



# SharkFest '18 Europe



## **Kerberos: An Introduction**

by looking at packets!

Eddi Blenkers

@PcapReader



# About me?



- 15+ years of network analysis
- Currently IT Security

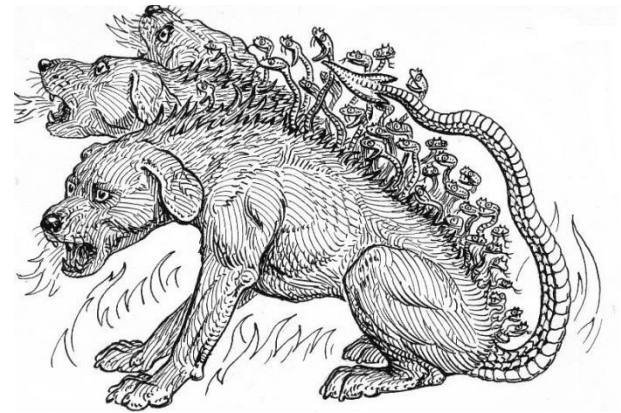




# About Kerberos



- Developed at MIT as part of the Athena project
- Offers authentication and authorization through a central server
- Widely used in Windows Domains
- UDP- and TCP-Port 88





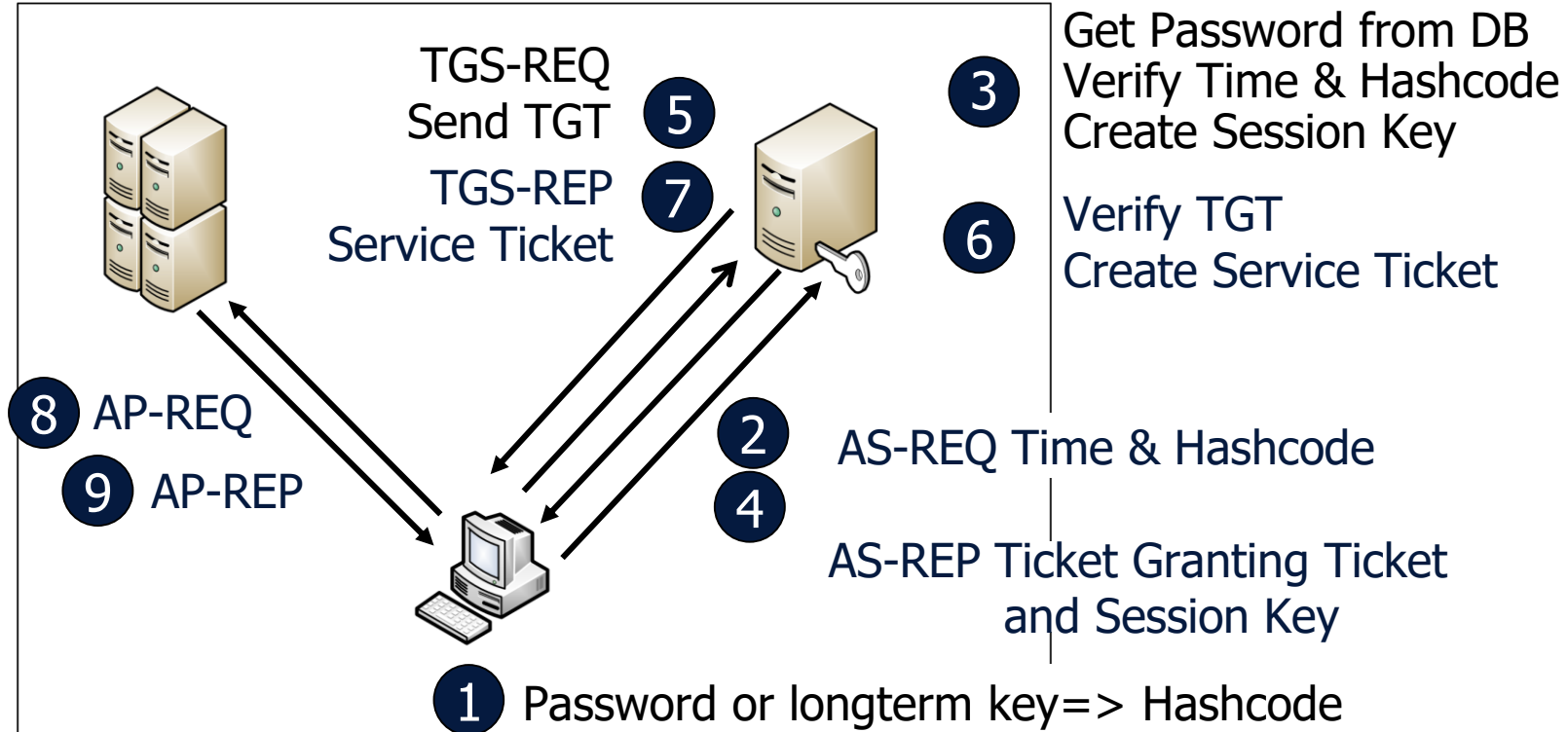
# Acronyms and Vocabulary



- Client Principle = The users Account Name
- Server Principle = The service desired by the user
- SPN = Service Principal Name
- KDC = Key Distribution Center  
Usually your Domain Controller



# Authentication Process





# The Wireshark View



- AS-REQ = User presents password, gets TGT
- TGS-REQ = User presents TGT, gets Service Ticket

| No.  | Time    | Source      | Protocol | SNameString                 | CNameString                | Info                                       |
|------|---------|-------------|----------|-----------------------------|----------------------------|--|
| 6516 | 747.622 | 10.20.20.20 | KRB5     | krbtgt,outerrिम.local       | darth.vader@outerrिम.local | AS-REQ                                     |
| 6517 | 747.641 | 10.1.1.2    | KRB5     | krbtgt,outerrिम.local       |                            | KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED    |
| 6524 | 747.671 | 10.20.20.20 | KRB5     | krbtgt,outerrिम.local       | darth.vader@outerrिम.local | AS-REQ                                     |
| 6526 | 747.691 | 10.1.1.2    | KRB5     | krbtgt,OUTERRIM.LOCAL       | darth.vader                | AS-REP                                     |
| 6535 | 747.712 | 10.20.20.20 | KRB5     | krbtgt,OUTERRIM.LOCAL,ho... |                            | TGS-REQ                                    |
| 6539 | 747.731 | 10.1.1.2    | KRB5     | host,tiefighter.outerrिम... | darth.vader                | TGS-REP                                    |
