

Лабораторная работа 1-В (20_09)

Кибербезопасность предприятия

Ищенко Ирина Мишина Анастасия Дикач Анна
Галацан Николай Амуничников Антон
Барсегян Вардан Дудырев Глеб
Дымченко Дмитрий

Содержание

1 Цель тренировки	5
2 Выявленные уязвимости и последствия	6
2.1 Уязвимая версия axis2	7
2.1.1 Описание инцидента	7
2.1.2 Решение	8
2.1.3 Последствия App Backdoor	11
2.2 Уязвимая версия программы CoolReaderPDF	12
2.2.1 Описание инцидента	13
2.2.2 Решение	14
2.2.3 Последствия Manager meterpreter	16
2.3 Уязвимая версия IGSS	17
2.3.1 Описание инцидента	17
2.3.2 Решение	18
2.3.3 Последствия IGSS meterpreter	21
3 Вывод	23
Список литературы	24

Список иллюстраций

2.1 Уязвимости и последствия	6
2.2 Событие на VipNet IDS NS	7
2.3 Добавление инцидента axis2	8
2.4 Подключение по ssh	9
2.5 Добавление правила в утилите	9
2.6 Стартовая страница сервера Apache Tomcat	10
2.7 Добавление axis2.war	10
2.8 Нажатие на кнопку	10
2.9 Установленная сессия с нарушителем	11
2.10 Автозапуск backdoor	11
2.11 Отключение автозапуска	12
2.12 Удаление исполняемого файла и заверение сессий с машиной нарушителя	12
2.13 Событие на VipNet IDS NS	13
2.14 Добавление инцидента CoolReaderPDF	14
2.15 Подключение к Manager Workstation 1	15
2.16 Ошибка	15
2.17 Добавленное правило	16
2.18 Добавленное правило	16
2.19 Список установленных соединений	17
2.20 Остановка процесса	17
2.21 Событие на VipNet IDS NS	18
2.22 Добавление инцидента IGSS	18
2.23 Подключение	19
2.24 Брандмауэр включён	20
2.25 Исключения	21
2.26 Соединение с машиной нарушителя	22
2.27 Остановка процесса	22
3.1 Уязвимости и последствия	23

Список таблиц

1 Цель тренировки

Разобраться с сценарием действий нарушителя “Защита данных сегмента АСУ ТП”. Выявить и устраниить уязвимости и их последствия.

2 Выявленные уязвимости и последствия

По ходу выполнения тренировки были выявлены следующие уязвимости (рис. 2.1):

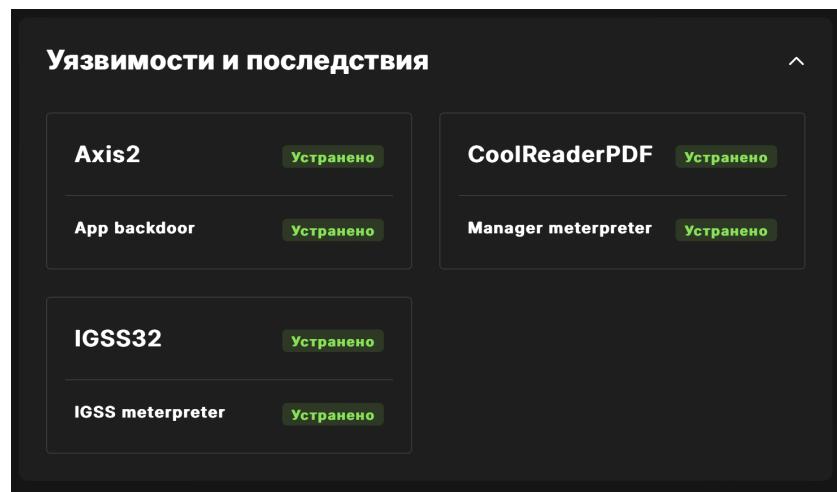


Рис. 2.1: Уязвимости и последствия

Уязвимость 1. Уязвимая версия axis2 (CVE-2010-0219)

Последствие. App Backdoor

Уязвимость 2. Уязвимая версия программы CoolReaderPDF (CVE-2012-4914)

Последствие. Manager meterpreter-сессия

Уязвимость 2. Уязвимая версия IGSS (CVE-2011-1567)

Последствие. IGSS meterpreter-сессия

2.1 Уязвимая версия axis2

Уязвимая версия axis2 установлена на AppServer под управлением Apache Tomcat. В типовом шаблоне информационной системы используется для развертывания веб-сервисов, работает через порт 8080.

Эксплуатируемая уязвимость – CVE-2010-0219. Компонент Axis2 SAP BusinessObjects содержит учетную запись и пароль администратора по умолчанию.

Из конфигурационного файла axis2.xml можно получить данные учетной записи администратора, авторизоваться и загрузить вредоносный сервис для исполнения команды

2.1.1 Описание инцидента

С помощью АМТИР нашли правило обнаружения вторжений. Для (CVE-2010-0219) нашли необходимое правило (рис. 2.2).

The screenshot shows two windows side-by-side. The left window is titled 'События' (Events) and displays a list of events. A single event is selected, showing details: Date and time: 08.03.01 827 20.09.2025; Source: eth2; Priority: Высокий (High); Type: Сигнатурное событие (Signature event); Protocol: TCP; Event ID: 3006394; Client application: Mozilla/5.0 (Macintosh; Intel Mac OS X 13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36; Resource domain name: 192.168.1.100. The right window is titled 'Событие 08:03:01.827 20.09.2025' and provides detailed information about the event, including its general information and analysis rule.

Рис. 2.2: Событие на VipNet IDS NS

Далее перешли к заполнению инцидента (рис. 2.3).

