Секция «Компьютерное право и информационная безопасность»

Автоматизация поиска уязвимостей в информационной системе

Научный руководитель – Фролов Андрей Евгеньевич

Шумилова Антонина Вадимовна

Студент (бакалавр)

Алтайский государственный университет, Физико-технический факультет, Кафедра прикладной физики, электроники и информационной безопасности, Барнаул, Россия

E-mail: shumilova.ant@yandex.ru

Создать безупречную информационную инфраструктуру невозможно. Ни одна система не застрахована от атак злоумышленника, недочетов рабочего персонала, либо иных уязвимостей. Однако, как гласит один из постулатов В. И. Ярочкина - автора учебника по информационной безопасности: «Угрозы легче предупредить, чем устранять результаты их воздействия» [1]. Это утверждение является основополагающим для любой деятельности, охватывающей сферу информационной безопасности. Одним из инструментов, позволяющих предупредить угрозы информационной безопасности является аудит - именно это понятие является центральным в данной курсовой работе.

Аудит — это специальная проверка соответствия информационной системы организации установленным требованиям и/или нормам.

Цели проведения аудита информационной безопасности [3]:

- независимая оценка состояния защищенности информационной системы;
- анализ возможностей осуществления угроз безопасности (рисков, связанных с некомпетентностью персонала, способов использования уязвимостей для проникновения в систему, приведение системы в состояние отказа в обслуживании);
- оценка соответствия информационной системы существующим стандартам в области информационной безопасности;
- поиск «узких» мест в системе защиты информационной системы;
- разработка рекомендаций для повышения защищённости информационной системы

Существует несколько способов классифицировать понятие «аудит». Например, по признаку регулярности:

- Внешний аудит (разовое мероприятие, проводимое по инициативе руководства организации).
- Внутренний аудит (непрерывный процесс контроля уровня защищённости в информационной системе).

По типу организации:

- экспертный аудит безопасности, в процессе которого выявляются недостатки в системе мер защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре обследования;
- инструментальный анализ защищенности информационной системы, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечении системы;

- оценка соответствия рекомендациям Международных стандартов, а также требованиям руководящих документов ФСТЭК;
- комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

В данной работе будет воспроизведена ситуация внешнего инструментального аудита информационной системы, в частности - элемента вычислительной сети, с использованием прикладного программного обеспечения.

Рынок сканеров уязвимостей активно развивается, и мировая IT-индустрия готова предложить множество разнообразных продуктов. Однако учитывая, что для проведения легитимного аудита вычислительной сети необходимо наличие специального сертификата ФСТЭК, мы обратим особенное внимание на отечественные предложения.

Программные продукты, прошедшие сертификацию ФТСЭК, имеют гарант качества в сфере информационной безопасности. Перечислим несколько Российских сканеров уязвимостей от разных производителей, имеющих сертификат ФСТЭК:

- XSpider (Производитель: Positive Technologies, сертификат соответствия ФСТЭК России № 3247 от 24 октября 2014 года, действительный до 24 октября 2024 года).
- Сканер-ВС (Производитель: НПО «Эшелон», сертификат соответствия ФСТЭК России № 2204 от 13 ноября 2010 года, действительный до 13 ноября 2024 года).
- RedCheck (Производитель: АЛТЭКС-СОФТ, сертификат соответствия ФСТЭК России № 3172, действительный от 23 июня 2014 года до 23 июня 2025 года).

Объектом проведения аудита вычислительной сети организации выберем сервер, отвечающий за работу серверной части комплекса «1С:Предприятие». Этот объект сетевой инфраструктуры можно считать наиболее важным по причине того, что именно на нём расположены базы данных, с которыми регулярно работают сотрудники предприятия. Чтобы избежать утечку конфиденциальной информации и персональных данных необходимо в первую очередь провести аудит вышеупомянутого элемента информационной системы.

Исходя из функционала обозреваемых средств анализа защищённости, наиболее подходящими для целей сканирования сервера являются Сканер-ВС и RedCheck. Поскольку оба программных продукта имеют примерно равные характеристики, выбор производился исходя из качества отчётной выдачи об уязвимостях и простоты установки. В этом ключе преимущество имеет RedCheck.

Анализ защищённости будет проводится средствами программного продукта RedCheck.

Для работы с RedCheck необходимо следующее программное обеспечение:

- Microsoft .NET Framework full 4.6.1 или выше (для версий консоли 2.6.5...);
- СУБД SQL Server 2012 и выше (все редакции, включая Express).

В ходе проведения сканирования, ПО RedHeck были составлены отчеты, представленные в виде диаграмм, списков и графиков. Полученные данные представлены на Рисунке 1.

Из отчетов видно, что наибольшую опасность представляют составляющие Windows Server 2019 - это может означать, что ОС давно не проходила процедуру стандартных обновлений.

