ЛЕКЦИЯ №7

«Контроль целостности данных и компонентов ОС»

по дисциплине

«Безопасность операционных систем»

Текст лекции рассмотрен и одобрен на заседании кафедры протокол № ____ от " " 201__ г.

(Слайд 1. Титульный слайд)

Уважаемые студенты! Сегодня вы продолжаете изучение дисциплины «Безопасность операционных систем». Лекция №8 «Контроль целостности данных и компонентов ОС», за ней одноименное практическое занятие. Продолжительность лекции - два академических часа, практического занятия - 2 академических часа.

Слайд 2 (вопросы занятия)

- Целостность данных.
- Системы контроля целостности.
- Доверенная загрузка.

- Tripware
- Целостность пакетов дистрибутивов
- SecretNet
- Модули доверенной загрузки
- ELAM, UEFI, TPM

Целостность

Целостность информации - состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Целостность системы = Целостность данных + Целостность программ.
Целостность данных:

- при доступе;
- при передаче;
- при хранении.

Целостность программ:

- при запуске;
- при выполнении;
- при хранении.

Принципы действия некоторых систем контроля целостности:

- формирование БД контрольных сумм и периодическая проверка соответствия объектов эталонам;
- проверка цифровых подписей для исполняемых файлов перед их выполнением.

Уровни целостности (integrity levels) в Windows

В Windows Vista/7 реализована новая функциональная возможность, известная как ***Обязательный контроль целостности*** (Mandatory integrity control, MIC). Управление осуществляется с помощью элемента списка контроля доступа (access control entry, ACE) в системном списке контроля доступа (system access control list, SACL) защищаемого объекта (например, файла, процесса, ключа реестра и т. д.). Каждый процесс имеет уровень целостности (integrity level), и дочерние процессы наследуют уровень целостности от родительских.

Когда пользователь входит в систему, Windows Vista/7 присваивает ему идентификатор целостности (integrity SID). Этот SID содержит метку целостности, которая определяет уровень доступа маркера пользователя (token), и, следовательно, указывает уровень полномочий, которых этот пользователь может достигнуть. Integrity SID имеет следующий формат: S-1-16-<label>, где <label> представляет уровень целостности. Во время проверки прав доступа Windows Vista/7 проверяет уровень целостности, присвоенный пользователю, и если он доминирует (то есть это число больше уровня целостности объекта или равно ему), пользователю разрешается модифицировать или удалять объект, в противном случае попытка доступа будет отклонена.

Обычные пользователи имеют средний уровень, при повышении уровня полномочий они получают высокий. Объекты, защищенные

механизмом WRP, имеют такие ACL, что доступ к ним имеет только сервис TrustedInstaller, а все остальные учетные записи, включая SYSTEM, имеют право только на чтение и исполнение.

Уровень целостности (Integrity Access Level)	Системные привилегии
Высокий (High)	Административные — можно устанавливать файлы в папку Program Files и вести запись в защищенные ключи реестра, например, в HKEY_LOCAL_MACHINE
Средний (Medium)	Пользовательские — можно создавать и модифицировать файлы в собственных папках и вести запись в ключи реестра в составе дерева HKEY_CURRENT_USER
Низкий (Low)	Недоверенные (Untrusted) — с таким уровнем привилегий можно вести запись только в папки наподобие Temporary Internet Files\Low и ключи реестра наподобие HKEY_CURRENT_USER\Software\LowRegistry

Уровни целостности:

- системный (для системных процессов)
- высокий (для процессов с правами администраторов)
- средний (для пользовательских процессов)
- низкий (отдельные пользовательские процессы - например, IE, Chrome)

Папки тоже имеют уровни целостности, и по умолчанию им присваивается средний уровень.

Изоляция привилегий пользовательского интерфейса (UIPI) построена так, чтобы процессы с более низким уровнем целостности не могли манипулировать процессами с более высоким уровнем. Однако эта модель не является непроходимой стеной по двум причинам:

