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

Памятка: стенд KOMRAD в VirtualBox

Что вы будете делать

1. Установить VirtualBox.
2. Установить Extension Pack той же версии, что и VirtualBox.
3. Подготовить VM с Astra Linux 1.7 или 1.8.
4. Скачать демо-версию KOMRAD Enterprise SIEM 4.5 у вендора или получить файл от преподавателя.
5. Установить KOMRAD в Astra Linux.
6. Импортировать Windows 10 в VirtualBox.
7. Подключить Windows 10 как источник событий.
8. В продвинутом варианте добавить вторую Linux/Astra VM.

Сеть VirtualBox

Все VM должны видеть друг друга по IP:

- KOMRAD VM;
- Windows 10 VM;
- Linux/Astra VM, если выполняете продвинутый вариант.

Проверьте в Linux/Astra:

```
ip a
ping -c 3 KOMRAD_IP
```

Проверьте в Windows:

```
ipconfig
ping KOMRAD_IP
```

Если VM не видят друг друга, сначала исправьте сеть VirtualBox. Без сети события не попадут в SIEM.

Установка KOMRAD

Используйте фактическое имя файла, который вы получили от вендора или преподавателя.

Шаблон:

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

Пример для Astra Linux 1.7 из документации:

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

Пример из локального учебного комплекта для Astra Linux 1.8:

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

После установки откройте в браузере:

```
https://KOMRAD_IP
```

Если браузер предупреждает о сертификате, в учебном стенде это ожидаемо. Преподаватель отдельно покажет, как импортировать корневой сертификат, если это понадобится.

Windows 10 источник

1. Импортируйте образ Windows 10 в VirtualBox.
2. Проверьте сеть до KOMRAD.
3. Установите WMI-агент от имени администратора.
4. В KOMRAD включите WMI-агент и настройте сбор журнала `Security`.
5. Сгенерируйте события:

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

Команда `wevtutil cl Security` очищает журнал Security. Выполняйте ее только в учебной VM.

Linux/Astra источник

Для первого теста используйте безопасное сообщение:

```
logger "KOMRAD lab: test syslog message from Linux source"
```

Затем можно сгенерировать учетные события:

```
sudo useradd komrad_lab
sudo passwd komrad_lab
su - komrad_lab
sudo -l
ssh wronguser@localhost
```

Если SSH в вашей Linux VM не установлен или не запущен, пропустите SSH и зафиксируйте это в отчете.

Что обязательно записать в отчет

- IP-адрес KOMRAD.
- IP-адрес Windows 10.
- IP-адрес Linux/Astra, если был.
- Какой установщик KOMRAD использовали.
- Какие события сгенерировали.
- Какие события увидели в KOMRAD.
- Какие проблемы возникли и как вы их проверяли.