Moorhead CCDC Challenge
Version: 1.0

Overview

This is part of a series of weekend practice sessions for the CCDC. The systems will be reset on Ethiopia.mait.minnesota.edu for the group. The group will work on the listed items, create a report, amount of time for activity, and report participants. All reports must follow the CCDC Business Guidelines.

Tasks and Reporting

1. Identify and change all administration logins and passwords on each system. Have the operating system report last password change time.
2. Create an alternate administration account on all systems. Have the operating system report last password change time.
3. Identify for each host all the accounts able to login over the network. List any accounts using SSH keys.
4. Create a backup of all critical files on the system. Report the computer hash value for each backup. Report the storage location of each backup.
5. Identify all non-administrative logins on each system. Create and report a csv file to change all passwords.
6. Identify all logins/logons currently logged into each system. Report a method to force off any unwanted logins/logons.
7. Identify and list all non-human associate accounts with full administrative privileges.
8. Report the configuration of setting an appropriate message of the day on each host.
9. Report the configuration of a system to allow GUI access to all required GUI applications.
10. Report all the necessary open ports for each host. Provide the firewall listing only necessary ports are open.
11. Report the routing table for each system. Report if the routing is correct.
12. Report the DNS settings for each system. Report if the settings are correct.
13. Report all the changes made to implement DNSsec. Identify the security enhancement provided by DNSsec.
14. Report the anti-malware, backdoor, and rootkit detection on each hosts. Report any remediation necessary.
15. Report the log configuration for each host. Explain why auditd is not found on an Linux host. Explain how Windows hosts will be set with Group Policy.
16. Report the configuration for all appropriate hosts to forward log files to the Splunk server. Report an analysis of the data in Splunk.
17. Report the configuration for all appropriate host to utilize OSSEC and/or Wahzuh. Report an analysis of data in Splunk and Wahzuh.
18. Report the configuration and all scheduled task of cron or task scheduler on all hosts. Report which tasks must remain for host operation.
19. Report the configuration of AppArmor, SELinux, or similar option for appropriate hosts. Identify the security enhancement provided.
20. Report the configuration of IPsec for all hosts. Identify the security enhancement provided.
21. Report the configuration of update for each host. Provide the validation all updates are provided from a trusted source.
22. Report for each host any AI agents installed. Provide the permission level of each agent.
23. Report the output of using tools like Microsoft's RAMPART and Clarity on all hosts.
24. Report the configuration and types of scans run from NMAP. Generate a network map suitable for the CISO.

25. Report a network traffic analysis showing who each host is talking.
26. Report other current attacks, defense, and remediation against this system.
27. Report the configuration of a container server running at least one useful container enhancing security. Identify the security enhancements of the container.
28. Identify all important data files on all systems. Report how you will know the data has been stolen and/or compromised. Report how quickly data theft/compromise is detected.
29. Provide a reporting system that gathers the necessary information from log files and elsewhere to report a red team attack or sabotage.

AI suggestions

These are some suggestions provided by AI during the development of practice. This is to give you some ideas. The original idea is each session would only take an hour.

Gemini Suggestion 01

To dominate at CCDC, speed and documentation are your primary weapons. During the initial "white inject" phase, your team needs to stabilize the environment while simultaneously hardening it. Below is the **CCDC Initial Hardening Drill** designed for a 6-student "Blue Team."

Team Roster & Role Assignment

Role	Primary Systems	Secondary Focus
Team Lead (TL)	Palo Alto 11 / Cisco Firepower	Inject Management & Monitoring
Linux Admin 1	Ubuntu eCom / Fedora Webmail	Scripting & Credential Rotation
Linux Admin 2	Oracle Splunk / VyOS Router	Log Aggregation & Networking
Windows Admin 1	WS 2019 AD-DNS / WS 2022 FTP	Domain Hardening & GPO
Windows Admin 2	WS 2019 Web / Ubuntu Workstation	IIS Security & Client Hardening
SOC Analyst	Splunk Dashboard	Real-time Alerting & Incident Reports

---

Assignment Sheet: Phase 1 (The First 60 Minutes)

Task 1: Credential Rotation (Login Password Changes)

Objective: Lock out default or compromised credentials without breaking service accounts.

- **Linux Team:** Use a loop to change all human user passwords. **Warning:** Do not change service accounts (like www-data or postgres) until dependencies are verified.
  - *Action:* chpasswd is your best friend for bulk changes.
- **Windows Team:** Change the Domain Admin password immediately. Create a "Break Glass" local admin on each server that is disconnected from the domain.
- **Networking:** Change the admin password on the Palo Alto and VyOS. Ensure the VyOS config is saved post-change.

Task 2: Discovery (List Administrators)

Objective: Identify every account with elevated privileges. Red Teams often hide "backdoor" admins with names like svc_sql or backup_admin.

- **Linux:** Audit /etc/sudoers, /etc/sudoers.d/, and the wheel or sudo groups.
  - *Command:* grep '^sudo:.*$' /etc/group and getent group wheel.
- **Windows:** Use PowerShell to export members of "Domain Admins," "Enterprise Admins," and local "Administrators" groups.
  - *Command:* Get-NetLocalGroupMember -Group "Administrators"
- **Network:** Check local user databases on the Firepower and Palo Alto.

Task 3: Redundancy (Create Alternate Administrators)

Objective: Ensure that if a Red Team locks a primary account, the team can still access the box.

- **Strategy:** Create a non-standard admin name (e.g., mstate_mgmt) on all systems.
- **Linux:** Ensure SSH keys are deployed for this new user and password authentication is disabled once verified.
- **Windows:** Deploy a new Domain Admin and a separate GPO that adds a specific "Team Admin" user to the local administrators group of all workstations.

