Team 01

Iowa State University

White Team Documentation

C3 2025 Cyber Defense Competition

December 6, 2025

Documentation Methodology

We utilized Notion as our central documentation and task management platform throughout the competition. This allowed us to categorize all vulnerabilities discovered, track remediation progress, and document all changes made to systems in real-time. Each team member could access and update the shared workspace, ensuring comprehensive documentation of our security operations.
The Notion workspace was organized into the following sections:

- Vulnerability Tracking: Each discovered vulnerability was logged with system name, severity, description, and remediation status
- Task Assignment: Security tasks were assigned to specific team members with priority levels and deadlines
- Change Log: All system modifications were documented with timestamps, affected systems, and configuration details
- Network Diagrams: Visual representations of network architecture and firewall rules
- Credentials Vault: Secure storage of updated passwords and access credentials

This systematic approach ensured that very few vulnerabilities went unaddressed, if any, and that all team members had visibility into the overall security posture of our infrastructure.

Public Services

We have configured the following services to be publicly accessible for IScorE scoring:

Domain Name	IP Address	Ports / Services
ad.team01.isucdc.com	64.39.3.10	389 (LDAP), 3389 (RDP)
jd.team01.isucdc.com	64.39.3.20	3389 (RDP)
ltv.team01.isucdc.com	64.39.3.30	22 (SSH)
news.team01.isucdc.com	64.39.3.40	22 (SSH), 8080 (HTTP API)
wstn.team01.isucdc.com	64.39.3.50	22 (SSH), 1883 (MQTT)
www.team01.isucdc.com	64.39.3.60	22 (SSH), 80 (HTTP)

Network Architecture

We implemented a defense-in-depth network architecture using three isolated network segments controlled by an OPNsense firewall. Due to competition infrastructure limitations, we utilized separate Proxmox bridges instead of VLAN tagging to achieve Layer 2 network isolation.

Network Segmentation Strategy

Our network design segregates systems based on trust level and function:

- **MGMT Network (10.10.10.0/24): Critical infrastructure including Active Directory, management systems, and security monitoring**
- **INTERNAL Network (10.10.20.0/22): Production workstations and public-facing web services**
- **UNTRUSTED Network (10.10.40.0/24): IoT devices and systems with physical access vulnerability**

This architecture enforces security boundaries through OPNsense firewall rules that control all inter-segment traffic. Layer 2 isolation is achieved using separate Proxmox bridges, which prevents systems on different bridges from communicating without routing through the firewall.

MGMT Network Rules

The MGMT network (Proxmox bridge team010) contains our most critical infrastructure. We configured the following firewall policy:

- MGMT systems have full outbound access for management operations and software updates
- All other networks can access MGMT systems only on port 389 for LDAP authentication
- IT Administrators can RDP to the Active Directory server from authorized systems
- All connections are logged for security monitoring and incident response

We placed the Active Directory server (10.10.10.10) in this segment because it is the authentication backbone for all systems. Compromise of AD would allow Red Team to pivot to all domain-joined machines, so we isolated it behind strict firewall rules.

INTERNAL Network Rules

The INTERNAL network (Proxmox bridge team011, subnet 10.10.20.0/22) hosts production services and employee workstations. We configured the following firewall policy:

- Journalist Desktop can access web servers for article management
- Web servers can query the News API for weather data
- All systems have DNS access (port 53) and internet access via proxy (199.100.16.100:3128)
- INTERNAL systems cannot initiate connections to MGMT network
- INTERNAL systems cannot initiate connections to UNTRUSTED network

This design prevents lateral movement if a public-facing service is compromised. An attacker gaining access to the web server would be blocked from reaching the Active Directory server or other critical management infrastructure.

UNTRUSTED Network Rules

The UNTRUSTED network (Proxmox bridge team012) contains the Lobby TV and Weather Station. This is our most restrictive segment because Red Team has physical access to the Lobby TV via vCenter console. We configured the following critical firewall policy:

- **UNTRUSTED to MGMT: COMPLETELY BLOCKED except:**
  - Both systems to AD (port 389) for LDAP authentication only
- **UNTRUSTED to INTERNAL: COMPLETELY BLOCKED except:**
  - Weather Station to News API (port 8080) for weather data push
  - Lobby TV to News API (port 8080) for broadcast stream
  - Both systems to AD (port 389) for LDAP authentication only
- DNS and proxy access allowed for legitimate functionality
- All UNTRUSTED outbound connections to internet are logged for C2 detection

This is our most critical security control. If Red Team compromises the Lobby TV through physical console access, they cannot pivot to our Active Directory server or any management systems. This prevents the most dangerous attack path in our network.

