



Player's Quick Start Guide

Last Updated
January 3, 2025

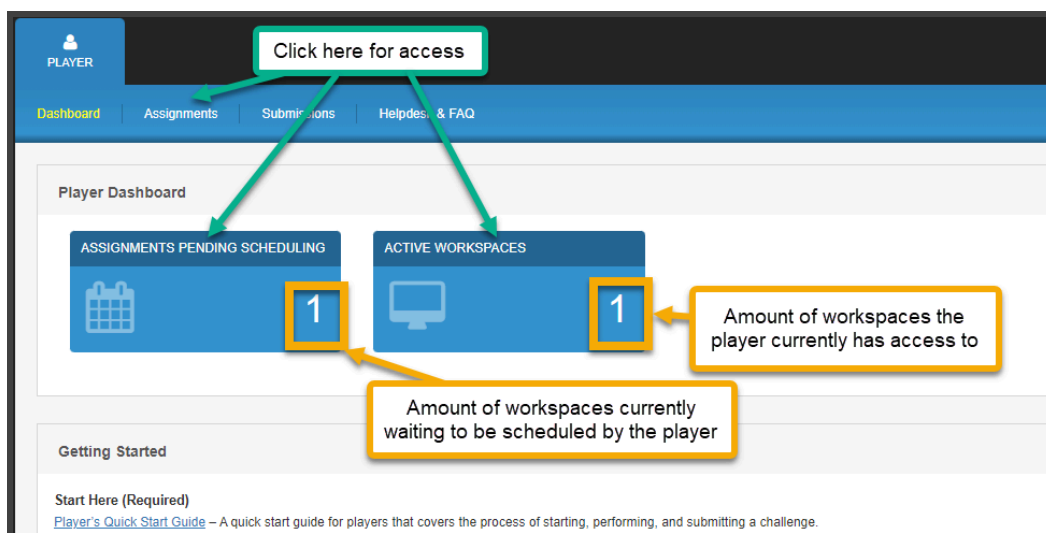
Table of Contents

1. [Scheduling & Accessing Workspaces Using the XP Cyber Range or NICE Challenge Webportal](#)
2. [Starting a Challenge](#)
3. [Performing a Challenge](#)
4. [Submitting a Challenge](#)
5. [Viewing Challenge Submissions](#)
6. [Challenge Tips & Top FAQs](#)
7. [Console Support & Availability](#)

Scheduling & Accessing Workspaces¹ Using the XP Cyber Range or NICE Challenge Webportal

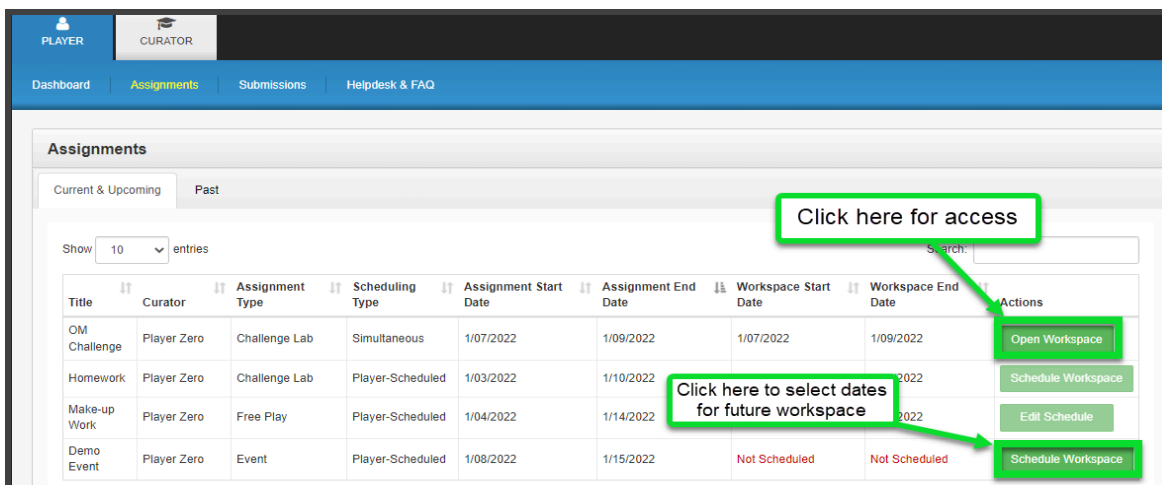
Workspaces Overview

Players must be added to an assignment² by a curator before they can gain access to a workspace and begin attempting challenges. The curator determines what challenges may be attempted, as well as how long players will have access to a workspace. Below are screenshots showing how to identify if a player has available workspaces or any workspaces pending scheduling.



Accessing an Active Workspace

Workspaces become available to players at approximately 3:00 AM (Pacific Time) on their designated start date. Once a workspace is available, players will see a button labeled "Open Workspace", which they can click on to continue with challenge selection and deployment. Workspaces expire at 11:59 PM (Pacific Time) on their designated end date, at which point any challenge attempts in progress will be submitted automatically.



¹ **Workspace** - A live environment assigned to a user for the purpose of attempting challenges.

² **Assignment** - A time window, defined by a Curator, in which a set of users may schedule workspaces or have workspaces scheduled for them for the purpose of performing challenges.

Scheduling a Workspace

Players³ must be added to a Player-Scheduled Assignment before they may schedule a workspace for themselves. If a player has an assignment that is pending workspace scheduling, the words "Not Scheduled" will appear in red under the assignments "Workspace Start Date" and "Workspace End Date" columns. Selecting the "Schedule Workspace" button will navigate them to the Workspace Scheduling page.

