

Отчёт по лабораторной работе №1

Дисциплина: Кибербезопасность предприятия

Астраханцева Анастасия
Ибатулина Дарья
Ганина Таисия
Шошина Евгения
Кадирова Мехрубон
Хассан Факи Абакар
(группа НФИбд-01-22)

Содержание

1 Цель работы	4
2 Задание	5
3 Теоретическое введение	6
4 Выполнение лабораторной работы	8
5 Выводы	28
6 Список литературы	29

Список иллюстраций

4.1	Получение доступа через уязвимый Apache Axis 2	8
4.2	AM EXPLOIT Generic Command Injection in HTTP URI	9
4.3	AM POLICY Apache Axis2 v1.6 Default Admin Credential	9
4.4	ET TROJAN Possible Metasploit Payload Common Construct Bind_API	10
4.5	Уязвимая версия IGSS AM Exploit 7T Interactive Graphical SCADA Buffer Overflow	10
4.6	Процесс аутентификации	11
4.7	Добавление правила в iptables для блокировки доступа к axis2.xml	12
4.8	Проверка правил	12
4.9	Устранена уязвимость Axis2	13
4.10	Процесс evil.conf	13
4.11	Переход к редактированию файла	14
4.12	Редактирование файла /var/spool/cron/crontabs/tomcat	14
4.13	Удалили строку	15
4.14	Удаление вредоносного файла и завершение процесса	16
4.15	Устранена первая уязвимость и её последствие	16
4.16	Доступ к Manager Workstation	17
4.17	Windows defender firewall	17
4.18	Этап создания нового правила брандмауэра	18
4.19	Окно настройки создаваемого правила	19
4.20	Проверка в «Мониторе брандмауэра Защитника Windows»	20
4.21	Устранена уязвимость 2 (CoolReaderPDF)	20
4.22	Список всех TCP-соединений	21
4.23	taskkill /f /pid 5348	22
4.24	Полностью устранена вторая уязвимость и её последствия	23
4.25	Удаленный доступ к SCADA-сервер	23
4.26	“Пуск” - “Accessories” - “System Tools” - “Security center”	24
4.27	Брандмауэр	24
4.28	Убрали из исключений IGSS Dataserver	25
4.29	Уязвимость IGSS32 была устранена	26
4.30	TCP-соединение	26
4.31	Полностью устранена третья уязвимость и её последствия	27

1 Цель работы

Целью лабораторной работы является изучение методов обнаружения, анализа и устранения последствий компьютерных атак в сегменте автоматизированных систем управления технологическим процессом (АСУ ТП) на базе программного комплекса “Ampire”. Работа направлена на формирование навыков защиты данных от внешних нарушителей, использующих уязвимости в программном обеспечении, и освоение инструментов мониторинга сетевой безопасности, таких как ViPNet IDS NS, ViPNet TIAS и Security Onion.

2 Задание

1. Изучить типовые уязвимости, используемые при атаке на сегмент АСУ ТП.
2. Проанализировать последовательность действий нарушителя на каждом этапе атаки.
3. Освоить методы детектирования атак с использованием средств мониторинга и анализа безопасности.
4. Выполнить мероприятия по устраниению последствий атаки.
5. Отработать навыки анализа сетевых соединений и процессов с помощью стандартных утилит.

3 Теоретическое введение

Автоматизированные системы управления технологическим процессом (АСУ ТП) представляют собой комплекс программно-аппаратных средств, предназначенных для автоматизации управления производственными процессами в промышленности. В условиях растущей цифровизации такие системы становятся уязвимыми для компьютерных атак, которые могут привести к нарушению производственных процессов, утечке данных или физическому ущербу. Программный комплекс “Ampire” (Киберполигон Ampire) предназначен для обучения методам обнаружения, анализа и устранения последствий таких атак в симулированной среде.

Сценарий №4 “Защита данных сегмента АСУ ТП” моделирует действия внешнего нарушителя, обладающего знаниями в области инструментов для проведения компьютерных атак и техник постэксплуатации. Уровень сложности сценария оценивается как 7 из 10, что учитывает количество уязвимостей, типы узлов в шаблоне информационной системы и сложность детектирования. Нарушитель начинает с сканирования сети (195.239.174.0/24), выявления уязвимого сервера с открытым портом 8080 (Axis2 на AppServer), получения учетных данных из конфигурационного файла axis2.xml и загрузки backdoor. Далее генерируется вредоносный PDF-файл для эксплуатации переполнения буфера в CoolReaderPDF на хосте Manager Workstation 1, что приводит к meterpreter-сессии. Завершающий этап — сканирование внутренней сети (10.10.3.0/24) и эксплуатация уязвимости в IGSS на SCADA Server, с установкой удаленной сессии.

Последствия включают установку reverse_shell соединений и meterpreter-

сессий, которые позволяют нарушителю закрепиться в системе и расширить доступ. Для детектирования используются:

- ViPNet IDS NS: Обнаружение вторжений через анализ сетевых пакетов, выявление этапов атаки (например, чтение axis2.xml или подключение на порт 4445).
- ViPNet TIAS: Интеллектуальный анализ событий на основе CEF-сообщений от сенсоров, классификация подозрительных инцидентов.
- Security Onion: Инструмент на базе Ubuntu с компонентами Snort, Suricata, Zeek, OSSEC, Sguil, Squert и Elastic Stack для полного захвата пакетов, обнаружения вторжений и анализа (включая визуализацию в Kibana и Squert).

Устранение уязвимостей включает настройку правил в iptables или Windows Firewall, обновление ПО до актуальных версий и удаление вредоносных файлов/процессов с помощью команд (например, kill, taskkill, rm).

4 Выполнение лабораторной работы

1. Заполнение карточек инцидентов.

