PARTICIPANT'S MEMO. MCTF INTERNATIONAL 2025

MCTF-I (International) is a student team competition in the field of information security organized by the Moscow Technical University of Communications and Informatics (MTUCI) for its foreign partner universities.

RULES, GENERAL TERMS AND DEFINITIONS

These rules are subject to change at any time before the start of the final stage. Be sure to read them again right before the game starts, so you don't miss anything :) But we will try to warn you at least a day in advance.

1. The competition is a team computer security competition based on the Capture the flag rules among student teams from higher educational institutions in world that provide training in the field of Information Security.
2. Only teams consisting of students from one university in your country are eligible to participate in the Competition. A team consists of university students and no more than one graduate from the previous year.
   - The size of the team must be at least 3 (three) and not more than 7 (seven) people;
   - The age of participants at the date of the final competitions (March 12, 2025) cannot exceed 26 years.
   - The maximum number of participating teams is no more than 14. The organizers reserve the right to limit the number of teams from one university.
3. The final stage of the competition takes place in person.
   - Guest teams may participate online (in case of a justified reason for not being able to attend in person).
4. The jury is a group of people responsible for conducting the Competition.
   The jury undertakes to:
   - Determine the winners of the Competition honestly and impartially;
   - Inform teams in advance about any changes during the Competition;
   - Assist teams in resolving any issues not related to the tasks of the Competition.
     The jury has the right to:
   - Make decisions in critical situations;
   - Require teams to comply with the requirements of this regulation;
   - Disqualify and penalize teams for violating the established rules.

5. All game services, as well as the system for checking the results of task completion, are developed by the technical commission and kept secret until the start of the Competition.
6. Flag format: `[A-Z0-9]{31}=`
   Flag lifetime is limited, and outdated flags do not affect scoring.
7. The verification system is an automatic system that enters flags into the services, checks the serviceability of the services and assigns points. The points awarded, along with the status of the services, are displayed on the scoreboard.
   The services can be in one of the following states:
   - **UP** - the service is available over the network, responds to requests and behaves as expected by the verification system;
   - **CORRUPT** - the service is accessible over the network but cannot return one of the previous flags;
   - **MUMBLE** - some of the service's functionality is not working. For example, registration in the service has been disabled, and the user cannot use it;
   - **DOWN** - the service is unavailable over the network.
     Points for attack and defense depend on the state of the service.
8. A game round is a period of time during which the verification system enters new flags into the services and checks for old flags. All rounds last an equal amount of time.
9. The game begins with the distribution of identical archives to participants, containing a pre-prepared set of vulnerable services, VPN configs for connecting to «vulnbox» and team members, as well as an additional team token. For the first hour after receiving the game image, network segments are closed, and teams should focus on administering their game server and analyzing vulnerabilities. After this hour, the network opens, and for 6 hours teams can exploit vulnerabilities in order to obtain flags from other teams.
10. Teams are allowed to:
    - Do whatever they want inside their network segment. Most likely, teams will want to change the configuration of their server and close vulnerabilities in their services;
    - Attack other teams within the game network.
11. Teams are forbidden to:
    - Attack the organizers' systems;
    - Generate a large amount of traffic that poses a threat to the stability of the organizers' systems or other teams;
    - Engage in inter-team interaction during the game.
    - To transfer services, as well as the values of «flags», to anyone except team members;
    - To receive «flags» from persons who are not registered as team members.
    - To perform all the aforementioned actions on behalf of other teams.
12. The jury may disqualify a team or penalize it by deducting a certain number of points for violating the established rules and disrupting the Competition in any other way.
13. The competition organizers make every effort to ensure that the game is of high quality and interesting. However, exceptional situations may arise during the game. Teams

should be understanding of this possibility and of the decisions taken by the organizers in these situations.

FAQ

Date / time of the event / where is it held?

Date: March 12, 2024.
Time: 11:00 a.m. — 5:00 p.m.
Network opening time: 12:00 a.m.
Venue: Aviamotornaya Street, building 39, MTUCI Congress Center.

What board do we use?

https://gitlab.com/adplatf/adplatf

Scoreboard

Scoreboard: http://mctf.ru/
Beautiful game visualization with real-time flying flags:
http://mctf.ru/circle/

Bonuses for First Blood

Only a beautiful icon :)

Where can I get the token and VPN configs?

Before the start of the game, captains of all teams will be sent zip archives containing:

- Client configs for connecting to the game network (OpenVPN).
- VulnBox connection config (OpenVPN).
- The token you will need to submit flags.

How will vulnerable services be issued?

You will be given zip archives that will contain vulnerable services wrapped in «Docker Compose».

How do we host vulnerable services?

- Self-hosting
- Cloud - this option provided by organizers for beginners

What is the difference between Self - Hosting and Cloud?

- **Self-hosting** - independent hosting of vulnerable services on your own VM, means that you customize your environment and manage your system resources yourself
- **Cloud** - the organizers prepare everything for you, the VM already has OpenVPN config and vulnerable services running, but resources on this VM are limited

What are the hardware resources on the VMs being issued?

CPU: 8
MEM: 12 GB
Storage: 120 GB

Flag format

`int FLAG_LENGTH = 32` - flag length
`char[] ALPHABET = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ"` - alphabet
`flag.charAt(FLAG_LENGTH - 1) == '='` - the last character is '='
`FLAG_RE = r'[A-Z0-9]{31}='` - regular expression for the flag

Which port for flags?

80 port

What are the parameters?