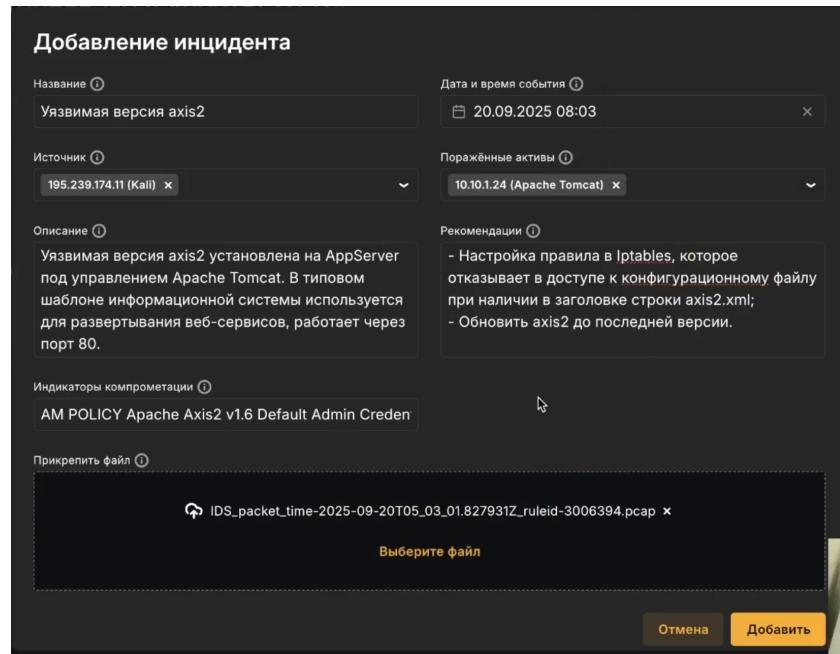


Рис. 2.3: Добавление инцидента axis2

2.1.2 Решение

Открываем KeePass. Находим Apache Tomcat и подключаемся к нему по ssh via Putty (рис. 2.4).

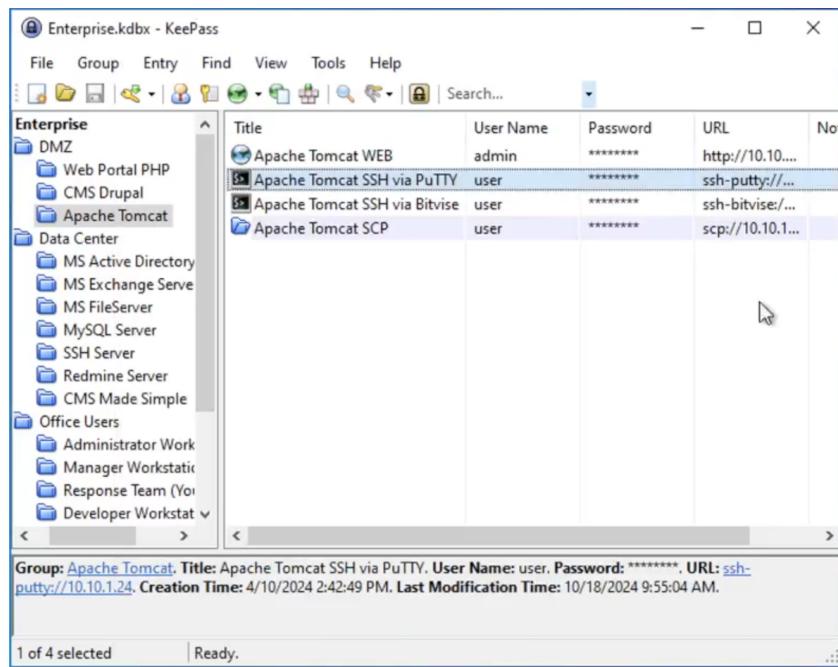


Рис. 2.4: Подключение по ssh

- Настройка правил в Iptables. В утилите iptables добавить правило (iptables -I INPUT 1 -j REJECT -p tcp --dport 8080 -m string --string "axis2.xml" --algo kmp), которое отказывает в доступе к конфигурационному файлу при наличии в заголовке строки axis2.xml (рис. 2.5).

```
user@app-server: ~
# Using username "user".
Last login: Wed May 14 10:07:59 2025
user@app-server:~$ su -
Password:
root@app-server:~# iptables -I INPUT 1 -j REJECT -p tcp --dport 8080 -m string --string "axis2.xml" --algo kmp
root@app-server:~# iptables -L INPUT -n --line-numbers
Chain INPUT (policy DROP)
num  target     prot opt    source          destination
1    REJECT    tcp   --  0.0.0.0/0      0.0.0.0/0          tcp  dpt:8080
STRING match "axis2.xml" ALGO name kmp TO 65535 reject-with icmp-port-unreachable
2    ufw-before-logging-input  all   --  0.0.0.0/0      0.0.0.0/0
3    ufw-before-input  all   --  0.0.0.0/0      0.0.0.0/0
4    ufw-after-input  all   --  0.0.0.0/0      0.0.0.0/0
5    ufw-after-logging-input  all   --  0.0.0.0/0      0.0.0.0/0
6    ufw-reject-input  all   --  0.0.0.0/0      0.0.0.0/0
7    ufw-track-input  all   --  0.0.0.0/0      0.0.0.0/0
root@app-server:~#
```

Рис. 2.5: Добавление правила в утилите

2. Обновить axis2 до последней версии. Войти на Tomcat сервер (в адресной строке браузера набрать <http://10.10.1.24:8080>). Нажать на кнопку Manager App (рис. 2.6).