Task 4: Early Warning (Detecting Unauthorized Logins)

Objective: See the Red Team before they see you.

- **SOC Analyst:** Set up a Splunk "Quick View" for Event ID **4624** (Successful Login) and **4625** (Failed Login) for Windows, and Accepted password for SSH on Linux.
- **Palo Alto:** Configure "Log Forwarding" to the Splunk server for all GlobalProtect or Management UI login attempts.
- **Linux Team:** Deploy a simple auditd rule or a watcher script:

Bash
tail -f /var/log/auth.log | grep "Accepted"

Practice Drill Evaluation Criteria
To pass this drill, the team must provide the Team Lead with the following "Deliverables" within the allotted time:

1. **The "Credential Ledger":** A secure (offline or encrypted) list of all new passwords.
2. **The "Admin Audit":** A list of all accounts found on the systems that were deleted/disabled.
3. **The "Connection Map":** A VyOS and Firewall verification that only management IPs can SSH/RDP into the servers.
4. **The "Splunk Proof":** A screenshot of the SOC Analyst's dashboard showing a successful alert triggered by a "test" unauthorized login attempt.

Expert Tip: On the **Fedora 42** and **Ubuntu 24** boxes, check for authorized_keys files immediately. Red Teams love persistence via SSH keys more than they love passwords.

Gemini Suggestion 02

In CCDC, the first 60 minutes—often called the **"Survival Hour"**—is a race between your team's hardening scripts and the Red Team's persistence mechanisms. With 8 students, you have the luxury of dedicated specialists.
Here is your prioritized battle plan and team assignment sheet.

The "Survival Hour" Team Roster

Role	Primary Systems	Student Assignment
Team Lead (TL)	Palo Alto / Firepower / Injects	**Student 1**
Windows Admin 1	AD-DNS / Windows Web	**Student 2**
Windows Admin 2	WS 2022 FTP / Ubuntu Workstation	**Student 3**
Linux Admin 1	Ubuntu 24 eCom / VyOS Router	**Student 4**
Linux Admin 2	Fedora 42 Webmail / Oracle 9	**Student 5**
SOC / SIEM	Oracle 9 (Splunk)	**Student 6**
Network Engineer	Palo Alto / Cisco Firepower	**Student 7**
Intelligence/Injects	All Systems (Documentation)	**Student 8**

Prioritized Activity List (Minutes 0–60)
1. Immediate Lockdown & Visibility (0–15 Minutes)
The goal is to stop the "low-hanging fruit" attacks.

- **Network (Student 7):** Log into the Palo Alto and Cisco Firepower. Immediately **disable any "Permit Any" rules**. Restrict management access to only the designated internal management subnet.
- **Linux (Students 4 & 5):** Open a terminal and run last and w to see who is currently logged in. Immediately change the root password and your own user password.

- **Windows (Students 2 & 3):** Change the Domain Admin password. Open **Active Directory Users and Computers** and look for any recently created accounts (sort by "WhenCreated").
- **SIEM (Student 6):** Verify Splunk is receiving logs from the Palo Alto. This is your "canary in the coal mine."

2. Credential & Access Audit (15–30 Minutes)

The Red Team is likely already in. You need to find their backdoors.

- **List Administrators:** * **Windows:** Run net localgroup administrators on every box. Document any names that aren't on your official roster.
    - **Linux:** Check /etc/sudoers and /etc/sudoers.d/. Look for NOPASSWD entries.
- **Create Alternate Admins:** Create one "clean" administrative account on each box with a complex 20+ character password. This is your "Break Glass" account if the Red Team locks you out of the primary admin.
- **Detecting Unauthorized Logins:** * **Student 6 (SOC):** Create a real-time dashboard for "Failed Login Attempts" and "New User Created" events.
    - **Student 4 (Linux):** Check /home/user/.ssh/authorized_keys. **Delete everything** in those files unless you specifically put it there.

3. Service Stabilization (30–45 Minutes)

Keep your points flowing. Hardening is useless if the services go down.

- **E-Com & Webmail (Students 4 & 5):** Verify the web services are up. Change the database passwords (MySQL/PostgreSQL) and update the web config files immediately so the site doesn't break.
- **FTP & DNS (Students 2 & 3):** Ensure the Windows FTP server isn't allowing anonymous uploads. Check DNS for any "shadow" records pointing to external IPs.
- **VyOS (Student 4):** Verify the routing table. Ensure there isn't a "backdoor" route sending traffic to a Red Team-controlled subnet.

4. Final Hardening & Documentation (45–60 Minutes)

Prepare for the first "Business Inject."

- **Student 8 (Intelligence):** Collect all new passwords, IP changes, and deleted account names from the team. Prepare the first **Incident Report (IR)** if any unauthorized activity was found.
- **TL (Student 1):** Review the Palo Alto logs. Look for beacons (repeated small outbound connections). Tell the Network Engineer to block those IPs.
- **All Admins:** Disable all unnecessary services (e.g., Telnet, R-services, older versions of SMB).

Assignment Sheet: Performance Metrics

Task	Minimum Success Criteria
Login Security	All default passwords changed; no two systems share the same local admin password.
Admin Audit	A spreadsheet exists listing every account with sudo/admin rights across all 9 systems.
Persistence Kill	All .ssh/authorized_keys are cleared; Scheduled Tasks/Cron jobs audited.
Detection	Splunk triggers an alert within 30 seconds of a failed login attempt.

Coach's Note: If you see a student typing slowly, have them use a "Cheat Sheet" of pre-written commands. In CCDC, **Command Line proficiency = Life.** Do not use GUIs where a PowerShell or Bash script can do it faster.