| 6547 | 747.842 | 10.20.20.20 | DCERPC   |                             |                            | Bind: call_id: 3, Fragment: Single, 3 cont |
| 6548 | 747.861 | 10.1.1.2    | DCERPC   |                             |                            | Bind_ack: call_id: 3, Fragment: Single, ma |



# Preauth Required?



- 1st AS-REQ should result in Preauth Required
- 2nd AS-REQ should be without error
- 2nd Request encrypts the current time with Password

| No.  | Time    | Source      | Protocol | SNameString                 | CNameString                | Info                                       |
|------|---------|-------------|----------|-----------------------------|----------------------------|--|
| 6516 | 747.622 | 10.20.20.20 | KRB5     | krbtgt,outerrim.local       | darth.vader@outerrim.local | AS-REQ                                     |
| 6517 | 747.641 | 10.1.1.2    | KRB5     | krbtgt,outerrim.local       |                            | KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED    |
| 6524 | 747.671 | 10.20.20.20 | KRB5     | krbtgt,outerrim.local       | darth.vader@outerrim.local | AS-REQ                                     |
| 6526 | 747.691 | 10.1.1.2    | KRB5     | krbtgt,OUTERRIM.LOCAL       | darth.vader                | AS-REP                                     |
| 6535 | 747.712 | 10.20.20.20 | KRB5     | krbtgt,OUTERRIM.LOCAL,ho... |                            | TGS-REQ                                    |
| 6539 | 747.731 | 10.1.1.2    | KRB5     | host,tiefighter.outerrim... | darth.vader                | TGS-REP                                    |
| 6547 | 747.842 | 10.20.20.20 | DCERPC   |                             |                            | Bind: call_id: 3, Fragment: Single, 3 cont |
| 6548 | 747.861 | 10.1.1.2    | DCERPC   |                             |                            | Bind_ack: call_id: 3, Fragment: Single, ma |



