..

As-Is Process Analysis of UNF Cyber Competition Team Preparation and Competition Execution

1. Research Phase

This paper documents the current (“as-is”) preparation and competition processes used by UNF cyber competition teams. The purpose of this phase is to establish a baseline of current methods, identify first-impression gaps, and lay a foundation for later comparison with higher-performing schools and the development of a future student-run training curriculum.

The survey used for this phase was titled **UNF Cyber Competition Performance Study Questionnaire**. Eighteen people consented to having their responses used in this study. Four people did not pass the survey's screening portion. Because some respondents skipped questions, percentages vary slightly by item depending on the number of people who answered each question.

This first as-is analysis uses survey responses as the primary data source and includes both quantitative (multiple-choice) and qualitative (long-form) responses. Additional responses will be collected after the qualifiers to improve sample coverage and validate patterns identified in this first pass.

---

2. Document Phase

This section documents the team's current-state process for preparing for and conducting competitions. Following the as-is process analysis practice, the process is described chronologically (preparation process first, then competition execution process), followed by key process inputs and outputs.

2.1 Current As-Is Preparation Process (Before Competition)

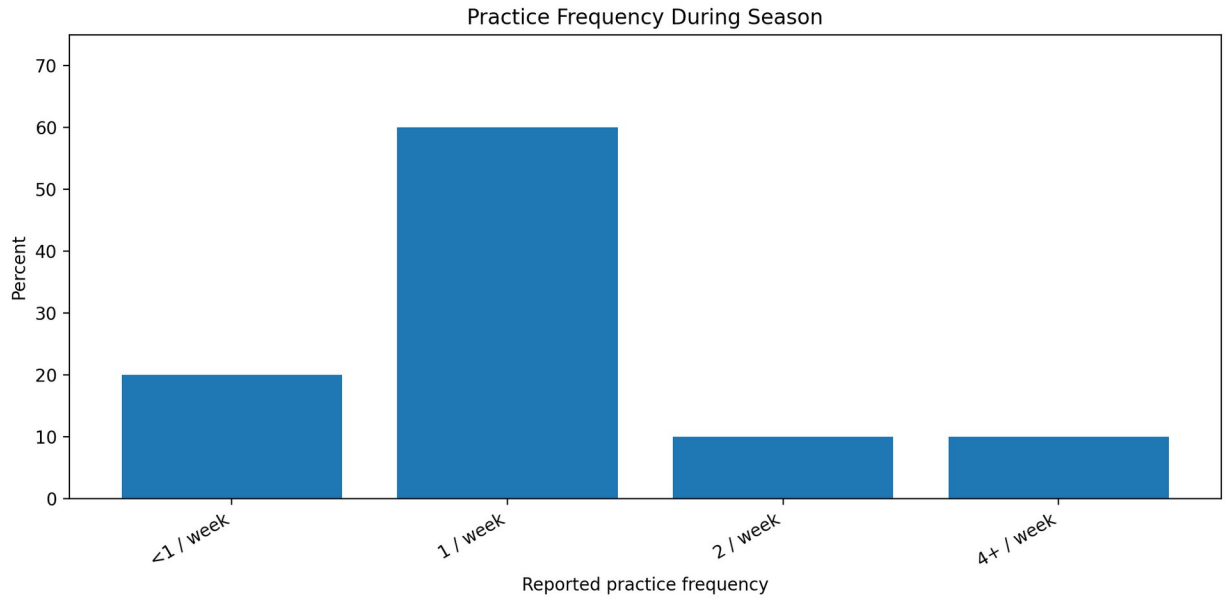
Based on survey responses, the current preparation process is centered on limited weekly practices, usually short and focused on technical labs rather than full competition simulation.

Practice Frequency

..