Gemini Suggestion 03

To survive the "Survival Hour," your team must treat the environment as **already compromised**. This plan prioritizes visibility (Splunk/Time) alongside hardening, ensuring that when you find a threat, your logs have accurate timestamps for Incident Reports (IRs).

Need to add auditd to Linux and configure Windows logging

The 8-Person "Blue Team" Roster

Role	Primary Systems	Student Assignment
Team Lead (TL)	Palo Alto / Firepower / Injects	**Student 1**
Windows Admin 1	AD-DNS / WS 2019 Web	**Student 2**
Windows Admin 2	WS 2022 FTP / Ubuntu Workstation	**Student 3**
Linux Admin 1	Ubuntu 24 eCom / VyOS 1.4.3	**Student 4**
Linux Admin 2	Fedora 42 Webmail / NTP Setup	**Student 5**
SOC / SIEM	Oracle 9 (Splunk Server)	**Student 6**
Log Architect	Splunk Forwarder Deployment	**Student 7**
Intelligence/IR	Documentation & Evidence Prep	**Student 8**

Prioritized First 60-Minute Activity List

Phase 1: Establish Truth & Perimeter (0–15 Minutes)

- **Secure Time (Student 5):** Configure the **Fedora 42** box as the internal NTP master. Sync it to a reliable external stratum (or the competition-provided source). Point the VyOS router and all servers to this Fedora box. **Why:** Accurate logs are useless if timestamps don't match across systems.
- **Perimeter Lockdown (Student 1 & 7):** On the Palo Alto and Firepower, change admin credentials immediately. Apply a "Management Plane" ACL so only specific internal IPs can access the UI/SSH.
- **Root Credential Rotation (Students 2, 3, 4):** Change Administrator and root passwords. Use a long, complex passphrase. Do not use the same password for Windows and Linux.

Phase 2: Visibility & Splunk Setup (15–40 Minutes)

- **Splunk Server Setup (Student 6):** Log into the **Oracle 9** box. Start the Splunk service. Set up a "Receiver" on port 9997. Create indexes for wineventlog, linux_auth, and net_logs.
- **Splunk Forwarders (Student 7):** * **Windows:** Deploy the Universal Forwarder (UF) via PowerShell to the AD-DNS, Web, and FTP servers. Configure them to send Security, System, and Application logs.
    - **Linux:** Install the UF on the eCom and Webmail servers. Monitor /var/log/auth.log, /var/log/secure, and web server access logs.
- **Admin Discovery (Students 2, 3, 4):** * **Linux:** grep ':0:' /etc/passwd to find UID 0 accounts.
    - **Windows:** Get-ADGroupMember -Identity "Domain Admins" and check local Administrators groups.

Phase 3: Persistence Removal (40–60 Minutes)

- **Kill Backdoors (Students 2, 3, 4, 5):** * **Linux:** Clear all /home/*/.ssh/authorized_keys. Check crontab -l for all users and look for reverse shells.
    - **Windows:** Check **Task Scheduler** for suspicious triggers. Audit **Startup** folders and the Run registry keys.

- **Create Alternate Admins:** Create a "clean" admin account on each system (e.g., mstate_admin) with a unique password for recovery.
- **Traffic Audit (Student 1):** Check Palo Alto logs for high-port outbound traffic (potential Command & Control beacons). Block these IPs immediately.

Assignment Sheet: Technical Requirements

1. Splunk Forwarder Quick-Start (Student 7)

On Linux systems, use the following to quickly point to Student 6's Oracle 9 server:

Bash

```
/opt/splunkforwarder/bin/splunk add forwarder-server <ORACLE_9_IP>:9997
/opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log -index linux_auth
```

2. Secure NTP Configuration (Student 5)

On the **VyOS 1.4.3** Router:

Bash

```
set system ntp server <FEDORA_IP>
```

On **Windows** (via Command Prompt as Admin):

DOS

```
w32tm /config /manualpeerlist:"<FEDORA_IP>" /syncfromflags:manual /reliable:YES /update
w32tm /resync
```

3. Critical Login Detection (Student 6)

In Splunk, create an alert for:

- **Windows:** EventCode=4624 (Successful Login) WHERE TargetUserName != "mstate_admin".
- **Linux:** "Accepted password for" AND NOT "mstate_admin".

Deliverables for the Team Lead (at Minute 60)

1. **The Master Password Vault:** Encrypted list of all rotated credentials.
2. **The NTP Sync Report:** Confirmed list showing all 9 systems have the same system time.
3. **The SIEM Confirmation:** Student 6 confirms data is flowing from all 9 systems into Splunk.
4. **The "Purge" List:** A list of all unauthorized accounts deleted and backdoors closed for the first Incident Report.

To maintain visibility during a CCDC event, deploying **Universal Forwarders (UFs)** is your team's highest priority after password changes. The UF is a lightweight version of Splunk that consumes minimal resources while securely shipping logs to your Indexer (the Oracle 9 Splunk Server).

Part 1: Linux Installation (Ubuntu 24 / Fedora 42 / Oracle 9)

On Linux, we prioritize the command line for speed and scriptability across multiple boxes.