# Service Tickets



- Delivered in TGS-REP by the KDC
- TGS-REP is forwarded to desired service

| No.  | Time    | Source      | Protocol | SNameString                 | CNameString | Info                  |
|------|---------|-------------|----------|-----------------------------|-------------|-----------------------|
| 7226 | 769.222 | 10.20.20.20 | KRB5     | krbtgt,OUTERRIM.LOCAL,ci... |             | TGS-REQ               |
| 7229 | 769.242 | 10.1.1.2    | KRB5     | cifs,Tattoine               | darth.vader | TGS-REP               |
| 7232 | 769.242 | 10.20.20.20 | SMB2     | cifs,Tattoine               |             | Session Setup Request |

```
  v sname
    name-type: KRB5-NT-SRV-INST (2)
    v sname-string: 2 items
      SNameString: cifs
      SNameString: Tattoine
  v enc-part
    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    kvno: 1
    cipher: 397801138b1ea69335ded1034ba011605743f3fde80ad566...
```





# Encryption Algorithms



- Defined per GPO, avoid RC4 and DES
- Add AES for legacy systems after SW-Update

| No.  | Time    | Source      | Protocol | SNameString           | CNameString                | Info                                    |
|------|---------|-------------|----------|-----------------------|----------------------------|---|
| 6516 | 747.622 | 10.20.20.20 | KRB5     | krbtgt,outerrim.local | darth.vader@outerrim.local | AS-REQ                                  |
| 6517 | 747.641 | 10.1.1.2    | KRB5     | krbtgt,outerrim.local |                            | KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED |
| 6524 | 747.671 | 10.20.20.20 | KRB5     | krbtgt,outerrim.local | darth.vader@outerrim.local | AS-REQ                                  |
| 6526 | 747.691 | 10.1.1.2    | KRB5     | krbtgt,OUTERRIM.LOCAL | darth.vader                | AS-REP                                  |
| 6535 | 747.712 | 10.20.20.20 | KRB5     | krbtgt,OUTERRIM.LOCAL | ho                         | TGS-REQ                                 |

▼ etype: 6 items

```
ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
ENCTYPE: eTYPE-DES-CBC-MD5 (3)
```



# SharkFest '18 Europe



## Analyzing Kerberos With Wireshark

Eddi Blenkers

@PcapReader



# Message Type Numbers



- Kerberos identifies each message type with a code number

| No. | Abbreviation | Function                       |
|-----|--------------|--------------------------------|
| 10  | AS-REQ       | Request Ticket-Granting Ticket |
| 11  | AS-REP       | Ticket-Granting Ticket         |
| 12  | TGS-REQ      | Request Service Ticket         |
| 13  | TGS-REP      | Service Ticket                 |
| 30  | KRB-ERROR    | error                          |



# Kerberos Errors



- Kerberos traffic has a well-defined pattern:
  - AS-REQ followed by AS-REP
  - TGS-REQ followed by TGS-REP
- In case of an error, AS-REP or TGS-REP is replaced by an error message



# Typical Errors



- Client Principal Unknown  
→ Username unknown
- Service Principal Unknown  
→ Service or Hostname unknown

| No. | Time  | Source      | Protocol | CNameString                 | Info                                       |
|-----|-------|-------------|----------|-----------------------------|--|
| 76  | 2.540 | 10.20.20.20 | KRB5     | Kendal.Ozzel@outerrim.local | AS-REQ                                     |
| 77  | 2.558 | 10.1.1.1    | KRB5     |                             | KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN |



# Kerberos Display Filter



- Kerberos messages, including authentication to applications:

**kerberos**

- Only Kerberos messages, but exclude routine messages

**kerberos**

**and (tcp.port == 88 or udp.port == 88)**

**and not kerberos.msg\_type in {10 11 12 13}**



# Response Too Big



- Kerberos over UDP has a size limit
- Response too big forces the connection to TCP

