CCDC Championship Preparation Guide

5-Day Intensive Training Manual

Document Version: 1.0

Competition Date: Friday - Sunday

Preparation Window: 5 Days

Website: https://ccdc.x1000.ai

Organization: LIGHT HOPE LLC · Boston, MA

TABLE OF CONTENTS

EXECUTIVE SUMMARY

What is CCDC?

The Collegiate Cyber Defense Competition (CCDC) is the largest collegiate cyber defense competition in the United States. Unlike CTF competitions that focus on offensive skills, CCDC tests **enterprise defense operations** under real-world pressure.

The Core Truth

> *"**"CCDC is not about who hacks best—it is about who keeps the business running under fire."**"*

What You'll Face

- **8-hour competition** defending a live corporate network
- **Professional Red Team** attacking your infrastructure in real-time
- **Business Injects** requiring policy documents, reports, and communications
- **Scoring Engine** checking service availability every few minutes

Scoring Model

```
TOTAL SCORE = Service Uptime (~50%) + Inject Completion (~50%) - Red Team Penalties
```

Component	Weight	Description
Service Uptime	~50%	Keep web, email, DNS, database running
Business Injects	~50%	Complete CEO requests, write policies, incident reports
Red Team Penalties	Negative	Deducted for each successful compromise
IR Reports	Bonus	Quality reports can reduce penalties up to 50%

THE EIGHT IRON RULES

These rules have been distilled from championship-winning teams. Memorize them. Live them.

Rule 1: Service Priority Is Absolute

*"**Scored services are sacred. Never take actions that break what's being tested.**"*

Why It Matters

- Service uptime is ~50% of your score
- Every minute of downtime costs points that CANNOT be recovered
- Red Team penalties can be reduced through IR reports; service downtime cannot

Implementation

- ■ Know ALL scored services before competition starts
- ■ Before ANY change, ask: "Will this affect scored services?"
- ■ Check service status every 5 minutes
- ■ Have rollback plan before making changes
- ■ Assign primary AND backup owner for each service

Quick Commands

```
# Windows - Check services
Get-Service | Where-Object {$_.Status -eq "Running"}

# Linux - Check services
systemctl list-units --type=service --state=running
```

Rule 2: No Lone Wolf Operations

*"**All changes must be announced before execution and confirmed after.**"*

Why It Matters

- Prevents stepping on teammates' work
- Creates accountability trail for White Team
- Speeds up incident investigation
- Required for professional documentation

Implementation

- ■ Announce: "I am about to [change] on [system]"
- ■ Wait for Captain acknowledgment on major changes
- ■ Make the change
- ■ Verify success
- ■ Announce: "[Change] complete, verified working"
- ■ Log in Change Log

Communication Template

```
[TIME] [NAME]: Planning to [ACTION] on [SYSTEM]
Reason: [WHY]
Impact: [EXPECTED EFFECT]
Rollback: [HOW TO UNDO]
```

Rule 3: Identity Over Surface

*"**Credential hygiene supersedes superficial hardening. Change defaults first.**"*

Why It Matters

- Red Team tries default credentials in FIRST 5 MINUTES
- One compromised credential = full network access
- Credential attacks are #1 initial access method

First 15 Minutes Priority

1. [ ] Change Administrator/root passwords on ALL systems
2. [ ] Change Domain Admin password
3. [ ] Disable Guest accounts
4. [ ] Document ALL credential changes
5. [ ] Change service account passwords (carefully!)

Password Standards

- Minimum 12 characters
- Different password for each system
- Document in secure credential log
- Share only with those who need it

Rule 4: Logs Are Not Optional

*"**If it's not logged, you cannot prove it happened—or didn't.**"*

Why It Matters

- Incident reports require evidence
- Can reduce Red Team penalties by up to 50% with good documentation
- Enables proactive threat detection

Enable Immediately

```
# Windows - Enable PowerShell logging
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name "EnableScr

# Windows - Audit policy
auditpol /set /category:"Account Logon" /success:enable /failure:enable
auditpol /set /category:"Account Management" /success:enable /failure:enable

# Linux - Verify logging
systemctl status rsyslog
tail -f /var/log/auth.log
```

