Подготовка 1

- Предоставить компьютерным криминалистам физический доступ к инспектируемой системе.
- Выполнить побитовую копию диска исследуемой системы.
- Наличие физического доступа также может быть использовано для отсоединения исследуемой системы от внешних сетей
- Изучить детали функционирования сети/ системы в нормальных условиях. Заранее подготовить, задокументировать и держать данную информацию в надежном месте. Документация должна содержать детали стандартного использования портов, стандартные правила сетевого траффика и списки критических файлов (SUID и GUID) для возможности отследить характер и природу изменений.
- Изучить детали стандартной работы типовых сервисов на производственных серверах. В случае необходимости обратиться к эксперту по *nix-системам.

Обнаружение 2

Необычные учетные записи

Поиск необычных записей осуществляется в /etc/passwd, особенно под UID 0. Также проверить /etc/group и /etc/shadow.

Поиск файлов-сирот, потенциально оставленных использованными в атаке удаленными учетными записями: *# find / \(-nouser –o –nogroup \) -print*

Необычные файлы

- Поиск среди SUID и GUID файлов:

 # find / -uid 0 \(–perm -4000 –o –perm 2000 \) –print

- Поиск файлов с нехарактерных названиями, например начинающихся на “.”,”..” или “ “:

*# find / -name “ *“ –print*
*# find / -name “. *“ –print*
*# find / -name “.. *“ –print*

- Поиск больших файлов (>10Мб)

 # find / -size +10MB –print

- Поиск процессов, инициированных удаленными файлами: *# lsof +L1*

Обнаружение 2

- Поиск необычных файлов в /proc и /tmp. Данные директории часто используются хакерами для складирования данных или вредоносного ПО.

Необычные сервисы

Выполнить chkconfig для проверки запущенных сервисов:
 # chkconfig --list

Необычные процессы

 # ps -aux
Для неизвестных процессов: *lsof –p [pid]*
Внимание: теоретически, руткиты могут изменить результаты цитируемых здесь команд.

Для успешного обнаружения используемых хакерами процессов необходимо знание стандартных процессов системы. Следует обратить особое внимание на процессы, запущенные под UID 0.

Необычная сетевая активность

Для обнаружения сетевых снифферов:
Поиск в логах ядра интерфейсов, находящихся в режиме приема всех сетевых пакетов:
“*kernel: device eth0 entered promiscuous mode*”

Использовать *# ip link* для обнаружения флажка “PROMISC”. Использовать *ifconfig* для перекрестного контроля.

- Обнаружение необычной активности портов: *# netstat –nap* и *# lsof –i* для информации о процессах на портах.
- Поиск необычных записей MAC на LAN:

 # arp -a

- Идентифицировать все необычные IP адреса в сети.

Необычные автоматизированные задачи

- Поиск необычных заданий, запланированных пользователями из /etc/cron.allow. Обратить особое внимание на cron jobs от UID 0 (root):

 # crontab –u root -l

- Поиск необычных cron jobs по всей системе:

 # cat /etc/crontab and *# ls –la /etc/cron.**

Необычные записи логов

Поиск необычных записей логов, затрагивающих подозрительные события, как например:

Обнаружение 2

- Большое количество неудачных попыток авторизации для локальных или удаленных средств удаленного доступа (sshd, ftpd, etc.)

- Логи программ удаленного вызова процедур (RPC), содержащие большое количество нестандартных символов.

- Большое количество ошибочных Apache логов
- Перезагрузки оборудования
- Перезагрузки ПО

В большинстве *nix систем логи находятся в /var/log:

/var/log/message: Общие оповещения и системные логи
/var/log/auth.log: Логи авторизации
/var/log/kern.log: Логи ядра
/var/log/cron.log: Cron логи (cron job)
/var/log/maillog: Логи почтового сервера
/var/log/httpd/: Логи доступа Apache и логи ошибок
/var/log/boot.log: Логи загрузки системы
/var/log/mysqld.log: Логи базы данных MySQL
/var/log/secure: Логи авторизации
/var/log/utmp или **/var/log/wtmp:** Логи входа в систему

Для просматривания логов возможно использование cat или grep: *# cat /var/log/httpd/access.log | grep "GET / signup.jsp"*

Необычные логи ядра

- Поиск необычных событий в логах ядра.

dmesg
Детализация информации системы и ядра:
lsmod
lspci

- Для поиска известных руткитов использовать rkhunter и chkrootkit.

