Методическое и техническое обеспечение практической части обучения специалистов ГосСОПКА в МТУ

Московский технологический университет

к.ф.-м.н. Зязин Андрей Валентинович
к.т.н. Тимаков Алексей Анатольевич
Жанкевич Антон Олегович

Что сделано

Создана учебно-методическая и материальная база для обучения специалистов ГосСОПКА

Реализуется подготовка специалистов по противодействию КА в рамках специальности «Компьютерная безопасность» (специализация «Анализ безопасности компьютерных систем»)

Введены курсы повышения квалификации по направлениям: анализ защищенности информационной системы и информационно-телекоммуникационной сети предприятия; мониторинг компьютерных атак

Формируемые навыки

- проведение технического анализа безопасности сетевой инфраструктуры;
- проведение технического анализа безопасности Web-приложений и баз данных;
- использование автоматизированных средств оценки защищенности компьютерных систем;
- выполнение основных мероприятий по развертыванию, настройке и подготовке к работе инфраструктуры обнаружения компьютерных атак (и управления событиями безопасности в сети предприятия (организации) ;
- настройка взаимодействия IDS с SIEM системами, а также с другими средствами защиты информации в контексте мониторинга компьютерных инцидентов;
- проведение первичных мероприятий по реагированию на компьютерные атаки;
- анализ сетевого трафика, циркулирующего в защищаемой информационной системе.

Перспектива

Курсы повышения квалификации по направлениям: Анализ защищенности мобильных приложений (IOS и Android) и Web – приложений; анализ защищенности АСУ ТП.

Курс повышения квалификации в формате комплексного учения – набор занятий практической направленности, в ходе которых слушатели не получают новых теоретических знаний, а совершенствуют свои навыки, выполняя задания в соответствии с заданным сценарием.

Примерные сценарии

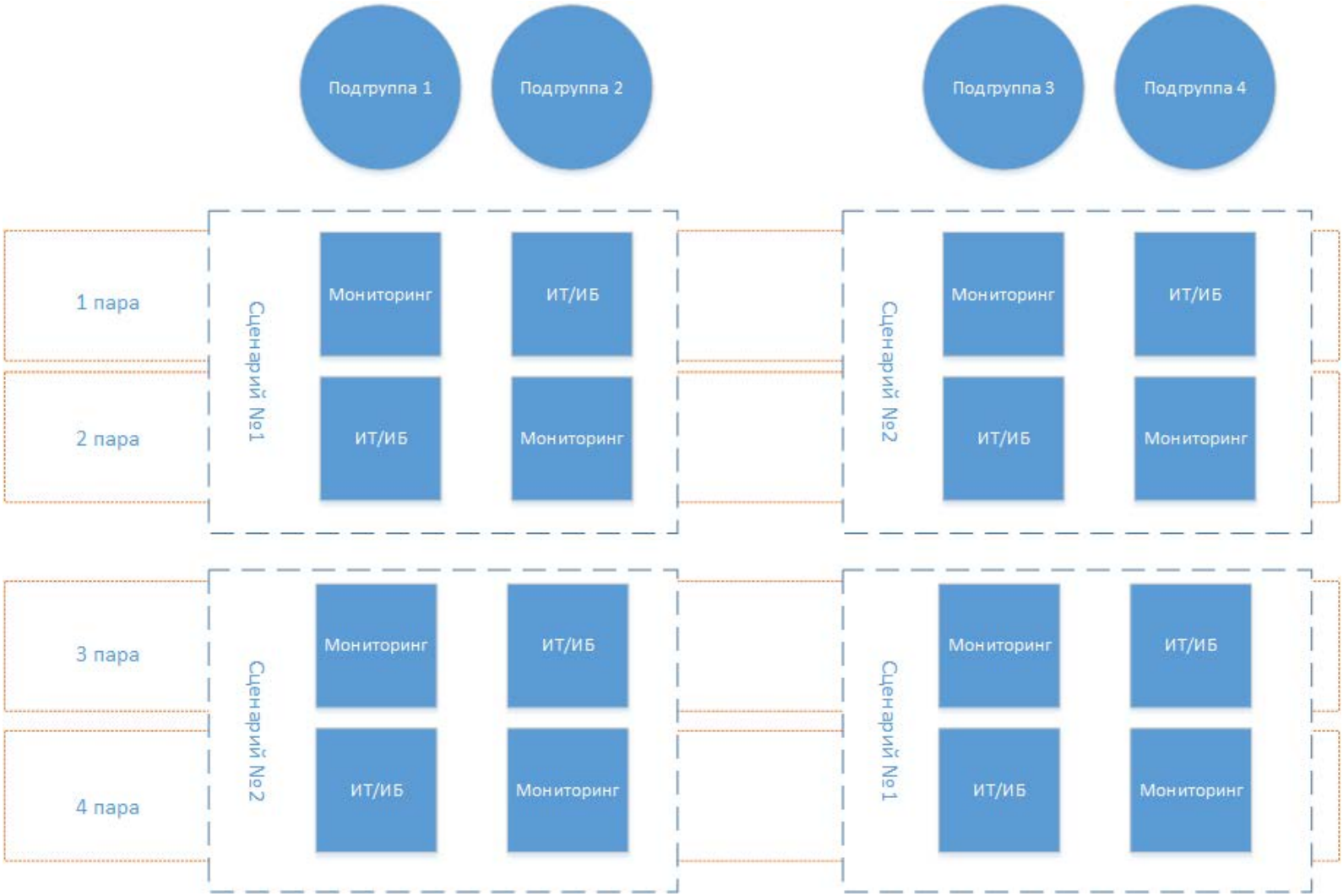
Базовые сценарии:

- Захват контроллера домена предприятия (DMZ → AD)
- Захват машины системного администратора (Почта → АРМ Администратора)
- Атака на программное обеспечение бухгалтерии (мобильное приложение → ПО бухгалтера)
- Фальсификация показания датчиков индустриального оборудования (внутренний нарушитель → сегмент АСУ ТП)

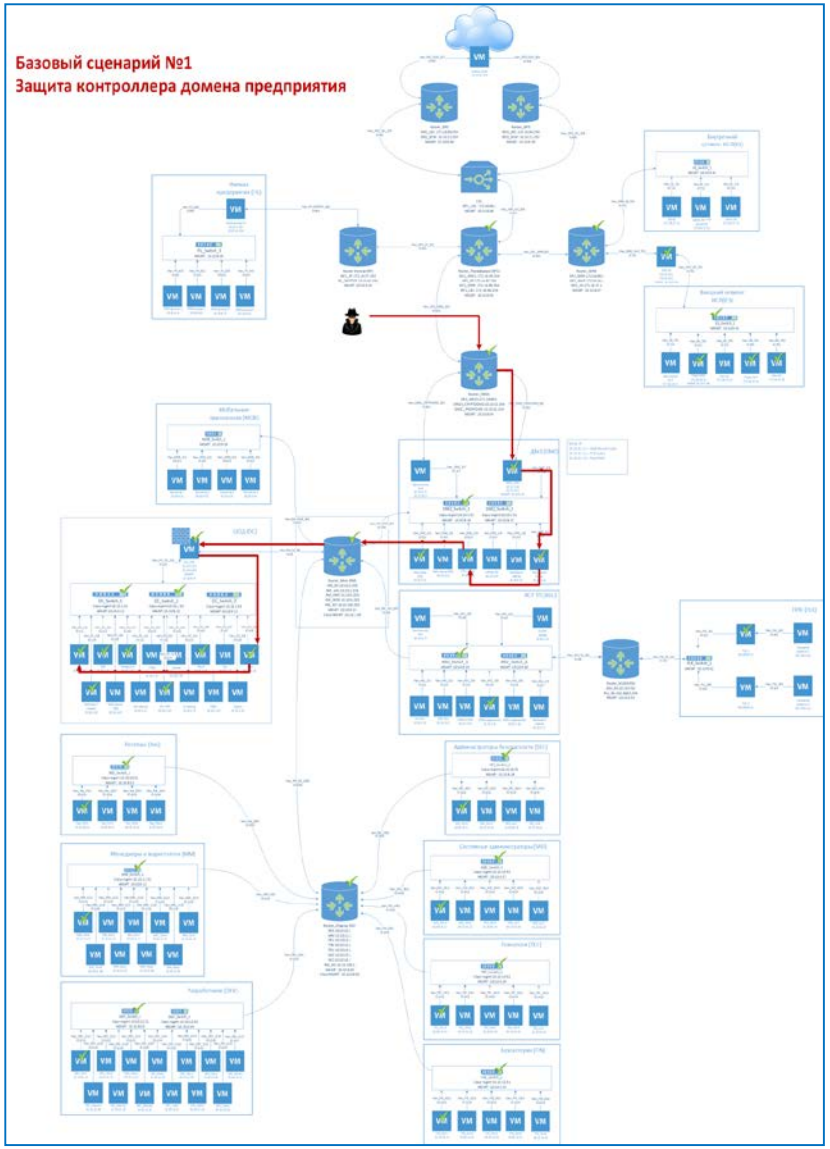
Комплексные сценарии:

- Захват центрального маршрутизатора предприятия
- Компрометация баз данных различных отделов предприятия

План учебного дня



Пример. Действия нарушителя.




```
┌─[root@parrot]─[/home/researcher/Documents/CyberPolyghon]
└──╼ #python simple_attack.py
[*] Configure nmap for scanning...

nmap -sV -p 1-1024 -oX - 10.0.9.41

[*] Start nmap scanning...

        port : 22 state : open
        port : 80 state : open
        port : 443 state : open

[*] Analysis scan result...
```

