AHMAD ALLOBANI

SARA ISAID

SAJA MATAR

DELEGATION

IN ACTIVE DIRECTORY

AUTHENTICATION COURSE

Business Need

The **University of Jordan (JU)** needed a secure and organized way for its employees to share files within their departments.

To address this, **a web portal** was developed, allowing employees to:

- Log in using their university credentials
- View and download files specific to their department
- Ensure that no other departments can view their resources

Portal Requirements

What are the key security and access requirements for the portal?

Access Control

Enforce strict departmental isolation. Employees should only access file shares belonging to their own department, based on predefined permissions.

Authentication

Ensure all users are securely authenticated through Active Directory, maintaining centralized identity management and domain trust.e identity verification via Active Directory

Auditing

Monitor and log all access events to file shares for accountability, security investigations, and compliance with internal policy.

Departmental Access Control (ACL Configuration)

SECURITY CONCERNS

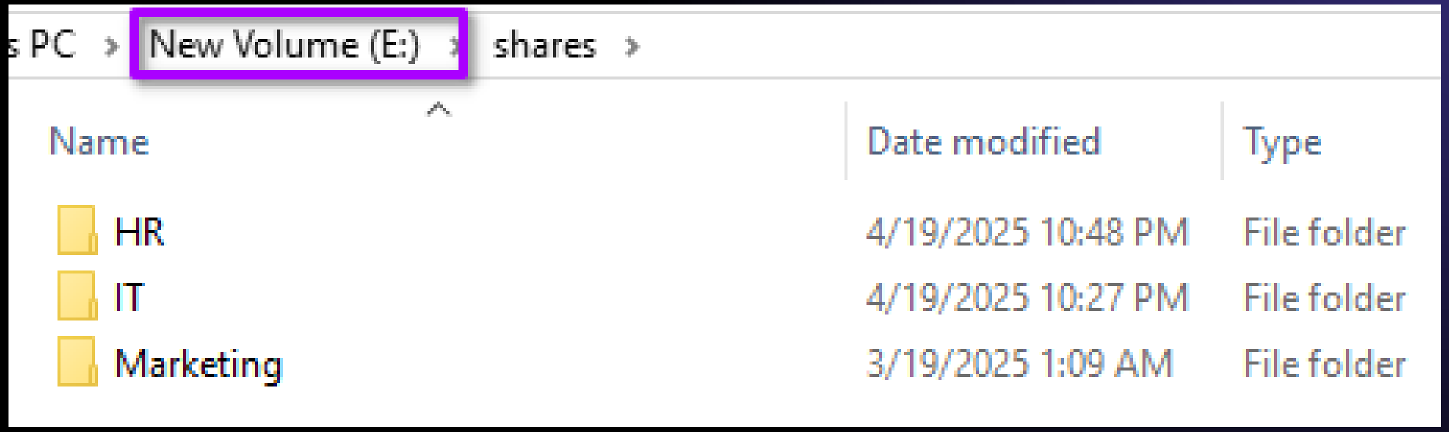
a dedicated partition was created on the File Server to store departmental data. This prevents unauthorized access across volumes and simplifies permission management.

DEPARTMENT MANAGEMENT

Separate AD security groups were created for each department. Users were added based on their department, and these groups were used to enforce folder-level access through ACLs.

