

Лабораторная Работа №1.

Кибербезопасность предприятия

Боровиков Даниил Александрович, Хрусталев Влад Николаевич, Гисматуллин
Артем, Тщесноков Артёмий Pavlovich, Коннова Татьяна, Нефедова Наталья,
Уткина Алина, Бансимба Клодели

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Сценарий №2

Защита контроллера домена предприятия

Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам компании. 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.

Сканирование на SQL-инъекции

The screenshot displays the ViPNet IDS NS web interface. The left sidebar contains navigation options: Мониторинг, Информанель, События, Отчеты, Управление, Сетевое окружение, Методы анализа, Правила анализа, Оповещения, and Интеграция. The main area is titled 'События' and shows a table of events for the last 24 hours. The table columns are: У., Дата и время, Код события, К., Название правила, and others. The event list includes several entries for 'AM SQL Generic SQLi in HTTP URI' and one for 'ET WEB_SERVER Possible MySQL SQL Attempt Inform...'. The event '12:19:02.374 18...' is selected and highlighted in blue. To the right, a detailed view of this event is shown, including 'Общая информация' (General information) and 'Правило анализа' (Analysis rule).

События

События за последние 24 часа

У.	Дата и время	Код события	К.	Название правила	Пр
12:19:02.133 18...	2017808	1	ET WEB_SERVER Possible MySQL SQL Attempt Inform...	w TO	
12:19:02.147 18...	2017808	1	ET WEB_SERVER Possible MySQL SQL Attempt Inform...	w TO	
12:19:02.147 18...	3111675	1	AM SQL Generic SQLi in HTTP URI 'SELECT FROM INF...	w TO	
12:19:02.211 18...	3004388	1	AM SQL Generic SQLi in HTTP URI 'UNION SELECT' qu...	w TO	
12:19:02.211 18...	3297187	1	AM SQL Generic SQLi in HTTP URI 'UNION SELECT' qu...	w TO	
12:19:02.221 18...	3297187	1	AM SQL Generic SQLi in HTTP URI 'UNION SELECT' qu...	w TO	
12:19:02.221 18...	3004388	1	AM SQL Generic SQLi in HTTP URI 'UNION SELECT' qu...	w TO	
12:19:02.241 18...	3111949	1	AM SQL Generic SQLi in HTTP URI 'SELECT CASE' query	w TO	
12:19:02.253 18...	3111949	1	AM SQL Generic SQLi in HTTP URI 'SELECT CASE' query	w TO	
12:19:02.353 18...	3111949	1	AM SQL Generic SQLi in HTTP URI 'SELECT CASE' query	w TO	
12:19:02.374 18...	3112442	1	AM SQL Generic SQLi in HTTP URI 'SELECT SLEEP' qu...	w TO	
12:19:02.374 18...	2016935	1	ET WEB_SERVER SQL Injection Select Sleep Time Delay	w TO	
12:19:07.387 18...	3112442	1	AM SQL Generic SQLi in HTTP URI 'SELECT SLEEP' qu...	w TO	

« < Страница 1 > »

Событие 12:19:02.374 18.09.2025

Событие | Источник | Получатель | Пакет

Общая информация

Дата и время: 12:19:02.374 18.09.2025
Интерфейс захвата: eth2
Уровень важности: Высокий
Тип события: Сигнальное событие
Протокол: TCP
Код события: 2016935
Клиентское приложение: sqfmap/1.7.2#stable (https://sqfmap.org)
Доменное имя ресурса: 195.239.174.95

Правило анализа

Класс: web-application-attack
Группа: web_server
Название: ET WEB_SERVER SQL Injection Select Sleep Time Delay
Описание:

Figure 1: Сканирование на SQL-инъекции

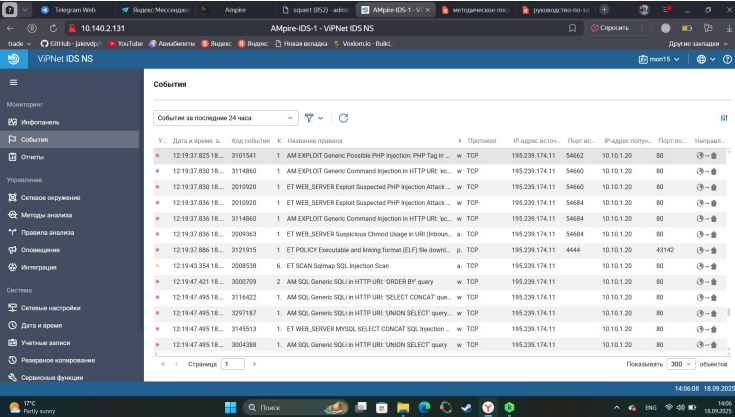
Детектирование SQL-инъекции

The screenshot displays the VIPNet IDS NS web interface. The left sidebar contains navigation options: Мониторинг, Информанель, События, Отчеты, Управление, Сетевое окружение, Методы анализа, Правила анализа, Оповещения, Интеграция, Система, Сетевые настройки, Дата и время, Учетные записи, Резервное копирование, and Сервисные функции. The main panel, titled 'События', shows a table of events for the last 24 hours. The table columns are: У., Дата и время, Код события, К., Название правила, Протокол, IP-адрес источ..., Порт ис..., IP-адрес получ..., Порт по..., and Направ... The events list includes several 'ET SCAN Suspicious inbound' alerts for various ports (3306, 1433, 1521, 5432) and two 'AM EXPLOIT Possible Google Chrome' alerts. The bottom status bar shows the time 14:04:34 on 18.09.2025 and the temperature 17°C.

У.	Дата и время	Код события	К.	Название правила	Протокол	IP-адрес источ...	Порт ис...	IP-адрес получ...	Порт по...	Направ...
1	12-18-00.640 18...	2010937	1	ET SCAN Suspicious inbound to MySQL port 3306	b. TCP	195.239.174.11	48255	10.10.1.24	3306	→
2	12-18-00.741 18...	3227018	1	ET SCAN Behavioral Unusually fast Terminal Server Tra...	n. TCP	195.239.174.11	48257	10.10.1.24	3389	→
3	12-18-00.741 18...	2010937	1	ET SCAN Suspicious inbound to MySQL port 3306	b. TCP	195.239.174.11	48257	10.10.1.24	3306	→
4	12-18-05.112 18...	2010935	1	ET SCAN Suspicious inbound to MSSQL port 1433	b. TCP	195.239.174.11	48255	10.10.1.24	1433	→
5	12-18-05.213 18...	2010935	1	ET SCAN Suspicious inbound to MSSQL port 1433	b. TCP	195.239.174.11	48257	10.10.1.24	1433	→
6	12-18-06.217 18...	2010936	1	ET SCAN Suspicious inbound to Oracle SQL port 1521	b. TCP	195.239.174.11	48255	10.10.1.24	1521	→
7	12-18-06.317 18...	2010936	1	ET SCAN Suspicious inbound to Oracle SQL port 1521	b. TCP	195.239.174.11	48257	10.10.1.24	1521	→
8	12-18-07.017 18...	2010939	1	ET SCAN Suspicious inbound to PostgreSQL port 5432	b. TCP	195.239.174.11	48255	10.10.1.24	5432	→
9	12-18-07.117 18...	2010939	1	ET SCAN Suspicious inbound to PostgreSQL port 5432	b. TCP	195.239.174.11	48257	10.10.1.24	5432	→
10	12-18-15.045 18...	3200655	1	AM EXPLOIT Possible Google Chrome < 97.0.4692.99 ...	c. TCP	10.10.2.15	80	10.10.4.10	53499	→
11	12-18-38.777 18...	3200655	1	AM EXPLOIT Possible Google Chrome < 97.0.4692.99 ...	c. TCP	10.10.2.15	80	10.10.4.10	53566	→
12	12-18-59.031 18...	3194701	1	ET POLICY Possible Web Crawl using Wget var1	a. TCP	195.239.174.11	49196	10.10.1.20	80	→