| No. . | Time   | Source   | Destination | Info   |
|-------|--------|----------|-------------|--|
| 77    | 46.833 | 10.1.0.1 | 10.0.0.2    | AS-REQ   |
| 78    | 46.834 | 10.0.0.2 | 10.1.0.1    | KRB Error: KRB5KRB_ERR_RESPONSE_TOO_BIG                  |
| 79    | 46.834 | 10.1.0.1 | 10.0.0.2    | 1037 > 88 [SYN] Seq=0 win=65535 Len=0 MSS=1460           |
| 80    | 46.834 | 10.0.0.2 | 10.1.0.1    | 88 > 1037 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 |
| 81    | 46.835 | 10.1.0.1 | 10.0.0.2    | 1037 > 88 [ACK] Seq=1 Ack=1 Win=65535 Len=0              |
| 82    | 46.835 | 10.1.0.1 | 10.0.0.2    | AS-REQ   |
| 83    | 46.836 | 10.0.0.2 | 10.1.0.1    | AS-REP   |
| 84    | 46.836 | 10.1.0.1 | 10.0.0.2    | 1037 > 88 [FIN, ACK] Seq=307 Ack=1438 Win=64098 Len=0    |
| 85    | 46.836 | 10.0.0.2 | 10.1.0.1    | 88 > 1037 [ACK] Seq=1438 Ack=308 Win=64240 Len=0         |
| 86    | 46.836 | 10.0.0.2 | 10.1.0.1    | 88 > 1037 [RST, ACK] Seq=1438 Ack=308 Win=0 Len=0        |
| 87    | 46.838 | 10.1.0.1 | 10.0.0.2    | TGS-REQ  |
| 88    | 46.839 | 10.0.0.2 | 10.1.0.1    | TGS-REP  |



# SharkFest '18 Europe



## **Kerberos Advanced Topics**

Eddi Blenkers

@PcapReader





# Use Case: New File Server



- Like all computers, file servers are replaced
- If they get a new name, all shares have to be remapped: Scripts, Links etc.
- DNS Alias (CNAME) allow an easy migration
- Really?



# It works, does it?



| No. | Time  | Source      | Destination | Protocol | Length | Info   |
|-----|-------|-------------|-------------|----------|--------|--|
| 1   | 0.000 | 10.20.20.20 | 10.1.1.1    | DNS      | 80     | Standard query 0x85ea A yavin.outerrim.local   |
| 2   | 0.012 | 10.1.1.1    | 10.20.20.20 | DNS      | 115    | Standard query response 0x85ea A yavin.outerrim.local CNAME hoth.outerrim.local A 10.1.1.3 |

## DNS: Locate Servers IP Adress

|   |       |             |             |      |     |                             |
|---|-------|-------------|-------------|------|-----|-----------------------------|
| 6 | 0.032 | 10.20.20.20 | 10.1.1.3    | SMB  | 213 | Negotiate Protocol Request  |
| 7 | 0.052 | 10.1.1.3    | 10.20.20.20 | SMB2 | 306 | Negotiate Protocol Response |
| 8 | 0.052 | 10.20.20.20 | 10.1.1.3    | SMB2 | 232 | Negotiate Protocol Request  |
| 9 | 0.072 | 10.1.1.3    | 10.20.20.20 | SMB2 | 366 | Negotiate Protocol Response |

## Establish SMB Session

|    |       |             |             |      |      |   |
|----|-------|-------------|-------------|------|------|---|
| 13 | 0.092 | 10.20.20.20 | 10.1.1.2    | KRB5 | 1079 | TGS-REQ   |
| 14 | 0.112 | 10.1.1.2    | 10.20.20.20 | TCP  | 60   | 88 → 56457 [ACK] Seq=1 Ack=1626 Win=65536 Len=0 |
| 15 | 0.112 | 10.1.1.2    | 10.20.20.20 | KRB5 | 161  | KRB Error: KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN      |

## SMB Session works. User is happy.

|    |       |             |             |      |     |   |
|----|-------|-------------|-------------|------|-----|---|
| 19 | 0.212 | 10.20.20.20 | 10.1.1.3    | SMB2 | 220 | Session Setup Request, NTLMSSP_NEGOTIATE  |
| 20 | 0.232 | 10.1.1.3    | 10.20.20.20 | SMB2 | 387 | Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE |
| 21 | 0.233 | 10.20.20.20 | 10.1.1.3    | SMB2 | 701 | Session Setup Request, NTLMSSP_AUTH, User: OUTERRIM\drk-1                         |
| 22 | 0.262 | 10.1.1.3    | 10.20.20.20 | SMB2 | 159 | Session Setup Response  |
| 23 | 0.263 | 10.20.20.20 | 10.1.1.3    | SMB2 | 184 | Tree Connect Request Tree: \\yavin.outerrim.local\IPC\$                           |
| 24 | 0.282 | 10.1.1.3    | 10.20.20.20 | SMB2 | 138 | Tree Connect Response   |
| 25 | 0.282 | 10.20.20.20 | 10.1.1.3    | SMB2 | 178 | Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO                                  |
| 26 | 0.282 | 10.20.20.20 | 10.1.1.3    | SMB2 | 190 | Create Request File: wksvc  |