Respondents described the current preparation process as relying on limited weekly practices during the season:

- **60%** reported **one structured practice per week**
- **20%** reported **less than one practice per week**
- **10%** reported **two practices per week**
- **10%** reported **four or more practices per week**



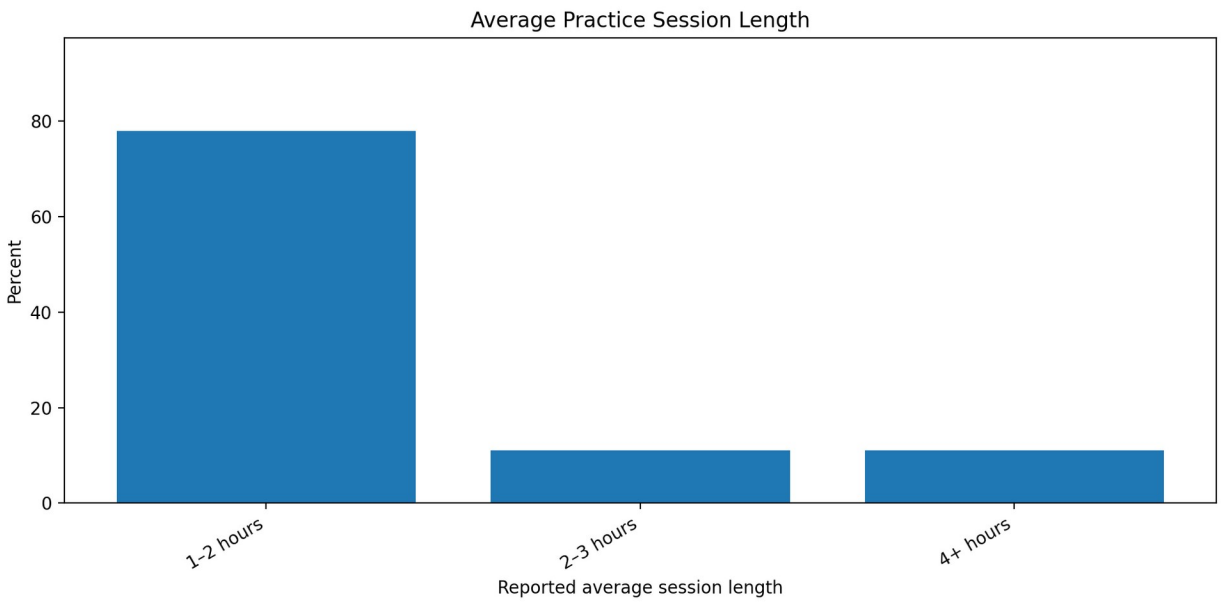
This indicates that the dominant preparation pattern is one weekly team-run practice session.

Practice Length

For average practice length:

- **78%** reported **one to two hours**
- **11%** reported **two to three hours**
- **11%** reported **more than four hours**

..



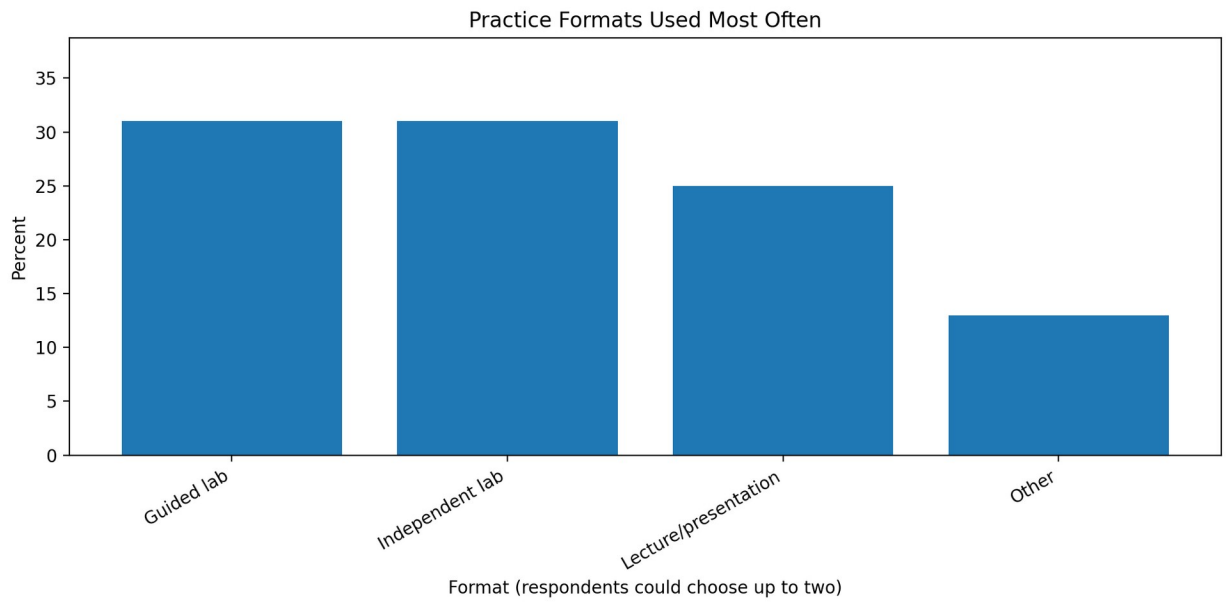
This suggests the standard team practice is short and may not provide enough time for realistic scenario work, role coordination, and debriefing in the same session.