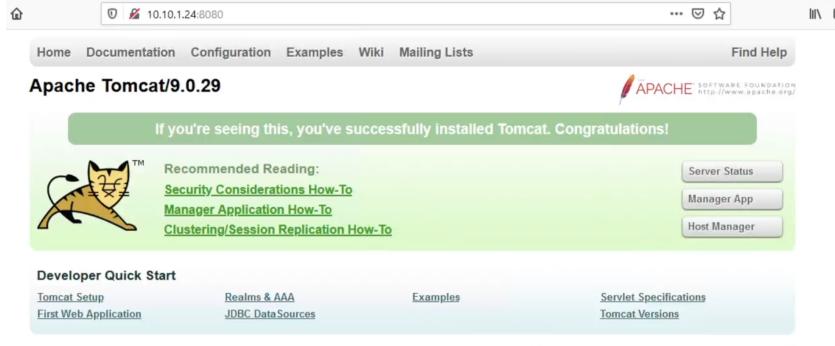


Рис. 2.6: Стартовая страница сервера Apache Tomcat

Войти под учетной записью администратора (admin / qwe1231@#). В таблице Applications найти строку с записью axis2 и нажать на кнопку Undeploy. Загрузить WAR файл axis2 актуальной версии. В поле WAR file to deploy нажать на Choose file, далее выбрать загруженный файл и нажать на кнопку Deploy (рис. 2.7)(рис. 2.8).

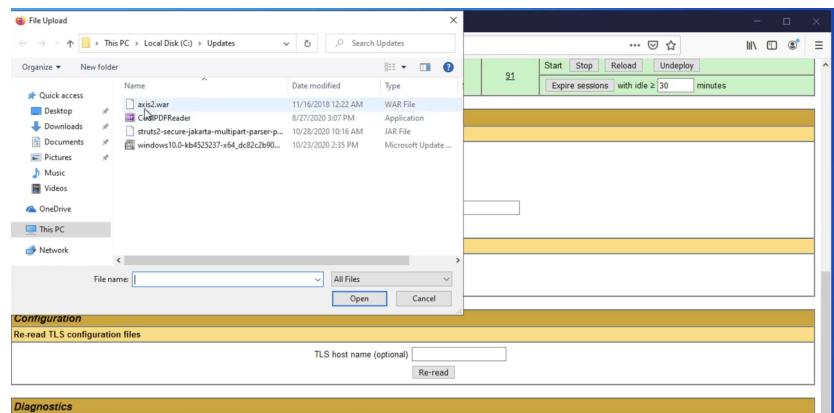


Рис. 2.7: Добавление axis2.war



Рис. 2.8: Нажатие на кнопку

Деактивировать уязвимую версию axis2. В таблице Applications найти строку с записью axis2 и нажать на кнопку Stop. После остановки приложения axis2 остается в таблице, уязвимость будет успешно устранена.

2.1.3 Последствия App Backdoor

Нарушитель для закрепления на уязвимой машине загружает файл, исполнение которого устанавливает Reverse Shell соединение с машиной нарушителя. Установленную сессию веб-сервера с IP-адресом нарушителя (195.239.174.11) и имя запущенного процесса можно обнаружить при помощи команды «sudo ss -tp» (рис. 2.9).

```

user@app-server:~$ sudo ss -tp
State      Recv-Q   Send-Q Local Address:Port          Peer Address:Port
CLOSING     1       190    127.0.0.1:8080           127.0.0.1:49356
ESTAB      0       0      195.239.174.11:80        127.0.0.1:17295
CLOSING     1       190    127.0.0.1:54914          127.0.0.1:8080
CLOSING     1       190    127.0.0.1:54908          127.0.0.1:8080
ESTAB      64      0      195.239.174.11:80        10.10.1.241:443
FIN-WAIT-1  0       190    127.0.0.1:54940          10.10.1.241:443
ESTAB      0       0      127.0.0.1:244648         195.239.174.11:7777
CLOSING     1       190    127.0.0.1:54915          127.0.0.1:8080
CLOSING     1       190    127.0.0.1:54926          127.0.0.1:8080
CLOSING     1       190    127.0.0.1:54979          127.0.0.1:8080
ESTAB      0       0      127.0.0.1:54920          10.10.1.250:5044
CLOSING     1       190    127.0.0.1:54976          127.0.0.1:8080
CLOSING     1       190    127.0.0.1:54970          127.0.0.1:8080
CLOSING     1       190    127.0.0.1:54998          127.0.0.1:8080
CLOSING     1       190    127.0.0.1:54976          127.0.0.1:8080
ESTAB      0       0      195.239.174.11:80        10.10.1.241:443
CLOSING     1       190    127.0.0.1:54914          127.0.0.1:8080
ESTAB      0       189    127.0.0.1:54958          127.0.0.1:8080
CLOSING     1       0      [:ffff:127.0.0.1]:8080  [:ffff:127.0.0.1]:54956
FIN-WAIT-3  0       0      [:ffff:127.0.0.1]:8080  [:ffff:127.0.0.1]:54956
FIN-WAIT-1  0       20376   [:ffff:10.10.1.241]:8080 [:ffff:10.10.1.241]:54947
ESTAB      0       0      [:ffff:127.0.0.1]:8080  [:ffff:127.0.0.1]:54988
FIN-WAIT-2  0       0      [:ffff:127.0.0.1]:8080  [:ffff:127.0.0.1]:54988
ESTAB      0       0      [:ffff:127.0.0.1]:8080  [:ffff:127.0.0.1]:54924