# What really happens ...



| No. | Time  | Source      | Destination | Protocol | Length | Info   |
|-----|-------|-------------|-------------|----------|--------|--|
| 1   | 0.000 | 10.20.20.20 | 10.1.1.1    | DNS      | 80     | Standard query 0x85ea A yavin.outerrim.local   |
| 2   | 0.012 | 10.1.1.1    | 10.20.20.20 | DNS      | 115    | Standard query response 0x85ea A yavin.outerrim.local CNAME hoth.outerrim.local A 10.1.1.3 |
| 3   | 0.014 | 10.20.20.20 | 10.1.1.3    | TCP      | 66     | 56456 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                        |
| 4   | 0.032 | 10.1.1.3    | 10.20.20.20 | TCP      | 66     | 445 → 56456 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1              |
| 5   | 0.032 | 10.20.20.20 | 10.1.1.3    | TCP      | 60     | 56456 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0  |
| 6   | 0.032 | 10.20.20.20 | 10.1.1.3    | SMB      | 213    | Negotiate Protocol Request   |
| 7   | 0.052 | 10.1.1.3    | 10.20.20.20 | SMB2     | 306    | Negotiate Protocol Response  |
| 8   | 0.052 | 10.20.20.20 | 10.1.1.3    | SMB2     | 232    | Negotiate Protocol Request   |
| 9   | 0.072 | 10.1.1.3    | 10.20.20.20 | SMB2     | 366    | Negotiate Protocol Response  |
| 10  | 0.073 | 10.20.20.20 | 10.1.1.2    | TCP      | 66     | 56457 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                         |
| 11  | 0.092 | 10.1.1.2    | 10.20.20.20 | TCP      | 66     | 88 → 56457 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1               |
| 12  | 0.092 | 10.20.20.20 | 10.1.1.2    | TCP      | 60     | 56457 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0   |
| 13  | 0.092 | 10.20.20.20 | 10.1.1.2    | KRB5     | 1679   | TGS-REQ  |
| 14  | 0.112 | 10.1.1.2    | 10.20.20.20 | TCP      | 60     | 88 → 56457 [ACK] Seq=1 Ack=1626 Win=65536 Len=0  |
| 15  | 0.112 | 10.1.1.2    | 10.20.20.20 | KRB5     | 161    | KRB Error: KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN   |

SNameString: cifs  
SNameString: yavin.outerrim.local



# ... could be more secure



| No. | Time  | Source      | Destination | Protocol | Length | Info  |
|-----|-------|-------------|-------------|----------|--------|---|
| 19  | 0.212 | 10.20.20.20 | 10.1.1.3    | SMB2     | 220    | Session Setup Request, NTLMSSP_NEGOTIATE  |
| 20  | 0.232 | 10.1.1.3    | 10.20.20.20 | SMB2     | 387    | Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE |
| 21  | 0.233 | 10.20.20.20 | 10.1.1.3    | SMB2     | 701    | Session Setup Request, NTLMSSP_AUTH, User: OUTERRIM\drk-1                         |
| 22  | 0.262 | 10.1.1.3    | 10.20.20.20 | SMB2     | 159    | Session Setup Response  |
| 23  | 0.263 | 10.20.20.20 | 10.1.1.3    | SMB2     | 184    | Tree Connect Request Tree: \\yavin.outerrim.local\IPC\$                           |
| 24  | 0.282 | 10.1.1.3    | 10.20.20.20 | SMB2     | 138    | Tree Connect Response   |

- NTLM Secure Service Provider
  - NTLMSSP identifier: NTLMSSP
  - NTLM Message Type: NTLMSSP\_AUTH (0x00000003)
  - Lan Manager Response: 00000000000000000000000000000000
  - LMv2 Client Challenge: 0000000000000000
- NTLM Response: 56b76966c6bd9cb91e4875078267d97401010
  - Length: 340
  - Maxlen: 340
  - Offset: 158

Susceptible to a  
Man-in-the-Middle attack

NTLMv2 Response: 56b76966c6bd9cb91e4875078267d974010100000000000...