1. **Download:** Use wget to pull the .deb (Ubuntu) or .rpm (Fedora/Oracle) package from your team's internal file share or the Splunk website.
2. **Install:**
    - **Ubuntu:** sudo dpkg -i splunkforwarder-<version>.deb
    - **Fedora/Oracle:** sudo rpm -i splunkforwarder-<version>.rpm
3. **Initialize:** * sudo /opt/splunkforwarder/bin/splunk start --accept-license
    - Set a strong local CLI password when prompted.
4. **Connect to Indexer:**
    - sudo /opt/splunkforwarder/bin/splunk add forwarder-server <SPLUNK_SERVER_IP>:9997

5. **Add Monitoring:** * sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log -index linux_auth
    - sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/syslog

---

Part 2: Windows Installation (Server 2019/2022)
For Windows, the GUI is often faster for initial setup unless you have a PowerShell script ready.

1. **Run Installer:** Launch the .msi installer as an Administrator.
2. **Deployment Server:** Skip this unless the competition provides a Deployment Server.
3. **Receiving Indexer:** Enter the IP address of your **Oracle 9 Splunk Server** and port **9997**.
4. **Log Selection:** Check the boxes for:
    - **Application**
    - **Security** (Critical for login detection!)
    - **System**
5. **Service Account:** Select **"Local System"** to ensure it has permissions to read all log files.
6. **Verify:** Open a Command Prompt as Admin and run:
    - "C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" list forward-server

---

Part 3: To Install or Not to Install? (Network Appliances)
In CCDC, you have three primary networking devices: **Palo Alto 11**, **Cisco Firepower 7**, and **VyOS 1.4.3**.
Why you should NOT install the UF on them:

1. **Incompatibility:** Palo Alto and Cisco Firepower are **closed-platform appliances**. They run proprietary operating systems. You cannot (and should not) attempt to install third-party Linux binaries on them; doing so could crash the device or disqualify your team.
2. **Stability:** VyOS is Debian-based, which technically allows for an install, but it is a **critical infrastructure** node. Adding third-party services increases the attack surface and consumes CPU/RAM needed for routing.

The Correct Approach: Syslog & API
Instead of a Forwarder, you must use **Syslog** or **Log Forwarding Profiles**.

- **Palo Alto/Firepower:** Go to the "Log Forwarding" or "Syslog" settings in the Management UI. Point the logs to the IP of your Splunk Server on **UDP Port 514**.
- **VyOS:** Use the native CLI to send logs to Splunk:

Bash
set system syslog host <SPLUNK_SERVER_IP> facility all level info

- **Splunk Side:** On the Oracle 9 server, you must go to **Settings > Data Inputs > UDP** and enable port **514** to receive these network logs.

Summary for Students
Rule of Thumb: If it's a standard OS (Windows/Linux), install the **Forwarder**. If it's a network appliance (Firewall/Router), use **Syslog**.

Gemini Suggestion 04

In a CCDC environment, implementing **IPSec (Internet Protocol Security)** can significantly enhance security, but it comes with a high "complexity tax" that can be dangerous during a live competition. Whether or not it is a "good" move depends on your team's speed and the specific network topology. Here is the expert breakdown of why it helps and why it might hurt.

---

1. How IPSec Enhances CCDC Security

IPSec provides a suite of protocols that ensure **Confidentiality, Integrity, and Authentication** at the IP layer.

- **Encryption of Internal Traffic (Confidentiality):** By default, traffic between your Windows AD server and your Ubuntu workstation might be unencrypted (e.g., LDAP, SMB, or HTTP). If a Red Team member gains a foothold on one box, they will use tools like tcpdump or Wireshark to sniff passwords in transit. IPSec encrypts this "East-West" traffic, making sniffed packets useless.
- **Mutual Authentication:** IPSec can be configured to require a pre-shared key (PSK) or certificate before two machines even talk to each other. This prevents **Man-in-the-Middle (MITM)** attacks and makes it much harder for a Red Team "rogue" device to join the network and start scanning.
- **Secure Remote Management:** Using an IPSec VPN tunnel from the **VyOS router** to the **Palo Alto** ensures that your management traffic is isolated from the competition's "dirty" network.

---

2. The Strategic Reasoning: Pros vs. Cons

The "Pros" (The Security Win)

1. **Defeats Lateral Movement:** Even if the Red Team compromises the **Ubuntu Workstation**, they cannot easily "pivot" to the **Windows AD Server** if those two machines require an IPSec tunnel to communicate.
2. **Anti-Spoofing:** IPSec headers include sequence numbers, which prevent **Replay Attacks** where a Red Team member captures a valid login packet and tries to "replay" it later to gain access.

The "Cons" (The Competition Risk)

1. **Performance Overhead:** Encrypting and decrypting every packet adds CPU load. On older or resource-constrained VMs (like a heavily loaded **Oracle 9** Splunk server), this can cause lag or service failures, losing you points.
2. **Complexity & Service Breaks:** If you misconfigure the IPSec policy on the **Windows Server 2019 AD** box, it may stop responding to DNS queries or Authentication requests. In CCDC, **Availability** is just as important as **Security**. If the service checker can't reach your server, you lose points.
3. **The "Visibility" Conflict:** If you encrypt all internal traffic, your **Cisco Firepower 7** or **Palo Alto** may no longer be able to perform Deep Packet Inspection (DPI) on that traffic because it can't "see" inside the encrypted tunnel.

---

3. Recommended Approach for CCDC

If you decide to use IPSec, do not try to "boil the ocean" by encrypting everything. Use a **Targeted IPSec Strategy**:

- **Priority 1: Management Tunnels.** Use IPSec to connect your VyOS router to any off-site management nodes. This is the standard "VPN to VPN" configuration.
- **Priority 2: High-Value Pairs.** If you have time, create an IPSec transport-mode rule between your **AD/DNS Server** and your **Windows Web Server**. This protects the most sensitive database/authentication traffic.
- **Avoid:** Don't put IPSec on the **Fedora Webmail** or **Ubuntu eCom** servers for public-facing traffic unless the inject specifically requires it. You want the service checkers to have the easiest path possible to verify your services are up.

