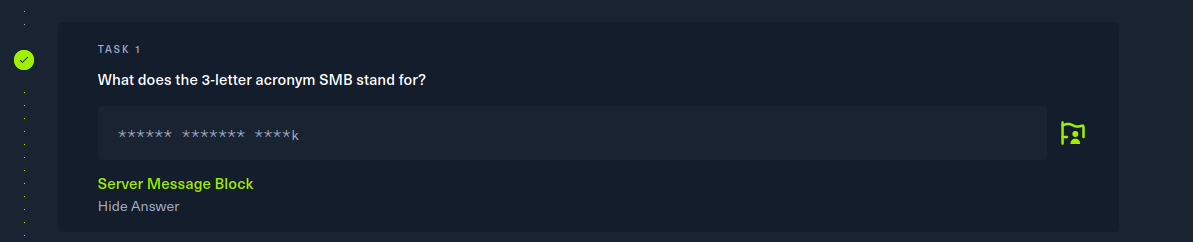
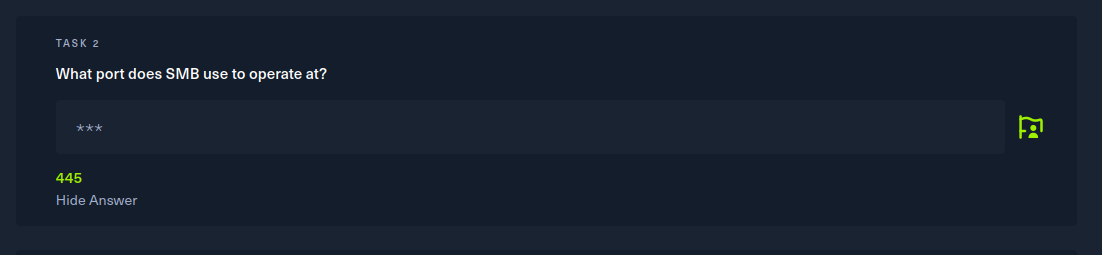
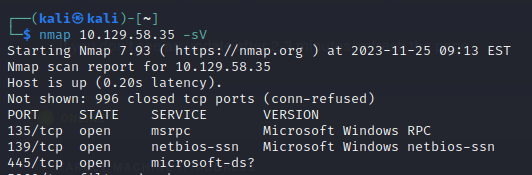
1. Starting Point Dancing
2. Question 1



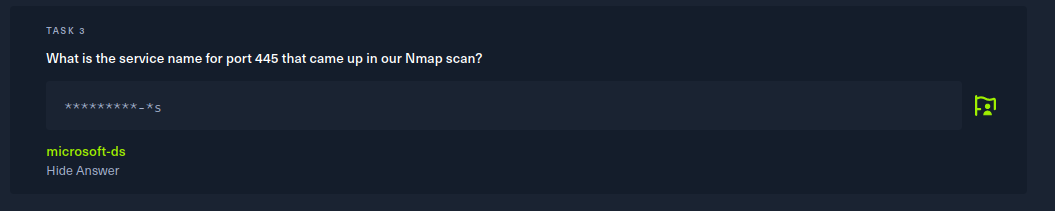
1. Question 2



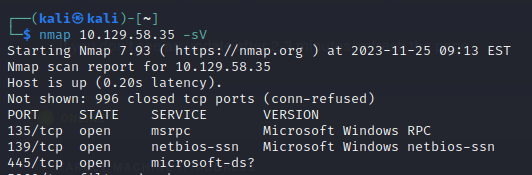
Jalankan “Nmap -sV”



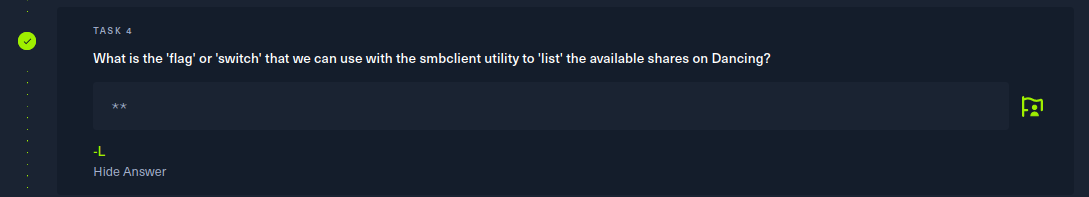
1. Question 3



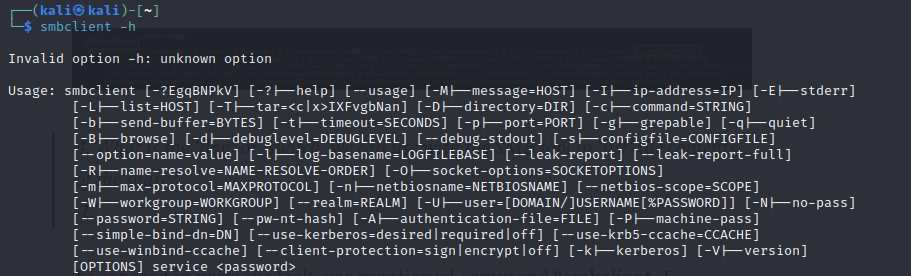
Jalankan “Nmap -sV”



