



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

МАТЕРИАЛЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Технологии хранения в системах кибербезопасности

| | |
|--|---|
| | <i>(наименование дисциплины (модуля) в соответствии с учебным планом)</i> |
| Уровень | специалитет |
| | <i>(бакалавриат, магистратура, специалитет)</i> |
| Форма обучения | очная |
| | <i>(очная, очно-заочная, заочная)</i> |
| Направление(-я) подготовки | 10.05.04 Информационно-аналитические системы безопасности |
| | <i>(код(-ы) и наименование(-я))</i> |
| Институт | Кибербезопасности и цифровых технологий (ИКБ) |
| | <i>(полное и краткое наименование)</i> |
| Кафедра | КБ-2 «Прикладные информационные технологии» |
| | <i>(полное и краткое наименование кафедры, реализующей дисциплину (модуль))</i> |
| Лектор | к.т.н., Селин Андрей Александрович, Бугаев Александр Александрович |
| | <i>(сокращенно – ученая степень, ученое звание; полностью – ФИО)</i> |
| Используются в данной редакции с учебного года | 2024/2025 |
| | <i>(учебный год цифрами)</i> |
| Проверено и согласовано « ____ » _____ 2024 г. | А.А. Бакаев |
| | <i>(подпись директора Института/Филиала с расшифровкой)</i> |

Москва 2024 г.

ПРАКТИЧЕСКАЯ РАБОТА № 4

«Знакомство с инструментами для работы с частично структурированными данными на примере документо-ориентированной СУБД MongoDB»

Цель работы – получение практических навыков работы с MongoDB.

Задание:

1. Запустите Unix-подобную систему (например, Debian 12.6.0 64-bit¹).
2. Создайте пользователя с именем формата **fio_nn**,
где **f** – первая буква фамилии на латинице;
i – первая буква имени на латинице;
o – первая буква отчества на латинице (при наличии),
nn – двузначный номер по списку в группе.

Добавьте его в группу `sudo`. **Все дальнейшие действия необходимо выполнять от имени созданного пользователя.**

3. Запустите терминал и установите Docker и Docker Compose.
4. Разверните MongoDB и Mongo Express с помощью Docker Compose.

Требования к запускаемым сервисам:

- последние 2 цифры номера порта, на котором будет развернут сервис, должны соответствовать номеру по списку в группе (например, для 3 – 12303, 8003, 9903 и т.п.);
- имя контейнера должно заканчиваться на символ подчеркивания и инициалы ФИО (например, для Иванова Петра Дмитриевича – `mongo_ipd`, `mongo-express_ipd`).

5. Создайте в MongoDB базу данных с именем в формате **fio_nn** (см. п. 2).
6. Создайте коллекцию с именем **test_nn**, где **nn** – номер по списку.

¹ Можно скачать готовый образ виртуальной машины по ссылке
<https://sourceforge.net/projects/osboxes/files/v/vb/14-D-b/12.6.0/64bit.7z/download>

7. Зайдите в контейнер MongoDB с помощью команды **docker exec**:

sudo docker exec -it mongo_ipd bash

Выйти из контейнера можно с помощью команды **exit**.

8. Запустите консоль MongoDB (/bin/mongosh) со своими параметрами:

mongosh --host localhost --port 27017 -u root -p password

Выйти из консоли можно с помощью команды **exit**.

9. Подключитесь к ранее созданной БД. Пример:

use ipd_07

10. Проверьте, что все корректно работает. Например, командой **db.stats()**:

```
test> use ipd_07
switched to db ipd_07
ipd_07> db.stats()
{
  db: 'ipd_07',
  collections: Long('2'),
  views: Long('0'),
  objects: Long('0'),
  avgObjSize: 0,
  dataSize: 0,
  storageSize: 8192,
  indexes: Long('2'),
  indexSize: 8192,
  totalSize: 16384,
  scaleFactor: Long('1'),
  fsUsedSize: 62231244800,
  fsTotalSize: 1081101176832,
  ok: 1
}
ipd_07> |
```

11. Изучите основные команды и потренируйтесь в их выполнении:

- добавление одного документа;
- добавление нескольких документов;
- удаление и обновление документов;
- поиск по документам;
- пагинация и сортировка документов;
- получение количества документов и другие.

Примеры можно посмотреть по ссылке: <https://metanit.com/nosql/mongodb>.

12. Изучите матрицу MITRE ATT&CK (описывает тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру):

- <https://attack.mitre.org> (официальный адрес);
- <https://mitre.ptsecurity.com/ru-RU> (версия на русском языке от компании Positive Technologies).