Technical Summary

IPSec operates in two modes:

1. **Transport Mode:** Encrypts only the payload; used for host-to-host communication.

2. **Tunnel Mode:** Encrypts the entire IP packet; used for gateway-to-gateway (VPN) communication.

Expert Verdict: Use IPSec for **Gateway-to-Gateway** (VyOS to Palo Alto) to secure the backbone. Only use **Host-to-Host** (Windows to Windows) if your team is ahead on injects and has practiced the configuration until it can be done in under 5 minutes.

Gemini Suggestion 05

Adding Wazuh to your CCDC environment can shift your posture from passive logging (Splunk) to active host-based defense (XDR). While Splunk is king for data visualization, Wazuh excels at detecting specific "red team" techniques like file tampering and rootkits.

1. Integration Strategy: The "XDR Powerhouse"

In this environment, you would typically install the **Wazuh Manager** on a dedicated Linux server (or alongside Splunk on the Oracle 9 box, if resources allow) and deploy **Wazuh Agents** to all endpoints.

- **Windows (AD, Web, FTP):** Install the MSI agent. It provides immediate visibility into registry changes and suspicious PowerShell execution.
- **Linux (Ubuntu, Fedora, Oracle):** Use the .deb or .rpm packages. Wazuh will monitor /etc/shadow, /etc/sudoers, and critical web directories for unauthorized changes.
- **Network Appliances (VyOS, Palo Alto, Firepower):** Since you cannot install agents on these, you use **Agentless Monitoring** via SSH or **Syslog** integration to the Wazuh Manager.

---

2. Advantages (The "Why")

Feature	Benefit to CCDC Team
File Integrity Monitoring (FIM)	Alerts you the *second* a Red Team member modifies a config file or adds a web shell.
Active Response	Can be configured to **automatically block an IP** at the OS level (using iptables or Windows Firewall) after X failed login attempts.
Vulnerability Detection	Scans your 9 systems for known CVEs and misconfigurations (like weak SSH settings) during the first 10 minutes.
Rootkit Detection	Periodically scans the kernel and system binaries for hidden malware that standard logging might miss.

---

3. Disadvantages (The "Caution")

- **Resource Intensive:** The Wazuh Manager requires significant RAM and CPU. Running it on the same box as Splunk could cause both to lag, leading to a "visibility blackout."
- **Complexity & False Positives:** Out of the box, Wazuh can be noisy. "Active Response" can accidentally block your own students if they mistype a password too many times, leading to self-inflicted service outages.
- **Installation Time:** Deploying agents and configuring rules takes time away from password rotation and injects. In CCDC, every minute counts.

---

4. Implementation Assignment (Student 6 or 7)

To get Wazuh running quickly alongside your Splunk setup:

1. **Deployment:** Use the "one-liner" installation script on the Linux boxes to save time:

Bash

```
curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh && sudo bash wazuh-install.sh -a
```

2. **Configuration (FIM):** Point Wazuh to monitor your eCom and Webmail directories (e.g., /var/www/html).
3. **Cross-Integration:** Configure Wazuh to forward its alerts to Splunk. This gives you the **threat detection** of Wazuh with the **beautiful dashboards** of Splunk in a single "glass pane."

Coach's Verdict: Only add Wazuh if you have an 8th student who is already comfortable with it. If the team is struggling with basic Splunk forwarders, **skip Wazuh**—the risk of misconfiguration breaking your services is higher than the benefit of the additional alerts.

In your current CCDC topology, the **Oracle 9 Splunk Server** is the most logical choice to host the Wazuh Manager, but it requires a very specific configuration to prevent a "visibility crash."
Here is the strategic breakdown of why this system is ideal and how to manage the risks.

---

1. Why the Oracle 9 (Splunk) Box is the Choice

- **Centralized Data Consolidation:** Since this system is already acting as your "Security Nerve Center" for Splunk, placing Wazuh here allows you to keep your monitoring infrastructure isolated from your "Production" boxes (like the eCom or Webmail servers).
- **OS Stability:** Oracle Linux 9 is a Red Hat Enterprise Linux (RHEL) derivative. Wazuh is natively optimized for the RHEL/CentOS/Oracle family, often showing better stability in high-throughput environments than on Ubuntu.
- **Ease of Integration:** It is significantly easier to pipe Wazuh alerts into Splunk (via a local forwarder or API) if both services are on the same local loopback.

---

2. The "CCDC Danger" (Resource Contention)

The biggest risk in CCDC is **Resource Starvation**. Both Splunk and Wazuh (specifically the Wazuh Indexer/OpenSearch component) are extremely RAM-heavy.

The Reasoning for a "Shared" Box:

In many CCDC competitions, you are limited by the number of virtual machines you are allowed to have. You rarely get a "spare" high-performance VM just for Wazuh. By combining them on the Oracle 9 box, you maximize the utility of your most powerful server.

---

3. Implementation Plan: The "Low-Footprint" Setup

To make this work without crashing the server during an attack, Student 6 must follow these "Survival" settings:

- **Split the Heap:** By default, both Splunk and the Wazuh Indexer will try to claim 50% of the system RAM. You must manually cap the Wazuh Indexer's JVM heap (usually in jvm.options) to **1GB or 2GB** for an environment of only 9 agents.
- **Prioritize the Manager:** If the system starts to lag, disable the **Wazuh Dashboard** (the Web UI) and keep only the **Manager** and **Indexer** running. You can view the alerts in Splunk instead.
- **Agentless for Appliances:** Use the Oracle 9 box to pull syslog from the **VyOS 1.4.3** and **Palo Alto**. This prevents you from having to "hack" an agent onto your critical network path.

