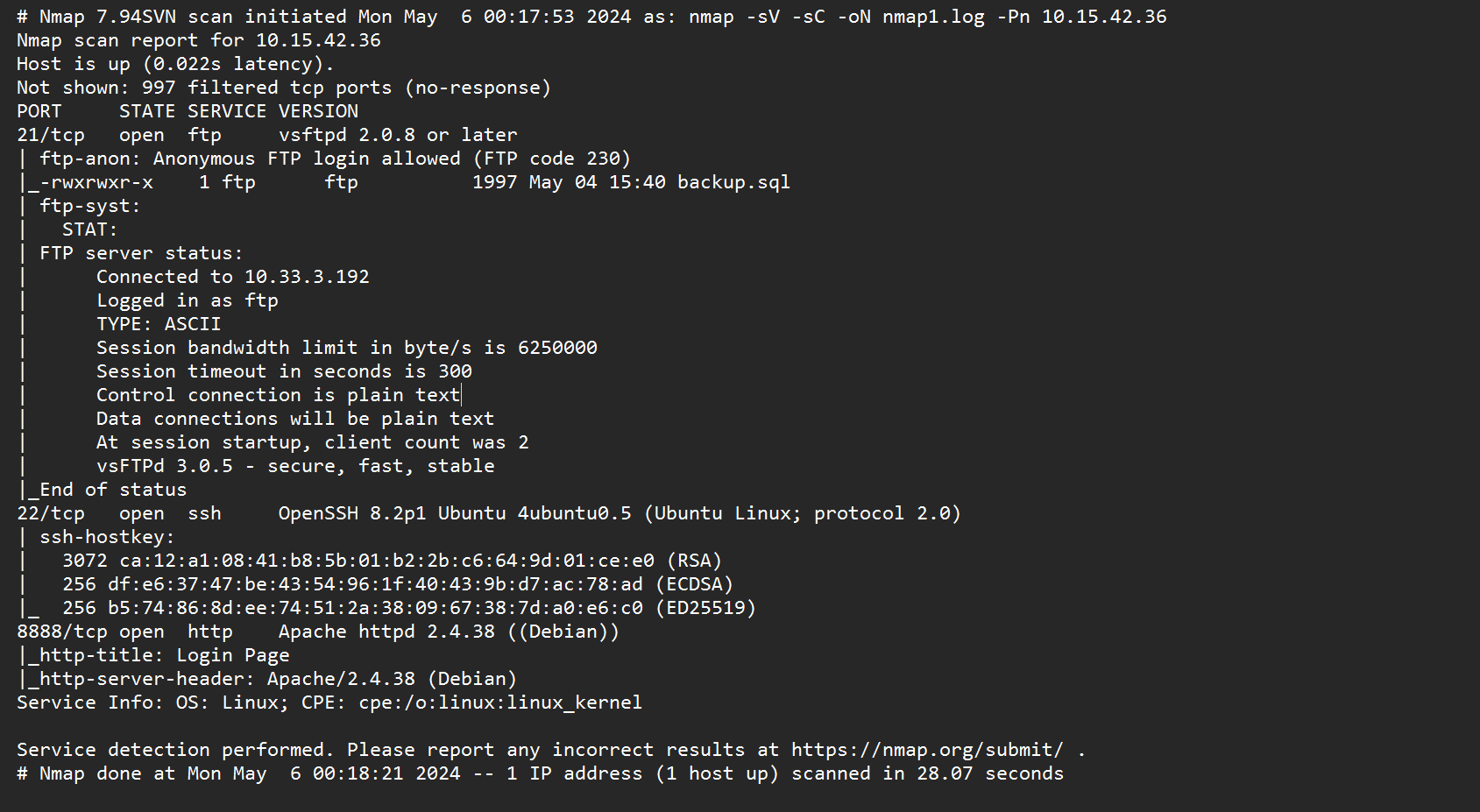
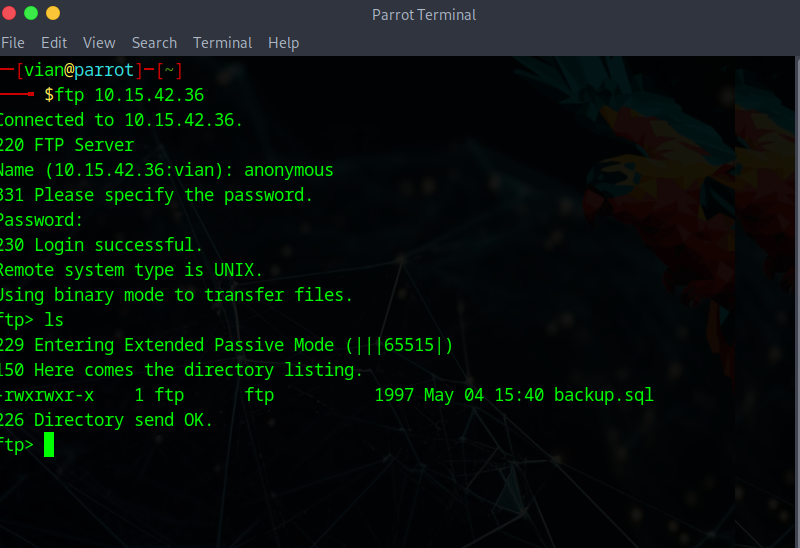
**10.15.42.36**

