**Дистрибутивы Linux для параноиков**

**Subgraph OS**



Несмотря на то, что Subgraph OS легко освоить и использовать, это, по мнению многих, одна из самых безопасных операционных систем. На самом деле, многие утверждают что Subgraph OS, это безопасная операционная система Linux, для технически не подкованных пользователей. Частично по той причине, что Subgraph OS (назовём её СОС), предназначена для нубов, и она поставляется со всеми параметрами конфиденциальности и безопасности, которые настраиваются автоматически. Плюс, многие другие дистрибутивы, которые сделаны для безопасности, требует значительных системных ресурсов, и могут использоваться только с определённым оборудованием. Они так же станут настоящим адом, для тех, кто не привык к многоступенчатой установке и настройке Linux систем. Одна из целей дизайна СОС заключается в том, чтобы уменьшить количество мест для атаки, через которые пользователь может быть уязвим, через несколько функций, в том числе: Автоматизированная надёжная защита, через изолирование приложений, с использованием контейнеров — это труднопроизносимо, да? СОС включает в себя интересную функцию под названием ОЗ, которая является системой программ для изоляции. Через ОЗ, система изолирует программы, так что если злоумышленник воспользуется лазейкой в безопасности, то весь остальной компьютер будет оставаться в неизменном состоянии. Это делается путём разделения доступа приложений к другой части компьютера, поэтому, если злоумышленник взломает безопасность одного приложения, это не даст ему доступа к другим функциям. Обязательное полное шифрование всего рабочего стола, через систему импорта fde, СОС включает в себя так же обязательное полное шифрование диска по умолчанию, так что пользователь может легко начинать с простейшего уровня безопасности. Анонимность через ToR — ах да, «Т» слово! СОС перенаправляет весь Ваш трафик через ToR, что делает его более трудным для взлома злоумышленников, это ещё усложняет определение Вашего физического местоположения. СОС имеет много других функций безопасности, загуглите для получения полной информации.

**Trusted End Node Security (TENS)**



The Distro Formerly Known as Lightweight Portable Securit — «Дистрибутив ранее известный как лёгкой и портативной безопасности» в настоящее время официально называется Trusted End Node Security (TENS). Tens, как и СОС, создаёт безопасную вычислительную среду из надёжных носителей, и предназначен для компьютеров на базе Intel. Его основа на базе операционной системы Linux, с установкой с компакт-диска или USB-накопителя. Он предназначен, для того чтобы служить надёжным конечным узлом, он загружается только в RAM. В сущности это может превратить ненадёжную систему, например, домашний компьютер, в отлично защищённый сетевой клиент. Одна из его основных функций: Мастер шифрования(EW)- это простой, но сильный файл и шифратор папок, предназначен для защиты личной, конфенеденциальной, но не секретной, информации. Написанный на Java, может шифровать все типы файлов. Он совместим с Windows, Mac, Linux, Solaris и другие типы компьютеров, которые включают в себя поддержку Java. Вы можете знать эту информацию или даже может быть и не знать, что дизайнеры Tens не кто иные, как Министерство Обороны США, так что я предполагаю, что использование данной ОС, зависит от того, насколько Вы доверяете им! Есть одна вещь, которую стоило бы отметить: если Вы решите использовать Google в этой ОС, в частности Chrome, и попробуете нажать на первые не сколько результатов, Вы можете получить предупреждение, как это:



По словам самих DoD, ссылки всё же находятся в безопасности, они гораздо подробнее описывают это на своём официальном сайте. Во всяком случае, размещение фактической ссылки для скачивания, а это якобы небезопасно, здесь, это инциатива, по защите программного обеспечения. Так что, Вы можете нажать, на свой страх и риск…

**Arch Linux**



Arch Linux, по словам своих создателей, является «лёгкой и гибкой операционной системой Linux, которая пытается сделать Linux максимально простым». Это дистрибутив Linux, для компьютеров на базе архитектуры IA-32, x86-64 и ARM. По большей части всё строится на основе двойных пакетов, который легко поможет поддержать производительность на текущем оборудовании. Для ускорения частых изменений пакетов, Arch Linux использует пакман (аббревиатура “package manager”), разработанный Джаддом Винетом, если Вы подумали, что я имею в виду игру от Атари, то мне жаль Вас разочаровывать! Одним из самых интересных пакетов, которые можно найти в «поиске» (на официальном сайте) не Accerciser, интерактивный Python доступный Explorer для рабочего стола GNOME; wireshark командная строка, для бесплатного сетевого протокола анализатора Unix и Windows; и abiword, полнофункциональный текстовый редактор. Так что да — это очень забавно, но я уверен, что Вы задаётесь вопросом, каковы же функции безопасности? Ось имеет довольно много защитных функций, они включают в себя: Разрешения файловой системы,Шифрование диска,Обязательный контроль доступа Изолирование приложений.

Есть и другие, но они не будут так хороши, без одно важного элемента. Что это? Что же ещё? Вы должны выбрать безопасный пароль для защиты каждой части системы! Создание пароля Diceware, может Вам помочь, ведь слабые пароли означают лёгкую добычу для хорошего хакера. Чтобы понять какие пароли хорошие, а какие нет, советую читать ArchWiki, собственно там рекомендуют Diceware. Одна из причин, того что сильные пароли являются неотъемлемой частью Оси заключается в том, что она использует эти пароли для защиты многих важных пакетов, таких как учётные записи пользователей, шифрование файловых систем. Если Вы не хотите, чтобы совершенно незнакомые люди сунулись туда, куда лезть не следует, не используйте пароли вроде «password». Есть намного больше полезного в Arch Linux, можно увидеть не которые другие приложение посетив Вики по Linux.