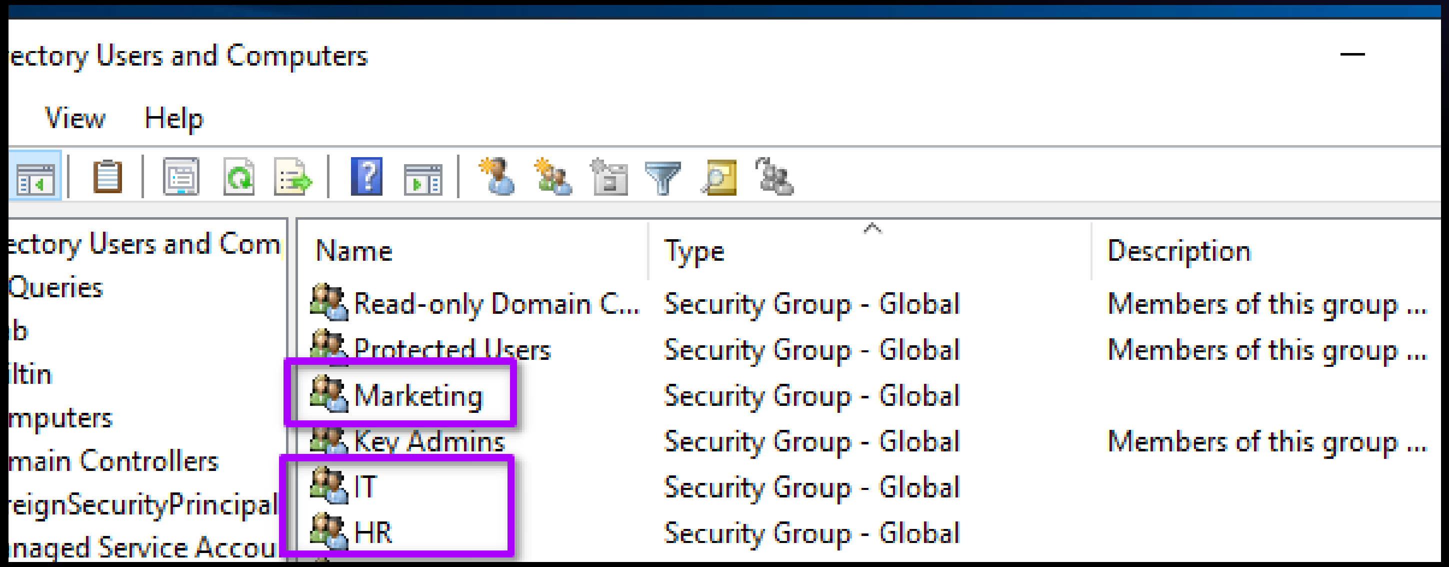
NTFS PERMISSIONS (ACLS)

These ACLs define which users or groups can read, write, or modify the contents of each folder. Only members of the corresponding Active Directory security group were granted access to their department's folder.

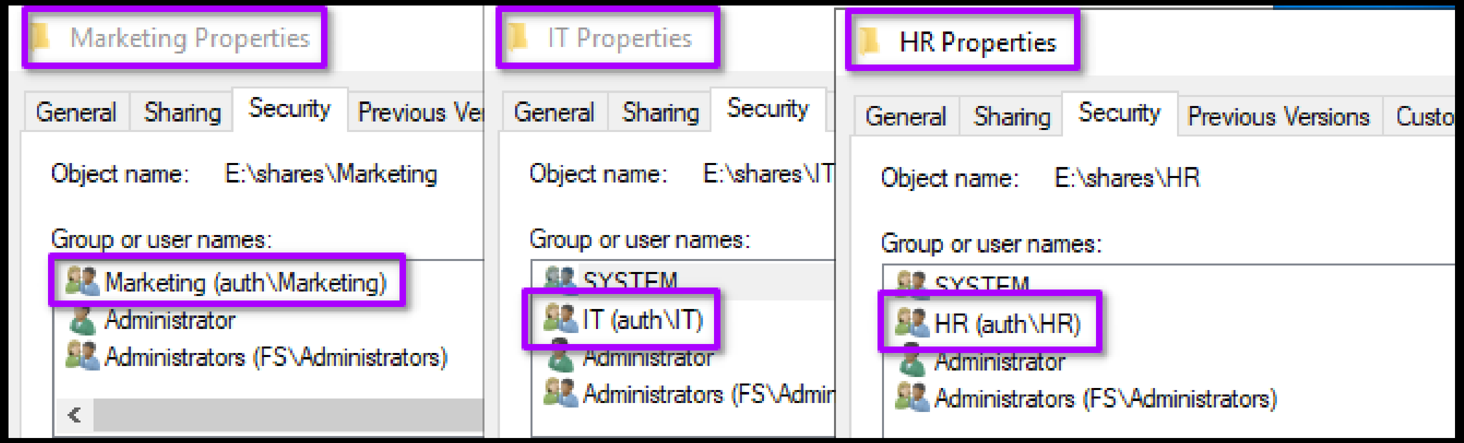


s PC › New Volume (E:) › shares ›

Name	Date modified	Type
HR	4/19/2025 10:48 PM	File folder
IT	4/19/2025 10:27 PM	File folder
Marketing	3/19/2025 1:09 AM	File folder



Name	Type	Description
Read-only Domain C...	Security Group - Global	Members of this group ...
Protected Users	Security Group - Global	Members of this group ...
Marketing	Security Group - Global	
Key Admins	Security Group - Global	Members of this group ...
IT	Security Group - Global	
HR	Security Group - Global	



Marketing Properties

Object name: E:\shares\Marketing

Group or user names:
Marketing (auth\Marketing)
Administrator
Administrators (FS\Administrators)

IT Properties

Object name: E:\shares\IT

Group or user names:
SYSTEM
IT (auth\IT)
Administrator
Administrators (FS\Admin

HR Properties

Object name: E:\shares\HR

Group or user names:
SYSTEM
HR (auth\HR)
Administrator
Administrators (FS\Administrators)