1. nmap -sV -sC -oN nmap1.log -Pn 10.15.42.36

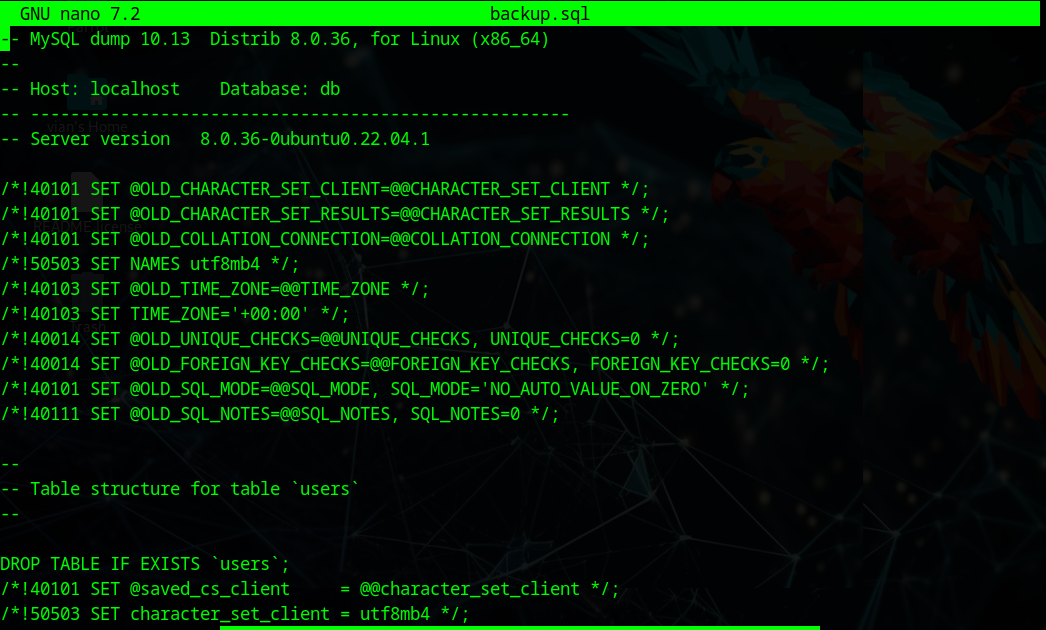


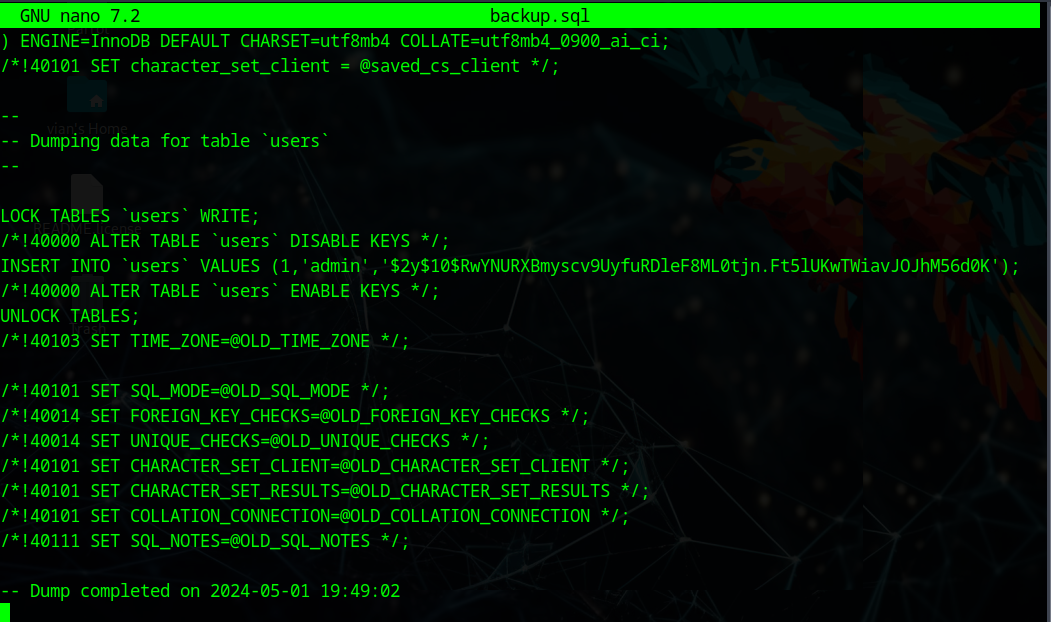
1. Port 21

Open ftp 10.15.42.36



Isi file backup.sq dil ftp 10.15.42.36