WAN Configuration and External Connectivity

Our WAN interface presented unique challenges due to the competition network design. We received multiple /32 host routes instead of a traditional subnet, which required special configuration:

- **Far Gateway Configuration:** The gateway (64.39.3.254) is not on the same Layer 2 segment as our WAN IPs. We enabled the "Far Gateway" and "Upstream Gateway" options in OPNsense to allow routing to a gateway outside our local subnet.
- **1:1 NAT Mappings:** We configured 1:1 NAT to map external IPs to internal systems, allowing IScorE scoring while maintaining network segmentation.
- **Proxy Configuration:** All internet-bound traffic routes through the competition proxy (199.100.16.100:3128). We configured this at the firewall level and on individual systems.
- **Scorer Access:** We created specific WAN firewall rules allowing the IScorE scoring system (49.10.235.154) to access required ports on each public service while blocking all other unsolicited inbound traffic.

Application Security

We identified and remediated critical vulnerabilities in the news website and weather backend applications. Our security audit revealed multiple high-severity issues that could allow attackers to compromise the entire news station infrastructure.

SQL Injection (Critical - CWE-89)

Location: weather-backend/backend.go, POST /weather endpoint

Problem: The weather data ingestion endpoint was constructing SQL queries using string formatting with unsanitized user input. This vulnerability would allow attackers to inject arbitrary SQL commands, potentially extracting sensitive data, modifying weather records, or executing administrative database operations.

Fix Applied: We replaced all string-formatted queries with parameterized SQL statements using placeholders. The database driver now properly escapes all user input, preventing SQL injection attacks.

Verification: We tested with malicious payloads including single quotes, SQL keywords, and comment characters. The parameterized queries properly escaped all input and prevented any unauthorized database operations.

API Key Exposure (High - CWE-200)

Location: news-website/nuxt.config.ts and app/pages/weather.vue

Problem: The API key flag was exposed in the public runtime configuration, making it accessible to anyone visiting the website through browser developer tools or by inspecting the JavaScript bundle. This key protects access to weather data endpoints and should never be client-accessible.

Fix Applied: We restructured the application to move the API key to private server-side configuration. We created a new server-side API route at /server/api/weather.ts that handles authentication with the backend. Client-side code now makes requests to our own API route instead of directly to the backend with the API key.

Verification: We inspected browser console, network requests, and the compiled JavaScript bundle to confirm the API key is no longer exposed. The weather page continues to function correctly while the sensitive credential remains server-side only.

Broken Access Control (High - CWE-862)

Location: weather-backend/backend.go, POST /weather endpoint

Problem: The weather data upload endpoint did not require any authentication. This would allow unauthorized users to inject arbitrary weather data into the database, corrupting forecasts displayed on the website and potentially manipulating broadcast content on the Lobby TV.

Fix Applied: We implemented API key validation on the POST handler. The endpoint now checks for a valid x-api-key-flag header and rejects requests without proper authentication with a 401 Unauthorized response.

Verification: We tested POST requests without an API key, with an invalid API key, and with a valid API key. Only properly authenticated requests are accepted. The weather station service can still push data successfully with the correct API key.

Hardcoded Credentials (High - CWE-798)

Location: Multiple files including weather-backend/backend.go and news-website/server/db.ts

Problem: Database credentials and API keys were hardcoded directly in source code. This creates multiple security risks including credential exposure in version control history, inability to rotate credentials without code changes, and potential exposure through code repositories or backups.

Fix Applied: We refactored both applications to read all credentials from environment variables. We created systemd service override files at /etc/systemd/system/weather-backend.service.d/override.conf and /etc/systemd/system/news-website.service.d/override.conf that securely store credentials using the Environment directive.

Verification: We removed all hardcoded credentials from source code, confirmed services start correctly with environment variables, tested database connectivity from both applications, and verified API authentication still works correctly.

Threat Hunting Activities

We conducted systematic threat hunting across all systems to identify and remove Red Team persistence mechanisms. Our approach involved checking multiple layers where attackers commonly establish backdoors.

Windows Systems (AD, JD)

Scheduled Tasks

We enumerated all scheduled tasks and identified several suspicious entries with random names, hidden attributes, and execution of PowerShell scripts from temporary directories. We removed these tasks using the Unregister-ScheduledTask cmdlet and continue to monitor for new suspicious scheduled tasks.

WMI Event Subscriptions

We checked WMI event subscriptions which can be used for persistence. We queried the root\Subscription namespace for __EventFilter, __EventConsumer, and __FilterToConsumerBinding objects to identify malicious subscriptions. We removed suspicious WMI persistence mechanisms and implemented regular checks.

Malicious Services

We audited all Windows services for suspicious entries. We looked for services with unusual names, services running from unusual directories, and services with random or obfuscated executables. We stopped and deleted identified malicious services.

