Welcome to the DEF CON 31 Capture the Flag Final!

Document version: 1.0.2

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

- **1.0.2** - Updated the King of the Hill scoring algorithm.
- **1.0.1** - Added mapping between teams and IDs in Game Network section.
- **1.0** - Initial release.

Schedule

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

Date and Time:	Friday, August 11 from 10:00 - 18:00 PDT
	Saturday, August 12 from 10:00 - 18:00 PDT
	Sunday, August 13 from 10:00 - 14:00 PDT
Location:	Caesar's Forum, Rooms 204 and 205

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. We will have a captain's meeting 15 minutes before the game (09:45) and 15 minutes after the game (18:15). 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*, which means there are more matches than last year despite having qualified less teams. The expected schedule is as follows:

Friday, July 11 (Underlined Matches will have commentary, all matches are streamed)

Latest schedule available at: https://livectf.challonge.com/livectf_defcon2023

- **CTF setup - 11am:** Laptop Test Window
  - Please test your devices to ensure compatibility with our capture equipment!
- **12pm - 1pm:** Stream A / Match 1: mhackeroni vs. P1G BuT S4D
- **12am - 1pm:** Stream A / Match 2: TWN48 vs. HypeBoy
- **2pm - 3pm:** Stream B / Match 3: Norsecode vs. Shellphish
- **2pm - 3pm:** Stream B / Match 4: Straw Hat vs. undef1ned
- **3pm - 4pm:** Stream C / Match 5: Blue Water vs. Match 1 winner

- **3pm - 4pm:** Stream C / Match 6: SuperDiceCode vs. Match 2 winner
- **4pm - 5pm:** Stream D / Match 7: Maple Mallard Magistrates vs. Match 3 winner
- **4pm - 5pm:** Stream D / Match 8: orgakraut vs. Match 4 winner

Saturday, July 12

- **10am - 11am:** Stream E / Match 9: Loser of Match 5 vs. Loser of Match 4
- **10am - 11am:** Stream E / Match 10: Loser of Match 6 vs. Loser of Match 3
- **11am - 12pm:** Stream F / Match 11: Loser of Match 7 vs. Loser of Match 2
- **11am - 12pm:** Stream F / Match 12: Loser of Match 8 vs. Loser of Match 1
- **12pm - 1pm:** Stream G / Match 13: Winner of Match 10 vs. Winner of Match 9
- **12pm - 1pm:** Stream G / Match 14: Winner of Match 12 vs. Winner of Match 11
- **2pm - 3pm:** Stream H / Match 15: Winner of Match 6 vs. Winner of Match 5
- **2pm - 3pm:** Stream H / Match 16: Winner of Match 8 vs. Winner of Match 7
- **3pm - 4pm:** Stream I / Match 17: Loser of Match 15 vs. Winner of Match 14
- **3pm - 4pm:** Stream I / Match 18: Loser of Match 16 vs. Winner of Match 13

Sunday, July 13

- **10am - 11am:** Stream J / Match 19: Winner of Match 18 vs. Winner of Match 17
- **11am - 12pm:** Stream K (Semi-Final) / Match 20: Winner of Match 16 vs. Winner of Match 15
- **1pm - 2pm:** Stream L (Lower Final) / Match 21: Loser of Match 20 vs. Winner of Match 19
- **2pm - 3pm:** Stream M (Grand Final) / Match 22: Winner of Match 21 vs. Winner of Match 20

Communication

Communication between Nautilus Institute and teams will happen in two 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 corner of 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 July 24, 2023 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. 8 people will be allowed at each team table at a time. 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).
    f. Stealing another team's physical authentication token.

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

We have two changes from last year:

1. 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. 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. 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).
2. 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.

Otherwise, the rules this year are the same:

- 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.
- 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.

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

Team Name	Team Number	Subnet	Service IP
BlueWater	1	10.0.1.0/24	10.10.1.1
Maple Mallard Magistrates	2	10.0.2.0/24	10.10.2.1
Orgakraut	3	10.0.3.0/24	10.10.3.1
SuperDiceCode	4	10.0.4.0/24	10.10.4.1
TWN48	5	10.0.5.0/24	10.10.5.1
StrawHat	6	10.0.6.0/24	10.10.6.1
Norsecode	7	10.0.7.0/24	10.10.7.1
mhackeroni	8	10.0.8.0/24	10.10.8.1

P1G_BuT_S4D	9	10.0.9.0/24	10.10.9.1
Shellphish	10	10.0.10.0/24	10.10.10.1
Undef1ned	11	10.0.11.0/24	10.10.11.1
hypeboy	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.

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.

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.2023.nautilus.institute:5000/

Each service's container image will be named the same as that service. The *original base version* will be tagged **:base**. Every modified version of the service that has been deployed to game boxes by our infrastructure will be tagged **:live-<timestamp>** .

To obtain service images, you will need to log in and pull from the registry:

```
$ docker login registry.finals.2023.nautilus.institute:5000
$ docker pull registry.finals.2023.nautilus.institute:5000/team/$TEAM/live/$SERVICE:base
```

You can find your registry credentials on the scoreboard. You will have a read/write credential and a read-only credential. It is your responsibility to keep your registry credentials safe!

You can make changes to the service in the form of a new image layer on top of the base service image. Services may have restrictions on the max **uncompressed** size of the new image layers (including metadata). See the scoreboard for any information about service patch restrictions.

To apply a patch to your service, tag your patched image under the **staging** namespace as **:latest** and push it back to the registry:

```
$ docker tag my_patched_image:latest
  registry.finals.2023.nautilus.institute:5000/team/$TEAM/staging/$SERVICE:latest
$ docker push registry.finals.2023.nautilus.institute:5000/team/$TEAM/staging/$SERVICE:latest
```

Our infrastructure will deploy the patch ***immediately*** and you will incur a patching penalty for that round (see scoring section below). 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 once they have been deployed to the game network.

To validate if your patch deployed successfully or failed due to errors/restrictions you can request the following page for image status:

```
$ IMAGE_DIGEST="$(docker inspect $MY_IMAGE_NAME -f '{{ .Id }}')"
$ curl https://registry.finals.2023.nautilus.institute:5000/status/$TEAM/$IMAGE_DIGEST
```

Points and Scoring

In the DEF CON 31 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.2023.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:**
  - 1 point is awarded per unique, active flag stolen from another team
  - 1 point is awarded to all teams whose service is UP per team whose service is DOWN
- **Defense:**
  - 1 point is awarded to all teams whose service is UP and *did not* have their flag stolen
  - A team's service will be considered DOWN if it has been patched during that round
  - There is no additional penalty for patching multiple times during a single round
  - Your service is considered DOWN if you submit a patch and it fails our SLA check

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:** 12
- **Rank 2:** 7
- **Rank 3:** 4
- **Rank 4:** 2
- **Rank 5:** 1
- **Ranks 6-12** will receive 0 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 21 points. These two teams will receive 10.5 points for that round.

LiveCTF

Points will be awarded as follows:

- **1st place:** 1337 points
- **2nd place:** 1000 points
- **3rd place:** 900 points
- **4th place:** 800 points
- **5-6th place:** 700 points
- **7-8th place:** 600 points
- **9-12th place:** 500 points