**Nibbles**

Перша машина для відпрацювання базових навичок котрі я здобув у модулі getting started.

**сканування (scanning).**

Першим ділом, проскануємо систему на наявність відкритих портів та дізнаємось які служби працюють на цих портах.

**nmap -p- --open -oA Nibbles\_full\_tcp\_scan 10.129.65.175** – сканування всіх можливих портів, але виводить ті що відкриті.

**-p-** – флаг що вказує на всі можливі порти.

**--open** – флаг що повертає нам тільки відкриті порти.

**-oA** –флаг щозаписує результат сканування уфайл **Nibblles\_full\_tcp\_scan** з розширеннями gnmap, nmap та xml.

A screen shot of a computer

AI-generated content may be incorrect.

На скріншоті ми бачимо результат сканування.

Порт 22 (**ssh**) – порт що викорстовується для віддаленого доступу.

Порт 80 (**http**) – порт на якому працює віб-сервер

Тепер ми можемо зробити детальне сканування цих портів щоб дізнатися якіж саме сервіси там працюють. Це ми можемо зробити задопомогою команди **nmap -p 22,80 -A -oA Nibbles\_detailed\_scan 10.129.65.175**

**-A** –цей флаг, робить наше сканування більш агресивним і глибоким для отримання додаткової інофрмації. Він робить наше сканування більш помітнішим та замає більше часу на сканування кожного порта.

A computer screen shot of a program

AI-generated content may be incorrect.

На скріншоті ми бачимо більш детальнішу інфомарцію, що може нам допомогти знайти прогалини на цих портах.

Порт 22 (**ssh**) – працює **ssh** версії **OpenSSH 7.2p2** Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

Порт 80 (**http**) – працює **Apache** версії 2.4.18

Також бачимо що наша ціль використовує систему **Linux** дистрибутив **Ubuntu**.

**Веб перечислення (Web enumerating)**

Тепер коли ми знаємо що на нашій цілі працює веб-сервер, ми можемо відвідати його щоб пошукати чи є там вразливість.

A screen shot of a computer

AI-generated content may be incorrect.

На цьому сайті ми бачимо тільки напис Hello world!, тому давайте переглянемо вихідний код сторінки через комбінацію **Ctrl + U**.

A screenshot of a computer

AI-generated content may be incorrect.

Ми бачимо що в нас є піддомен **nibbleblog**, давайте перейдемо туди.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.Тепер ми маємо робочу сторінку, треба її дослідити. Ми бачимо що сервер використовує **Nibbleblog**. Тепер звичайним запитому у гугл можемо пошукати публічні експлоїти на нього.

Ми бачимо що є вразливість на версії 4.0.3, вона дозволяє відправляти довільний PHP-код на веб-сервер.

Тепер ми ретельно перевіримо наявність інших стоірнок на сервері за допомогою **Gobuster**.

**gobuster dir -u http://10.129.65.175/nibbleblog/ --wordlist /usr/share/seclists/Discovery/Web-Content/common.txt**

**A screenshot of a computer program

AI-generated content may be incorrect.**

Ми бачимо інші сторінки цього веб-сервера, треба перевірити їх. Після перевірки, ми зрозуміли, що на веб-сервері налаштований блеклист, логін admin та сторінка адміністратора у папці content/private є файл config, у ньому ми можемо побачити згадку про nibbles. Тепер ми можемо спробувати підібрати логін **admin** та пароль **nibbles**.

**A screenshot of a computer

AI-generated content may be incorrect.**

**Експлуатація (Exploitation)**

Тепер нам треба дослідити панель адміністратора.

A screenshot of a computer

AI-generated content may be incorrect.

Нас зацікавила вкалдка plugins, там ми можемо побачити плагін **My image**, можемо через нього спробувати віддправити невеличкий **PHP-код** та перевірити його.

A screen shot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

Коли ми впевнились що наш код дійшов до сервера ми можемо написати скрипт для **зворотньої оболонки(reverse shell**).

A computer screen with white text

AI-generated content may be incorrect.

Тепер нам треба відкрити порт прослуховування командою **nc**.

A computer screen shot of a code

AI-generated content may be incorrect.

Завантажуємо файл shell.php і ми ортимуємо доступ до нашої цілі.

A computer screen shot of a computer code

AI-generated content may be incorrect.

**Підвищення привилеїв (Privileges escalation)**

Як тільки ми отримали доступ до хоста, нам треба зробити оболонку більш зручншіою за допомогою команд **python3 -c 'import pty; pty.spawn("/bin/bash")'**, далі натискаємо Ctrl + Z, пишемо stty raw -echo, далі fg і два рази натискаємо Enter.

Тепер ми можемо пошукати можливості як підвищити свої привілеї за дпомогою комади **sudo -l**.

A screen shot of a computer code

AI-generated content may be incorrect.

Ми бачимо які файли ми можемо виконати від імені **sudo**.

Тепер ми додаємо наш Bash-код до цього файлу і виконуємо його через sudo та ставимо прослуховування на нашому хості.  


Запускаємо скрипт та робимо з’єднання

A screenshot of a computer

AI-generated content may be incorrect.

**Заключення**

Це перший мій путівник, який я зробив для розвитку своїх навичок документацій та закріплення тих навичок, що я використав для взламу свого першого ящика. Надалі я буду робити технічні та не технічні документації і завантажувати їх на свій **Github**.