360° Ampire

КОНФЕРЕНЦИЯ КИБЕРПОЛИГОНОВ

Вместе против цифровой уязвимости

24 апреля

г.Москва, Кибердом

360° Ampire

Как разработать уязвимый узел и довести его до прода

Ильин Антон Сергеевич,

Руководитель направления
Моделирования атак,
Перспективный мониторинг

Ampire 360°

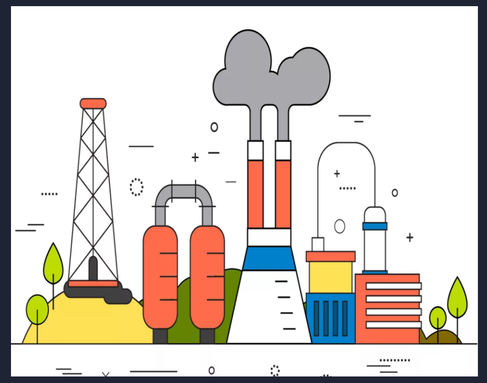
Киберполигон Ampire

Платформа киберполигона

Инфраструктура и шаблоны

Ampire – это учебно-тренировочная платформа, на базе которой можно реализовать цифровой двойник реальной инфраструктуры.

Модель инфраструктуры

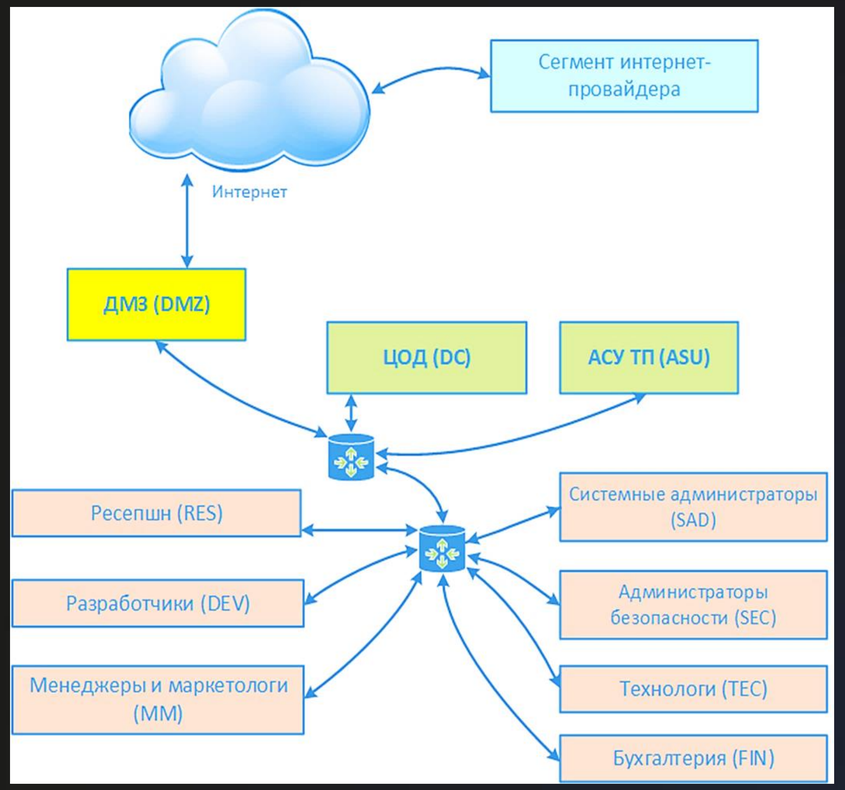


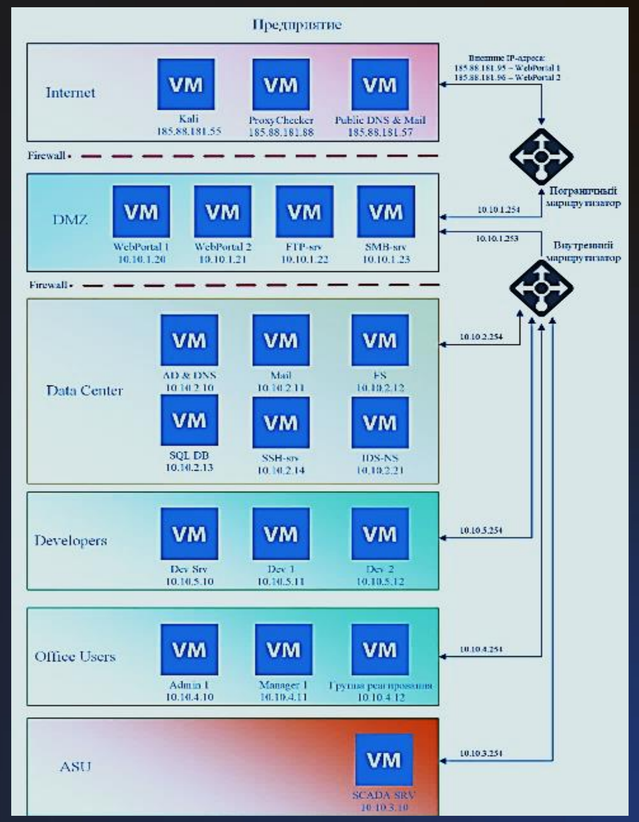