Practice Format

Respondents were asked which practice formats were used most often (with the ability to select one or two). The most common responses were:

- **Guided lab (31%)**
- **Independent lab (31%)**
- **Lecture/presentation (25%)**
- **Other (13%)** (not specified)

..



Notably:

- **0%** selected **mock competition**
- **0%** selected **tabletop exercises** (injects, communications, reporting)

This indicates that the current preparation process emphasizes technical exposure but does not commonly include competition-like role execution, injection handling, or reporting workflow practices.

Mock Competition Frequency

Respondents were separately asked how often full mock competitions were conducted:

- **56%** said **never**
- **44%** said **once per season**

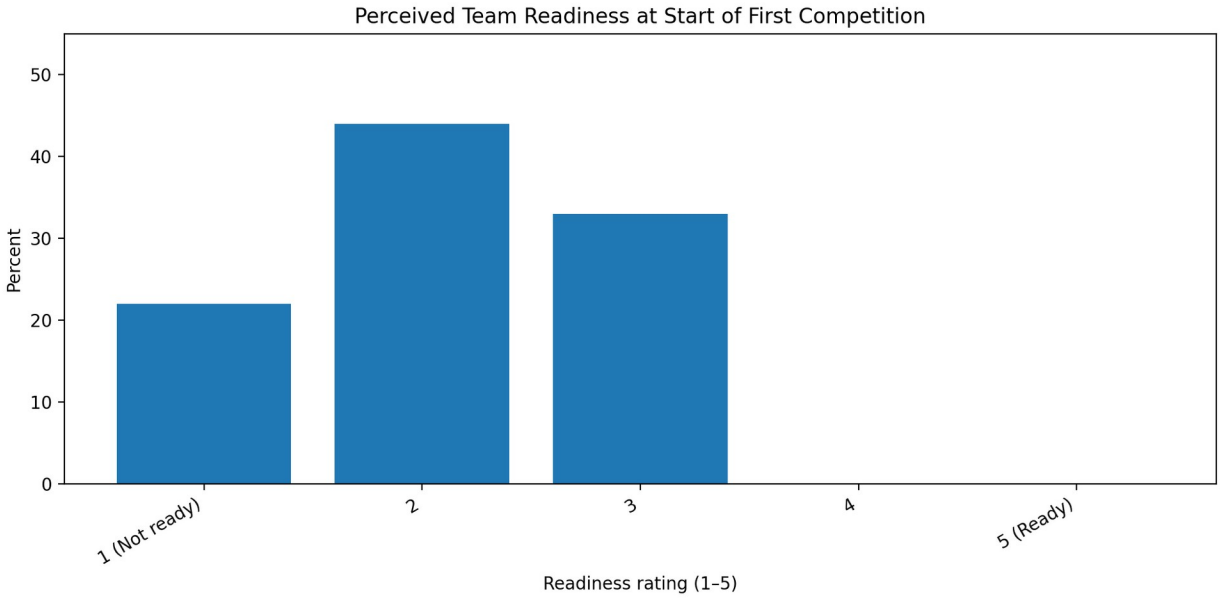
No respondents reported repeated or routine mock competitions.

Team Readiness at Start of Competition

Respondents rated readiness at the beginning of the first competition on a scale from 1 (“not ready”) to 5 (“ready”):

..

