OTUS

Безопасность Linux

Курс про обеспечение комплексной безопасности локальной и сетевой инфраструктуры, построенной на базе Linux

Длительность курса: 112 академических часов

1 Введение

1 **Знакомство**

— введение в проблематику — что такое ИБ, зачем, почему. Как ИБ затрагивает процессы системного администрирования;
— рассказ о модулях курса;
— демонстрация инструментов. Какие будут использоваться, откуда их взять, как с ними работать.

Домашние задания

1 ДЗ 1 “Знакомство”

Цель: Установить необходимое для работы ПО

Требования к рабочему месту:

ОС: macos или любой linux. В случае windows крайне рекомендуется создать рабочую vm (далее admin-vm) с linux на борту (+gui) и перенести выполнение всех работ на неё.
RAM: не менее 8gb, оптимально 16gb

Установить необходимое для работы ПО:
vagrant (в случае схемы admin-vm ставить на основной хост)
virtualbox (в случае схемы admin-vm ставить на основной хост)
ssh client
curl
ide, например pycharm

2 Потенциальные цели для атаки со стороны злоумышленников

1 **Разведка**

— уязвимость, атака, эксплойт;
— типичные сценарии проведения атак;
— классификация сетевых атак (авторское);
— классификация сетевых атак (MITRE);
— детали процесса сбора информации (reconnaissance).

Домашние задания

1 Разведка

Цель: исследование публичных источников для сбора информации об организации

https://github.com/bykvaadm/OS/tree/master/webvulns/lab1

---

2 **Сканирование**

— вспоминаем модель tcp\ip + Wireshark;
— пробуем на сканеры типа nmap, openvas на подготовленной виртуалке.

Это занятие направлено на то, чтобы в целом пощупать руками со стороны злоумышленника, чем наши сервера торчат наружу, и какие данные мы можем собрать, зная IP-адрес сервера.

Домашние задания

1 ДЗ 2 “Сканирование и разведка”

В данном дз предлагается выполнить 2 задачи:
1) используя навыки с занятия по разведке попробовать “нарыть” данных о текущей организации слушателя. Предполагается 2 сценария работы - минимальный пердполагает что каждый ищет информацию о своей организации, со “звездочкой” - каждый желающий может выдать стартовую информацию о своей организации и любой желающий может осуществить поиск. В конце данные сравниваются и дополняются для полноты картины об организации. Подробно описано тут:
https://github.com/bykvaadm/OS/tree/master/webvulns/lab1

2) Используя навыки по сканированию и проведенной разведке рассмотреть следующие варианты:
Просканировать собственную организацию
Просканировать учебный образ
Подробности по ссылке:
https://github.com/bykvaadm/OS/tree/master/webvulns/lab3

2 сканирование

https://github.com/bykvaadm/OS/tree/master/webvulns/lab3

3 Программное обеспечение

1 **Как ставить ПО**

— удивительно, но через репозитории. Что это такое?
— Pin версий — неизбежный конфликт;
— автоматические обновления;
— проверка подписи;
— удаление лишних программ;
— синхронизация времени;
— настройка криптографического профиля FIPS на всей системе.

Домашние задания

1 ДЗ 4 “ПО”

Цель: В этом дз предлагается создать подготовленный для будущего распространения vagrant box.

\Симулируем предподготовленный образ который будет распространяться как основа для образов организации.
Собираем список обязательного программного обеспечения и их версии
Настраиваем автоматическое обновление
Настраиваем apt-cacher-ng
Разбираемся с пиннингом
Настраиваем ntp
Настраиваем fips

4 Файловые системы и шифрование данных

1	**Требования к файловой системе**	— а что такое файловая система? — настройка неиспользуемых файловых систем; — права доступа до критичных системных файлов; — создаем белые списки пользователей, которые могут использовать at и cron; — поиск и настройка доступа к файлам.
2	**Пакеты openssl и stunnel**	— про криптографию и шифры; — научимся приемам шифрования отдельных сетевых соединений, файлов, каталогов и разделов ОС.
3	**Использование серверных и клиентских сертификатов на примере Web-приложения на базе nginx+MySQL+PHP**	— что такое сертификат; — почему зелененький? — учимся генерировать запросы (csr) и подписывать их — азы утилиты openssl. Домашние задания 1 ДЗ 3 “ФС и данные” Установить и настроить nginx с аутентификацией клиентов по сертификату

5 Безопасное конфигурирование

1 **Управляем серверами**

— рассказ об утилитах удаленного взаимодействия с сервером: ssh, telnet;
— почему telnet небезопасно — показать перехват пароля;
— настройки ssh: от генерирования ключей до перенаправления портов;
— демонстрация возможностей проброса портов;
— Jump host — почему так любят и админы и офицеры ИБ, использование в сертификации;
— приветствие или как рассмешить хакера.

---

2 **Управляем десятками серверов**

— какие бывают системы управления конфигурацией (Ansible + Puppet, ...);
— push и pull модели с точки зрения ИБ;
— какие методики обеспечения доставки конфигурации используются;
— целостность конфигурации — git и merge request.