Для обнаружения и анализа атак использовались средства ViPNet IDS NS. Были зафиксированы следующие ключевые инциденты, соответствующие этапам атаки (рис. 4.1, 4.2, 4.3, 4.4, 4.5)

Получение доступа через уязвимый Apache Axis2

Основная информация Чат В работе

Дата и время события 16.09.2025 09:39

Описание Получение несанкционированного доступа к файлам и приложениям. AM EXPLOIT Generic Path Traversal in HTTP URI var 21

Индикаторы компрометации web-application-attack

Рекомендации Обновить axis2, добавить правило в iptable для блокировки доступа к конфигурационному файлу

Прикрепленные файлы IDS_packet_time-2025-09-16T06_39_23.332563Z_ruleid-3106358.pcap

Оценка ★ ★ ★ ★ ★

Автор Ибатуллина Дарья @1f5222645@yafur.ru

Ответственный Ганин Тимур @1f5222645@yafur.ru

Источник 195.239.174.11

Пораженные активы 10.10.1.24

Рис. 4.1: Получение доступа через уязвимый Apache Axis 2

AM EXPLOIT Generic Command Injection in HTTP URI: 'netcat' in request

Основная информация Чат Новый

Дата и время события 16.09.2025 09:39

Описание Задокументирован HTTP-запрос к веб-серверу. Попытка выполнить командную инъекцию/удаленный запуск утилиты

Индикаторы компрометации web-application-attack

Рекомендации Изолировать хост, заблокировать источник, проверить процессы/соединения и завершить подозрительные, сменить пароли и ключи, обновить веб-приложение и компоненты

Прикрепленные файлы IDS_packet_time-2025-09-16T06_39_39.688936Z_ruleid-3111399.pcap

Оценка ★ ★ ★ ★ ★
Автор Ибрагимова Дарья
ИД #153226434@pfur.ru
Ответственный Не заполнено
Источник 195.239.174.11
Пораженные активы 10.10.1.24

Рис. 4.2: AM EXPLOIT Generic Command Injection in HTTP URI

AM POLICY Apache Axis2 v1.6 Default Admin Credential (CVE-2010-0219)

Основная информация Чат Новый

Дата и время события 16.09.2025 09:39

Описание Уязвимая версия axis2 установлена на AppServer под управлением Apache Tomcat. В типовом шаблоне информационной системы используется для развертывания веб-сервисов, работает через порт 80

Индикаторы компрометации attempted-admin

Рекомендации - Настройка правила в Iptables, которое отказывает в доступе к конфигурационному файлу при наличии в заголовке строки axis2.xml; - Обновить axis2 до последней версии.

Прикрепленные файлы IDS_packet_time-2025-09-16T06_39_45.884269Z_ruleid-3006394.pcap

Оценка ★ ★ ★ ★ ★
Автор Ибрагимова Дарья
ИД #153226434@pfur.ru
Ответственный Не заполнено
Источник 195.239.174.11
Пораженные активы 10.10.1.24

Рис. 4.3: AM POLICY Apache Axis2 v1.6 Default Admin Credential

ET TROJAN Possible Metasploit Payload Common Construct Bind_API (from server)

Основная информация Чат

Новый

Дата и время события: 16.09.2025 09:52

Описание: Возможная активность трояна / Metasploit bind-payload — подозрительный байт-контент в ответе сервера (Client Endpoint)

Индикаторы компрометации: trojan-activity

Рекомендации: Изолировать зараженный хост от сети, заблокировать источник через iptables, ограничить исходящий трафик залогиненного пользователя, завершить подозрительное соединение, пропустить антивирусное сканирование, удалить или восстановить систему из чистой резервной копии, сменить все пароли и ключи, установить обновления ОС и приложений

Прикрепленные файлы: IDS_packet_time-2025-09-16T06_52_31.569047Z_ruleid-2025644.pcap

Рис. 4.4: ET TROJAN Possible Metasploit Payload Common Construct Bind_API

Уязвимая версия IGSS AM Exploit 7T Interactive Graphical SCADA Buffer Overflow 0d

Основная информация Чат

В работе

Дата и время события: 16.09.2025 09:52

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

Индикаторы компрометации: web-application-attack

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

Прикрепленные файлы: IDS_packet_time-2025-09-16T06_52_19.7810822_ruleid-3006078.pcap

Рис. 4.5: Уязвимая версия IGSS AM Exploit 7T Interactive Graphical SCADA Buffer Overflow

- Инцидент 1: Сработало правило AM EXPLOIT Generic Path Traversal in HTTP URI, что свидетельствует о попытке злоумышленника получить несанкционированный доступ к файлам через уязвимость в Apache Axis2.
- Инцидент 2: Зафиксирован HTTP-запрос к веб-серверу. Попытка выполнить командную инъекцию/удалённый запуск утилит.

Инцидент 3: Уязвимая версия axis2 установлена на AppServer под управлением Apache Tomcat. В типовом шаблоне информационной системы используется для развертывания веб-сервисов, работает через порт 80.

- Инцидент 4: Этот инцидент сигнализирует о возможной активности трояна или полезной нагрузки Metasploit (bind-payload), обнаруженной в ответе сервера. Это подтверждает, что злоумышленник успешно установил бэкдор на SCADA-сервере.
- Инцидент 5: 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. Устранение первой уязвимости и последствия (Axis2, App backdoor).

На скриншоте (рис. 4.6) показан процесс аутентификации на целевом хосте:

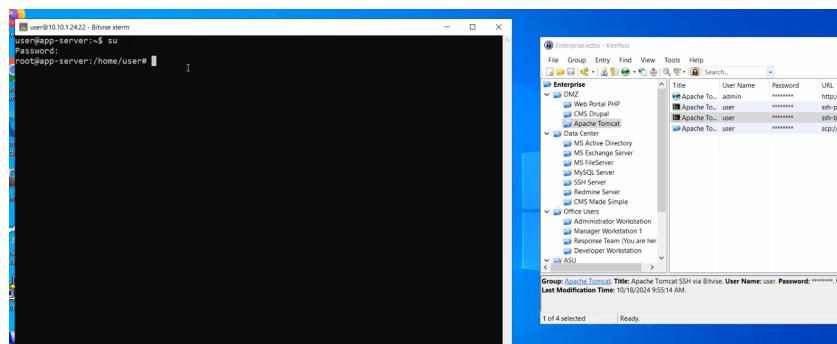


Рис. 4.6: Процесс аутентификации

Для блокировки доступа к конфигурационному файлу axis2.xml и предотвращения эксплуатации уязвимости CVE-2010-0219 в межсетевой экран iptables было добавлено специальное правило (рис. 4.7, 4.8)

Команда `sudo iptables -I INPUT 1 -j REJECT -p tcp --dport 8080 -m string --string "axis2.xml" --algo kmp` — добавляет правило в начало цепочки INPUT, которое отклоняет (REJECT) все входящие TCP-пакеты на порт 8080, если в них содержится строка axis2.xml.

