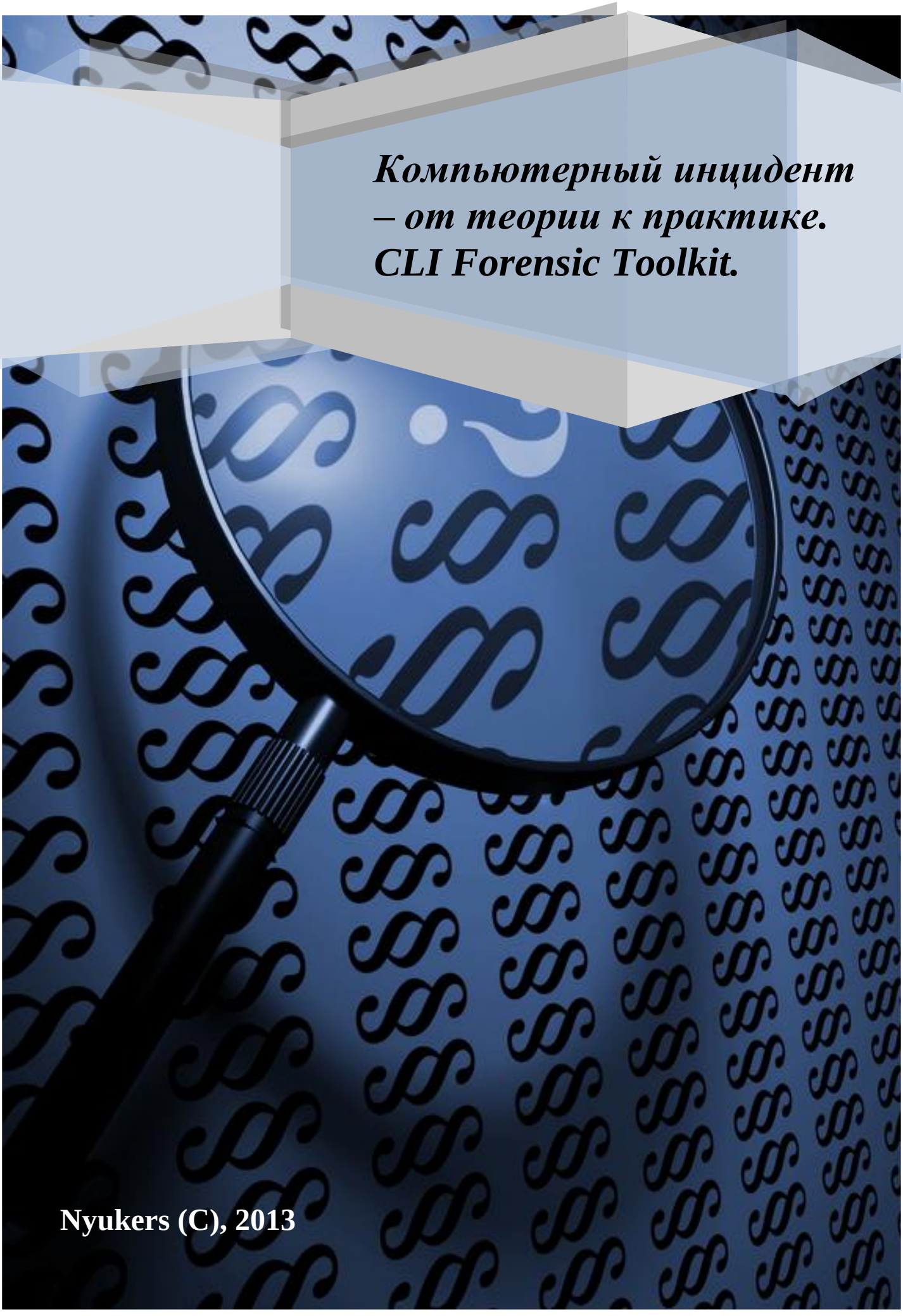

Компьютерный инцидент – от теории к практике. CLI Forensic Toolkit.

Nyukers (C), 2013

От автора

Пять назад изучал очень интересное руководство по исследованию компьютерных инцидентов. Автор документа подавал его даже для печати в солидный журнал. Но оказалось, что у рецензента было свое видение термина "**компьютерный инцидент".** Также резко выделялось практическое направление руководства, а это со слов того же рецензента будет мало понятно читателям журнала. Возможно он был прав – существуют же глянцевые издания и для теоретиков. Поэтому сегодня предлагаю это руководство вам, обновленное и дополненное.

От теории компьютерных инцидентов к практике их исследования. Бесплатный инструментарий исследователя. Это может каждый!

Оглавление

Компьютерный инцидент

Компьютерный инцидент - это аномальное явление, которое может влиять на конфиденциальность, целостность и доступность информации. Такой случай может указывать как на сбой в системе так и на злонамеренные действия. Сегодня субъектами совершения злоупотребления с использованием информационных технологий могут быть как сотрудники финансово-хозяйственных структур, так и посторонние лица, не работающие в банковских структурах - злоумышленники. Последние в большинстве случаев работают самостоятельно, по собственной инициативе, но не исключается также их сговор с отдельными работниками кредитно-финансовых учреждений. Поэтому общепринятый термин "офицер безопасности" приобрел иной смысл - информационного. Только когда за защиту каждого хоста корпоративной сети будет отвечать опытный офицер безопасности, имеющий в своем распоряжении необходимые инструменты защиты, можно будет говорить об адекватных мерах в отношении возможных внештатных случаев. Экспертиза аномального явления требует некоторого времени не только на поиск соответствующих специалистов, но и на ее производство, а при исследовании часто важным фактором, позволяющим сохранить необходимую доказательную информацию, является оперативность. Именно поэтому исследования компьютерных инцидентов приходиться проводить теми силами, которые существуют в данный момент. В этом случае исследователь сам не застрахован от ошибок [2].