Figure 2: Детектирование SQL-инъекции

Загрузка вредоносного файла



События

События за последние 24 часа

У...	Дата и время	Код события	К	Название правила	Протокол	IP-адрес источ...	Порт ис...	IP-адрес получ...	Порт по...	Направл...
*	12-19-37.825 18...	3101541	1	AM EXPLOIT Generic Possible PHP Injection: PHP Tag in ...	w TCP	195.239.174.11	54662	10.10.1.20	80	→
*	12-19-37.830 18...	3114860	1	AM EXPLOIT Generic Command Injection in HTTP URI: 'ec...	w TCP	195.239.174.11	54660	10.10.1.20	80	→
*	12-19-37.830 18...	2010920	1	ET WEB_SERVER Exploit Suspected PHP Injection Attack ...	w TCP	195.239.174.11	54660	10.10.1.20	80	→
*	12-19-37.836 18...	2010920	1	ET WEB_SERVER Exploit Suspected PHP Injection Attack ...	w TCP	195.239.174.11	54684	10.10.1.20	80	→
*	12-19-37.836 18...	3114860	1	AM EXPLOIT Generic Command Injection in HTTP URI: 'ec...	w TCP	195.239.174.11	54684	10.10.1.20	80	→
*	12-19-37.836 18...	2009363	1	ET WEB_SERVER Suspicious Chmod Usage in URI (bboun...	a TCP	195.239.174.11	54684	10.10.1.20	80	→
*	12-19-37.886 18...	3121915	1	ET POLICY Executable and linking format (ELF) file downl...	p TCP	195.239.174.11	4444	10.10.1.20	43142	→
*	12-19-43.354 18...	2008538	6	ET SCAN Sqlmap SQL Injection Scan	a TCP	195.239.174.11		10.10.1.20	80	→
*	12-19-47.421 18...	3000709	2	AM SQL Generic: SQLi in HTTP URI: 'ORDER BY' query	w TCP	195.239.174.11		10.10.1.20	80	→
*	12-19-47.495 18...	3116422	1	AM SQL Generic: SQLi in HTTP URI: 'SELECT CONCAT' que...	w TCP	195.239.174.11		10.10.1.20	80	→
*	12-19-47.495 18...	3297187	1	AM SQL Generic: SQLi in HTTP URI: 'UNION SELECT' query...	w TCP	195.239.174.11		10.10.1.20	80	→
*	12-19-47.495 18...	3145513	1	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection ...	w TCP	195.239.174.11		10.10.1.20	80	→
*	12-19-47.495 18...	3004388	1	AM SQL Generic: SQLi in HTTP URI: 'UNION SELECT' query	w TCP	195.239.174.11		10.10.1.20	80	→

Страница 1

Показывать 300 объектов

14:06:08 18.09.2025

Figure 3: Загрузка вредоносного файла

Инцидент атака на веб сервер

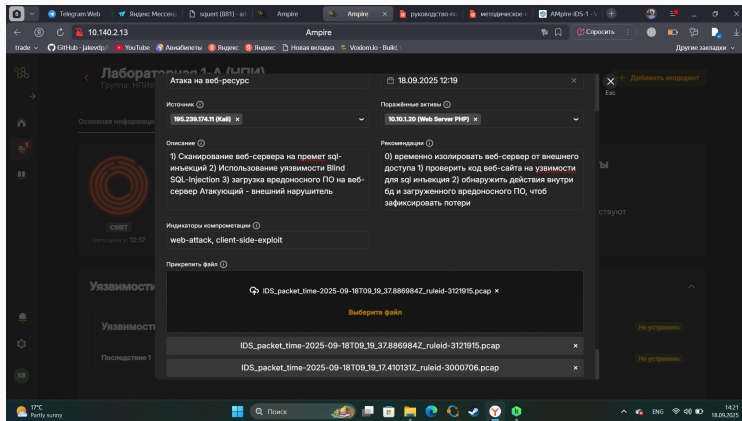


Figure 4: Инцидент атака на веб сервер

RDP Brute-force

The screenshot displays the AMpire-IDS-1 - ViPNet IDS NS web interface. The left sidebar contains navigation options: Мониторинг, Информанты, События, Отчеты, Управление, Сетевое окружение, Методы анализа, Правила анализа, Соповещение, Интеграция, Система, Сетевые настройки, Дата и время, Учетные записи, Резервное копирование, and Сервисные функции. The main content area is titled "События" and shows a table of events for the last 24 hours. The table has columns: У., Дата и время, Код события, К, Название правила, П, Протокол, and IP. The event at 12:22:01.454 18.09.2025 is highlighted. The right panel shows details for this event, including "Общая информация" (Date and time, Interface, Level, Type, Protocol, Code) and "Правило анализа" (Class, Group, Name, Description, Text).