The screenshot shows the MITRE ATT&CK web interface. The top navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and a Blog. Below the navigation bar, there are filters for layout (side), showing sub-techniques, and hiding sub-techniques. The main content area displays the 'Enterprise' matrix, which is a grid of techniques categorized by tactics. The tactics listed are Reconnaissance (10 techniques), Resource Development (8 techniques), Initial Access (10 techniques), Execution (14 techniques), Persistence (20 techniques), Privilege Escalation (14 techniques), Defense Evasion (43 techniques), and Credential Access (17 techniques). Each tactic is represented by a box containing a list of techniques with their IDs and names. For example, under Reconnaissance, techniques include Active Scanning (3), Gather Victim Host Information (4), Gather Victim Identity Information (3), Gather Victim Network Information (6), Gather Victim Org Information (4), Phishing for Information (4), and Search Closed. Under Resource Development, techniques include Acquire Access, Acquire Infrastructure (8), Compromise Accounts (3), Compromise Infrastructure (8), Develop Capabilities (4), Establish Accounts (3), Obtain Capabilities (7), and Search Closed. Under Initial Access, techniques include Content Injection, Drive-by Compromise, Exploit Public-Facing Application, External Remote Services, Hardware Additions, and Phishing (4). Under Execution, techniques include Cloud Administration Command, Command and Scripting Interpreter (10), Container Administration Command, Deploy Container, Exploitation for Client Execution, and Inter-Process Communication (3). Under Persistence, techniques include Account Manipulation (6), BITS Jobs, Boot or Logon Autostart Execution (14), Boot or Logon Initialization Scripts (5), Browser Extensions, and Compromise Host Software Binary. Under Privilege Escalation, techniques include Abuse Elevation Control Mechanism (6), Access Token Manipulation (5), Account Manipulation (6), Boot or Logon Autostart Execution (14), Boot or Logon Initialization Scripts (5), and Direct Volume Access. Under Defense Evasion, techniques include Abuse Elevation Control Mechanism (6), Access Token Manipulation (5), BITS Jobs, Build Image on Host, Debugger Evasion, Deobfuscate/Decode Files or Information, Deploy Container, and Direct Volume Access. Under Credential Access, techniques include Adversary-In-the-Middle (3), Brute Force (4), Credentials from Password Stores (6), Exploitation for Credential Access, Forced Authentication, and Forge Web Credentials (2).

The screenshot shows a detailed view of the MITRE ATT&CK matrix, organized into six columns: Разведка (Reconnaissance), Подготовка ресурсов (Resource Development), Первоначальный доступ (Initial Access), Выполнение (Execution), Закрепление (Persistence), and Повышение привилегий (Privilege Escalation). Each column contains a list of techniques with their IDs and names. For example, under Разведка, techniques include T1595 (Активное сканирование), T1592 (Сбор информации об атакуемых узлах), T1589 (Сбор информации об атакуемых пользователях), and T1590 (Сбор информации об атакуемой сетевой инфраструктуре). Under Подготовка ресурсов, techniques include T1650 (Приобретение доступа), T1583 (Приобретение инфраструктуры), T1586 (Компрометация учетных записей), T1584 (Компрометация сторонней инфраструктуры), and T1587. Under Первоначальный доступ, techniques include T1659 (Внедрение контента), T1189 (Теневая (drive-by) компрометация), T1190 (Недостатки в общедоступном приложении), T1133 (Внешние службы удаленного доступа), T1200 (Подключение дополнительных устройств), and T1566. Under Выполнение, techniques include T1651 (Средства администрирования облака), T1059 (Интерпретаторы командной строки и сценариев), T1609 (Средства администрирования контейнера), T1610 (Развертывание контейнера), and T1203 (Эксплуатация уязвимостей в клиентских ПО). Under Закрепление, techniques include T1098 (Манипуляции с учетной записью), T1197 (Задания BITS), T1547 (Автозапуск при загрузке или входе в систему), T1037 (Сценарии инициализации при загрузке или входе в систему), and T1176. Under Повышение привилегий, techniques include T1548 (Обход механизмов контроля привилегий), T1134 (Манипуляции с токенами досту), T1098 (Манипуляции с учетной записью), and T1547 (Автозапуск при загрузке или входе в систему).

13. Скачайте данные матрицы в формате JSON:

<https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json>

14. Напишите программу/скрипт для загрузки данных матрицы из скачанного файла в БД. Ниже приведен **пример** на языке Python.