Поставленная проблема имеет два аспекта: общие ошибки, допускаемые соответствующими сотрудниками отделов защиты информации при расследовании случаев, связанных с компьютерами и защиту (блокирование или уничтожение) информации, установленный на компьютерах их непосредственными пользователями или злоумышленником.

Рассмотрим некоторые типичные ошибки, которые часто случаются при проведении исследования инцидентов по отношению к компьютерной информации.

Ошибка 1. Запуск компьютера с ОС, которая на нем установлена, в течение исследования.

Первое и основное правило, которое неукоснительно должно выполняться: не допускается погрузка (перезагрузка) такого компьютера с использованием операционной системы самого компьютера! Такое правило объясняется довольно просто: злоумышленнику не составляет особого труда установить на компьютере программу для уничтожения информации на жестком или гибком магнитном диске, записав такую "мину" через модификацию операционной системы. После того как данные и сама разрушительная программа уничтожены, никто не сможет вероятных сказать, был ли компьютер-жертва специально оснащенный такими программами, или это результат небрежности при исследовании? Поэтому прежде всего необходимо убедиться через настройки BIOS и аппаратную конфигурацию компьютера относительно текущего приоритета электронных носителей для загрузки ОС на исследовании компьютере.

Ошибка 2. Отсутствие проверки компьютера на наличие вирусов и программных закладок.

Для проверки компьютера на наличие вирусов и программных закладок (программ-шпионов, перехватчиков нажатий на клавиши клавиатуры и т.п.), необходимо выполнять загрузку компьютера не из операционной системы находящейся в нем, а из своего заранее

подготовленного носителя. Кстати, такой проверке подлежат все носители информации - дискеты, магнитооптические диски и другие носители информации, которые принадлежат пользователю этого компьютера.

Для повышения достоверности результатов проверки относительно отсутствия программных закладок необходимо использовать наряду с антивирусным еще и специализированное ПО [17]: Lavasoft Ad-Aware, Xcleaner, Anti-keylogger.

Желательно для проверки использовать несколько версий программного обеспечения одного типа от разных производителей ПО с актуальными базами уязвимостей.

Ошибка 3. Допуск к компьютера пользователя этого компьютера при исследовании.

Серьезной ошибкой есть допуск к исследуемому компьютеру его пользователя для помощи при его исследовании. Сам пользователь с непониманием сложившейся ситуации может спровоцировать процесс безвозвратного уничтожения (повреждения) информации путем выполнения простых, на первый взгляд, действий, например, перезагрузка ОС компьютера. Это особенно касается случаев при расследовании деятельности связанной с Интернетом и отсутствием или очисткой с "уважительным" причинам журналов работы пользователя с ПО "Internet Explorer" и "Outlook Express", либо подобного.

Ошибка 4. Не отключение компьютера, который подвергся атаке, от информационной сети физически.

Работа в режиме одного монопольного пользователя на Windows-системе не даст возможности злоумышленнику и вредным процессам получать доступ к машине или изменять каким-либо образом ее состояние во время исследования.

Если не отключить машину от сети, может случиться так, что злоумышленник отменит действия, которые делаются исследователем на машине.

Ошибка 5. Не принятие возможных мер для снятия образа жесткого диска атакованного компьютера.

Прежде чем начинать анализ инцидента, нужно сделать полный бекап атакованой системы. Возможно в будущем понадобится вернуться к этим файлам. Создание "низкоуровневой" резервной копии является очень важным процессом, поскольку вполне вероятно, что понадобится вернуть атакованую машину в то состояние, в котором она находилась именно в момент, когда впервые было замечено несанкционироанное вторжение. Также, файлы могут понадобится для официального расследования. Заметьте, и отметьте дату резервной копии и храните ее в безопасном для хранения данных месте.

Корректные действия по устранению последствий инцидентов в компьютерной безопасности стоят на втором месте по важности, уступая лишь превентивным мерам по предотвращению этим инцидентов. Неправильная обработка, или сбор имеющейся информации может нанести непоправимый вред исследованию. Исследователи должны хорошо знать, какую информацию они намерены собирать, а также какие инструменты они могут использовать и какое влияние окажут эти инструменты на саму систему. Желательно, чтобы это влияние было нулевым!

Полный цикл компьютерного расследование проводится в шесть этапов [4, 11]:

1- получение оперативной информации системы (live response);
2- дублирование данных;
3- анализ полученных данных;
4- составление отчета и создание рекомендаций;
5- мероприятия по устранению последствий данного инцидента;
6- мероприятия по предотвращению подобных инцидентов в будущем.

Исследователи предполагают, что не каждая несанкционированное событие требует

полного исследования. Понятно, что каждый инцидент требует различных действий от исследователей. Существуют определенные типы информации, которые могут быть собраны и быстро проанализированы для того, чтобы определить, какие дальнейшие шаги следует сделать. Живой ответ позволяет собрать кратковременно существующие данные, которые теряются, когда машина-жертва выключается. Живой ответ может быть единственным шансом, если не зависящие от вас обстоятельства не позволяют выключить машину. Такой ответ может быть критически важным не только для определения дальнейших действий исследователя, но и с финансовой точки зрения. Исключение системы может оказаться очень дорогостоящим, тогда как необходимая для определения природы инцидента информация может быть легко собрана без этого. Поэтому лицо, ответственное за устранение инцидента должно хорошо понимать, какая информация может и должна быть собрана именно на этом начальном этапе.