Rule 5: Every Anomaly Gets a Ticket

> *"**Suspicious? Write it down. Incidents emerge from ignored warnings.**"*

Why It Matters

- Small anomalies often precede major compromises
- Documentation helps identify patterns
- Creates evidence trail for incident reports

What Counts as Anomaly

- ■ Failed login attempts (any number)
- ■ Unknown processes running
- ■ Unexpected network connections
- ■ Files modified unexpectedly
- ■ New user accounts
- ■ Unusual scheduled tasks

Anomaly Log Format

```
TIME: [HH:MM]
SYSTEM: [hostname/IP]
OBSERVED: [what you saw]
SEVERITY: [LOW/MEDIUM/HIGH/CRITICAL]
ACTION: [what you did]
STATUS: [OPEN/INVESTIGATING/RESOLVED]
```

Rule 6: Contain First, Diagnose Later

> *"**Stop the bleeding. Elegant fixes lose points; quick containment wins.**"*

Why It Matters

- Every second of active compromise costs points
- Full forensics can wait; stopping damage cannot
- Quick containment reduces Red Team penalties

Containment Actions (in order)

1. Kill malicious processes
2. Disable compromised accounts
3. Block attacker IPs at firewall
4. Isolate system if necessary
5. THEN investigate

Quick Containment Commands

```
# Windows - Kill process
taskkill /PID [PID] /F

# Windows - Disable account
net user [username] /active:no

# Windows - Block IP
netsh advfirewall firewall add rule name="Block Attacker" dir=in action=block remoteip=[IP]

# Linux - Kill process
kill -9 [PID]

# Linux - Lock account
usermod -L [username]

# Linux - Block IP
iptables -A INPUT -s [IP] -j DROP
```

Rule 7: Scorched Earth Is Defeat

*"**Service destruction to deny Red Team is a failed strategy. Defend, don't delete.**"*

Why It Matters

- Destroying services = losing points
- Red Team still gets points for forcing you to destroy
- Rebuilding takes time away from defense
- White Team penalizes destructive tactics

What NOT To Do

- ■ Delete critical system files
- ■ Format drives as "defense"
- ■ Disable all network access
- ■ Uninstall services to "protect" them

What TO Do

- ■ Block specific attacker IPs (not all IPs)
- ■ Disable compromised accounts (not all accounts)
- ■ Restart services (not uninstall them)
- ■ Restore from backup (not delete data)

Rule 8: Injects Are Not Optional

*"**Business tasks carry weight. Ignoring injects for "security" still loses.**"*

Why It Matters

- Injects are ~50% of your score
- Technical excellence means nothing without inject completion
- White Team specifically watches inject response quality

Inject Process

1. Receive inject → Log immediately
2. Assign to appropriate team member
3. Note deadline prominently
4. Begin work immediately
5. Quality check before submission
6. Submit with time buffer
7. Confirm submission received

Quality Standards

■ Professional formatting
■ Complete answer to all requirements
■ Proofread for errors
■ Evidence/documentation attached
■ Submitted before deadline

5-DAY BATTLE PLAN

Overview

Day	Focus	Outcome
1	Foundation & Roles	Team structure finalized, templates ready
2	Technical Hardening	All members can harden their systems
3	Detection & Response	Team can detect and respond to attacks
4	Full Simulation	4-hour mock competition completed
5	Final Prep & Rest	Materials ready, team rested

DAY 1: FOUNDATION & ROLES

Morning (3 hours): Team Structure

Define 8-Person Team Structure

Role	Primary Focus	Backup Responsibility
Captain	Coordination, decisions, external comms	Overall oversight
Windows/AD Lead	AD, GPO, authentication	Windows servers
Linux Lead	Services, web, databases	Linux systems
Network Lead	Firewall, monitoring, IDS	Network devices
IR Lead	Incident response, forensics	Evidence collection
Inject Lead	Business tasks, documentation	Report writing
Support 1	Windows/Linux backup	Flexible support

Support 2	Network/IR backup	Flexible support

Communication Protocol

1. Establish communication channel (Slack/Discord/in-person)
2. Define status update frequency (every 15-30 minutes)
3. Establish escalation procedure
4. Practice "No Lone Wolf" announcements