Команда `sudo iptables -L INPUT -n --line-numbers` — выводит текущие правила цепочки INPUT с номерами строк для проверки.

```
user@app-server: ~
Chain ufw-user-logging-forward (0 references)
pkts bytes target prot opt in     out      source          destination

Chain ufw-user-limit (0 references)
pkts bytes target prot opt in     out      source          destination
    0     0 LOG      all  --  *      *      0.0.0.0/0      0.0.0.0/0
        limit: avg 3/min burst 5 LOG flags 0 level 4 prefix "[UFW LIMIT BLOCK]"
    "
    0     0 REJECT   all  --  *      *      0.0.0.0/0      0.0.0.0/0
        reject-with icmp-port-unreachable

Chain ufw-user-limit-accept (0 references)
pkts bytes target prot opt in     out      source          destination
    0     0 ACCEPT   all  --  *      *      0.0.0.0/0      0.0.0.0/0

root@app-server:/home/user# sudo iptables -I INPUT 1 -j REJECT -p tcp --dport 80
80 -m string --string "axis2.xml" --algo kmp
root@app-server:/home/user# sudo iptables -L INPUT -n --line-numbers
```

Рис. 4.7: Добавление правила в iptables для блокировки доступа к axis2.xml

```
user@app-server: ~
    0     0 REJECT   all  --  *      *      0.0.0.0/0      0.0.0.0/0
        reject-with icmp-port-unreachable

Chain ufw-user-limit-accept (0 references)
pkts bytes target prot opt in     out      source          destination
    0     0 ACCEPT   all  --  *      *      0.0.0.0/0      0.0.0.0/0

root@app-server:/home/user# sudo iptables -I INPUT 1 -j REJECT -p tcp --dport 80
80 -m string --string "axis2.xml" --algo kmp
root@app-server:/home/user# sudo 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:/home/user#
```

Рис. 4.8: Проверка правил

На скриншоте (рис. 4.9) видно, что у нас устранена первая уязвимость (Axis2), и можно приниматься за последствия.

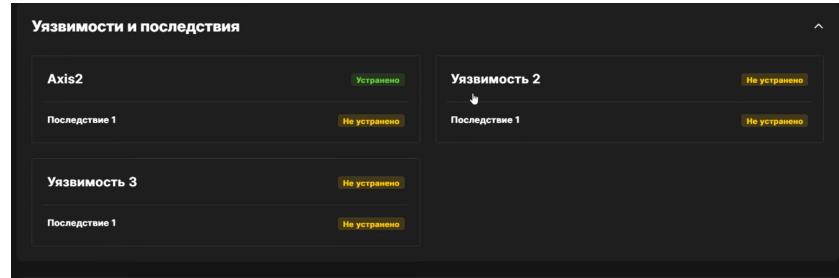


Рис. 4.9: Устранена уязвимость Axis2

Для полной проверки с помощью утилиты `ss` было выявлено установленное соединение с IP-адресом злоумышленника 195.239.174.11 на порт 7777, связанное с процессом `evil.conf` (PID 8367). Данное соединение является обратным shell-соединением (backdoor), установленным нарушителем, и подлежало немедленному завершению (рис. 4.10)

```
user@app-server: ~
x 14100 users:(("sshd",pid=11576,fd=3), ("sshd",pid=11574,fd=3))
ESTAB 0 0 10.10.1.24:55718 195.239.174.11:-
7777 users:(("evil.conf",pid=8367,fd=3))
CLOSING 1 190 127.0.0.1:34556 127.0.0.1:-
http-alt
FIN-WAIT-1 0 190 127.0.0.1:34714 127.0.0.1:-
http-alt
ESTAB 0 0 [::ffff:10.10.1.24]:http-alt [::ffff:10.10.1.253]:-
58975 users:(("java",pid=598,fd=116))
ESTAB 0 0 [::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:-
34728 users:(("java",pid=598,fd=128))
FIN-WAIT-2 0 0 [::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:-
34686
ESTAB 0 0 [::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:-
34702 users:(("java",pid=598,fd=214))
FIN-WAIT-2 0 0 [::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:-
34644
ESTAB 0 0 [::ffff:10.10.1.24]:58486 [::ffff:195.239.174.11]:-
4422 users:(("java",pid=598,fd=530))
FIN-WAIT-2 0 0 [::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:-
34658
FIN-WAIT-2 0 0 [::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:-
34626
ESTAB 0 0 [::ffff:127.0.0.1]:http-alt [::ffff:127.0.0.1]:-
```

Рис. 4.10: Процесс `evil.conf`

Переход к редактированию файла планировщика заданий `crontab` для пользователя `tomcat` (рис. 4.11)

```
user@app-server: ~
34658  FIN-WAIT-2 0      [::ffff:127.0.0.1]:http-alt      [::ffff:127.0.0.1]:
34626  ESTAB     0      [::ffff:127.0.0.1]:http-alt      [::ffff:127.0.0.1]:
34714  users:(("java",pid=598,fd=54))
FIN-WAIT-2 0      [::ffff:127.0.0.1]:http-alt      [::ffff:127.0.0.1]:
34676  FIN-WAIT-1 0      20376  [::ffff:10.10.1.24]:http-alt      [::ffff:10.10.1.253]:
20226  ESTAB     0      [::ffff:10.10.1.24]:http-alt      [::ffff:10.10.1.253]:
40148  users:(("java",pid=598,fd=130))
ESTAB     0      [::ffff:10.10.1.24]:http-alt      [::ffff:10.10.1.253]:
61668  users:(("java",pid=598,fd=125))
CLOSE-WAIT 1      0      [::ffff:10.10.1.24]:http-alt      [::ffff:195.239.174.11]:
33071  users:(("java",pid=598,fd=529))
FIN-WAIT-2 0      0      [::ffff:127.0.0.1]:http-alt      [::ffff:127.0.0.1]:
34598  FIN-WAIT-2 0      [::ffff:127.0.0.1]:http-alt      [::ffff:127.0.0.1]:
34612  ESTAB     0      20375  [::ffff:10.10.1.24]:http-alt      [::ffff:10.10.1.253]:
64496  users:(("java",pid=598,fd=127))
root@app-server:/home/user# /var/log/syslog
bash: /var/log/syslog: Permission denied
root@app-server:/home/user# nano /var/spool/cron/tomcat
```

Рис. 4.11: Переход к редактированию файла

В файле tomcat (рис. 4.12, 4.13) было обнаружено вредоносное задание

* * * /opt/tomcat/webapps/evil.conf

```
user@app-server: ~
GNU nano 3.2          /var/spool/cron/crontabs/tomcat
[ Read 4 lines ]
^G Get Help  ^C Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Рис. 4.12: Редактирование файла /var/spool/cron/crontabs/tomcat

```
user@app-server: ~
GNU nano 3.2          /var/spool/cron/crontabs/tomcat
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontask installed on Tue Sep 16 09:40:38 2025)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)

[ Read 4 lines ]
```

Рис. 4.13: Удалили строку

После отключения автозапуска следующим шагом стало непосредственное удаление самого файла evil.conf и завершение активного процесса, который он запустил (рис. 4.14, 4.15). Эти действия полностью нейтрализуют последствие атаки – “App Backdoor”. После этого на сервере не остаётся ни вредоносного кода, ни механизмов его автоматического запуска. После проведения всех мероприятий была проверена общая картина устранения уязвимостей и последствий атаки.