```

Рис. 2.9: Установленная сессия с нарушителем

Событие автозапуска backdoor файла наблюдается в журнале /var/log/syslog (рис. 2.10).

```

y.
Sep 20 12:17:33 localhost systemd[1]: vipnet_epp_bash_monitor.service: Succeeded.
Sep 20 12:17:33 localhost systemd[1]: Started ViPNet Endpoint Protection Bash Monitor.
Sep 20 12:17:46 localhost systemd[1]: Starting ViPNet Endpoint Protection Bash Monitor...
Sep 20 12:17:46 localhost systemd[1]: Configuration file /etc/systemd/system/sc6_struts2.service is m
y.
Sep 20 12:17:47 localhost systemd[1]: vipnet_epp_bash_monitor.service: Succeeded.
Sep 20 12:17:47 localhost systemd[1]: Started ViPNet Endpoint Protection Bash Monitor.
Sep 20 12:17:52 localhost systemd[1]: Starting ViPNet Endpoint Protection Bash Monitor...
Sep 20 12:17:52 localhost systemd[1]: Configuration file /etc/systemd/system/sc6_struts2.service is m
y.
Sep 20 12:17:53 localhost systemd[1]: vipnet_epp_bash_monitor.service: Succeeded.
Sep 20 12:17:53 localhost systemd[1]: Started ViPNet Endpoint Protection Bash Monitor.
Sep 20 12:18:01 localhost systemd[1]: Starting ViPNet Endpoint Protection Bash Monitor...
Sep 20 12:18:01 localhost CRON[9725]: (tomcat) CMD (/opt/tomcat/webapps/evil.conf)
Sep 20 12:18:01 localhost systemd[1]: Configuration file /etc/systemd/system/sc6_struts2.service is m
y.
user@app-server:~$ 

```

Рис. 2.10: Автозапуск backdoor

Последовательность действий для закрытия данной полезной нагрузки:

- убрать автозапуск исполняемого файла из стоптаб пользователя tomcat по пути /var/spool/cron/стоптабс/tomcat (рис. 2.11);

- удалить исполняемый файл evil.conf по пути /opt/tomcat/webapps/ с помощью команды rm evil.conf;
 - завершить все активные сессии с машиной нарушителя с помощью команды kill (рис. 2.12).

```
[user@app-server: ~]
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab installed on Sat Sep 20 08:03:50 2025)
# (Cron version --- $Id: crontab.c,v 2.13 1996/01/17 03:20:37 vixie Exp $)

~
```

Рис. 2.11: Отключение автозапуска

```

root@app-server:~# cd /opt/tomcat/webapps/
root@app-server:~/opt/tomcat/webapps# rm evil.conf
root@app-server:/opt/tomcat/webapps#
root@app-server:/opt/tomcat/webapps# ss -tpe
State      Recv-Q   Send-Q Local Address:Port          Peer Address:Port
LISTEN     0        0      10.10.1.24:8080           10.10.2.17:25004
LISTEN     0        0      10.10.1.24:57630          10.10.2.17:25004
CLOSING    1        190     127.0.0.1:155128          127.0.0.1:https-alt
FIN-WAIT-1  0        190     127.0.0.1:55248          127.0.0.1:https-alt
CLOSING    1        190     127.0.0.1:155214          127.0.0.1:https-alt
ESTABLISHED 0        64      10.10.1.24:44330         10.10.2.17:17777
ESTABLISHED 0        0      10.10.1.24:440408         195.239.174.11:7777
CLOSING    1        190     127.0.0.1:155142          127.0.0.1:https-alt
CLOSING    1        190     127.0.0.1:155172          127.0.0.1:https-alt
CLOSING    1        190     127.0.0.1:155173          127.0.0.1:https-alt
FIN-WAIT-1  0        190     127.0.0.1:155238          127.0.0.1:https-alt
ESTABLISHED 0        0      10.10.1.24:39320          10.10.1.25:5044
CLOSING    1        190     127.0.0.1:155186          127.0.0.1:https-alt
CLOSING    1        190     127.0.0.1:155203          127.0.0.1:https-alt
ESTABLISHED 0        0      10.10.1.24:44330         10.10.2.17:17777
CLOSING    1        190     127.0.0.1:155102          127.0.0.1:https-alt
CLOSING    1        190     127.0.0.1:155112          127.0.0.1:https-alt
ESTABLISHED 0        0      10.10.1.24:44106         195.239.174.11:4433
FIN-WAIT-2  0        0      [{ffff:f127.0.0.1}:http-alt  [{ffff:f127.0.0.1}:http-alt
FIN-WAIT-2  0        0      [{ffff:f127.0.0.1}:http-alt  [{ffff:f127.0.0.1}:http-alt
FIN-WAIT-2  0        0      [{ffff:f127.0.0.1}:http-alt  [{ffff:f127.0.0.1}:http-alt
ESTABLISHED 0        0      [{ffff:f127.0.0.1}:http-alt  [{ffff:f127.0.0.1}:http-alt
CLOSE_WAIT  1        0      [{ffff:f127.0.0.1}:http-alt  [{ffff:f129.239.174.11}:17793
ESTABLISHED 0        0      [{ffff:10.10.1.24}:40024  [{ffff:10.10.1.24}:40024
FIN-WAIT-2  0        0      [{ffff:f127.0.0.1}:http-alt  [{ffff:f127.0.0.1}:http-alt
FIN-WAIT-2  0        0      [{ffff:f127.0.0.1}:http-alt  [{ffff:f127.0.0.1}:http-alt
FIN-WAIT-2  0        0      [{ffff:f127.0.0.1}:http-alt  [{ffff:f127.0.0.1}:http-alt

root@app-server:/opt/tomcat/webapps# kill 5994
root@app-server:/opt/tomcat/webapps#

```

Рис. 2.12: Удаление исполняемого файла и заверение сессий с машиной нарушителя

В результате проведенных действий нейтрализовано последствие, которое обусловлено атакой нарушителя.

2.2 Уязвимая версия программы CoolReaderPDF

На хосте Manager Workstation 1 установлена уязвимая версия программы CoolReaderPDF. Хост используется для приема писем по публичной и корпоративной электронной почте. Эксплуатируемая уязвимость – CVE-2012-4914.