Afternoon (3 hours): Templates & Tools

Print and Prepare

- ■ Captain Status Board (print 3 copies)
- ■ Asset Inventory Sheet (print 5 copies)
- ■ Change Log (print 10 copies)
- ■ Incident Report Template (print 10 copies)
- ■ First 15 Minutes Checklist (print 8 copies)
- ■ Command Reference (print 8 copies, laminate if possible)

Test Equipment

- ■ All laptops working
- ■ Required software installed
- ■ Documentation accessible offline
- ■ Backup power/cables available

Evening (2 hours): Role Assignments

Each Member Must Know

1. Their primary system/service responsibilities
2. Their backup responsibilities
3. Who to escalate to
4. Location of all templates

Homework

- • Review Command Reference for your role
- • Read Iron Rules implementation checklist

- Get good sleep

DAY 2: TECHNICAL HARDENING

Morning (3 hours): Windows Hardening

All Windows Team Members Practice

First 15 Minutes Tasks

```
# Change local admin password
net user Administrator [NewPassword]

# Disable Guest account
net user Guest /active:no

# List all users
net user

# List admin group members
net localgroup Administrators

# Check running services
Get-Service | Where-Object {$_.Status -eq "Running"}
```

Active Directory Tasks

```
# List Domain Admins
Get-ADGroupMember "Domain Admins"

# List all AD users
Get-ADUser -Filter *

# Reset AD password
Set-ADAccountPassword -Identity [user] -Reset -NewPassword (ConvertTo-SecureString "[pass]" -AsPlainText -Force)

# Disable AD account
Disable-ADAccount -Identity [username]
```

Enable Logging

```
# Enable audit policy
auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
auditpol /set /category:"Account Management" /success:enable /failure:enable

# Check Security log
Get-EventLog -LogName Security -Newest 50
```

Afternoon (3 hours): Linux Hardening

All Linux Team Members Practice

First 15 Minutes Tasks

```
# Change root password
passwd root

# List all users with shells
cat /etc/passwd | grep -v nologin | grep -v false

# Lock user account
usermod -L [username]

# Check running services
systemctl list-units --type=service --state=running

# Check listening ports
ss -tlnp
```

Service Hardening

```
# Check SSH config
cat /etc/ssh/sshd_config

# Disable root SSH login (edit sshd_config)
# PermitRootLogin no

# Restart SSH
systemctl restart sshd

# Check for cron jobs
crontab -l
cat /etc/crontab
ls -la /etc/cron.d/
```

Enable Logging

```
# Check logging service
systemctl status rsyslog

# Watch auth log
tail -f /var/log/auth.log

# Check for failed logins
grep "Failed password" /var/log/auth.log
```

Evening (2 hours): Network Hardening

Network Team Practice

Firewall Basics (iptables)

```
# List current rules
iptables -L -n -v

# Block specific IP
iptables -A INPUT -s [IP] -j DROP

# Allow specific port
iptables -A INPUT -p tcp --dport [port] -j ACCEPT

# Save rules
iptables-save > /etc/iptables/rules.v4
```

Windows Firewall

```
# Check firewall status
Get-NetFirewallProfile

# Enable firewall
Set-NetFirewallProfile -Enabled True

# Block IP
netsh advfirewall firewall add rule name="Block [IP]" dir=in action=block remoteip=[IP]
```

DAY 3: DETECTION & RESPONSE

Morning (3 hours): Attack Detection

Recognize These Patterns

1. Brute Force Attack

Indicators:

- Multiple failed logins from same source
- Event ID 4625 (Windows) repeated
- "Failed password" in auth.log (Linux)

Response:

```
# Windows - Find failed logins
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4625} -MaxEvents 20

# Linux - Find failed logins
grep "Failed password" /var/log/auth.log | tail -20
```

2. New Account Created

Indicators:

- Event ID 4720 (Windows)
- /etc/passwd modified (Linux)
- Unknown account in admin groups

Response:

```
# Windows - Recent account events
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4720}

# Linux - Check recent changes
ls -la /etc/passwd
cat /etc/passwd | grep -v nologin
```

3. Scheduled Task/Cron Created

Indicators:

- Event ID 4698 (Windows)
- New files in /etc/cron.d/ (Linux)
- Tasks running from unusual paths

Response:

```
# Windows - List scheduled tasks
schtasks /query /fo LIST /v | Select-String "TaskName|Run As|Task To Run"

# Linux - Check all cron
for user in $(cut -f1 -d: /etc/passwd); do echo "=== $user ==="; crontab -u $user -l 2>/dev/null; done
```

4. Lateral Movement

Indicators:

- SMB connections to admin shares (C$, ADMIN$)
- SSH from internal to internal
- PsExec or WMI usage

Response:

```
# Windows - Check SMB connections
Get-SmbSession
netstat -an | findstr ":445"

# Linux - Check SSH connections
ss -tnp | grep ssh
who
```

Afternoon (3 hours): Incident Response Drill

Run 3 Tabletop Scenarios

Scenario 1: Credential Compromise

> *""You notice an admin account logging in from an unknown IP. What do you do?""*

Expected Response:

1. Alert Captain immediately
2. Identify which account
3. Disable the account
4. Block the source IP
5. Check for persistence
6. Begin incident report

Scenario 2: Service Disruption

""The web server suddenly stops responding to scoring checks. What do you do?""

Expected Response:

1. Alert Captain immediately
2. Check service status
3. Check logs for errors
4. Restart service if needed
5. Verify scoring engine checks pass
6. Investigate root cause
7. Document everything

Scenario 3: Persistence Found

""You find a suspicious scheduled task that runs a script from C:\Temp. What do you do?""

Expected Response:

1. Document the task details
2. Alert Captain
3. Copy the script for analysis (don't run it!)
4. Delete the scheduled task
5. Delete the script
6. Check for other persistence
7. Write incident report

Evening (2 hours): Inject Practice

Practice These Inject Types

1. Policy Document

""The CEO needs a Password Policy document within 30 minutes.""

Template Structure:

```
PASSWORD POLICY
Company: [Name]
Date: [Date]
Version: 1.0
```

```
1. PURPOSE
This policy establishes password requirements...

2. SCOPE
All employees, contractors, and systems...

3. REQUIREMENTS
- Minimum 12 characters
- Must contain uppercase, lowercase, numbers, symbols
- Changed every 90 days
- No password reuse for 12 generations

4. ENFORCEMENT
Violations may result in...

Approved by: [Name/Title]
```

2. Executive Briefing

> *""Brief the CEO on current security status in 5 minutes.""*

Template Structure:

```
SECURITY STATUS BRIEFING
Time: [HH:MM]
Presenter: [Name]

CURRENT STATUS: [GREEN/YELLOW/RED]

SERVICES: [X/Y] operational

INCIDENTS:
- [Count] incidents detected
- [Count] contained
- [Count] under investigation

RISKS:
- [Top risk]
- [Second risk]

RECOMMENDATIONS:
- [Action item]

QUESTIONS?
```

DAY 4: FULL SIMULATION

The Mock Competition (4-6 hours)

Setup

1. Captain sets up Status Board
2. All members at stations
3. Timer set for 4 hours
4. "External evaluator" (coach/mentor) ready to send injects

Simulation Timeline

Time	Event	Team Action
0:00	Competition starts	Begin First 15 Minutes checklist
0:15	Network mapped	Start hardening priority systems
0:30	First inject arrives	Inject Lead assigns and tracks
1:00	"Attack" begins	Detection team monitors
1:30	Incident detected	IR Lead takes charge
2:00	Second inject arrives	Balance incident and inject
2:30	Service goes down	Rapid recovery
3:00	Third inject arrives	Inject Lead prioritizes
3:30	Major incident	Full team response
4:00	Competition ends	Final documentation

Evaluator Should Simulate

• 3-4 business injects
• 2-3 "attacks" (disable account, stop service, create suspicious task)
• 1 major incident requiring team coordination
• Time pressure

After-Action Review

1. What went well?
2. What broke down?
3. Where did communication fail?
4. What would we do differently?
5. Update procedures based on lessons

