Analysis

nmap

```
nmap -sC -sV 10.10.11.250
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-03 15:08 CET
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 15:08 (0:00:00 remaining)
Nmap scan report for 10.10.11.250
Host is up (0.11s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-02-03 14:08:55Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: analysis.htb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: analysis.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3306/tcp open  mysql         MySQL (unauthorized)
Service Info: Host: DC-ANALYSIS; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -2s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-02-03T14:09:13
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.85 seconds
```

fuzz

```
ffuf -c -u http://analysis.htb/ -H "Host: FUZZ.analysis.htb" -w /usr/share/wordlists/wfuzz/general/medium.txt -http2

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://analysis.htb/
 :: Wordlist         : FUZZ: /usr/share/wordlists/wfuzz/general/medium.txt
 :: Header           : Host: FUZZ.analysis.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

internal                [Status: 403, Size: 1268, Words: 74, Lines: 30, Duration: 181ms]
:: Progress: [1659/1659] :: Job [1/1] :: 151 req/sec :: Duration: [0:00:11] :: Errors: 0 ::

#Lo añadimos en /etc/hosts
internal.analysis.htb

#Nos dirigimos a: http://internal.analysis.htb/
```