During assignment creation, curators⁴ specify a date range for players to schedule workspaces for themselves. This is the *Assignment Phase*. On the Workspace Scheduling page, players are prompted to select a date range within the Assignment Phase during which they would like to gain access to a workspace.

Workspace Scheduling: CSE 200 Week 1 - Player One

Schedule a Workspace

You are scheduling a workspace (i.e., where assignment challenges can be attempted) for the following:

Assignment Phase: 01/08/2022 - 01/15/2022

Player: [Redacted]

This assignment allows for scheduling one workspace for one day during the assignment phase.

Schedule Early!
The earlier you schedule a workspace, the more likely you will get the days you prefer. Once scheduled, you may update or cancel a workspace anytime before the day (in Pacific Time) the workspace is scheduled to start.

Next-Day Workspaces
You must schedule workspaces at least the day before you want them to start, even if that means on July 14th at 11:58 PM PT you schedule a workspace for July 15th.

Start Date* **End Date***

January 2022

Su	Mo	Tu	We	Th	Fr	Sa
						8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

Submit

Assignment Phase

³ **Player** - A user which performs challenges; often a student.

⁴ **Curator** - A user which adds players, creates assignments, and reviews challenge attempts; often a professor.

Starting a Challenge⁵ Using the XP Cyber Range or NICE Challenge Webportal

Selecting a Challenge

Once inside an active workspace, players are presented with a sortable list of available challenges with two available action buttons. The “View” button displays expanded challenge information and the “Deploy” button will deploy that challenge onto the current workspace.

The screenshot shows the NICE Challenge Webportal interface. At the top, there's a navigation bar with 'Dashboard', 'Assignments', 'Submissions', and 'Helpdesk & FAQ'. Below this, the page title is 'CSE 200 | Player Zero' with a timer '0 46h 41m Left'. A search bar and a 'Show 10 entries' dropdown are present. The main table lists challenges with columns: Type, Work Role, Challenge Title, Difficulty, Time, OS, and Actions. The first row is highlighted, showing a 'Technical' challenge for a 'Cyber Defense Analyst' role, titled 'Networking Anomalies: The Packet Capture Edition [NG]' with a difficulty of 3 stars and a time of 1 hour. Below the table, there are tabs for 'Challenge Details', 'Network Map', and 'NICE Framework & CAE KU Mapping'. The 'Challenge Details' tab is active, showing the challenge title, author, framework category, specialty area, work role, task description, scenario, additional information, and login credentials (Username: playerone, Password: password123). At the bottom, there's another table listing more challenges, including 'Preventative Protection: Thwarting the Imminent Threat [NG]' and 'Preventative Protection: Thwarting the Imminent Threat [NG] (Complexity 1)'.

Type	Work Role	Challenge Title	Difficulty	Time	OS	Actions
Technical	Cyber Defense Analyst	Networking Anomalies: The Packet Capture Edition [NG]	★★★	1h	Linux	Deploy Hide

Challenge Details

Networking Anomalies: The Packet Capture Edition

Author: Alexander Hillock & Daniel Killam & Luis Pena
Framework Category: Protect and Defend
Specialty Area: Cybersecurity Defense Analysis
Work Role: Cyber Defense Analyst
Task Description: Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
Scenario
Our security analyst has been busy with other work recently and is in need of some assistance. She needs help viewing some network traffic logs to identify if any weird activity is going on that could potentially be threats to our network resources. We need you to review a set of logs and identify malicious activity if it exists.
Additional Information
More details and objectives about this challenge will be introduced during the challenge meeting, which will start once you begin deploying the challenge.
You will be able to check your progress during this challenge using the check panel within the workspace once the challenge is deployed. The checks within the check panel report on the state of some or all of the required tasks within the challenge.
Once you have completed the requested tasks, you will need to document the methodology you used with as much detail and professionalism as necessary. This should be done on the documentation tab within the workspace once the challenge is deployed. Below the main documentation section be sure to include a tagged list of applications you used to complete the challenge.
Your username/password to access all virtual machines and services within the workspace will be the following...
Username: playerone
Password: password123
The web form used for this challenge accepts a limited number of entries.

Technical	Cyber Defense Incident Responder	Preventative Protection: Thwarting the Imminent Threat [NG]	★★★	1h	Windows	Deploy View
Technical	Cyber Defense Incident Responder	Preventative Protection: Thwarting the Imminent Threat [NG] (Complexity 1)	★★★	1h	Windows	Deploy View

This list is organized by a variety of useful information including the following...

- **Type** - At this time there are 3 different types of challenges. Technical, which is a challenge where the player generally needs to alter (i.e. install/update software, fix issues, etc) the VMs within the environment⁶ in order to reach a desired end state. Hybrid, which is a challenge where the player observes and analyzes the state of the VMs within the environment and writes a report/policy as the primary deliverable. Threat Sandbox, where the player is educated about a threat and encouraged to experiment with it in the environment.

⁵ **Challenge** - A defined scenario, based on a DoD Cyber Workforce Framework and NICE Framework Task from the perspective of a DoD Cyber Workforce Framework and NICE Framework Work Role. Often includes a business scenario, meeting chat, and checks. Each challenge is designed to work within a specific environment.

⁶ **Environment** - A defined set of VM images, configurations, and extended context. It is designed to create a realistic set of systems, networks, and users which support a fictitious organization with a defined purpose.