**Cyborg Linux (a.k.a. Cyborg Hawk Linux)**



Это странно, что название Cyborg Linux, вызвал образы Терминатора или Робокопа в моей голове? Нет, наверное, нет. Его создатели смело описали его как «передовой, красивый и мощный дистрибутив». Ну, они могут подвердить это? Cyborg Linux, как и многие другие дистрибутивы, например Kali Linux, состоит из большого разнообразия средств, направленных на проведение расследований и оценки Вашей уязвимости. Среди них: Angry IP Scanner — очень быстрый IP порт и сканнер, который может сканировать в любом диапозоне. Nmap — бесплатный, с открытым исходным кодом сканер, совместимый с Windows и Unix. Ghost Phisher — приложение компьютерной безопасности, которое включает в себя поддельные DNS-сервера, DHCP-сервер фейк, подделку http-сервера и другие ценные «оружия», так сказать. WebScarab — основна для анализа приложений, взаимодействующих через протоколы http и https. Действительно, эти средства не просто посмотреть что же такого в этом deepweb, это огромный арсенал киборга. В целом, он включает в себя более 750 различных инструментов для тестирования на проникновение. Я не знаю Вас, но в моём распоряжение Cyborg Linux, вызвал эмоции, как у ребёнка в магазине конфет (пусть и потенциально смертельных). Это также совершенно бесплатно, что весьма удобно, особенно для тех из нас, у кого ограниченный бюджет. В придачу, он имеет полную поддержку виртуальной машины. Конечно, я не рекомендую его для начинающих, но это и не те для кого Cyborg Linux предназначается.

**Security Onion**



Девиз **Security Onion** звучит как “peel back the layers of your network». Он как Киборг и Arch Linux — это дистрибутив Linux, созданный для безопасности так и для тестирования на проникновение. Security Onion основан на Ubuntu, которая, веришь ты или нет, анон, тоже весьма безопасна! Так же, как и его современники Linux, Security Onion с полным хранилищем инструментов, в том числе: Snort — система предотвращения вторжения сети, с открытым исходным кодом. Suricata — бесплатная, с открытым исходным кодов, утилита для обнаружения угроз Bro — анализ сетевой структуры OSSEC (Open Source HIDS SECurity) — Unix-система безопасности монитора, которая следит за всеми аспектами деятельности. Главное преимущество заключается в том, что Security Onion легко сочетает в себе три основные функции — полный захват пакетов, сетевые и хост-системы обнарудения вторжения, и множество мощных средств для системного анализа. Security Onion обеспечивает полный захват пакетов, используя netsniff-ng, установив бесплатный сетевой набор Linux. Security Onion построен на распределение клиент-сервреной модели, это означает, что «датчик» работает как клиент, и поэтому «сервер» — это что ещё? — сервер! Как и при других испытаниях, ориентированных на руки для дистрибутивов Linux, Вам придётся потратить изрядное количество времени, чтобы сначала привыкнуть, а затем научиться пользоваться, но как только Вы это сделаете, Вы, наверное, почти не сможете остановиться. Это далеко не так просто, как Subgraph OS, но Вы будете чувствовать, что можете сделать с ним гораздо больше. Я не уверен, на данный момент, является ли ли он лучшим на самом деле, среди других дистрибутивов Linux, служащим аналогичным целям. Для того, чтобы это определить, какой же из них является лучшим из них, надо устроить конкурс какой-то. Эй, ребята, кто хочет «Distros Wars» ?

**Pentoo**



Как следует из названия, он предназначен для тестирования. Pentoo является безопасно-ориентированной операционной системой на компакт-диске, основанной на Gentoo. Основное различие, заключается в том, что он включает в себя множество специализированных инструментов, таких как: Хорошее ядро с AuFS патчами Поддержку загрузку модулей, в стиле Slax Поддержку технологии Cuda/OpenCL

Его команда разработчиков состоит из нескольких парней, которые оказались большими поклонниками Gentoo, и хотели создать собственную версию. Они известны под именами Grimmlin, Zero\_Chaos, Антон Большаков (blshkv), и Стефан Кун (Wuodan). Если Вы не знакомы с Gentoo, возможно, было бы не плохо познакомиться с этой ОС, прежде чем нырять в омут с головой в Pentoo, хотя — это Ваш выбор, конечно. Если вам интересно, то просто проверьте их сайт и посмотрите сами, какими ресурсами они располагают. На одной странице они рассказывают, что полезно для начинающих, полезный код, который можно использовать для настройки системы при запуске. Например: Changes=/dev/sdXY позволит Вам указать, где хранить конфиги и тд. В случае, если у Вас есть раздел жёсткого диска в FAT, Вы можете задать его здесь, так что Вы должны сами указать, что собираетесь что-либо хранить на нём. У меня сложилось впечатление, что Pentoo, несмотря на установленный дистрибутив, находится в своего роде бета-фазе, так что будьте осторожны с ним. С другой стороны, может быть, Вы могли бы побыть одним из подопытных кроликов, чтобы проверить его, и, возможно, даже способствовать его развитию!