Средства обнаружения

Автоматизированный нарушитель

Модель инфраструктуры

Шаблон – набор виртуальных машин, логически объединенных и изолированных на уровне сети.

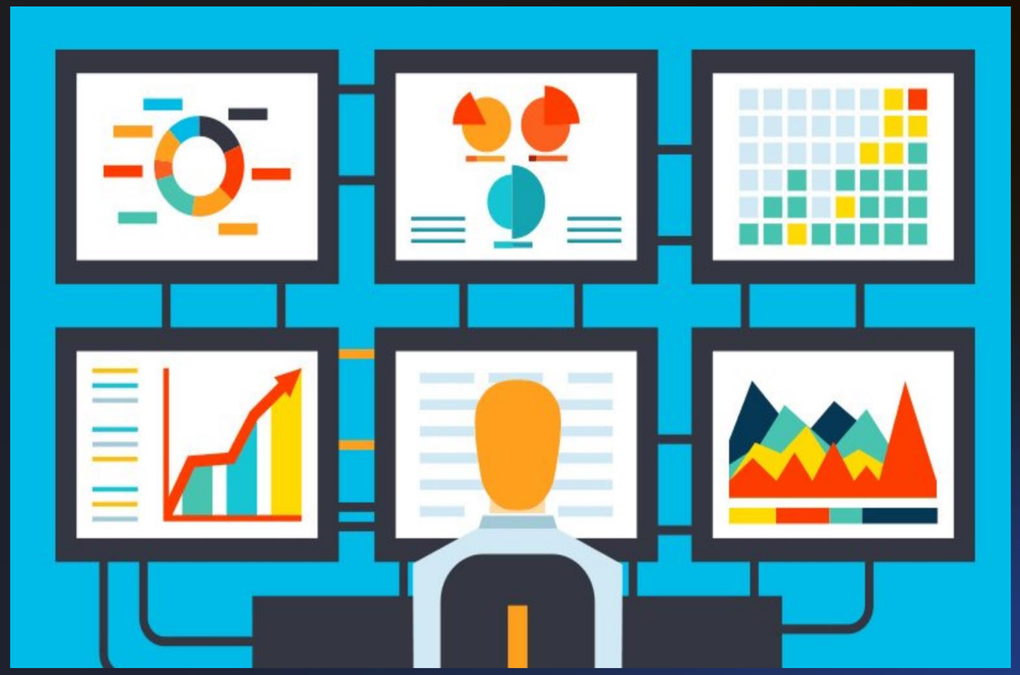




Средства обнаружения

Ampire дает возможность интеграции различных сетевых и хостовых сенсоров.

- ViPNet IDS NS
- ViPNet IDS HS
- ViPNet TIAS
- IDS/IPS Snort
- IDS/IPS Suricata
- ViPNet EndPoint Protection
- ELK
- Security Onion

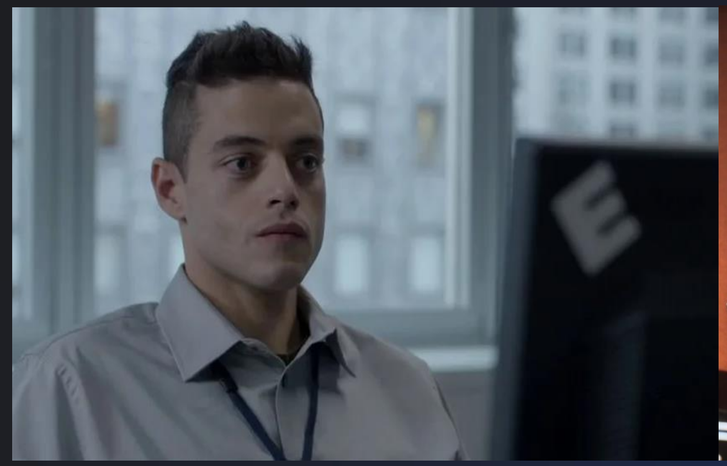


Автоматизированный нарушитель

Реализован на базе дистрибутива Kali linux. Киберполигон дает возможность трех вариантов размещения нарушителя в шаблоне:

Внешний нарушитель – действует из внешнего сегмента. Характер наглый.
Не женат.

Внутренний нарушитель – притворяется сотрудником компании. Характер скрытный.
Не женат.



Зараженный узел – узел из инфраструктуры шаблона, подвергшийся воздействию нарушителя или вредоносного ПО.

Развитие киберполигона

Этапы развития киберполигона

Первые версии киберполигона – один набор виртуальных машин, 6 базовых сценариев

Версия 1.1 – внедрение механизма **Конфигуратор**

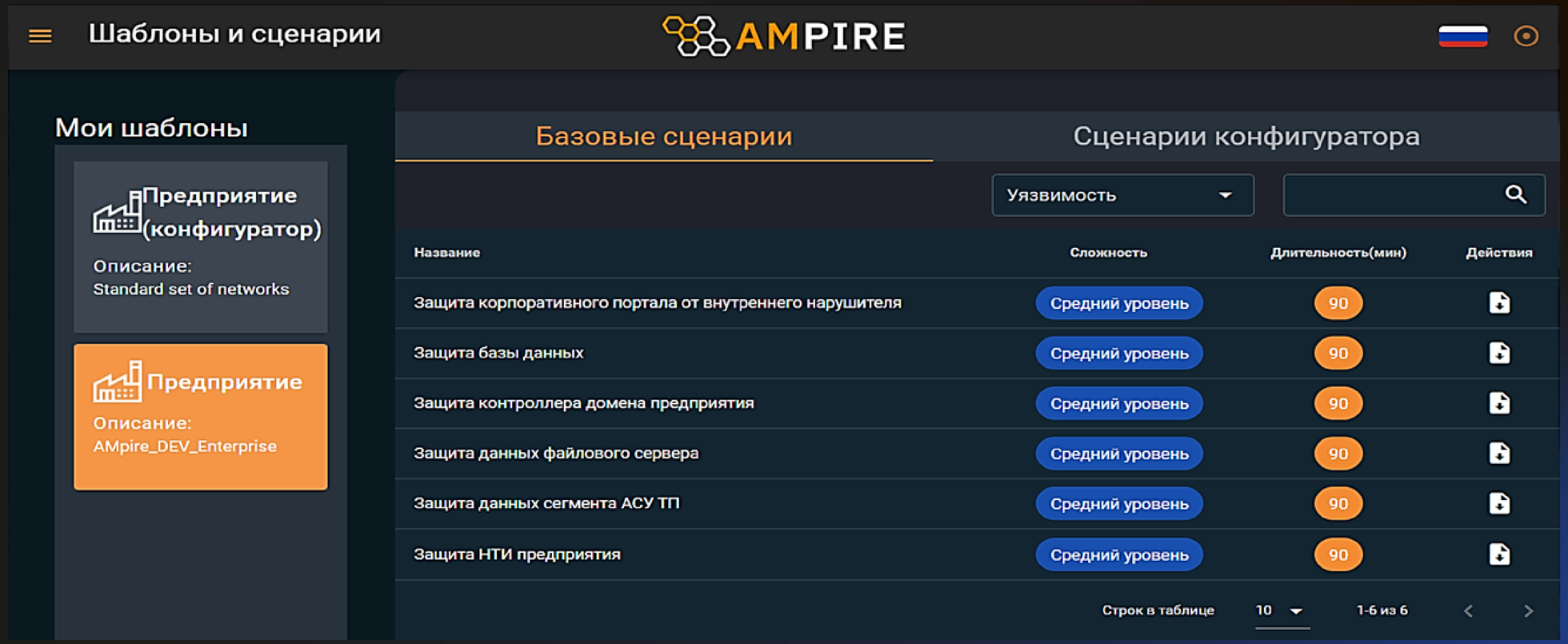
Версия 1.2 – добавлен режим **OSINT**

Версия 1.3 – добавлен режим **RedTeam**

Версия 1.4 – добавление двух базовых сценариев и режима **CSIRT**

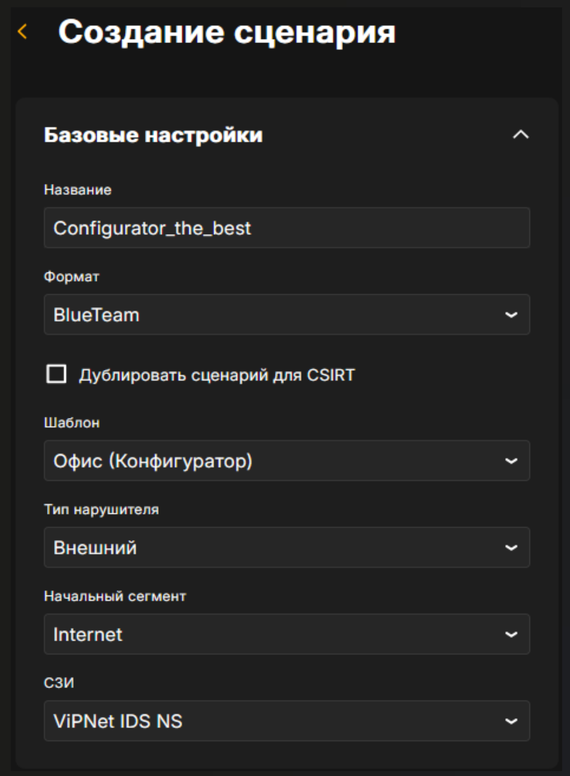
Базовые сценарии

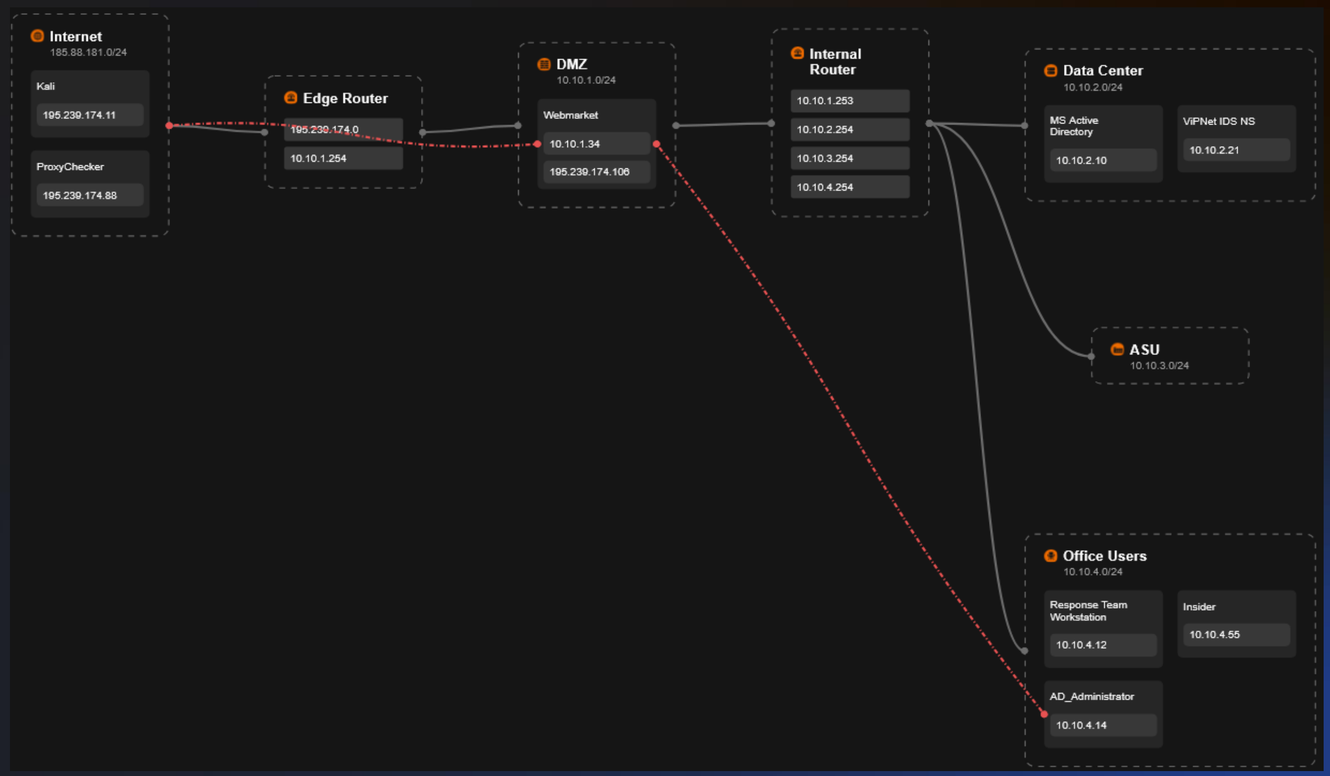
Базовые сценарии киберполигона



Конфигуратор

Идея конфигуратора – дать возможность преподавателю самостоятельно формировать вектор атаки и шаблон тренировки.