- **Work Role** - This field comes directly from the DoD Cyber Workforce Framework and NICE Framework and is what the challenge is mapped to/designed from in terms of content.
- **Challenge Title** - The challenge's name.
- **Difficulty** - The relative difficulty of the challenge.
- **Time** - The relative time it should take to complete the challenge.
- **OS (Operating System)** - The main operating system used to complete the challenge. This does not, however, mean that the challenge is limited to that operating system completely.

Understanding Challenge Details

When reviewing challenges, the top-level (what is displayed in the list) information is only to help players find what they are looking for, in general. More important details can be found below this layer, they become visible once the “View” action is used. The various sections under the “Challenge Details” tab are listed and explained below...

- **Framework Category/DCWF Element, Work Role, & Task Description** - These fields come directly from the DoD Cyber Workforce and NICE Framework and are what the challenge is mapped to/designed from in terms of content.
- **Scenario** - A brief business scenario written to give a realistic take on how this challenge could manifest using real-world context.
- **Additional Information** - Extra information that will aid in the completion of a challenge. Often this section includes important details that are required to complete a challenge properly.

Understating Known Issues

The tab labeled “Known Issues” can be clicked to reveal information about known issues related to the selected challenge. This section will display a detailed description of the issue along with any known workarounds and the potential impact the issue may pose to the challenge submission report.

The screenshot shows the 'CSE 200 Week 1 | John Smith' interface. At the top, there are navigation tabs: Dashboard, Assignments, Submissions, and Helpdesk & FAQ. Below this, the user's name and a timer (8h 11m Left) are displayed. A search bar contains the text 'network operation'. Below the search bar, there is a table of challenges. The table has columns for Type, Work Role, Challenge Title, Difficulty, Time, OS, and Actions. Two challenges are listed: 'Networking Woes: The Monitor We Need' (Hybrid, Network Operations Specialist) and 'Security Begins & Never Ends with Updates' (Technical, Network Operations Specialist). The 'Known Issues' tab is highlighted in green. Below the table, the 'Known Issues' section is expanded, showing details for the 'Networking Woes: The Monitor We Need' challenge. It includes a 'Minor Environmental Impediment' section with a workaround, affected checks, and submission report impact. Another 'Minor Environmental Impediment' section is also visible.

Type	Work Role	Challenge Title	Difficulty	Time	OS	Actions
Hybrid	Network Operations Specialist	Networking Woes: The Monitor We Need	★★☆	⌛⌛⌛	Multiple	Deploy View
Technical	Network Operations Specialist	Security Begins & Never Ends with Updates	★★☆	⌛⌛⌛	Multiple	Deploy Hide

Challenge Details **Known Issues** Network Map NICE Framework & CAE KU Mapping

Minor Environmental Impediment
Rebooting the Prod-Web VM results in the Joomla website becoming inaccessible from other machines on the network.
Workaround:
If the Joomla website becomes inaccessible after rebooting Prod-Web, run the following command as playerone on Prod-Web:
sudo iptables -D INPUT -j REJECT --reject-with icmp-host-prohibited
Affected Checks:
Joomla Updated
Submission Report Impact:
Players that reboot the Prod-Web machine and do not implement the provided workaround will encounter slightly more difficulty while completing the affected checks.

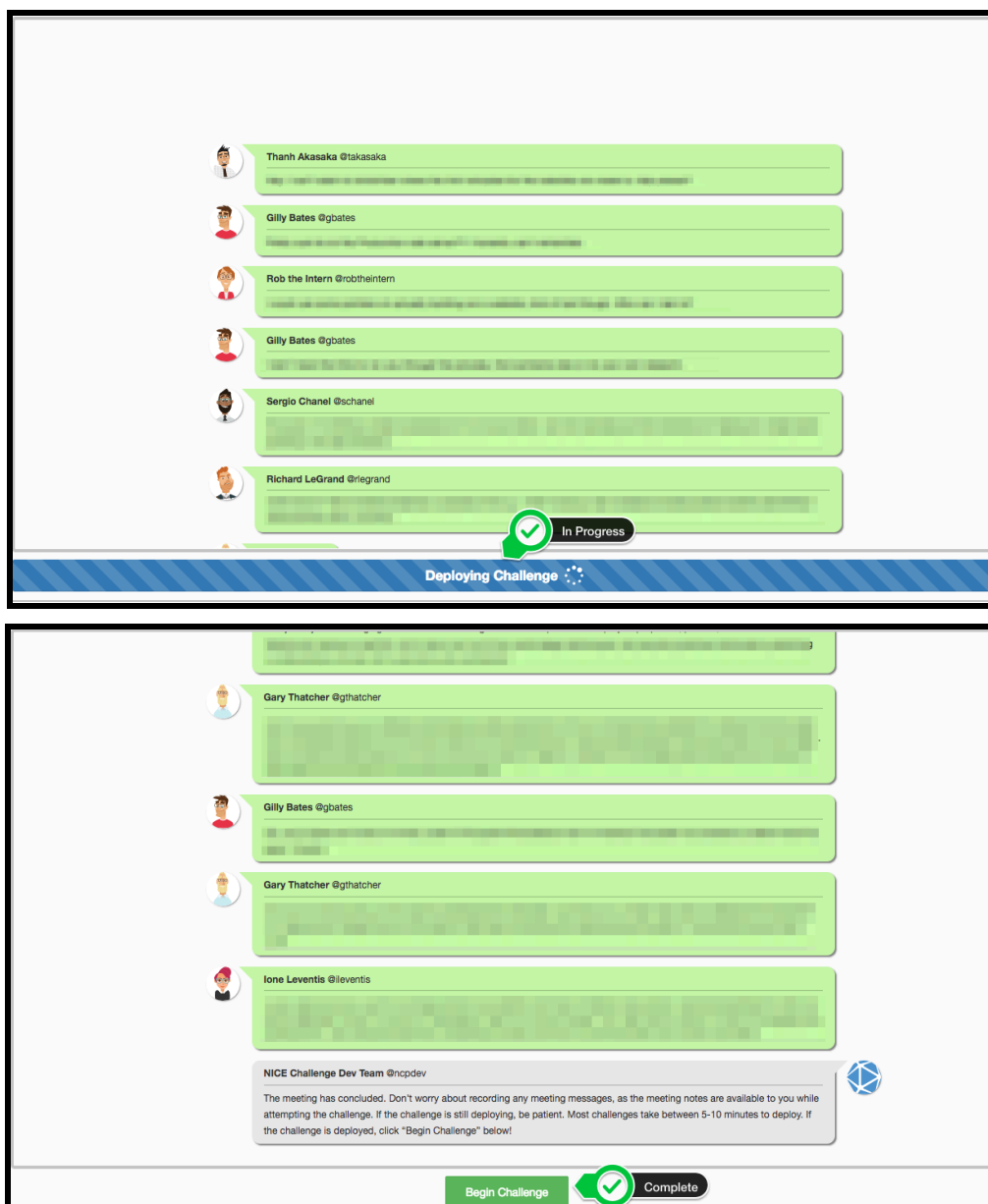
Minor Environmental Impediment
Due to the age of certain systems within the environment, achieving a desirable (green) state for the affected check is more difficult than originally intended.
Workaround:
Players must update Joomla by setting the update channel to the following URL:

Challenge Deployment

Challenge deployment, on average, takes between 5-10 minutes once the deployment request leaves the queue. However, some challenges take longer to deploy than others. In the cases that the challenge will take longer than 10 minutes to deploy the average deployment time is listed in the “Additional Information” section of the “Challenge Details” tab.

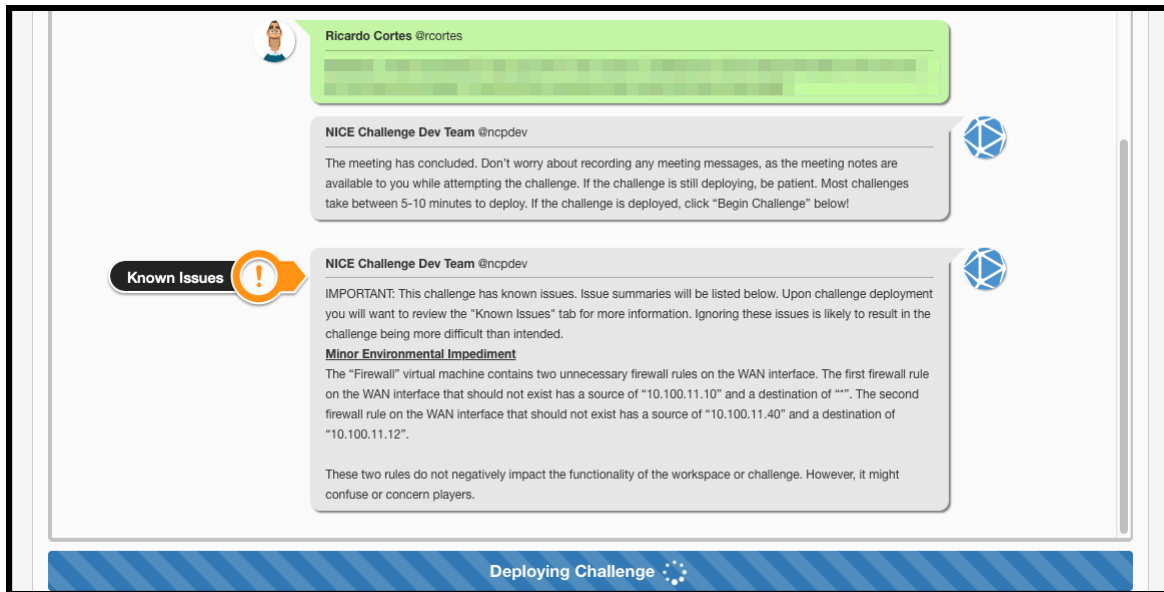
After clicking “Deploy”, players will be presented with the Meeting Chat interface. During this phase, players will witness a meeting take place among fictitious colleagues which will provide valuable details regarding the tasks at hand.

Once the challenge has finished deploying, the progress bar at the bottom of the screen will be replaced by a button that reads “Begin Challenge”.



Known Issues Reminder

Players will be reminded of any known issues related to any particular challenge once the meeting has concluded. Details of the known issue, along with workarounds and potential impact on checks, will be listed in a gray chat bubble sent from the Dev Team.



Returning to Challenge Selection After Deployment

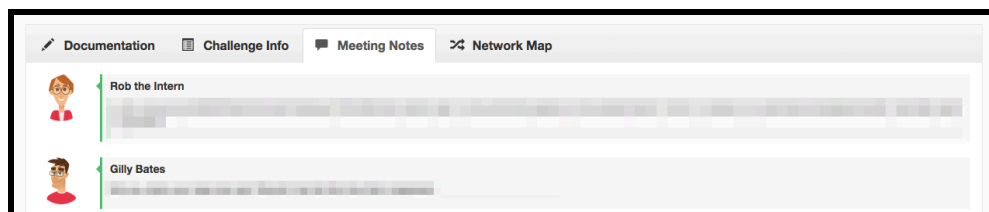
If players wish to select/deploy a new challenge they will need to end the current challenge attempt. This can be done by selecting the "Documentation" tab within the active workspace, providing written documentation, and using the green button labeled "Submit Challenge Attempt" located on the top right of the screen.

