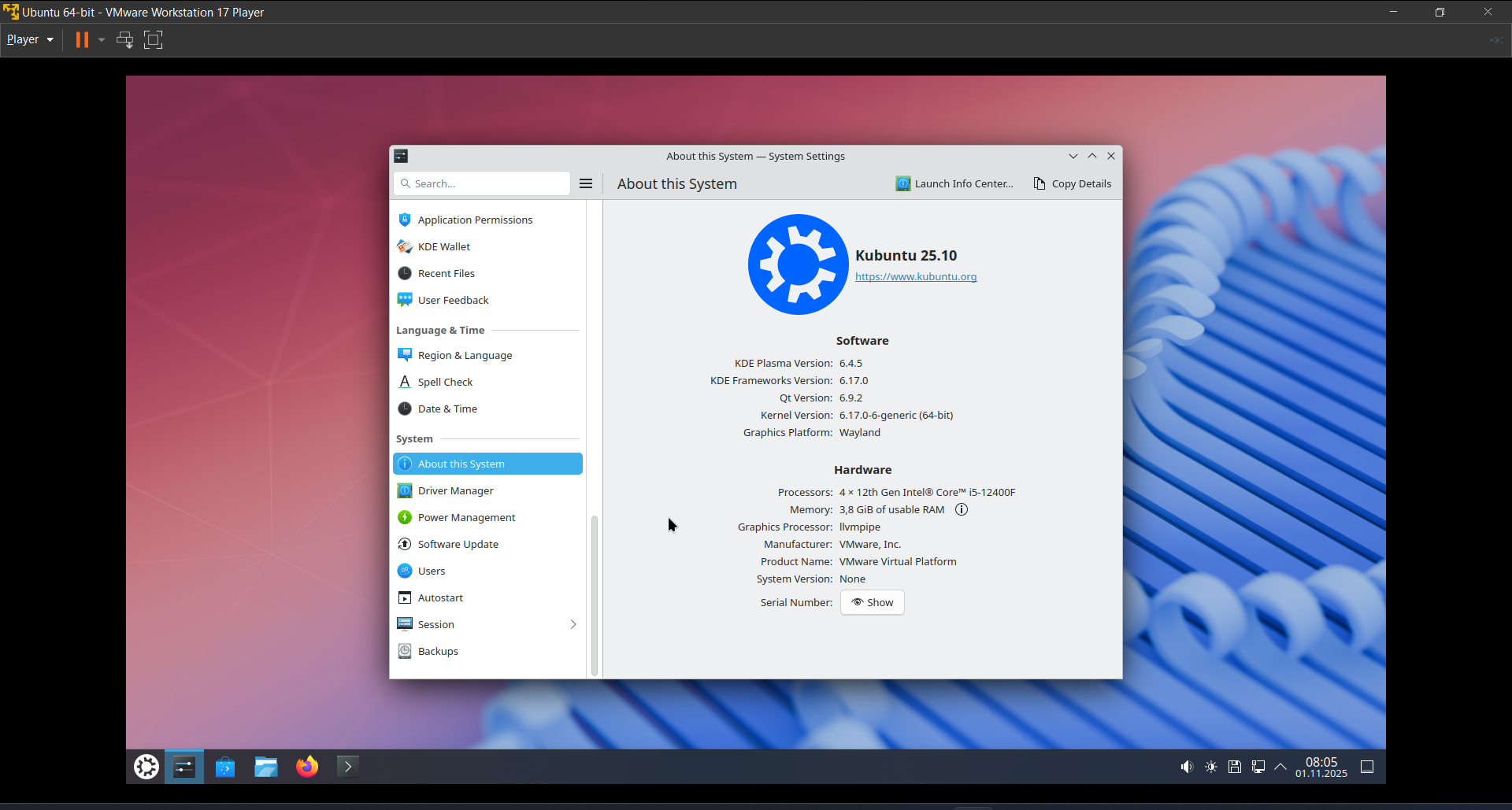
Политика безопасности Linux

Настройка политики безопасности в Linux Kubuntu будет состоять из 3 основных пунктов:

1. Настройка брандмауэра
2. Защита от вредоносного ПО
3. Настройка доступа к общему каталогу

Они позволят защитить системные бреши системы от вредоносных программ и пользователей.

Версия Linux Kubuntu: 25.10.



1. Настройка брандмауэра

Брандмауэр (Firewall) — это важнейший инструмент для контроля сетевого трафика и защиты системы от несанкционированных подключений. В Ubuntu используется утилита UFW (Uncomplicated Firewall).

* 1. Открываем терминал и вводим команду sudo ufw enable.

A computer screen with a black screen

AI-generated content may be incorrect.

Рисунок 1 – Окно терминала

A computer screen with a black screen

AI-generated content may be incorrect.

Рисунок 2 - Результат включения брандмауэра

* 1. Если вам необходимо разрешить доступ через конкретный порт выполните команду sudo ufw allow (порт). Чтобы заблокировать доступ через конкретный порт, выполните sudo ufw deny (порт):

A computer screen with a black screen

AI-generated content may be incorrect.

Рисунок 3 - Результат открытия и закрытия портов

1. Защита от вредоносного ПО

Руткит — это вредоносное программное обеспечение (ПО), которое маскирует присутствие других вредоносных программ в системе, скрывая файлы, процессы и другую активность от антивирусов и самого пользователя

Используйте rkhunter для проверки на наличие руткитов и вредоносного ПО.

* 1. Откройте терминал и введите команду sudo apt install rkhunter для установки пакета

A screen shot of a computer

AI-generated content may be incorrect.

Рисунок 4 - Успешная установка rkhunter

* 1. После установки выполните сканирование командой sudo rkhunter –check:

A screen shot of a computer

AI-generated content may be incorrect.

Рисунок 5 – Выполнение команды сканирования

A computer screen shot of a computer screen

AI-generated content may be incorrect.

Рисунок 6 – Результат сканирования

1. Настройка доступа к общему каталогу

Ваш домашний каталог по умолчанию будет доступен каждому пользователю в системе. Так что если у вас есть гостевая учетная запись, то гость сможет получить полный доступ ко всем вашим личным файлам и документам. Но вы можете сделать его доступным только вам.

* 1. Введите команду chmod 0700 /home/имя\_пользователя, если нам необходимо, чтобы доступ к папке был только у нашего пользователя.

A computer screen with a black screen

AI-generated content may be incorrect.

Рисунок 7 – Ввод команды в терминал

Она устанавливает права таким образом, чтобы владельцу папки, то есть вам было доступно все, а другие пользователи даже не могли посмотреть содержимое.

* 1. В качестве альтернативы можно использовать команду chmod 0750 /home/имя\_пользователя, которые предоставят доступ на чтение в вашей папке для пользователей из той же группы, что и вы:

A computer screen with a black screen

AI-generated content may be incorrect.

Рисунок 9 – Ввод команды в терминал