Technical Architecture

The environment simulates a classic multi-tier enterprise setup. The IIS server acts as the frontend, but cannot directly access file resources secured by ACLs without proper delegation. Kerberos handles authentication, but faces limitations in multi-hop scenarios — which we'll explore in the next slide

WEB TIER: IIS SERVER

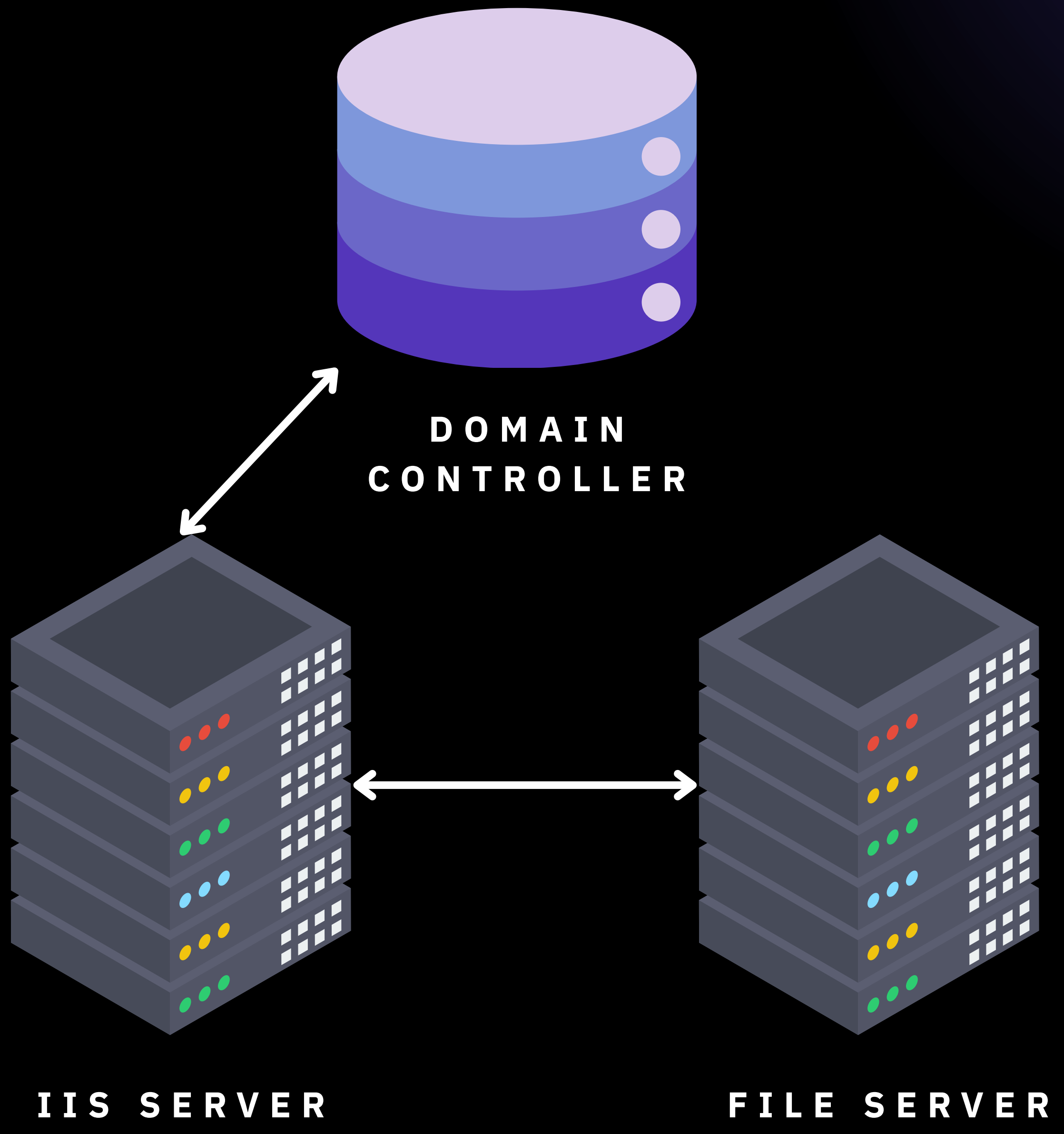
Front-End component.

STORAGE TIER: FILE SERVER

Back-end component

AUTHENTICATION TIER: DOMAIN CONTROLLER

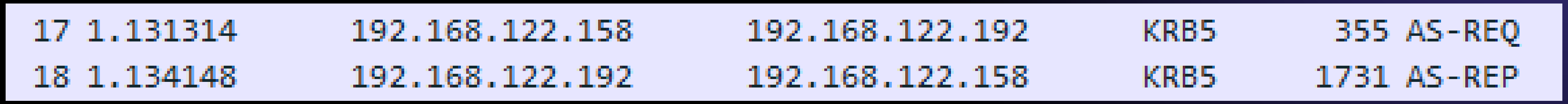
Heart of active directory.



