# Отчет по итогам выполнения сертификационного испытания «Белый Хакер»

## Иван Иванов

### Введение

В данном отчете представлена информация о результатах прохождения сертификационного испытания "Белый Хакер".

Отчет должен включать в себя подробное описание всех выполненных шагов по достижению целей, содержать необходимые технические комментарии, скриншоты, выполненные команды и их вывод.

### Цели испытания

Целью испытания является решение ряда задач, расположенных в специально подготовленной лабораторной среде . При решении заданий испытуемый должен продемонстрировать знания и навыки из арсенала Белого Хакера и достичь описанных в каждом задании целей.

### Выполнения испытательных заданий

### Задание 1

**IP-Адрес задания**: 1.2.3.4

Ниже приведено описание выполненных шагов при решении задания 1

### Сканирование портов

Было выполнено сканирование портов с помощью утилиты nmap

nmap -Pn -n -F 1.2.3.4

Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-27 16:49 +03

Nmap scan report for 1.2.3.4

Host is up (0.071s latency).

Not shown: 95 closed tcp ports (conn-refused)

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3000/tcp open ppp

5000/tcp open upnp

8000/tcp open http-alt

Таким образом были обнаружены открытые TCP-порты 22, 80, 3000, 5000, 8000.

Далее была обнаружена уязвимость в сетевом сервисе на порту 3000. Для её эксплуатации использовался модуль metasploit windows/module/name:

use ...

set RHOST...

set RPORT...

set payload ...

exploit

После этого был получен reverse shell на машине атакующего. Ниже приведен скриншот получения reverse shell и чтения флага из файла /root/flag.txt

<тут скриншот>

### SQL-инъекция

Далее с помощью полученного доступа была проведена атака на машину с сетевым именем target.

В веб-приложении http://target:5000 была обнаружена страница /profile.php. Параметр **id** этой страницы был уязвим к SQL-инъекции.

Атакующий выполнил атаку с использованием техники Union-Based.

Для получения флага была использован запрос:

/profile.php?id='+union+select+1,2,flag+from+secrets+--+

В результате получен флаг:

cybered{155e0f70561b8f53fd56784d387f59a3}

Скриншот получения флага приведен ниже


### Задание 2

....