

ФГБОУ ВО «Московский технологический университет»

Институт комплексной безопасности и специального приборостроения

Кафедра КБ-1 «Защита информации»

**Дисциплина:** «Теоретические основы компьютерной безопасности»

**Отчет по практической работе № 2**

**Тема:** «Модель Харисона-Руззо-Ульмана (HRU-модель)»

**Выполнил:**

Студент группы БББО-05-20

Кутьин Захар Сергеевич

**Проверил:**

Кунин Н.Т.

Москва, 2022

**1-й шаг.** Пользователь-злоумышленник дает права на “write”, “execute” каталога доверенному пользователю .

**Command** “Добавить права доступа на каталог от владельца” (***, ,*** ):

if *“own”* ∈ [***,*** ]

then

***Enter***{ *“write”, “execute”* } ***into*** [***,*** ];

end if

**end command**

|  |  |  |  |
| --- | --- | --- | --- |
|  | – secret | – no secret | – secret |
|  | own, r, w, e | r, w, e | own, r, w, e |
|  | - | own, r, w, e | - |

**2-й шаг**. Пользователь-злоумышленник создает в своем каталоге файл троянской программы , дает на него права “read”, “write”, “execute” для субъекта , объявляет о каких-либо полезных свойствах и возможностях программы и ожидает запуска доверенным пользователем троянской программы. Команда перехода и соответствующее изменение матрицы доступа выглядят так:

**Command** “Создать файл” (***,*** ):

if *“write”* ∈ [***,*** ]

then

***Create object ;***

***Enter*** { *“own”, “read”, “write”, “execute”* } ***into***[***,*** ]**;**

end if

if { *“read”, “write”* } ⊆ [***,*** ]

then

***Enter*** { *“read”, “write”, “execute”* } ***into*** [***,*** ];

end if

**end command**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | – secret | – no secret | – secret | – trojan |
|  | own, r, w, e | r, w, e | own, r, w, e | r, w, e |
|  | - | own, r, w, e | - | own, r, w, e |

**3-й шаг**. Доверенный пользователь запускает троянскую программу , которая автоматически приобретает его права доступа.

**Command** “Запустить файл” (***,*** ):

if { *“read”, “write”, “execute”* } ⊆ [***,*** ]

then

***Create object ;***

***Enter*** { *“read”, “write”, “execute”* } ***into***[***,*** ]**;**

***Enter*** { *“read”, “write”, “execute”* } ***into***[***,*** ]**;**

end if

if { *“own”, “read”, “write”, “execute”* } ⊆ [***,*** ] and { *“own”, “read”, “write”, “execute”* } ⊆ [***,*** ]

then

***Enter*** { *“read”, “write”, “execute”* } ***into*** [***,*** ];

***Enter*** { *“read”, “write”, “execute”* } ***into*** [***,*** ];

end if

**end command**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | – secret | – no secret | – secret | – trojan |
|  | own, r, w, e | r, w, e | own, r, w, e | r, w, e |
|  | - | own, r, w, e | - | own, r, w, e |
|  | r, w, e | r, w, e | r, w, e | r, w, e |

**4-й шаг.** На основе скрытых возможностей троянская программа копирует содержимое секретного файла в несекретный каталог , обеспечивая возможность не доверенному пользователю ознакомится с секретной информацией, прямо ему недоступной.

**Command** “Скопировать файл программой и ” (**,** , ):

if *“read”* ∈ [***,*** ] and *“write”* ∈ [***,*** ]

then

***Create object ;***

***Enter*** { *“own”, “read”, “write”, “execute”* } ***into***[***,*** ]**;**

***Enter*** *“read”* ***into* [, ];**

***Read(, );***

***Write(, );***

end if

***Destroy subject ;***

**end command**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | – secret | – no secret | – secret | – trojan | – secret |
|  | own, r, w, e | r, w, e | own, r, w, e | r, w, e | - |
|  | - | own, r, w, e | - | own, r, w, e | r |

**Вывод:** я изучил основные положения модели Харисона-Руззо-Ульмана (HRU-модель), научился строить пошаговый сценарий атаки путем отображения последовательности команд в матрице доступа в соответствии с HRU-моделью, тем самым выявив недостаток данной модели. Основной проблемой является отсутствие контроля за порождением потоков информации, в частности, контроля за порождением субъектов.