Уязвимый узел

Уязвимый узел – основной элемент любого сценария в киберполигоне.

- **Виртуальная машина**
- **Содержит 1 или более уязвимостей**
- **Содержит 1 или более последствий эксплуатации уязвимости**
- **Чекеры**
- **Документация в установленном формате**

Развитие нарушителя

Развитие конфигуратора и увеличение количества уязвимых узлов, потребовало развития и автоматизированного нарушителя.

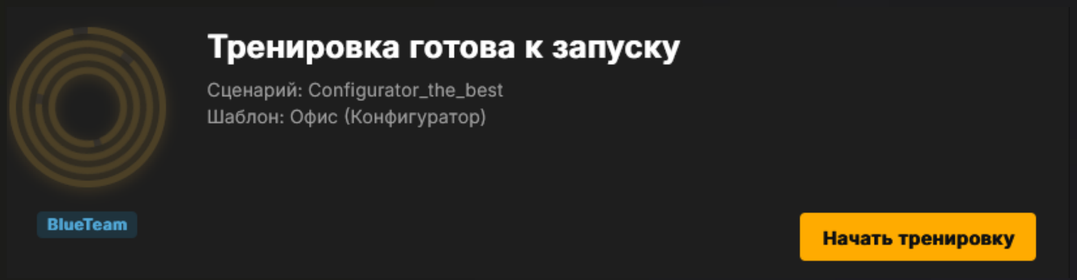
Нарушитель раньше:

- Запуск python-скрипта сценария

Нарушитель сейчас:

- Парсинг вектора атаки
- Запуск скриптов атаки и последствий по вектору
- Определение сетевой доступности уязвимого узла
- Модуль сканирования
- SSH - тунеллирование
- Проброс портов
- Отправка логов атаки
- От него не спрятаться

После нажатия “Начать тренировку”



- Вектор отправляется к нарушителю
- Определение доступности узла
- Запуск скрипта эксплуатации уязвимости и последствия уязвимого узла
- Определение расположения следующего узла
- Проброс портов через захваченный узел
- Эксплуатация уязвимости на следующем узле

Vector.json

```
{
  "actions": [
    {
      "action": "sql_injection_rce",
       "payload": “meterpreter",
      "scan": true,
      "stage": "SQL Injection RCE эксплуатация",
      "target": "195.239.174.106"
    },
    {
      "action": "exploit_coldfusion_misconfig",
      "payload": “crontab_backdoor",
      "scan": false,
      "stage": "ColdFusion эксплуатация",
      "target": "10.10.2.40"
    }
  ],
  "language": "ru",
  "sc_name": “Configurator_the_best",
  "type": "dynamic"
}
```

После нажатия “Начать тренировку”

Тренировка запущена. Производится атака 50%...

01:29:01

Сценарий: Configurator_the_best
Шаблон: Офис (Конфигуратор)

Vector.json

webmarket

...

