Бесу файрволл не помеха

или тонкий клиент Thinstation, как доступный способ уменьшить периметр уязвимости

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

ЭПОХА БОЛЬШИХ ПЕРЕМЕН В СФЕРЕ ИТ

- Кардинальные изменения в операционных системах
- Удаленная работа вне офиса
- Виртуализация и контейнеризация
- «Облака» — суть чужие компьютеры
- Беспроводные устройства, «умные» устройства дома и в офисе

КАК ЭТО ВЛИЯЕТ НА НАШУ БЕЗОПАСНОСТЬ

- Хактивизм во всех видах
- Организованные APT-группы и массовый рынок уязвимостей нулевого дня
- Хакер-конструкторы и вредоносное ПО (malware), как бизнес-процесс
- Массовое использование методов социальной инженерии

УГРОЗЫ С ТЕХНИЧЕСКОЙ СТОРОНЫ

- Уязвимости нулевого дня
- Ошибки конфигурации
- Социальная инженерия
- Атаки на «цепочку поставщиков»
- Закрепление, повышение привилегий, боковое перемещение

УГРОЗЫ ПО СПОСОБУ РЕАЛИЗАЦИИ

- «Ковровые бомбардировки»
- Удаленные «целевые атаки»
- Локальные «целевые атаки»

ЗАЩИТА

- SIEM,IDS, IPS
- Сети с нулевым доверием
- Виртуализация
- Терминальные серверы и фермы, VDI
- Тонкие клиенты
- Групповые политики

ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ

1. Работа без прав администратора
2. Политика ограниченного использования программ
3. Отключение неиспользуемых служб
4. Обновления
5. Брандмауэр
6. Резервное копирование
7. Антивирус

Если у меня стоит антивирус, я полностью защищен от вирусов?

— **Алексей Лукацкий**
бизнес-консультант по информационной безопасности Positive Technologies

вопрос эксперту

Если у меня стоит антивирус, я полностью защищен от вирусов?

Соответственно, полагаться на антивирус я бы не стал, и именно поэтому в базовых рекомендациях по ИБ для рядовых пользователей и корпораций **установка антивируса не входит даже в десятку защитных мер.**

Если у меня стоит антивирус, я полностью защищен от вирусов?

Если у вас стоит антивирус, то вы не защищены ни от чего. **Существует множество сервисов, которые позволяют проверить вредоносный код** на недетектируемость популярными антивирусами и средствами защиты конечных устройств.

ДОПОЛНИТЕЛЬНЫЕ ОГРАНИЧЕНИЯ

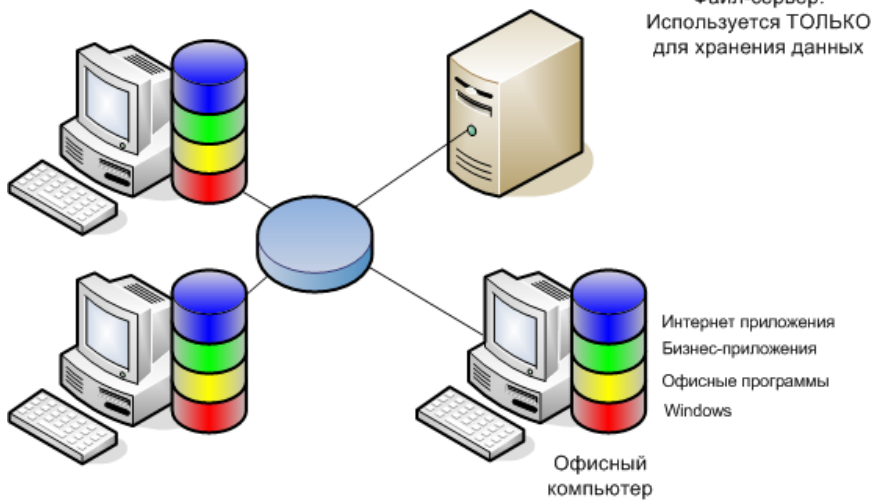
- Ограничения удаленного доступа по IP
- Сильные пароли
- Отключение виртуальных каналов в случае удаленного доступа по RDP

