

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

Julia. Установка и настройка. Основные принципы.

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

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

- Козлов В.П., Гаинэ А., Шуваев С., Джахангиров И.З, Хватов М.Г.
- НФИбд-02-22
- Российский университет дружбы народов

Выполнение лабораторной 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».

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.

Активировали WireGuard и зашли на сайт платформы

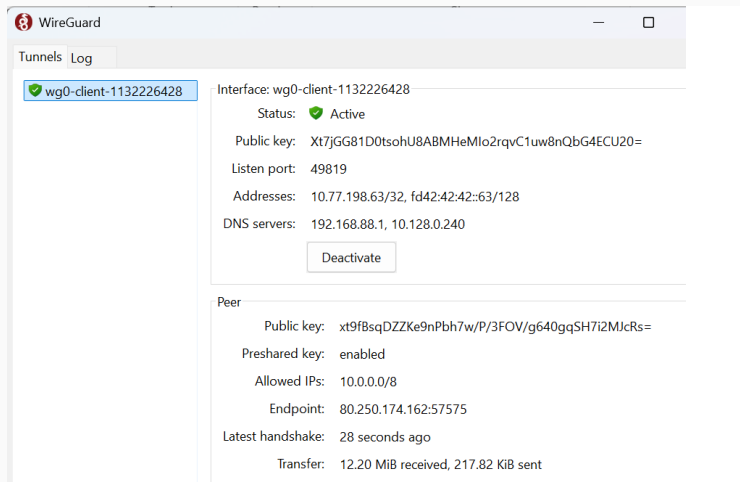
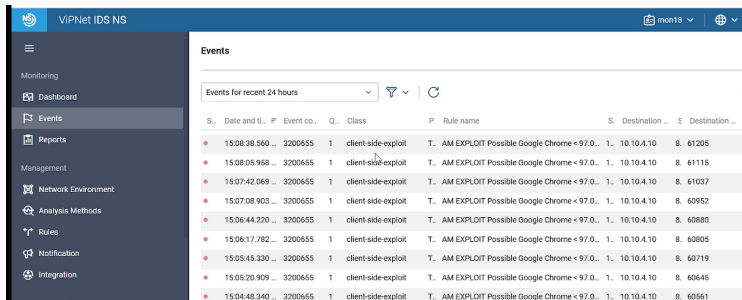


Figure 1: Установка Chocolatey

На сайте ViPNet IDS NS просмотрели атакованные ip-адреса и суть атак



The screenshot displays the ViPNet IDS NS web interface. On the left is a dark sidebar with a menu containing 'Monitoring' (with sub-items 'Dashboard' and 'Events') and 'Management' (with sub-items 'Network Environment', 'Analysis Methods', 'Rules', 'Notification', and 'Integration'). The main area is titled 'Events' and shows a table of recent security incidents. A filter dropdown is set to 'Events for recent 24 hours'. The table lists events with columns for source IP, date, event count, class, priority, rule name, and destination IP. All listed events are 'client-side-exploit' attacks detected by rule 'AM EXPLOIT Possible Google Chrome < 97.0...'. The source IPs are all 10.10.4.10, and the destination IPs range from 61205 to 60561.

S...	Date and ti...	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	B.	61205
•	15:08:05.958 ...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	B.	61115
•	15:07:42.069 ...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	B.	61037
•	15:07:08.903 ...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	B.	60952
•	15:06:44.220 ...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	B.	60880
•	15:06:17.782 ...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	B.	60805
•	15:05:45.330 ...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	B.	60719
•	15:05:20.909 ...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	B.	60645
•	15:04:48.340 ...	3200655	1	client-side-exploit	T...	AM EXPLOIT Possible Google Chrome < 97.0...	1...	10.10.4.10	B.	60561

Figure 2: Атакованные ip-адреса

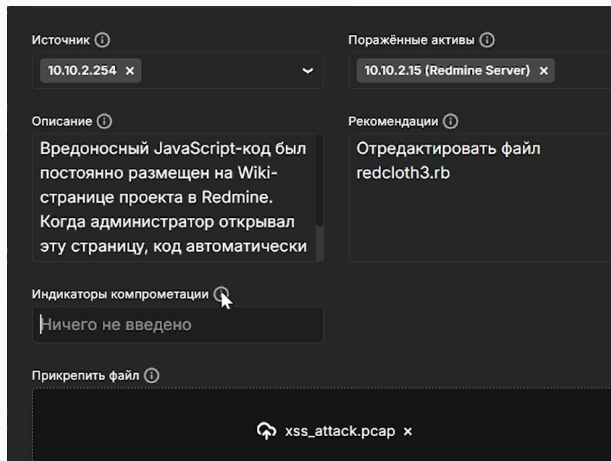
Добавили карточку инцидента Weak Password

Добавление инцидента

Название ⓘ	Дата и время события ⓘ
Weak user password	28.09.2025 09:02
Источник ⓘ	Поражённые активы ⓘ
10.10.4.13 (Developer) x	10.10.4.11 (Manager Workstation 1) x
Описание ⓘ	Рекомендации ⓘ
Слабый пароль	Поменять пароль, удалить evil task
Индикаторы компрометации ⓘ	
trojan-activity с 10.10.4.13 на 10.10.4.	