Переполнение стека в программе CoolPDFReader позволяет удаленно выполнять код при чтении специально сгенерированного документа. В данном случае сгенерированный документ соединен с некоторым стандартным отчетом. При просмотре последней страницы происходит эксплуатация уязвимости. Уязвимости подвержена программа чтения CoolReaderPDF версии 3.0.2.256, которая позволяет удаленным нарушителям выполнять произвольный код через документ PDF с созданным потоком. При просмотре начальной части документа программа работает стандартно. При попытке просмотра седьмой страницы программа не реагирует на команды пользователя («зависает»), нарушитель получает сессию.

2.2.1 Описание инцидента

С помощью AMTIP нашли правило обнаружения вторжений. Для (CVE-2012-4914) не нашли необходимое правило, но для определения времени инцидента было выбрано правило ET TROJAN (рис. 2.13).

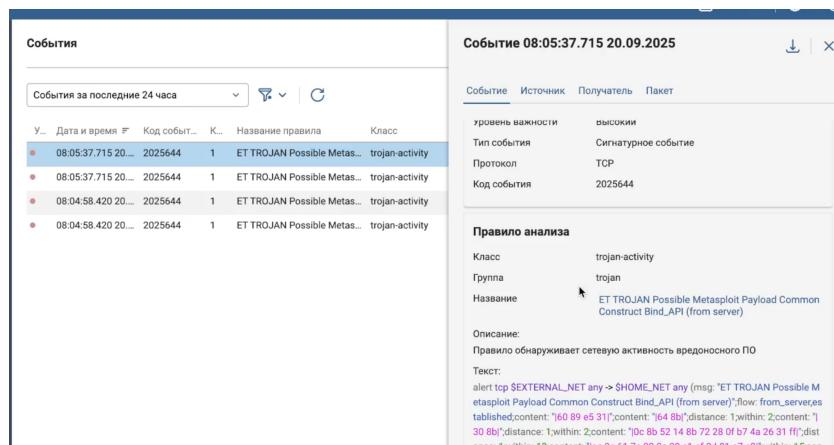


Рис. 2.13: Событие на VipNet IDS NS

Далее перешли к заполнению инцидента (рис. 2.14).

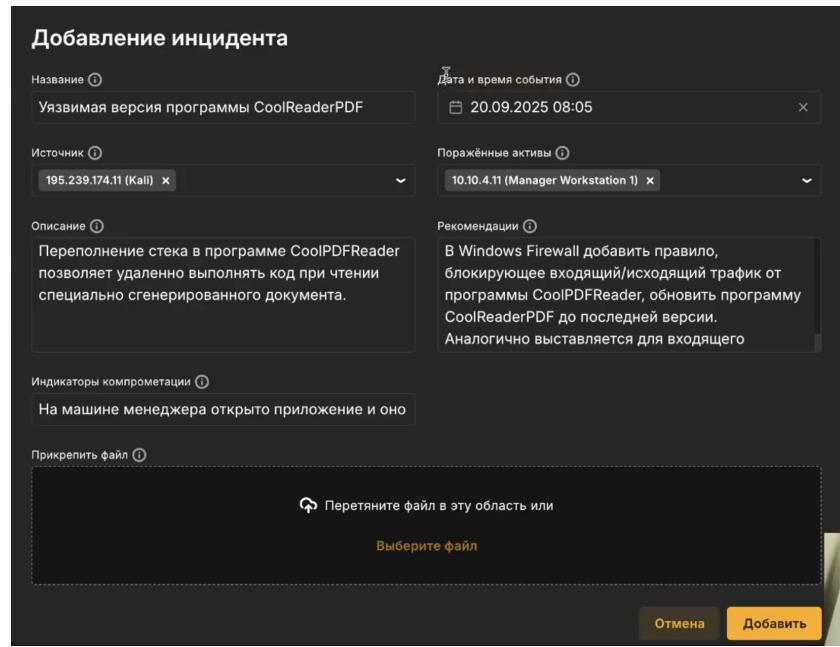


Рис. 2.14: Добавление инцидента CoolReaderPDF

2.2.2 Решение

Открываем KeePass. Находим Manager Workstation 1 и подключаемся по rdp от админа (рис. 2.15).

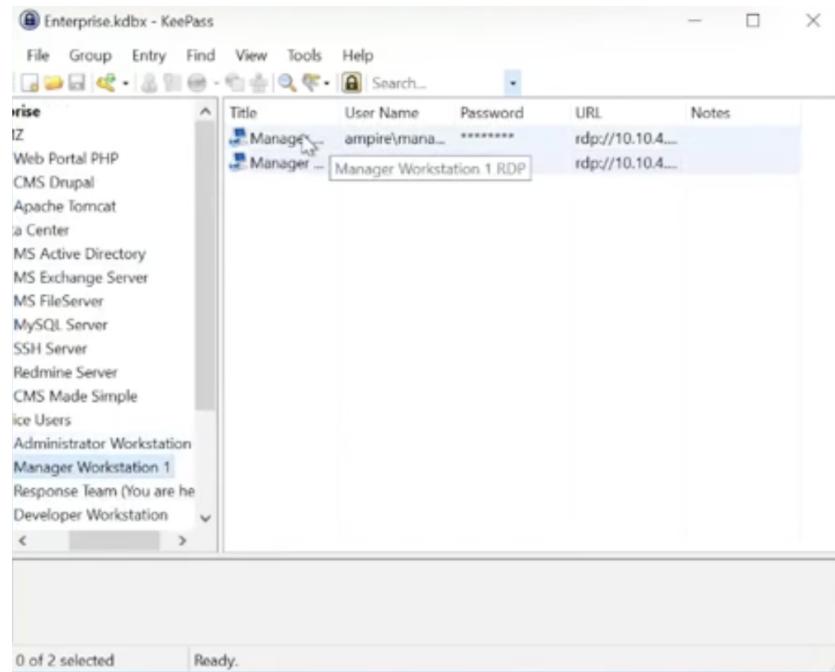


Рис. 2.15: Подключение к Manager Workstation 1

Встретили ошибку (рис. 2.16).