В ходе анализа уязвимостей были составлены следующие рекомендации:

1. Устранение уязвимостей критического уровня значимости (Рисунок 2):

- Установка обновлений системы.
- Включение брандмауэра (на момент анализа защищенности он был выключен) для устранения уязвимостей связанных с TCP/IP.
- Удаление подозрительного ПО.

2. Устранение уязвимостей высокого уровня возможно только путем установки обновлений системы (Рисунок 3). Уязвимости связанные cMicrosoftedge iie11 были устранены путем запрета запуска данного ПО на сервере, и включены в общий план по установке обновлений.
3. Устранение уязвимостей среднего уровня возможно только путем установки обновлений системы (Рисунок 4).
4. Устранение уязвимостей низкого уровня возможно также только путем установки обновлений системы (Рисунок 5).

В ходе анализа защищенности сервера были обнаружены следующие проблемы:

- Отсутствие какой-либо политики установки обновлений, в следствии чего многие компоненты имеют потенциальные уязвимости.
- Брандмауэр сервера находится в выключенном состоянии.
- Наличие стороннего программного обеспечения, не имеющего реальной необходимости для присутствия на сервере.

Источники и литература

1) Ярочкин, В. И. Информационная безопасность: учебник для вузов / В. И. Ярочкин. — Москва: Гаудеамус, 2004. — 313 с. — (Учебные издания для бакалавров).
2) Методика оценки угроз безопасности информации. – М.: ФСТЭК России, 2021. – 9 с.
3) Ярочкин, В. И. Информационная безопасность: учебник для вузов / В. И. Ярочкин. — Москва: Гаудеамус, 2004. — 18 с. — (Учебные издания для бакалавров).
4) Вопросы Федеральной службы по техническому и экспортному контролю: указ Президента Рос. Федерации от 16 августа 2004 г. №1085 // Собр. законодательства Рос. Федерации. — 2004. — № 34. — Ст. 3541.
5) XSpider. [Электронный ресурс]: сайт содержит информацию данном программном продукте – Режим доступа: https://www.ptsecurity.com/ru-ru/products/xspider/ – Загл. с экрана. Посл. посещение: 9.01.2022.
6) Сканер-ВС. [Электронный ресурс]: сайт содержит информацию данном программном продукте – Режим доступа: https://scaner-vs.ru/ – Загл. с экрана. Посл. посещение: 9.01.2022.
7) RedCheck. [Электронный ресурс]: сайт содержит информацию данном программном продукте – Режим доступа: ttps://www.redcheck.ru/ – Загл. с экрана. Посл. посещение: 9.01.2022.

Иллюстрации

Продукт / Риск	Критический	Высокий	Средний	Низкий	Недоступно	Всего
cpe:/o:microsoft:windows_server_2019	5	77	39	0	9	299
cpe:/a:microsoft:edge	0	6	0	0	0	12
cpe:/a:microsoft:ie:11	0	2	0	0	0	9
cpe:/a:openssl:openssl	0	0	4	0	0	8
cpe:/a:microsoft:.net_framework:4.7.2	0	2	1	0	0	2
cpe:/a:microsoft:sql_server:2019	0	0	0	0	0	0
Всего	**5**	**86**	**44**	**0**	**9**	**330**

Рис. 1. Таблица распределения уязвимостей по программным продуктам

Хост	ALTX ID	Риск	Название
10.101.1.101	338607	Критический	Уязвимость удаленного выполнения кода Windows TCP/IP (10/13/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\drivers\tcpip.sys (10.0.17763.1282)*
10.101.1.101	340813	Критический	Уязвимость удаленного выполнения кода Windows Network File System (11/10/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\drivers\clfs.sys (10.0.17763.1217)*
10.101.1.101	347793	Критический	Уязвимость удаленного выполнения кода Windows TCP/IP (02/09/2021)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\drivers\tcpip.sys (10.0.17763.1282)*
10.101.1.101	347794	Критический	Уязвимость удаленного выполнения кода в Windows Graphics Component (02/09/2021)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\win32kfull.sys (10.0.17763.1339)*
10.101.1.101	347795	Критический	Уязвимость удаленного выполнения кода Windows Camera Codec Pack (02/09/2021)

Рис. 2. Список критических уязвимостей

10.101.1.101	334329	Высокий	Уязвимость несанкционированного получения прав в ядре Windows (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\wiaservc.dll (10.0.17763.973)*
10.101.1.101	334330	Высокий	Уязвимость удаленного выполнения кода Microsoft Graphics (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\win32kfull.sys (10.0.17763.1339)*
10.101.1.101	334335	Высокий	Уязвимость удаленного выполнения кода Windows Font Driver Host (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\win32kfull.sys (10.0.17763.1339)*
10.101.1.101	334337	Высокий	Уязвимость удаленного выполнения кода Windows Media (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\WMADMOD.DLL (10.0.17763.592)*
10.101.1.101	334340	Высокий	Уязвимость удаленного выполнения кода Jet Database Engine (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\SysWOW64\msjet40.dll (4.0.9801.24)*
10.101.1.101	334343	Высокий	Уязвимость несанкционированного получения прав Windows CDP User Components (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\cdpusersvc.dll (10.0.17763.1282)*
10.101.1.101	334346	Высокий	Уязвимость несанкционированного получения прав в Windows GDI (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\win32kfull.sys (10.0.17763.1339)*
10.101.1.101	334358	Высокий	Уязвимость несанкционированного получения прав Windows Registry (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\ntoskrnl.exe (10.0.17763.1339)*
10.101.1.101	334362	Высокий	Уязвимость несанкционированного получения прав Windows Print Spooler (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\localspl.dll (10.0.17763.1282)*
10.101.1.101	334365	Высокий	Уязвимость несанкционированного получения прав Windows Registry (08/11/2020)