Important Submission Note: If players start any challenge and need/want to end the challenge attempt, that challenge attempt will be recorded. All challenge attempts are recorded and sent to the curator for assessment as submissions.

Performing a Challenge Using the XP Cyber Range or NICE Challenge Webportal

Gathering Information from Meeting Chat

Once a challenge has started to deploy onto an active workspace the Meeting Chat animation will display **VERY** important information, often **CRITICAL** to the completion of the challenge. After the meeting animation has concluded, this information can be reviewed by selecting the "Meeting Notes" tab. Players should review all of these communications carefully at the beginning of each challenge.



Understanding & Tracking Checks⁷

After reviewing the challenge's meeting chat, the second thing a player should review is the challenge's checks. Technical challenges often have many checks, Hybrid challenges often have none, and Threat Sandboxes often have one that is used to indicate if the threat is still active or not. Fields in the check section have the following types of data in them...

- **Status** - This field will show either a red ✖ (denoting an incomplete objective), yellow ✖ (denoting an obstructed check), a green ✔ (denoting a complete objective), and a grey ? (denoting an unchecked objective).
- **Check Description** - This field displays text related to the check, usually a brief description of what the check is looking for.
- **Status Info** - This field will show extended status information relating to a check's status.
- **Last Changed** - This field shows the last time the check status changed. This is not to be confused with when a check was last run. Checks generally run every 60 seconds unless otherwise stated in the check description.

The screenshot shows the 'CSE 200 Week 1 | Player One' interface. On the left, the 'Virtual Machines' section lists three machines: Backup, Database, and Dev-Web, all with a 'Powered On' status. On the right, the 'Checks' section is highlighted with a green border and contains a table with the following data:

Status	Check Description	Check Type	Check State	Last Changed
✖	Guest Admin Privileges Disabled	Challenge Check ?	Undesireable State	04:16 PM PST
✖	Joomla Updated	Challenge Check ?	Undesireable State	04:16 PM PST
✖	Vulnerable FTP Updated	Challenge Check ?	Undesireable State	04:17 PM PST

When doing a technical challenge, the main objective is reached when all the checks are reporting back a green ✔ in the status field.

⁷ **Check** - A monitored state, condition, or event within a challenge usually correlated with a challenge objective.

Consoling into VMs & Login Details

Having reviewed the meeting chat for context and the checks that need to be satisfied, it is finally time to get into the VMs. Using the context and the network map, the player should be able to identify what VMs need to be interacted with. If working on a technical challenge, the player will likely need to make changes to these VMs within the workspace. When doing a hybrid challenge, however, they often need only observe specified information within.

The screenshot displays the 'CSE 200 Week 1 | Player One' interface. The top navigation bar includes 'PLAYER' and 'CURATOR' tabs, with 'PLAYER' selected. Below this is a blue bar with 'Dashboard', 'Assignments', 'Submissions', and 'Helpdesk & FAQ'. The main content area is divided into two sections: 'Virtual Machines' and 'Checks'.

Virtual Machines

Having issues with mouse/keyboard input or connecting to VM consoles?

Machine Name	Status	Actions	Open Console ?
Backup	Powered On	Action	HTML5 VMRC
Database	Powered On	Action	HTML5 VMRC
Dev-Web	Powered On	Action	HTML5 VMRC
Domain-Controller	Powered On	Action	HTML5 VMRC
Fileshare	Powered On	Action	HTML5 VMRC
Firewall	Powered On	Action	HTML5 VMRC
Mail	Powered On	Action	HTML5 VMRC
Prod-Web	Powered On	Action	HTML5 VMRC
Router	Powered On	Action	HTML5 VMRC

Checks

Status	Check Description	Check Type	Check State	Last Changed
✖	Guest Admin Privileges Disabled	Challenge Check ?	Undesireable State	04:16 PM PST
✖	Joomla Updated	Challenge Check ?	Undesireable State	04:16 PM PST
✖	Vulnerable FTP Updated	Challenge Check ?	Undesireable State	04:17 PM PST

At the bottom of the interface, there are three tabs: 'Documentation', 'Lab Info', and 'Known Issues'.

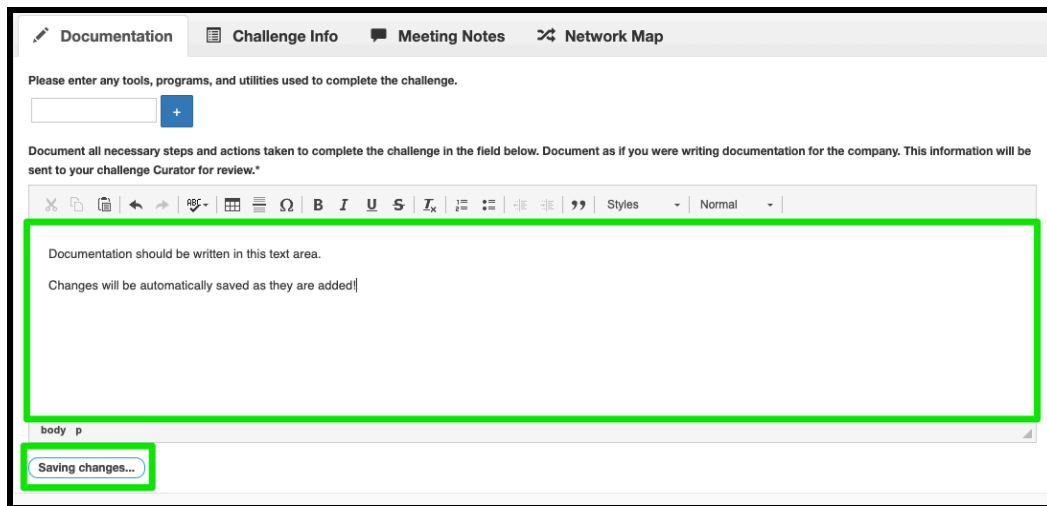
Machine/Service/Application Logins within the environment should always be the same unless the challenge, under the additional information field or meeting chat, states otherwise. The normal login credentials are the following...

