Welcome to the DEF CON 33 Capture the Flag Final!

Document version: 1.0.0

The DEF CON CTF is a team-based, attack-defend hacking competition. Each team will be given access to a game network where they must defend their own network services via patches while attacking other teams' network services via exploits. There will also be some extra "King of the Hill" challenges where teams will compete directly in a separate activity for time or resources. Additionally, we've partnered with LiveCTF again to bring back the bracket-based individual tournament for additional points.

Version History

- **1.0.0** – Initial release.

Schedule

The CTF will be run for 3 consecutive days as follows:

Date and Time:	Friday, August 8 from 10:00 - 17:00 PDT Saturday, August 9 from 10:00 - 17:00 PDT Sunday, August 10 from 10:00 - 12:00 PDT
Location:	Las Vegas Convention Center, West Hall, Level 1, Exhibit Hall 1, southeast corner, space 209; come in from door W1

Teams will be allowed into the CTF room 1 hour before the event begins on each day (09:00) to set up their networking equipment and prepare for the game. Exit and re-entry during the pre-game period is not possible. We will have a captain's meeting 15 minutes before the game (09:45) and 15 minutes after the game (17:15). The captain's meeting will happen with or without you, so arrive on time!

LiveCTF

The LiveCTF schedule is subject to change based on how events play out during the CTF and whether or not anything breaks. This year's event is double-elimination.

At 10:00am we'll be running compatibility tests. You **must** test your HDMI, USB-C, and/or network interfaces prior to participating. If your hardware is not compatible, it is up to your team to identify a suitable replacement before your round starts. We require all output to be 1080p, with no multiple displays.

An up-to-date schedule is available at https://livectf.challonge.com/livectf_defcon2025

Communication

Communication between Nautilus Institute and teams will happen in three places:

1. In-person in the CTF room
2. The DEF CON Discord guild
3. The ticketing system on the scoreboard

In-Person

Nautilus Institute personnel will be located in the designated area in the room and most will be wearing white lab coats. Feel free to ask us anything, but please understand that not every NI member will be able to answer every question. During times when we have a high volume of requests, or in situations where we need to, we will ask you to authenticate with us via a physical token that is associated with your team.

To authenticate with us, we will be providing a physical token to each team captain on the first day of the CTF. *Anyone* who presents that token to us will be considered the representative of the team. Please make sure to keep your token safe and do not give it to anyone you don't trust to make decisions for your whole team. Treat these like you would treat the keys to your house.

Discord

On August 7, 2025, every team received an email requesting that up to 4 Discord IDs be provided for team members that should be given access to the #ctf-captains-text channel. This channel should be used for public communications between Nautilus Institute and all teams. Private communication can take place in DMs (feel free to ask in #ctf-captains-text *which* NI member should be DMed for a certain problem).

Scoreboard Tickets

The scoreboard (see section below on scoring) itself has a ticketing system. This system can also be used to submit requests from your team to us and will be monitored during the CTF. Responses to submitted tickets will also be shown on the scoreboard in the ticketing system.

Game Rules

1. All Nautilus Institute decisions are final.
2. The DEF CON CTF is a reverse engineering and exploitation competition first and foremost. Actions not taken in that spirit are likely out of bounds.
3. If you are caught cheating, we will disqualify you.
4. At least 12 people will be allowed at each team table at a time – we may expand once we see how the room works with 12. There is no limitation on overall team size.
5. The following are examples of actions and areas that are in-bounds:
    a. Accessing the following networks:
        i. The network you receive through the ethernet cable to your table.
        ii. The network given to attack other teams.
        iii. The network given to access the scoreboard.
        iv. The internet.
    b. Interacting with challenges on opponents' boxes.
    c. Polling challenge information to build your own scoreboards.
        i. We may require you to throttle or stop excessive traffic.
6. The following are examples of actions and areas that are out-of-bounds and may result in disqualification:
    a. Attacks on the game infrastructure that include, but are not limited to:
        i. Tampering with networking equipment and cabling

ii. Conducting Denial-of-Service attacks.
iii. Exploiting the administrative infrastructure.
iv. Attacking the hypervisor that is running the services.

b. Accessing networks outside of those specified in 5a above.
c. Any act which prevents another team from fairly participating in the game.
d. Collusion with other teams.
e. Violating the DEF CON Code of Conduct (https://defcon.org/html/links/dc-code-of-conduct.html).

This is a hacking competition, and we welcome creative solutions to problems within it. Some of these solutions may exist in a gray area that our rules do not clearly address. If you feel you are in that gray area, please consult a representative of Nautilus Institute for clarification.