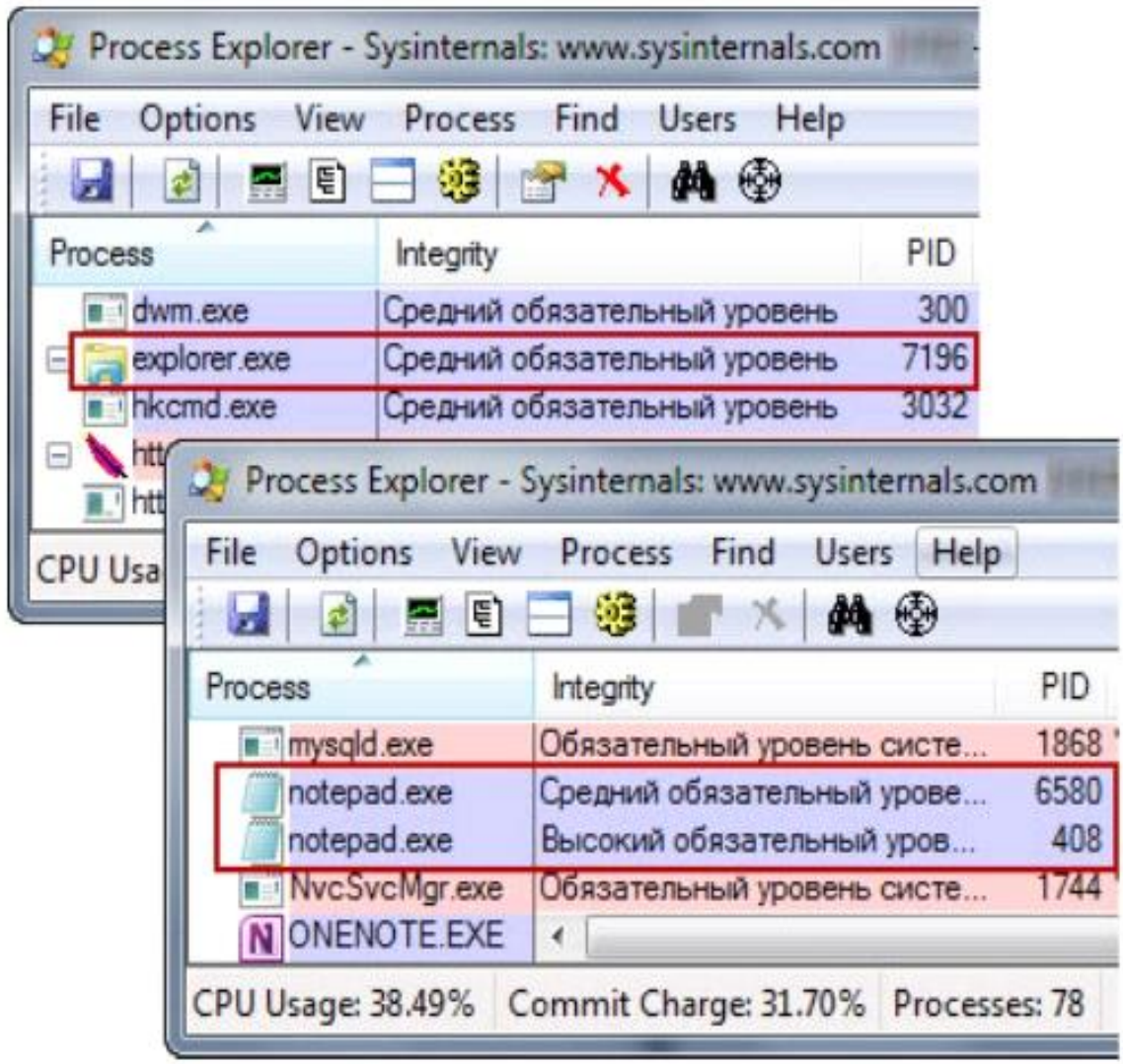
- Процессы с более низких уровней могут читать данные из процессов более высоких уровней.
- Возможны атаки с низких уровней на соседние процессы процессов более высоких уровней через общую сессию и память, приводящие к некорректной работе.

За соблюдением правил целостности следит **UAC** (User Access Control).

Утилита **Process Explorer** отображает уровень целостности процессов в столбце Integrity Levels, который можно добавить из View – Select Columns – Process Image.

Утилита **PsExec** позволяет запускать процессы с низким уровнем целостности.

Системная команда **icacls** умеет показывать уровень целостности папок и разделов реестра. Аналогичный функционал есть в утилите **AccessChk** от Sysinternals.



Например, Notepad с PID 6580 открыт с обычными правами и имеет ***средний*** уровень целостности, а Notepad с PID 408 запущен от имени администратора и имеет ***высокий*** уровень. Проводник, explorer.exe с PID 7196, запускается с обычными правами и ***средним*** уровнем.

