Киберполигон Ampire

Российская платформа для тренировки специалистов по обеспечению информационной безопасности

Сергей Нейгер
Перспективный мониторинг

Атакуют, обязательно атакуют

Хулиганы

Криминал

Наемники

Кибервойска

Проактивная позиция

Не можем повлиять

- Сам факт атаки.
- Квалификация атакующего.
- Инструментарий.
- Объем ресурсов.

Можем повлиять

- Стоимость атаки.
- Скорость реакции.
- Содержание реакции.
- Собственный опыт.
- Планы и изменения.

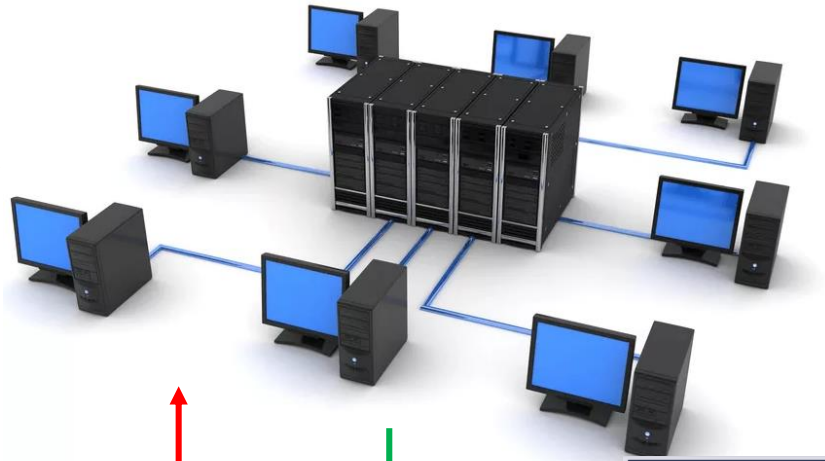
Способность действовать в экстренной ситуации зависит не от уровня знаний, а от уровня подготовки

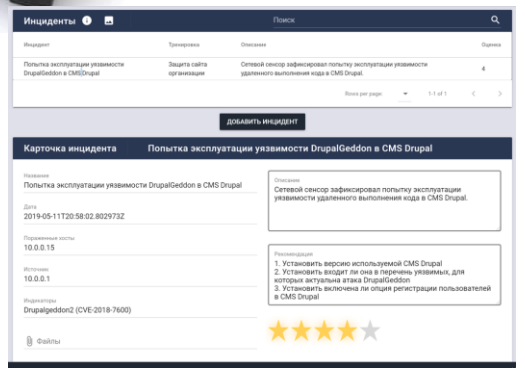
Целевая аудитория

- Школьники и студенты с базовым знанием TCP/IP сетей, которые планируют работать в сфере защиты информации.
- ИБ-специалисты, которые хотели бы выделиться среди других кандидатов глубокими знаниями в определенных областях.
- ИТ-специалисты: новички и те, кто хотел бы увеличить перечень навыков в резюме.

AMPIRE

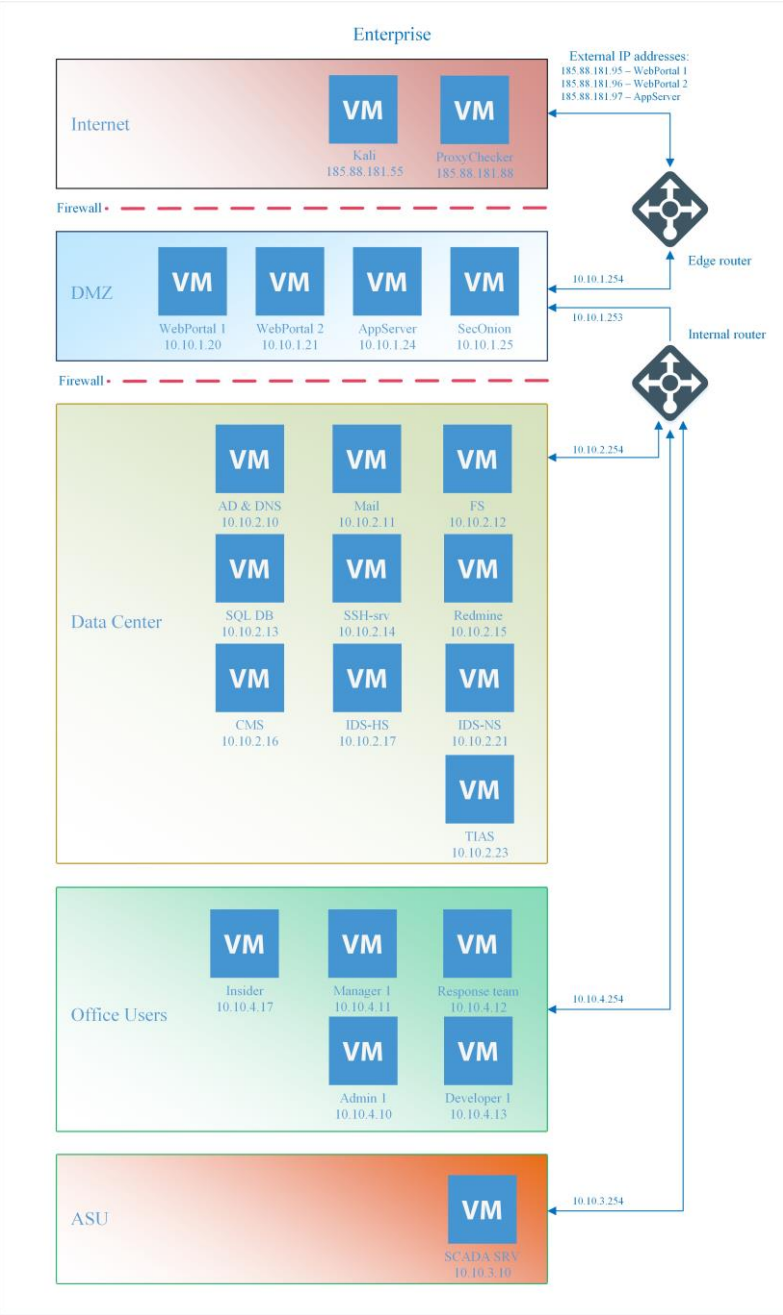
Наша учебно-тренировочная платформа содержит сценарии различной сложности для проведения киберучений, сертификационных тестов и отработки необходимых навыков.