Вариант набора инструментальных средств исследователя (CLI Forensic Toolkit)

Обычно при возникновении инцидента существуют первые шаги, ведущие к лог-файлам, например, таких как журнал событий (EventLog). Однако, после совершения атаки может остаться дополнительный процесс, который выполняется в памяти компьютера. Информация об этом процессе, такая как полный командный путь, принадлежность к имени пользователя, может быть беспрепятственно получена блоком утилит [5, 6, 7, 12, 13, 21]:

```
@ echo перечень открытых IP-портов
fprt
openports-lines-path
PortQry.exe-local-v
@ echo список процессов, выполняющихся в системе
pslist
tasklist
@ echo список служб, выполняющихся в системе
sclist
@ echo перечень последних входов пользователей в систему
psloggedon
ntlast
ntlast-v
@ echo перечень событий в системе которые регистрируются в журнале
auditpol
@ echo перечень библиотек типа DLL, загруженных в систему
listdlls
@ echo перечень задач, которые выполняются по расписанию
at
schtasks
```

Эти утилиты могут предоставить много информации о ресурсах, используемые процессом, но основной информации, названной выше, должно быть вполне достаточно для администратора или исследователя за устранение и обнаружения чего-либо подозрительного или необычного.

Временные метки на файловой системе, связанные с обращениями к файлам:

dir / t: a / o: d / s c: \

Временные метки на файловой системе, которые отвечают последним изменениям в файлах:

dir / t: w / o: d / s c: \

Временные метки на файловой системе, которые отвечают созданию файлов:

dir / t: c / o: d / s c: \

Злоумышленники могут скрывать свои инструментальные средства на томах NTFS через механизм, известный как "потоковая" передача файлов (file streaming). Когда инструментальные средства скрытые таким образом, то файлы в которых они спрятаны, не изменяются в размерах. Поэтому для выявления потоковых файлов используются следующие утилиты [18]:

lads c: \ / s

sfind c: \

При получении живой ответы важно исследователю прежде всего сделать резервную копию Windows EventLog как в двоичном так и в текстовом виде [10, 14]:

```
@ echo двоичный формат журналов
cscript evt.vbs / Host: Hostname
```

где evt.vbs имеет вид:

```
strComputer = "."
Set objArgs = WScript.Arguments
Set objNamedArgs = objArgs.Named
HostName = objNamedArgs ( "Host")
Set objWMIService = GetObject ( "winmgmts:" _
& "(ImpersonationLevel = impersonate, (Backup, Security))! \ \" & _
strComputer & "\ root \ cimv2")
Set colLogFiles = objWMIService.ExecQuery _
( "Select * from Win32_NTEventLogFile where LogFileName = 'Application'")
For Each objLogfile in colLogFiles
errBackupLog = objLogFile.BackupEventLog (HostName & "_app.evt")
If errBackupLog <> 0 Then
Wscript.Echo "The Application eventlog could not be backed up."
End If
Next
Set colLogFiles = objWMIService.ExecQuery _
( "Select * from Win32_NTEventLogFile where LogFileName = 'Security'")
For Each objLogfile in colLogFiles
errBackupLog = objLogFile.BackupEventLog (HostName & "_sec.evt")
If errBackupLog <> 0 Then
Wscript.Echo "The Security eventlog could not be backed up."
End If
Next
Set colLogFiles = objWMIService.ExecQuery _
( "Select * from Win32_NTEventLogFile where LogFileName = 'System'")
For Each objLogfile in colLogFiles
errBackupLog = objLogFile.BackupEventLog (HostName & "_sys.evt")
If errBackupLog <> 0 Then
Wscript.Echo "The System eventlog could not be backed up."
End If
Next
```

@ echo текстовый формат журналов
dumpel-l security-f USB_sec.txt
dumpel-l application-f USB_app.txt
dumpel-l system-f USB_sys.txt

В следующем блоке можно получить огромное количество информации о NetBIOS соединения исследуемой системы:
net use
net session
net file
net share
srvcheck \ \ Hostname
net view
net user
net accounts
net localgroup
net start
net config server
net config workstation
nbtstat-c
nbtstat-n
nbtstat-s

Для сбора временной информации, специфичной для Internet и Ethernet соединений системы используем блок команд:
netstat-ano
netstat-r
arp-a
ipconfig / all

Исследователь инцидентов должен получить содержимое Clipboard пострадавшей системы. В Clipboard могут храниться важные улики, даже содержимое файлов или пароли [7, 19]:
@ echo текстовый формат содержимого
pclip.exe
@ echo текстовый формат содержимого или двоичный формат в виде изображения формата JPG
clpview.exe / c

Если открыто на экране или свернут в панели задач окно "command prompt", то этот факт следует задокументировать, а затем запустить в нем команду doskey / history для получения истории выполненных команд.

Исследователю может также понадобиться информация из реестра подозреваемой машины. Хотя эта информация не может считаться временной, часто информация из реестра помогает принять решение относительно состояния исследования: есть смысл или нет выключать компьютер для снятия образа жесткого диска, и т.п. Особенно это касается содержания ключей реестра автозапуска программ при старте системы [14, 19]:
reg query "HKLM \ Software \ Microsoft \ Windows NT \ CurrentVersion \" / v
autorunsc-s-w-a
reg query "HKLM \ Software \ Microsoft \ Windows NT \ CurrentVersion \ WinLogon"
reg query "HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Run" / s

```
reg query "HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce" / s
reg query "HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnceEx" / s
reg query "HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices" / s
reg query "HKLM \ Software \ Microsoft \ Windows NT \ CurrentVersion \ AeDebug" / v
Debugger
reg query "HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run" / s
reg query "HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce" / s
reg query "HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnceEx" / s
reg query "HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices" / s
reg query "HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ URL \ Prefixes" / s
reg query "HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ URL \
DefaultPrefix" / s
reg query "HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ Browser
Helper Objects" / s
@ echo архив кустов реестра ОС в двоичном формате
reg export HKLM HKLM.reg
reg export HKCU HKCU.reg
reg export HKCR HKCR.reg
reg export HKCC HKCC.reg
reg export HKU HKUsers.reg
```

