Отчет по лабораторной работе №1-В
«ЗАЩИТА ДАННЫХ СЕГМЕНТА АСУ ТП»

Кибербезопасность предприятия

Апареев Д.А
Игнатенкова В.Н.
Демидович Н.М.
Ендонова А.В.

Машковцева К.С.

Шубнякова Д.И.

Содержание

1. Цель работы

Целью данной лабораторной работы является освоение практических навыков выявления, анализа и устранения уязвимостей информационных систем, а также последствий компьютерных атак на критически важный сегмент предприятия — автоматизированные системы управления технологическим процессом (АСУ ТП).

2. Задание

Обнаружить, проанализировать и закрыть уязвимости:

1. Уязвимая версия Apache Axis2 (CVE-2010-0219);
2. Уязвимая версия программы CoolReaderPDF (CVE-2012-4914);
3. Уязвимая версия IGSS (CVE-2011-1567).

Определить и устранить последствия эксплуатации уязвимостей:

1. App Backdoor (последствие уязвимости 1);
2. Manager meterpreter-сессия (последствие уязвимости 2);
3. IGSS meterpreter-сессия (последствие уязвимости 3).

Разработать и применить меры по устранению выявленных уязвимостей и их последствий.

3. Теоретическое введение

VipNet IDS (Intrusion Detection System) — это система обнаружения вторжений, предназначенная для мониторинга сетевого трафика, выявления подозрительной активности и генерации оповещений о потенциальных атаках. В рамках данной работы используется для детектирования этапов атаки нарушителя.

VipNet TIAS (Threat Intelligence Analytics System) — аналитическая система, предназначенная для автоматического выявления инцидентов информационной безопасности на основе интеллектуального анализа событий.

Security Onion — дистрибутив для мониторинга сетевой безопасности, включающий в себя такие инструменты, как Snort, Suricata, Zeek, OSSEC, Squil, Squert и Elastic Stack для полного захвата пакетов, обнаружения угроз и анализа.

АСУ ТП — автоматизированные системы управления технологическим процессом. Защита данного сегмента является критически важной, так как компрометация может привести к серьезным технологическим и экономическим последствиям.

Уязвимость CVE-2010–0219 (Apache Axis2) — наличие учетной записи администратора по умолчанию (admin/axis2) в компоненте Axis2, позволяющее злоумышленнику загрузить и выполнить произвольный вредоносный веб-сервис.

Уязвимость CVE-2012–4914 (CoolReaderPDF) — переполнение стека при открытии специально сгенерированного PDF-документа, приводящее к удаленному выполнению кода.

Уязвимость CVE-2011–1567 (IGSS) — переполнение стека в программе IGSSdataServer.exe при выполнении операции ListAll, позволяющее злоумышленнику получить удаленный доступ к системе.

Meterpreter — полезная нагрузка (payload) фреймворка Metasploit, предоставляющая злоумышленнику расширенный контроль над скомпрометированной системой.

4. Выполнение лабораторной работы

4.1 Обнаружение уязвимостей и последствий

Для обнаружения подозрительной активности и инцидентов безопасности использовались средства VipNet IDS NS, VipNet TIAS и Security Onion.

4.1.1 Обнаружение уязвимости "Уязвимая версия Axis2 (CVE-2010-0219)"

В журналах VipNet IDS NS было зафиксировано событие с сигнатурой "AM POLICY Apache Axis2 v1.6 Default Admin Credential (CVE-2010-0219)", указывающее на попытку доступа к конфигурационному файлу `axis2.xml` и использование учетных данных по умолчанию.

Рисунок 1: Событие в VipNet IDS NS о попытке эксплуатации уязвимости Axis2

Анализ в VipNet TIAS подтвердил данное событие как подозрительное.

