Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

Лабораторная работа №2

По дисциплине «ССВТ»

Тема: «Hack the box»

Выполнил:

Студент 3 курса

Группы ИИ-21(2)

Литвинюк Т. В.

Проверил:

Соловчук А. М.

Брест 2024

Цель работы: взломать машину Hack The Box.

Ход работы:

Вариант: Headless.

Сначала просканируем порты:

Nmap scan report for headless.htb (10.10.11.8)

Host is up (0.35s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

| ssh-hostkey:

| 256 90:02:94:28:3d:ab:22:74:df:0e:a3:b2:0f:2b:c6:17 (ECDSA)

|\_ 256 2e:b9:08:24:02:1b:60:94:60:b3:84:a9:9e:1a:60:ca (ED25519)

5000/tcp open upnp?

| fingerprint-strings:

| GetRequest:

| HTTP/1.1 200 OK

| Server: Werkzeug/2.2.2 Python/3.11.2

| Date: Sun, 24 Mar 2024 15:26:43 GMT

| Content-Type: text/html; charset=utf-8

| Content-Length: 2799

| Set-Cookie: is\_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB\_Zfs; Path=/

| Connection: close

| <!DOCTYPE html>

| <html lang="en">

| <head>

| <meta charset="UTF-8">

| <meta name="viewport" content="width=device-width, initial-scale=1.0">

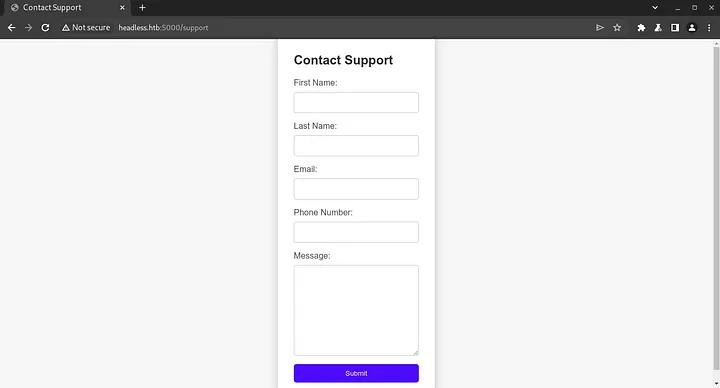
| <title>Under Construction</title>

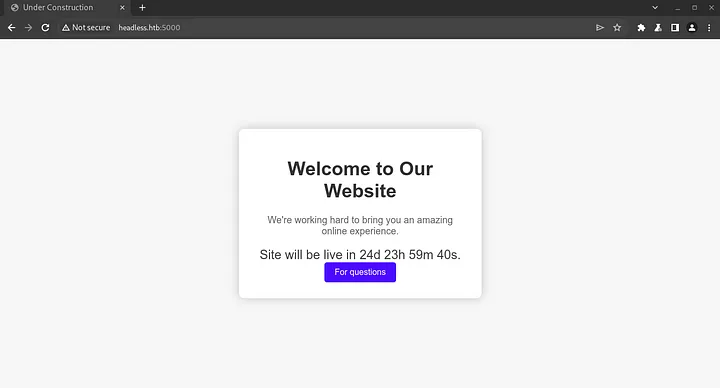
| <style>

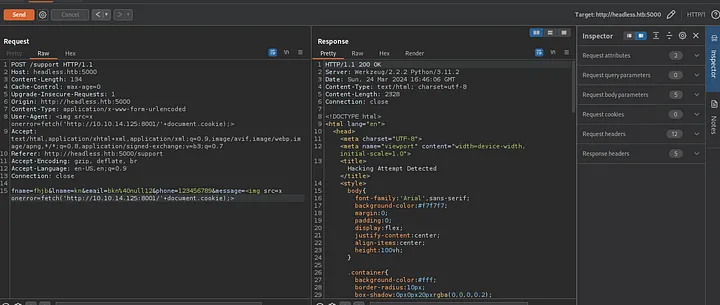
| body {

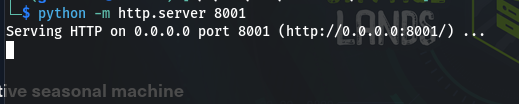
| font-family: 'Arial', sans-serif;

| background-color: #f7f7f7;

На порту 5000 находится главная страница сайта.

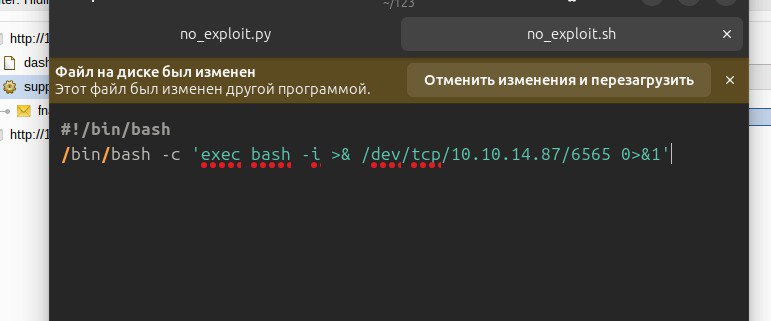


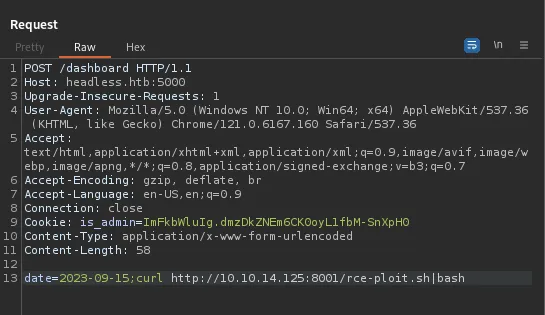
Получаем куки, которые позволят залогинится на сайте как админ