14.1. Установите библиотеки mitreattack-python и pymongo:

```
pip install mitreattack-python
```

```
pip install pymongo
```

Документация по библиотеке mitreattack-python:

<https://mitreattack-python.readthedocs.io/en/latest/index.html>

Документация по библиотеке pymongo:

<https://pymongo.readthedocs.io/en/stable>

14.2. Напишите скрипт:

```
1 from mitreattack.stix20 import MitreAttackData
2 from pymongo import MongoClient
3 import json
4
5 # Подключение к MongoDB (root:example - ваши логин и пароль)
6 client = MongoClient('mongodb://root:example@localhost:27017/')
7 db = client['ipd_07']
8 collection = db['groups']
9
10 # Создание объекта MitreAttackData
11 mitre_attack_data = MitreAttackData("enterprise-attack.json")
12
13 # Получение данных об APT-группах
14 groups = mitre_attack_data.get_groups()
15
16 # Цикл по каждой группе
17 for group in groups:
18     group_json = json.loads(str(group))
19
20     # Получение информации о техниках, используемых группой
21     techniques_used_by_group = mitre_attack_data.get_techniques_used_by_group(group.id)
22     group_json['techniques'] = []
23     for technique in techniques_used_by_group:
24         # Наполнение списка используемых группой техник
25         group_json['techniques'].append(technique['object']['name'])
26
27     # Получение информации о ПО, используемом группой
28     software_used_by_group = mitre_attack_data.get_software_used_by_group(group.id)
29     group_json['software'] = []
30     for s in software_used_by_group:
31         # Наполнение списка используемого группой ПО
32         group_json['software'].append(s['object']['name'])
33
34     # Загрузка информации о группе в БД
35     collection.insert_one(group_json)
```

15. Загрузите с помощью программы/скрипта данные в MongoDB.

Viewing Collection: groups



[New Document](#) [New Index](#)

[Simple](#) [Advanced](#)

Key Value String [Find](#)

Delete all 163 documents retrieved

1 2 3 4 5 > >>

| _id | type | id | created_by_ref | created | modified | name | description |
|---|---------------|--|--|--------------------------|--------------------------|---------------|---|
|   670edb3e8c62597766f5ab82 | Intrusion-set | Intrusion-set--01e28736-2ffc-455b-9880-ed4d1407ae... | Identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5 | 2021-01-06T17:46:35.134Z | 2024-04-17T22:10:56.266Z | Indrik Spider | [Indrik Spider] (https://attack.mitre.org/groups/G...) |

```

42 x_mitre_modified_by_ref: 'identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5',
43 x_mitre_version: '1.0',
44 techniques: [
45   'Steal Web Session Cookie',
46   'Exfiltration to Cloud Storage',
47   'Spearphishing Link',
48   'Malware',
49   'Data Transfer Size Limits',
50   'Hidden Files and Directories',
51   'Upload Malware',
52   'Replication Through Removable Media',
53   'Exfiltration Over C2 Channel',
54   'Drive-by Target',
55   'Link Target',
56   'Malware',
57   'Web Protocols',
58   'Ingress Tool Transfer',
59   'ARP Cache Poisoning',
60   'Tool',
61   'Data from Local System',
62   'Malicious Link',
63   'DLL Side-Loading',
64   'Registry Run Keys / Startup Folder',
65   'File and Directory Discovery',
66   'System Owner/User Discovery',
67   'Archive Collected Data',
68   'Match Legitimate Name or Location',
69   'Modify Registry',
70   'Scheduled Task',
71   'Digital Certificates',
72   'Code Signing'
73 ],
74 software: [
75   'PlugX',
76   'Cobalt Strike'
77 ]

```

16. Выполните несколько поисковых запросов в данной коллекции. Например: поиск групп, которые используют определенную технику или ПО; поиск группы по названию.

17. С помощью запроса в MongoDB выведите списки техник и ПО, используемых группировками по убыванию частоты использования (название техники – сколько групп использует; название ПО – сколько групп использует). Пример:

Viewing Collection: groups

[New Document](#) [New Index](#)

[Simple](#) [Advanced](#)

```
{
  $unwind: "$techniques",
  $group: { _id: "$techniques", count: { $sum: 1 } },
  $sort: { count: -1 }
}
```

Projection

☒ Aggregate query

[Find](#)

Delete all 419 documents retrieved

1 2 3 4 5 > >>

| _id | count |
|--|-------|
| Malicious File | 79 |
| Ingress Tool Transfer | 77 |
| Spearphishing Attachment | 75 |
| PowerShell | 70 |
| Tool | 68 |

Разберитесь с синтаксисом операторов **\$unwind**, **\$group**.

18. Выберите две техники и две программы, используемых АРТ-группами, из выборки, полученной по следующему правилу:

- в списках, полученных в п. 16, найдите технику/ПО по вашему номеру в списке;
- ваша выборка будет состоять из найденной техники/ПО и +/-2 от нее (выборка из 5 элементов).

19. Опишите две выбранные техники (название, описание техники; ссылка на страницу техники на любом из двух ресурсов из п. 12).

20. Опишите две выбранных программы (название ПО; для чего и как используется; ссылка на ПО, если есть в открытом доступе – часто размещены на GitHub).