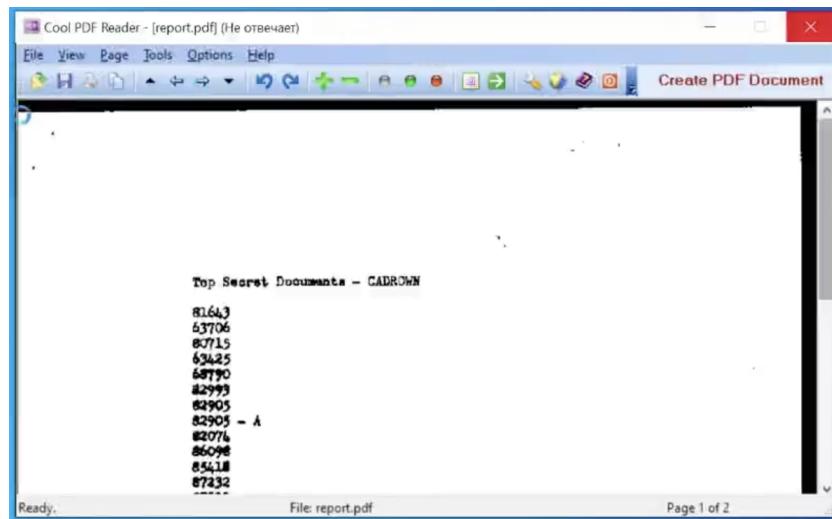


Рис. 2.16: Ошибка

Открываем Windows Firewall with Advanced Security и добавляем правило для входящих подключений и исходящих подключений (рис. 2.17)(рис. 2.18).

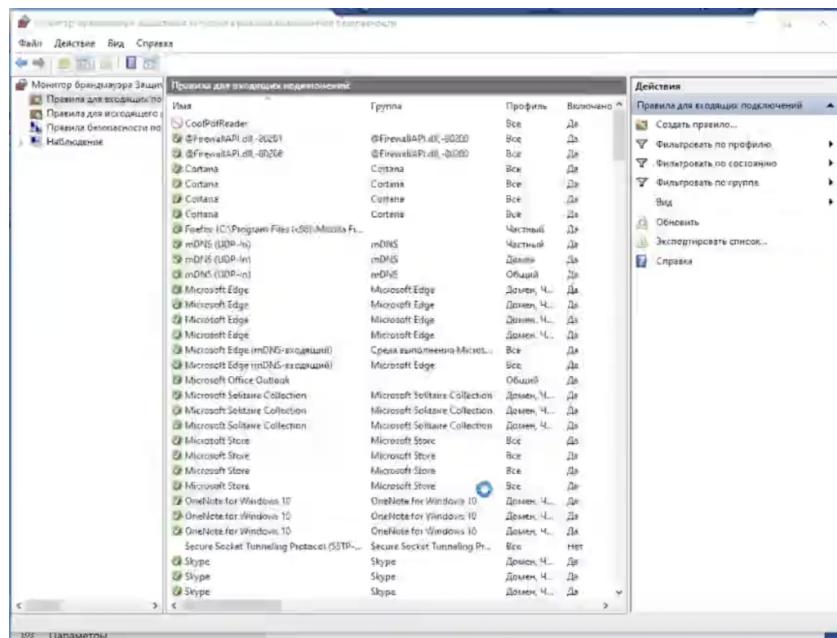


Рис. 2.17: Добавленное правило

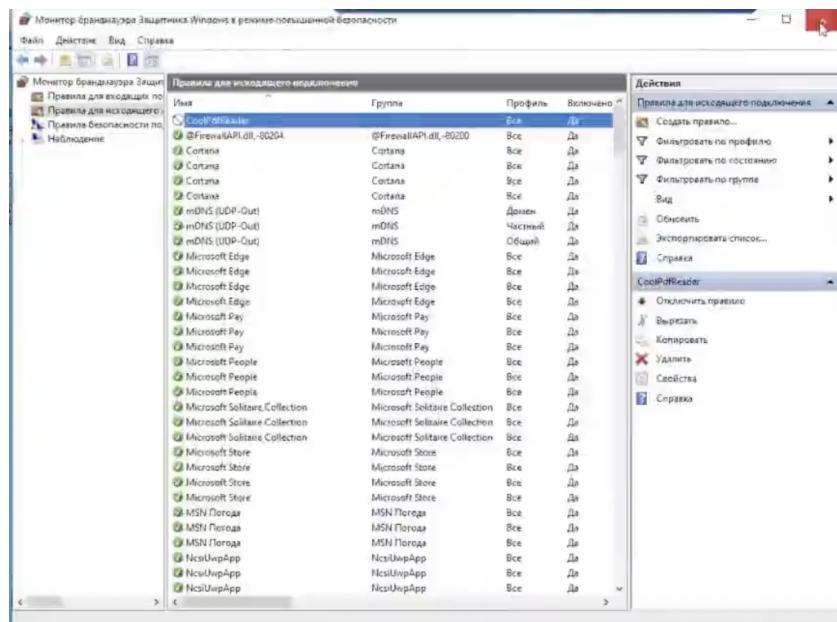


Рис. 2.18: Добавленное правило

2.2.3 Последствия Manager meterpreter

Вследствие переполнения стека нарушитель устанавливает reverse_shell

соединение с хостом Manager 1. Установленную сессию узла Manager Workstation 1 с IP-адресом нарушителя (195.239.174.11) и имя запущенного процесса можно обнаружить при помощи утилиты netstat с ключами –bno (рис. 2.19).