УМЕНЬШАЕМ ПЕРИМЕТР УЯЗВИМОСТИ

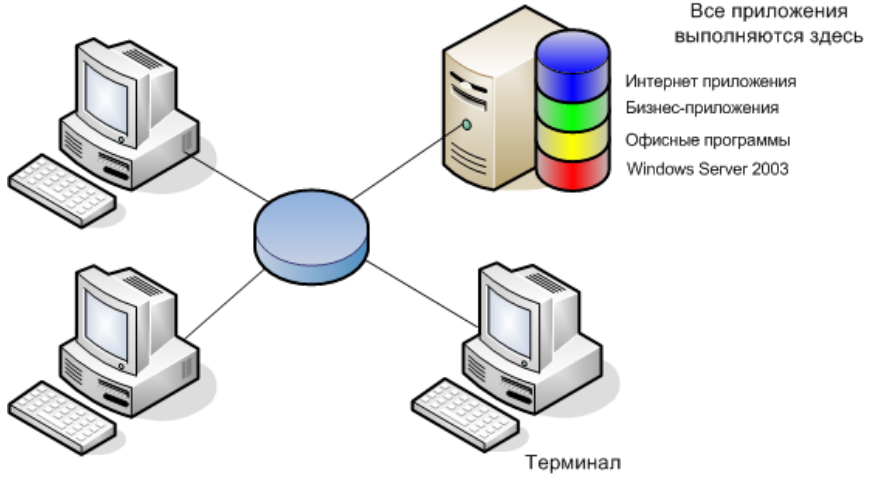
- Толстый клиент — дополнительная угроза
- Тонкий клиент — неизменяемый образ, минимальный размер
- Программное обеспечение для тонких клиентов — большой выбор
- Thinstation и его клоны
- WTware, Ponix, LTSP и т.д.

ТОЛСТЫЙ КЛИЕНТ VS ТОНКИЙ КЛИЕНТ

Обычная офисная сеть



Терминальная сеть



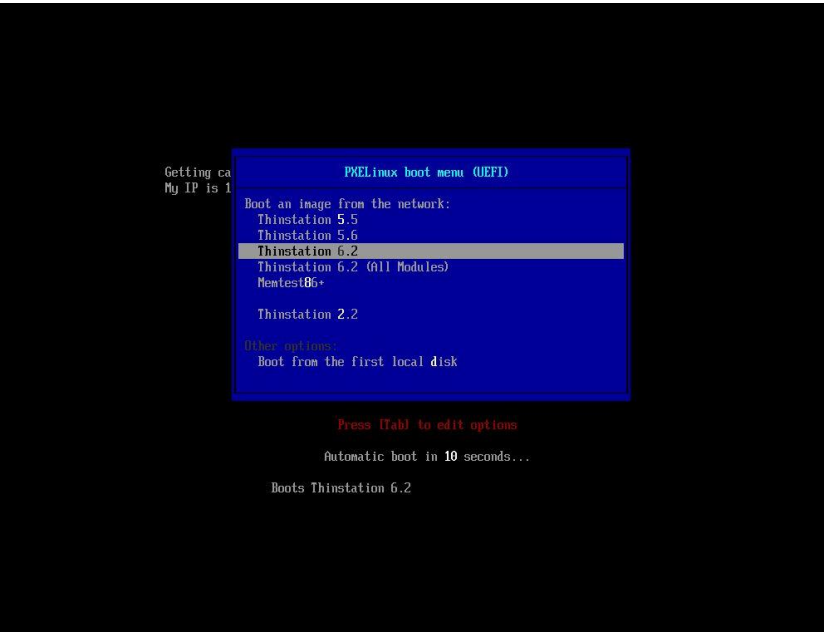
Thinstation — тонкий клиент с открытым исходным кодом

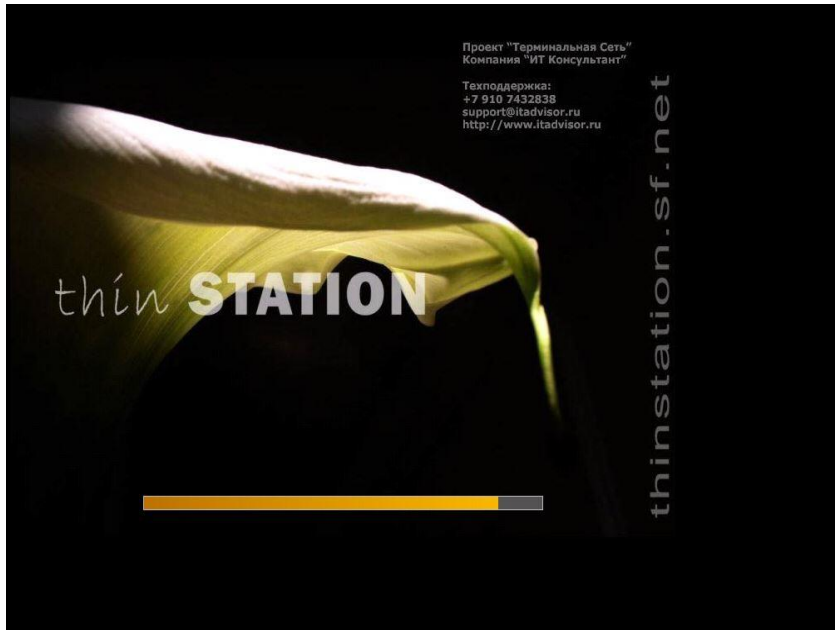
- Linux, основа — дистрибутив Crux Linux
- Открытый код
- Пересборка пакетов
- Добавляем свои пакеты
- Конфигурируем, как хотим

