Competencies in Action: Evidencing Competencies within the NCAE Cyber Games

Jake Mihevc and James Rice
Mohawk Valley Community College
NCAE Cyber Games

Pilot framework ideas:

1)Leverage Evidencing Competencies Work Group ABCDE model

2)Reference/align with workforce frameworks such as DCWF and NICE FW

3)Consider alignment with CAE KU Outcomes

4)Work towards competencies “in a contested environment”

5)Address proficiency levels

6)Provide a clear summary of what the participant did to earn badge

Operationalizing Data with Scripting

Operationalizing Data with Scripting Competency Statement: Predicts Actor's competence at leveraging scripts to operationalize data in a contested environment.		
ABCDE	Description	Notes
Actor/Audience	Entry Level CS/Cyber college student	
Behavior	Derived from DCWF Task 6470: Read, interpret, write, modify, and execute simple scripts (e.g. PERL, VBS) on Windows and UNIX systems (e.g, those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	
Context	Services Inject: Once Database comes online and inject is released, 2 hours to script a solution to the problem leveraging the newly available data in a contested environment. Username and password data (hashes) added to a database requires verification by scripted means. Offensive team empowered to attack the integrity of the data, to which the script should filter valid data versus corrupted/compromised data. AND Hacker Troll House: Big Troll level - 10 minutes to automate task in bash/python while adversarial scripts work as disruptions and deterrence.	
Degree	(Team) Contribute to the completion of a scripting-focused Service Inject in the context of the description. AND (Individual) Complete one scripting focused Hacker Troll House level within 10 minutes.	
Employability	Provides a solution that is viable and adheres to industry best practices where applicable.	

CAE IN CYBERSECURITY COMMUNITY

NCAE CYBER GAMES

PLAY | LEARN | PROTECT

Operationalizing Data with Scripting

Database Inject

The cyber security and quality assurance teams have teamed up to try and eliminate weak passwords from our user database. They have tasked you with figuring out who has a password in the user database from the provided password_list.txt list. User data will be posted into your teams MySQL server; utilize the following instructions to start receiving data:

1. SSH into your database server VM
2. Connect to the mySQL database service with the command: `mysql -u root`
3. Run the following mySQL commands:

```
CREATE DATABASE IF NOT EXISTS inject_password_dump;
CREATE USER 'qa_team'@'%' IDENTIFIED BY 'myQAPassw0rdInj3ct';
GRANT ALL PRIVILEGES ON inject_password_dump.* TO 'qa_team'@'%';
USE inject_password_dump;
CREATE TABLE IF NOT EXISTS users (username VARCHAR(255), password_hash TINYTEXT, UNIQUE(username));
```

User passwords are hashed with the SHA1 algorithm when posted to the database. You must figure out a way to associate these values with the provided passwords. We follow a standard username convention: ${LAST_NAME}${FIRST_INITIAL} (Example: John Doe would be doej). The provided names will need to be converted to following the standard username convention. It appears we have had some erroneous data making its way into our systems. Ensure all submitted users are present in the user_names.txt file. Failure to validate this data may slow down remediation efforts.

Files:

- user_names.txt
- password_list.txt

Submit your findings to https://inject.ncaecybergames.org/ and ensure you are following the provided example below:

```
{
  "username": {
    "firstname": "first",
    "lastname": "last",
    "password": "password"
  },
  "doej": { // This should be your generated value from the name provided
    "firstname": "John",
    "lastname": "Doe",
    "password": "12345" // This should be the password you discovered
  }
```