- Username/Login: playerone
- Password: password123

Submitting a Challenge

Writing Documentation & Drafts

While completing the challenge, or at the end of the challenge, players need to document their challenge solution. The player should format their documentation as professionally as possible and document with as much detail as they feel is needed to clearly explain their solution.

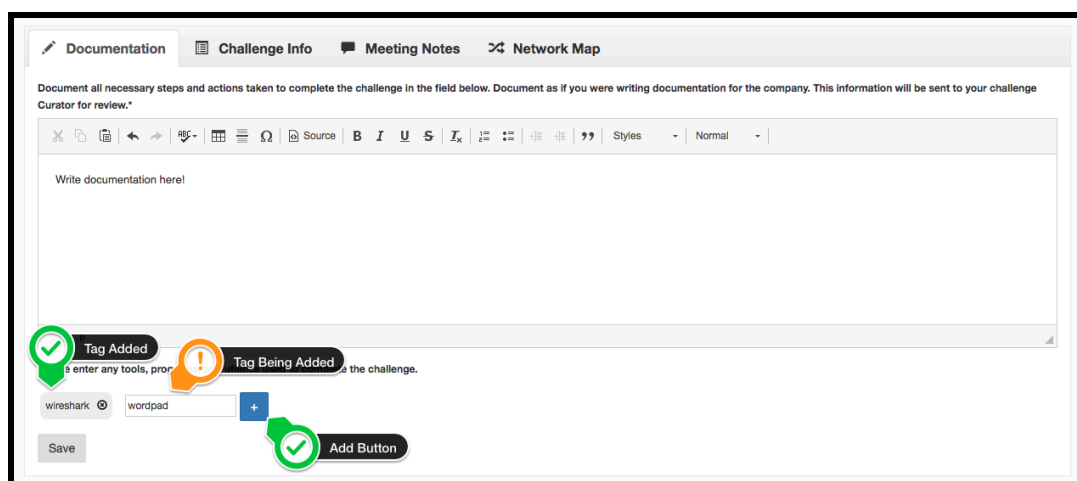


The screenshot shows the 'Documentation' tab selected in a workspace. At the top, there are four tabs: 'Documentation', 'Challenge Info', 'Meeting Notes', and 'Network Map'. Below the tabs, a prompt reads: 'Please enter any tools, programs, and utilities used to complete the challenge.' This is followed by a text input field with a blue plus button to its right. Below this, another prompt reads: 'Document all necessary steps and actions taken to complete the challenge in the field below. Document as if you were writing documentation for the company. This information will be sent to your challenge Curator for review.*' This is followed by a rich text editor with a toolbar containing various formatting options like bold, italic, underline, strikethrough, link, unlink, bulleted list, numbered list, indent, outdent, and styles. The text area contains the placeholder text: 'Documentation should be written in this text area. Changes will be automatically saved as they are added!'. At the bottom left of the text area, there is a small status bar showing 'body p'. Below the text area, a green button labeled 'Saving changes...' is highlighted with a green box.

Player documentation is automatically saved whenever changes are made to the text area. This is so that if the player loses their internet connection or accidentally navigates away from their workspace they will not lose their documentation while the challenge is still in progress. A message will display below the text area whenever the process of saving documentation is occurring.

Adding Software/Utilities/Coding Languages to the Tools Used List

Along with documenting their solution to the challenge, players will want to tag software applications, operating system utilities, and coding languages utilized in their solution in the tools used list. However, coding languages should only be added when the player uses a coding language to write a script or program to aid in their completion of a challenge.



This screenshot shows the same 'Documentation' tab as the previous one, but with additional elements. The text area now contains the placeholder text: 'Write documentation here!'. Below the text area, there is a 'Tools Used' section. It features a list of tags: 'wireshark' and 'wordpad'. To the right of the 'wordpad' tag is a blue plus button. Below the tags, there is a 'Save' button and an 'Add Button' button. Above the 'Add Button' button, there is a green checkmark icon and a message: 'Tag Added'. Above the 'wordpad' tag, there is an orange warning icon and a message: 'Tag Being Added'. The 'Add Button' button is highlighted with a green box.

Final Submission & Ending the Challenge Attempt

Once the player is satisfied with their challenge attempt, has documented their solution, and has added their tools used, it is time to end the challenge attempt. This is done by clicking the “Submit Challenge Attempt” button located on the top right of the page. Do **NOT** hit this button until the attempt is **COMPLETELY DONE**. A player **CANNOT** take the submission back or edit it once it is submitted. This will end the challenge attempt and send the results to their curator.