У.	Дата и время	Код события	К	Название правила	П	Протокол	IP
12:19:53.855	18.09.2025	2008538	2	ET SCAN Sqlmap SQL Injection Scan	a	TCP	195
12:20:23.338	18.09.2025	3227008	1	ET SCAN Potential SSH Scan var1	a	TCP	195
12:21:52.373	18.09.2025	2001330	1	ET INFO RDP - Response To External Host	m	TCP	10
12:21:52.373	18.09.2025	2001330	1	ET INFO RDP - Response To External Host	m	TCP	10
12:21:52.605	18.09.2025	2001330	1	ET INFO RDP - Response To External Host	m	TCP	10
12:21:52.605	18.09.2025	2001330	1	ET INFO RDP - Response To External Host	m	TCP	10
12:22:01.454	18.09.2025	2012709	1	ET POLICY MS Remote Desktop Administrator Login Requ...	p	TCP	10
12:22:01.454	18.09.2025	2012709	1	ET POLICY MS Remote Desktop Administrator Login Requ...	p	TCP	10
12:22:01.454	18.09.2025	2012709	1	ET POLICY MS Remote Desktop Administrator Login Requ...	p	TCP	10
12:22:01.473	18.09.2025	2001330	1	ET INFO RDP - Response To External Host	m	TCP	10
12:22:01.473	18.09.2025	2001330	1	ET INFO RDP - Response To External Host	m	TCP	10

Событие 12:22:01.454 18.09.2025

Общая информация

Дата и время: 12:22:01.454 18.09.2025
Интерфейс заголовка: eth2
Уровень важности: Низкий
Тип события: Сигнатурное событие
Протокол: TCP
Код события: 2012709

Правило анализа

Класс: protocol-command-decode
Группа: policy
Название: ET POLICY MS Remote Desktop Administrator Login Request
Описание: Сигнатуры возможного нарушения политики информационной безопасности
Текст: ...

