Instructions for teams participating in the Attack-Defense CTF ASICS 2024

1. Objectives of the Attack-Defense Competition

• Defense: Protect the services you are assigned from being attacked by the opposing team.

• Attack: Exploit vulnerabilities on other teams' systems to capture flags.

• Scores: You will receive points for keeping your flags safe and attacking to capture flags from other teams.

2. Accessing Your Systems and Environment

• Each team will be assigned their own Docker virtual machines where the services are running and the flags are protected.

• You will be provided with an SSH account “ctf” to log into your virtual machine and perform defensive actions.

• “ctf” account: This is the main account that you will use to access, monitor, and protect the system. However, this account has limited editing rights on some files and system configurations to ensure fairness.

How to log in to your team's Docker VM:

1/ Use SSH to log in to your VM: ssh ctf@[VM-IP]

2/ Enter the password provided for the ctf account.

3. Defense Tasks

<u>Protect Services and Flags:</u>

• Protect services: Your service can be a website, network service, or database. You need to monitor and protect them from attacks from the opposing team. Make sure these services are always running, without interruption.

• To check the status of the service, you can use the following command in the VM:

service [service name] status

• Protect flags: Flags are placed in a special file (usually /flag/flag.txt). Your team needs to protect this flag so that it cannot be obtained by other teams.

<u>Limitations of the “ctf” account:</u>

• The “ctf” account does not have access to or change system configuration files. You can only edit files belonging to the service you need to protect.

• You can modify the configuration files of the service and/or the firewall within the limits allowed to protect the services.

<u>Some typical defensive actions:</u>

• Fix vulnerabilities: Find and fix exploitable vulnerabilities in your service (e.g. patch security configuration, change service configuration).

• Configure firewall: Set up firewall rules to protect the service from untrusted IPs (depending on the challenge requirements, you will be granted/not granted permission to edit the firewall).

4. Attack Mission

Exploiting other teams' vulnerabilities:

• Your goal is to find and exploit vulnerabilities in the services of opposing teams. When you successfully exploit, you will be able to get their flag.

• The default flag is saved in the /flag/flag.txt file on the other team's virtual machine, unless there are other special rules.

Attack approaches:

• Exploitation: Use attack techniques based on service vulnerabilities (e.g. SQL Injection, Remote Code Execution).

• Flag capture: After successfully exploiting the other team's service, you will find the flag in the /flag/flag.txt file. Get the flag and submit it to the system to score the attack.

5. Flag Changing and Scoring System

• Automatic flag changing: The system will change the flag content after a certain period of time. Therefore, teams must continuously attack and protect the new flag.

• Defense points: Your service must always be active and the flag must be protected. If your service is down or attacked, you will lose points.

• Attack Points: Each time you capture a flag from an opposing team, you will receive attack points.

6. Restrictions and Rules

• Do not turn off the service: If you turn off the service to prevent another team from attacking, the system will detect it and you will lose points.

• Do not sabotage the system: Do not intentionally sabotage or crash another team's virtual machine other than to exploit vulnerabilities to capture flags.

• Respect the rules of the game: All actions must comply with the rules of the organizer. Any cheating or breaking of the rules will be strictly handled.

7. Recommended

• Divide the work: It is recommended to divide your team into two groups, one specializing in defense and one specializing in attack to optimize efficiency.

• Continuously check the service: Regularly check the status of your service to ensure that it is not successfully attacked by another team.

• Monitor flag changes: When the system changes flags, you need to quickly update your flag protection status and prepare for the next attacks.