---

4. Why not the other systems?

System	Why it fails as a Wazuh Server
Ubuntu eCom / Fedora Webmail	These are "Production" targets. If the Red Team lands a rootkit here, they will immediately kill the Wazuh Manager to hide their tracks.

System	Why it fails as a Wazuh Server
Windows AD Server	The Wazuh Manager is designed for Linux. While a Windows manager technically exists, it is harder to troubleshoot and lacks the robust scripting capabilities of the Linux version.
VyOS / Palo Alto	These are network appliances. Installing a heavy management stack here would likely cause a kernel panic or break your routing table.

Summary for the Team
System: Oracle 9 (Splunk Server)
Primary Goal: Install the Wazuh Manager here, cap the memory usage immediately, and use it as a "Threat Detection Engine" that feeds its findings into your Splunk dashboards for a single, unified view of the battlefield.

Gemini Suggestion 06

To survive a CCDC event where the Red Team is actively deploying rootkits and boot-level persistence, your team must move beyond simple "password changes." You are now in a **Hostile Environment Recovery** mindset.
Below is the weekend practice design and assignment sheet.

Weekend Drill: "Operation Deep Clean"
Duration: 48 Hours (Simulation of Competition Intensity)
Focus: Persistence Removal, Kernel Integrity, and Layered Defense.
Team Roster (8 Students)

Role	Assigned Systems	Student Name
Team Lead / IR	All (Final Sign-off)	
Windows Admin 1	AD/DNS & WS 2019 Web	
Windows Admin 2	WS 2022 FTP & Workstation	
Linux Admin 1	Ubuntu 24 eCom & VyOS	
Linux Admin 2	Fedora 42 & Oracle 9	
Network Architect	Palo Alto 11 & Firepower 7	
Threat Hunter 1	Wazuh/Splunk Implementation	
Threat Hunter 2	Rootkit/Boot Audit Specialist	

Assignment Sheet: Specific Technical Tasks
1. Boot Record & Kernel Integrity (Priority: High)

- **Linux (Admin 1 & 2):** * Verify the integrity of the bootloader. Check /boot/grub/grub.cfg for suspicious init overrides.
    - Check for loaded kernel modules using lsmod. Use modinfo on anything unfamiliar.
    - **Activity:** Practice reinstalling the GRUB bootloader from a live environment to clear MBR/GPT malware.
- **Windows (Admin 1 & 2):** * Run bootrec /fixmbr and bootrec /fixboot concepts in your lab.
    - Check the **Secure Boot** status. Audit the Windows Boot Configuration Data (BCD) using bcdedit /enum.

2. Rootkit Detection (Priority: High)

- **Linux Specialist:** * Deploy and run rkhunter and chkrootkit.

    - **Critical:** Practice the "Known Good Binary" technique. Use debsums -c (Ubuntu) or rpm -V (Fedora/Oracle) to check if system binaries like ls, ps, and netstat have been replaced by the Red Team.
- **Windows Specialist:** * Use **GMER** or **RootkitRevealer** to look for hidden processes and registry keys.
    - Audit the C:\Windows\System32\drivers folder for unsigned or recently modified .sys files.

3. Anti-Malware & Active Scanning (Priority: Medium)

- **Deployment:** * **Linux:** Install and configure **ClamAV** with a fresh freshclam update. Schedule a scan of /var/www and /tmp.
    - **Windows:** Ensure Windows Defender is active and real-time protection is toggled **ON**. Run a full scan immediately.
- **Wazuh (Threat Hunter 1):**
    - Enable **Rootcheck** in the Wazuh ossec.conf.
    - Set up alerts for "File Integrity Monitoring" (FIM) on critical paths like /etc/shadow and C:\Windows\System32\config\SAM.

4. Hardened Firewall Configuration (Priority: Critical)

- **Network Architect:**
    - **Palo Alto 11:** Implement a "Default Deny" rule. Only allow ports 80/443 (Web), 25/587 (Email), and 21 (FTP) to the specific server IPs.
    - **Cisco Firepower:** Enable **Intrusion Prevention (IPS)** profiles. Specifically, look for "Reverse Shell" signatures.
- **Host-Based Firewalls (All Admins):**
    - **Linux:** Configure ufw or firewalld. Block all inbound traffic except management IPs and required services.
    - **Windows:** Use GPO to enforce "Windows Defender Firewall with Advanced Security." Disable all "File and Printer Sharing" unless strictly necessary.

The "Red Team" Simulation Scenario (For Practice)

During this weekend drill, the **Team Lead** should secretly inject one of the following "malware" types every 4 hours for the students to find:

1. **A Cron Job/Scheduled Task:** A simple script that adds a new admin user every 10 minutes.
2. **A Web Shell:** A .php or .asp file in a hidden directory.
3. **A Modified Binary:** Replace /bin/ls with a script that emails a list of files to a "fake" attacker IP before running the real command.

Deliverables for Sunday Review

1. **The "Hardening Log":** A list of all firewall rules applied to each of the 10 systems.
2. **The "Integrity Report":** Proof of debsums or rpm -V passing on all Linux boxes.
3. **The "Detection Proof":** A screenshot from Splunk/Wazuh showing an alert triggered by a test rootkit or unauthorized boot change.

Coach's Note: Rootkits win by being invisible. If your ps command says there are 40 processes, but your Wazuh agent says there are 42, **you have found the Red Team.** Trust your SIEM over your local tools.

