目录

Task1: What is Offensive Security? 什么是进攻性安全?

> The process of breaking into computer systems, exploiting **software bugs**, and finding **loopholes** in application to gain **unauthorized access** to them.

想要打败黑客,就要先成为黑客(就像星爷《九品芝麻官》里说的,想惩治贪官,就要比贪官还奸).

Find vulnerabilities and recommending patches before a cybercriminal does.

Offensive security $\Leftrightarrow$ Defensive Security

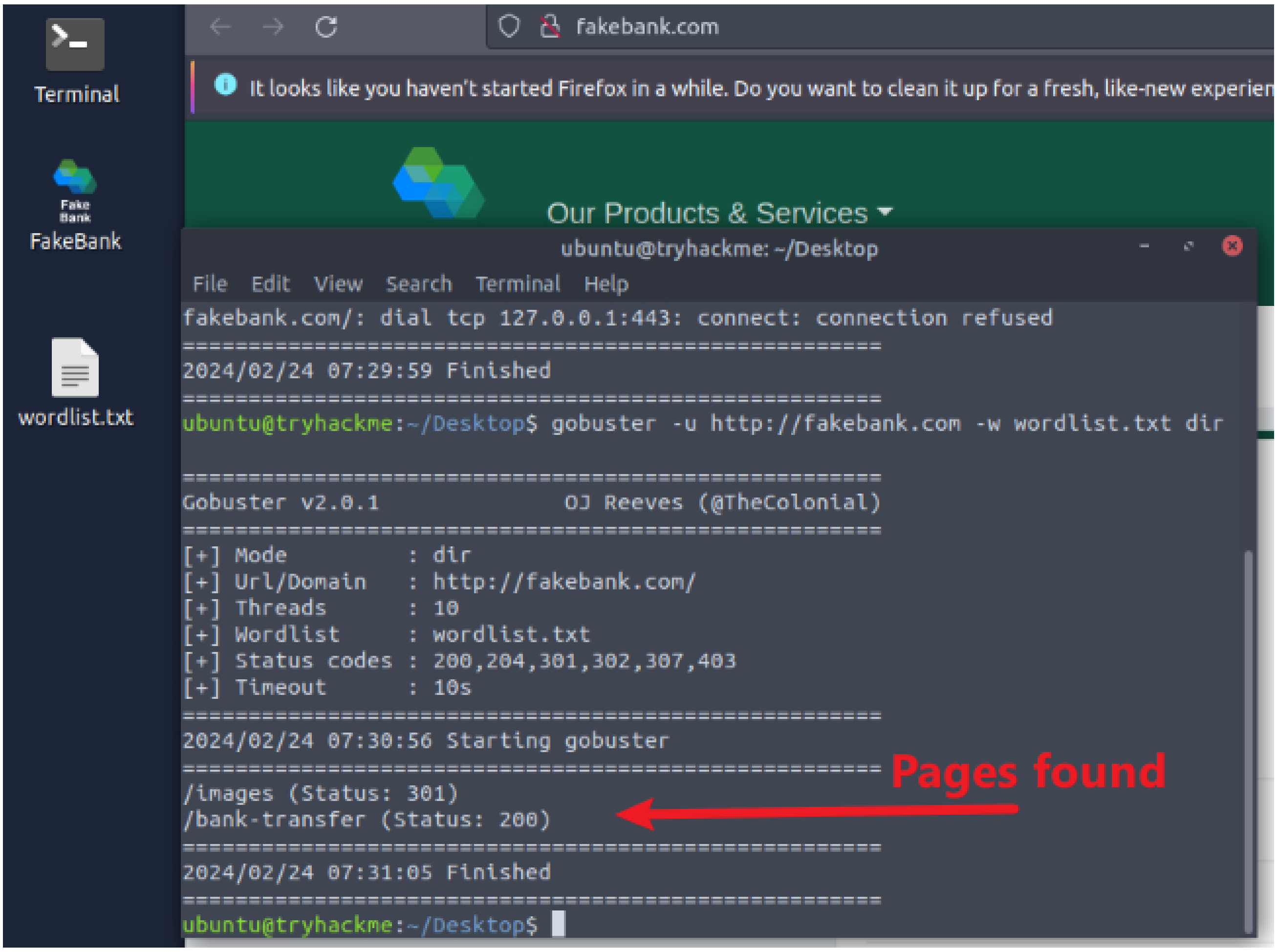
❓ Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

❗ Defensive Security

Task2: Hacking your first machine 黑入你的第一台机器

在介绍Cyber Security Careers和offensive security之前,先当一个黑客体验一下.