```

user@app-server: ~
FIN-WAIT-2 0      0      [::ffff:127.0.0.1]:http-alt      [::ffff:127.0.0.1]:^
34676
FIN-WAIT-1 0      20376  [::ffff:10.10.1.24]:http-alt      [::ffff:10.10.1.253]:^
20226
ESTAB     0      0      [::ffff:10.10.1.24]:http-alt      [::ffff:10.10.1.253]:^
40148    users:(["java",pid=598,fd=130])
ESTAB     0      0      [::ffff:10.10.1.24]:http-alt      [::ffff:10.10.1.253]:^
61668    users:(["java",pid=598,fd=125])
CLOSE-WAIT 1      0      [::ffff:10.10.1.24]:http-alt      [::ffff:195.239.174.11]:^
33071    users:(["java",pid=598,fd=529])
FIN-WAIT-2 0      0      [::ffff:127.0.0.1]:http-alt      [::ffff:127.0.0.1]:^
34598
FIN-WAIT-2 0      0      [::ffff:127.0.0.1]:http-alt      [::ffff:127.0.0.1]:^
34612
ESTAB     0      20375  [::ffff:10.10.1.24]:http-alt      [::ffff:10.10.1.253]:^
64496    users:(["java",pid=598,fd=127])
root@app-server:/home/user# /var/log/syslog
bash: /var/log/syslog: Permission denied
root@app-server:/home/user# nano /var/spool/cron/crontabs/tomcat
root@app-server:/home/user# nano /var/spool/cron/crontabs/tomcat
root@app-server:/home/user# cd /opt/tomcat/webapps
root@app-server:/opt/tomcat/webapps# rm evil.conf
root@app-server:/opt/tomcat/webapps# kill 8367
root@app-server:/opt/tomcat/webapps#

```

Рис. 4.14: Удаление вредоносного файла и завершение процесса

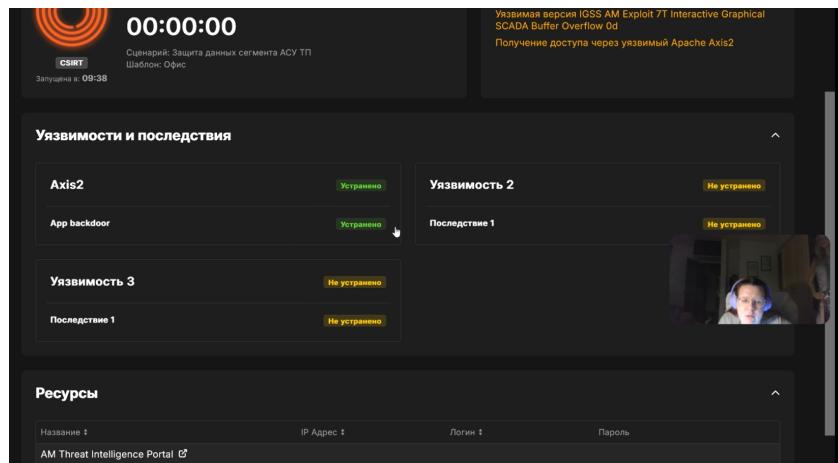


Рис. 4.15: Устранена первая уязвимость и её последствие

2. Устранение второй уязвимости и её последствий.

Для продолжения лабораторной работы по устранению других уязвимостей (CoolReaderPDF) были получены учетные данные для доступа к рабочей станции менеджера (рис. 4.16).

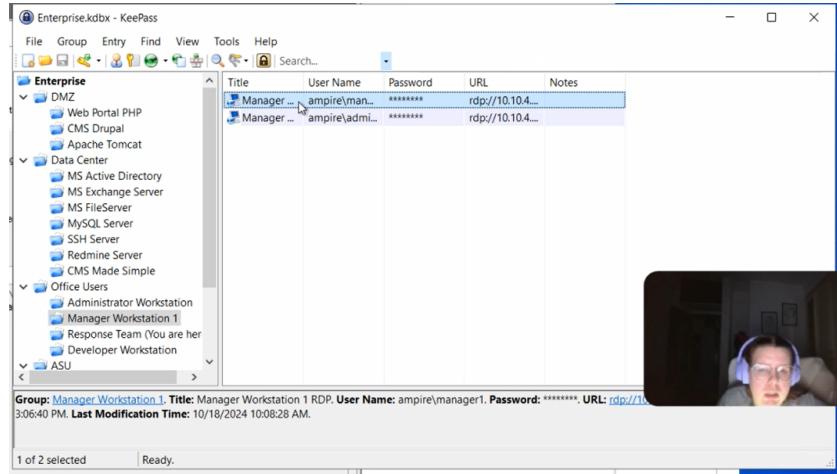


Рис. 4.16: Доступ к Manager Workstation

Была реализована блокировка сетевого трафика для уязвимой программы CoolReaderPDF, что является ключевой мерой по предотвращению дальнейшего распространения вредоносного кода и установления обратных соединений с машиной злоумышленника (рис. 4.17, 4.18, 4.19, 4.20, 4.21).

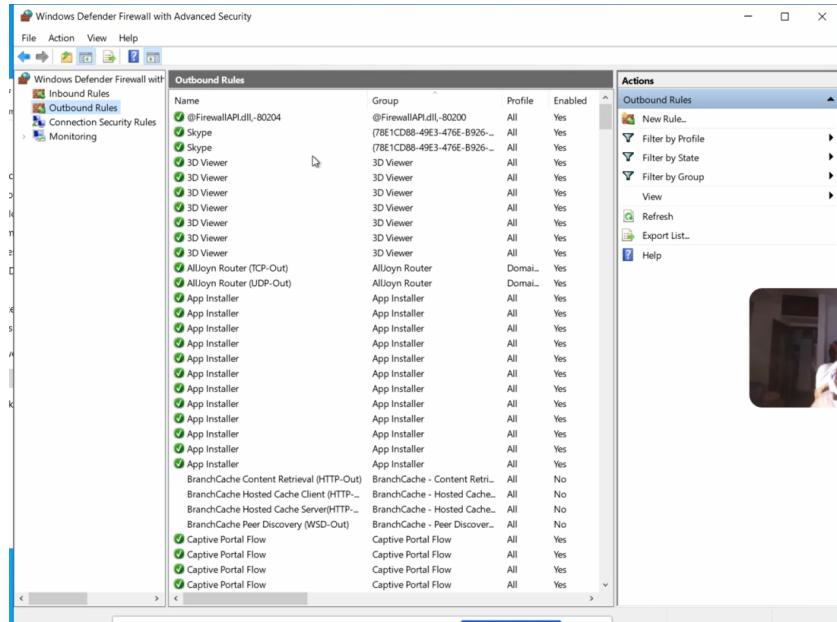


Рис. 4.17: Windows defender firewall

На скриншоте ниже показан начальный этап создания нового правила бранд-

мауэра. Выбран тип правила «Для программы», что позволяет заблокировать сетевую активность конкретного приложения.

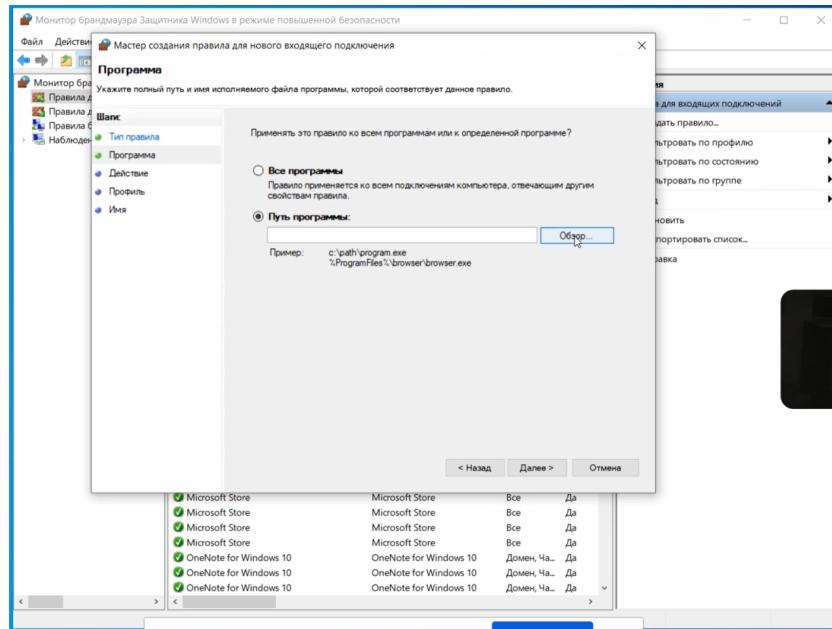


Рис. 4.18: Этап создания нового правила брандмауэра

Далее отображено окно настройки создаваемого правила:

- Указано имя правила: CoolPDFReader.
- Выбрано действие «Блокировать подключение», которое запрещает любое входящее и исходящее сетевое взаимодействие для уязвимой программы.

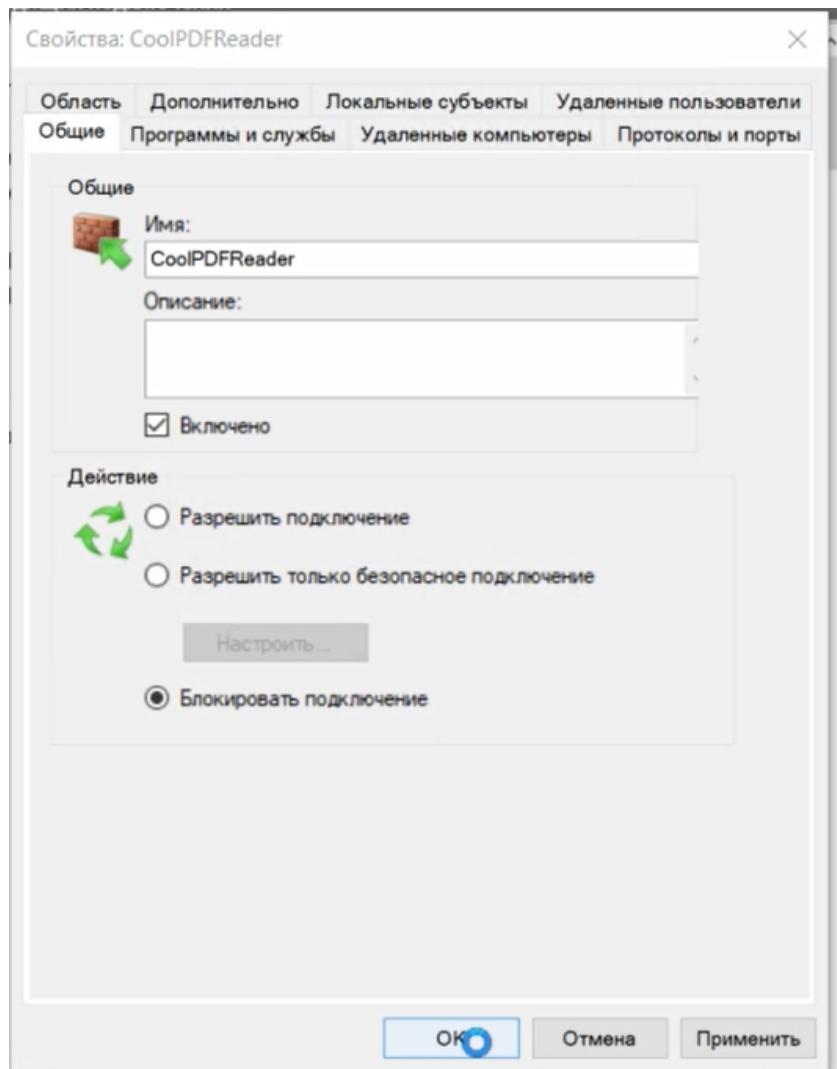


Рис. 4.19: Окно настройки создаваемого правила

На скриншоте ниже выполняется проверка в «Мониторе брандмауэра Защитника Windows». В списке правил для входящих подключений присутствует созданное правило CoolPDFReader. Это подтверждает, что уязвимое приложение теперь изолировано от сети, что предотвращает его использование злоумышленником для получения удаленного доступа.

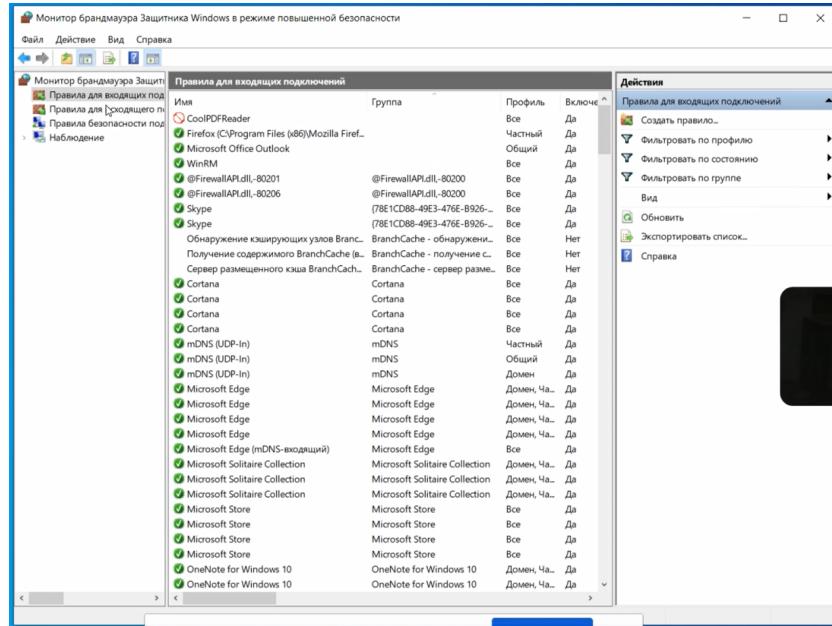