Figure 5: RDP Brute-force

Инцидент атака а хост, Brute-force

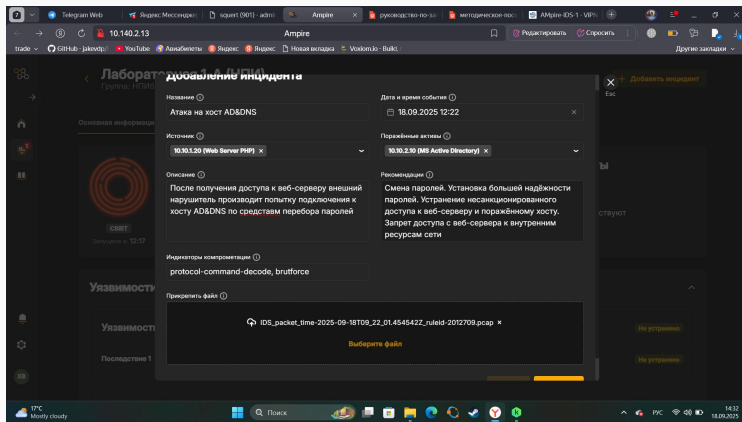


Figure 6: Инцидент атака а хост, Brute-force

Инцидент Атака на Administration WS

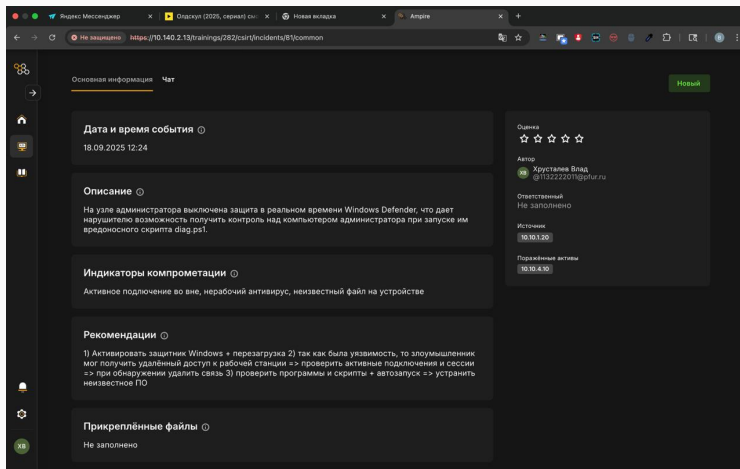


Figure 7: Инцидент Атака на Administration WS

PHP reverse shell

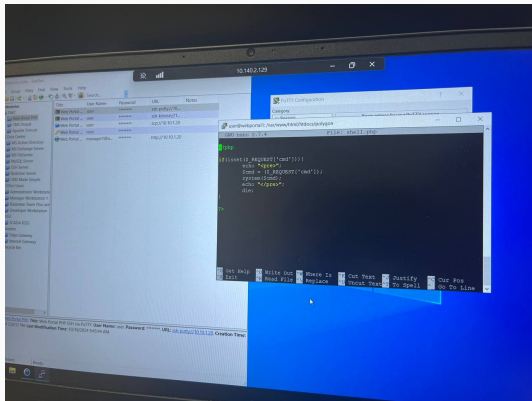


Figure 8: PHP reverse shell

Поиск места уязвимого параметра

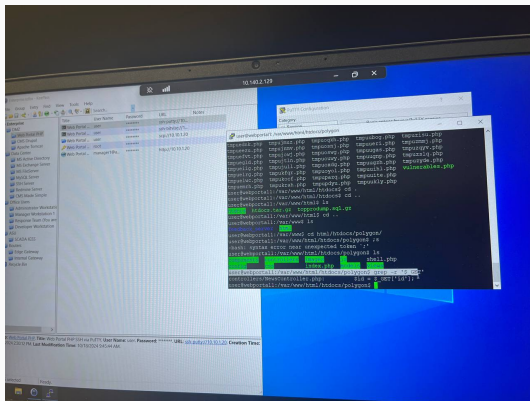


Figure 9: Поиск места уязвимого параметра

Измененная функция `actionView`

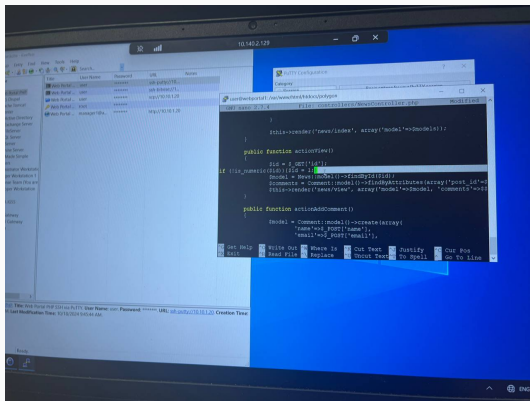


Figure 10: Измененная функция actionView

Удаление вредоносного файла

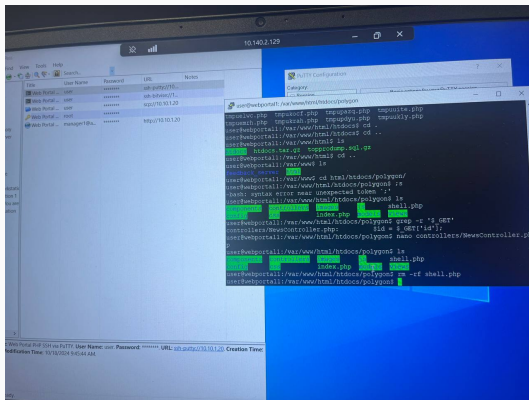