Поэтому, перетащить файл с рабочего стола в блокнот с PID 408 не получиться.

Программы хранят свои данные и настройки в папке %userprofile%\appdata в трех разных папках.

Roaming — «легкая» папка. Если в организации профили перемещаемые, ее содержимое копируется на сервер.

Local — «тяжелая» папка. Помимо прочего внутри нее, в папке Temp, хранятся временные файлы. Поэтому ее содержимое на сервер не копируется, чтобы не задерживать процесс входа/выхода из системы.

LocalLow — содержит данные, записанные с низким уровнем целостности, и сама она имеет такой же уровень.

Проверка и восстановление системных файлов Windows

Средство проверки системных файлов — служебная программа Windows, которая позволяет пользователям выполнять поиск повреждений в системных файлах Windows и восстановить поврежденные файлы.

Данные для восстановления хранятся в файле защиты ресурсов Windows (WRP).

Запуск команды осуществляется под правами администратора.

sfc /scannow

Команда sfc/scannow производит сканирование всех защищенных системных файлов и заменяет их в случае повреждения на расположенные в сжатой системной папке % WinDir %\System32\dllcache.

После завершения процесса, может появиться одно из следующих сообщений:

- Защита ресурсов Windows не обнаружила нарушений целостности.
- Защите ресурсов Windows не удалось выполнить запрошенную операцию.
- Защита ресурсов Windows обнаружила поврежденные файлы и успешно восстановило их. Подробные сведения включены в журнал CBS Журнал % WinDir %\Logs\CBS\CBS.log.
- Защита ресурсов Windows обнаружила поврежденные файлы, но не удалось устранить некоторые из них. Подробные сведения включены в журнал CBS Журнал % WinDir %\Logs\CBS\CBS.log.

Для просмотра подробных сведений в файле журнала можно сформировать отдельный файл по утилите sfc с помощью команды:

findstr /c:"[SR]" %windir%\Logs\CBS\CBS.log

Результатом будет Sfcdetails.txt.

Для восстановления поврежденного файла вручную необходимо стать его владельцем и заменить на заведомо корректную копию.

Системы контроля целостности для Windows

Одним из примеров системы является SecretNet.

В Secret Net реализован механизм контроля целостности, который позволяет поставить на контроль изменения ресурсов компьютера, файлов, директорий, элементов реестра windows. Для элементов Secret Net и Windows в модуле контроль программ и данных есть шаблоны, которые включаются по умолчанию. При этом администратор может создавать свои задания и шаблоны реакции на изменения, менять методы контроля.

Контроль целостности может осуществляться как по содержимому файлов, так и по атрибутам, правам доступа, дате и времени последнего изменения. При обнаружении несоответствия можно игнорировать инцидент, блокировать компьютер или автоматически восстанавливать измененные файлы.

Замкнутая программная среда позволяет ограничить список запускаемых пользователем приложений. При запуске приложений автоматически проверяется их целостность.

Кроме того, часто для контроля целостности СЗИ и средств ОС применяются отдельные компоненты СЗИ, например, integrity от "Криптопакет", Provizor от Avast.

Некоторые коммерческие системы контроля целостности файлов для ОС Windows:

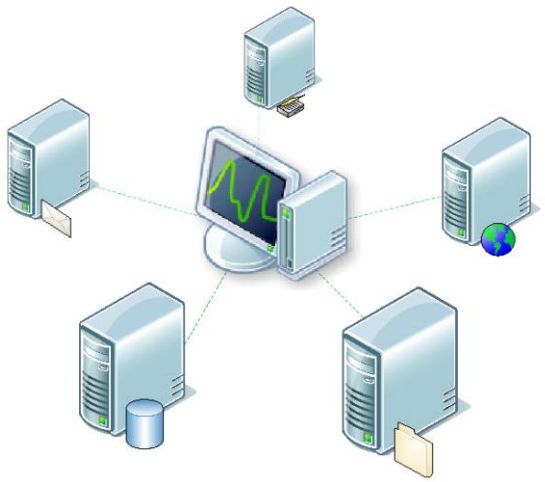
- CimTrak
- Qualys
- Verisys

На практическом занятии будет рассмотрена Verisys.

Verisys

Verisys - это продвинутая система монитоинга целостности файлов для Windows, Linux.

