Отчет по лабораторной работе №2-A «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

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 устранению 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. 1](#fig-001)), ([рис. 2](#fig-002)).

|  |
| --- |
| Рисунок 1: Сканирование на предмет SQL-инъекций |

|  |
| --- |
| Рисунок 2: Сканирование на предмет SQL-инъекций |

Видим использование определенного типа инъекции (Blind SQL-Injection) ([рис. 3](#fig-003)), а также загрузку вредоносного файла с php скриптом, что может указывать на использование php reverse shell и выставление права доступа на выполнение ([рис. 4](#fig-005)).

|  |
| --- |
| Рисунок 3: Детектирование SQL-инъекции |

|  |
| --- |
| Рисунок 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. 5](#fig-004)).

|  |
| --- |
| Рисунок 5: Пакет к событию |

Заполним карточку инцидента ([рис. 6](#fig-006)).

|  |
| --- |
| Рисунок 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. 7](#fig-007)). Увидим подозрительное соединение с внешним сервером.

|  |
| --- |
| Рисунок 7: Список установленных соединений |

Заполним карточку инцидента ([рис. 8](#fig-008)).

|  |
| --- |
| Рисунок 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. 9](#fig-010)). Мы ввели эту команду на узле администратора 10.10.4.10 и действительно получили, что отключение мониторинга с параметром True, значит, защита антивируса отключена.

|  |
| --- |
| Рисунок 9: Настройки Windows Defender |

Заполним карточку инцидента ([рис. 10](#fig-011)).

|  |
| --- |
| Рисунок 10: Карточка инцидента |

### 4.2.4 Обнаружение последствия “Admin meterpreter”

Установленную сессию с нарушителем обнаружили при помощи утилиты netstat с ключами –ano ([рис. 26](#fig-027)).

|  |
| --- |
| Рисунок 11: Соединение с машиной нарушителя |

Заполняем карточку инцидента ([рис. 12](#fig-035)).

|  |
| --- |
| Рисунок 12: Карточка инцидента |

### 4.2.5 Обнаружение уязвимости “Слабый пароль учетной записи”

С помощью ViPNet IDS NS в сетевом трафике обнаруживаются множественные попытки подключения к хосту AD&DNS с портом 3389 ([рис. 13](#fig-013)), сканирование системы, что может говорить о попытках подбора пароля([рис. 14](#fig-015)). Также если мы зайдем на сам узел Active Directory, откроем Viewer Properties, перейдем в необходимую директорию с событиями (TerminalServeces…), 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 |

Заполняем карточку инцидента ([рис. 15](#fig-016)).

|  |
| --- |
| Рисунок 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. 16](#fig-017)). Альтернативный способ обнаружения этого последствия - непосредственно зайти в Active Directory Users and Computers, где мы увидим странного нового пользователя ([рис. 17](#fig-018)), ([рис. 18](#fig-019)).

|  |
| --- |
| Рисунок 16: Переход в отслеживание событий |

|  |
| --- |
| Рисунок 17: Нахождение hacker в AD User & Computers |

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

Заполняем карточку инцидента ([рис. 19](#fig-020))

|  |
| --- |
| Рисунок 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. 20](#fig-024)).

|  |
| --- |
| Рисунок 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. 21](#fig-025)).

|  |
| --- |
| Рисунок 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 ssс 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. 22](#fig-026)).

|  |
| --- |
| Рисунок 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. 23](#fig-029)): REG DELETE "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware. Подтвердили действие, далее в Windows Defender перезапустили Virus & Threat Protection ([рис. 24](#fig-030)) и включили Real-time Protection ([рис. 25](#fig-031))

|  |
| --- |
| Рисунок 23: Удаление записи DisableAntiSpyware в реестре |

|  |
| --- |
| Рисунок 24: Интерфейс Windows Defender |

|  |
| --- |
| Рисунок 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. 26](#fig-027)).

|  |
| --- |
| Рисунок 26: Соединение с машиной нарушителя |

Для устранения завершили сессию с машиной нарушителя при помощи команды taskkill /f /pid ([рис. 27](#fig-028)).

|  |
| --- |
| Рисунок 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. 28](#fig-033)), на узле MS Active Directory.

|  |
| --- |
| Рисунок 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 найшли и удалилинового привилегированного пользователя с именем «Hacked» ([рис. 29](#fig-034)).

|  |
| --- |
| Рисунок 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. 30](#fig-022)) ([рис. 31](#fig-023)).

|  |
| --- |
| Рисунок 30: Выполненные карточки |

|  |
| --- |
| Рисунок 31: Закрытые уязвимости и последствия |

# Список литературы

1. CVE-2019-18890 POC (Proof of Concept) [Электронный ресурс].

2. Redmine [Электронный ресурс].

3. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атака "Ampire". Сценарий №2 «ЗАЩИТА КОНТРОЛЛЕРА ДОМЕНА ПРЕДПРИЯТИЯ» [Электронный ресурс]. O’Reilly Media. 24 с.