Backdoor User Accounts on AD

Critical Finding: We discovered a backdoor account 'taco' that had been created with administrator privileges. We attempted to remove this account and encountered issues with the 'Administrators' group name not being found in PowerShell, indicating possible Active Directory corruption or tampering. We continued troubleshooting and successfully removed unauthorized accounts.

Linux Systems

Malicious Cron Jobs

Finding on LTV: We found a malicious root cron job executing a hidden script .super_secret.sh that creates a backdoor user 'richard' with a blank password. We removed this cron job and the associated script.

Additional Systems: Many other Linux systems had similar scripts designed to exfiltrate /etc/shadow contents or create backdoor accounts. We systematically removed these cron jobs across all affected systems.

Malicious Systemd Services

Finding on WWW: We discovered a suspicious apt process (PID 168308) holding locks on the package manager. Investigation with lsof revealed this was actually an installation of 'chkrootkit', which appeared to be a persistence mechanism disguised as a security tool. We terminated this process.

Finding on NEWS - copier.service: We found a malicious systemd service 'copier.service' that copies /etc/shadow to /tmp and sets world-readable permissions (777). This would allow any user to read password hashes. We disabled and removed this service.

Finding on NEWS - network-broadcast.service: We discovered a service that broadcasts /etc/shadow contents over the network using netcat to broadcast address 255.255.255.255 on port 1337. This would leak all password hashes to anyone on the network. We disabled and removed this service.

LD_PRELOAD Backdoors

Finding on WSTN: The weather-station.service had a malicious LD_PRELOAD environment variable set to /usr/lib/libssl.so.1.1. This forces the service to load a malicious library that can hijack code execution. We removed this environment variable from the service configuration.

PAM Configuration Vulnerabilities

Critical Finding on WWW and WSTN: The PAM configuration in /etc/pam.d/common-auth was set to allow null passwords using the 'nullok_secure' option. This would allow any account with a blank password to authenticate via SSH or local console. We removed this dangerous configuration from both systems.

System Hardening

Beyond removing Red Team persistence mechanisms, we implemented defensive hardening measures across all systems.

Windows Systems

Critical Windows Update Issue on AD

Finding: We discovered that Windows Update service was completely disabled on the Active Directory server (error code 0x80070422). This means the system is not receiving critical security patches.

Impact: Windows Server 2019 base installations are highly vulnerable to exploits like EternalBlue (MS17-010), BlueKeep (CVE-2019-0708), SMBGhost (CVE-2020-0796), Zerologon (CVE-2020-1472), and PrintNightmare (CVE-2021-34527). Without security updates, these vulnerabilities remain exploitable.

Remediation: We re-enabled the Windows Update service and initiated installation of critical security patches. This is ongoing due to the large number of missing updates.

Firewall Configuration

We enabled Windows Firewall on all profiles (Domain, Private, Public) and configured rules to block unnecessary inbound ports while allowing only required services such as RDP and LDAP.

Linux Systems

SSH Configuration Hardening

Applied to All Linux Systems: We hardened SSH configuration across all Linux systems (WWW, NEWS, WSTN, LTV, generalUbuntu). The original configuration had password authentication enabled, empty passwords allowed, and TCP forwarding permitted without restrictions.

Remediation: We reconfigured /etc/ssh/sshd_config on all systems to disable password authentication and empty passwords, enable public key authentication, disable TCP forwarding, and restrict TTY access. We maintained these changes while ensuring legitimate administrative access remains functional.

Missing Security Updates Repository

Critical Finding on Most Linux Systems: On the majority of our Debian/Ubuntu systems, the security updates repository was commented out in /etc/apt/sources.list. This means the systems were not receiving security patches for known vulnerabilities.

Remediation: We uncommented the security repository lines and ran apt update && apt upgrade to install all available security patches. This addresses known vulnerabilities that Red Team could exploit.

MD5 Hash Usage on NEWS

Finding: The NEWS system was using MD5 for password hashing, which is cryptographically broken and vulnerable to rainbow table attacks and rapid brute-forcing.

Remediation: We reconfigured the system to use SHA-512 for password hashing, which provides significantly stronger protection against password cracking attempts.

Package Manager Configuration

We configured apt to use the competition proxy for package downloads and ensured all systems can properly update packages through the proxy. We also verified that package repositories are using HTTPS where possible.

Current System Status

All required services are operational and accessible to IScorE. The following table summarizes the current status of each system:

System	Status	Services	Notes
AD (10.10.10.10)	Operational	LDAP (389), RDP (3389)	Security patches being installed
JD (10.10.20.10)	Operational	RDP (3389)	Proxy configured for internet access
LTV (10.10.40.20)	Operational	SSH (22), Broadcast display	Isolated from MGMT network
NEWS (10.10.21.x)	Operational	SSH (22), API (8080)	Security fixes applied, backdoors removed
WSTN (10.10.40.10)	Operational	SSH (22), MQTT (1883)	Weather data flowing correctly
WWW (10.10.21.x)	Operational	SSH (22), HTTP (80)	Security fixes applied, website functional
OPNsense	Operational	Firewall, NAT, routing	Far Gateway configured, all rules active

Challenges and Resolutions

During the setup and hardening phase, we encountered several technical challenges that required creative solutions.