NTProofStr: 56b76966c6bd9cb91e4875078267d974

Response Version: 1

Hi Response Version: 1

Z: 000000000000

Time: Oct 31, 2018 13:42:24.975148200 UTC

NTLMv2 Client Challenge: 0facebcaafb150f3



# Solution



Run this command on the target computer:

```
C:\> netdom computername hoth.outerrim.local  
      /add:yavin.outerrim.local
```

Verify the results:

```
C:\> netdom computername hoth /enum
```



# Delegation



- Kerberos tickets can be forwarded from a frontend server to a backend system
- Classic Example:  
Webserver forwards ticket to an SQL server  
→ This is called "delegation"
- S4U2P = Service for User to Proxy  
Constrained or Unconstrained Delegation



# Delegation



- Not for users in the group "Protected Users"
- Can be unconstrained or constrained
- Constrained delegation limits services who can forward tickets or process forwarded tickets



# The Wireshark View



Filter: `kerberos and (tcp.port == 88 or udp.port == 88)` Expression... Clear Apply

| No. | Time   | Source     | Destination | Info   |
|-----|--------|------------|-------------|--|
| 426 | 37.039 | 10.0.0.2   | 10.0.100.2  | TGS-REP  |
| 436 | 37.043 | 10.0.100.2 | 10.0.0.2    | TGS-REQ  |
| 440 | 37.044 | 10.0.0.2   | 10.0.100.2  | KRB Error: KRB5KDC_ERR_BADOPTION NT Status: STATUS_NOT_SUPPORTED |
| 463 | 37.058 | 10.0.100.2 | 10.0.0.2    | TGS-REQ  |
| 466 | 37.062 | 10.0.0.2   | 10.0.100.2  | TGS-REP  |

[-] Kerberos TGS-REQ

- [-] Record Mark: 2337 bytes
  - Pvno: 5
  - MSG Type: TGS-REQ (12)
- [-] padata: PA-TGS-REQ
- [-] KDC\_REQ\_BODY
  - Padding: 0
  - [-] KDCOptions: 40830000 (Forwardable, Renewable, **Constrained Delegation**, Canonicalize)
  - Realm: TEST.DE
  - [-] Server Name (Enterprise Name): pc-hq-win7\$@TEST.DE





# Website Worth a Bookmark



- Noteworthy blog from Will "harmj0y" Schroeder
- <https://posts.specterops.io/another-word-on-delegation-10bdb3cd94a>





# SharkFest '18 Europe



## **Tales from the Mos Eisley Cantina Episode 1: The Bloated Ticket**

Eddi Blenkers

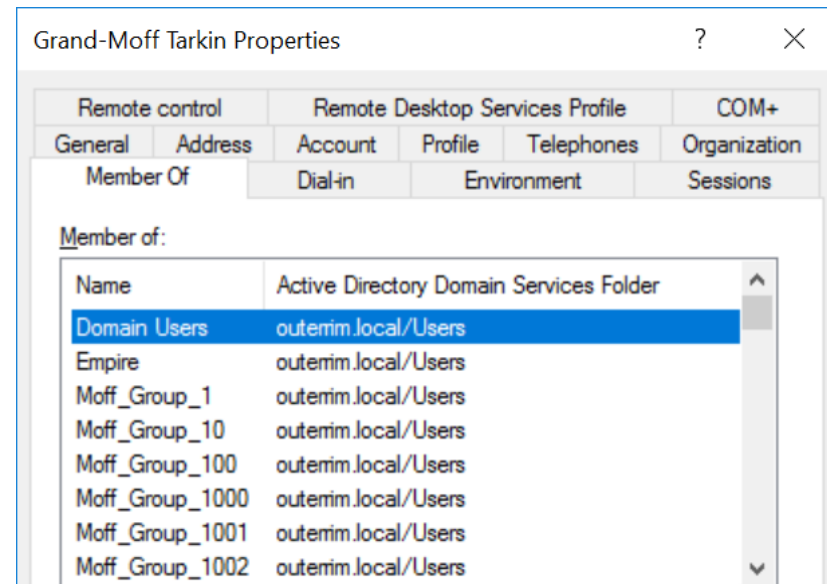
@PcapReader



# Beware of Large Tickets



- Tickets should be max. 48.000 Byte
- Users should be a member in max. 1.015 groups





# Odd on the Command Line



```
C:\> net user grand-moff.tarkin /domain  
System error 1783 has occurred.
```

**The stub received bad data.**


```
C:\> net user luke.skywalker /domain  
User name           luke.skywalker  
Full Name           Luke Skywalker  
...
```



# Odd in the GUI




Remote Desktop Connection

 An authentication error has occurred.  
During a logon attempt, the user's security context accumulated too many security IDs.