sql_injection_rce

meterpreter

exploit_coldfusion

crontab_backdoor

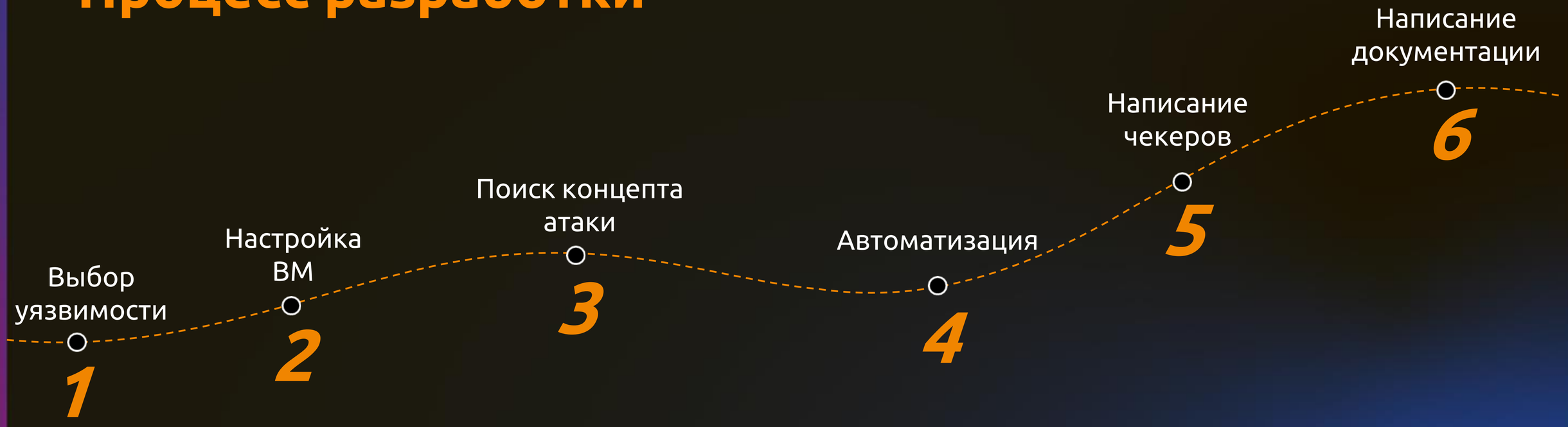
ColdFusion

Ampire 360°

Как разработать УУ для Ampire

Как разработать уязвимый узел

Процесс разработки



Ampire 360°

Выбор уязвимости

Критерии выбора уязвимости

- Актуальность
- Простота воспроизведения
- RCE
- Закрытие через правку кода
- Наличие модуля Metasploit или опубликован POC
- Свободное ПО

Ampire 360°

Выбор уязвимости

Ресурсы для поиска уязвимостей

CVE Details – большое количество фильтров, информация о том, существует ли для уязвимости эксплоит и модуль в Metasploit.

Репозиторий Poc-in-GitHub – автоматически обновляющаяся база, есть ссылки на Proof of Concept (PoC).

База данных rapid7 – содержит последние вышедшие модули для Metasploit.

Настройка виртуальной среды

Подготовка виртуального стенда

Для проверки найденного POC или msf-модуля нужно создать виртуальную инфраструктуру из двух машин в одной сети:

- Kali Linux
- ВМ с уязвимым сервисом

Ampire 360°

Автоматизация

Взаимодействие с metasploit

Фреймворк metasploit написан на Ruby и не поддерживает Python-скрипты по умолчанию.
Но существуют библиотеки, позволяющие взаимодействовать с remote procedure call (RPC) metasploit. М
ы используем библиотеку pymetasploit3.
После установки библиотеки, можем запустить RPC-listener.

msfrpcd -P Ampire -n -a 127.0.0.1

-P - password
-n - disable database
-a - bind IP address

Автоматизация

Библиотека pymetasploit3

Pymetasploit3 – библиотека python, позволяющая взаимодействовать с фреймворком metasploit.

Полезные классы библиотеки:

MsfRpcClient — класс библиотеки для взаимодействия с RPC фреймворка.

MsfConsole — класс, который обеспечивает взаимодействие с консолью метасплойта.

Run_module_with_output — метод класса, при помощи которого осуществляется исполнение выбранного модуля атаки и пэйлоада.

Скрипт проверки статуса

Написание чекера

После автоматизации атаки на уязвимый узел необходимо написать скрипт-чекер.

Чекер проверяет статус уязвимости и пэйлоада на узле и возвращает словарь, в котором ключи – названия уязвимости и пэйлоада, а значения – их статусы в виде булевых значений True или False.

{“vuln”: True, “Payload”: False}

- True – уязвимость плагина wpdiscuz не устранена
- False – пэйлоад meterpreter устранен

Документация

Написание сопроводительной документации

- Описание уязвимого узла
- Условия эксплуатации уязвимости
- Описание хода атаки
- Способы обнаружения эксплуатации уязвимости и реализации последствий средствами ОС и СЗИ
- Способы закрытия уязвимости
- Описание применяемых последствий и способов их нейтрализации
- Список использованных средств разработки: библиотеки, версии ПО и пр.