EXPLOIT RISK: vsftpd 2.0.8 server, vsftpd 3.0.5 ftp server

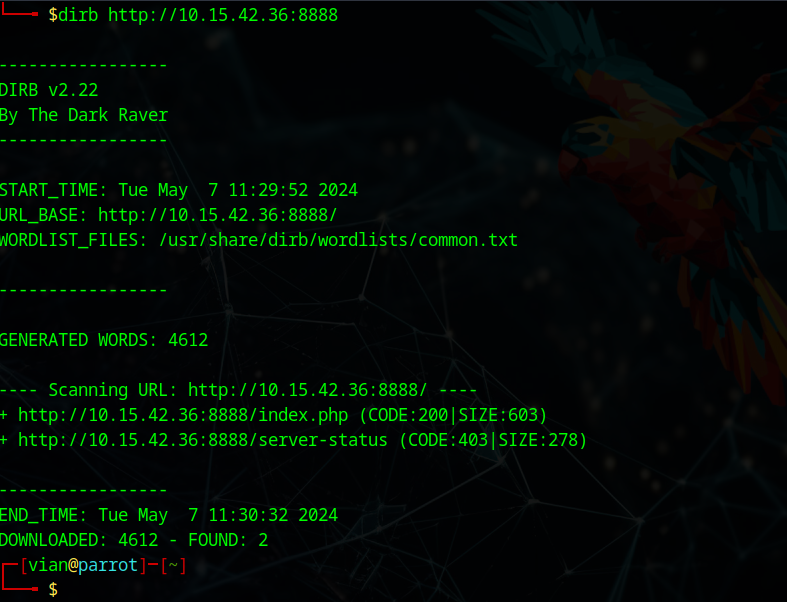
1. Port 22

EXPLOIT RISK **CRITICAL** : **CVE-2023-38408** OpenSSH 8.2p1 Ubuntu 4ubuntu0.5can be exploited

