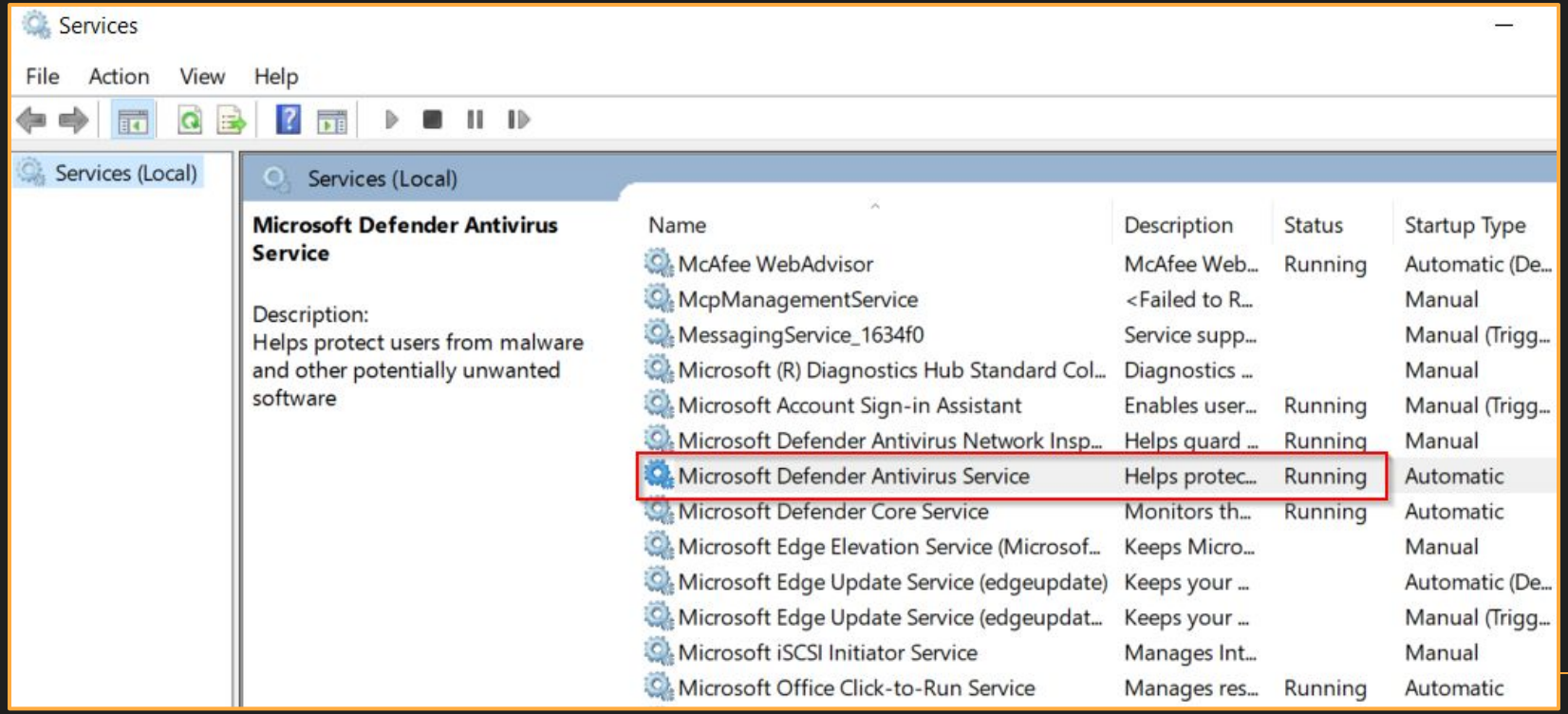
- Define what a service is
- Identify common CCDC services
- Understand service methodology
  - Install
  - Troubleshoot
- Understand service security
  - Configurations
  - Triaging