- 打开终端Terminal
- 找到隐藏的网页



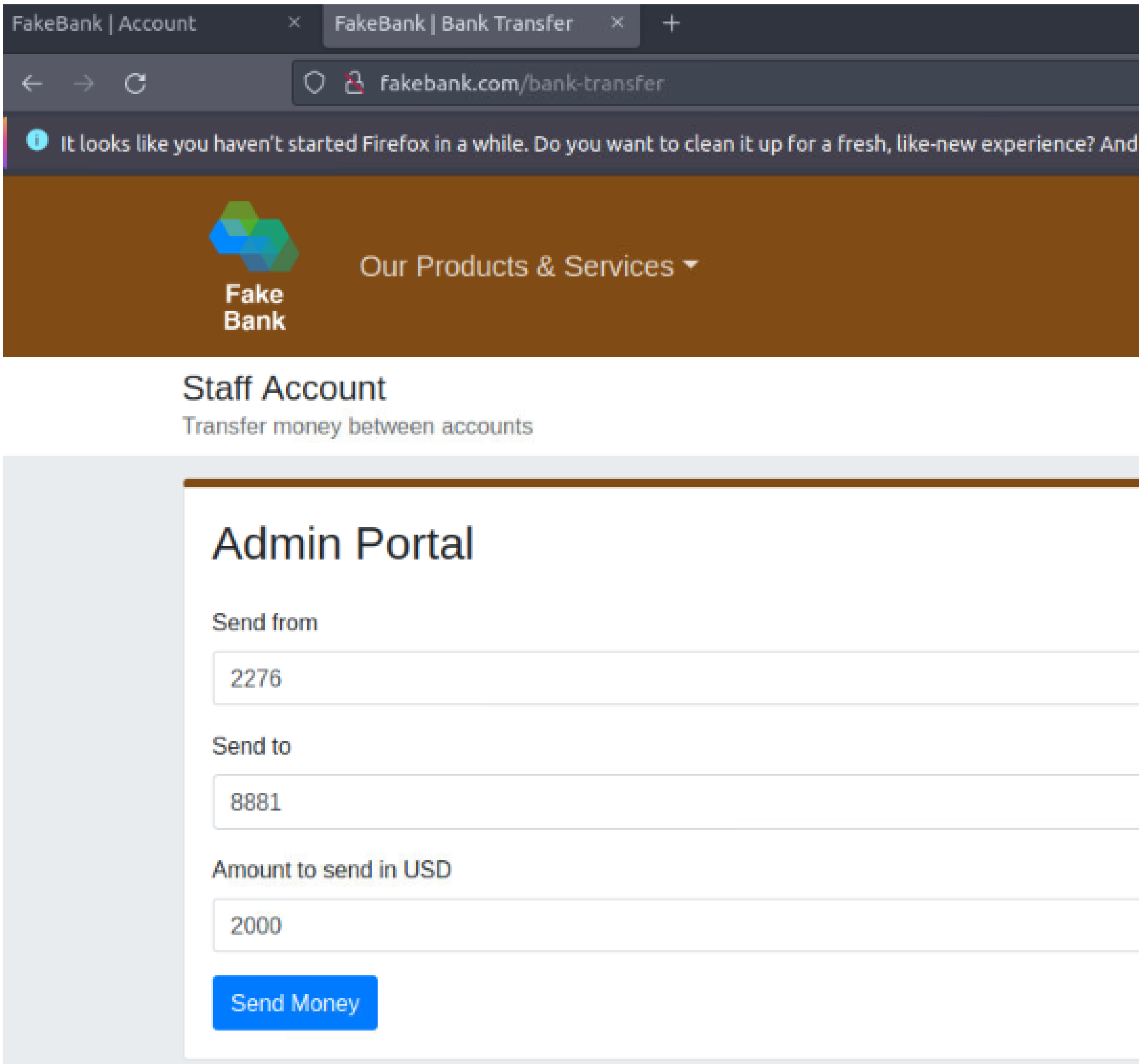
执行的命令为

```
gobuster -u http://fakebank.com -w wordlist.txt dir
```

-u 表示给出网页的状态(301表示Redirect重定向,200表示HTTP连接成功网页可访问)

-w 表示使用给定txt文件中的单词迭代查询隐藏网页.