Рис. 4.20: Проверка в «Мониторе брандмауэра Защитника Windows»

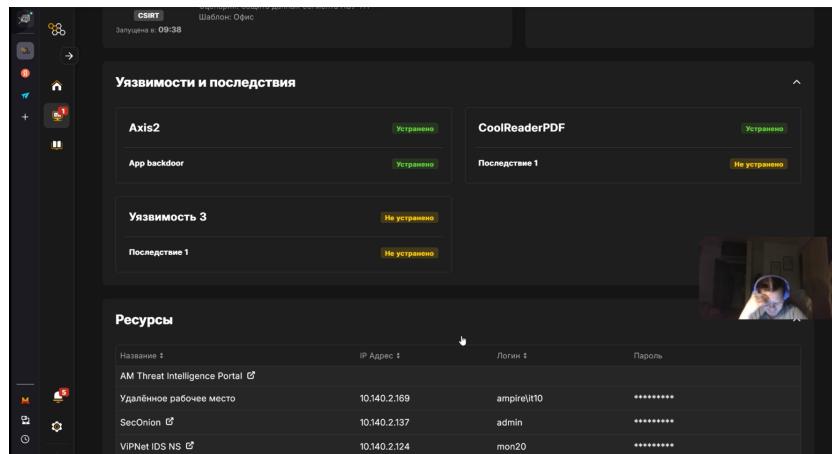


Рис. 4.21: Устранена уязвимость 2 (CoolReaderPDF)

Далее работали с последствием этой уязвимости.

После открытия командной строки была выполнена команда `netstat -bno`, которая выводит список всех TCP-соединений вместе с именами процессов и их PID (рис. 4.22).

Выбрать Администратор: Windows PowerShell					
TCP	10.10.4.11:50401	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50402	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50403	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50404	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50405	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50406	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50407	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50408	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50409	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50410	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50411	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50412	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50413	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50414	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50415	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50416	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50417	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50418	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50419	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50420	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50421	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50422	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50423	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50424	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50425	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50426	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50427	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50428	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50429	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50430	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50431	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50432	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50433	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50434	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:50435	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50436	195.239.174.12:443	TIME_WAIT	0	
TCP	10.10.4.11:50437	10.10.1.21:80	TIME_WAIT	0	
TCP	10.10.4.11:60438	195.239.174.11:4445	ESTABLISHED	5348	
[CoolPDFReader.exe]					
TCP	127.0.0.1:33333	127.0.0.1:49632	ESTABLISHED	4	
Не удается получить сведения о владельце					
TCP	127.0.0.1:49632	127.0.0.1:33333	ESTABLISHED	8164	
[EppLocalConsole.exe]					
PS C:\Users\administrator> ■					

Рис. 4.22: Список всех TCP-соединений

Для устранения угрозы была выполнена команда: `taskkill /f /pid 5348`. Эта команда принудительно (`/f`) завершает процесс с идентификатором 5348 (рис. 4.23).