- `checkInterval: 20` - determines the interval in seconds between checks.
- `checksInRound: 3` - defines the number of checker runs per round.
  The first check always happens at 0 seconds of each minute, then every `checkInterval` seconds.
  Thus, `checksInRound * checkInterval` make up the length of a round in seconds.
- `totalRounds: 360` - determines the number of rounds in the game. After they are completed, the game and score freeze will automatically end.
- `flagLifeLength: 5` - defines the number of rounds during which you can submit a flag before it becomes obsolete.
- `scoreInflation: true` - inflation.
- `initialScore: 5000` - determines the FP that the team will have on this service at the beginning of the game.

Attack - Data

```
http://mctf.ru/attack_data
```

Scoring parameters

More information about scoring can be found here

Destructive Farm

Protocol - **HTTP**

Curl request example:

```
curl -X PUT -H 'Content-Type: application/json' -H 'X-Team-Token: <token>'
http://<board ip>/flags --data '["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA="]'
```

Flags are sent via an HTTP request `PUT /flags` for board IP.
The headers must contain `X-Team-Token` with the token team name.

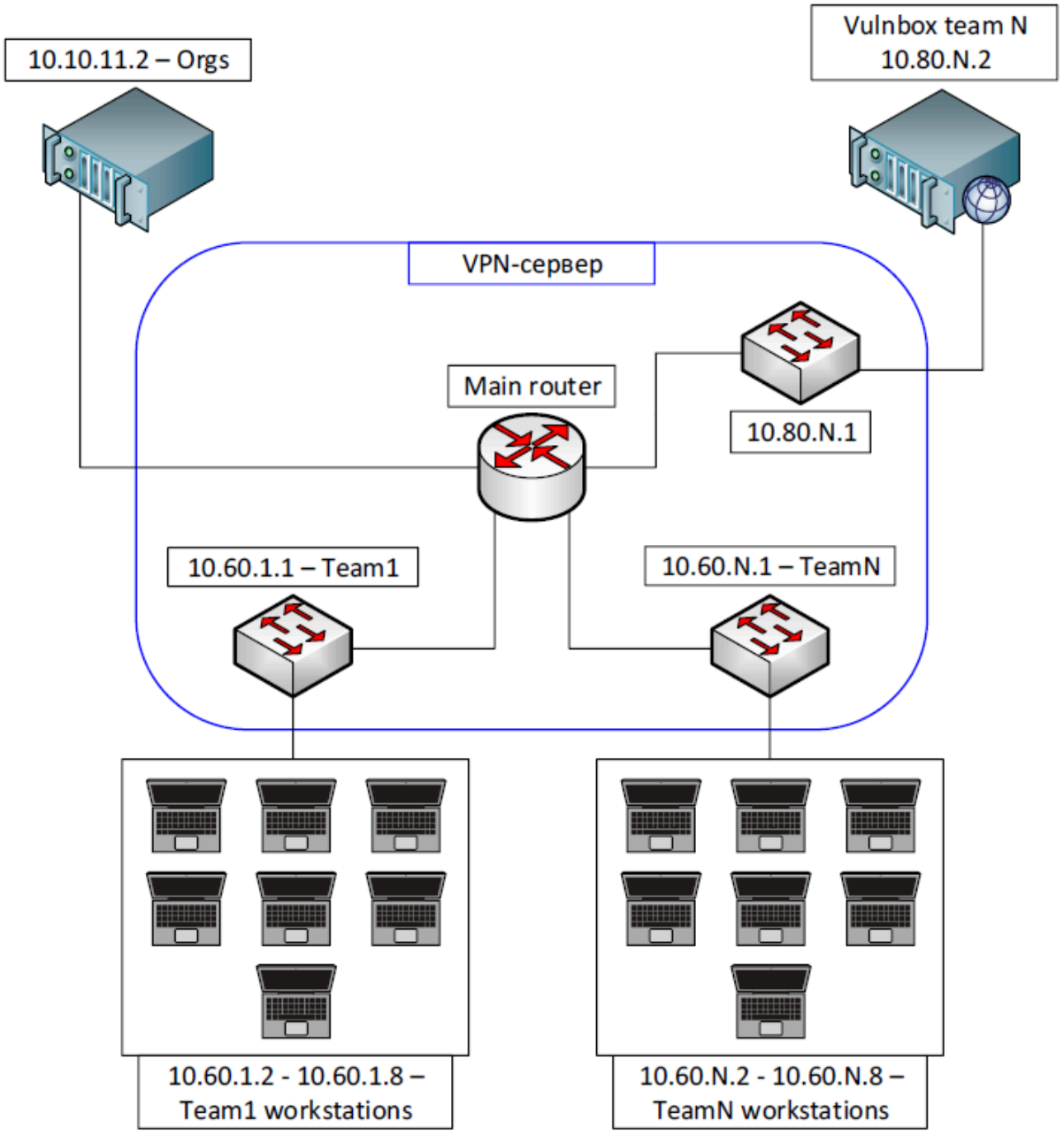
DestructiveFarm config

```
'SYSTEM_PROTOCOL': 'ructf_http',
'SYSTEM_URL': 'http://mctf.ru/flags',
'SYSTEM_TOKEN': '<token>',
```

How the network works

1. Network access is always open within one `teamN`
2. From `teamN` to `vulnN` at any time.

3. From `teamN` to `vulnN` in open network, `M ! = N`



Have a good game and good luck!

Clips how the Attack/Defense CTF works:

- https://www.youtube.com/watch?v=RkaLyji9pNs&t=238s&ab_channel=LiveOverflow
- https://www.youtube.com/watch?v=Uv5v60A2tL8&ab_channel=media.ccc.de