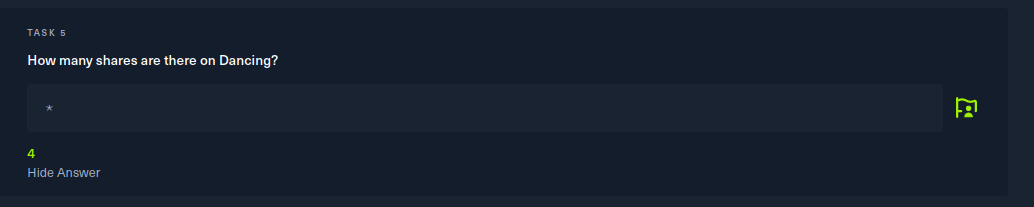
1. Question 4



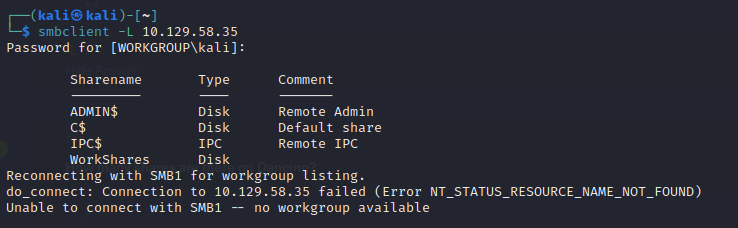
Jalankan “smbclient -h”



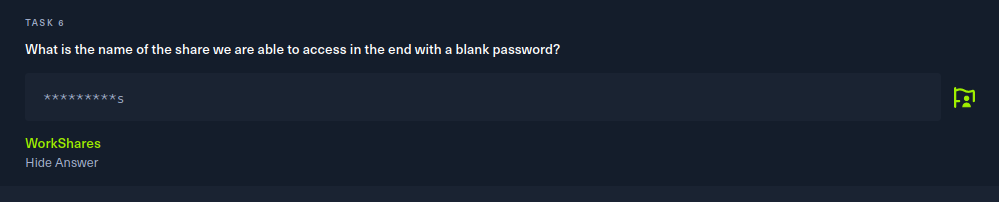
1. Question 5



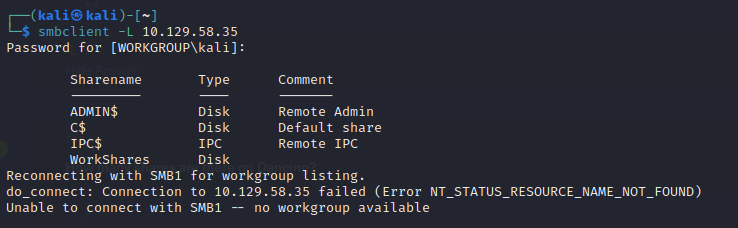
Jalankan “smbclient -L ‘target ip’”