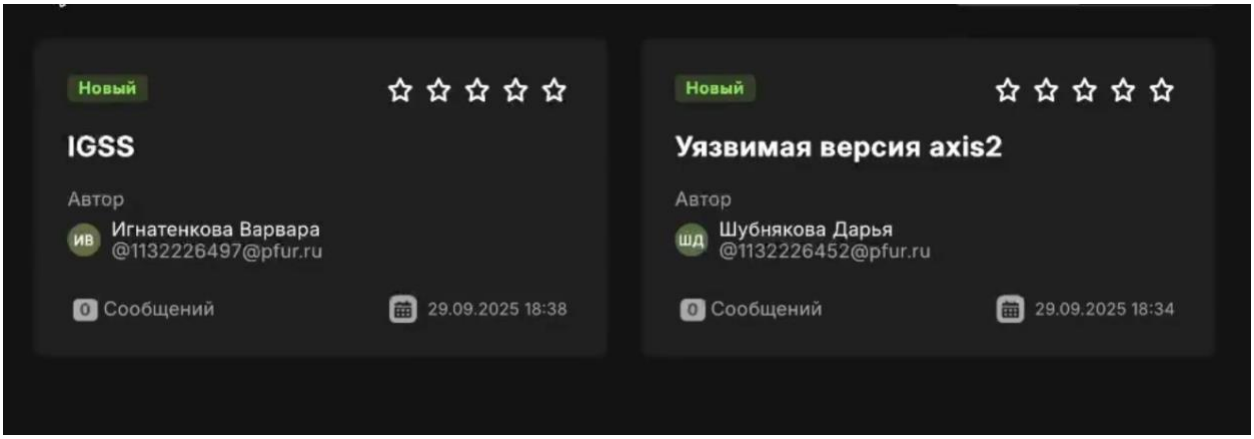

Рисунок 2: Подтверждение инцидента в VipNet TIAS

4.1.2 Обнаружение последствия "App Backdoor"

После успешной эксплуатации уязвимости Axis2 нарушитель загрузил на сервер (AppServer) backdoor-файл. В VipNet IDS были зафиксированы события, связанные с установлением обратного соединения (reverse shell) с IP-адресом нарушителя.

На самом сервере наличие backdoor подтверждается командой `ss -tp`, показывающей установленные сетевые соединения, а также записью в журнале `/var/log/syslog` о автозапуске файла через cron.

Рисунок 3: Обнаружение установленного соединения с нарушителем с помощью ss -tp

Рисунок 4: Запись об автозапуске backdoor в /var/log/syslog

4.1.3 Обнаружение уязвимости "Уязвимая версия CoolReaderPDF (CVE-2012–4914)"

На этапе атаки на рабочую станцию менеджера в VipNet IDS были зафиксированы события загрузки и передачи PDF-документа. Последующая активация полезной нагрузки была детектирована по событиям, связанным с установлением meterpreter-сессии.

Рисунок 5: События в VipNet IDS, связанные с атакой на CoolReaderPDF

4.1.4 Обнаружение последствия "Manager meterpreter-сессия"

Факт установления сессии на рабочей станции менеджера подтверждается с помощью утилиты `netstat -bno` в Windows, которая отображает установленные соединения и связанные с ними процессы.

Рисунок 6: Обнаружение обратного соединения с нарушителем на Manager Workstation с помощью netstat

4.1.5 Обнаружение уязвимости "Уязвимая версия IGSS (CVE-2011–1567)"

Атака на сервер АСУ ТП была детектирована VipNet IDS по событиям сканирования порта 12401 и последующей попытки эксплуатации уязвимости в IGSSdataServer.exe.

Рисунок 7: События в VipNet IDS, связанные с атакой на IGSS

4.1.6 Обнаружение последствия "IGSS meterpreter-сессия"

На сервере АСУ ТП с помощью `netstat -bno` было обнаружено установленное соединение с IP-адресом нарушителя, связанное с процессом, запущенным эксплойтом.

Рисунок 8: Обнаружение обратного соединения на SCADA Server

4.2 Устранение уязвимостей и их последствий

4.2.1 Устранение уязвимости "Уязвимая версия Axis2" и последствия "App Backdoor"

1. Устранение последствия (App Backdoor):

- На сервере AppServer был найден и удален файл backdoor (`evil.conf`), расположенный по пути `/opt/tomcat/webapps/`.

