Руководство для организаторов

1. Общие положения

Каждая задача (например, `forensic-a` ... `forensic-i`) представляет собой автономный сценарий, создающий набор артефактов и автоматически генерирующий уникальный флаг в формате

`forensic{<64-символьная_hex-строка>}`

Флаг формируется при запуске генератора задачи и сохраняется в служебный файл `.flag` внутри каталога задачи. Организаторы обязаны зарегистрировать значение флага в жюрейской системе до удаления артефактов.

2. Порядок генерации заданий

1. Подготовьте сервер или рабочую машину с инструментами: bash, python3, openssl и библиотека `scapy` (для задач, генерирующих pcap).
2. В каталоге проекта выполните скрипты-генераторы задач (пример):

   ```
   chmod +x forensic-*/generate.sh
   ./forensic-a/generate.sh
   python3 forensic-b/generate.py
   ```

   (имена скриптов могут отличаться; используйте соответствующие вашему проекту).
3. После выполнения в каждой папке появятся артефакты и служебный файл `.flag`.

3. Регистрация флагов

1. Прочитайте флаг из скрытого файла, например:

   ```
   cat forensic-a/.flag
   ```
2. Внесите значение флага в жюрейскую систему (CTFd, RootTheBox или аналог) *точно* в том виде, как оно записано — без пробелов и переносов.
3. Повторите операцию для каждой задачи, удостоверившись в уникальности каждого флага.

4. Удаление служебных данных

После того как все флаги внесены в жюрейскую систему, необходимо предотвратить возможность их восстановления:

1. Убедитесь, что флаги корректно зарегистрированы в системе приёма ответов.
2. Удалите файлы `.flag` с перезаписью содержимого. На сервере с GNU coreutils можно использовать:

   ```
   shred -u forensic-*/.flag
   ```

   Если `shred` отсутствует:

   ```
   dd if=/dev/zero of=forensic-a/.flag bs=1 count=$(stat -c%s
   forensic-a/.flag) && rm -f forensic-a/.flag
   ```
3. Проверьте отсутствие оставшихся скрытых файлов:

```
find . -type f -name ".flag"
```

Ожидается пустой вывод.

5. Контроль корректности заданий

Перед публикацией:

1. Запустите генераторы и убедитесь, что создаются ожидаемые артефакты (pcap, txt, tgz и т.п.).
2. Прогоните предоставленные решающие скрипты (например `solve_*.py` / `solve_*.sh`) на локальных артефактах, чтобы убедиться, что они восстанавливают флаг.
3. Упакуйте артефакты для публикации, убедившись, что `.flag` отсутствует в архиве:

```
tar -czf forensic-a.tar.gz forensic-a/
tar -tzf forensic-a.tar.gz | grep .flag  # не должно ничего выводить
```

6. Безопасность и хранение флагов

- Все флаги хранятся исключительно в системе оценки (жюрейской базе) до завершения соревнования.
- Запрещается разглашать или сохранять флаги в общедоступных местах (чатах, репозиториях и т.п.).
- После окончания соревнования рекомендуется полностью удалить рабочие каталоги генерации:

```
rm -rf /path/to/forensic-*
```

7. Рекомендации по публикации

1. Для публикации участникам предоставляйте только артефакты (архивы с логами/pcap/файлами). *Не включайте* исходные генераторы и скрытые файлы `.flag`.
2. В комплекте с задачей размещайте краткую формулировку `task.txt` и (опционально) контрольную сумму (SHA256) каждого архива для проверки целостности:

```
sha256sum forensic-a.tar.gz > forensic-a.sha256
```

3. В описании задачи оставляйте минималистичную подсказку, не раскрывающую метод извлечения флага.