ANTCOLONY

Linux IR

Подсказки для системных администраторов

Для кого:

Системные администраторы нередко оказываются на передовой в вопросах обеспечения компьютерной безопасности.
Данный справочник направлен на то, чтобы помочь выявлять признаки компрометаций системы.

Когда использовать:

Регулярно (каждый день, каждую неделю или при каждом входе в управляемую вами систему) проходите эти простые шаги, чтобы обнаружить необычное поведение, которое может быть следствием взлома компьютера. Каждая из этих команд запускается непосредственно в системе.

Разделы:

НЕ ПАНИКУЙТЕ при обнаружении аномалий!

Возможно, ваша система подверглась атаке, а может быть, и нет. Пожалуйста, немедленно свяжитесь с группой по реагированию на инциденты, чтобы сообщить об обнаруженных явлениях и получить дальнейшие указания к действиям.

Нестандартные процессы и службы

Посмотрите на все запущенные процессы:

```
# ps –aux
```

Ознакомьтесь с «нормальными» процессами для данной системы. Ищите необычные процессы. Уделяйте особое внимание процессам с привилегиями root (UID 0)

Если вы обнаружили незнакомый процесс, проведите более детальное исследование с помощью:

```
# lsof –p [pid]
```

Данная команда показывает все файлы и порты, используемые запущенным процессом.

Если на вашем компьютере установлен chkconfig, запустите его, чтобы увидеть, какие службы включены на разных уровнях запуска:

```
# chkconfig --list
```

Нестандартные файлы

Ищите необычные корневые файлы SUID:

```
# find / -uid 0 –perm -4000 –print
```

Для этого требуется знание стандартных файлов SUID.
Ищите необычно большие файлы (**размером более 10МБ**):

```
# find / -size +10000k –print
```

Для этого требуется знание стандартных больших файлов.
Ищите файлы с именами, обозначенными точками и пробелами ("...", ".. ", ". ", и "), которые используются для маскировки файлов:

```
# find / -name " " –print
# find / -name ".. " –print
# find / -name ". " –print
# find / -name " " –print
```

Ищите процессы, которые завершают работу с файлами, на которые не были установлены ссылки, или обращаются к ним (т.е. количество ссылок равно нулю).
Злоумышленник может скрывать данные в таких файлах или запускать бэкдор из них:

```
# lsof +L1
```

Нестандартные файлы 01

На компьютере Linux с установленным RPM (RedHat, Mandrake и т. д.) запустите инструмент RPM для проверки пакетов:

```
# rpm –Va | sort
```

Проверяет размер, контрольную сумму MD5, права доступа, тип, владельца и группу каждого файла с информацией из базы данных RPM для поиска изменений.
Вывод включает:
S – размер файла отличается
M – режим отличается (права доступа)
5 – MD5 отличается
D – номер устройства не совпадает
L – путь readLink не совпадает
U – владелец пользователя отличается
G – владелец группы отличается
T – время изменения отличается

Обратите особое внимание на изменения, связанные с элементами в /sbin, /bin, /usr/sbin и /usr/bin.

В некоторых версиях Linux этот анализ автоматизирован с помощью встроенного скрипта проверки пакетов.

Необычное использование сети

Ищите признаки promiscuous mode, что может указывать на присутствие сниффера:

```
# ip link | grep PROMISC
```

Обратите внимание, что команда ifconfig не сможет точно указать на promiscuous mode в ядре Linux 2.4, поэтому, пожалуйста, используйте "ip link" для его обнаружения.

Ищите необычные прослушиваемые порты:

```
# netstat –nap
```

Узнайте больше о запущенных процессах, прослушивающих порты:

```
# lsof –i
```

Для выполнения этих команд требуется знать, какие порты TCP и UDP обычно прослушиваются в вашей системе. Ищите отклонения от нормы.

Ищите необычные записи ARP, сопоставляя IP-адреса с MAC-адресами, которые не подходят для локальной сети:

```
# arp –a
```

Этот анализ требует подробного представления о том, какие адреса должны быть в локальной сети.
В небольшом и/или специализированном LAN (например, в DMZ) ищите необычные IP-адреса.

Нестандартные запланированные задачи

Ищите задания cron, запланированные пользователем root, и любые другие учетные записи с идентификатором пользователя UID 0:

```
# crontab –u root –l
```

Ищите необычные общесистемные задания cron:

```
# cat /etc/crontab
# ls /etc/cron.*
```

Нестандартные учётные записи

Ищите в /etc/passwd новые учетные записи в списке, отсортированном по UID:

```
# sort –nk3 –t: /etc/passwd | less
```

Будут отображены стандартные учётные записи, но так же могут появиться странные учётные записи, особенно с UID < 500

Также обратите внимание на учётные записи с UID 0:

```
# egrep ':0+:' /etc/passwd
```

Для систем, использующих несколько методов аутентификации:

```
# getent passwd | egrep ':0+:'
```

Присмотритесь к потерянным файлам, которые могут указывать на то, что временная учётная запись злоумышленника была удалена:

```
# find / -nouser -print
```

Нестандартные записи в log'ax

Просмотрите файлы системного журнала на предмет подозрительных событий, в том числе:

- Включен promiscuous mode
- Большое количество неудачных попыток аутентификации или входа в систему с помощью средств локального или удаленного доступа (например, telnetd, sshd и т.д.).
- RPC программы с записью в журнале, содержащей большое количество (> 20) странных символов (например, ^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM)
- Для систем, на которых запущены веб-серверы: Количество логов Apache с сообщением "ошибка" превышает норму
- Перезагрузки и/или перезапуски приложений

Другие необычные элементы

Низкая производительность системы:

`$ uptime` – смотрите на "load average"

Чрезмерное использование памяти:

`$ free`

Внезапное уменьшение доступного дискового пространства:

`$ df`

Дополнительные вспомогательные инструменты

www.chkrootkit.org

Chkrootkit ищет аномалии в системах, вызванные программами типа RootKit в user-mode и kernel-mode

www.tripwire.org

Tripwire отслеживает изменения критически важных системных файлов. Бесплатно для Linux для некоммерческого использования

http://www.cs.tut.fi/~rammer/aide.html

AIDE также следит за изменениями критических системных файлов

http://www.cisecurity.org/

Центр интернет-безопасности выпустил руководство по усилению безопасности Linux

www.bastille-linux.org.

Бесплатный скрипт Bastille предоставляет автоматизированное средство усиления безопасности для систем Linux