DAY 5: FINAL PREP & REST

Morning (2 hours): Materials Finalization

Print Final Copies

- ■ Captain Status Board (5 copies)
- ■ Asset Inventory (10 copies)
- ■ Change Log (20 copies)
- ■ Incident Report (15 copies)
- ■ Inject Response Template (15 copies)
- ■ Command Reference (10 copies)
- ■ This Guide (2 copies)

Equipment Check

- ■ All laptops charged and working
- ■ Power strips and extension cords
- ■ Ethernet cables (backup)
- ■ USB drives with templates
- ■ Pens, markers, highlighters
- ■ Sticky notes
- ■ Snacks and water

Contact Information

- ■ All team members' phone numbers
- ■ Emergency contact for each member
- ■ Competition venue address
- ■ Competition organizer contact

Afternoon: Light Review Only

30-Minute Review Per Person

- • Review your specific responsibilities
- • Review the Iron Rules
- • Review your system's commands
- • Ask any final questions

DO NOT

- Learn new techniques
- Make major changes to plans
- Stay up late studying
- Add stress

Evening: Rest & Preparation

Required

- Good dinner together (team bonding)
- Early to bed (8+ hours sleep)
- Clothes laid out
- Bag packed
- Alarm set

Team Captain

- Send encouraging message to team
- Confirm logistics for morning
- Review Status Board one more time
- Get good sleep

COMPETITION DAY PLAYBOOK

Before Arrival

Morning Of

- Good breakfast
- Arrive 30+ minutes early
- Bring all materials
- Positive mindset

The First 15 Minutes

MINUTE 0-2: ORIENTATION

- [ ] Receive competition packet
- [ ] Confirm team roster with White Team
- [ ] Set up Captain Status Board
- [ ] All members log into stations

MINUTE 2-5: NETWORK DISCOVERY

- [ ] Obtain network topology
- [ ] Document network range: _____
- [ ] Identify gateway: _____
- [ ] Identify DNS servers: _____

MINUTE 5-8: SYSTEM IDENTIFICATION

- [ ] List all Windows servers with IPs
- [ ] List all Linux servers with IPs
- [ ] Identify Domain Controller
- [ ] Document hostname for each system

MINUTE 8-12: SERVICE MAPPING

- [ ] Identify web server (HTTP/HTTPS)
- [ ] Identify email server (SMTP)
- [ ] Identify DNS server
- [ ] Identify database server
- [ ] Verify all scored services responding

MINUTE 12-15: CREDENTIAL & ASSIGNMENT

- [ ] Document provided credentials
- [ ] Verify logins work
- [ ] Assign owner to each system
- [ ] Announce first hardening priorities

Minutes 15-60: Initial Hardening

Priority Order

1. **Change ALL default passwords**
2. **Disable Guest accounts**
3. **Enable logging**
4. **Check for unauthorized accounts**
5. **Verify services still running**

Every 15 Minutes

- Captain: Update Status Board
- All: Report status to Captain
- IR Lead: Check logs for anomalies
- Inject Lead: Check inject queue

Ongoing Operations

Continuous

- ■ Monitor logs
- ■ Check service status
- ■ Watch for injects
- ■ Communicate changes

Every 30 Minutes

- ■ Full team status update
- ■ Captain Status Board update
- ■ Review anomaly log
- ■ Prioritize next actions

When Incident Detected

1. Alert Captain
2. Identify scope
3. Contain immediately
4. Preserve evidence
5. Begin IR report
6. Continue service monitoring

When Inject Arrives

1. Log receipt time
2. Note deadline
3. Assign owner
4. Begin work immediately
5. Quality check
6. Submit early
7. Confirm receipt

RED TEAM ATTACK PATTERNS

Attack Timeline

Time	Phase	What to Expect
0-15 min	Reconnaissance	Port scans, service enumeration
15-60 min	Initial Access	Default credentials, known exploits
1-2 hours	Persistence	Backdoors, scheduled tasks, new accounts
2-4 hours	Lateral Movement	Moving to other systems
4-6 hours	Escalation	Domain admin attempts
6-8 hours	Impact	Service disruption, data theft

Top Attack Techniques

1. Valid Accounts (T1078)

CCDC Relevance: VERY HIGH

Red Team WILL try default credentials in the first 5 minutes.