```

Administrator: Windows PowerShell
TCP 10.10.4.11:50401 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50402 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50403 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50404 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50405 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50406 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50407 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50408 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50409 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50410 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50411 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50412 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50413 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50414 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50415 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50416 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50417 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50418 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50419 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50420 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50421 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50422 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50423 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50424 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50425 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50426 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50427 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50428 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50429 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50430 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50431 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50432 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50433 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50434 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:50435 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50436 195.239.174.12:443 TIME_WAIT 0
TCP 10.10.4.11:50437 10.10.1.21:80 TIME_WAIT 0
TCP 10.10.4.11:60430 195.239.174.11:4445 ESTABLISHED 5348
[CoopPDFReader.exe]
TCP 127.0.0.1:33333 127.0.0.1:49632 ESTABLISHED 4
Не удается получить сведения о владельце
TCP 127.0.0.1:49632 127.0.0.1:33333 ESTABLISHED 8164
[EppLocalConsole.exe]

PS C:\Users\administrator> taskkill /f /pid 5348
Успешно: Процесс, с идентификатором 5348, успешно завершен.

PS C:\Users\administrator>

```

Рис. 4.23: taskkill /f /pid 5348

Обновление статуса в разделе «Уязвимости и последствия»: на данном скриншоте (рис. 4.24) отображается интерфейс управления уязвимостями в системе «Ampire».

- Уязвимость CoolReaderPDF также помечена как «Устранено».
- Последствие Manager meterpreter теперь также имеет статус «Устранено».

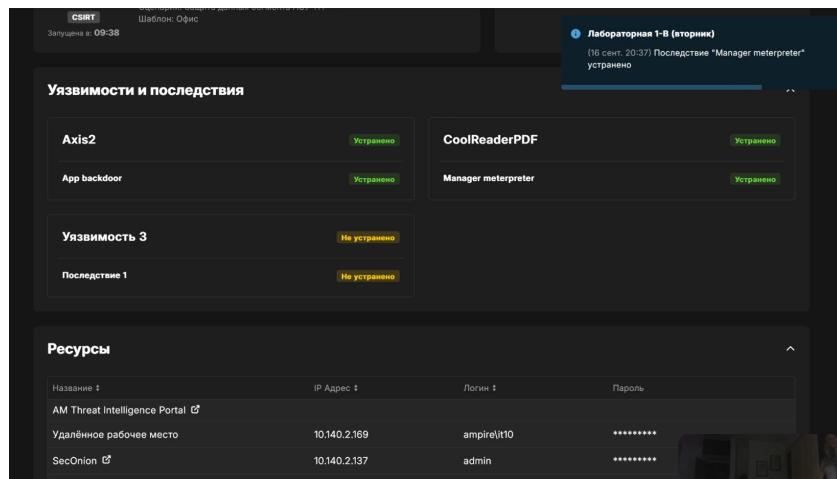


Рис. 4.24: Полностью устранена вторая уязвимость и её последствия

3. Устранение третьей уязвимости и её последствий.

Для проведения работ по защите SCADA-сервера необходимо было получить удалённый доступ к нему. Для этого был использован менеджер паролей KeePass (рис. 4.25)

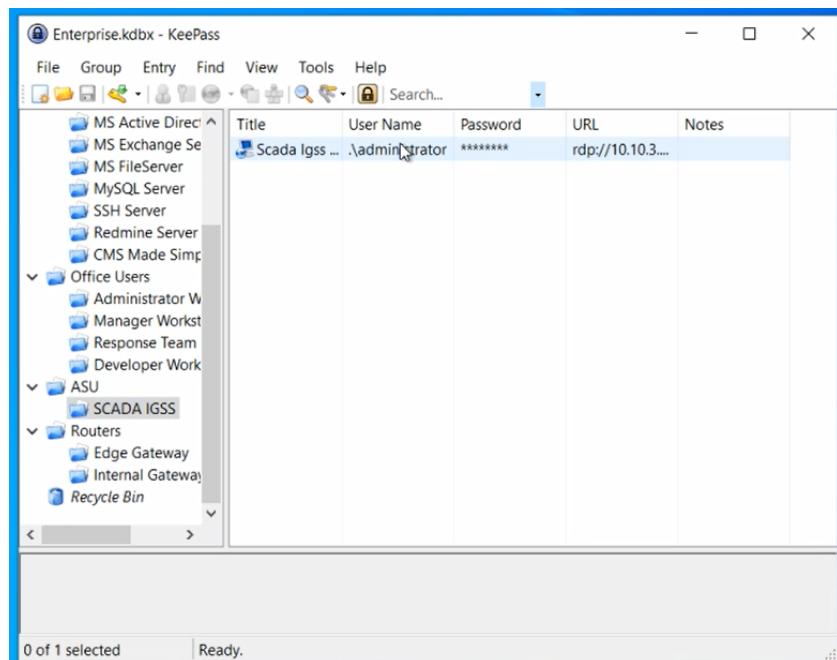


Рис. 4.25: Удаленный доступ к SCADA-сервер

Далее был запущен “Windows security center” (рис. 4.26): в меню “Пуск” - “Accessories” - “System Tools” - “Security center”.

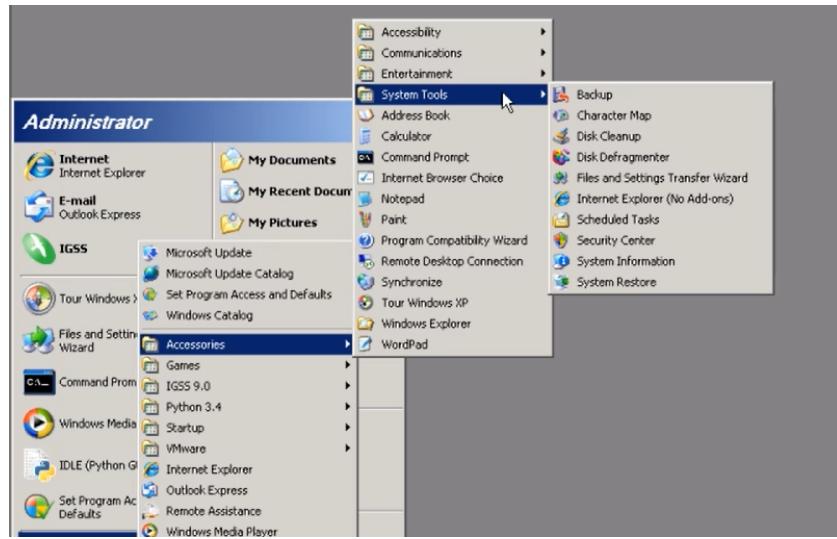


Рис. 4.26: “Пуск” - “Accessories” - “System Tools” - “Security center”

После этого мы включили брандмауэр (рис. 4.27).

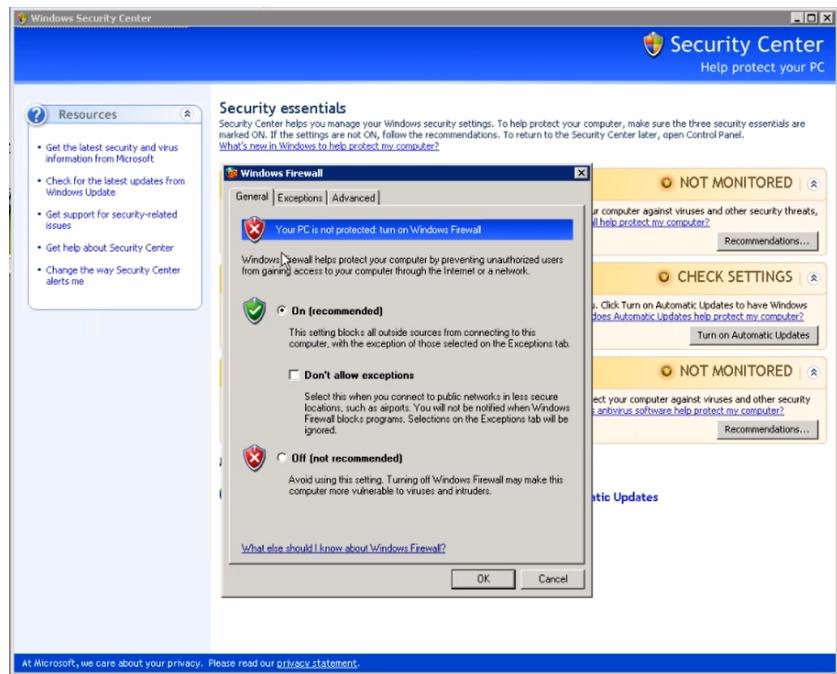


Рис. 4.27: Брандмауэр

На скриншоте (рис. 4.28) на вкладке “Исключения” брандмауэра виден список правил, для которых мы убрали из исключений IGSS Dataserver. Эти правила были использованы злоумышленником для эксплуатации уязвимости.

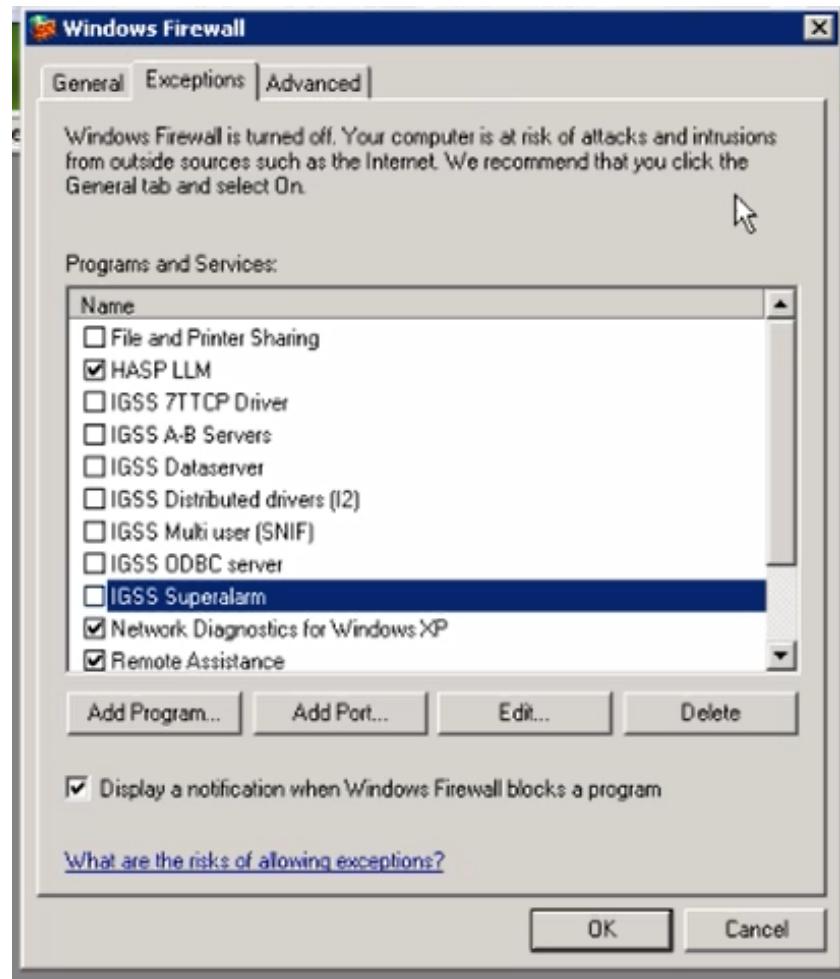


Рис. 4.28: Убрали из исключений IGSS Dataserver

На скриншоте (рис. 4.29) видно, что после настройки брандмауэра уязвимость IGSS32 была устранена, можно приниматься за последствия

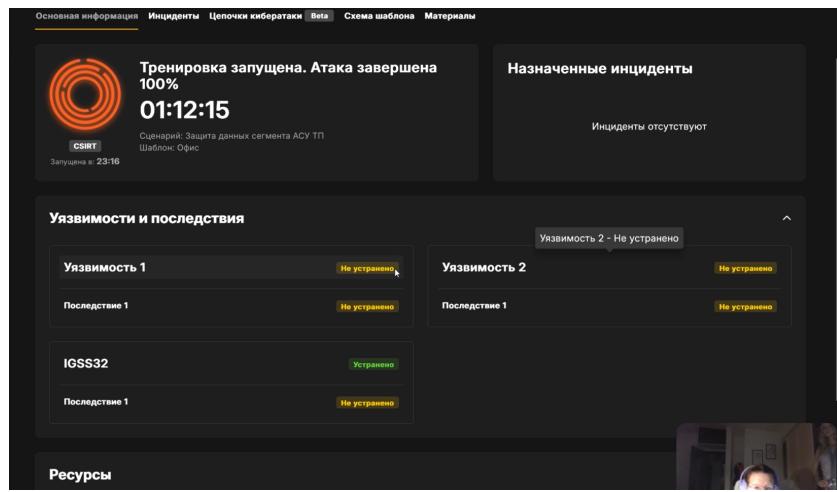


Рис. 4.29: Уязвимость IGSS32 была устранена

Команда netstat -bno (рис. 4.30) выявила установленное TCP-соединение между SCADA-сервером (10.10.3.10:1163) и IP-адресом злоумышленника (195.239.174.11:28002). Процесс, ответственный за соединение,— IGSSdataServer.exe (PID 2484).

Для нейтрализации угрозы процесс был принудительно завершен командой taskkill /f /pid 2484.