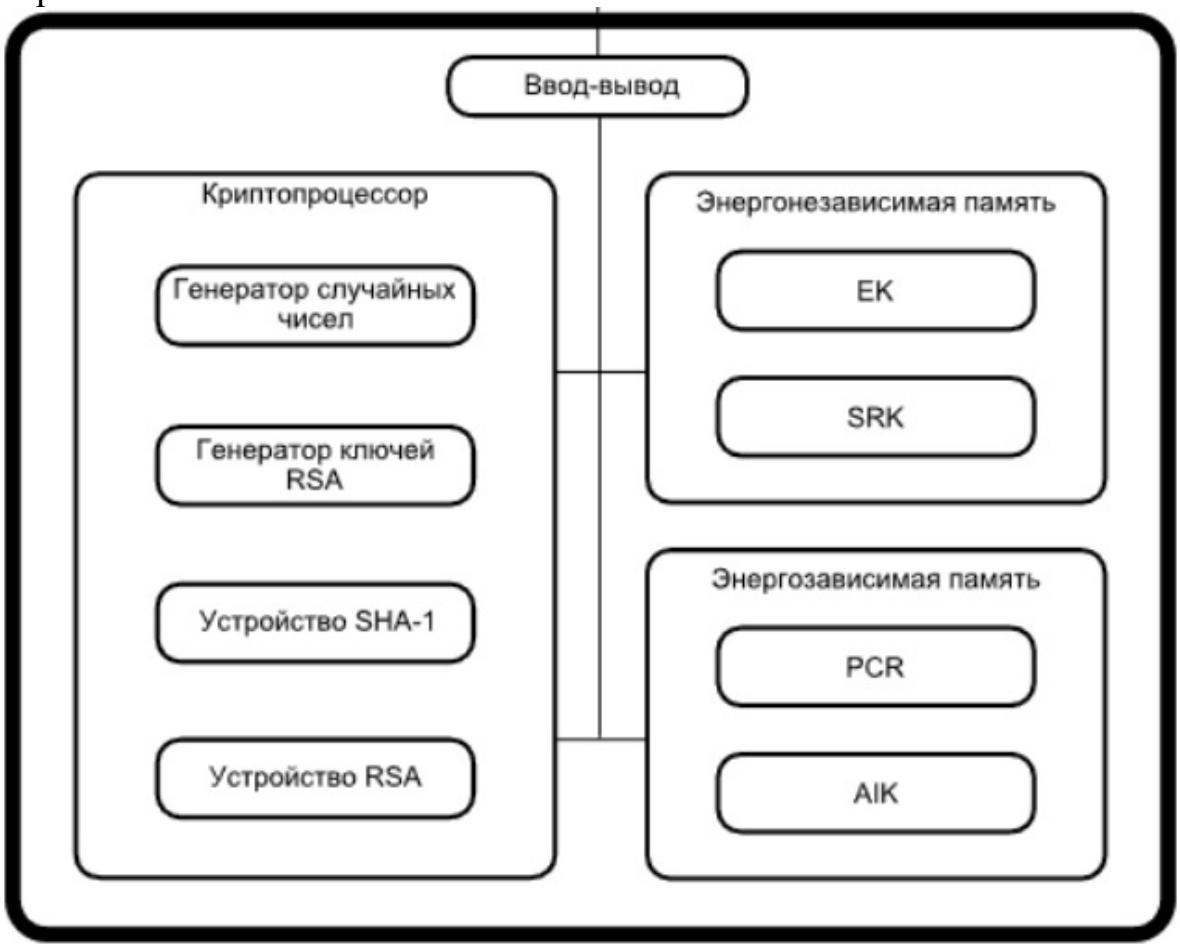
Ключевым компонентом Verisys является Центральная административная консоль, которая позволяет контролировать и настраивать Verisys-агентов.



Для облегчения и ускорения настройки система содержит набор преднастроенных шаблонов для мониторинга различных программ.

TPM

Trusted Platform Module (TPM) — название спецификации, описывающей криптопроцессор, в котором хранятся криптографические ключи для защиты информации, а также обобщенное наименование реализаций указанной спецификации, например, в виде «чипа TPM» или «устройства безопасности TPM».



PCR — это уникальные признаки TPM, в которых в зашифрованном виде содержится вся информация о целостности метрик системы, начиная с загрузки BIOS до завершения работы системы.

AIK — ключ RSA длиной 2048 бит, используемый только для подписей.

SRK (Storage Root Key) - корневой ключ.

