KOMRAD Enterprise SIEM 4.5 · Практика НОУ ДПО «УЦБИ "МАСКОМ"»

Практическая работа: три варианта

Общие правила

- Работайте только в учебных виртуальных машинах.
- Не используйте реальные учетные записи, персональные данные и рабочие системы.
- Все IP-адреса заменяйте на адреса своего стенда.
- В отчете фиксируйте факт, действие, результат в KOMRAD и вывод.
- Перед установкой KOMRAD подготовьте VirtualBox, Extension Pack, VM с Astra Linux 1.7/1.8 и сеть между VM.

Вариант 1. Теоретический минимум

Подходит, если не хватает ресурсов VM или установка не успела завершиться.

Задания:

1. Прочитайте раздаточный конспект.
2. Откройте официальную страницу продукта: https://npo-echelon.ru/komrad-siem/
3. Откройте документацию 4.5.X: https://docs.etecs.ru/komrad/docs/intro/
4. Из папки ГОСТов прочитайте названия и назначение документов 59547, 59548, 59709-59712.
5. Составьте таблицу: "этап SIEM" -> "какой ГОСТ помогает обосновать".
6. Ответьте письменно: какие события Windows и Linux вы бы обязательно собирали в организации и почему.

Результат: заполненный отчет без установки.

Вариант 2. Основной: KOMRAD + Windows

Цель: установить KOMRAD, подключить Windows-источник и увидеть события.

Шаги:

1. Подготовьте VM с Astra Linux 1.7 или 1.8 для KOMRAD в VirtualBox.
2. Получите демоверсию на странице продукта или используйте локальный учебный комплект.
3. Установите KOMRAD 4.5, используя фактическое имя `.run` файла из полученного дистрибутива:

```
chmod +x ./ИМЯ_ФАЙЛА_УСТАНОВЩИКА.run
sudo ./ИМЯ_ФАЙЛА_УСТАНОВЩИКА.run
```

Примеры:

```
chmod +x ./komrad_v4.5.22_astra_1.7_amd64.run
sudo ./komrad_v4.5.22_astra_1.7_amd64.run

chmod +x ./komrad_v4.5.22-demo_astra_1.8_amd64.run
sudo ./komrad_v4.5.22-demo_astra_1.8_amd64.run
```

4. Активируйте лицензию по инструкции преподавателя или вендора.
5. Откройте `https://KOMRAD_IP`.
6. Импортируйте образ Windows 10 в VirtualBox и проверьте `ping KOMRAD_IP`.
7. На Windows VM установите WMI-агент из полученного демо-комплекта от имени администратора.
8. В KOMRAD включите WMI-агент и настройте сбор журнала `Security`.
9. Сгенерируйте события:

```
net user komrad_lab P@ssw0rd! /add
net localgroup Administrators komrad_lab /add
net user komrad_lab NewP@ssw0rd!
wevtutil cl Security
```

10. Найдите события в "Событиях в реальном времени".
11. Опишите, какие события выглядят рутинными, а какие подозрительными.

Результат: отчет с событиями Windows.

Вариант 3. Продвинутый: KOMRAD + Windows + Linux

Цель: подключить два разных типа источников и сравнить события.

Выполните все шаги варианта 2, затем добавьте Linux VM.

Шаги для Linux:

1. Создайте или импортируйте вторую Linux/Astra VM в VirtualBox.
2. Проверьте сеть: Linux должен видеть `KOMRAD_IP`.
3. Настройте отправку syslog/auditd по методике преподавателя или документации.
4. Сгенерируйте события:

```
logger "KOMRAD lab: test syslog message from Linux source"
sudo useradd komrad_lab
sudo passwd komrad_lab
su - komrad_lab
ssh wronguser@localhost
sudo systemctl restart ssh
```

5. Найдите события Linux в KOMRAD.
6. Сравните Windows и Linux:

Вопрос	Ответ
Какой источник подключался проще?	
Какие события понятнее после нормализации?	
Какие события можно считать признаками инцидента?	
Что нужно настроить дополнительно в реальной организации?	

Результат: отчет с событиями Windows и Linux, выводами и минимум одним предложением по улучшению мониторинга.