Remote computer: 10.20.20.20

OK

Windows

 The mapped network drive could not be created because the following error has occurred:

During a logon attempt, the user's security context accumulated too many security IDs.

OK



# Kerberos Parameters



- HKLM\System\CurrentControlSet  
\Control\Lsa\Kerberos\Parameters
- Value name: **MaxTokenSize**  
Data type: **REG\_DWORD**  
Radix: **Decimal**  
Value data: **48000**





# SharkFest '18 Europe



## **Tales from the Mos Eisley Cantina Episode 2: Infiltrating a Network**

Eddi Blenkers

@PcapReader



# The Command Line



```
C:\> net use \\hoth.outerrim.local\c$  
/user:Kendal.Ozzel@outerrim.local abc
```

System error 86 has occurred.

The specified network password is not correct.





# The Wireshark View



- Different Return Codes for wrong password or for non-existing users

| No. | Time  | Source      | Protocol | CNameString                    | Info                                       |
|-----|-------|-------------|----------|--------------------------------|--|
| 76  | 2.540 | 10.20.20.20 | KRB5     | Kendal.Ozzel@outerrim.local    | AS-REQ                                     |
| 77  | 2.558 | 10.1.1.1    | KRB5     |                                | KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN |
| 92  | 2.799 | 10.20.20.20 | KRB5     | Moradmin.Bast@outerrim.local   | AS-REQ                                     |
| 93  | 2.818 | 10.1.1.1    | KRB5     |                                | KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN |
| 116 | 3.199 | 10.20.20.20 | KRB5     | Tiaan.Jerjerrod@outerrim.local | AS-REQ                                     |
| 117 | 3.218 | 10.1.1.1    | KRB5     |                                | KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED    |
| 124 | 3.238 | 10.20.20.20 | KRB5     | Tiaan.Jerjerrod@outerrim.local | AS-REQ                                     |
| 125 | 3.258 | 10.1.1.1    | KRB5     |                                | KRB Error: KRB5KDC_ERR_PREAUTH_FAILED      |
| 148 | 3.628 | 10.20.20.20 | KRB5     | Gial.Ackbar@outerrim.local     | AS-REQ                                     |
| 149 | 3.648 | 10.1.1.1    | KRB5     |                                | KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN |
| 180 | 4.048 | 10.20.20.20 | KRB5     | Cassian.Andor@outerrim.local   | AS-REQ                                     |
| 181 | 4.068 | 10.1.1.1    | KRB5     |                                | KRB Error: KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN |



# SharkFest '18 Europe



## Tales from the Mos Eisley Cantina Episode 3: Kerberoast

More Network Intfiltration

Eddi Blenkers

@PcapReader



# Kerberoast



- Powershell script that requests all available service tickets from a domain
- Output from the Powershell script can be processed by "John the Ripper" to reveal the password for the service account



# The Wireshark View



- Watch out for a large number of service requests in quick succession
- Especially interesting if coming from an usual source

| No.  | Time   | Source      | Destination | Protocol | CNameString | SNameString   | Info    |
|------|--------|-------------|-------------|----------|-------------|---|---------|
| 1728 | 22.069 | 10.20.20.20 | 10.1.1.2    | KRB5     |             | krbtgt,OUTERRIM.LOCAL,HTTP,kashyyyk.outerrim.local    | TGS-REQ |
| 1742 | 22.089 | 10.1.1.2    | 10.20.20.20 | KRB5     | darth.vader | HTTP,kashyyyk.outerrim.local                          | TGS-REP |
| 1750 | 22.129 | 10.20.20.20 | 10.1.1.2    | KRB5     |             | krbtgt,OUTERRIM.LOCAL,SQL,coruscant.outerrim.local    | TGS-REQ |
| 1757 | 22.149 | 10.1.1.2    | 10.20.20.20 | KRB5     | darth.vader | SQL,coruscant.outerrim.local                          | TGS-REP |
| 1765 | 22.259 | 10.20.20.20 | 10.1.1.2    | KRB5     |             | krbtgt,OUTERRIM.LOCAL,SWINVENTORY,hoth.outerrim.local | TGS-REQ |
| 1768 | 22.279 | 10.1.1.2    | 10.20.20.20 | KRB5     | darth.vader | SWINVENTORY,hoth.outerrim.local                       | TGS-REP |



