

Отчёт по лабораторной работе 1-С (НФИ-2)

**Программный комплекс обучения методам обнаружения,
анализа и устранения последствий компьютерных атак
«Ampire»**

Козлов В.П., Гаинэ А., Шуваев С., Джахангиров И.З, Хватов М.Г.

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	15
5	Список литературы	16

Список иллюстраций

3.1	Установка Chocolatey	7
3.2	Атакованные ip-адреса	8
3.3	Карточка инцидента Weak Password	8
3.4	Карточка инцидента XSS	9
3.5	Карточка инцидента SQL-injection	9
3.6	Файл redcloth3.rb атакованного ip-адреса	10
3.7	Удаление тега	10
3.8	Перезапуск службы веб-сервера	11
3.9	Удаление пользователя hacker	11
3.10	Файл query.rb	12
3.11	Редактирование query.rb	12
3.12	Перезапуск nginx	13
3.13	MS Active Directory	13
3.14	Сброс пароля	14
3.15	Удаление Evil Task	14

Список таблиц

1 Цель работы

Отработка на практике методов обнаружения, анализа и нейтрализации многоэтапной компьютерной атаки, направленной на кражу научно-технической информации предприятия, с использованием учебного программного комплекса «Ampire».

2 Задание

1. Обнаружить подбор пароля к файловому серверу и последующую загрузку вредоносного файла.
2. Выявить бэкдор на рабочей станции через анализ планировщика задач и запущенных процессов.
3. Зафиксировать кражу учётных данных (например, с помощью утилиты LaZagne) и их использование для доступа к Redmine.
4. Проанализировать XSS-атаку в Redmine, которая привела к включению REST API и созданию привилегированного пользователя.
5. Обнаружить слепую SQL-инъекцию, используемую для извлечения конфиденциальных данных из базы данных.
6. Нейтрализовать последствия атаки: удалить бэкдор, несанкционированного пользователя и внедрённый вредоносный код.
7. Устранить уязвимости: пропатчить Redmine от XSS (CVE-2019-17427) и SQL-инъекции (CVE-2019-18890), усилить политику паролей.

3 Выполнение лабораторной работы

Активировали WireGuard и зашли на сайт платформы (рис. 3.1)

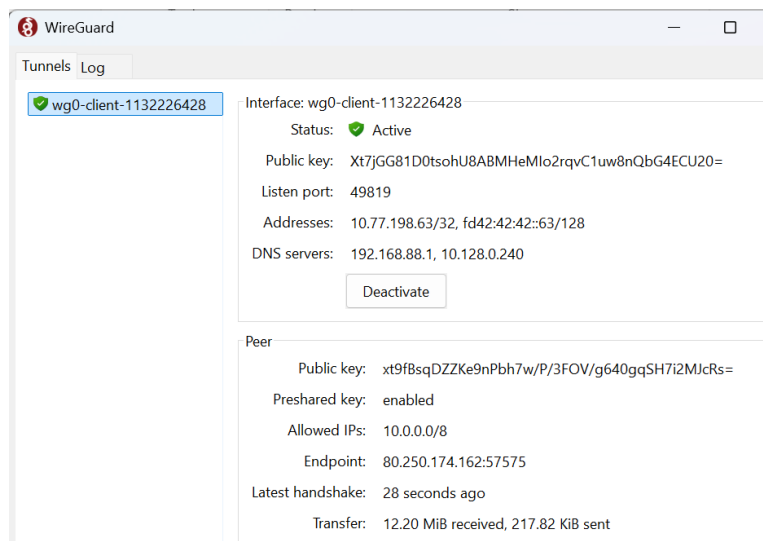


Рис. 3.1: Установка Chocolatey

На сайте ViPNet IDS NS просмотрели атакованные ip-адреса и суть атак (рис. 3.2)

S...	Date and ti...	P	Event co...	Q...	Class	P	Rule name	S...	Destination ...	S	Destination ...
15:08:38.560	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	61205	
15:08:05.958	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	61115	
15:07:42.069	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	61037	
15:07:08.903	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	60952	
15:06:44.220	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	60880	
15:06:17.782	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	60805	
15:05:45.330	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	60719	
15:05:20.909	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	60645	
15:04:48.340	...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	8	60561	

Рис. 3.2: Атакованные ip-адреса

Добавили карточку инцидента Weak Password (рис. 3.3)

Добавление инцидента

Название ⓘ: Weak user password

Дата и время события ⓘ: 28.09.2025 09:02

Источник ⓘ: 10.10.4.13 (Developer) ✕

Поражённые активы ⓘ: 10.10.4.11 (Manager Workstation 1) ✕

Описание ⓘ: Слабый пароль

Рекомендации ⓘ: Поменять пароль, удалить evil task

Индикаторы компрометации ⓘ: trojan-activity с 10.10.4.13 на 10.10.4

Рис. 3.3: Карточка инцидента Weak Password

Добавили карточку инцидента XSS (рис. 3.4)

