Практическое задание: безопасность ОС Linux
Разверните виртуальную машину на любом дистрибутиве, основанном на Debian (Ubuntu, Debian…).

Выполните настройку по чек-листу:

1. Установить SSH-сервер и настроить удалённое подключение по ключам, вместо пароля.
2. Создать нового пользователя с домашней директорией и выдать ему возможность запускать следующие утилиты без требования пароля:
   /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3
   usr/bin/systemctl
   sbin/ifup, /sbin/ifdown
3. Установить минимальную длину пароля для пользователя в 8 символов.
4. Установить на сервер пакеты Java.
5. Настроить автоматическое сканирование антивирусом всей ОС каждый понедельник в 4 утра. При этом раз в месяц должно происходить обновление базы данных антивирусов.
6. Настроить файервол на блокирование всего входящего и выходящего трафика.

_____

Описание процесса выполнения.
Для выполнения в качестве сервера использовал виртуальную машину ts (Ubuntu), и хостовую nn (Linux mint).

1. Установил SSH-сервер sudo apt-get install ssh. Настроил удаленное подключение по ключам, для этого сгенерировал пару ключей ssh-keygen, и публичный ключ добавил на сервер при помощи команды sudo ssh-copy-id ts@192.168.1.66, введя пароль. На сервере в конфигурационном файле /etc/ssh/sshd_config раскомментил PubkeyAuthentication yes, также отключил вход по паролю на сервере и хосте, рестартнул sshd командой sudo systemctl restart sshd. Далее подключичился уже по ключам. Содержимое конфигурационного файла sshd скрин1 , скрин1-2 , скрин1-3 .

2. Удаленно создал нового пользователя (с домашней директорией) на сервере с именем tsnew и паролем скрин2 .
Чтобы выдать возможность запускать без требования пароля указанные в задании утилиты, добавил в /etc/sudoers (на удаленной машине)данную строчку
tsnew ALL=(ALL) NOPASSWD: /sbin/route, /sbin/iptables, /usr/bin/nmap, /usr/sbin/hping3, /usr/bin/systemctl, /sbin/ifup, /sbin/ifdown , сохранив изменения.
Вывод ls в директории Home скрин3 . Вывод файла passwd скрин4 , скрин4-2 . Вывод файла sudoers скрин5 , скрин5-2 . Перезагрузил систему проверил доступ без пароля на утилите iptables командой sudo iptables -L, пароль не запросился. Скрин6.

3. Чтобы установить минимальную длину пароля в 8 символов, отредактировал файл /etc/pam.d/common-password через nano. В строке password requisite pam_pwquality.so retry=3 в конец добавил строчку minlen=8, сохранил изменения. Скрин7

4. Установил на сервер пакеты Java с помощью команды sudo apt install default-jdk .
Ставил полную версию JDK (Java Development Kit), которая включает компоненты,

предназначенные для запуска, компиляции и разработки Java-программ и содержит по умолчанию в себе редакцию JRE. Проверил результат установки скрин8 .

5. Установил clamav командой sudo apt install clamav clamav-daemon clamav-freshclam. Используя впн обновил базы сигнатур sudo freshclam, в процессе возникла ошибка /var/log/clamav/freshclam.log is locked by another process, остановил выполнение сервиса clamav командой sudo systemctl stop clamav-freshclam, после этого повторно запустил обновление, прошло успешно. Далее sudo systemctl start clamav-freshclam , проверил статус - active (running) и просканировал, созданный для теста файл clamscan testclmv. Скрин9 . Создал в кронтабе две задачи: 0 4 * * 1 /usr/bin/clamscan -i -r / (сканирование антивирусом всей ОС каждый понедельник в 4 утра, -i вывод только инфицированных файлов, -r рекурсивное сканирование); 0 0 1 * * /usr/bin/freshclam (обновление сигнатур в первый день каждого месяца) Скрин10 .

6. Проверил текущие правила брандмауэра sudo iptables -L, выставил запрет на входящий и исходящий трафик командами sudo iptables -P INPUT DROP и sudo iptables -P OUTPUT DROP, снова проверил изменения в правилах. Скрин11