Сбор информации о системе:

1. Создаём скрипт через nano:

* #!/usr/bin/bash
* clear
* после этого сохраняем наш скрипт под именем – recon.sh
* выходим из nano.

1. Делаем скрипт исполняемым: chmod +x recon.sh
2. Продолжаем редактировать скрипт и сохранять его через nano:

Техт скрипта:

#!/usr/bin/bash

clear

echo "---Recon is in progress---"

echo "Getting hostname"

host=$(hostname)

echo "Getting distro and kernel"

disinfo=$(uname -v)

echo "Getting users"

users=$(cat /etc/passwd)

echo "Getting processes"

pro=$(systemctl | grep running)

echo "Writing results"

mkdir recon

touch ./recon/info.txt

echo "$host" > ./recon/info.txt

echo "$disinfo" >> ./recon/info.txt

printf '%s/n' "$users" >> ./recon/info.txt

printf '%s/n' "$pro" >> ./recon/info.txt

echo "Done"

1. Открываем исполняемый скрипт, он исполняется и записывает собираемую информацию в файл info.txt, расположенный в созданной нами директории recon.