Cyber Defense Analyst

Cyber Defense Analyst (PR-CDA-001) Competency Statement: Predicts Actor's competence at monitoring and analyzing system activity in a contested environment.		
ABCDE	Description	Notes
Actor/Audience	Entry Level CS/Cyber college student	
Behavior	Derived from NICE: Task T0259: Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity. Task T0258: Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities. Task T0023: Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources. Task 0291: Examine network topologies to understand data flows through the network. T0290: Determine tactics, techniques, and procedures (TTPs) for intrusion sets. T0155: Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	
Context	During the Competition: Services Inject: Unexpectedly the web server goes down due to a targeted attack. The team must leverage the SIEM and NDR tools to identify the malicious activity that is the root cause. The team must understand how traffic flows into their environment using their topology map (T0291)in order to investigate the attack via their SIEM and NDR tools (T0259). As the webserver will be live throughout the competition, the students must determine which events (network or log) are benign (ex. scoring engine) and which are malicious (T0023,T0258). Once the team has declared an incident, they must complete an incident response report (we provide a template) to document their findings and associated impact (T0155). This report must include TTPs mapped to the MITRE framework (T0290).	
Degree	Team must successfully identify and explain the malicious activity to the 'CISO' (staff member who will evaluate work against industry standards). This includes review of the incident report and discussion around how the incident impacts the 'business'. time allowed/expected for completion: 2 hours	
Employability	This is a common series of tasks for an analyst type role in the industry. Exposure to this type of thinking and problem solving is directly comparable to real world tasks.	

Cyber Defense Analyst

433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
472	Coordinate with enterprise-wide cyber defense staff to validate network alerts.
723	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.
745	Perform cyber defense trend analysis and reporting.
750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.
767	Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy.
800	Provide daily summary reports of network events and activity relevant to cyber defense practices.
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
956	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.
958	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.
959	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
1107	Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR).
1108	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).
1111	Identify applications and operating systems of a network device based on network traffic.
427	Develop content for cyber defense tools.
559B	Analyze and report system security posture trends.
559A	Analyze and report organizational security posture trends.
576	Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.
593A	Assess adequate access controls based on principles of least privilege and need-to-know.
716A	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
717A	Assess and monitor cybersecurity related to system implementation and testing practices.
782	Plan and recommend modifications or adjustments based on exercise results or system environment.
806A	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
880A	Work with stakeholders to resolve computer security incidents and vulnerability compliance.
938A	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.
1103	Determine tactics, techniques, and procedures (TTPs) for intrusion sets.
1104	Examine network topologies to understand data flows through the network.
1105	Recommend computing environment vulnerability corrections.
1109	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
1110	Isolate and remove malware.
1111	Identify applications and operating systems of a network device based on network traffic.
1112	Reconstruct a malicious attack or activity based off network traffic.
1113	Identify network mapping and operating system (OS) fingerprinting activities.
2062	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the NE or enclave.
2611	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.