Не менее ценной может стать информация об установленных servicepack и обновления на исследуемой системе [10, 14, 20]:

```
reg query "HKLM \ Software \ Microsoft \ Windows NT \ CurrentVersion \ Hotfix \" / v
reg query "HKLM \ Software \ Microsoft \ Updates \ Internet Explorer 6 \ SP1 \" / v
reg query "HKLM \ Software \ Microsoft \ Updates \ Internet Explorer 6 \ SP2 \" / v
@ echo ОС WinXP
reg query "HKLM \ Software \ Microsoft \ Updates \ Windows XP \" / v
reg query "HKLM \ Software \ Microsoft \ Updates \ Windows XP \ SP1 \" / v
reg query "HKLM \ Software \ Microsoft \ Updates \ Windows XP \ SP2 \" / v
reg query "HKLM \ Software \ Microsoft \ Updates \ Windows XP \ SP3 \" / v
@ echo ОС Win2003
reg query "HKLM \ Software \ Microsoft \ Updates \ Windows 2003 \" / v
reg query "HKLM \ Software \ Microsoft \ Updates \ Windows 2003 \ SP2 \" / v
reg query "HKLM \ Software \ Microsoft \ Updates \ Windows 2003 \ SP3 \" / v
@ echo запрос через MBSA
mbsacli / hf / v
@ echo запрос через WMI
cscript hotfixes.vbs
где hotfixes.vbs имеет вид:
strComputer = "."
Set objWMIService = GetObject ( "winmgmts:" _
& "(ImpersonationLevel = impersonate)! \ \" & StrComputer & "\ root \ cimv2")
Set colQuickFixes = objWMIService.ExecQuery _
( "Select * from Win32_QuickFixEngineering")
For Each objQuickFix in colQuickFixes
Wscript.Echo "Компьютер:" & objQuickFix.CSName
Wscript.Echo "Сервиспак ID:" & objQuickFix.HotFixID
Wscript.Echo "Описание:" & objQuickFix.Description
Wscript.Echo "Дата установки:" & objQuickFix.InstallDate
Wscript.Echo "Под каким пользователем установлено:" & objQuickFix.InstalledBy
Next
```

Важной информацией может стать расширенный перечень не системного ПО установленного в ОС [10]:

```
@ echo запрос через WMI
cscript installed.vbs
```

где installed.vbs имеет вид

```
strComputer = "."
Set objWMIService = GetObject ( "winmgmts: \ \" & strComputer & "\ root \ default")
Set colItems = objWMIService.ExecQuery ( "Select * From InstalledSoftware")
For Each objItem in colItems
Wscript.Echo "Key name:" & objItem.KeyName
Wscript.Echo "Display Name:" & objItem.DisplayName
Wscript.Echo "Display Version:" & objItem.DisplayVersion
Wscript.Echo "Install Location:" & objItem.InstallLocation
Wscript.Echo "Installation Date:" & objItem.InstallDate
Wscript.Echo "Install Source:" & objItem.InstallSource
Wscript.Echo "Uninstall String:" & objItem.UninstallString
Next
```

Однако здесь следует отметить, что такой запрос не дает достоверной информации по следующим причинам:
- существует ПО, которое не оставляет информацию относительно своего места нахождения (Install Location) и дать установки (Installation Date);
- существует ПО, которое вообще не требует инсталляции и может бути запущено в ОС после простого копирования на диск системы.

При расследовании эксперту-офицеру безопасности часто необходимо возобновить действия пользователя на компьютере или те, которые были проведены от имени пользователя. Разумеется, когда пользователь компьютера такая же жертва как и сам атакованный компьютер, то это предполагает один план действий. Если же пользователь компьютера "замел следы своего творчества", то в этом случае процесс трудный, но не безнадежен. Благо, что последние версии Windows оставляют следы действий пользователя во многих местах. Из анализа данных и взаимной корреляции временных меток этих данных можно восстановить действия пользователя или пользователей за определенный период.

Вот неполный перечень источников данных в системе Windows:
- отдельного более развернутого толкования заслуживает анализ журналов событий в системе (log-файлы). Для подобного анализа удобно использовать инструментальное средство типа LogParser [22], который позволяет с минимальными знаниями языка запросов SQL изучить практически любые отчеты txt-формата. Естественно для такого же анализа использовать инструментарий WMI, который имеет достаточную универсальность и даже прототип SQL-языка язык WQL [10];
- буфер обмена "Clipboard": нахождение информации как в текстовом так и в двоичном формате, которая возможно отсутствует в файлах ОС;
- корзина "Recycle bin": файл INFO2 в папках RECYCLER для томов под NTFS и папках Recycled для томов под FAT32;
- точки восстановления "System Volume Information": файлы change.log.x и временные дампы журналов событий и реестра ОС (snapshot);
- временные файлы работы, создаваемых при работе с сервисами сети Интернет: файл index.dat от "Internet Explorer" или "Netscape Communicator" который содержит информацию о деятельности пользователя как в Интернете так и на локальных дисках,

файлы почтовых папок *. pst и *. dbx от почтовых клиентов "OutlookExpress", файлы *. tbb от поштового клиента "The Bat!", fat.db, файлы *. hst и *. msf от поштового клиента "Netscape / Mozilla";
- файлы thumb.db в любой папке где есть или были графические файлы;
- файл подкачки оперативной памяти: pagefile.sys.

После того, как первоначальная информация была собрана необходимо получить контрольные суммы (MD5-хэш) системных файлов Windows, перечень которых следует подготовить заранее. В процессе анализа можно будет сравнить эти контрольные суммы с эталонами, которые были собраны ранее на тестовом компьютере.

