Чек-лист параметров безопасности ОС на базе Linux

Имя узла	
IP-адрес	
Версия ядра	
Комментарий	

№	Действие по настройке параметров безопасности	Отметка о выполнении
1	**Настройка авторизации в системе**	
1.1	Убедиться в отсутствии пользователей с пустыми паролями	
1.2	Обеспечить отключение входа суперпользователя в систему по протоколу SSH	
2	**Контроль за механизмами получений привилегий**	
2.1	Обеспечить ограничение доступа к команде su	
2.2	Ограничить список пользователей sudo и выполняемых команд	
3	**Настройка прав доступ к объектам файловой системы**	
3.1	Установить корректные права доступа к файлам настройки пользователей	
3.2	Установить корректные права доступа к файлам запущенных процессов	
3.3	Установить корректные права доступа к файлам, выполняемым с помощью cron	
3.4	Установить корректные права доступа к файлам, выполняемым с помощью sudo	
3.5	Установить корректные права доступа к стартовым скриптам системы	
3.6	Установить корректные права доступа к системным файлам заданий (конфигурационным файлам) cron	
3.7	Установить корректные права доступа к пользовательским файлам заданий cron	
3.8	Установить корректные права доступа к исполняемым файлам и библиотекам ОС	
3.9	Установить корректные права доступа к SUID/SGID-приложениям	
3.10	Установить корректные права доступа к содержимому домашних каталогов пользователей	
3.11	Установить корректные права доступа к домашним каталогам пользователей	
4	**Настройка средств защиты ядра Linux**	
4.1	Ограничить доступ к журналу ядра	
4.2	Заменить ядерные адреса в /proc и других интерфейсах на 0	
4.3	Инициализировать динамическую ядерную память нулем при ее выделении	
4.4	Запретить слияние кэшей ядерного аллокатора	
4.5	Инициализировать механизм IOMMU	
4.6	Рандомизировать расположение ядерного стека	
4.7	Включить средства защиты от аппаратных уязвимостей центрального процессора (для платформы x86)	
4.8	Включить защиту подсистемы eBPF JIT ядра Linux	
5	**Уменьшение периметра атаки ядра Linux**	
5.1	Отключить устаревший интерфейс vsyscall	
5.2	Ограничить доступ к событиям производительности	
5.3	Отключить монтирование виртуальной файловой системы debugfs	
5.4	Отключить системный вызов kexec_load	
5.5	Ограничить использование user namespaces	
5.6	Запретить системный вызов bpf для непривилегированных пользователей	
5.7	Запретить системный вызов userfaultfd для непривилегированных пользователей	
5.8	Запретить автоматическую загрузку модулей ядра, отвечающих за поддержку дисциплины линии терминала	
5.9	Отключить технологию Transactional Synchronization Extensions (TSX)	
6	**Настройка средств защиты пользовательского пространства со стороны ядра Linux**	
6.1	Запретить подключение к другим процессам с помощью ptrace	
6.2	Ограничить небезопасные варианты прохода по символическим ссылкам (symlinks)	
6.3	Ограничить небезопасные варианты работы с жесткими ссылками (hardlinks)	
6.4	Включить защиту от непреднамеренной записи в FIFO-объект, контролируемый атакующим	
6.5	Включить защиту от непреднамеренной записи в файл, контролируемый атакующим	
6.6	Запретить создание core dump для некоторых исполняемых файлов	