- **0%** selected **5**
- **0%** selected **4**
- **33%** selected **3**
- **44%** selected **2**
- **22%** selected **1**



These results indicate that participants generally perceived the team as underprepared entering the competition season.

Perceived Undertrained Areas

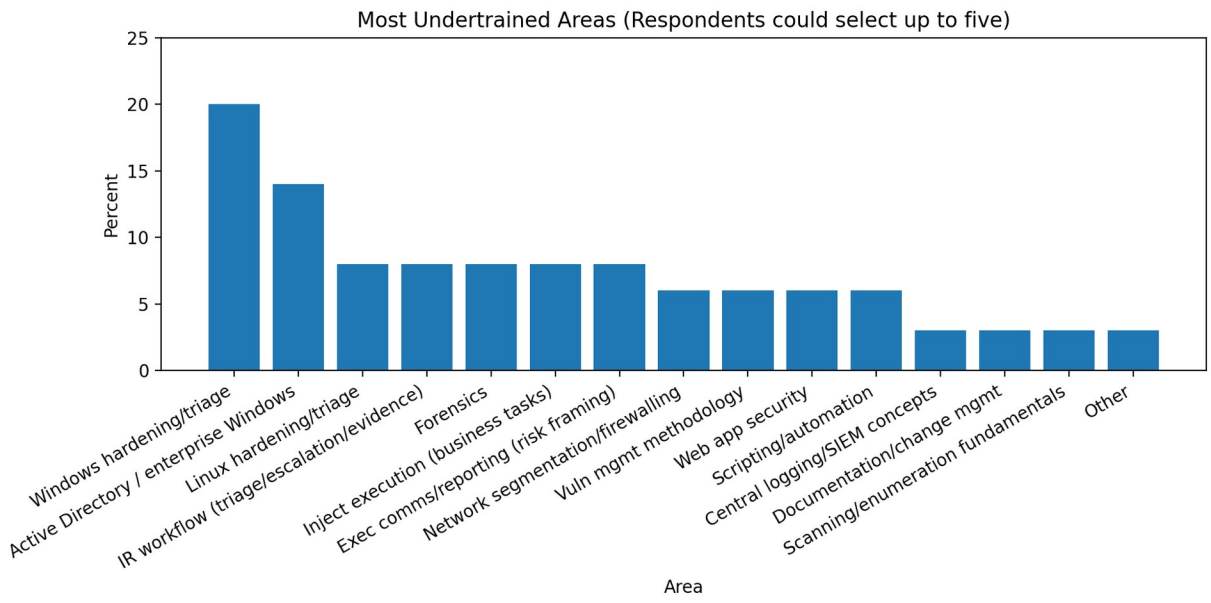
Respondents could select up to five undertrained areas. The most frequently selected were:

- **Windows hardening and triage (20%)**
- **Active Directory or enterprise Windows (14%)**
- **Linux hardening and triage (8%)**

..

- **Incident response workflow (triage, escalation, evidence) (8%)**
- **Forensics (8%)**
- **Inject execution (business tasks) (8%)**
- **Executive communication and reporting (risk framing) (8%)**
- **Network segmentation or firewalling (6%)**
- **Vulnerability management methodology (6%)**
- **Web application security (6%)**
- **Scripting or automation (PowerShell, Bash, Python) (6%)**
- **Central logging or SIEM concepts (3%)**
- **Documentation and change management (3%)**
- **Scanning and enumeration fundamentals (3%)**
- **Other (3%)**

..