# SharkFest '18 Europe



## **Tales from the Mos Eisley Cantina Episode 4: Golden & Silver Ticket**

Eddi Blenkers

@PcapReader



# Golden Tickets



- The "Golden Ticket" is a forged TGT
- Allows requesting tickets for all services
- Requires privileged access to a DC
- Use mimikatz
  - Obtain the password hash for the account krbtgt
  - Use this hash to forge a TGT
  - The KDC will not notice, that it didn't issue this TGT



# Visibility in Wireshark



- Interesting things happen in memory, not on the network
- Not really a case for Wireshark



# Silver Tickets



- Requires knowledge of the password for a service account (Remember Kerberoast?)
- Use the password to forge a service ticket





# Visibility in Wireshark



- Again, interesting things happen in memory.
- The service tickets just happen to be there.
- You might notice the ticket being presented without a TGS-REQ.
  - The ticket could be cached from an earlier request.
  - A full capture from the workstation should reveal a backdoor and other attacker activities.



# More on Golden Tickets



One of many articles on the web:

<https://digital-forensics.sans.org/blog/2014/11/24/kerberos-in-the-crosshairs-golden-tickets-silver-tickets-mitm-more>





# SharkFest '18 Europe



## **Kerberos More Advanced Topics**

Eddi Blenkers

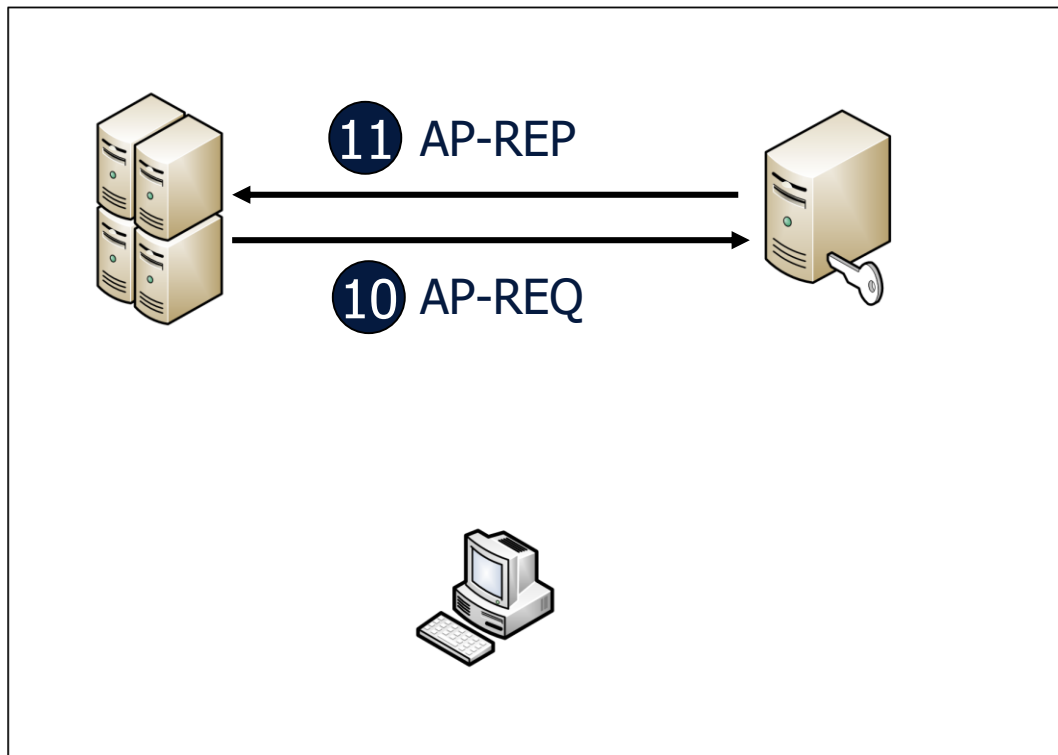
@PcapReader



# Privilege Account Certificate



- Allows the Server to verify if a ticket has been tampered with.
- Only checked if ...
  - application has the SeTcbPrivilege privilege "Act as part of the operating system"
  - application is a service
  - Kerberos config doesn't prevent PAC check





# PAC



- <https://blogs.msdn.microsoft.com/openspecification/2009/04/24/understanding-microsoft-kerberos-pac-validation/>





# Questions?