```
Administrator: Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -bno
Active Connections
 Proto  Local Address          Foreign Address        State      PID
 TCP    10.10.3.10:1163        195.239.174.11:28002  ESTABLISHED 2484
 TCP    10.10.3.10:3389        10.10.4.12:57945      ESTABLISHED 868
 TCP    [unknown component(s)] -- 10.10.4.12:57945      TIME_WAIT   0
 TCP    127.0.0.1:1249         127.0.0.1:12401       TIME_WAIT   0
 TCP    127.0.0.1:1250         127.0.0.1:12401       TIME_WAIT   0
 TCP    127.0.0.1:1259         127.0.0.1:12401       TIME_WAIT   0
 TCP    127.0.0.1:1260         127.0.0.1:12401       TIME_WAIT   0

C:\Documents and Settings\Administrator>taskkill /f /pid 2484
SUCCESS: The process with PID 2484 has been terminated.

C:\Documents and Settings\Administrator>-
```

Рис. 4.30: TCP-соединение

Панель управления (рис. 4.31) подтвердила успешное устранение уязвимости IGSS32 и последствия IGSS meterpreter. Все ключевые этапы атаки были нейтра-

лизованы.

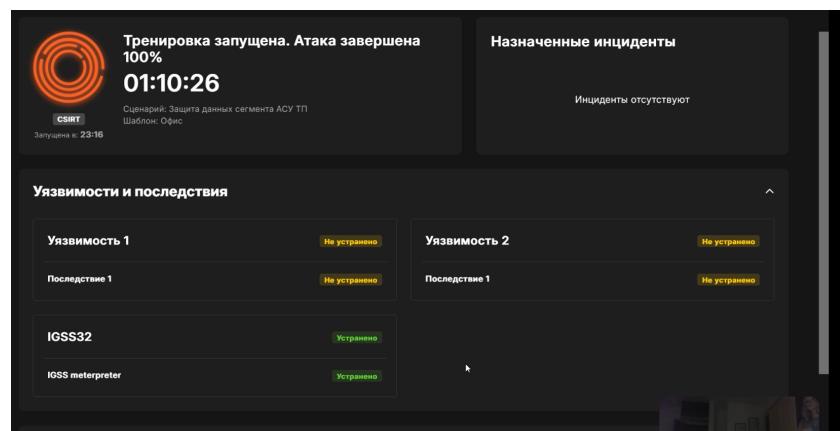


Рис. 4.31: Полностью устранена третья уязвимость и её последствия

5 Выводы

В ходе выполнения лабораторной работы был успешно отработан сценарий комплексной кибератаки на сегмент АСУ ТП и проведены мероприятия по её обнаружению и нейтрализации.

6 Список литературы

1. CVE-2010-0219 – Apache Axis2 Default Credentials
2. CVE-2012-4914 – CoolPDF Reader Stack Buffer Overflow
3. CVE-2011-1567 – IGSS Stack Buffer Overflow
4. IGSS – Interactive Graphical SCADA System
5. iptables man page
6. Security Onion Documentation
7. ViPNet IDS NS – Руководство администратора
8. Metasploit Unleashed – Free Ethical Hacking Course