Активные подключения					
Имя	Локальный адрес	Внешний адрес	Состояние	PID	
TCP [TermService [svchost.exe]]	10.10.4.11:3389	10.10.4.12:51946	ESTABLISHED	528	
TCP [OUTLOOK.EXE]	10.10.4.11:52635	10.10.2.11:443	ESTABLISHED	5292	
TCP [CoolPDFReader.exe]	10.10.4.11:52701	195.239.174.11:4445	ESTABLISHED	4776	
TCP	10.10.4.11:52738	10.10.2.11:443	TIME_WAIT	0	
TCP	10.10.4.11:53759	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:53760	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:53761	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:53762	195.239.174.12:443	TIME_WAIT	0	

Рис. 2.19: Список установленных соединений

Для устранения полезной нагрузки необходимо завершить соединение с машиной нарушителя с помощью команды taskkill /f /pid (рис. 2.20).

```
C:\Users\administrator>taskkill /f /pid 4776
Успешно: Процесс, с идентификатором 4776, успешно завершен.

C:\Users\administrator>
```

Рис. 2.20: Остановка процесса

2.3 Уязвимая версия IGSS

Эксплуатируемая уязвимость – CVE-2011-1567.

Переполнение стека в программе с графическим интерфейсом IGSSdataServer.exe при использовании операции ListAll ведет к удаленному выполнению кода и прямому подключению нарушителя к серверу.

2.3.1 Описание инцидента

С помощью АМТИР нашли правило обнаружения вторжений. Для Эксплуатируемая уязвимость – (CVE-2011-1567) нашли необходимое правило (рис. 2.21).

События

Событие 08:05:27.368 20.09.2025

Событие	Источник	Получатель	Пакет
08:05:27.368 20.09.2025	eth2	Высокий	Сигнатурное событие
08:05:27.368 20.09.2025	TCP	3006078	AM Exploit 7T Interactive Graphical SCADA Buffer Overflow 0d

Общая информация

Дата и время: 08:05:27.368 20.09.2025
 Интерфейс захвата: eth2
 Уровень важности: Высокий
 Тип события: Сигнатурное событие
 Протокол: TCP
 Код события: 3006078

Правило анализа

Класс: web-application-attack
 Группа: exploit
 Название: AM Exploit 7T Interactive Graphical SCADA Buffer Overflow 0d
 Описание: Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости.

Рис. 2.21: Событие на VipNet IDS NS

Далее перешли к заполнению инцидента (рис. 2.22).

Добавление инцидента

Название: Уязвимая версия IGSS

Дата и время события: 20.09.2025 08:05

Источник: 10.10.4.11 (Manager Workstation 1)

Поражённые активы: 10.10.3.10 (ASU Server)

Описание: Переполнение стека в программе с графическим интерфейсом IGSSDataServer.exe при использовании операции ListAll ведет к удаленному выполнению кода и прямому подключению нарушителя к серверу

Рекомендации: Ограничить внешний доступ к уязвимому приложению, используя встроенный межсетевой экран

Индикаторы компрометации: AM Exploit 7T Interactive Graphical SCADA Buffer Ov

Прикрепить файл: IDS_packet_time-2025-09-20T05_05_27.368336Z_ruleid-3006078.pcap

Выберите файл

Отмена Добавить

Рис. 2.22: Добавление инцидента IGSS

2.3.2 Решение

Открываем KeePass. Находим SCADA IGSS и подключаемся по rdp (рис. 2.23).

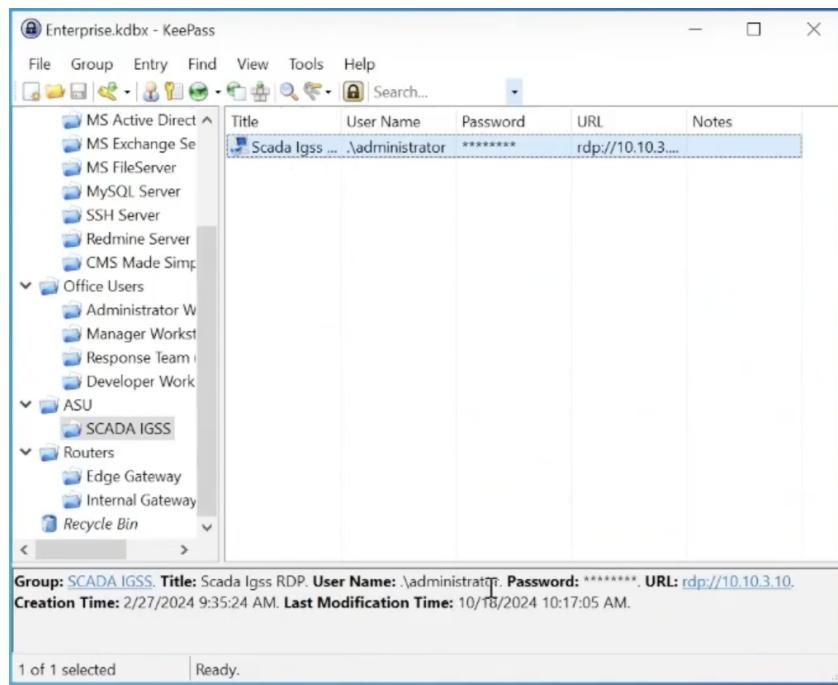


Рис. 2.23: Подключение

Включить брандмауэр Windows, выделить пункт «Не разрешать исключения» или убрать из исключений IGSS DataServer (рис. 2.24) (рис. 2.25).