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

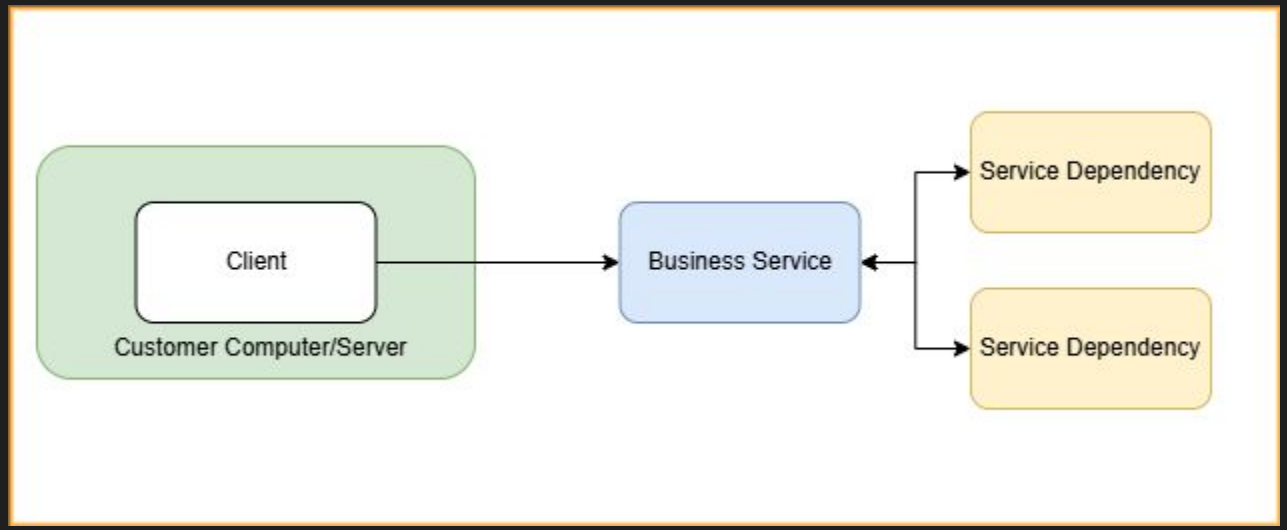


Windows Key + r ⇒ services.msc + enter

Example: Host Service

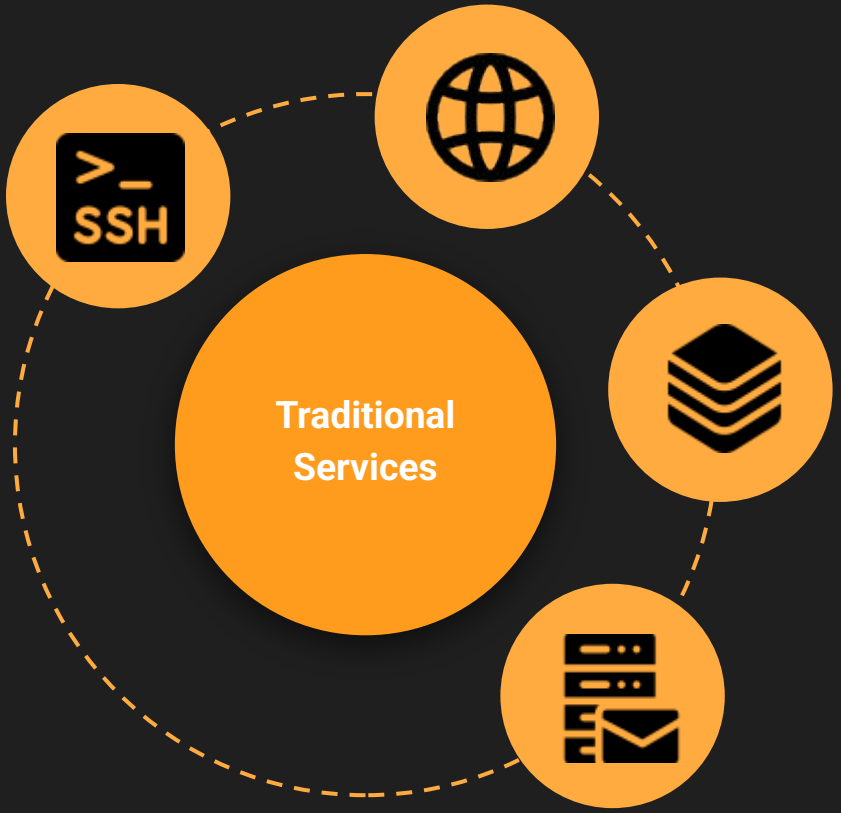
```
┌──(root㉿kali)-[/tmp/arsenal-kit]
└─# [07/4/24 7:22:22] systemctl list-units --type=service | head
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  binfmt-support.service              loaded active exited  Enable support for additional executable binary formats
  colord.service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

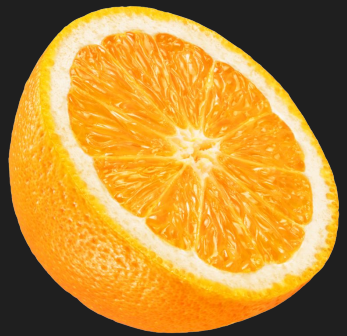
- What would impact the role of this service?
  - DOS?
  - Defacement?
- What impact does exploitation have to us?
  - Command Execution?
  - Information exposure?
- Requirements for the attack?
  - Network access?
  - (Un)authenticated?

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

- Comp just started and you've found that the services scored on your VM are a website and FTP file share.
- What is the first thing you should do?
  a. Set up firewall rules
  b. Identify open ports
  c. Look for the config files of both services
  d. ?

Services may be using non-default ports!

Example 2

- The Threat Hunter just informed you that a strange IP just established an SSH connection to your VM. However, SSH (port 22) is a scored service for your machine.
- What should you do? (multiple may be correct)
  a. Restart the SSH service
  b. Add a firewall rule to block SSH for now
  c. Check SSH and auth logs
  d. Kill all established SSH connections
  e. ? Rotate passwords

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

Management

Functionally, examples

Security