Результаты исследования (в виде файлов) нужно защитить с помощью **цифровой подписи**. С помощью цифровой подписи можно определить авторство данных и гарантировать их целостность, то есть отсутствие в этих результатах любых изменений. При добавлении цифровой подписи к результатам их можно передать дальше для более глубокого анализа другому исследователю или в качестве приложения прикрепить до окончательного отчета. Цифровые подписи в Windows создаются с помощью цифровых сертификатов [15]. Исследователь сам может создать собственный сертификат с помощью программы SelfCert.exe из пакета Microsoft Office. Тогда цифровая подпись, например, файла результата result.txt с помощью сертификата под именем "FIO_Investigator" накладывается просто:

```
cScript putsign.vbs
```

где putsign.vbs являются:

```
set objSigner = WScript.CreateObject ( "Scripting.Signer")
objSigner.SignFile "result.txt", "FIO_Investigator"
```

Проверка цифровой подписи будет не более сложной задачей:

```
cScript signcheck.js
```

где signcheck.js являются:

```
var Signer, File, ShowUI, FileOK;
Signer = WScript.CreateObject ( "Scripting.Signer");
File = "result.txt";
FileOK = Signer.VerifyFile (File, false);
if (FileOK) WScript.Echo ( "Файл" + File + "является надежным");
else WScript.Echo ( "Файл" + File + "поврежден!");
```

Инструментальные средства для дублирования жесткого диска (получение образа) пораженной системы, а также инструменты для дальнейшего анализа таких образов достаточно известны и подробно представлены во многих источниках [3, 4, 6, 11].

Применение набора инструментальных средств

После сбора необходимых утилит целесообразно добавить автоматизацию их использования с помощью скриптов, что уменьшит возможность ошибок и потери информации. Можно предложить несколько вариантов реализации этого:

1. Копирование, например, на дискету набора утилит и написания скрипта, который их запускает, имеет много преимуществ. Во-первых, процесс автоматизирован и может легко быть улучшен модификацией скрипта. Во-вторых, использование внешнего накопителя,

позволяет выводить собранную информацию на сам накопитель, не затрагивая возможные улики на жестком диске системы. В третьих, автоматизируя процесс, исследователь инцидента имеет меньше шансов совершить ошибку, такую как опечатка в наборе команды или ввод неправильных ключей в аргументах команды. В четвертых, есть возможность быстро сделать дубль получения результатов для самоконтроля.

2. Другой метод получения информации из системы без записи ее на жесткий диск состоит в перенаправление ее на другой компьютер по сети. Одна из наиболее популярных программ, предлагающих такую возможность - это Netcat [5].

3. Альтернативой использованию Netcat может быть разработка пакета программ, основанный на технологии клиент-сервер, где весь процесс сбора и передачи информации автоматизирован. Проект такого пакета можно увидеть на Forensics Server Project (FSP) [7], где компоненты сервера и клиента написанные на скриптовом языке Perl. FSP является попыткой использовать скриптового языка для запуска утилит, сбора и экспресс-анализа данных с компьютера-жертвы.

4. Альтернативным методом для исследователя инцидентов может быть создание CD с утилитами и скриптами. Это позволяет записать большее количество утилит на один носитель, включая и Windows утилиты типа nbtstat.exe, netstat.exe, net.exe т.п., что обеспечит дополнительную безопасность за счет гарантированного использования оригинальных утилит и невозможности их компрометации в процессе использования.

Поскольку командной оболочки ОС на машине-жертве может быть изменена (так происходит после того, как учетная запись администратора был сломан), то человек, расследует атаку, не может доверять ее выводам. Поэтому при расследовании инцидента исследователь должен принести свою собственную оболочку. Надежная командная оболочка - это оригинальный файл cmd.exe. Кроме того, чтобы не нарушать файлы на исследуемой машине, он должен иметь на отдельном носителе все сопутствующие библиотеки (DLL) и вспомогательные файлы, необходимые для работы каждого исполняемого файла с нашего набора инструментов.

Здесь уместно будет предложить использования в качестве носителя инструментария CD с Windows XP собран по технологии Windows Preinstallation Envinronment [8].
Microsoft Windows Preinstallation Environment (WinPE) является облегченной версией Windows XP, который запускается с любого носителя достаточной емкости - в частности, только для чтения. Система предназначена для подготовки компьютера к установке полноценной ОС. С помощью WinPE можно разбить жесткий диск на разделы и отформатировать их, получить доступ к локальной сети и существующим разделам, включая имеющие формат NTFS, а также попытаться восстановить работу системы и спасти данные.

Иными словами, это так сказать »**LiveCD»** на базе Windows, способный загружаться с любого носителя (CD / DVD / Flash-память) даже при полном отсутствии жесткого диска. На таком диске может находиться загружаемая (bootable) ОС Windows XP Pro плюс необходимые инструменты исследователя инцидента как с command line interface, т.е. запускаемых в командной строке, так и с GUI-интерфейсом, антивирусные сканеры, другое [9]. При использовании LiveCD для получения живой ответе можно использовать просто как надежный носитель набора инструментов исследователя. Как уже сказано выше, для организации носителя ответы используется известная утилита Netcat, позволяющий передачу собранной информации по сети на машину-адресат, на которой будет проведена дальнейшая экспертиза. Чтобы не использовать сеть - можно предложить

в качестве носителя ответы использования USB flash-drive, который к тому же сейчас имеет и программная защита данных. В этом случае собранные данные не уязвимы к перехвату, потери или искажения при передаче по сети. В случае загрузки с LiveCD следует учитывать что исследователь может работать сразу на этапе анализа имеющихся данных. То есть, он не получит полной живой ответа, и не тратит время на дублировании данных. К тому же в этом случае у него есть реальная возможность выяснить проблемы с аппаратным обеспечением компьютера-жертвы и их возможным влиянием на случившееся, а также таким образом можно избежать тех типичных ошибок исследования о которых уже шла речь.

Одно из основных положений компьютерной экспертизы заключается в том, чтобы никоим образом не изменить первичные доказательства. К сожалению загрузочный диск DOS или Windows 98 содержит файл io.sys с жестко закодированными ссылками на диск "C: \". Если на исследуемой машине, например, используется сжатие диска DriveSpace, то наш загрузочный диск может попытаться загрузить драйвера с логического диска "C: \" и смонтировать логично несжатые файловую систему, изменяя дату и временные метки на файлах уплотненного диска. Чтобы этого не случилось, нужно исправить или сам файл io.sys или использовать опять же LiveCD. А вариант LiveCD с возможностью загрузки с CD нескольких операционных систем (DOS, Windows 98, Windows XP, Linux, другие) по выбору вообще может быть идеальным средством для исследователя. Например, наиболее дешевое и простое решение объединить большие возможности сетевых утилит систем типа Linux с Windows является использование пакета Cygwin [16].