Detection:

- Multiple failed logins followed by success
- Login from unusual IP
- Login outside normal hours

Response:

- Change ALL default passwords immediately
- Enable account lockout
- Monitor auth logs continuously

2. Scheduled Tasks (T1053)

CCDC Relevance: VERY HIGH

Favorite persistence method for Red Team.

Detection:

- Event ID 4698 (Windows)

- New cron jobs
- Tasks from unusual paths

Response:

- Audit all scheduled tasks immediately
- Remove unauthorized tasks
- Monitor task creation

3. Create Account (T1136)

CCDC Relevance: VERY HIGH

Check for new accounts constantly.

Detection:

- Event ID 4720 (Windows)
- /etc/passwd changes (Linux)
- New members in admin groups

Response:

- Document all legitimate accounts
- Immediately disable unknown accounts
- Alert on any account creation

4. SMB/Admin Shares (T1021.002)

CCDC Relevance: VERY HIGH

Primary Windows lateral movement.

Detection:

- Access to C$, ADMIN$ shares
- PsExec execution
- Service creation on remote systems

Response:

- Restrict admin share access
- Monitor SMB traffic
- Use network segmentation

5. SSH Lateral Movement (T1021.004)

CCDC Relevance: VERY HIGH

Primary Linux lateral movement.

Detection:

- SSH between internal systems
- New authorized_keys entries
- SSH from unusual source

Response:

- Change SSH keys and passwords
- Restrict SSH access
- Monitor SSH logs

Quick Detection Reference

Attack	Windows Indicator	Linux Indicator	Immediate Action
Brute Force	Event 4625 (many)	"Failed password" in auth.log	Block source IP
New Admin	Event 4720 + 4732	/etc/passwd + /etc/group	Disable account
Scheduled Task	Event 4698	crontab changes	Remove task
Service Install	Event 7045	systemd unit created	Stop and remove
Lateral (SMB)	Event 5140/5145	N/A	Block source
Lateral (SSH)	N/A	SSH from internal	Kill session

COMMAND REFERENCE

Windows Commands

User Management

```
# List all users
net user

# Change password
net user [username] [newpassword]

# Disable account
net user [username] /active:no

# List admins
net localgroup Administrators

# Add to group
net localgroup Administrators [user] /add
```

Service Management

```
# List services
Get-Service

# Start service
Start-Service [servicename]

# Stop service
Stop-Service [servicename]

# Restart service
Restart-Service [servicename]
```

Network

```
# Show connections
netstat -ano

# Show listening ports
netstat -an | findstr LISTENING

# Find process on port
netstat -ano | findstr :[port]

# IP configuration
ipconfig /all
```

Process Management

```
# List processes
tasklist

# Kill process
taskkill /PID [PID] /F

# Kill by name
taskkill /IM [name].exe /F
```

Event Logs

```
# Security events
Get-EventLog -LogName Security -Newest 50

# Failed logins
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4625} -MaxEvents 20

# Account created
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4720}
```

Scheduled Tasks

```
# List tasks
schtasks /query /fo LIST /v
```

```
# Delete task
schtasks /delete /tn [taskname] /f
```

Firewall

```
# Check status
Get-NetFirewallProfile

# Enable
Set-NetFirewallProfile -Enabled True

# Block IP
netsh advfirewall firewall add rule name="Block" dir=in action=block remoteip=[IP]
```

Active Directory

```
# List Domain Admins
Get-ADGroupMember "Domain Admins"

# List all users
Get-ADUser -Filter *

# Reset password
Set-ADAccountPassword -Identity [user] -Reset -NewPassword (ConvertTo-SecureString "[pass]" -AsPlainText -Force)

# Disable account
Disable-ADAccount -Identity [username]
```

Linux Commands

User Management

```
# List users
cat /etc/passwd

# Users with shells
cat /etc/passwd | grep -v nologin | grep -v false

# Change password
passwd [username]

# Lock account
usermod -L [username]

# List sudoers
cat /etc/sudoers
getent group sudo
```

Service Management

```
# List services
systemctl list-units --type=service

# Check service
systemctl status [service]

# Start service
systemctl start [service]

# Stop service
systemctl stop [service]

# Restart service
systemctl restart [service]
```