结果显示,网站根目录下/bank-transfer是可访问的

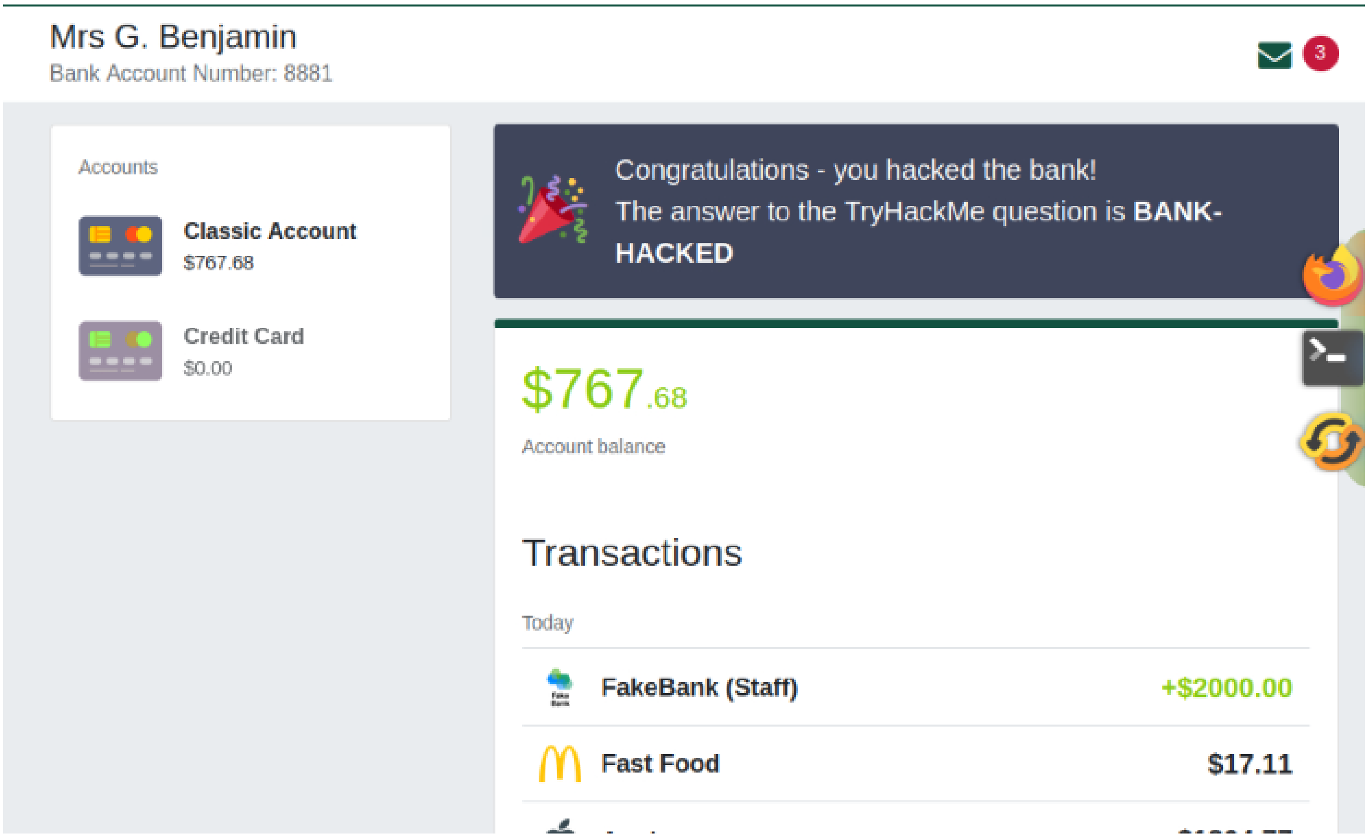


按网站提示,将帐户2276的钱转2000$到账户8881中.

再加到自己账户确认到账情况,并得到

通关密码:

BANK-HACKED



补充说明:

如果你的身份是penetration tester或是security consultant,那么你刚才的操作就相当于对公司网站进行漏洞检测.

Task3:Careers in cyber security

在网络安全行业,有许多可选的职种,列举一部分如下:

- Penetration Tester: Responsible for testing technology products for finding exploitable security vulnerabilities.
- Red Teamer - Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.
- Security Engineer - Design, monitor, and maintain security controls, networks, and systems to help prevent cyberattacks.