Figure 3: Карточка инцидента Weak Password

Добавили карточку инцидента XSS



The image shows a dark-themed user interface for an incident response system. It features a grid of four panels. The top-left panel, titled 'Источник' (Source), contains a dropdown menu with the value '10.10.2.254'. The top-right panel, titled 'Поражённые активы' (Affected assets), contains a dropdown menu with the value '10.10.2.15 (Redmine Server)'. The bottom-left panel, titled 'Описание' (Description), contains a text area with the text: 'Вредоносный JavaScript-код был постоянно размещен на Wiki-странице проекта в Redmine. Когда администратор открывал эту страницу, код автоматически'. The bottom-right panel, titled 'Рекомендации' (Recommendations), contains a text area with the text: 'Отредактировать файл redcloth3.rb'. Below these panels is a section titled 'Индикаторы компрометации' (Compromise indicators) with a text input field containing 'Ничего не введено'. At the bottom is a section titled 'Прикрепить файл' (Attach file) with a file upload button and a list of attached files, including 'xss_attack.pcap'.

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

Figure 4: Карточка инцидента XSS

Добавили карточку инцидента SQL-injection

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

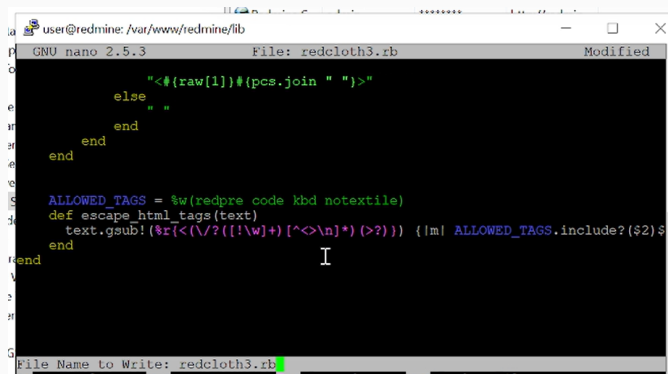
Figure 5: Добавили карточку инцидента SQL-injection

Атака XSS. Открыли на редактирование файл redcloth3.rb атакованного ip-адреса

```
user@redmine: /var/www/redmine/lib
Using username "user".
Last login: Wed Mar 12 13:14:21 2025
user@redmine:~$
user@redmine:~$
user@redmine:~$ ls
NUL  sc5_blind_sqli_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  tmp
Gemfile          app           config.ru   files  public   vendor
Gemfile.lock     appveyor.yml  db          lib    script
README.rdoc      bin           doc         log    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
I
```

Figure 6: Файл redcloth3.rb атакованного ip-адреса

Атака XSS. Удалили тег pre из разрешенных тегов, которые не будут экранированы

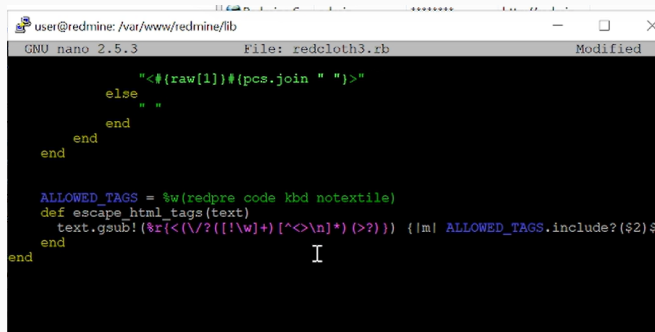


```
user@redmine: /var/www/redmine/lib
GNU nano 2.5.3 File: redcloth3.rb Modified
    "<#{raw[1]}#{pcs.join " ">"
  else
    " "
  end
end
end
end

ALLOWED_TAGS = %w(redpre code kbd notextile)
def escape_html_tags(text)
  text.gsub!(/%r{<(<\/?([!\\w]+) [^<>\n]*)(>?)}) { |m| ALLOWED_TAGS.include?($2)$
end
end
```

Figure 7: Удаление тега

Атака XSS. Перезапустили службу веб-сервера: `sudo systemctl restart nginx.service`



```
user@redmine: /var/www/redmine/lib
GNU nano 2.5.3      File: redcloth3.rb      Modified

    "<#{raw[1]}#{pcs.join " ">"
  else
    " "
  end
end
end

ALLOWED_TAGS = %w(redpre code kbd notextile)
def escape_html_tags(text)
  text.gsub!(/<\/?([!w]+)[^<>\n]*(>?)) { |m| ALLOWED_TAGS.include?($2)$
end
end
```

