ANTCOLONY

Windows 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

Ищите необычные/неожиданные процессы и сосредоточьтесь на процессах с именем пользователя SYSTEM или Administrator (или на пользователях из группы Administrators). Вам необходимо быть знакомым с обычными процессами и службами и искать отклонения.

Используя графический интерфейс, запустите Task Manager

```
C:> taskmgr.exe
```

Используя командную строку:

```
C:> tasklist
C:> wmic process list ful
```

Также ищите необычные службы.

Используя графический интерфейс:

```
C:> services.msc
```

Используя командную строку:

```
C:> net start C:> sc query
```

Для получения списка служб, связанных с каждым процессом:

```
C:> tasklist /svc
```

Необычное использование сети

Посмотрите на общие файлы и убедитесь, что у каждого из них есть определённое бизнес-назначение:

```
C:> net view \127.0.0.1
```

Посмотрите, у кого есть открытая сессия с компьютером:

```
C:> net session
```

Посмотрите, какие сессии этот компьютер открыл с другими системами:

```
C:> net use
```

Посмотрите на активность NetBIOS над TCP/IP:

```
C:> nbtstat –S
```

Ищите необычные прослушивающие TCP и UDP порты:

```
C:> netstat –na
```

Для постоянно обновляемого и прокручиваемого вывода этой команды каждые 5 секунд:

```
C:\> netstat –na 5
```

Флаг –o показывает идентификатор процесса-владельца:

```
C:> netstat –nao 5
```

Флаг –b показывает имя исполняемого файла и загруженные DLL для сетевого соединения.

```
C:> netstat –naob 5
```

Обратите внимание, что флаг –b использует чрезмерные ресурсы ЦП. Опять же, вам нужно понимать обычное использование портов для системы и искать отклонения.

Также проверьте конфигурацию файерволла Windows:

```
C:> netsh firewall show config
```

Нестандартные запланированные задачи

Ищите необычные запланированные задачи, особенно те, которые выполняются от имени пользователя из группы Administrators, от имени SYSTEM или с пустым именем пользователя. Используя графический интерфейс, запустите планировщик задач:

Start ▶ Programs ▶ Accessories ▶ System Tools ▶ Scheduled Tasks

Используя командную строку:

```
C:> schtasks
```

Также проверьте другие элементы автозагрузки на предмет неожиданных записей, не забывая проверить каталоги автозагрузки пользователей и разделы реестра.

Используя графический интерфейс, запустите msconfig и посмотрите вкладку:

Start ▶ Run , msconfig.exe

Используя командную строку:

```
C:> wmic startup list full
```

Нестандартные учётные записи

Ищите новые, неожиданные учётные записи в группе Administrators:

```
C:> lusrmgr.msc
```

Нажмите на Groups, дважды щёлкните по Administrators, затем проверьте участников этой группы.

Это также можно сделать в командной строке:

```
C:> net user
C:> net localgroup administrators
```

Нестандартные файлы и ключи реестра

Проверьте использование дискового пространства, чтобы выявить внезапное значительное уменьшение свободного места, используя графический интерфейс (щёлкните правой кнопкой мыши по разделу) или введите:

```
C:> dir c:
```

Ищите необычно большие файлы:

Start ▶ Search ▶
For Files of Folders... Search Options ▶ Size ▶
At Least 10000KB

Ищите странные программы, упомянутые в разделах реестра, связанных с запуском системы:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
```

Обратите внимание, что вам также следует проверить аналоги HKCU (замените HKLM на HKCU выше).

Используя графический интерфейс:

```
C:> regedit
```

Используя командную строку:

```
C:> reg query <reg key>
```

Нестандартные записи в log'ах

Проверьте свои журналы на наличие подозрительных событий, таких как:

- «Служба журнала событий была остановлена»
- «Защита файлов Windows неактивна в этой системе»
- «Защищённый системный файл [имя файла] не был восстановлен до исходной, действительной версии, потому что защита файлов Windows...»
- «Служба MS Telnet успешно запущена»

Ищите большое количество неудачных попыток входа в систему или заблокированные учётные записи.
Чтобы сделать это с помощью графического интерфейса, запустите средство просмотра событий Windows:

```
C:> eventvwr.msc
```

Используя командную строку:

```
C:> eventquery.vbs | more
```

Или, чтобы сосредоточиться на определённом журнале событий:

```
C:> eventquery.vbs /L security
```

Другие необычные элементы

Ищите необычно медленную работу и один необычный процесс, перегружающий ЦП:

Task Manager▶Process and Performance tabs

Ищите необычные сбои системы, выходящие за рамки обычного уровня для данной системы.

Дополнительные вспомогательные инструменты

Инструменты для сопоставления прослушивающих TCP/UDP портов с программой, прослушивающей эти порты:

http://www.foundstone.com/

Fport — инструмент командной строки

http://www.microsoft.com/technet/sysinternals

TCPView — инструмент с графическим интерфейсом

Дополнительные инструменты для анализа процессов:

http://www.microsoft.com/technet/sysinternals

Process Explorer — инструмент с графическим интерфейсом

http://www.diamondcs.com.au/

TaskMan+ — инструмент с графическим интерфейсом

http://www.cisecurity.org/

Центр интернет-безопасности выпустил различные шаблоны безопасности Windows и инструменты оценки безопасности бесплатно