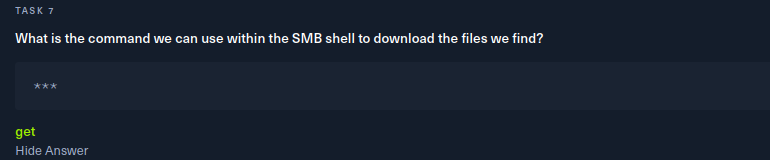
1. Question 6

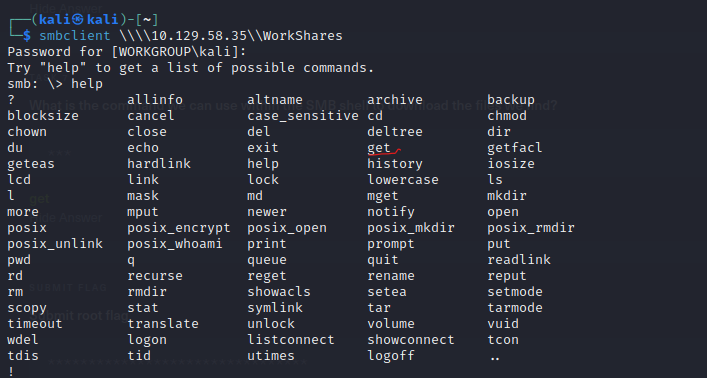


Karena hanya WorkShares yang saat di connect tidak perlu memasukkan password

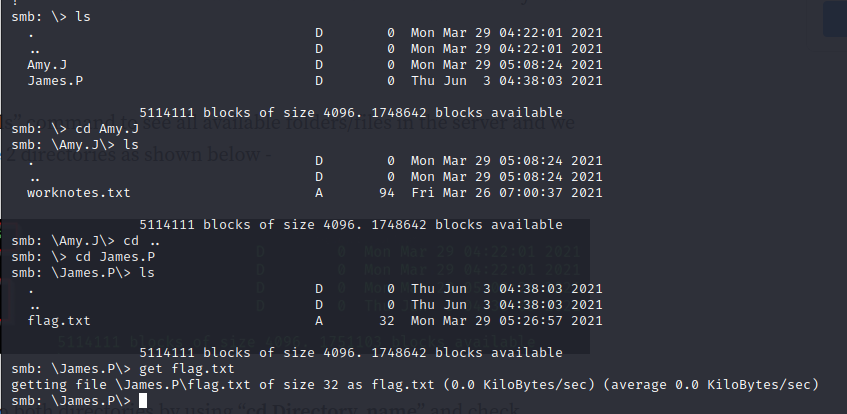


1. Question 7



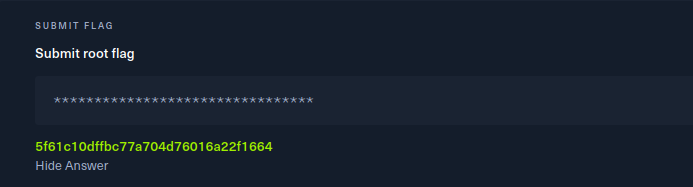


1. Question 8



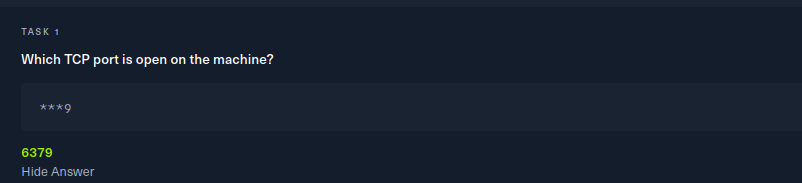
Lalu masuk ke terminal dan mencoba membuka menggunakan nano



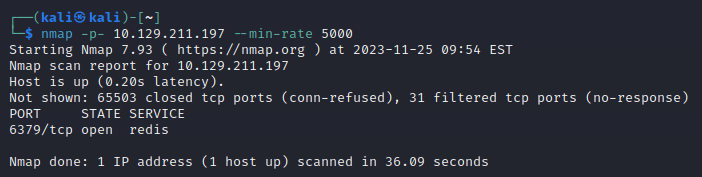


Starting point redeemer

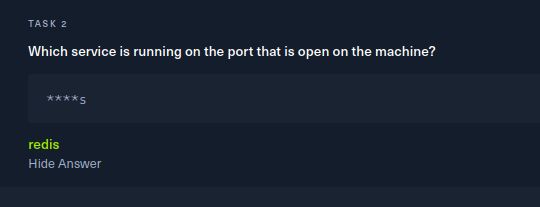
1. Question 1

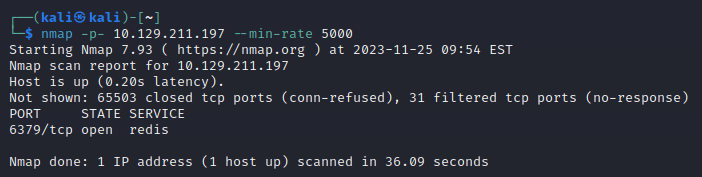


“jalankan nmap -p- ‘ipaddress-nya’ –min-rate 5000”