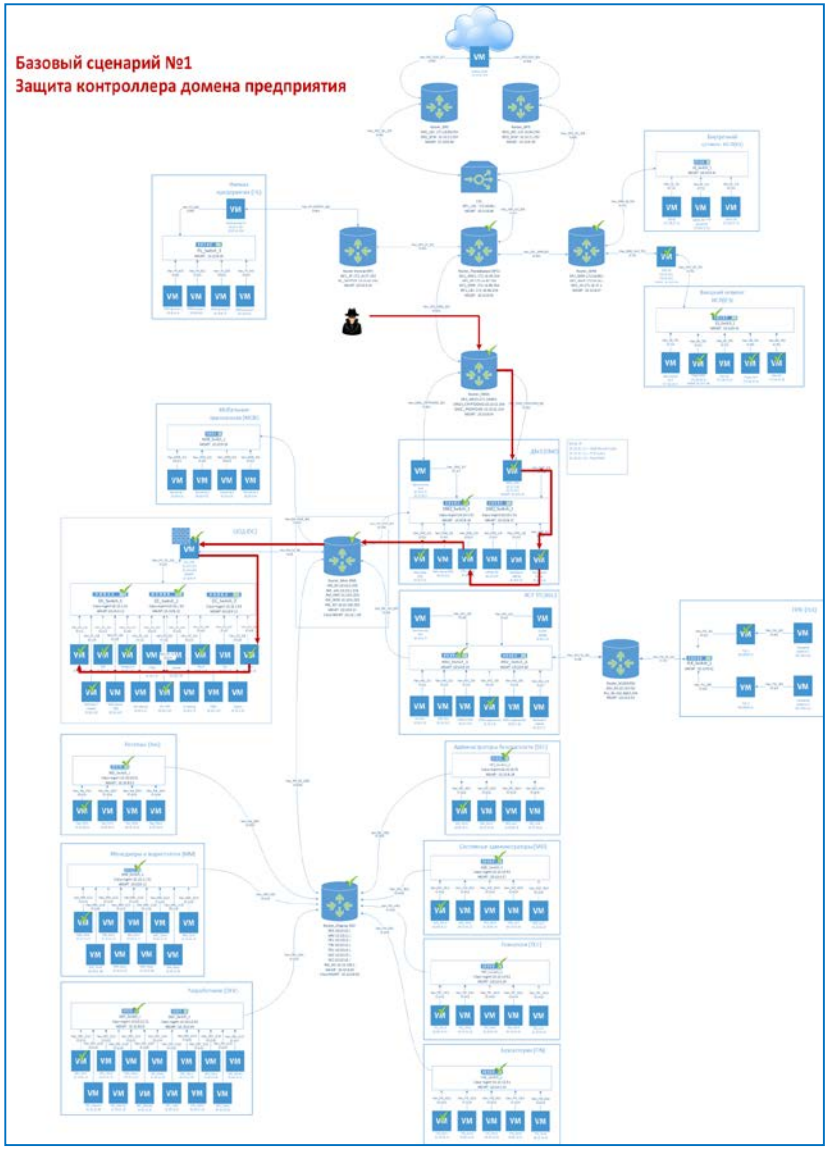
Результат атаки

Stage1	Waiting for attacks	Успех
Stage2	Scanning port	Успех
Stage3	Scanning port completed	Успех

Описание сценария/действий робота внешнего нарушителя:

- Робот сканирует порты веб-сервера организации и находит открытый 80 порт;
- Робот сканирует директории веб-сервера и находит директорию с компонентом, который позволяет выполнить сторонний код;
- …
- …
- С позиции почтового сервера робот подключается к контроллеру домена, используя перехваченный пароль администратора домена.

Пример. Действия учебных групп



Мониторинг:

- Зафиксировать сканирование портов на web-сервере. Сообщить команде реагирования о проводимой атаке;
- …
- …
- Завести инциденты;
- Предложить корректирующие и коррективные действия.

ИТ/ИБ:

- Получив информацию о попытке аутентификации на контроллере домена с почтового сервера от команды мониторинга, ограничить перечень узлов, с которых можно аутентифицироваться на контроллере домена;
- …
- Получив информацию о сканировании портов на web-сервере компании, осуществить проверку на доступность служебных сервисов из сети Интернет.

А как же CTF?

CTF	Комплексные учения по отработанным сценариям
Анализ защищенности web-приложений	**CTF**
Анализу защищенности мобильных приложений	Анализ текущего состояния документации инфраструктуры предприятия
Анализу защищенности АСУ ТП	Рекомендации по настройке существующих СЗИ в инфраструктуре предприятия
Анализу сетевого трафика	Настройка и подключение к инфраструктуре предприятия элементов СЗИ
Активное сканирование ресурсов	Порядок фиксация КИ
Реверс инжиниринг программного обеспечения	Рекомендации по внесению изменений в существующие регламенты предприятия
	Реагирование на КИ в реальном времени
	Процедура обмена информации о КИ между организациями и ЦМ ГосСОПКА

Базовая кафедра № 252
Института кибернетики
Московского технологического университета

ziazin@mirea.ru