Или в качестве альтернативы возможно использование **виртуальных машин** с помощью программного обеспечения от VMWare (Worksation / Server), Microsoft (Virtual PC) или Innotek (VirtualBox [23]). То есть исследователь имеет в своем использовании несколько виртуальных операционных систем с необходимым набором инструментов для исследования, которые кстати можно перенастраюваты за ситуацией. В таком варианте важно то что исследователь имеет возможность запустить несколько разнотипных ОС одновременно, при этом возможно исследование через сеть, сетевая карта самого компьютера исследователя работает в bridged mode, то есть каждая виртуальная ОС выглядит как отдельный компьютер в сети. В противном случае для быстрого развертывания образа с компьютера жертвы исследования также возможно использование виртуальной ОС. При этом не требуется отдельный компьютер, данные для экспертизы защищены вроде "песочницы", есть возможность делать мониторинг исследуемой системы с помощью снимков текущего состояния (snapshot). Обычно есть возможность запустить более чем один экземпляр образа одновременно для сравнения.

Еще в одном случае возможно оперативное исследования образа жертвы с использованием виртуальной ОС, который находится на диске USB-flash Или размещен при помощи так называемой функции "Shared folders". Во всех этих случаях исследователю нет необходимости волноваться за функционирование самой виртуальной ОС от возможной активности вредоносного кода в исследовании системы, так как восстановление и запуск новой виртуальной ОС с шаблона это дело нескольких минут.

Бесплатный коррелятор данных

Как известно, сами по себе операционные логи в компьютерных системах доказательной силы по случаю выявления атаки не имеют. Доказательством атаки могут служить только производные от этих логов, а именно:

- протокол осмотра пораженного атакой узла
- заключение эксперта-специалиста по информационной безопасности
- квалифицированная интерпретация логов.

Поддержка корректности и неизменнолсти логов на этапе их жизненного цикла от генерации одной программой до интерпретации человеком или другой программой является обязательной.
При этом содержимое разных лог-файлов как с самого узла так и имеющих к инциденту отношение, но находящихся вне узла (на других узлах) может:

- совпадать
- быть подножеством другого
- частично пересекаться по времени или другому признаку
- дополнять друг друга по времени или другому признаку
- не совпадать.

Поэтому **доказательная сила логов заключается в их корректной интерпретации.** Следовательно основная работа эксперта во время интерпретации заключается в выявлении взаимосвязей между различными записями в лог-файлах, которые отражают те или иные события. Другими словами, специалист занимается ручной корреляцией событий. К примеру если это сервер MS IIS то отслеживание событий web-сайта приходиться выполнять напрямую по следующим журналам:

- системный
- безопасность
- приложения
- служба каталогов
- сервер IIS
- служба репликации файлов
- сервер DNS.

При этом сами типы корреляций могут быть следующие:

- **локальная корреляция**, осуществляемая непосредственно на защищаемом узле. В этом процессе участвует система обнаружения и предотвращения атак уровня узла если таковая имеется, которая либо отражает атаку, о чем оповещает администратора безопасности, либо нет
- **корреляция со сведениями об операционной системе**. Если Windows-атака направлена на Unix-узел, то ее можно просто игнорировать. Если же ОС входит в список уязвимых для данной атаки, то в действие вступает следующий вариант корреляции
- **корреляция атак и уязвимостей**. Следуя определению атаки, она не может быть успешна, если атакуемый узел не содержит соответсвующей уязвимости. Таким образом, сопоставляя данные об атаке с информацией об уязвимостях атакуемого узла, можно с уверенностью будет сказать, применима ли зафиксированная атака к вашей сети и, если да, то нанесет ли она вам какой-либо ущерб
- **корреляция по времени наступления события**. Корреляция позволяющая сопоставить разнородные события от разных источников в один момент времени и представить общую схему атаки
- **корреляция по типу события**. Некоторое событие повлекло или могло повлечь другое событие. Такую корреляцию довольно сложно реализовать простыми инструментами и поэтому в этом случае требуется вмешательство специалистов, которые расследуют инциденты.

Конечно не обязательно строить корреляцию вручную. Число автоматических систем корреляции постоянно растет и к ним, например, можно отнести:

- Forensics компании.
- Private l компании Open Systems.
- Security Manager компании Intellitactics.
- SPECTRUM Security Manager компании Aprisma Management Technologies.
- SystemWatch компании OpenService.
- ArcSight одноименной компании.
- neuSECURE компании GuardedNet.

Компания IBM предлагает систему RealSecure SiteProtector, которая обладает механизмами консолидации, агрегирования и корреляции событий, получаемых не только от всех своих решений в области обнаружения атак и анализа защищенности, но и от межсетевых экранов Check Point Firewall-1 и Cisco PIX Firewall. Компания Cisco предлагает систему CiscoWorks Security Information Management Solution, которое построено на базе широко известной за рубежом системы управления информационной безопасности netForensics одноименной компании. Компания Symantec предлагает систему Symantec Incident Manager и семейство DeepSight, вошедшее в пакет предложений Symantec после покупки последней компании SecurityFocus. Все вышеперечисленное для эксплуатации требует определенных инвестиций и подготовленных кадров. А что делать если таких кадров нет или соответствующие средства не выделяются должным образом? Количество различных задач, а следовательно, и их логов которые нуждаются в нашем контроле растет с каждым годом. Оперативность визуального контроля как и его точность зависит от человеческого фактора как никогда. К сожалению не многие руководители понимают опасность роста такого риска. Ряд технических вопросов ложится на авось которого зовут - администратор Боб, забывая что Боб такой же человек как и все остальные. И что делать сейчас Бобу?!