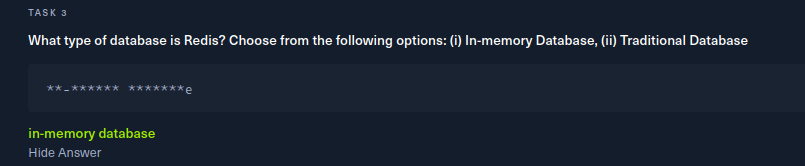


1. Question 2

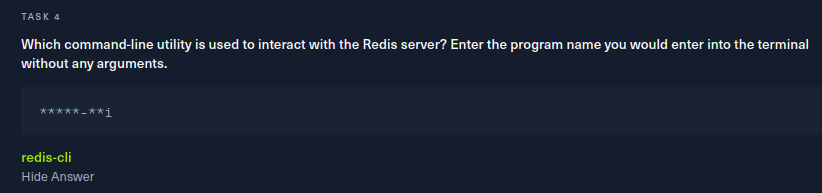




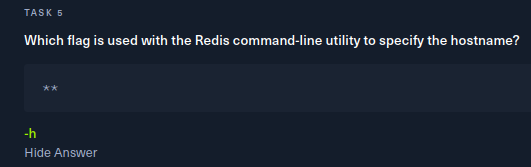
1. Question 3



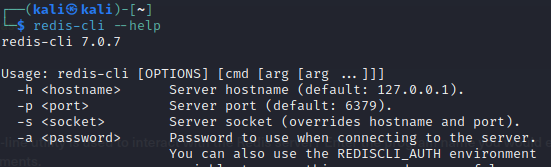
1. Question 4



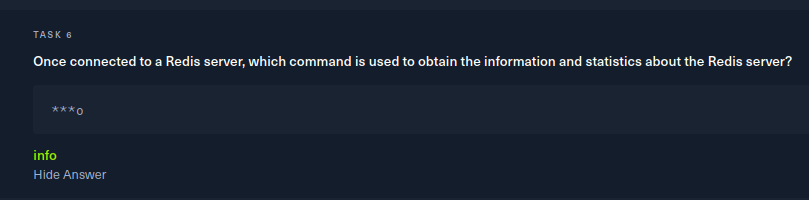
1. Question 5



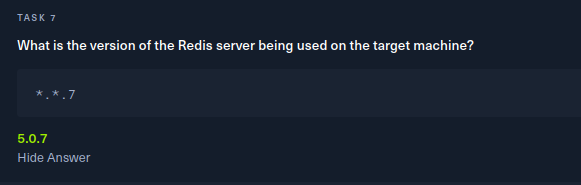
Dengan mengetikkan



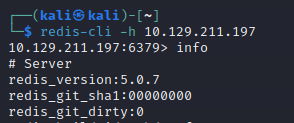
1. Question 6



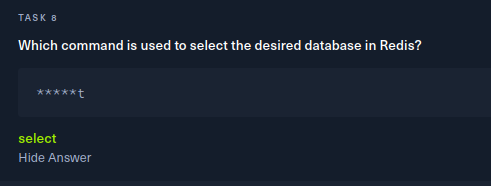
1. Question 7



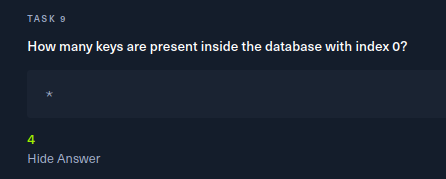
Dengan mengetikkan redis-cli -h “ipaddress” 🡪 info



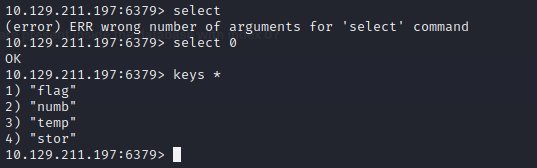
1. Question 8



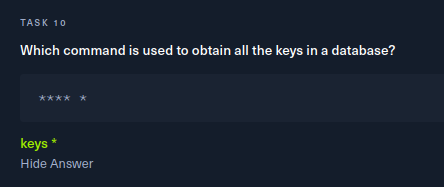
1. Question 9



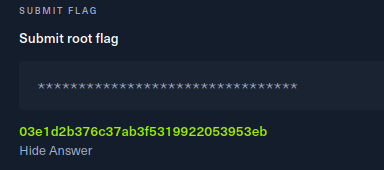
Dengan mengetikkan



1. Question 10



1. Question 11



Dengan mengetik



1. a. Report 1

**[CVE-2023-38546] cookie injection with none file**

Jenis kerentanan: cookie injection

Tingkat seveity: Low

CVSS score: 0.5

Remidiasi: Enkripsi yang valid

b. Report 2

**IDOR vulnerability on profile picture changing mechanism which discloses other user's profile picture.**

Jenis kerentanan: IDOR Vulnerability

Tingkat seveity: Medium

CVSS score: 1

Remidiasi: Penggunaan session token

c. Report 3

**HTML injection in search UI when selecting a circle with HTML in the display name**

Jenis kerentanan: XSS-Stored

Tingkat seveity: Low

CVSS score: 0.5

Remidiasi: Content Security Policy (CSP). Terapkan kebijakan keamanan konten (Content Security Policy) untuk membatasi jenis sumber daya yang dapat dimuat dan memitigasi risiko XSS.