Network

```
# Show connections
ss -tunapl

# Listening ports
ss -tlnp

# Find process on port
lsof -i :[port]

# IP configuration
ip addr
```

Process Management

```
# List processes
ps aux

# Find process
ps aux | grep [name]

# Kill process
kill -9 [PID]

# Kill by name
pkill [name]
```

Logs

```
# Auth log
tail -f /var/log/auth.log

# System log
tail -f /var/log/syslog

# Failed SSH
grep "Failed password" /var/log/auth.log

# Successful SSH
```

```
grep "Accepted" /var/log/auth.log
```

Cron Jobs

```
# List current user cron
crontab -l

# List all users cron
for user in $(cut -f1 -d: /etc/passwd); do echo "=== $user ==="; crontab -u $user -l 2>/dev/null; done

# System cron
cat /etc/crontab
ls -la /etc/cron.d/
```

Firewall (iptables)

```
# List rules
iptables -L -n -v

# Block IP
iptables -A INPUT -s [IP] -j DROP

# Allow port
iptables -A INPUT -p tcp --dport [port] -j ACCEPT

# Save rules
iptables-save > /etc/iptables/rules.v4
```

TEMPLATES

Incident Report Template

```
INCIDENT REPORT
===============

INCIDENT ID: IR-____-___
DATE/TIME DETECTED: _________________
REPORTED BY: _________________
SEVERITY: [ ] Critical [ ] High [ ] Medium [ ] Low
STATUS: [ ] Open [ ] Investigating [ ] Contained [ ] Resolved

EXECUTIVE SUMMARY:
_____________________________________________________________________
_____________________________________________________________________

AFFECTED SYSTEMS:
| Hostname | IP | Role | Impact |
```

```
|----------|-----|------|--------|
|          |     |      |        |

TIMELINE:
| Time | Event | Action |
|------|-------|--------|
|      | Detected |        |
|      | Contained |        |
|      | Resolved |        |

INDICATORS OF COMPROMISE:
- IP Addresses:
- User Accounts:
- File Paths:
- Processes:
```

Captain Status Board

```
CAPTAIN STATUS BOARD
====================
Competition: _________________ Date: _________________

TEAM STATUS (Update every 15 min)
| Role | Name | Task | Status |
|------|------|------|--------|
| Captain | | | [ ]G [ ]Y [ ]R |
| Windows/AD | | | [ ]G [ ]Y [ ]R |
| Linux | | | [ ]G [ ]Y [ ]R |
| Network | | | [ ]G [ ]Y [ ]R |
| IR Lead | | | [ ]G [ ]Y [ ]R |
| Inject Lead | | | [ ]G [ ]Y [ ]R |
| Support 1 | | | [ ]G [ ]Y [ ]R |
| Support 2 | | | [ ]G [ ]Y [ ]R |

SERVICE STATUS (Update every 5 min)
| Service | Status | Last Check |
|---------|--------|------------|
| Web HTTP | [ ]UP [ ]DOWN | |
| Web HTTPS | [ ]UP [ ]DOWN | |
| DNS | [ ]UP [ ]DOWN | |
| Email | [ ]UP [ ]DOWN | |
| Database | [ ]UP [ ]DOWN | |
| AD/LDAP | [ ]UP [ ]DOWN | |

INJECT TRACKER
| ID | Due | Description | Owner | Status |
|----|-----|-------------|-------|--------|
| | | | | [ ]NEW [ ]WIP [ ]DONE |
```

Change Log Entry

```
CHANGE LOG ENTRY
================

ENTRY #: ___
TIME: ___:___
CHANGED BY: _________________
SYSTEM: _________________
CHANGE TYPE: [ ] Config [ ] Account [ ] Firewall [ ] Service [ ] Other
APPROVED BY: _________________

DESCRIPTION:
_____________________________________________________________________

REASON:
_____________________________________________________________________

VERIFICATION:
_____________________________________________________________________

ROLLBACK PLAN:
_____________________________________________________________________
```

CASE STUDIES

Case Study 1: NECCDC 2025

Champion: UMass Lowell

Scenario

Healthcare organization facing third-party vendor risks.