OPNsense Gateway Configuration

Challenge: The gateway (64.39.3.254) was not on the same Layer 2 segment as our WAN interface IP addresses. All WAN IPs were configured as /32 host routes, and attempting to add a default route resulted in "Network is unreachable" errors.

Root Cause: Standard gateway configuration requires the gateway to be on the local subnet. The OPNsense WAN interface had multiple /32 host routes but the gateway was not reachable at Layer 2.

Solution: We discovered the "Far Gateway" option in OPNsense that allows routing to a gateway outside the local network segment. We enabled both "Far Gateway" and "Upstream Gateway" options, then manually added the default route using the command line. This allowed OPNsense to successfully route traffic through the competition gateway.

Proxy Configuration

Challenge: All systems needed to use the competition proxy (199.100.16.100:3128) for internet access, but Windows systems did not have this configured by default, Linux package managers needed specific proxy settings, and applications required individual configuration.

Solutions:

- Windows: Configured proxy in Settings → Network → Proxy
- Linux: Added proxy configuration to /etc/environment and apt configuration files
- Applications: Configured proxy settings individually for each service as needed

Network Connectivity Issues

Challenge: Systems could not communicate across network segments even though firewall rules appeared correct.

Root Cause: VMs were assigned to incorrect Proxmox bridges. For example, we initially had the Journalist Desktop (JD) on team010 (MGMT) instead of team011 (INTERNAL).

Solution: We verified each VM's bridge assignment in Proxmox UI under VM → Hardware → Network Device. We corrected any misassignments and verified connectivity after changes.

IScorE Service Timeouts

Challenge: Services were showing as down or timed out in IScorE even though they appeared to be running.

Root Causes:

- WAN firewall rules were not allowing the scorer IP (49.10.235.154)
- NAT port forward rules were incomplete or incorrect
- Services were not actually running despite appearing to be up

Solutions: We added specific WAN rules allowing the scorer IP to access required ports on each service. We verified all NAT port forwards were correctly configured. We checked actual service status using systemctl and confirmed services were listening on the correct ports. We learned to wait 2-3 minutes after configuration changes before assuming they had failed.

Ongoing Security Measures

We continue to maintain and improve our security posture through ongoing monitoring and hardening activities.

Continuous Monitoring

- Regular review of OPNsense firewall logs for blocked connection attempts and suspicious patterns
- Monitoring systemd service status across all Linux systems
- Checking Windows scheduled tasks and WMI subscriptions for new persistence mechanisms
- Reviewing Active Directory user accounts and group memberships
- Monitoring UNTRUSTED network traffic for command and control activity

High Priority Items

- Complete Windows vulnerability patching (EternalBlue, BlueKeep, SMBGhost, Zerologon, PrintNightmare)
- Implement ChaCha20 encryption for weather balloon data transmission
- Configure SecOnion for full network monitoring and intrusion detection
- Implement replay attack protection for weather data using timestamps or nonces
- Configure centralized logging for all systems
- Implement rate limiting on weather API endpoint

User Access Management

All systems are joined to the Active Directory domain (ad.team01.isucdc.com) for centralized user management. We have configured user access according to the scenario requirements:

- **IT Administrators:** Full administrative access to all systems via SSH/RDP
- **HR Staff:** RDP access to Active Directory for user management
- **Meteorologists:** SSH access to Weather Station to modify weather programs
- **Journalists:** RDP access to Journalist Desktop to manage articles

Conclusion

We have successfully implemented a defense-in-depth security architecture for CDC Channel 4 News. Our three-tier network segmentation strategy isolates critical infrastructure from compromised systems, particularly protecting the Active Directory server from the UNTRUSTED network where Red Team has physical access.

We identified and remediated four high-severity application vulnerabilities including SQL injection, API key exposure, broken access control, and hardcoded credentials. We conducted comprehensive threat hunting that uncovered numerous Red Team persistence mechanisms, including malicious scheduled tasks, WMI subscriptions, systemd services, cron jobs, backdoor user accounts, and LD_PRELOAD hijacking.

We hardened both Windows and Linux systems by addressing critical configuration weaknesses, including disabled security updates, weak SSH configurations, null password authentication, and weak password hashing. We configured OPNsense firewall rules that enforce strict network segmentation while maintaining required service availability for IScorE scoring.

All required services are operational and accessible to competition scoring. We continue to monitor for new Red Team activity and maintain our security posture through ongoing threat hunting and system hardening activities.