А найти бесплатный выход!

Вот хотя бы **MS LogParser**. Сокращенно LP. Что может LP достаточно подробно описано в интернете. Главное что LP позволяет поддерживать четыре основных механизма обработки анализируемых событий:

- консолидация (event consolidation).
- агрегирование (event aggregation).
- корреляция (event correlation).
- приоритезация (event prioritization).

Для уверенности приведу сравнение названных механизмов у такого гранда как RealSecure SiteProtector (далее SP) и простого LP в таблице.

Обработка событий	**SiteProtector + Security Fusion модуль**	**LogParser**	**Реализация**
1	2	3	4
Консолидация	есть	есть	SP – MS SQL LP - через ODBC DSN (OLE DB Provider) путем использования VBScript в БД любого типа

Агрегирование	есть	есть	LP - SQL запрос с последующей записью в БД
Корреляция	есть	есть	LP - SQL запрос к поддерживаемому формату источника данных или SQL запрос к неподдерживаемому формату источника данных через ODBC DSN (OLE DB Provider)
Приоретизация	есть	есть	LP - SQL запрос с последующей записью в БД или генерацией корректирующего скрипта
Блокировка атаки (Prevention System)	есть	ограничено	SP – Intrusion Prevention System LP - генерация корректирующего скрипта
Запрос из стороннего источника данных (third party source)	есть	есть	SP- Java plug-in LP - через ODBC DSN (OLE DB Provider) путем использования VBScript из источника любого типа
Многомерные отчеты (OLAP)	ограничено	есть	SP- встроенный модуль FastAnalysis на базе JRE LP- SQL запрос к предварительно подготовленным данным
API	есть	есть	SP - TCL, Java LP - COM object

К тому же LP позволяет обращаться ко многим форматам файлов данных напрямую. А за два шага (два SQL - запроса), через промежуточный формат NAT, можно скоррелировать данные практически из любых источников данных. Необходимы знания лишь известных языков SQL и VBScript (WSH+WMI), которые для современного системного администратора являются базовыми после английского. В зависимости от формата вывода можно выполнить мультиплексный вывод, т.е. в зависимости от события формируется название выходного файла. Напротив в мультиплексном вводе есть поддержка поля "LogFileName", пока не для всех форматов. Примеры реализации названных механизмов LP здесь не приводятся потому как их можно с успехом найти как на официальном сайте Microsoft.

Единственное, чего всегда не хватало LP - это удобного графического пользовательского интерфейса! Тяжело администратору со временем управлять различными запросами и скриптами, которые со временем у него накапливаются. Первой попыткой реализовать такую полезную функцию был независимый проект Visual LogParser. И было это 6 лет назад. К сожалению далее проект не развивался, поэтому на сегодня версия его так и осталась 1.0 beta. Visual LogParser доступен для скачивания даже сейчас, но мне так и не удалось его запустить, он упорно не хотел видеть сам LP.

И вот год назад сам Microsoft обратил свои взоры на фанов LP и… выпустил Log Parser Studio! **Log Parser Studio** (сокращенно **LPS**) позволяет хранить все запросы в одном централизованном расположении. Можно редактировать и создавать новые

запросы в редакторе запросов и сохранять их для последующего использования. Можно искать запросы по полнотекстовому индексу, а также экспортировать и импортировать библиотеки и запросы в разных форматах, что упрощает совместную работу, а также хранение различных типов отдельных библиотек для разных протоколов [24].

Как видите коррелятор данных на базе LP/LPS позволяет не делая дополнительных инвестиций за короткое время прозрачно настроить и:
- выполнять автоматически анализ журналов регистрации разнородных средств защиты, что позволяет существенно уменьшить время, затрачиваемое на такой анализ;
- сэкономить средства и время на анализ, который, в случае отсутствия механизма корреляции, приходится выполнять вручную, что требует уйму времени;
снизить число ложных срабатываний и оповещений о нарушениях политики безопасности.

Кофе от Microsoft

Для тех кто все еще сомневается, что выше речь шла о полезных инструментах я могу упомянуть следующее – с 2009-го года Microsoft работает над проектом под кодовым названием Cofee.

Что же это такое? Программный комплекс Cofee (Computer Online Forensic Evidence Extractor – интерактивный извлекатель доказательств из компьютеров) представляет собой USB-накопитель, на которой записано более 150 специализированных программ, помогающих собирать электронные доказательства нелегальной деятельности на месте преступления. Технически, система Cofee в большей степени ориентирована на работу с цифровыми уликами - фотографиями, записями мобильных телефонов, данными аудио и видео наблюдения. Однако, пожалуй, главным преимуществом технологии являются ее развитые аналитические возможности - Cofee способна создавать целостные данные из фрагментарных доказательных элементов таким образом, чтобы их можно было представить в суде.

Не каждый может получить в свое распоряжение флэшку с Cofee – Microsoft собирается тщательно контролировать распространение столь мощного инструмента. По некоторым неподтвержденным сведениям, инструменты Cofee позволяют обойти самые стойкие пароли с помощью специальных функций, тайно встроенных в Windows. Кроме того, утилиты Cofee позволяют извлечь электронные свидетельства преступлений с компьютеров таким образом, чтобы не оставлять за собой никаких следов, способных повлиять на принятие этих доказательств в суде.

Заметили аналогию? А ведь этим занимается не кто нибудь, а Microsoft ! И одна из самих полезных функций в Cofee – это корелляция выходных данных.

Выводы

Таким образом, любая аномалия, обнаруженная мониторинговой системой или человеком, может оказаться вредоносным инцидентом. После того, как событие расценивается как злонамеренное, персонал, отвечающий за решение таких проблем, должен руководствоваться специализированными процедурами, подготовкой для действий в подобных ситуациях. Выполнение этих процедур рекомендуется осуществлять поэтапно как отмечено в "Computer Security Incident Handling Step by Step" института SANS [3]:

1. **Подготовка (preparation).** Задачи, стоящие на данном этапе, должны быть решены до фактической реакции на злонамеренный инцидент. Они включают формализацию политик и процедур, обучение персонала и подготовку каналов связи для организации связи с людьми в вашей орагнаизации и за ее пределами.