EK — ключ RSA размером 2048 бит, идентифицирующий чип, а также все устройство, фундаментальный компонент TPM. Открытая часть называется PUBEK, закрытая — PRIVEK.

Доверенная загрузка в Windows

Дальнейшее развитие в Windows 8 получили аппаратные средства защиты данных. Теперь система оснащена несколькими новыми функциями, активируемыми через встроенную программу Unified Extensible Firmware Interface (UEFI) и через доверенный платформенный модуль Trusted Platform Module (TPM), который также может использоваться аппаратным средством защиты BitLocker в Windows Vista и более новых версиях. Протоколы Measured Boot и Secure Boot дают возможность идентифицировать руткиты и блокировать попытки вредоносных программ укрыться от операционной системы. Для функционирования протокола Measured Boot требуется модуль TPM, но можно обойтись и традиционной системой BIOS.

Secure Boot. В системе Windows 8 обеспечена возможность взаимодействия с протоколом UEFI Secure Boot, который является компонентом архитектуры защищенной загрузки Windows 8. Этот протокол предназначен для работы с аппаратными устройствами, на которых выполняются UEFI -совместимые системы BIOS, для проверки целостности существовавшей до установки Windows среды, а также для пресечения попыток вредоносного программного обеспечения модифицировать встроенные программы и запуститься до загрузки системы.

Интерфейс UEFI разрабатывается независимым форумом. Цель разработки — опираясь на современное оборудование, обеспечить возможность прямого взаимодействия предоперационной среды с аппаратными компонентами с помощью быстрых блоковых операций ввода-вывода без использования традиционных аппаратных прерываний. Спецификации UEFI определяются организацией Trusted Computing Group (TCG).

Протокол Secure Boot защищает встроенные программы компьютерного устройства от установки вредоносных загрузчиков операционных систем, которые могут скрывать свое присутствие от средств безопасности Windows.

Реализованная в Windows 8 архитектура целостности платформы также предусматривает использование технологии раннего запуска защиты от вредоносных программ Early Launch Anti-Malware (ELAM) и возможность проверки состояния клиента посредством сравнения начального состояния системы, записанного в модуле TPM устройства, с данными, содержащимися в удаленном центре проверки.

Инфраструктура открытых ключей Public Key Infrastructure (PKI) используется для формирования цепочки доверия. В процессе производства OEM-изготовители устанавливают платформенный ключ, защищающий микропрограммное обеспечение от опасных изменений. При запуске компьютера с установленным протоколом UEFI Secure Boot аппаратно реализованное программное обеспечение до передачи обработки проверяет состояние файлов запуска загрузки и микропрограмм на таких устройствах, как сетевые платы и видеоплаты.

Верификация осуществляется посредством сопоставления сигнатур, хранящихся в различных встроенных программах, с базами данных, где

хранятся санкционированные и запрещенные сигнатуры. Ваша системная плата должна иметь совместимость с интерфейсом UEFI, который необходимо активировать во встроенных программах перед установкой Windows 8.

Проверить, активирован ли протокол UEFI Secure Boot; для этого нужно выполнить следующую команду PowerShell:

confirm-SecureBootUEFI

Команда возвращает значение True, если Windows 8 выполняется в режиме UEFI.

Measured Boot. Это новая функция, доступная для антивирусных программ и базирующаяся на протоколе UEFI Secure Boot. Она подтверждает работоспособность системы на основе хранимого на микросхеме TPM журнального файла, который генерируется всякий раз во время загрузки системы.

Журнал содержит список хэшей, используемых для подтверждения целостности драйверов и компонентов, которые загружаются в процессе загрузки до запуска антивирусной программы. Журнальный файл может быть также защищен криптографическим ключом, выдаваемым модулю TPM. Будучи полностью загруженным, выполняемое в среде Windows антивирусное программное обеспечение может проверять хэши на наличие несанкционированных модификаций в загрузочных компонентах и драйверах.

Удаленная аттестация позволяет антивирусным программам, выполняемым на клиенте, направлять журнальный файл Measured Boot на сервер для верификации. Таким образом, при проверке собственной работоспособности клиентский компьютер не полагается исключительно на собственные данные.

Считается, что серверы более надежны, поэтому осуществляемое подобным образом подтверждение притязаний клиентских компьютеров является предпочтительным.