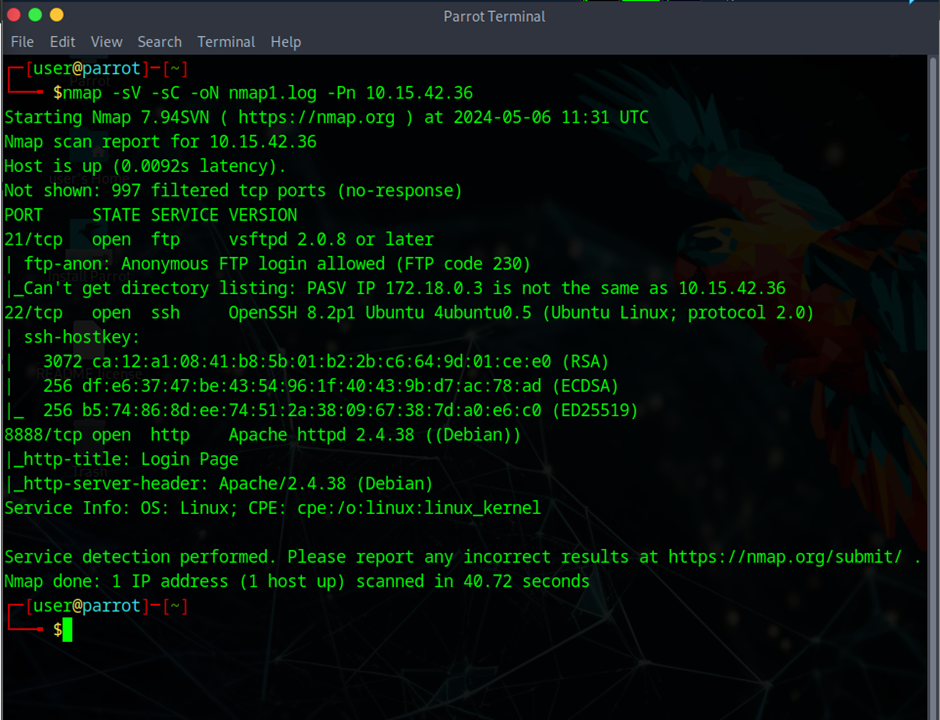
1. Port 8888

EXPLOIT RISK **HIGH** : **CVE-2019-0211** apache 2.4.38 exploit can be exploited

Masih menggunakan http sehingga mudah dibobol



1. Menjalankan nmap -sV -sC -oN nmap1.log -Pn 10.15.42.36 untuk mendapatkan informasi



Dari sini kita mendapatkan :

· Server HTTP: Sistem target menjalankan server web Apache versi 2.4.38 pada Debian Linux. Informasi ini dapat membantu Anda meneliti kerentanan potensial yang spesifik untuk versi Apache tersebut.

· Sistem Operasi: Sistem target menjalankan beberapa versi Linux, seperti yang ditunjukkan oleh entri "OS: Linux" dan "CPE: cpe:/o:linux:linux\_kernel". Distribusi Linux spesifik tidak diidentifikasi, tetapi informasi ini mempersempit pencarian Anda untuk kerentanan dan eksploitasi potensial.

· Aplikasi Web: Entri "http-title: halaman login" menunjukkan bahwa sistem target meng-host aplikasi web dengan halaman login. Ini bisa menjadi vektor serangan menarik jika Anda diizinkan untuk menguji kerentanan aplikasi web seperti injeksi SQL, cross-site scripting (XSS), atau cara melewati otentikasi.