- Из файла `/var/spool/cron/crontabs/tomcat` была удалена задача автозапуска backdoor

- С помощью команды `kill <PID>` были завершены все активные сессии, связанные с backdoor.

Рисунок 9: Удаление задачи из crontab

Рисунок 10: Удаление файла backdoor

2. Устранение уязвимости (CVE-2010–0219):

- Для блокировки доступа к конфигурационному файлу было добавлено правило в iptables: `iptables -I INPUT 1 -j REJECT -p tcp --dport 8080 -m string --string "axis2.xml" --algo kmp`.

- Альтернативным и более надежным решением является обновление Axis2 до актуальной версии через веб-интерфейс менеджера Tomcat или полная остановка (Stop) уязвимого приложения.

Рисунок 11: Добавление правила в iptables

Рисунок 12: Остановка приложения Axis2 в менеджере Tomcat

4.2.2 Устранение уязвимости "Уязвимая версия CoolReaderPDF" и последствия "Manager meterpreter-сессия"

1. Устранение последствия (Manager meterpreter):

На рабочей станции менеджера с помощью команды `taskkill /f /pid <PID>` был принудительно завершен процесс, установивший соединение с нарушителем.

Рисунок 13: Завершение процесса meterpreter на Manager Workstation

2. Устранение уязвимости (CVE-2012–4914):

Программа CoolReaderPDF была обновлена до последней версии, не подверженной уязвимости.

В качестве временной меры может быть настроено правило в брандмауэре, блокирующее исходящий трафик от приложения CoolReaderPDF.

4.2.3 Устранение уязвимости "Уязвимая версия IGSS" и последствия "IGSS meterpreter-сессия"

1. Устранение последствия (IGSS meterpreter):

На сервере АСУ ТП с помощью команды `taskkill /f /pid <PID>` был принудительно завершен процесс, связанный с атакой.

Рисунок 14: Завершение процесса meterpreter на SCADA Server

2. Устранение уязвимости (CVE-2011–1567):

Было включено и настроено исключение в Брандмауэре Windows, запрещающее несанкционированный доступ к IGSS DataServer.

Рекомендуется обновить ПО IGSS до защищенной версии.

Рисунок 15: Настройка Брандмауэра Windows для IGSS

4.3 Результат

После выполнения всех мероприятий по устранению уязвимостей и их последствий в средствах мониторинга (VipNet IDS, VipNet TIAS) более не фиксируется подозрительная активность, связанная с данным сценарием атаки. Все backdoor-файлы удалены, установленные злоумышленником соединения разорваны, а уязвимое ПО либо обновлено, либо защищено с помощью правил фильтрации.

Рисунок 16: Отсутствие активных инцидентов в VipNet TIAS после устранения

Рисунок 17: Подтверждение отсутствия вредоносных соединений с помощью netstat/ss

5. Выводы

В ходе выполнения лабораторной работы были успешно освоены практические навыки по защите сегмента АСУ ТП. Были отработаны методы обнаружения сложных многоэтапных атак с использованием современных средств защиты (VipNet IDS NS, VipNet TIAS, Security Onion). Приобретен опыт анализа сетевого трафика, системных логов и процессов для выявления последствий атак. Разработаны и применены эффективные меры по устранению уязвимостей и нейтрализации активных угроз, что позволило восстановить безопасность критически важной инфраструктуры предприятия.

Список литературы

1. Common Vulnerabilities and Exposures (CVE) — CVE-2010–0219 [Электронный ресурс].

2. Common Vulnerabilities and Exposures (CVE) — CVE-2012-4914 [Электронный ресурс].

3. Common Vulnerabilities and Exposures (CVE) — CVE-2011-1567 [Электронный ресурс].

4. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак "Ampire". Сценарий №4 «ЗАЩИТА ДАННЫХ СЕГМЕНТА АСУ ТП» [Электронный ресурс].

5. Официальная документация по VipNet IDS NS и VipNet TIAS [Электронный ресурс].

6. Официальный сайт и документация Security Onion [Электронный ресурс].