Система ELAM

Если системный драйвер Windows ELAM активирован, он загружается первым. Этот компонент позволяет драйверу ELAM, установленному в антивирусном программном обеспечении, классифицировать драйверы как надежные и ненадежные.

Затем эта информация вновь поступает на драйвер Windows ELAM, который определяет, нужно ли инициализировать следующие один за другим загрузочные драйверы на основе политики инициализации соответствующего драйвера.

Политику ELAM Boot-Start Driver Initialization Policy вы можете обнаружить в разделе Group Policy, доступ к которому осуществляется

последовательным выбором пунктов Computer Configuration, Administrative Templates, System, Early Launch Anti-Malware.

Активировав Boot-Start Driver Initialization Policy, вы можете настроить эту политику таким образом, чтобы инициализировались только надежные драйверы; надежные драйверы и драйверы с неизвестным статусом; надежные драйверы, драйверы с неизвестным статусом, а также ненадежные, но критически важные драйверы — или все драйверы. Если ваши аппаратные средства оснащены модулем TPM, модуль Windows Defender готов к взаимодействию со средствами ELAM без какой-либо предварительной настройки.

Электронный замок "Соболь"

Электронный замок "Соболь" – аппаратно-программное средство защиты ПК, сервера от несанкционированного доступа. «Соболь» применяется как устройство, обеспечивающее защиту как автономного ПК так и рабочей станции или сервера, входящих в состав локальной вычислительной сети.

Защита осуществляется за счет двухфакторной аутентификации, запрета загрузки ОС с внешних носителей, контроля целостности программной среды и ряда других факторов.

В частности, контроль целостности функционирует под управлением операционных систем, использующих следующие файловые системы: NTFS5, NTFS, FAT32, FAT16 и FAT12.

Администратор имеет возможность задать режим работы электронного замка, при котором будет блокирован вход пользователей в систему при нарушении целостности контролируемых файлов. Контроль целостности программной среды - позволяет контролировать неизменность файлов и физических секторов жесткого диска до загрузки операционной системы. Для этого вычисляются некоторые контрольные значения проверяемых объектов и сравниваются с ранее рассчитанными для каждого из этих объектов эталонными значениями.

Формирование списка подлежащих контролю объектов с указанием пути к каждому контролируемому файлу и координат каждого контролируемого сектора производится с помощью программы управления шаблонами контроля целостности.

Контроль целостности системного реестра Windows - повышает защищённость рабочих станций от несанкционированных действий внутри операционной системы.

Контроль конфигурации - ПАК «Соболь» позволяет контролировать неизменность конфигурации компьютера –PCI-устройств, ACPI, SMBIOS и оперативной памяти. Данная возможность существенно повышает защиту рабочей станции.

Linux

SysChk - инструмент для мониторинга целостности файловой системы для Linux. Он отслеживает неизменность файлов и каталогов, включая User Ownership, Group Ownership, File Permissions, Modified Time, Md5 Hash.

OSSEC - это хостовая система обнаружения вторжений с открытым исходным кодом. Она выполняет анализ логов, контроль целостности, мониторинг реестра ОС Windows, обнаружение руткитов, оповещения и реагирование на вторжения в реальном времени. Поддерживаемые ОС: Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows.

Open Source Tripwire - бесплатное программное обеспечение с исходным кодом, предназначенное для мониторинга целостности файловых систем.

Другие системы:

- AIDE (Advanced Intrusion Detection Environment)
- AFICK (Another File Integrity Checker)
- Samhain
- Stealth
- BSign
- Integrit
- Systraq

AIDE

AIDE — это система обнаружения атак уровня узла (Host-Based Intrusion Detection System, HIDS).

Возможности:

- Поддерживаемые хеши: md5, sha1, rmd160, tiger, crc32, sha256, sha512, whirlpool (additionally with libmhash: gost, haval, crc32b).
- Поддерживаемые атрибуты файлов: File type, Permissions, Inode, Uid, Gid, Link name, Size, Block count, Number of links, Mtime, Ctime and Atime.
- Поддержка для Posix ACL, SELinux, XAttrs and Extended file system attributes.
- Поддержка регулярных выражений.
- Поддержка сжатия БД с помощью gzip (если встроена zlib).
- Самодостаточные исполняемые файлы системы.