CAE IN CYBERSECURITY COMMUNITY

NCAE CYBERGAMES

PLAY | LEARN | PROTECT

Directly embedded

1) Consistent with existing competition framework

2) Optional but incentivized for participants/teams

3) Light/moderate student engagement

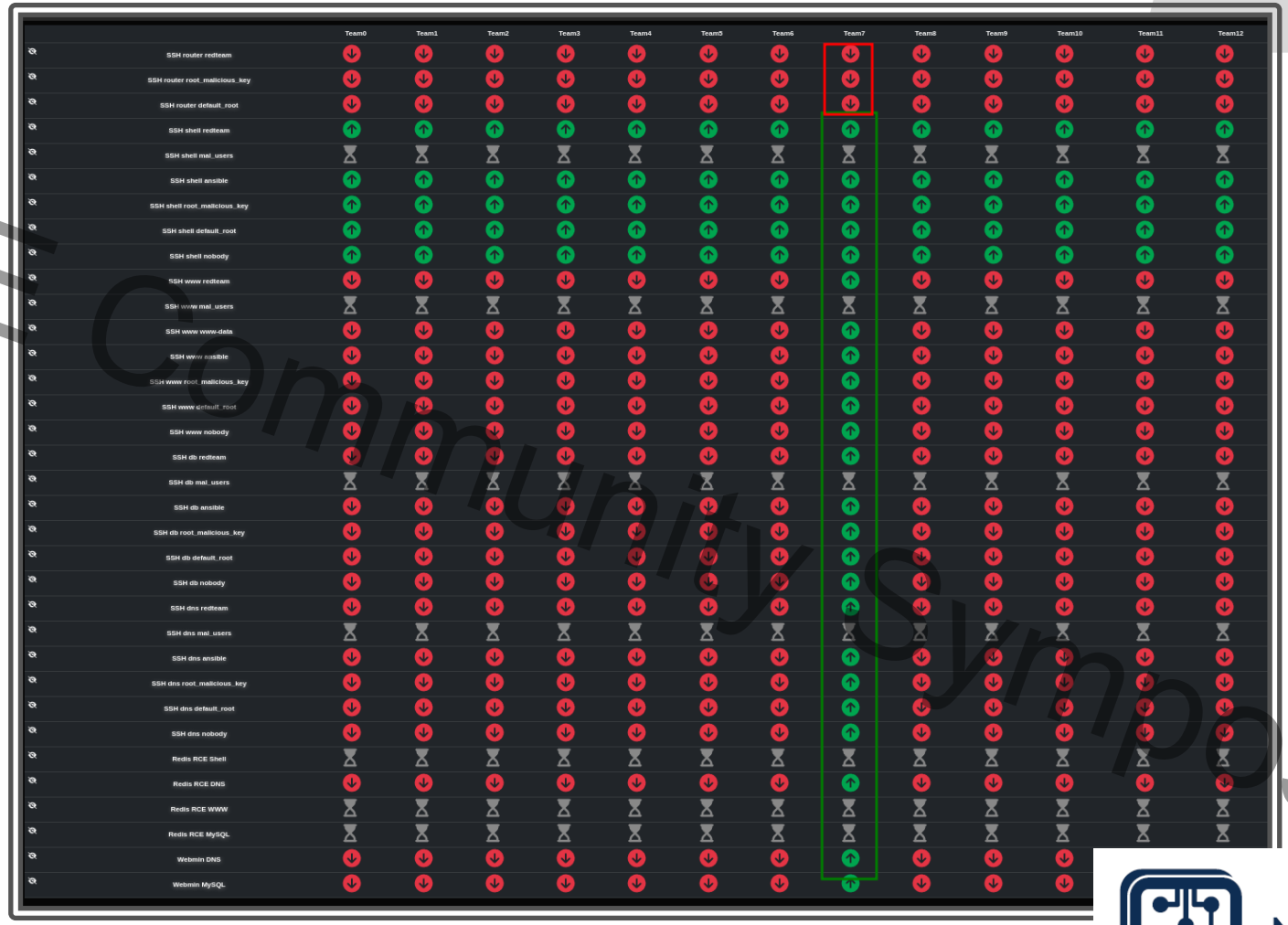
4) Scales well, manual attribution

5) Scripting: One task, one challenge

6) CDA: Five tasks, five flags.

7) Does an asynchronous singular experience evidence competency?