LiveCTF

This year's rules are broadly similar to 2024's:

- You **may not** have any outside live human help (subject to immediate disqualification).
- Other internet resources (yes, including ChatGPT!) are fair game.
- You **must** test your HDMI, USB-C, and/or network interfaces prior to participating. If your hardware is not compatible, it is up to your team to identify a suitable replacement before your round starts. We require all output to be 1080p, with no multiple displays. MacOS users, please disable "Night Shift".
- Participants **must** wear noise-blocking ear covers that will be provided along with sanitization wipes. No personal headphones allowed.
- Players may be shown at times on a camera feed being live-streamed. You are welcome to wear a mask, pull up a hood, or otherwise obfuscate your face if this causes any privacy concerns.
- Some rounds will have four players participating in the same challenge at the same time. One of the matches will have commentary, the other will not.
- Teams **may** swap out their representative between rounds but not during a round.
- A general category and/or description of the challenge will be provided before rounds.
- All rounds before the final round are double elimination. This means even a stroke of bad luck, or one bad result won't knock out a good competitor and they can always play back into the finals. Any team that loses twice before the final round is eliminated. The final round is the only single-elimination round (in other words, if the team from the lower bracket wins, there will not be an additional final round).
- Sudden death (and any hints before it) will be on a strict schedule identified before the round starts and independent of progress from either team.

Game Network

Teams will access the game network via ports 1-12 on the main switch. Each team will be provided with a single cable that puts them on a /24 network in the 10.0.x.0/24 range, with the router at the 10.0.x.1 address. You may connect an unmanaged switch to this network in order to connect the entire team. There is a DHCP server that will distribute leases to each team. The DNS server is 10.13.37.1.

Our game runs on the 10.0.0.0/8 address space. We strongly recommend not using 10.0.0.0/8 for your internal networking. Consider something in 192.168/16, or IPv6. We will operate our network, but cannot operate yours.

Services are accessible remotely via the router address of each team as shown in the following table:

Team Name	Team Number	Subnet	Service IP
MMM	1	10.0.1.0/24	10.10.1.1
Friendly Maltese Citizens	2	10.0.2.0/24	10.10.2.1
kalmarunionen	3	10.0.3.0/24	10.10.3.1
RePokemonedCollections	4	10.0.4.0/24	10.10.4.1
Blue Water	5	10.0.5.0/24	10.10.5.1
SuperDiceCode	6	10.0.6.0/24	10.10.6.1
mhackeroni	7	10.0.7.0/24	10.10.7.1
Nu1L	8	10.0.8.0/24	10.10.8.1
Shellphish	9	10.0.9.0/24	10.10.9.1
KuK Hofhackerei	10	10.0.10.0/24	10.10.10.1
this year's organizers	11	10.0.11.0/24	10.10.11.1
Cold Fusion	12	10.0.12.0/24	10.10.12.1

For example, if a team wished to talk to team 2's service, they would connect to 10.10.2.1 on the service's port.

Connecting to a service's port may cause it to launch a unique instance, in which case you will be given a second port to connect to on which the actual service will be listening.

Network activity is limited. At the time of writing, we have allocated 40mbps per team, and 15mbps of that 40mbps can be used for the internet. **50 concurrent** connections to services are allowed from your team; too many connections will get you a message to slow down. **These limits may change during the game.**

Other Game Interfaces

Scoreboard: https://scoreboard.finals.2025.nautilus.institute/ ; also has credentials for the registry and dashboard available

Registry: https://registry.finals.2025.nautilus.institute:5000/ ;

Dashboard: https://dashboard.finals.2025.nautilus.institute:9090/ ; also has documentation and notes on how service management works

Packet Captures

PCAPs will be provided through the scoreboard (see section below on scoring) at roughly 15-minute intervals, with a 15-minute delay. These PCAPs will be altered to hide the source of origin for attacks. PCAPs will not be provided for services scored over stealth ports.

Patches and Service Deployment

Attack/Defend services in this year's game will be deployed from a Docker Registry, which has a web frontend that will be available at:

https://registry.finals.2025.nautilus.institute:5000/

To obtain and submit container images, you must login with docker using the provided credentials. You will be provided with a pair of credentials on the scoreboard: `<team-name>` and `<team-name>-readonly`. The first account will have full access read and write to your container deployments. The second, readonly, account will only be able to read images.

```
$ docker login registry.finals.2025.nautilus.institute:5000
```

For each regular attack-defend service, your team will maintain a `:latest` service container image located at

```
$ docker pull registry.finals.2025.nautilus.institute:5000/team/$TEAM/live/$SERVICE:latest
```