Команды AIDE

Инициализация БД:
 # aide -i

Обновление БД
#mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db

Проверка системы

 # aide -C (без обновления aide.db.new)

Проверка системы
 # aide -u (с обновлением aide.db.new)

Сравнение БД без сканирования
 # aide --compare

Чтобы работало сравнение БД в конфигурации нужно определить БД для сравнения:
database_new=file:/var/lib/aide/aide.db.new

Пример настройки AIDE

/etc/aide/aide.conf:

```
########## my rules ##########
LogsMy = p+u+g
########## logs files ##########
=/var/log$ StaticDir
/var/log LogsMy
# не учитывать архивы вида log.0.gz
!/var/log/(.*)(\.gz)?$
!/var/log/(.*)(\.bz2)?$
########## etc files ##########
/etc/ ConfFiles
!/etc/mtab
!/etc/udev/rules.d
!/etc/adjtime
!/etc/cron.d/vz
########## ssh files ##########
/root/.ssh ConfFiles
!/root/.ssh/known_hosts
/home/user/.ssh ConfFiles
!/home/user/.ssh/known_hosts
```

OSSEC

OSSEC это хостовая система обнаружения вторжений (HIDS), свободная и с открытым исходным кодом. Она ведёт анализ системных логов, проверку целостности, наблюдение за реестром ОС Windows, обнаружение руткитов, оповещение в заданное время и если будет обнаружено какое-либо событие.

Возможности OSSEC соблюдают некоторые правила PCI DSS.

OSSEC состоит из основного приложения, программы-агента для ОС Windows и веб-интерфейса.

Установка сервера OSSEC
wget -q -O - https://www.atomicorp.com/installers/atomic | sh && yum install ossec-hids ossec-hids-server

Все файлы OSSEC хранятся в /var/ossec
Файл настроек /var/ossec/ossec.conf

Настройка отправки сообщений на почту:
<global>
<email_notification>yes</email_notification>
<email_to>root@domain.local</email_to>
<smtp_server>smtp.domain.local</smtp_server>
<email_from>osssec@domain.local</email_from>
<email_maxperhour>200</email_maxperhour>
</global>

За проверку целостности отвечает секция **<syscheck>**
Например,
<syscheck>
<!-- Frequency that syscheck is executed - default to every 22 hours -->
<frequency>79200</frequency>
<!-- Directories to check (perform all possible verifications) -->
<directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes">/bin,/sbin</directories>
<!-- Files/directories to ignore -->
<ignore>/etc/mtab</ignore>
<ignore>/etc/mnttab</ignore>
<ignore>/etc/hosts.deny</ignore>
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>

<ignore>/etc/adjtime</ignore>
<ignore>/etc/httpd/logs</ignore>
<ignore>/etc/utmpx</ignore>
<ignore>/etc/wtmpx</ignore>
<ignore>/etc/cups/certs</ignore>
<ignore>/etc/dumpdates</ignore>
<ignore>/etc/svc/volatile</ignore>
</syscheck>

Запуск серверной части
#service ossec-hids start

После запуска на почту должно прийти сообщение:
OSSEC HIDS Notification.
…
ossec: Ossec started.

--END OF NOTIFICATION

Для удобства настройки агентов можно добавить web-интерфейс.

Журнальный файл по умолчанию /var/ossec/logs/ossec.log.

Установка агента

wget -q -O - https://www.atomicorp.com/installers/atomic |sh && yum install ossec-hids ossec-hids-client

Для настройки связи агентов с сервером нужно запустить специальную утилиту **/var/ossec/bin/manage_agents**

Результат работы утилиты - строка base64, необходимая клиенту.
Общение клиентов с сервером происходит по **UDP/1514.**

Перезапуск сервера
 # service ossec-hid restart

Проверка агентов на сервере из консоли:
/var/ossec/bin/list_agents -a

Контроль целостности пакетов в RPM-based и Deb-based дистрибутивах

RPM:
 # rpm --verify -a
DEB:

 # dpkg --verify

Вывод

В данной лекции мы рассмотрели такой важный механизм безопасности как контроль целостности. Изучили конкретные реализации механизмов контроля целостности в ОС Linux, Windows.

Задание для СРС

Виртуализация.

Практическое занятие

Windows

Осуществить проверку системных файлов с помощью утилиты sfc (>=Windows Vista).

Установить и протестировать demo-версию Verisys.

Linux

Настройка контроля целостности бинарных файлов с помощью aide.

Мониторинг целостности /etc/ с помощью ossec и с отправкой отчетов на почту.

Контроль целостности исполняемых файлов с помощью BSign.