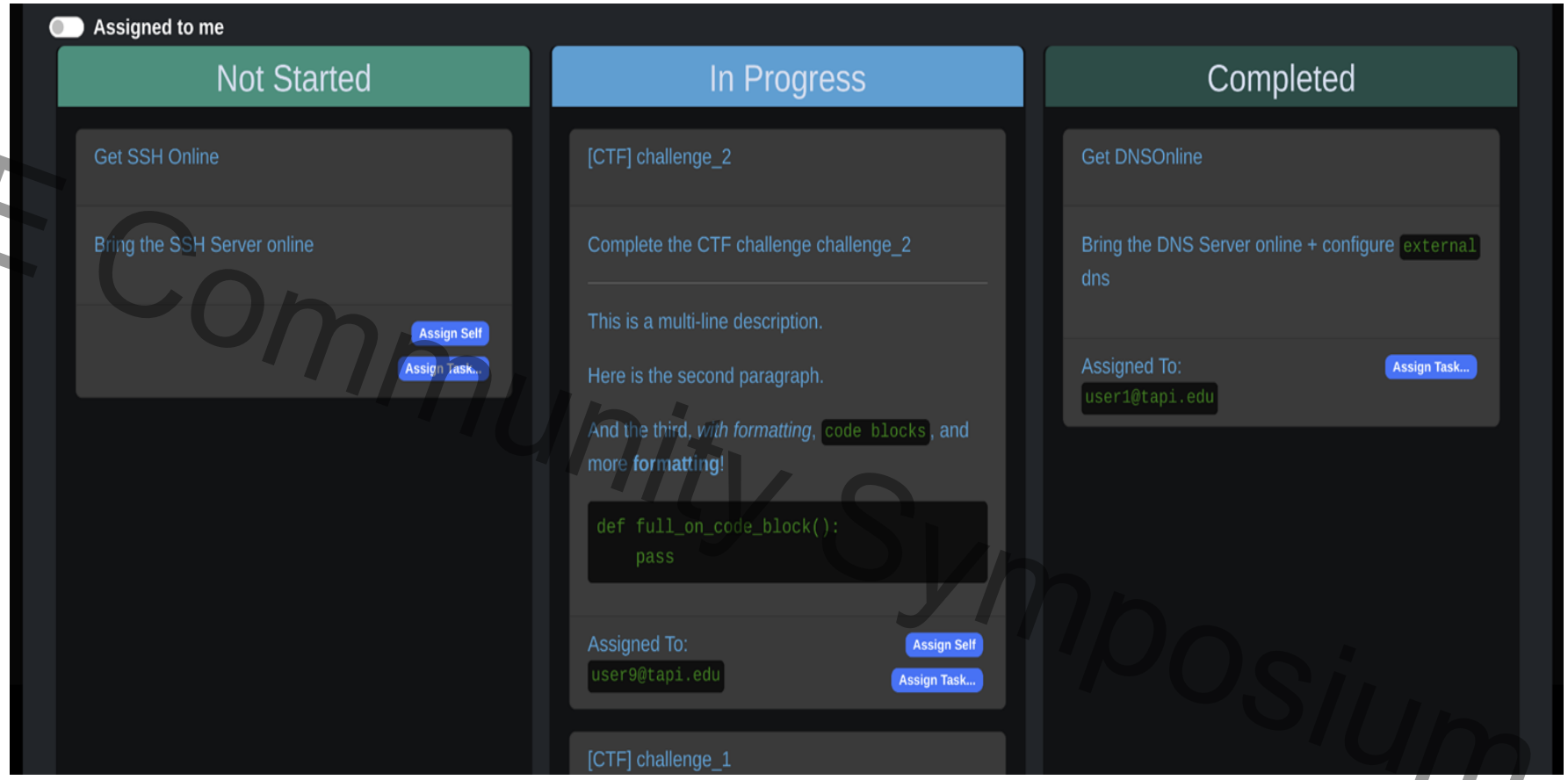
Positioning:
Red Team
Dashboard



CAE IN CYBERSECURITY COMMUNITY

NCAE CYBERGAMES
PLAY | LEARN | PROTECT

Positioning:
Kanban Prototyping tasking and assignment

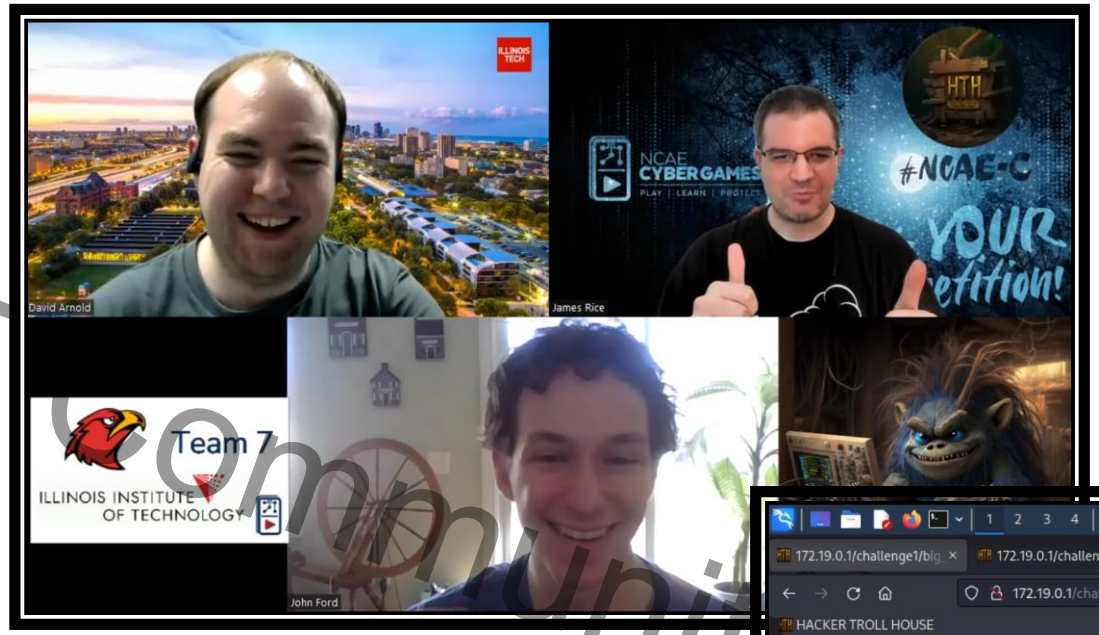


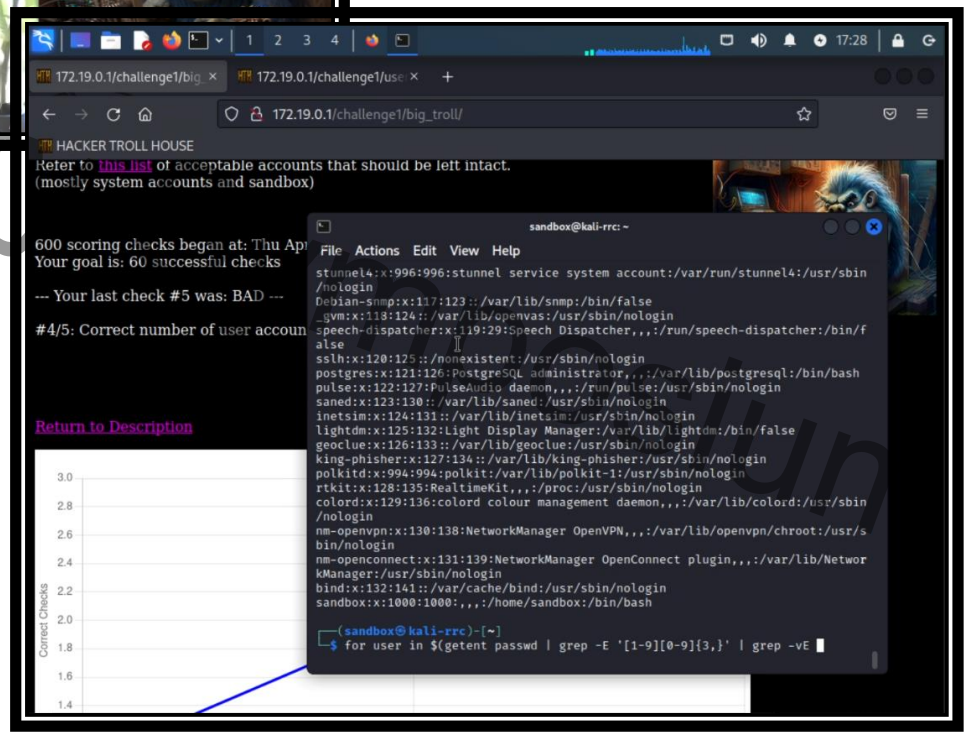
CAE IN CYBERSECURITY COMMUNITY

NCAE CYBERGAMES
PLAY | LEARN | PROTECT

Hacker Troll House

2023-2024 NCAE Cyber Games





Format: 2 students from each team selected for our in-person Invitational event.

Complete a series of fun challenges in a cyber gameshow style experience.

Hacker Troll House

1) Adjacent to existing competition framework

2) Optional but incentivized for participants/teams

3) Strong student engagement

4) Does not scale, direct attribution

5) Timed, sequential, can capture video

6) Designer set competency bar based on sampling industry professional performance.

Questions?

NCAE CYBER GAMES
PLAY | LEARN | PROTECT