Источник 10.10.2.254 x	Поражённые активы 10.10.2.15 (Redmine Server) x
Описание Вредоносный JavaScript-код был постоянно размещен на Wiki-странице проекта в Redmine. Когда администратор открывал эту страницу, код автоматически	Рекомендации Отредактировать файл redcloth3.rb
Индикаторы компрометации Ничего не введено	
Прикрепить файл xss_attack.pcap x	

Рис. 3.4: Карточка инцидента XSS

Добавили карточку инцидента SQL-injection (рис. 3.5)

Описание времени ответа (Time-based) или разному поведению приложения (Boolean-based). В сценарии использовалась Time-based атака с SLEEP()	Рекомендации Проверить обработку параметров subproject_id в query.rb
Индикаторы компрометации HTTP-запросы с SLEEP(), BENCHM	
Прикрепить файл sql_injection.pcap x Выберите файл	

Рис. 3.5: Карточка инцидента SQL-injection

Атака XSS. Открыли на редактирование файл redcloth3.rb атакованного ip-адреса (рис. 3.6)

```

user@redmine: /var/www/redmine/lib
$ Using username "user".
Last login: Wed Mar 12 13:14:21 2025
user@redmine:~$
user@redmine:~$ ls
NUL  sc5_blind_sql_i_chk.py
user@redmine:~$ cd /var
-bash: cd: /var: No such file or directory
user@redmine:~$ cd /var
user@redmine:/var$ cd /www
-bash: cd: /www: No such file or directory
user@redmine:/var$ cd /var/www/redmine/
user@redmine:/var/www/redmine$ ls
CONTRIBUTING.md  Rakefile      config      extra      plugins      logs
Gemfile           app           config.ru   fixtures   public        vendor
Gemfile.lock      appveyor.yml  db          lib        script
README.rdoc       bin           doc         lib        test
user@redmine:/var/www/redmine$ cd /var/www/redmine/lib
user@redmine:/var/www/redmine/lib$ ls
SVG  diff.rb  generators  plugins  redcloth3.rb  redmine  redmine.rb  tasks
user@redmine:/var/www/redmine/lib$ nano redcloth3.rb

```

Рис. 3.6: Файл redcloth3.rb атакованного ip-адреса

Атака XSS. Удалили тег pre из разрешенных тегов, которые не будут экранированы (рис. 3.7)

```

GNU nano 2.5.3      File: redcloth3.rb      Modified
1  " <#{raw[i]}#{pcs.join " "}>"
2  else
3  " "
4  end
5  end
6  end
7  end
8
9  ALLOWED_TAGS = %w(redpre code kbd notextile)
10 def escape_html_tags(text)
11   text.gsub!(/%<(\w+)?([!@#$%^&*~`'"/\:\;]+)?>/) { |m| ALLOWED_TAGS.include?($2) ?
12   }
13 end
14
15
16
File Name to Write: redcloth3.rb

```

Рис. 3.7: Удаление тега

Атака XSS. Перезапустили службу веб-сервера: `sudo systemctl restart nginx.service` (рис. 3.8)

```

user@redmine: /var/www/redmine/lib
GNU nano 2.5.3 File: redcloth3.rb Modified
    "<#{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 : "<\/?([!\\w]+)[^>\n]*(>?)>" }
end
end
I

```

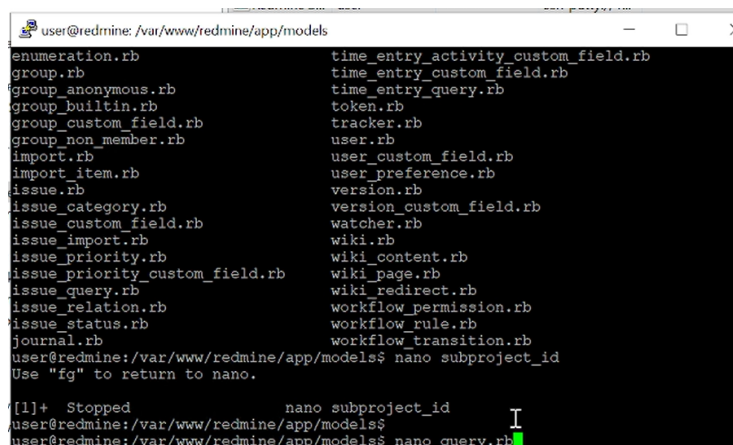
Рис. 3.8: Перезапуск службы веб-сервера

Последствия XSS. Удалили пользователя hacker (рис. 3.9)

Login	First name	Last name	Email	Administrator	Created	Last connection	
admin	Redmine	Admin	admin@example.net	✓	02/13/2020 02:10 PM	09/28/2025 04:11 PM	
DEV1	John	Doe	dev1@ampire.corp	✓	02/17/2020 08:18 AM	09/28/2025 04:11 PM	Lock Delete
DEV2	Jane	Dow	janedow@ampire.corp	✓	02/19/2020 12:31 PM	09/28/2025 04:11 PM	Lock Delete
hacker	hacker	hacker	hacker@hacker.ru	✓	09/28/2025 09:03 AM		Lock Delete

Рис. 3.9: Удаление пользователя hacker

Атака SQL-инъекция. Открыли файл query.rb на редактирование на 10.10.2.15 (рис. 3.10)