The screenshot shows the CSE 200 Week 1 Player interface. At the top, there are tabs for 'PLAYER' and 'CURATOR'. Below these are navigation links: 'Dashboard', 'Assignments', 'Submissions', and 'Helpdesk & FAQ'. The main header indicates 'CSE 200 Week 1 | Player One' and a timer showing '7h 18m 1s'. A green box labeled 'Finalize Submission' points to the 'Submit Lab' button in the top right corner.

Virtual Machines

Having issues with mouse/keyboard input or connecting to VM consoles?

Machine Name	Status	Actions	Open Console ?
Backup	Powered On	Action ▾	HTML5 VMRC
Database	Powered On	Action ▾	HTML5 VMRC
Dev-Web	Powered On	Action ▾	HTML5 VMRC

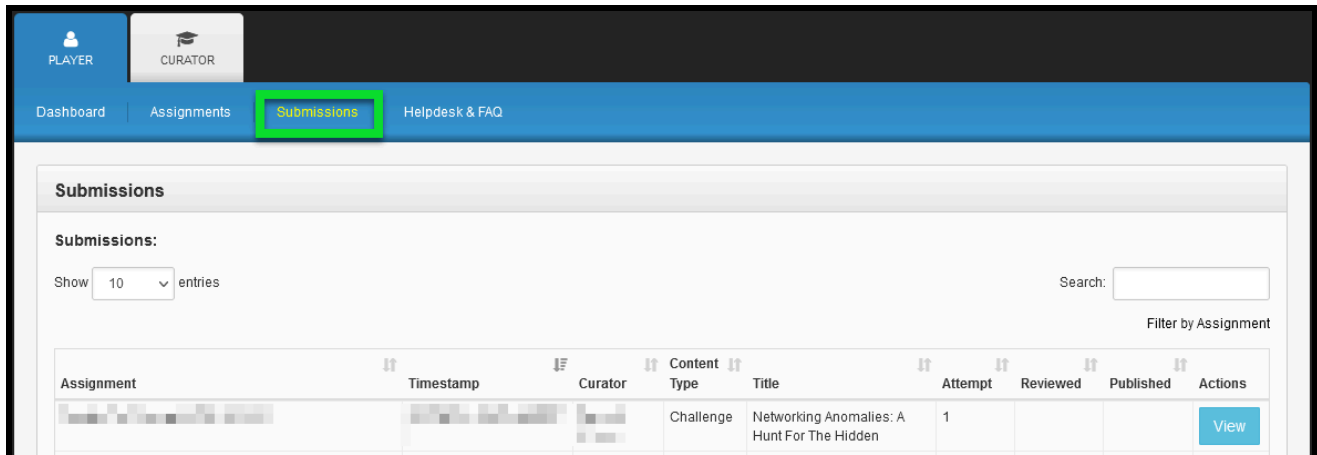
Checks

Status	Check Description	Check Type	Check State	Last Changed
✖	Guest Admin Privileges Disabled	Challenge Check ?	Undesireable State	04:16 PM PST
✖	Joomla Updated	Challenge Check ?	Undesireable State	04:16 PM PST
✖	Vulnerable FTP Updated	Challenge Check ?	Undesireable State	04:17 PM PST

Viewing Challenge Submissions

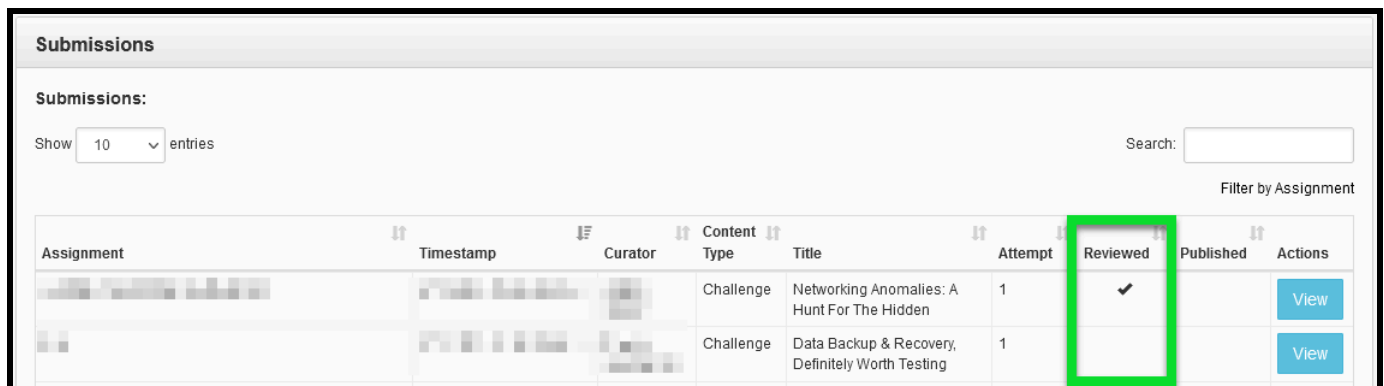
Navigating to the Submissions Page

Upon successfully logging in to the XP Cyber Range or NICE Challenge Webportal, players may navigate to the Submissions page by clicking on the “Submissions” link in the navbar. By default, challenge submissions will be sorted by date of submission.



Reviewing Challenge Attempts

Challenge submissions are listed in the table located in the upper half of the page. The table can be sorted by clicking on the table header corresponding to the criteria by which you wish to sort (assignment, timestamp, etc.). Challenge submissions that have been reviewed by the curator will display a checkmark in the column labeled “Reviewed”.