Gemini Suggestion 07

CCDC Practice Drill: Secure Infrastructure & Time Management

This 60-minute intensive drill focuses on rapid service hardening, synchronized time-keeping, and network visibility. In a CCDC environment, consistent time is not just a convenience—it is a requirement for log correlation and cryptographic stability (like IPSec and Kerberos).

Team Roster & Roles (8 Students)

Role	Primary Responsibility	Assigned Student
Team Lead	Inject Management, Reporting, IR Coordination	
Linux Admin 1	Slackware/Fedora Hardening, NTP Primary	
Linux Admin 2	Debian/Ubuntu Hardening, Logging	
Windows Admin 1	AD DS, DNS SEC, Group Policy	
Windows Admin 2	Application Hardening, IIS/SQL	
Network Lead	Firewall (Palo Alto), VPN, Traffic Analysis	
Security Analyst 1	Nmap Auditing, PCAP analysis	
Security Analyst 2	SIEM/Wazuh Monitoring, Credential Mgmt	

The Mission: "Operation Atomic Clock"

Time Limit: 60 Minutes

Phase 1: Infrastructure Synchronization (Minutes 0–20)

- **NTP Primary (Linux 1):** Configure the Fedora host as the internal "Stratum 1" source. Restrict access so only the internal subnet can query.
- **Domain Sync (Windows 1):** Ensure the Domain Controller is syncing from the Fedora NTP source. Use w32tm /config /manualpeerlist:"[IP]" /syncfromflags:manual /reliable:yes /update.
- **Network Sync (Network Lead):** Point the Firewall and any managed switches to the internal NTP source.

Phase 2: DNSSEC & Hardening (Minutes 20–45)

- **DNSSEC (Windows 1):** Sign the primary zone on the Windows DNS server. Distribute the "Trust Anchor" to the Linux clients.
- **Service Hardening (All Admins):** Identify and disable non-essential services (RSH, Telnet, FTP). Change default passwords immediately.
- **Visibility (Security 1 & 2):** Deploy Nmap scans to verify open ports. Security Analyst 2 must verify that logs are flowing to the central monitor.

Phase 3: Traffic Analysis & Mapping (Minutes 45–60)

- **Network Mapping:** The Network Lead and Security Analyst 1 must produce a "Flow Map" identifying the Top 5 talkers on the network.
- **Final Validation:** Team Lead verifies that all VMs can ping the NTP source and that DNSSEC validation is successful on at least one Linux and one Windows workstation.

Assignment Deliverables

Each student/pair must submit the following by the end of the 60-minute window:

1. **The "Top Talkers" Report:** A list of the 5 most active IP addresses and the protocols they are using.
2. **The Sync Table:** A spreadsheet showing each host, its current system time, and the "Offset" from the primary NTP server.
3. **The Verification Screenshot:** A screenshot of a successful dig +dnssec or a PowerShell Test-DnsServerDnsSecZoneSetting result.

Technical Reference: NTP & DNSSEC Flow

Implementation Notes

Pro-Tip for Admins: When configuring NTP on the Linux hosts, remember to check /etc/ntp.conf or /etc/chrony.conf depending on the distribution. For the Fedora 42/43 hosts, chronyd is the default. Ensure the firewall on the host (firewalld) allows UDP port 123.

Hardening Checkpoints (Post-Drill Review)

- Did we lose access to any systems due to firewall misconfigurations?
- Did the Windows Domain remain stable after DNSSEC was applied?
- How long did it take to identify the "Top Talkers"? (Target: <10 minutes).

Gemini Suggestion 08

CCDC Practice Drill: Secure Sync & Visibility
Drill Code: Blue Horizon
Duration: 60 Minutes (Hard Stop)
This drill simulates the "Initial 60" of a competition. Your objective is to secure time synchronization, validate DNS integrity, and establish network visibility while navigating restricted GUI access.

Team Roster (8 Students)

Role	Primary Systems	Student Name
Team Lead	Inject Mgmt / Coordination	
Linux Admin 1	Fedora 42 (NTP Primary), Ubuntu Ecom	
Linux Admin 2	Oracle 9 (Splunk/NTP Secondary), Ubuntu WS	
Windows Admin 1	Win 2019 AD/DNS	
Windows Admin 2	Win 2019 Web, Win 2022 FTP	
Network Admin	Palo Alto 11, VyOS 1.4.3	
Firewall Admin	Cisco Firepower 7	
Security Analyst	Traffic Analysis / Top Talkers	

Phase 1: Infrastructure & Hardening (0-30m)

- **Secure NTP:**

    - **Primary:** Configure **Fedora 42** as the authoritative time source for the internal network.
    - **Secondary:** Configure **Oracle 9 (Splunk)** as the secondary time server, syncing from Fedora.
    - **Clients:** All other systems (Windows/Linux/Network) must sync from these two internal sources only. Disable external NTP (pool.ntp.org).
- **DNSSEC:**
    - **Windows AD/DNS:** Enable DNSSEC on the primary lookup zone.
    - **Validation:** Ensure the Ubuntu and Fedora clients are validating signatures.

Phase 2: Visibility & Documentation (30-60m)

- **Network Diagram:** Create a logical map of the 10 systems including IP addresses and primary services.
- **Traffic Audit:** Identify **Top Talkers** (highest bandwidth consumers) and a **Communication Matrix** (who is talking to who/on what port).
- **Service Hardening:** Close high-risk ports (e.g., Telnet, clear-text FTP) once the sync is verified.