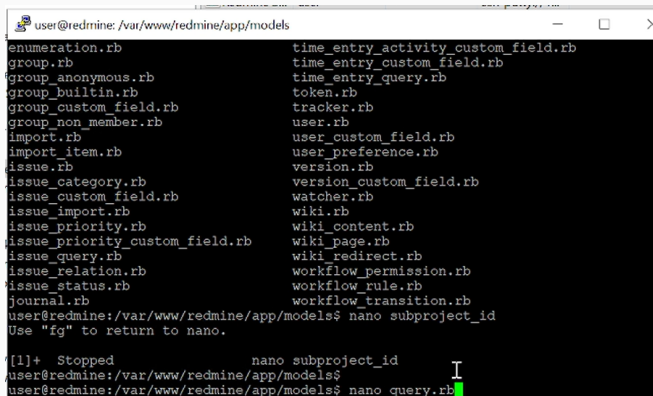
Figure 8: Перезапуск службы веб-сервера

Последствия XSS. Удалили пользователя hacker

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

Figure 9: Удаление пользователя hacker

Атака SQL-инъекция. Открыли файл query.rb на редактирование на 10.10.2.15

A terminal window with a title bar showing 'user@redmine: /var/www/redmine/app/models'. The terminal displays a two-column list of files in the directory. The files include enumeration.rb, group.rb, group_anonymous.rb, group_builtin.rb, group_custom_field.rb, group_non_member.rb, import.rb, import_item.rb, issue.rb, issue_category.rb, issue_custom_field.rb, issue_import.rb, issue_priority.rb, issue_priority_custom_field.rb, issue_query.rb, issue_relation.rb, issue_status.rb, journal.rb, time_entry_activity_custom_field.rb, time_entry_custom_field.rb, time_entry_query.rb, token.rb, tracker.rb, user.rb, user_custom_field.rb, user_preference.rb, version.rb, version_custom_field.rb, watcher.rb, wiki.rb, wiki_content.rb, wiki_page.rb, wiki_redirect.rb, workflow_permission.rb, workflow_rule.rb, and workflow_transition.rb. Below the list, the prompt 'user@redmine:/var/www/redmine/app/models\$' is followed by the command 'nano subproject_id'. The next line shows '[1]+ Stopped nano subproject_id'. The prompt is then followed by 'nano query.rb', where a green cursor is visible at the end of the line.

```
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
```

Figure 10: Файл query.rb

Атака SQL-инъекция. Отредактировали query.rb, заменив each на map

```
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 ]
```

Figure 11: Редактирование query.rb

Атака SQL-инъекция. Перезапустили nginx

```
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$
```

Figure 12: Перезапуск nginx

Атака Weak Password. Зашли на MS Active Directory

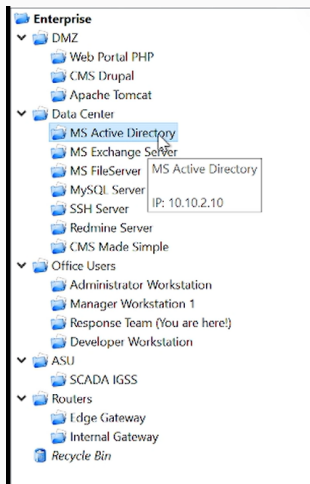


Figure 13: MS Active Directory

Атака Weak Password. Сбросили пароль на dev1

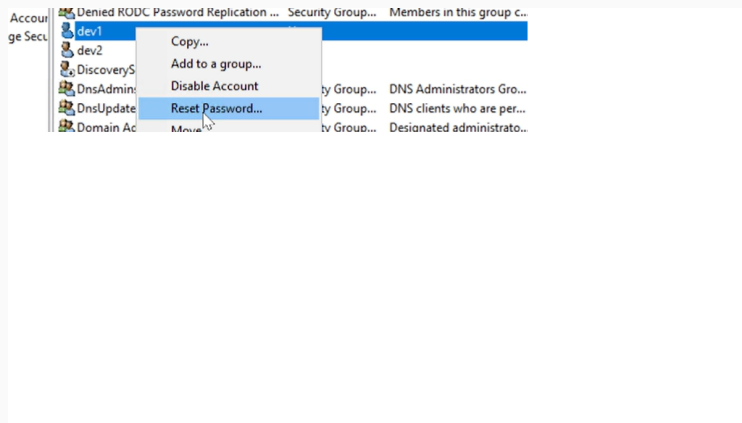


Figure 14: Сброс пароля

Последствие Weak Password. Удалили Evil Task из планировщика задач

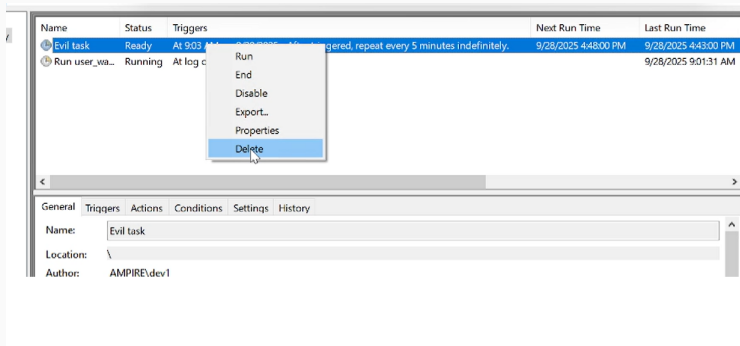


Figure 15: Удаление Evil Task

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