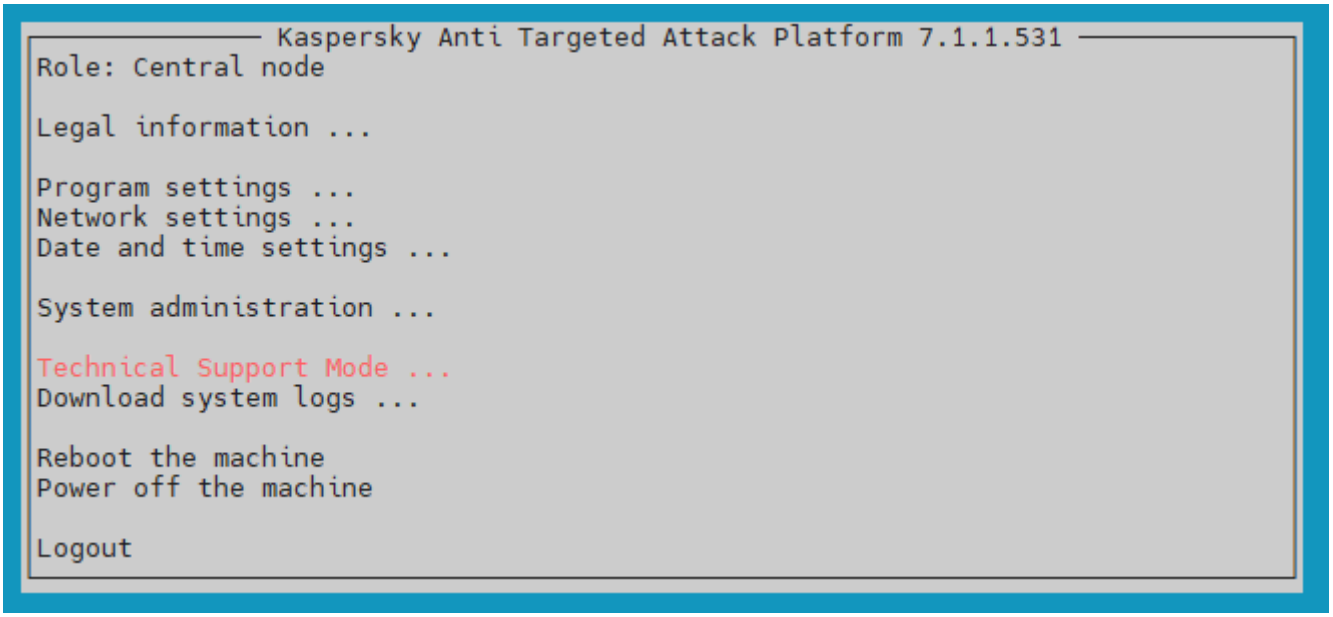
?????????? ?? ???????? ???? ??????? KATA || EDR

> *Примечение:* *данная статья является примером реализации сбора дампа событии*

> *Примечание:* *все действия выполняются в Technical Support Mode под учетной записью root*

1. Подключаемся по SSH к серверу KATA CN. Далее выбираем пункт **Technical Support Mode**



2. В открывшейся командной строке необходимо выполнить следующие команды.Сделайте его исполняемым:

```
sudo –i
```