Installation & Configuration

Threat Model

What is it?

user/root:bruh
Administrator:CCDC2025!

Lab Instructions

jessh.zip/2026ccdcfalllab

- We will group you up randomly so you can work with others
- Everyone should complete the lab on your own pod, but you can discuss methodology and implementation strategies
- We'll be walking around in case anyone has questions!

user/root:bruh
Administrator:CCDC2025!

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**

Tryouts Info!

Sep 19th - Sep 20th

(choose one in the form)

1 PM - 5 PM

Location: online

Sign-in:
jessh.zip/2026ccdcfallweek3

A briefing packet will be sent out the Friday before tryouts

Environment

- 2 Windows
- 2 Linux
- Router (not in scope, will not be touched)
- 1-3 services per machine

What's Gonna Happen?

- Pre-brief
- Creds for the machines will drop
- Access the VMs!
- NO GRACE PERIOD
  - Red team will start when you start
- Defend your boxes (ofc)
- Complete injects
  - Partially completed injects are better than no inject submissions
- Debrief
- No later than one week later: CCDC Results are out!
  - We're gonna try to get the results out as soon as we can o7

Yes :D

- Use tools (open source/free trial)
  - Free trials must be available for everyone (not just business accounts)
- Scripts
- Ask for box reverts
- AI can be used for troubleshooting/researching
  - Don't rely on it tho

No :(

- Cheating of any kind/dishonest behavior
- AI-written injects
- Paid tools
- Sabotaging other competitors
- Sabotaging infrastructure
- Accessing the environment before the start of competition
  - Signing into VMs
  - WE HAVE LOGS

Thanks!

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