The GUI Constraint: Solution Options

With only two GUI-capable clients (Ubuntu Workstation and one Windows server), students must use the following methods to manage the Palo Alto, Splunk, and Firepower web interfaces:

1. **SSH Port Forwarding (Local Tunneling):**
    - Use ssh -L 8443:palo_alto_ip:443 user@ubuntu-ws from a headless Linux box. This allows the student to open localhost:8443 in a local browser if they have a laptop connected to the management net.
2. **SOCKS Proxy:**
    - Establish a SOCKS5 proxy via SSH (ssh -D 8080 user@ubuntu-ws). Configure the browser's proxy settings to route all traffic through the Ubuntu workstation.
3. **Command Line Browsers (Last Resort):**
    - Use lynx or links on headless Linux systems for basic status checks, though this rarely works for complex modern JS-heavy UIs like Splunk.
4. **Windows Jump Box:**
    - Use RDP to the Windows GUI client and use its browser as a central management "Jump Box" for all web-based consoles.

Time Limit Enforcement Options

To simulate competition pressure, use one of the following:

- **The "Scripted Shutdown":** Set a cron job or scheduled task on all systems to shutdown at exactly 60 minutes.
- **The Firewall "Blackout":** Configure the VyOS router to drop all traffic between segments exactly one hour after the start command.
- **The Scoring Engine Simulation:** If deliverables (NTP/DNSSEC validation) are not uploaded to a shared folder by T+60, the team receives a "Service Down" penalty for the remainder of the weekend.

Required Deliverables

1. **Verification Table:** A list of all 10 systems, their current time (to the second), and their NTP peer status.
2. **DNSSEC Proof:** Output of dig +dnssec [domain] from a Linux host and Get-DnsServerDnsSecZoneSetting from Windows.
3. **Traffic Report:** A CSV or table listing: Source IP | Destination IP | Port | Byte Count.

CCDC Hardening & Competition Strategy
Competition Window: 60 Minutes (Hard Stop)
This drill emphasizes the "Blue Team" priority: **Harden without Breaking.** In CCDC, if a service goes down because you over-hardened it, you lose points just as surely as if you were hacked.

Team Assignments (Weekend Intensive)
The following students are assigned to the 60-minute intensive drill. Roles are cross-functional to ensure coverage if a system is compromised.

Student Name	Primary Role	Secondary Role	Focus Systems
Team Lead	Inject Manager	Reporter	All / Coordination
Admin A	Linux Lead	NTP/Splunk	Fedora 42, Oracle 9, VyOS
Admin B	Linux Support	App Security	Ubuntu Server (Ecom), Ubuntu WS
Admin C	Windows Lead	AD/DNSSEC	Win 2019 AD/DNS, Win 2022 FTP
Admin D	Windows Support	Web Security	Win 2019 Web, Win 2022 FTP
Net Specialist	Firewall Lead	Traffic Analysis	Palo Alto 11, Firepower 7
Security Analyst 1	Auditor	Incident Resp	Nmap, SIEM (Splunk) Logs
Security Analyst 2	Credential Mgr	Documentation	Password Policy, Diagramming

---

Master Hardening Checklist: Secure & Functional
The goal is to implement these within the first 45 minutes, leaving 15 minutes for validation and reporting.

1. Linux Systems (Ubuntu 24, Fedora 42, Oracle 9)
- **Initial Triage:** Change all default passwords (system and service accounts).
- **SSH Hardening:** Edit /etc/ssh/sshd_config. Disable PermitRootLogin, set MaxAuthTries 3, and enforce Protocol 2.
- **Kernel Tweaks:** Enable ASLR and DEP via /proc/sys/kernel/randomize_va_space.
- **Service Minimization:** Run systemctl list-unit-files --state=enabled and disable anything not required for the specific system role (e.g., disable CUPS/Printing on a Webmail server).
- **Logging:** Point all rsyslog or journald logs to the Oracle 9 Splunk server.

2. Windows Systems (Server 2019/2022)
- **GPO Implementation:** Enforce a strong Password Policy (12+ chars, complexity) and Account Lockout Policy (5 tries/30 mins).
- **DNSSEC:** Use the DNS Manager to sign the zone. Ensure the Fedora client can resolve via the AD DNS.
- **Remove Bloat:** Use Server Manager to remove "SMB 1.0" and any unnecessary roles.
- **WinRM Security:** If remote management is needed, enforce HTTPS for WinRM; otherwise, disable it.

3. Network & Security Appliances (Palo Alto, Cisco, VyOS)
- **Management Plane:** Restrict management access (HTTPS/SSH) to specific internal IP addresses only.
- **Explicit Deny:** Ensure the final rule on all firewalls is "Deny All" (Egress and Ingress).
- **NTP Sync:** Point all appliances to the Fedora 42 Primary NTP server.
- **Palo Alto BPA:** Run the Best Practice Assessment (BPA) tool if available to identify low-hanging fruit.

Time Limit Enforcement
To maintain the 60-minute pressure, choose one of the following "Live" enforcements:

1. **The Blackout:** At T+60, the coach disables the Virtual Network switch, simulating a total network failure if documentation isn't submitted.
2. **The Red Team Trigger:** At T+61, a scripted "Red Team" attack (automated scripts) is launched against any system that hasn't reported its hardening status.

Trusted References for Students
Students should keep these tabs open for quick syntax checks:

- **CIS Benchmarks:** The industry standard for system-specific configuration. CISecurity.org
- **NIST SP 800-123:** Guide to General Server Security. NIST Computer Security Resource Center
- **Palo Alto Best Practices:** Specifically for PAN-OS 11. Palo Alto Documentation
- **Cisco Firepower Hardening:** Secure Firewall Threat Defense Guide. Cisco.com Hardening
- **Splunk Hardening:** Securing the Splunk platform and data. Splunk Docs