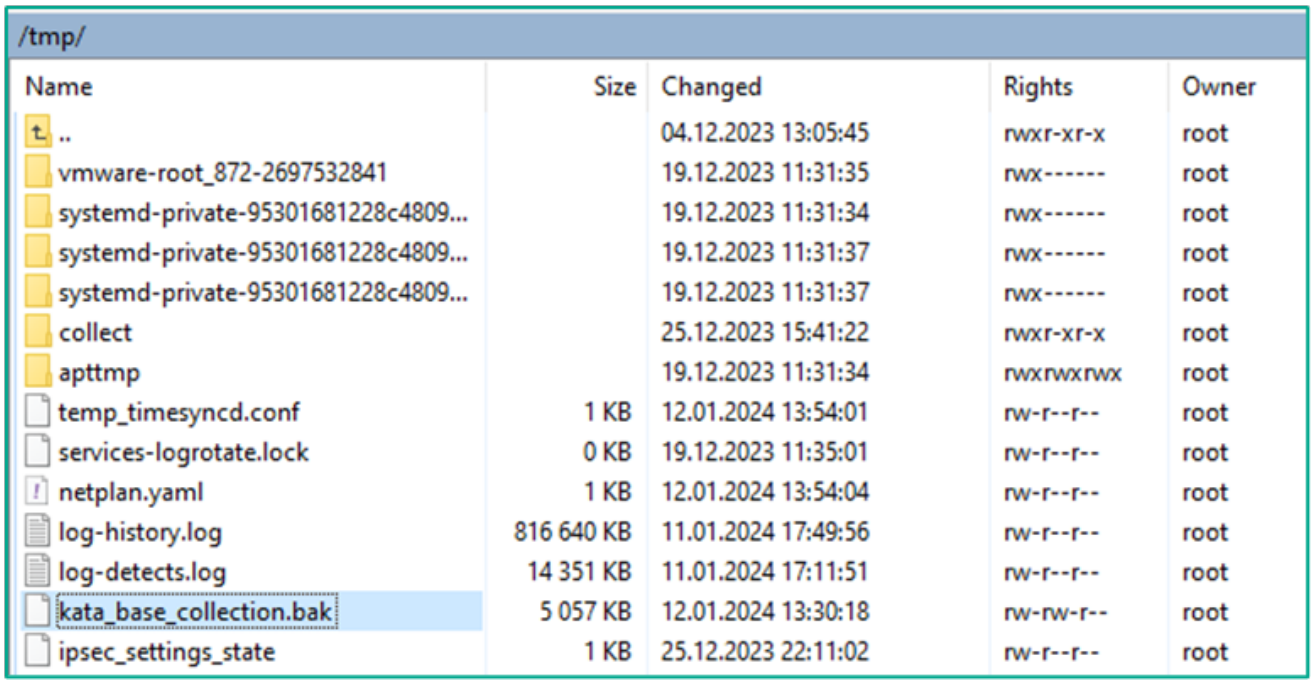
Необходимо будет снова ввести пароль.

3. Далее формируем дамп базы. Последовательно выполняем следующие команды.

```
docker exec $(docker ps -qf name=postgresql_server) /bin/bash -c "su - postgres -c \"pg_dump -Fc antiapt > /tmp/<имя файла>.bak\""
docker cp $(docker ps -qf name=postgresql_server):/tmp/<имя файла>.bak /tmp/
```

```
logout
```

4. Далее необходимо подключиться к серверу KATA, используя SFTP-клиент (например, WinSCP) и забрать файл из директории **/tmp**



/tmp/

Name	Size	Changed	Rights	Owner
..		04.12.2023 13:05:45	rwxr-xr-x	root
vmware-root_872-2697532841		19.12.2023 11:31:35	rwx------	root
systemd-private-95301681228c4809...		19.12.2023 11:31:34	rwx------	root
systemd-private-95301681228c4809...		19.12.2023 11:31:37	rwx------	root
systemd-private-95301681228c4809...		19.12.2023 11:31:37	rwx------	root
collect		25.12.2023 15:41:22	rwxr-xr-x	root
apttmp		19.12.2023 11:31:34	rwxrwxrwx	root
temp_timesyncd.conf	1 KB	12.01.2024 13:54:01	rw-r--r--	root
services-logrotate.lock	0 KB	19.12.2023 11:35:01	rw-r--r--	root
netplan.yaml	1 KB	12.01.2024 13:54:04	rw-r--r--	root
log-history.log	816 640 KB	11.01.2024 17:49:56	rw-r--r--	root
log-detects.log	14 351 KB	11.01.2024 17:11:51	rw-r--r--	root
kata_base_collection.bak	5 057 KB	12.01.2024 13:30:18	rw-rw-r--	root
ipsec_settings_state	1 KB	25.12.2023 22:11:02	rw-r--r--	root

Revision #3
Created 3 October 2025 10:48:46 by Administrator
Updated 6 February 2026 11:29:29 by Кирилл