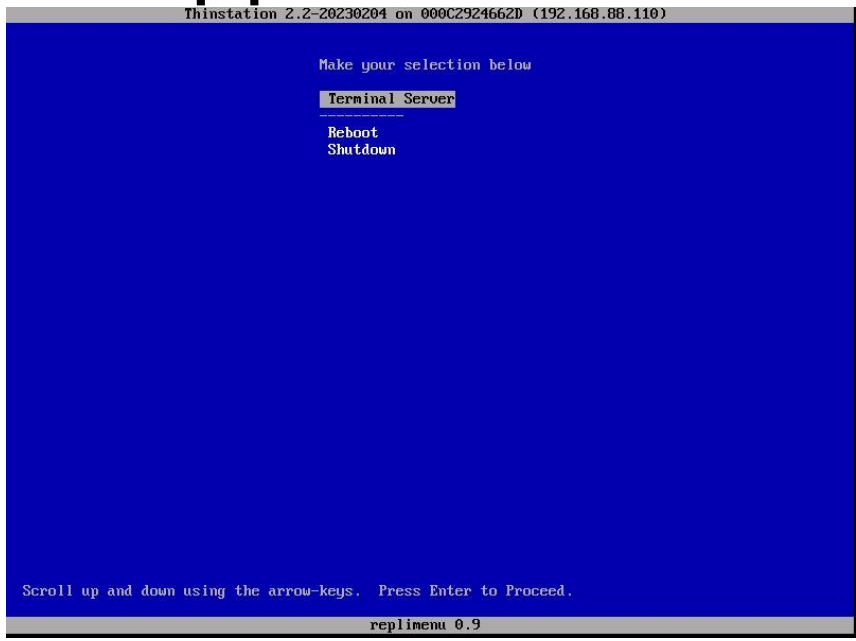
THINSTATION, КАК ЭТО УСТРОЕНО

- DHCPD
- TFTPD/HTTPD
- Pxelinux/ipxelinux
- Ядро
- Initrd
- Конфигурационные файлы + дополнительные пакеты