Figure 11: Удаление вредоносного файла

Список установленных соединений

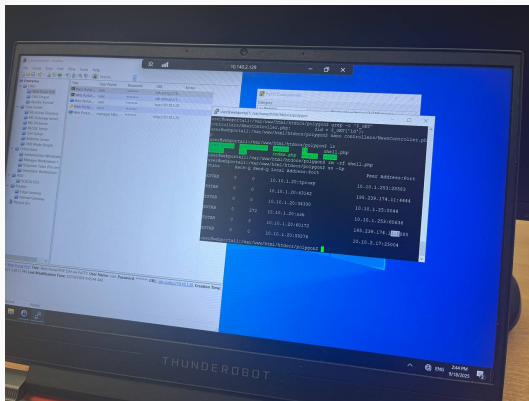


Figure 12: Список установленных соединений

Завершение сессий

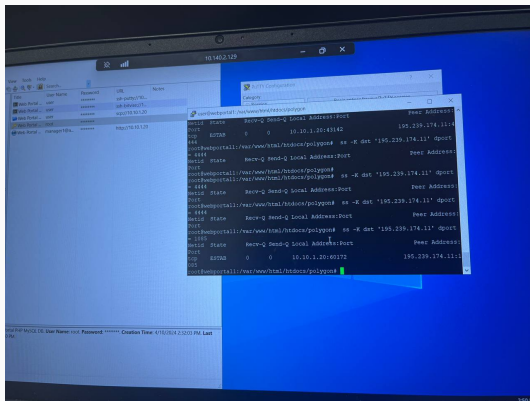


Figure 13: Завершение сессий

Удаление записи DisableAntiSpyware

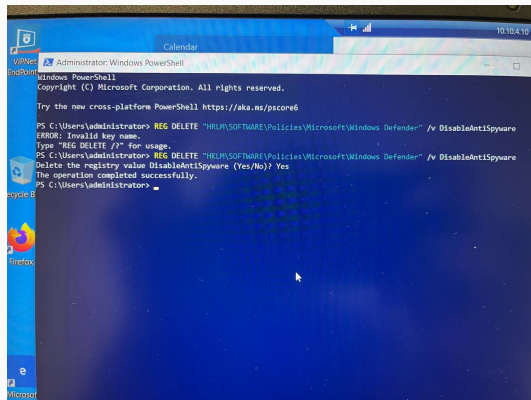


Figure 14: Удаление записи DisableAntiSpyware

Включение Real-time Protection

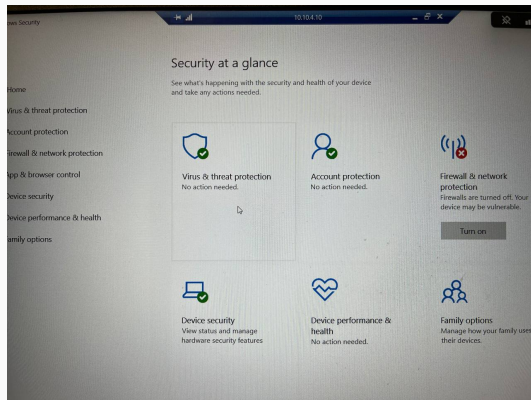


Figure 15: Включение Real-time Protection

Соединение с машиной нарушителя

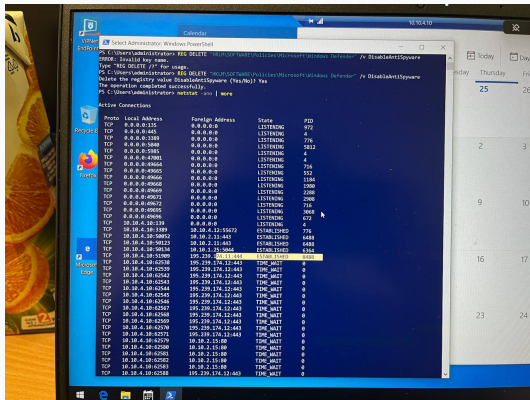


Figure 16: Соединение с машиной нарушителя

Остановка процесса

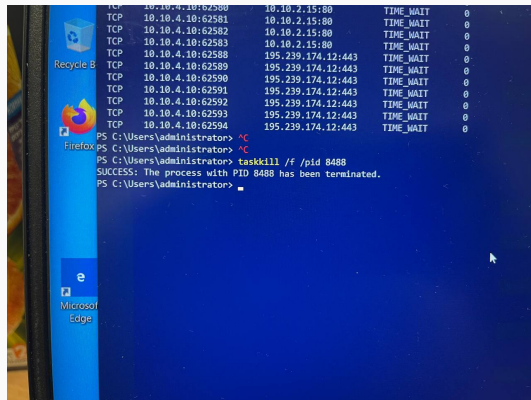


Figure 17: Остановка процесса