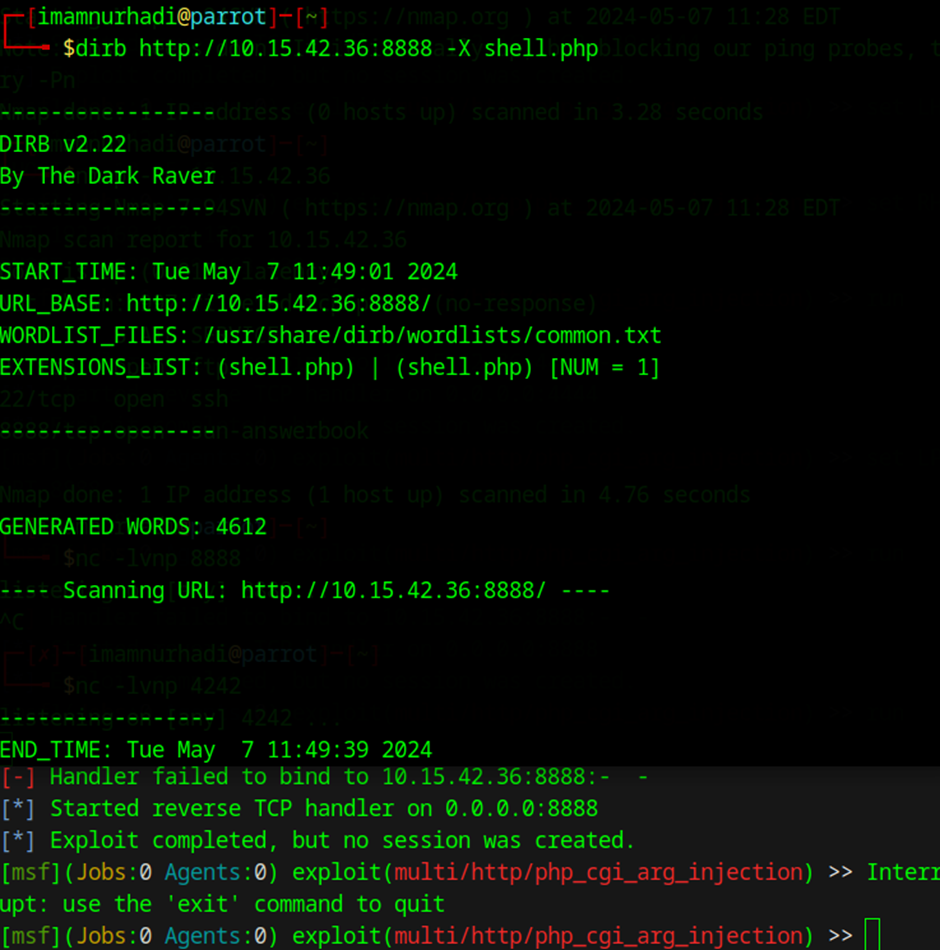
· Server SSH: Sistem target memiliki server OpenSSH yang berjalan pada versi 8.2p1 pada Ubuntu 4ubuntu0.5. Informasi ini dapat membantu Anda meneliti kerentanan potensial pada versi OpenSSH tersebut, serta kerentanan yang spesifik untuk Ubuntu.

Dapat bahwa service dari port 8888 adalah sun-answerbook. Ini dapat dilihat pada **CVE:**

[2002-2425](https://nvd.nist.gov/vuln/detail/CVE-2002-2425) terkait Sun AnswerBook2 1.x - Unauthorized Administrative Script Access

2. Mencoba mencari informasi terkait server dan dipatkankan http servernya merupakan apache 2.4.38 yang termask versi yang outdated dan ini

Mencoba mencari kerentanan web server apache yang outdated

3. Mencari web content pada http://10.15.42.36 :8888 untuk mencari file pada web server nya

Dan hasil saat dibuka dan tidak ditemukan shell.php sehingga tidak bisa dilakukan reverse shell exploit

4.

**10.15.42.7**

1. nmap -sV -sC -oN nmap1.log -Pn 10.15.42.7