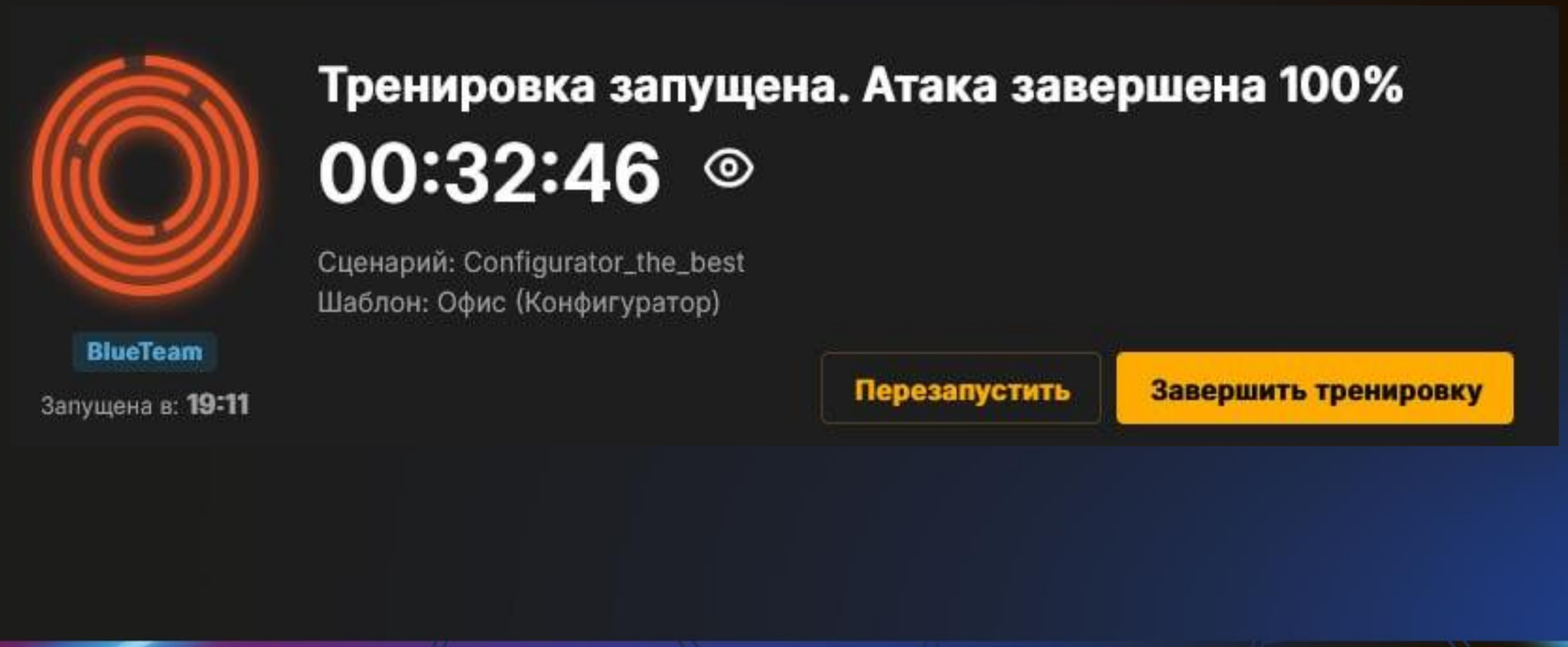
Сообщество Ampire

Разработка узлов в сообществе

1. Вступаете в сообщество Ampire
2. Предоставляете список уязвимостей для разработки
3. Одобрения командой Ampire одной из предложенных уязвимостей
4. Предоставляется доступ к git-репозиторию со вспомогательными скриптами и материалами
5. После разработки выгружаете узел на предоставленное облако
6. Узел попадает к команде разработки для интеграции в киберполигон
7. Вы попадаете в зал славы Ampire

Ampire ждет уязвимые узлы

Конец


Тренировка запущена. Атака завершена 100%
00:32:46
Сценарий: Configurator_the_best
Шаблон: Офис (Конфигуратор)
BlueTeam
Запущена в: 19:11
Перезапустить
Завершить тренировку

360° Ampire

Благодарю за внимание!