2. **Идентификация (indentification).** На данном этапе основные усилия исследователя-офицера безопасности должны быть направлены на присвоение инцидента статуса. Важно на этом этапе установить, действительно ли инцидент является злонамеренным. Если это подтверждается, то исследователь проводит оценку области инцидента, устанавливает последовательность мероприятий по сохранению информации с учетом накопленных доказательств и уведомляет соответствующие службы.

3. **Ограничение распространения (containment**). На данном этапе необходимо установить стадию для дальнейшего анализа, предотвращая в то же время эскалации инцидента. Так, исследователь создает резервные копии поражений систем для того, чтобы для дальнейшего использования были доступны первичные симптомы поражения. Исследователь также оценивает степень риска продолжающихся операций, просматривая журналы, обращаясь к экспертам и консультируясь со службой сопровождения систем. Ограничить распространение инцидента можно, определив степень расширения компрометации и выключив соответствующие системы или заблокировать доступ злоумышленнику.

4. **Искоренение (eradiction).** На данном этапе исследователь устанавливает причину злонамеренного инцидента, укрепляет защиту систем и закрывает уязвимости, которые могут позволить злоумышленнику продолжить атаку.

5. **Восстановления (recovery).** Этот этап посвящен восстановлению и проверке пораженных систем, возврату операций бизнеса в нормальное состояние и продлению внимательного наблюдения за скомпрометированным системами. На данном этапе организации необходимо решить, готова ли она возобновить осуществление операций в полном объеме.

6. **Этап завершения (follow up).** На данном этапе исследователь инцидента составляет отчет, в котором он оценивает действия команды, которая работала над данным инцидентом. Этот этап помогает повысить степень защищенности организации, решая те проблемы, которые могут в дальнейшем привести к возникновению компрометации. На данном этапе команда реагирования реализует действия, одобренные руководством.

Офицеры безопасности как исследователи компьютерных инцидентов могут сохранить большое количество времени, сил и нервов, готовясь к таким случаям заранее. Пожалуй, наиболее эффективными мерами подготовки к инцидентам является продуманный защиту хостов в сети, что поможет предотвратить их возникновение. Однако, инциденты все же случаются и исследователи должны быть готовы к адекватным действиям.

Полезные источники

1. Попов В. И. Информбандитизм и борьба с ним - офицеры безопасности. [http://www.confident.ru]

2. Голубев В.А., Хряпинський П.В. Особенности проведения следственных действий на початковову этапе расследования компьютерных преступлений. [http://www.crime-research.ru]

3. Inside Network Perimeter Security, By Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey Publisher: Sams Publishing Pub Date: March 04, 2005 ISBN: 0-672-32737-6 Pages: 768.

4. Кении Мандиа, Крис Проси прощения, Защита от вторжений. Расследование компьютерных преступлений,-М.: Издательство "ЛОРИ", 2005. - 476 с.

5. Разумов М., Руководство ответственного за устранение инцидентов в Win2k. [http://www.securitylab.ru]

6. Stephen Barish, Windows Forensics: A Case Study. [http://www.securityfocus.com/infocus/1653]

7. H. Carvey, Online Forensics of Win/32 System. [http://www.windows-ir.com/tools]

8. Microsoft Windows Preinstallation Environment (WinPE).

[http://www.microsoft.com/Rus/Licensing/Volume/Software_Assurance/AdvantagesOverview/WinPe]

9. LiveCD INFRA. [http://www.philka.ru]

10. Попов А.В., Шикина Е.А. Администрирование Windows с помощью WMI и WMIC. - М.: БХВ-Петербург, 2004. - 752 с: ил.

11. К.Дж.Джонс, М. Шема, Б. С. Джонсон, Анти-хакер. Средства защиты компьютерных сетей. Справочник профессионала. / Пер. с англ. - М.: СП ЭКОМ, 2003. - 688с.: Ил.

12. Fport - maps open TCP / UDP ports to running processes. [http://www.foundstone.com/resources/intrusion_detection.htm]

13. Windows 2000 Resource Kit. Auditpol - list system's audit policy. [http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp]

14. Windows 2000 Resource Kit. Dumpel - dumps Windows Event Log to human-readable text. [http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp]

15. А. Попов, Windows Script Host для Windows 2000/XP. - М.: БХВ - Петербург, 2003. - 640 с.

16. Unix tools and subsytem on Windows. [http://cygwin.com]

17. Компьютерная контрразведка или кто следит за нами ...

[http://www.zahist.narod.ru/analytic.htm]

18. LADS. [http://www.heysoft.de]

19.Winternals Administrator's Pak. [http://www.sysinternals.com]

20. Microsoft Baseline Security Analyzer.
[http://www.microsoft.com/technet/security/tools/mbsa2/datasheet.mspx]

21. Новые возможности средства PortQry 2.0. [http://support.microsoft.com/kb/310099]

22. Log Parser. [http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx]

23. VirtualBox. [http://www.virtualbox.org]

24. LogParser Studio. [http://blogs.technet.com/b/exchange_ru/archive/2012/04/25/log-parser-studio.aspx]

Как связаться с автором.

Вопросы, комментарии или предложения можно написать автору по следующему адресу электронной почты: mailto:nyukers@gmail.com

Канал **«Nyukers WebTV – только позитивное видео»**
http://youtube.com/nyukers
Блог **«Мультимедиа блог в облаках»**
http://nyukers.blogspot.com
Сайт **«Nyukers Media Age – свобода творчества !»**
http://nyukers.ucoz.net

Автор будет весьма признателен за конструктивные замечания и интересные отзывы.