

Второй тур заключительного этапа

1. Общие сведения

- Длительность: 6 часов.
- Формат: Взлом инфраструктуры (Pentest) с последующим составлением отчета.

2. Инфраструктура и доступ

- Участникам предоставляется доступ к двум виртуальным машинам (целевым хостам).
- Для начального доступа выдаются учетные данные (логин/пароль).
- Управление машинами (подключение, перезагрузка) и мониторинг рейтинга осуществляются через единую платформу соревнования.

3. Задача участников

- Провести тестирование на проникновение, получить привилегированный доступ к системам.
- Обнаружить и извлечь 10 флагов, размещенных на виртуальных машинах.
- Флаги могут располагаться в файлах или переменных окружения. Формат флагов обеспечивает их однозначную идентификацию.
- Распределение весов флагов: флаги уровня суперпользователя (root) стоят дороже пользовательского уровня (user). Точное расположение флагов на машинах заранее неизвестно.

4. Система оценки

- Баллы за флаги: начисляются согласно весу флага минус штраф по времени.
- Временной штраф: используется динамическая система оценки. За каждую минуту, прошедшую с начала соревнования до момента сдачи флага, из стоимости флага вычитается фиксированное количество баллов.
- Итоговая оценка: Суммарный счет конвертируется в 10-балльную шкалу.

5. Отчетность

Помимо сдачи флагов необходимо предоставить отчет о тестировании по утвержденному шаблону. Отчет должен содержать:

- Разведка (Reconnaissance): Определение границ тестирования, картография сети.
- Перечисление (Enumeration): Анализ активных сервисов и портов.
- Эксплуатация (Exploitation): Описание найденных уязвимостей, векторов атак, уровня критичности и использованных эксплойтов.
- Доказательства (PoC): Скриншоты, полученные флаги, доказательства получения доступа.
- Рекомендации: Меры по устранению уязвимостей (митигация/патчинг).

Задания второго тура заключительного этапа**VM 1 (хост внутри LAN)**

Закрепившись на одной из машин `vm2`, можно было начать сканировать сеть.

Например, `nmap` установлен в `jenkins`-контейнере. Запускаем

```
nmap 192.168.123.0/24
```

нашли наш `ip`-адрес (`192.168.123.14`)