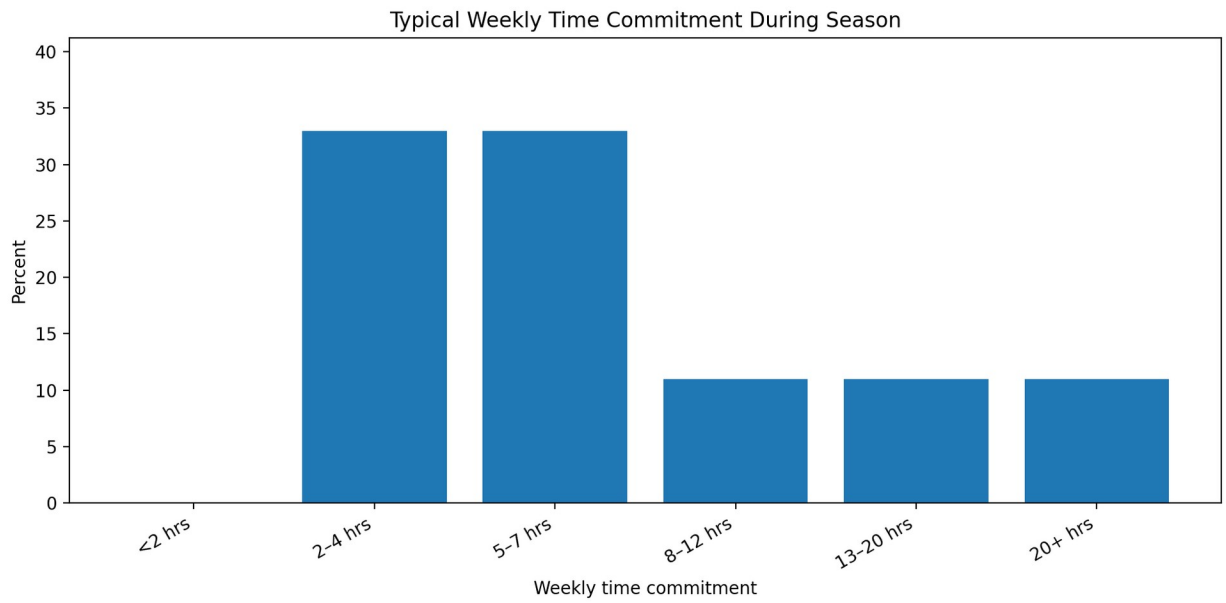
The strongest concentration is in **Windows/Active Directory and enterprise defense workflow**, which are core areas in many defensive competitions.

Typical Time Commitment (In-Season and Off-Season)

During the season, respondents reported the following weekly time commitment:

- **0%** less than 2 hours
- **33%** two to four hours
- **33%** five to seven hours
- **11%** eight to twelve hours
- **11%** thirteen to twenty hours
- **11%** more than twenty hours

..

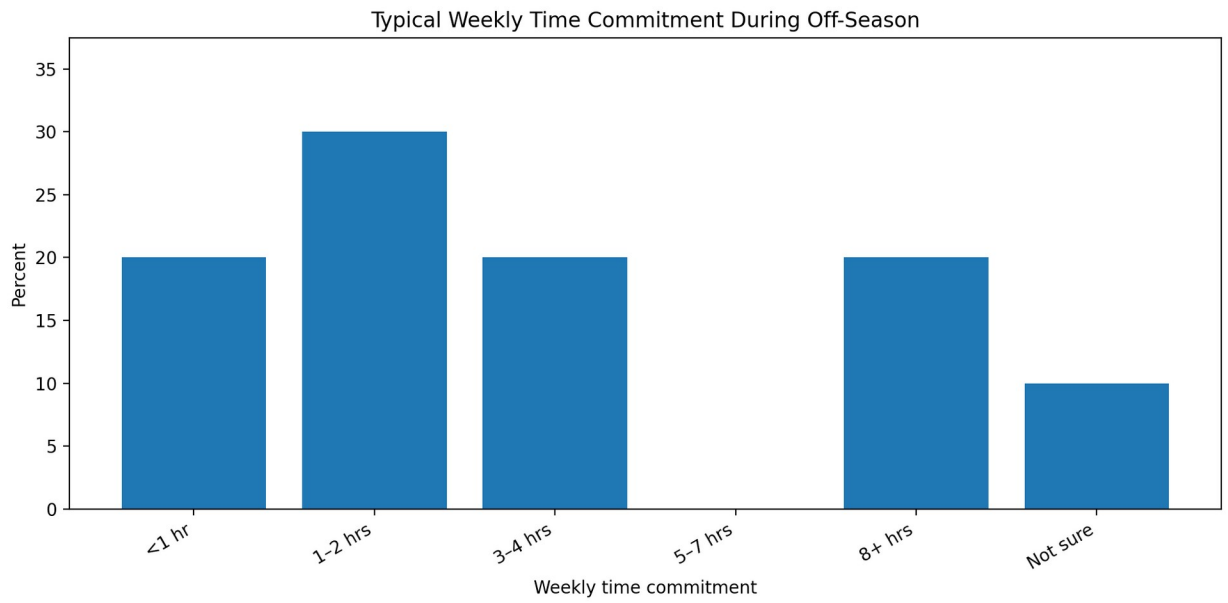


This suggests a split between a smaller, highly committed group and a larger group contributing moderate time.