Рис. 2.24: Брандмауэр включён

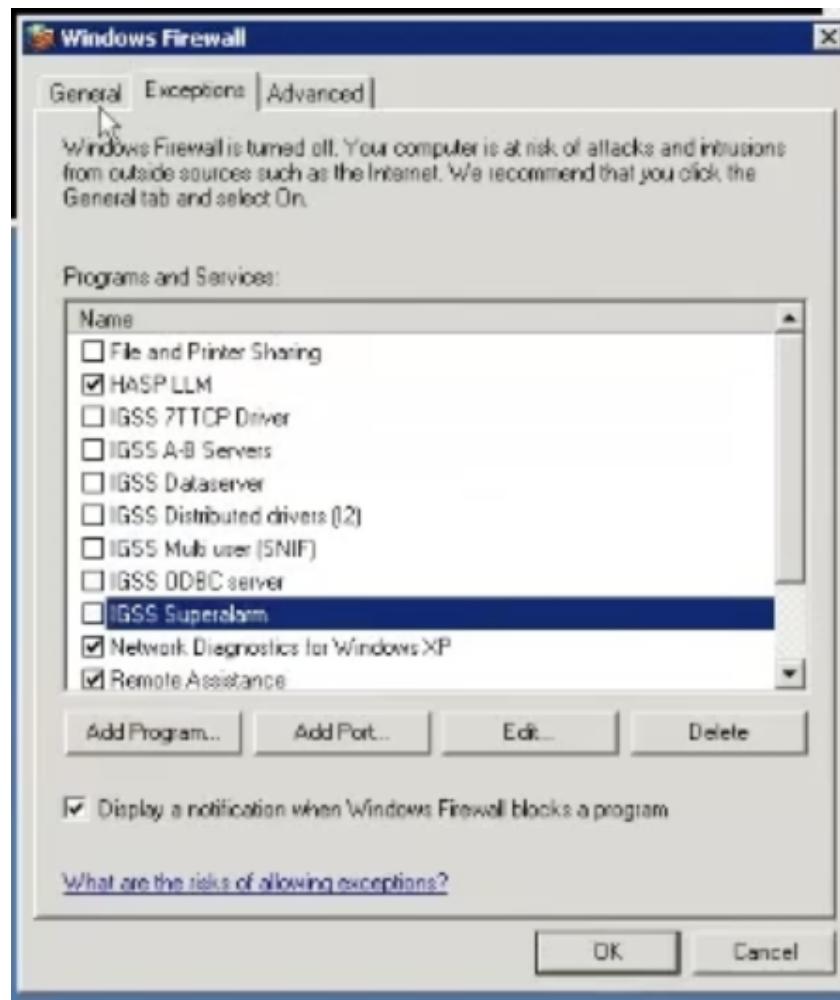


Рис. 2.25: Исключения

2.3.3 Последствия IGSS meterpreter

Вследствие переполнения стека нарушитель устанавливает reverse_shell соединение с узлом SCADA Server. Установленную сессию с IP-адресом нарушителя (195.239.174.11) и запущенный процесс можно обнаружить при помощи утилиты netstat с ключами –bno (рис. 2.26).

```
Windows Command Prompt  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
C:\Documents and Settings\Administrator>netstat -ano  
Active Connections  
Proto Local Address          Foreign Address        State      PID  
TCP   10.10.3.10:41411       195.239.174.11:20002 ESTABLISHED 1212  
[IGSSdataServer.exe]  
TCP   10.10.3.10:3389       -- unknown component(s) -- ESTABLISHED 868  
[svchost.exe]  
TCP   127.0.0.1:2745         127.0.0.1:12401    TIME_WAIT   0  
TCP   127.0.0.1:2746         127.0.0.1:12401    TIME_WAIT   0  
TCP   127.0.0.1:2754         127.0.0.1:12401    TIME_WAIT   0  
TCP   127.0.0.1:2755         127.0.0.1:12401    TIME_WAIT   0  
C:\Documents and Settings\Administrator>
```

Рис. 2.26: Соединение с машиной нарушителя

Для устранения полезной нагрузки необходимо завершить соединение с машиной нарушителя с помощью команды taskkill /f /pid (рис. 2.27).

```
C:\Documents and Settings\Administrator>taskkill /f /pid 1212  
SUCCESS: The process with PID 1212 has been terminated.  
C:\Documents and Settings\Administrator>
```

Рис. 2.27: Остановка процесса

В результате выполнения команды запущенный процесс завершен, последствие IGSS meterpreter успешно устранено.

3 Вывод

Разобрались с сценарием действий нарушителя “Защита данных сегмента АСУ ТП”. Выявили и устранили уязвимости и их последствия (рис. 3.1)

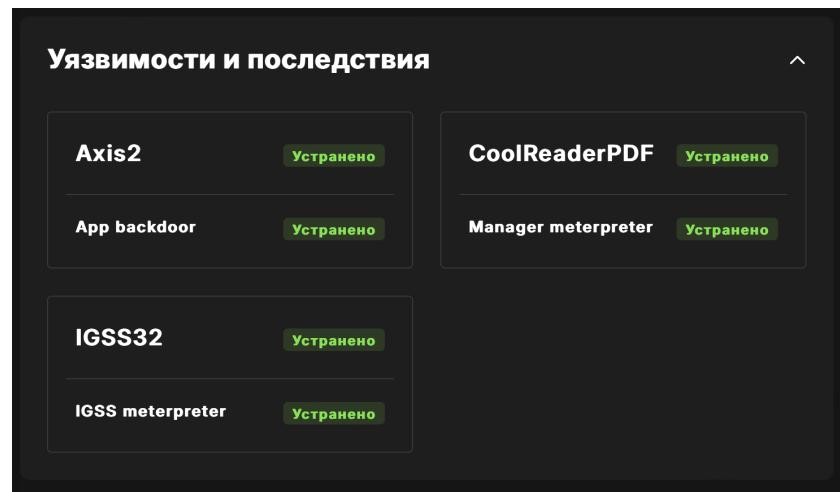


Рис. 3.1: Уязвимости и последствия

Список литературы