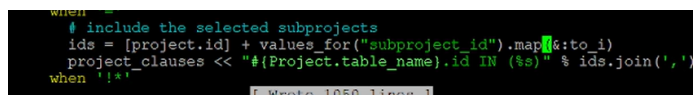


```
user@redmine: /var/www/redmine/app/models
enumeration.rb      time_entry_activity_custom_field.rb
group.rb            time_entry_custom_field.rb
group_anonymous.rb  time_entry_query.rb
group_builtin.rb    token.rb
group_custom_field.rb tracker.rb
group_non_member.rb user.rb
import.rb           user_custom_field.rb
import_item.rb      user_preference.rb
issue.rb            version.rb
issue_category.rb   version_custom_field.rb
issue_custom_field.rb watcher.rb
issue_import.rb     wiki.rb
issue_priority.rb   wiki_content.rb
issue_priority_custom_field.rb wiki_page.rb
issue_query.rb      wiki_redirect.rb
issue_relation.rb   workflow_permission.rb
issue_status.rb     workflow_rule.rb
journal.rb          workflow_transition.rb
user@redmine:/var/www/redmine/app/models$ nano subproject_id
Use "fg" to return to nano.

[1]+  Stopped                  nano subproject_id
user@redmine:/var/www/redmine/app/models$
user@redmine:/var/www/redmine/app/models$ nano query.rb
```

Рис. 3.10: Файл query.rb

Атака SQL-инъекция. Отредактировали query.rb, заменив each на map (рис. 3.11)



```
when '*'
  # include the selected subprojects
  ids = [project.id] + values_for("subproject_id").map{|&:to_i}
  project_clauses << "#{Project.table_name}.id IN (%s)" % ids.join(',')
when '*'
  [ Wrote 1050 lines ]
```

Рис. 3.11: Редактирование query.rb

Атака SQL-инъекция. Перезапустили nginx (рис. 3.12)

```

user@redmine:/var/www/redmine/app/models$ sudo systemctl restart nginx.service
[sudo] password for user:
user@redmine:/var/www/redmine/app/models$
user@redmine:/var/www/redmine/app/models$ sudo systemctl restart nginx.service
user@redmine:/var/www/redmine/app/models$

```

Рис. 3.12: Перезапуск nginx

Атака Weak Password. Зашли на MS Active Directory (рис. 3.13)

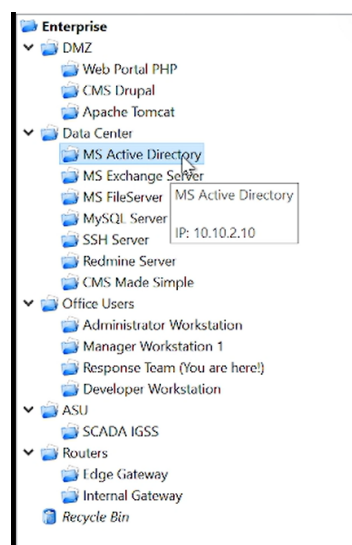


Рис. 3.13: MS Active Directory

Атака Weak Password. Сбросили пароль на dev1 (рис. 3.14)

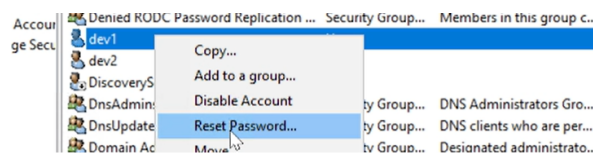


Рис. 3.14: Сброс пароля

Последствие Weak Password. Удалили Evil Task из планировщика задач (рис. 3.15)

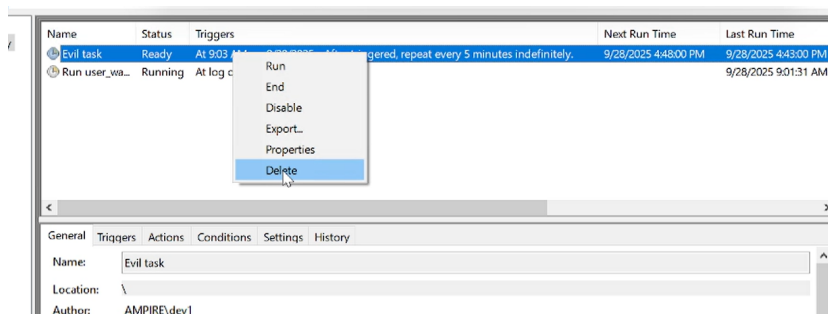


Рис. 3.15: Удаление Evil Task

Все атаки и их последствия успешно устранены

4 Выводы

Отработали на практике методы обнаружения, анализа и нейтрализации многоэтапной компьютерной атаки, направленной на кражу научно-технической информации предприятия, с использованием учебного программного комплекса «Ampire».

5 Список литературы

1. **CVE-2019-0630** — Common Vulnerabilities and Exposures.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0630>
2. **CVE-2019-17427** — Уязвимость XSS в Redmine.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17427>
3. **CVE-2019-18890** — Уязвимость Blind SQL-инъекции в Redmine.
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18890>