During the off-season, time commitment dropped:

- **20%** less than one hour
- **30%** one to two hours
- **20%** three to four hours
- **0%** five to seven hours
- **20%** eight or more hours
- **10%** not sure

..



This indicates reduced continuity outside the competition season.

2.2 Current As-Is Competition Execution Process (During Competition)

Survey responses also described how the team typically functions during competitions, including where breakdowns occur and how work is prioritized.

What Fails First

Respondents most frequently identified early failures in:

- **Basic service availability**
- **Tool familiarity under time pressure**
- **Team communication**
- **Role clarity and handoffs**
- **Inject completion**
- **Change tracking/documentation.**

..

- **Detecting compromise while services still appear online**

This suggests that competition breakdowns are often operational and coordination-related, rather than solely technical knowledge problems.

Workflow Performance During Competition

Respondents rated the team's performance in key workflow categories (triage, change tracking, detection, response/recovery, inject execution responses) clustered mostly around weak to mixed performance, with limited strong ratings.

The weakest process areas were:

- **Response and recovery**
- **Change tracking and avoiding self-inflicted outages.**
- **Triage and prioritization consistency**

Inject execution was rated somewhat better than some technical workflow categories, but respondents also reported that injects often suffer when technical issues escalate.

Self-Inflicted Outages and Change Management

Respondents indicated that self-inflicted outages or major setbacks due to team changes occurred, with the most common answer being **"a few times."** This supports the conclusion that change control and change tracking are not consistently applied during competition.

Logging and Monitoring

Most respondents described logging/monitoring during competition as:

- **No central logging, mostly manual checks**, or
- **Basic logging, but not centralized**

A smaller group indicated central logging existed but was not used effectively. This suggests limited process maturity in the detection and monitoring workflow.

Inject and Reporting Performance

..

Respondents identified the most common inject/report blocker as:

- **The team is too busy with technical fires**

This indicates that injection and reporting issues are often downstream effects of unstable technical operations and weak workflow prioritization, rather than a lack of awareness of inject's importance.

Team Readiness Depth

Respondents most commonly estimated that only **one to two people** were truly competition-ready **4 to 8 weeks before competition**, indicating that readiness is concentrated in a small core rather than distributed across the team.

Practice Reliability and Leadership Impact

Respondents reported that practices sometimes fail to happen or become unproductive due to attendance or leadership issues. This indicates that process reliability is affected by team governance and consistency, not only training content.

2.3 Text-Based As-Is Process Map (Current State)

The following text-based process map summarizes the as-is process documented from the survey responses.

Preparation Phase (As-Is)

Inputs: student time, current team members, available practice sessions, existing lab access
Process:

1. Schedule team practice (usually once per week)
2. Conduct a short session (typically guided lab, independent lab, or lecture)
3. Limited or no tabletop workflow practice (injects/reporting/communications)
4. Rare or no full mock competition simulation
5. Individual practice outside sessions varies significantly by member.

..

6. The team enters the competition with mixed readiness.

Outputs: partial technical preparation, weak workflow practice, small competition-ready core

Competition Phase (As-Is)

Inputs: competition roster, assigned systems/roles, competition environment
Process:

1. Initial hardening and service checks
2. Reactive response to outages and urgent issues
3. Triage and changes are handled inconsistently.
4. Monitoring relies on manual checks or weak logging integration.
5. Technical incidents consume time.
6. Inject/report tasks are delayed or deprioritized.
7. Team performance depends heavily on a small number of ready members.

Outputs: service instability, workflow inconsistency, reduced inject/report quality, uneven team performance

In the next section: To-be: What are the ***new*** processes and procedures our team should be using to be successful? How do we translate our weaknesses into strengths? Back this up with a detailed gap analysis between where we are and what we need to be doing.