Логи подключений по RDP

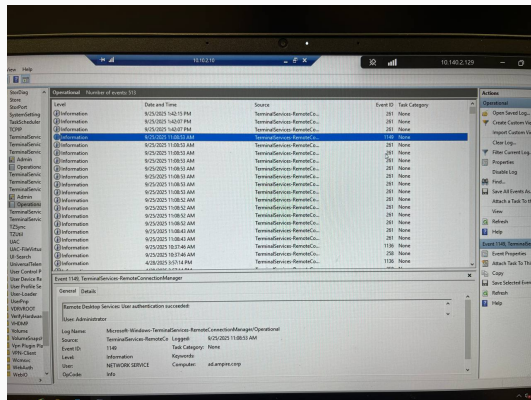


Figure 18: Логи подключений по RDP

Изменение пароля

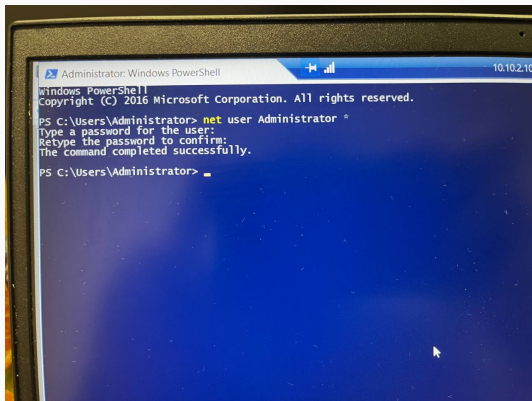


Figure 19: Изменение пароля

Лог добавления нового пользователя

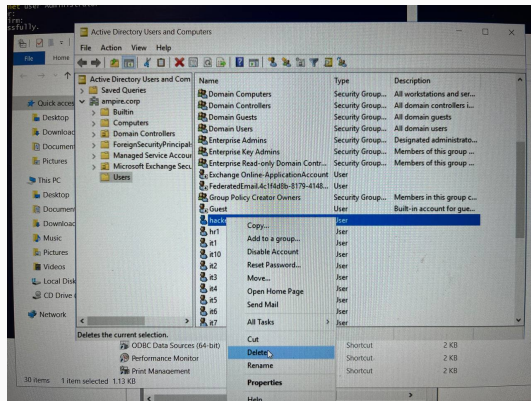


Figure 20: Лог добавления нового пользователя

Удаление пользователя

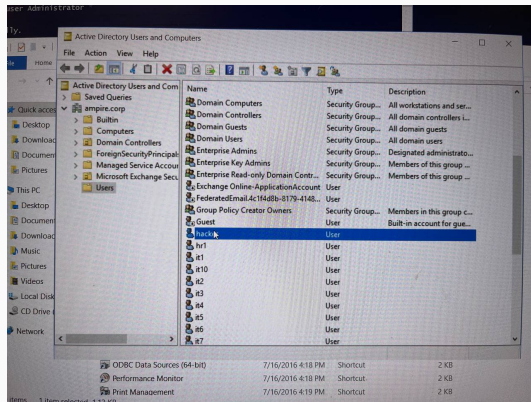


Figure 21: Удаление пользователя

Итоговый результат

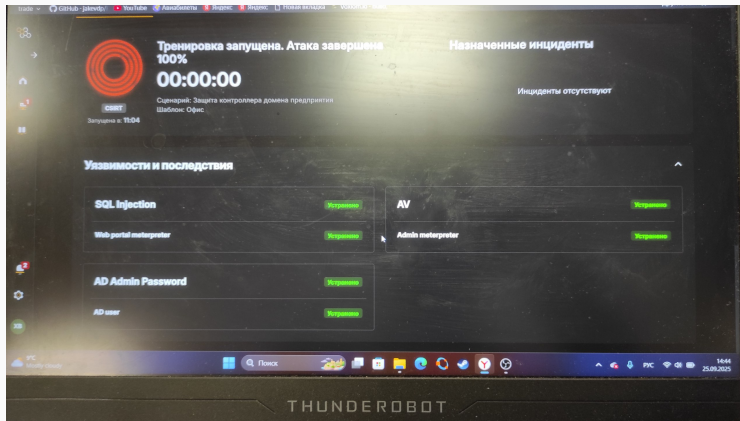


Figure 22: Итоговый результат

В рамках учебно-практического занятия на базе программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Аmpire» мы выполнили сценарий №2 «Защита контроллера домена предприятия».