Technology Stack

- AWS Cloud
- Palo Alto Firewall
- Kubernetes
- Graylog (SIEM)
- Teleport
- pfSense

Key Findings

- 60% of participants were first-time competitors
- Teams unfamiliar with Kubernetes ranked lower
- Log management (Graylog) was a critical differentiator
- Third-party risk assessment heavily tested

Lessons Learned

1. **Cloud security skills are essential** - Practice AWS/Azure before competition
2. **Container knowledge matters** - Kubernetes is increasingly common
3. **Centralized logging wins** - Teams with good log management detected attacks faster
4. **Vendor assessment is tested** - Prepare for third-party risk scenarios

Case Study 2: Nationals 2025

Champion: UC Irvine

Scenario

Biotechnology company protecting sensitive research data.

Key Competition Rules

- Risk assessment for tools was mandatory
- All configuration changes required documentation
- Gaming strategies (shutting services) were prohibited
- Documentation quality heavily weighted

Winning Strategies

1. **Intensive training** - Spring break and weekends
2. **Rapid onboarding** - System for new team members
3. **Documentation culture** - Everything written down
4. **Inject focus** - Business tasks given equal weight

Lessons Learned

1. **Document EVERYTHING** - It's half the battle
2. **Risk assessment must be automatic** - Practice until it's second nature
3. **No shortcuts** - Gaming strategies are penalized
4. **Professional communication** - White Team interaction matters

Common Success Patterns Across Champions

1. Documentation First

Champions document before, during, and after every action.

2. Team Discipline

Clear roles, communication protocols, and escalation paths.

3. Balanced Focus

Equal attention to services AND business injects.

4. Adaptability

Ability to handle new technologies and unexpected scenarios.

5. Practice

Championship teams practice more. There are no shortcuts.

CHAMPIONSHIP MINDSET

The Mental Game

Before Competition

- **Confidence**: You have prepared. Trust your training.
- **Focus**: This is one competition. Do your best.
- **Team**: You succeed or fail together.

During Competition

- **Stay calm**: Panic causes mistakes.
- **Communicate**: No lone wolves.
- **Prioritize**: Not everything is urgent.
- **Document**: Write it down.

When Things Go Wrong

- **Breathe**: Take 3 deep breaths.
- **Contain**: Stop the bleeding first.
- **Communicate**: Tell the team.
- **Move on**: Don't dwell on mistakes.

Team Mantras

> *""Service uptime is sacred.""*
>
> *""Document everything.""*
>
> *""Contain first, diagnose later.""*
>
> *""We win together.""*

The Champion's Edge

The difference between good teams and champions is not technical skill alone. It's:

1. **Discipline** - Following the Iron Rules even under pressure
2. **Communication** - Constant, clear, professional
3. **Balance** - Technical defense AND business tasks
4. **Resilience** - Recovering quickly from setbacks
5. **Unity** - Supporting each other throughout

FINAL CHECKLIST

5 Days Before

- ■ Team roles assigned
- ■ Templates printed
- ■ Equipment tested
- ■ Communication channel confirmed

4 Days Before

- ■ Technical hardening practiced
- ■ All members can do basic tasks
- ■ Command reference reviewed

3 Days Before

- ■ Detection drills completed
- ■ Incident response practiced
- ■ Inject practice done

2 Days Before

- ■ Full simulation completed
- ■ Lessons learned documented
- ■ Procedures updated

1 Day Before

- ■ Materials finalized
- ■ Equipment packed
- ■ Good sleep

Competition Day

- ■ Good breakfast
- ■ Arrive early
- ■ Positive mindset
- ■ Execute the plan

RESOURCES

Online Training Platform: https://ccdc.x1000.ai

Official NCCDC: https://nationalccdc.org

MITRE ATT&CK;: https://attack.mitre.org

MITRE D3FEND: https://d3fend.mitre.org

Remember:

> *"**"CCDC is not about who hacks best—it is about who keeps the business running under fire."**"*

This guide was created by CCDC.x1000.ai - Elite Blue Team Training Platform

LIGHT HOPE LLC · Boston, MA

EMPOWER GOOD WITH AI

Good luck, champions. You've got this.