Active

```
└─$ nmap -sC -sV -p 53,88,135,139,389,445,464,593,636,3268,3269,5722,9389 -oN allports_detailed.nmap 10.10.10.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-09 15:33 EDT
Nmap scan report for active.htb (10.10.10.100)
Host is up (0.095s latency).

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-09-09 19:33:58Z)
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: active.htb, 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: active.htb, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5722/tcp open  msrpc         Microsoft Windows RPC
9389/tcp open  mc-nmf        .NET Message Framing
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-09-09T19:34:48
|_  start_date: 2023-09-09T19:27:46
|_clock-skew: -8s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.25 seconds
```

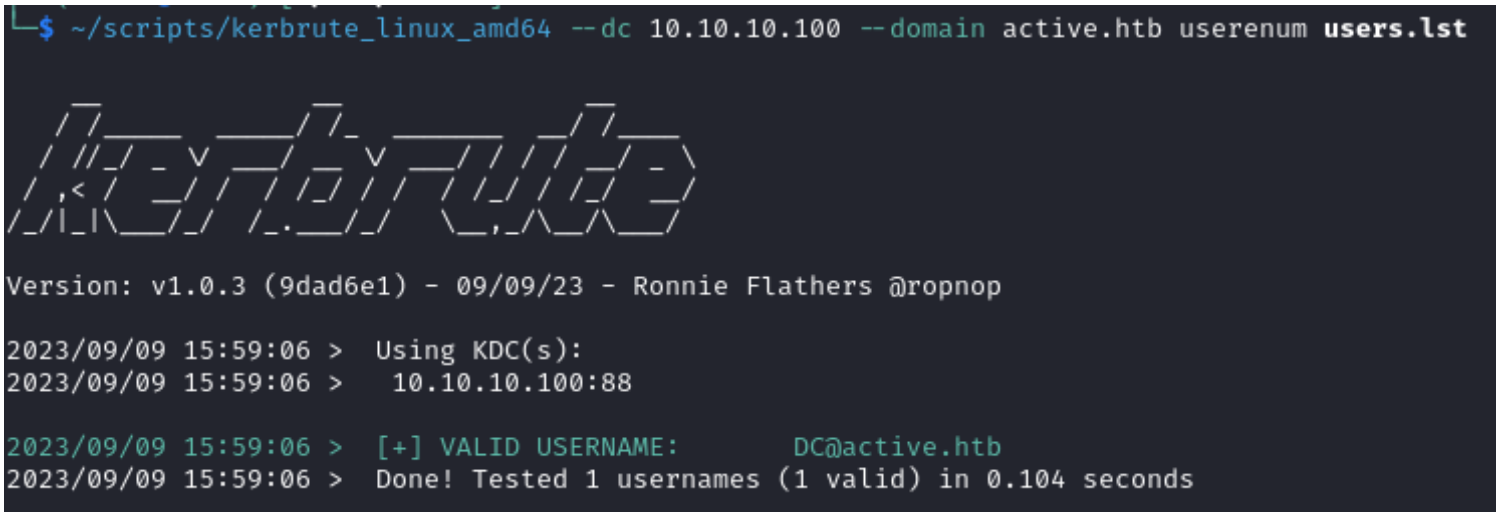
Enumeration

To start off, smb, ldap, and rpc do not allow anonymous access

smbclient -U '%' -L \\\\10.10.10.100\\ lists shares

smbclient -U '%' -N \\\\10.10.10.100\\Replication

```
└─$ crackmapexec smb 10.10.10.100
SMB         10.10.10.100    445    DC               [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
```



^not actually too interesting

Looking more closely at the Replication share, there is an xml file with a group policy cpassword which is easility decrypted useing gpp-decrypt

svc_tgs:GPPstillStandingStrong2k18

Using the creds, we can access svc_tgs's files via the “Users” share which we can read now, including the user flag

Using bloodhound, we see that Administrator is kerberoastable

Administrator:Ticketmaster1968