Рис. 3. Список уязвимостей высокого уровня значимости

10.101.1.101	334331	Средний	Уязвимость повреждения памяти Media Foundation (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\WMVDECOD.DLL (10.0.17763.1)*
10.101.1.101	334332	Средний	Уязвимость несанкционированного получения прав Windows Radio Manager API (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\RMapi.dll (10.0.17763.348)*
10.101.1.101	334333	Средний	Уязвимость удаленного выполнения кода Jet Database Engine (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\SysWOW64\msjet40.dll (4.0.9801.24)*
10.101.1.101	334334	Средний	Уязвимость удаленного выполнения кода Jet Database Engine (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\SysWOW64\msjet40.dll (4.0.9801.24)*
10.101.1.101	334339	Средний	Уязвимость несанкционированного получения прав Windows CSC Service (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\cscsvc.dll (10.0.17763.1282)*
10.101.1.101	334341	Средний	Уязвимость несанкционированного получения прав Windows UPnP Device Host (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\upnphost.dll (10.0.17763.1339)*
10.101.1.101	334342	Средний	Уязвимость несанкционированного получения прав Windows Speech Runtime (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\Speech_OneCore\common\SpeechRuntime.exe (10.0.17763.1339)*
10.101.1.101	334347	Средний	Уязвимость несанкционированного получения прав Windows Accounts Control (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\Windows.AccountsControl.dll (10.0.17763.1339)*
10.101.1.101	334348	Средний	Уязвимость несанкционированного получения прав Connected User Experiences и Telemetry Service (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\diagtrack.dll (10.0.17763.1339)*
10.101.1.101	334351	Средний	Уязвимость несанкционированного получения прав Windows Custom Protocol Engine (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\rascustom.dll (10.0.17763.1007)*
10.101.1.101	334352	Средний	Уязвимость, приводящая к раскрытию информации DirectWrite (08/11/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\DWrite.dll (10.0.17763.1339)*

Рис. 4. Список уязвимостей среднего уровня значимости

10.101.1.101	334423	Низкий	Уязвимость ядра Windows, приводящая к раскрытию информации (BDU:2020-04064)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\wiaservc.dll (10.0.17763.973)*
10.101.1.101	335938	Низкий	Уязвимость, приводящая к раскрытию информации Microsoft Graphics (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\win32kfull.sys (10.0.17763.1339)*
10.101.1.101	335940	Низкий	Уязвимость ядра Windows, приводящая к раскрытию информации (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\ntoskrnl.exe (10.0.17763.1339)*
10.101.1.101	335941	Низкий	Уязвимость ядра Windows, приводящая к раскрытию информации (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\ntoskrnl.exe (10.0.17763.1339)*
10.101.1.101	335946	Низкий	Уязвимость, приводящая к раскрытию информации Microsoft Graphics (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\win32kfull.sys (10.0.17763.1339)*
10.101.1.101	335951	Низкий	Уязвимость Win32k, приводящая к раскрытию информации (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\win32kfull.sys (10.0.17763.1339)*
10.101.1.101	335955	Низкий	Уязвимость ядра Windows, приводящая к раскрытию информации (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\ntoskrnl.exe (10.0.17763.1339)*
10.101.1.101	335962	Низкий	Уязвимость Win32k, приводящая к раскрытию информации (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\win32kfull.sys (10.0.17763.1339)*
10.101.1.101	335963	Низкий	Уязвимость, приводящая к раскрытию информации Projected Filesystem (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\ntoskrnl.exe (10.0.17763.1339)*
10.101.1.101	335966	Низкий	Уязвимость, приводящая к отказу в обслуживании Windows в Hyper-V (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\hvax64.exe (10.0.17763.1339)*
10.101.1.101	335988	Низкий	Уязвимость ядра Windows, приводящая к раскрытию информации (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\ntoskrnl.exe (10.0.17763.1339)*
10.101.1.101	336011	Низкий	Уязвимость ядра Windows, приводящая к раскрытию информации (09/08/2020)
cpe:/o:microsoft:windows_server_2019			*C:\Windows\System32\ntoskrnl.exe (10.0.17763.1339)*

Рис. 5. Список уязвимостей низкого уровня значимости