**Cap**

**Сканування/збір інформації**

A screenshot of a computer

AI-generated content may be incorrect.

Сканування **nmap** нам виявило 3 порти.

21 – ftp (vsftpd 3.0.3)  
22 – ssh (OpenSSH 8.2p1)  
80 – http (Gunicorn)  
A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

Явних ризиків методом пошуку в google не знайдено.

Тепер треба перевірити саму сторінку веб-сервера.

A screenshot of a computer

AI-generated content may be incorrect.

Перевіряю усі сторінки.

<http://10.10.10.245/data/1> – тут ми можемо викачати файл логів і переглянути.

<http://10.10.10.245/ip> – тут ми можемо побачити мережеві інтерфейси цілі.

<http://10.10.10.245/netstat> – тут можна побачити активні підключення.

Ми можемо змінити id файла замінюючи значення в URL-адресі.

A screenshot of a computer

AI-generated content may be incorrect.

За допомгою Wireshark ми можемо відкрити цей файл і знайти інфомацію про вхід у систему.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.Ми бачимо що на ftp можна потрапити за допомогою логіна nathan та паролю Buck3tH4TF0RM3!

І так само можемо спробувати з SSH.

A computer screen shot of a computer

AI-generated content may be incorrect.

Тепер треба застосувати **linPEAS** для перевірки системи на вразливості для підвищення привілеїв.

A screen shot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

З документації <https://man7.org/linux/man-pages/man7/capabilities.7.html> виявляється можливість отримати **UID 0**, тобто **root** привілеї без паролю використовуючи **python**.

A screen shot of a computer

AI-generated content may be incorrect.