Хэши файлов

Проверить MD5 хэши файлов в /bin, /sbin, /usr/bin, /usr/sbin, а также в других директориях, содержащих бинарные файлы. Возможно использование AIDE.
Внимание: Данная операция может изменить метки последнего доступа к файлам. Рекомендуется осуществить операцию *после* завершения всех основных исследований.

Для систем, использующих RPM: *# rpm –Va | sort*
На некоторых Linux системах возможно использование скрипта *check-packages*.
На Solaris: # pkg_chk –vn
На Debian: # debsums –ac
На Openbsd: # pkg_delete -vnx
lsmod
lspci

Сдерживание 3

- Осуществить **побитовуя копию** содержимого диска инспектируемой системы на внешний носитель. Возможно использования *dd, ddrescue, FTK Imager,* CloneZilla, Encase, X-Ways или иного специализированного криминалистического ПО или оборудования.

- Создать копию системной памяти для дальнейшего анализа. Возможно использование **dd if=/dev/mem** of=/path/filename.

Если затронутая система критична для производственного процесса и не может быть отключена, создать резервную копию важных данных – на случай деструктивного поведения хакера и попыток удаления содержимого системы.

Если система некритична для производственного процесса, отключить подачу электрического питания. Если это лаптоп, притопить кнопку питания в течение нескольких секунд до полного отключения.

Если “живой” анализ системы не дает результата, необходимо приступить к расследованию по горячим следам в офлайн режиме, считая систему по умолчанию скомпрометированной.

Найти доказательства действий хакера:

- **Найти файлы, использованные злоумышленником**, включая удаленные (с использованием специализированного ПО) и установить их функционал в рамках данного использования. Эти сведения необходимы для оценки уровня угрозы.
- **Проверить файлы с недавним обращением.**
- **Проверить логи.**
- **Проверить общие сетевые ресурсы** на предмет распространения через них вредоносного ПО.
- **Установить каким образом злоумышленник получил доступ в систему**, рассмотрев все возможные варианты. Если не найдено доказательств вторжения извне, возможно был использован прямой физический доступ или помощь инсайдера.
- **Обновить ОС и ПО**: атакующая сторона могла воспользоваться уязвимостями.

Устранение 4

- Временно заблокировать доступ ко всем учетным записям, причастным к инциденту.
- Удалить файлы, установленные злоумышленниками.

Восстановление 5

Независимо от глубины проникновения хакеров и вашей осведомленности об инциденте, система остается потенциально уязвимой. **Наилучшее решение – тщательно проверив на наличие руткитов MBR, переустановить систему с нуля и применить все доступные обновления.** В данном случае также необходимо **сменить пароли для всех учетных записей**: пароли должны состоять из 12 и более символов, включать цифры, прописные и заглавные буквы и символы.

- Проверить целостность хранимых данных посредством MD5 хэширования.
- Восстановить все потенциально скомпрометированные бинарные файлы (Например в: /bin/su).

После инцидента 6

Отчет

Написать отчет об инциденте заражения; сделать отчет доступным членам Кризисной Группы. В рамках отчета необходимо раскрыть следующие темы:

- Причины инфекции
- Действия и сроки
- Верные действия
- Неверные действия
- Стоимость инцидента

Капитализация опыта

Формализовать и задокументировать опыт, накопленный в результате управления инцидентом с целью увеличения эффективности будущих действий.

SOCIETE GENERALE | CERT | SOCIETE GENERALE

Incident Response Methodology

cert.sg@socgen.com / cert.societegenerale.com / @certsg

IRM #3

Вторжение в *nix системы

Анализ атакуемых *nix систем

Автор IRM: CERT SG

Версия IRM: 1.4 (RU)

Об IRM

Данная методология по реагированию на инциденты ИБ является кратким руководством, предназначенным вниманию специалистов, работающих над проблемами безопасности:

- Системные администраторы
- Члены Security Operation Centers
- Начальники и представители отделов ИБ
- Представители CERT/CSIRT/IRT

Распространение IRM возможно в рамках SG Group.

В случае обнаружения признаков инцидента, следуйте рекомендациям IRM, делайте заметки, не поддавайтесь панике и немедленно оповестите свой CERT.

Фазы управления инцидентами ИБ

Шесть фаз управления инцидентами ИБ:

- **Подготовка**: подготовится к управлению инцидентом
- **Обнаружение**: идентифицировать проблему
- **Сдерживание**: ограничить негативный эффект
- **Устранение**: ликвидировать угрозу
- **Восстановление**: восстановить до нормального
- **После инцидента**: формализация и совершенствование процесса управления инцидентом

IRM предоставляет детальную информацию по каждой из фаз.