Группа мониторинга

Группа реагирования



← Этот по умолчанию.

Можем сделать кастом.

Базовые сценарии киберучений

- Защита базы данных предприятия.
- Защита контроллера домена предприятия.
- Защита файлового сервера предприятия (MS17-010).
- Защита данных сегмента АСУ ТП.
- Защита научно-технической информации предприятия.
- Защита корпоративного портала от внутреннего нарушителя.

СЗИ

ViPNet IDS NS

ViPNet IDS HS

ViPNet TIAS

IDS/IPS Snort

IDS/IPS Suricata

ELK

Security Onion

И почти любые другие

Типы проводимых занятий

- Киберучения.
- Анализ защищённости и аудит ИТ-инфраструктуры виртуальной организации.
- Противодействие группе реальных нарушителей (концепция Red Team и Blue Team).
- Лабораторные работы по настройке средств безопасности и прикладных сервисов.
- Киберквесты.

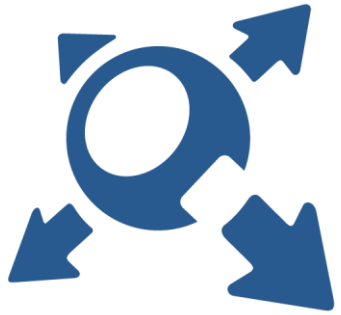
Минимум для участия

- Начальное знание сетевых технологий и TCP/IP стека.
- HTTP и основы построения веба.
- Основные типы компьютерных атак и уязвимостей ПО.
- Базовые знания по работе операционных систем.
- Принципы криптографической защиты информации, концепции симметричного и ассиметричного шифрования.

Навыки после прохождения курса

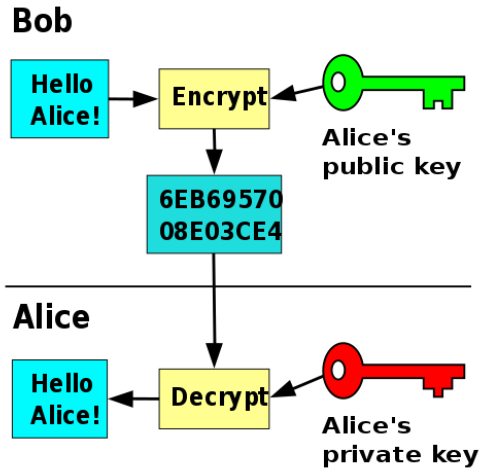
- Основные меры защиты сети, их преимущества и недостатки.
- Практика работы со средствами обнаружения вторжений (просмотр и фильтрация событий, правила выявления и реагирования на критичные события).
- Основные уязвимости веб-приложений и способы эксплуатации.






Навыки после прохождения курса

- Практика защиты веб-ресурсов при помощи WAF и исправления уязвимостей.
- Основные типы угроз для ОС и навыки защиты ОС.
- Средства защиты конечных точек.
- Криптографическая защита конфиденциальных данных при передаче и хранении.
- Навыки защиты технологический сетей.



Ключевые преимущества Ampire

- Полная независимость пользователя в проведении киберучений.
- Практические занятия для ИБ- и ИТ-специалистов любого уровня подготовки на «**двойнике**» реальной инфраструктуры.
- Полностью **автоматические сценарии атак**, разработанные экспертами по пентестам и базирующиеся на реальных инцидентах.
- Возможность создавать собственные сценарии по различным видам атак для ИТ-, ИБ-служб, операторов АСУТП, офиса, руководства.
- Подтверждение компетенций и развитие навыков группы реагирования на компьютерные атаки.
- ИТ-инфраструктура, СЗИ – все вместе на одной платформе!

Акция «За безопасность!»

Лицензии на перечисленные продукты предоставляются **на безвозмездной основе** на 6 месяцев!!!

Защита каналов связи	Системы управления и мониторинга	Защита рабочих станций и серверов	Обнаружение и предотвращение компьютерных атак
• ViPNet Coordinator VA • ViPNet xFirewall VA • ViPNet TLS Gateway VA • ViPNet PKI Client • ViPNet Client	• ViPNet Administrator • ViPNet Policy Manager	• ViPNet SafeBoot • ViPNet SafePoint • ViPNet IDS HS*	• ViPNet TIAS VA • ViPNet IDS MC VA • ViPNet IDS NS VA • ViPNet IDS HS*

Перевод отдела технической поддержки на усиленный режим работы и предоставление консультаций по подбору оптимальных решений для обеспечения информационной безопасности в рамках импортозамещения. Для получения консультации вы можете отправить электронное письмо с вопросами и контактными данными на адрес sos@infotecs.ru.

Спасибо за внимание!

И давайте посмотрим Ampire

Сергей Нейгер

Директор по развитию бизнеса компании
«Перспективный мониторинг»

Sergey.Neyger@amonitoring.ru

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news