---

3 **Бункер для секретов**

— CI/CD — о том, как в современном мире автоматизируются действия на серверах;
— бла-бла-бла о паролях или почему не нужно использовать спецсимволы;
— а где всё это хранить? Как хранить пароли для человека, как хранить пароли для машины — что под капотом парольных хранилищ в CI/CD;
— а как это всё доставлять? Хранение пароля в памяти — самый безопасный способ, и почему лучше не использовать встроенные парольные базы на примере jenkins.

Домашние задания

1 ДЗ 5 “Безопасное конфигурирование”

Играемся с jump host - пробуем различные модели проброса портов и цепочек jump хостов из виртуалок.
Запускаем преднастроенную лабу jenkins+gitlab server и пытаемся управлять раскаткой конфигурации на сервера через merge request
Запускаем преднастроенную лабу jenkins+vault и пытаемся распространять секреты на целевые приложения.

6 Аутентификация и управление доступом

1	**Управление учетными записями и домашними каталогами пользователей**	— требования к созданию пользователя; — какими параметрами можно ограничить; — где хранятся пароли; — PAM + OTP; — двухфакторная авторизация — что можно использовать для сертификации в ИБ.
2	**Модели безопасности в Linux**	— мандатная, дискреционная; — как назначать права пользователям и группам; — ACL (где и как хранятся); — атрибуты доступа suid, sgid, sticky-bit, umask; — su и sudo — в чем разница, и где кроется опасность.
3	**SELinux**	— больно, но иногда нужно. Практические аспекты в работе с SELinux.

Домашние задания

1 ДЗ 6 “Пользователи и доступы”

Скачиваем подготовленный box с ansible и ролями
Запускаем образ из предыдущего ДЗ в нескольких экземплярах
Пытаемся наладить user-management с помощью ansible
Пытаемся наладить распространение настроек pam, … с помощью ansible
Играемся с ACL (дз из suzenescape)
Играем с неправильными настройками sudo и повышаем привилегии
Задание по selinux

7 Что хранит тетрадочка вахтерши

1 **Журналирование**

— bash_history;
— syslog;
— dmesg;
— auth.log.

---

2 **Централизованное хранение логов и мониторинг**

— контрольные суммы, даты изменений файлов;
— мониторинг изменений важных файлов — офицер безопасности знает, что вы создали нового пользователя!
— требования по настройке регистрации системных событий;
— ELK-стэк + SIEM.

Домашние задания

1 ДЗ 7 “журналы”

Задача на ручной парсинг журнала с целью поиска неправомерных действий
Настройка auditd и пересылка событий в предподготовленную лабу с эластиком и кибаной

1 **Параметры загрузки ядра и загрузчики**

— grub и параметры при загрузке аутентификация в режиме восстановления;
— параметры ядра.

Домашние задания

1 ДЗ 8 “безопасная загрузка”

Выставить параметры при загрузке и добиться требования ввести пароли в режиме восстановления

9 Сетевое взаимодействие

1	**Чем разграничить доступ на сетевом уровне**	— какие бывают фаерволы: iptables, nftables, firewalld, uwd и прочий зоопарк; — как их настраивать.
2	**Инструментарий для выполнения проверок (сканеры безопасности)**	— научиться приемам работы с сетевыми сканерами, анализаторами и IDS\IPS\HIPS-системами.
3	**Виртуальные приватные сети**	— рассмотреть, какие бывают vpn-сервера в современном мире — от soho-решений, таких как openvpn, до enterprise-решений, которыми можно охватить всех пользователей, работающих удалённо; — как можно разграничить доступ к ресурсам различных пользователей при единой точке vpn-соединения.

Домашние задания

1 ДЗ 9 “Сетевая безопасность”

Настройка iptables
Настройка openvpn

10 Виртуальные среды и контейнеры

1	**Управление лимитами для дисковой подсистемы и контроля вычислительных ресурсов**	— научиться приемам работы для обеспечения лимитирования вычислительных ресурсов.
2	**Безопасность ФС Docker**	— проблемы root-пользователя в Docker. Как можно из Docker попасть в хост; — понимать проблемы безопасности при использовании Docker в продакшн-среде; — ужесточать политики безопасности при использовании Docker; — проводить аудит безопасности; — включать и настраивать лимиты и cpabilities; — сеть в Docker без шифрования и изоляция сегментов; — другие настройки для усиления безопасности Docker. Домашние задания 1 ДЗ 10 “лимиты, виртуальные среды и контейнеры” Настройка квотирования Что-то с докером

11 Итоговая проектная работа

1	**Выбор темы и организация проектной работы**	выбрать и обсудить тему проектной работы; спланировать работу над проектом; ознакомиться с регламентом работы над проектом. Домашние задания 1 Проектная работа
2	**Контроль соответствия требованиям политики безопасности**	
3	**Защита проектных работ**	защитить проект и получить рекомендации экспертов.