Viewing Challenge Attempt Details

Clicking the green button labeled “View” on any row will populate the Submission Review view, located below, with details corresponding to that particular challenge submission.

Understanding the Challenge Attempt View

The challenge attempt view includes submission details such as:

- Title
- Complexity
- Attempt Duration
- Check Status
- Tools Used
- Submitted Documentation
- Submission Feedback

Each challenge consists of a series of checks that players must satisfy in order to complete it. These checks, along with their descriptions, are listed in the section labeled “Final Check Details”.

An overall assessment of the player’s attempt to satisfy the challenge checks can be found under the section labeled “Full Check Pass”.

Players are asked to provide a list of any tools used during their challenge attempt. This list is displayed in the section labeled “Tools Used”.

Most challenges prompt the player to submit some sort of written documentation detailing how they arrived at a solution. This documentation will be displayed in the section labeled “Submitted Documentation”.

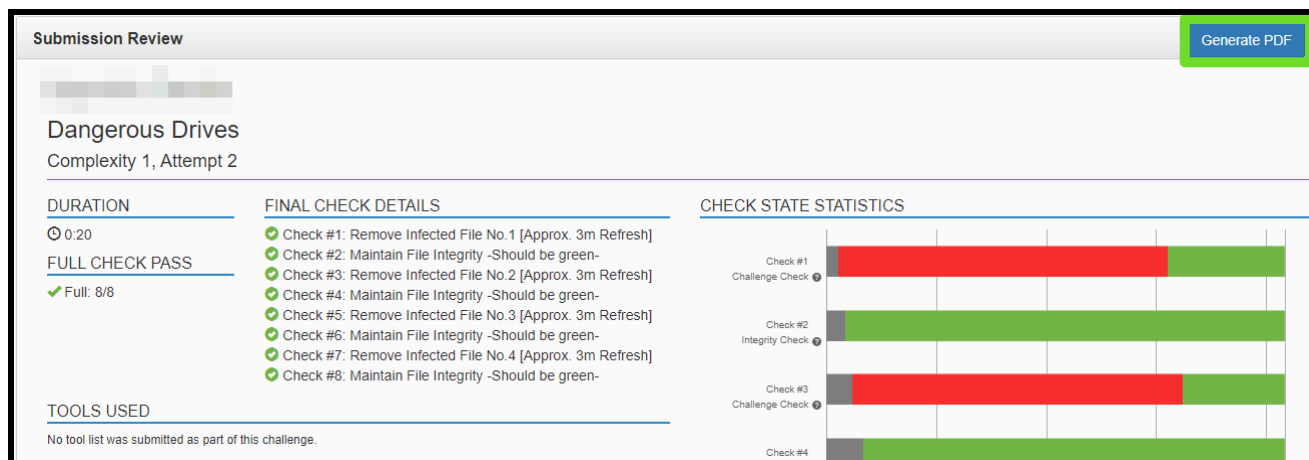
Once the curator has reviewed a challenge attempt, their finalized review is displayed in the area labeled “Submission Feedback” at the bottom of the page.



Exporting Submissions to PDF

Challenge submissions may be exported to PDF by clicking on the blue button labeled “Generate PDF” located on the top right of the Submission Review pane.

Generated PDFs include the DoD Cyber Workforce Framework and NICE Framework mappings associated with the challenge that was attempted. They may be printed out and presented to parties interested in the assessment of the skills of the player who performed the challenge.



Verification - An interested party may verify the authenticity of the printed report by scanning the QR code or visiting the address provided near the top of the document. The address provided will render a nearly identical PDF with values redacted to conserve privacy. The interested party may review the presented values and ensure they match the physical report they have been provided with.

Curator Publishing - Curators have the option to “publish” their reviews of challenge submissions. Once a curator publishes a review, they will no longer be able to alter that review. Upon publishing a review, they also consent to their name and the name of their educational institution appearing in a box labeled “Reviewed By” near the top of the document. PDFs generated from challenge attempts that do not have a review published by a curator will have a statement in place that explains the report has not yet been published and validity is not supported.

Challenge Tips & Top FAQs

Challenge Tips

Don't Forget About Additional Info!

When gathering information about what needs to be done for a challenge, make sure to also review the “Additional Information” section under the “Challenge” tab. The check descriptions and meeting chat draw the most attention, but missing something in additional info can really set a player back.

Checks Cycle Every Minute

This means that the second a player makes a change, it might not reflect in the check status for another 60 seconds. Make changes carefully and thoughtfully then be patient. Otherwise, a correct solution might slip through between checks.

Avoid Network & Permissions Changes

Unless the challenge is specifically asking the player to make changes to the network configuration, do not do this. Checks will often depend on these configurations remaining static. This tip is also true when it comes to permissions. Unless the challenge specifically instructs the player to, or it is obviously needed, do not alter permissions on files/services/users/servers to be more restrictive. Players are welcome to make note and suggest changes in their documentation, of course. However, again, it may restrict a check from functioning properly.

Top FAQ Articles

[*I am having issues solving a challenge, what should I do?*](#)

[*The HTML5 Console is Not Working Right! \(Mouse/Keyboard Input Issues\)*](#)

[*What is the username/password for X VM or X service in the workspace?*](#)

[*Can I copy and paste from my local machine to the virtual machines in the workspace?*](#)

[*Do I need to finish the challenge in one sitting or can I leave and come back to it later?*](#)

[*What time do assignments and workspaces begin and end?*](#)

Console Support & Availability

Review the XP Cyber Helpdesk article: [Which operating systems/web browsers are supported?](#)