## Защищенные мультисервисные телекоммуникационные системы

### № 1 Модель Харрисона-Руззо-Ульмана

**Задача 1. Построить матрицы и записать в виде команд сценарий атаки с помощью троянской программы в системах, функционирующих на основе модели Харрисона-Руззо-Ульмана (ХРУ)**

> Дано: Пусть имеется два субъекта: ⊠1 - доверенный пользователь, admin и ⊠2 - рядовой пользователь, user; и два каталога ⊠1 и ⊠2, владельцами которых являются пользователи ⊠1 и ⊠2. В каталоге ⊠1 имеется объект ⊠3 с секретной информацией. Исходная матрица доступа имеет вид: |S |⊠1| ⊠2| ⊠3| |—|—|—|—| |⊠1| own, r, w, e| r, w, e | own, r, w, e| |⊠2| | own, r, w, e | |

**Решение:**

Атакующий ⊠2 должен создать в своем каталоге o2 файл с трояном и дать права rwx пользователю ⊠1 на этот файл. Далее ожидает запуска доверенным пользователем ⊠1 ( или исп. команду sleep()) трояна из каталога o2. Главная цель убедить пользователя ⊠1 запустить файл. Когда пользователь ⊠1 запускает файл, троян скопирует секрет из o3 в o2, затем делегирует права доступа для атакующего ⊠2, который теперь может работать с тем же уровнем доступа, что и ⊠1. В итоге файл становится доступным для чтения ⊠2, и атакующий может его прочитать из каталога o2.

“““bash Command”создать файл” (⊠2, троян): if “write” ⊠ [⊠2, o2] then Создать объект троян; Ввести {“own”, “read”, “write”, “execute”} в [⊠2, троян]; end if if {“read”, “write”} ⊠ [⊠1, o2] then Ввести {“read”, “write”, “execute”} в [⊠1, троян]; end if end command “““

| S | ⊠1 (секрет) | ⊠2(секрета нет) | ⊠3(секрет) | ⊠4 (троян) |
|---|---|---|---|---|
| ⊠1 | own, r, w, e | r, w, e | own, r, w, e | r, w, e |
| ⊠2 | | own, r, w, e | | own, r, w, e |

“““bash Command”запустить файл” (s1,троян): if {“read”,“write”,“execute”} ⊠ [⊠1,троян] then Создать субъект ⊠(троян); Ввести { “read”,“write”,“execute”} в [⊠(троян),o2]; Ввести { “read”,“write”,“execute”} в [⊠(троян),троян]; end if if {“own”, “read”,“write”,“execute”} ⊠ [⊠1,o1] and {“own”, “read”,“write”,“execute”} ⊠ [⊠1,o3] then Ввести {“read”,“write”,“execute”} в [⊠(троян),o1]; Ввести {“read”,“write”,“execute”} в [⊠(троян),o3]; end if end command “““

| S | ⊠1 (секрет) | ⊠2(секрета нет) | ⊠3(секрет) | ⊠4 (троян) |
|---|---|---|---|---|
| ⊠1 | own, r, w, e | r, w, e | own, r, w, e | r, w, e |
| ⊠2 | | own, r, w, e | | own, r, w, e |
| ⊠(троян) | r, w, e | r, w, e | r, w, e | r, w, e |

“““bash Command”скопировать файл ⊠3 программой ⊠(троян) в ⊠2” (⊠(троян),o3,o2): if “read” ⊠ [stp,o3] and “write” ⊠ [⊠(троян),o2] then Создать объект o’; Ввести {“own”, “read”, “write”, “execute”} в [⊠(троян),o’]; Ввести “read” в [s2,o’]; Читать (⊠(троян),o3); Записать (⊠(троян), o’); end if Уничтожить субъект ⊠(троян); end command ““”

| S | ⊠1 (секрет) | ⊠2(секрета нет) | ⊠3(секрет) | ⊠4 (троян) | ⊠’= ⊠3(секрет) |
|---|---|---|---|---|---|
| ⊠1 | own, r, w, e | r, w, e | own, r, w, e | r, w, e | |
| ⊠2 | | own, r, w, e | | own, r, w, e | r |

**Задача 2. Построить сценарий аналогичной атаки. Отобразить последовательности команд перехода и изменений матрицы доступа.**

> Дано: Доверенный пользователь ⊠1 в исходном состоянии имеет на каталог ⊠2 только права чтения r. Исходная матрица доступа имеет вид: |S |⊠1| ⊠2| ⊠3| |—|—|—|—| |⊠1| own, r, w, e| r | own, r, w, e| |⊠2| | own, r, w, e | |

**Решение:**