Creating a Patched Image

Create a new container image which modifies files in the base container image. You can obtain the unmodified base image with the following tag:

```
$ docker pull registry.finals.2025.nautilus.institute:5000/team/$TEAM/live/$SERVICE:base
$ cat Dockerfile
FROM registry.finals.2025.nautilus.institute:5000/team/$TEAM/live/$SERVICE:base
COPY my_patched_version_foo /foo # patch the /foo file
$ docker build –t my-amazing-patch:latest .
```

Submitting a Patch

Your modified container image must pass our service validation checks. Push your patched container to the following staging tag to submit the patch:

```
$ docker tag my-amazing-patch:latest
  registry.finals.2025.nautilus.institute:5000/team/$TEAM/staging/$SERVICE:latest
$ docker push registry.finals.2025.nautilus.institute:5000/team/$TEAM/staging/$SERVICE:latest
```

Checking Patch Status

You can view a list of your recent patch submissions at
https://registry.finals.2025.nautilus.institute:5000/patches

Failed Patch Submissions

To ensure a secure supply chain, patched images are inspected and validated before they can be deployed. A patched image may be rejected for many reasons.

- If the image has more than 10 additional "new layers" the patch will be **rejected**. A "new layer" is defined as a layer in the patched image which is not present in the base image.

- If the total size difference of any "new layers" in the patched image is over a service specific limit the patch will be **rejected**. The total size difference is defined in this way:

The sum of running `gzip -l` to get the uncompressed size on each “new layer” data-file stored within a standard docker registry:2.

The registry server and the Nautilus have final say on the measured modification size of any submitted image. The size of the image on your local storage backend may differ.

Note: due to how container layers work, modifying any bytes within a file counts as the entire file’s size within the new layer.

- During patch validation a hidden suite of feature tests will be ran against the image. If the patched image fails or errors the tests during this feature validation, the patch will be **rejected**.

Feature tests should avoid triggering bugs in the service, but may test for specific service or protocol configurations, use shared confidential material to authenticate with elevated permissions, or perform other special actions. Starting base service images **may** pass feature validation.

- A patch/image may also be **rejected** for other reasons as defined by Nautilus.

See the scoreboard for any information about any additional service patch restrictions, if any.

Successful Patch Deployment

If a patch passes all validation checks, it will then be deployed. Once the patch has been deployed, our infrastructure will re-tag the image as **live-<timestamp>** with the timestamp of when the patch went live.

Patches for all teams will ***immediately*** be made available to every other team through the registry along with being deployed across the game network.

Points and Scoring

In the DEF CON 33 CTF Final, your total score will be the sum of the following:

TOTAL = ATTACK + DEFENSE + KOTH + LIVECTF

To score flags, you will need to sign into the scoreboard with your team name and password. Your password will be given to team captains before the game starts. Flag submission requires a POST to the scoreboard via HTTPS.

The scoreboard is located at:

https://scoreboard.finals.2025.nautilus.institute/

Scores on the scoreboard will, by default, be delayed by 3 rounds. We reserve the right to change this delay at any time and will make our best effort to communicate if and when it changes.

Attack-Defense

Points for Attack-Defense services are split into two components (Attack and Defense points) that are each awarded every round, per service:

- **Attack:**

    - 100 points are awarded per unique, active flag stolen from another team
    - 25 points are awarded if the attacker launches the challenge in stealth mode, which doesn't leave packet captures
- **Defense:**
    - 1200 defense points are available per service per round, divided between teams that did not have a flag stolen:
        - 1 team defends, they get 1200 points
        - 2 teams defend, 600 points each
        - 3 teams defend, 400 points each
        - 4 teams defend, 300 points each
        - 5-6 teams defend, 200 points each
        - 7-12 teams defend, 100 point each
    - There is no penalty for patching, but you may only submit one successful patch per 5 minute interval.

Flags are considered 'active' for 3 rounds (the current round and the two preceding it). This should be roughly equivalent to 10-15 minutes of real-world time.

King of the Hill

Points for King of the Hill will be awarded every round while the service is active according to where each team is ranked within that round:

- **Rank 1:** 1200
- **Rank 2:** 700
- **Rank 3:** 400
- **Rank 4:** 200
- **Rank 5:** 100
- **Ranks 6-12** will receive 000 points

If a tie occurs between ranks, all ranks involved will have their points added together and then split between the teams that have tied. Example: Teams ranked 2 and 3 are tied. This is a total of 2100 points. These two teams will receive 1050 points for that round.

LiveCTF

Points will be awarded as follows:

- **1st place:** 133700 points
- **2nd place:** 100000 points
- **3rd place:** 90000 points
- **4th place:** 80000 points
- **5-6th place:** 70000 points
- **7-8th place:** 60000 points
- **9-12th place:** 50000 points