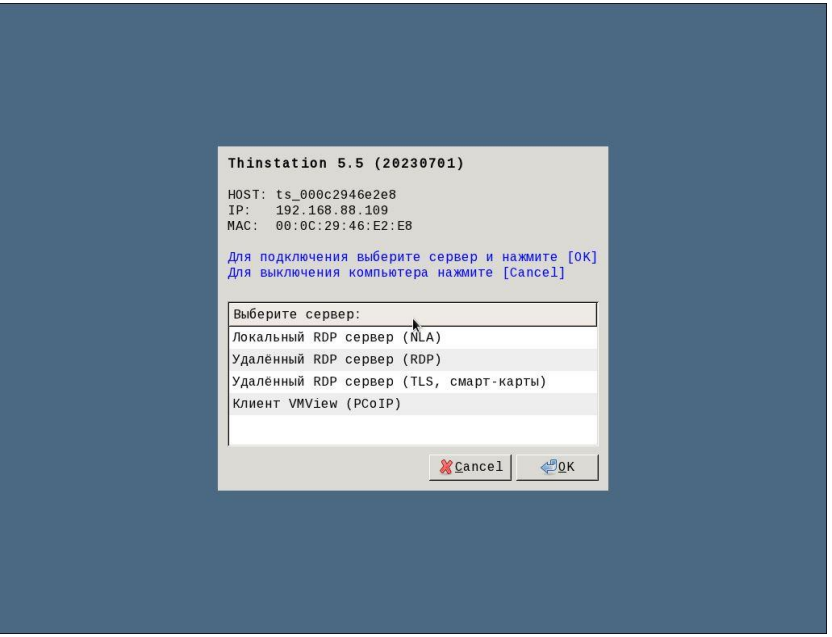
THINSTATION, КАК ЭТО ВЫГЛЯДИТ

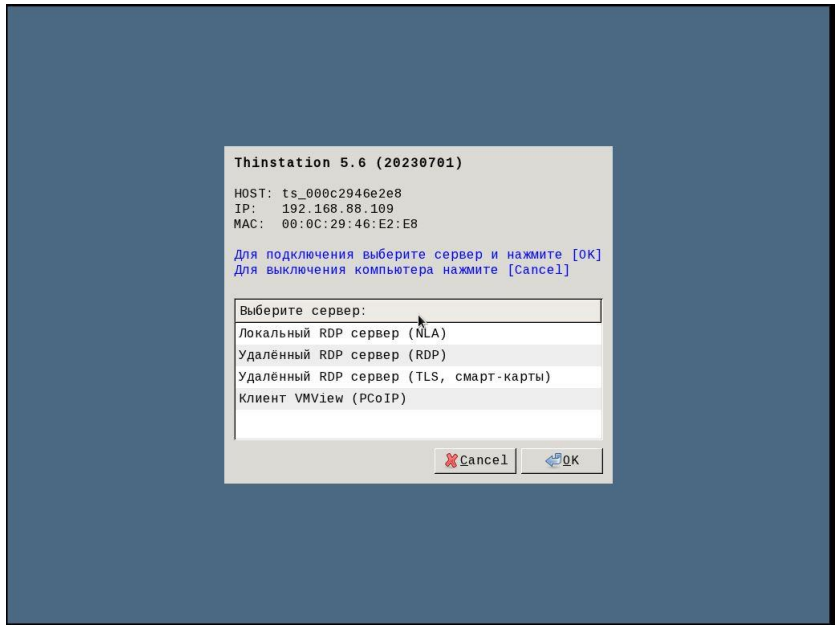


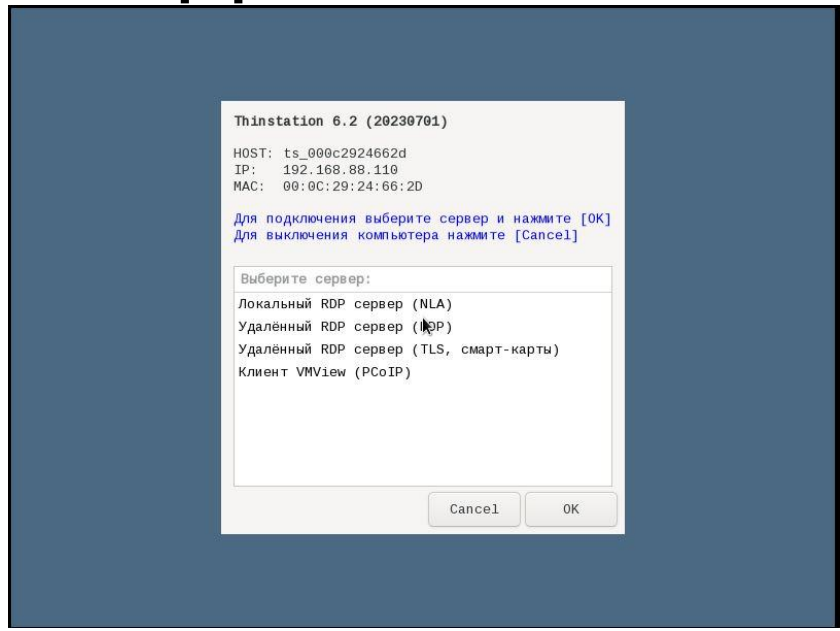




THINSTATION, КАК ЭТО ВЫГЛЯДИТ







THINSTATION, КАК ЭТО РАБОТАЕТ

- Картинки меню
- Конфигурационные файлы, виды сессий
- Поддержка RDS ферм
- Поддержка NLA

THINSTATION, В ЧЕМ ПРЕИМУЩЕСТВО

- Уменьшает периметр уязвимостей
- Поддерживает широкий спектр оборудования
- Продлевает жизненный цикл оборудования
- Нетребователен к ресурсам, загрузочный образ 30Мб
- Расширяем дополнительным функционалом
- Настраиваем чуть меньше, чем полностью

ЧТО ДЕЛАТЬ?

- Ревизия оборудования и используемых программных решений
- Составить список угроз
- Думать, принимать решения
- Готовы помочь

Ссылки в Telegram

Канал «Проект "Терминальная сеть"»

https://t. me/pts_itadvisor

Группа «Проект "Терминальная сеть"»

https://t. me/+j3PErS9wuVgzMDZi