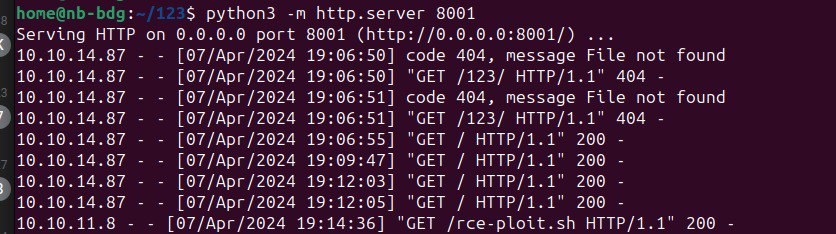


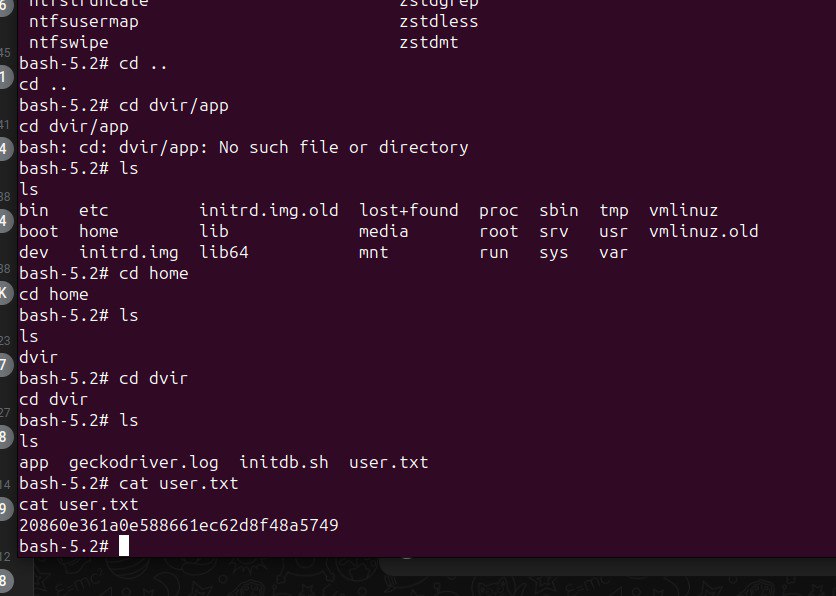
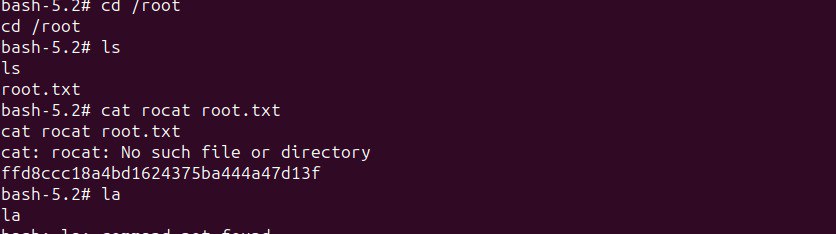


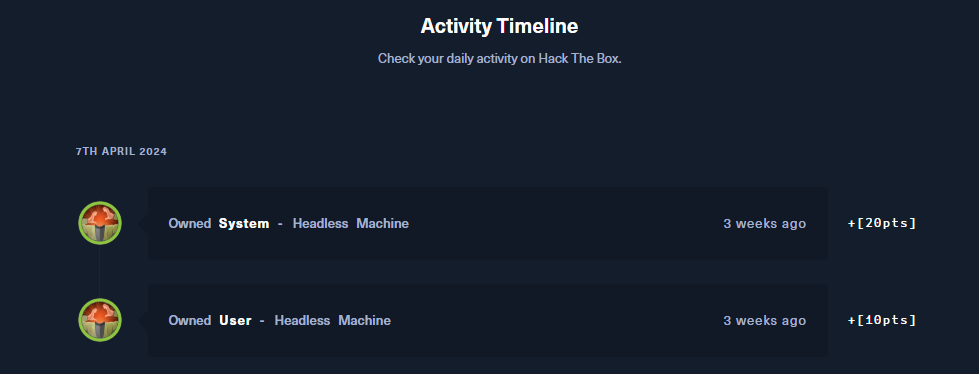
Вставляем полученные куки в запрос, создаем скрипт для управления сервером удаленно, запускаем сервер и отправляем запрос по ендпоинту /dashboard.







Мы получили доступ к терминалу сервера. Теперь мы можем найти файлы user.txt и root.txt для получения флагов.



**Вывод**: в ходе лабораторной работы я научился базовым навыкам по взлому серверов.