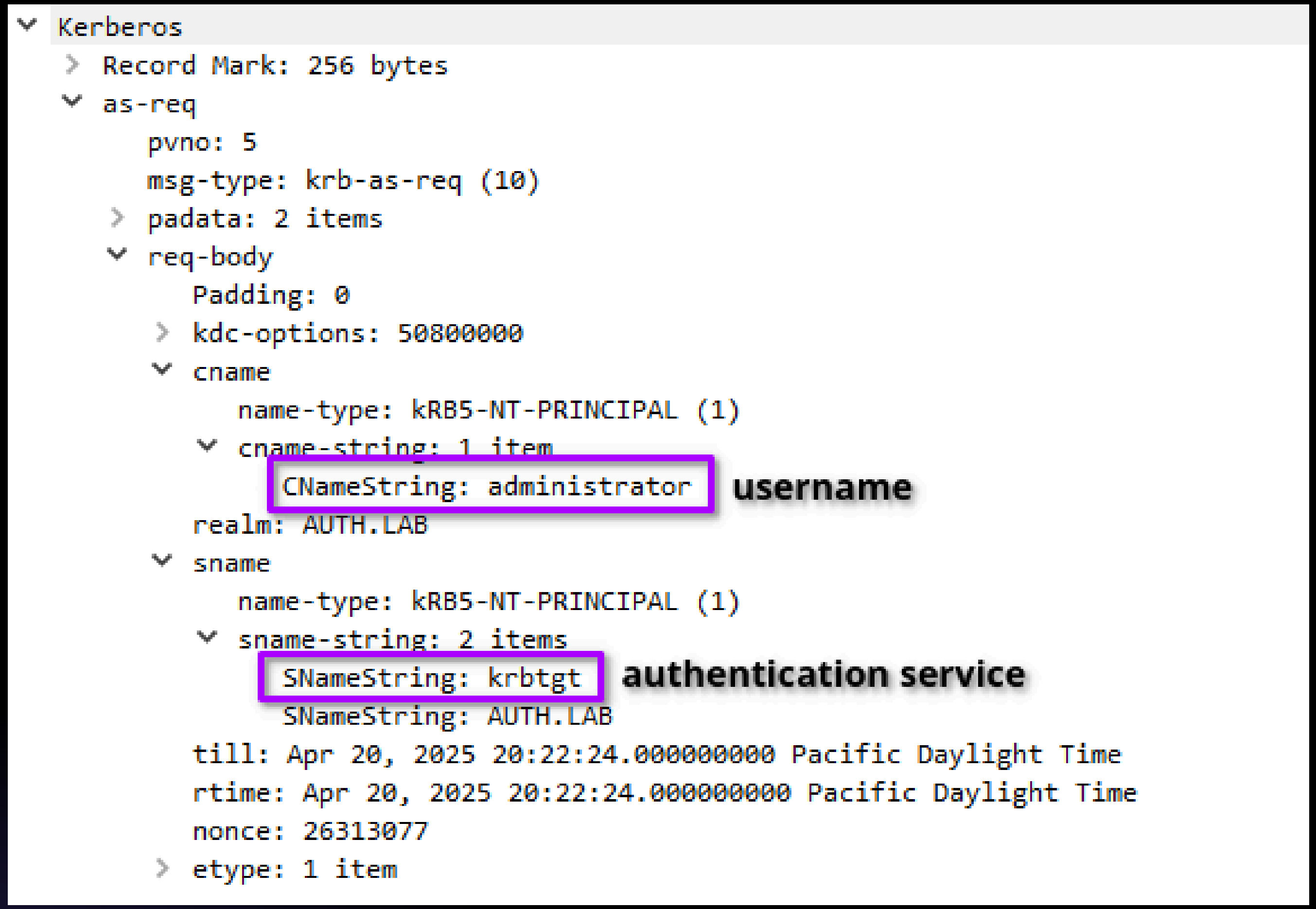
Kerberos Authentication Flow

USER LOGS IN TO THE DOMAIN

The user obtains a Ticket Granting Ticket (TGT) from the Domain Controller (DC) using their username and password (Kerberos AS-REQ / AS-REP).



```
17 1.131314      192.168.122.158     192.168.122.192     KRB5     355 AS-REQ
18 1.134148      192.168.122.192     192.168.122.158     KRB5    1731 AS-REP
```

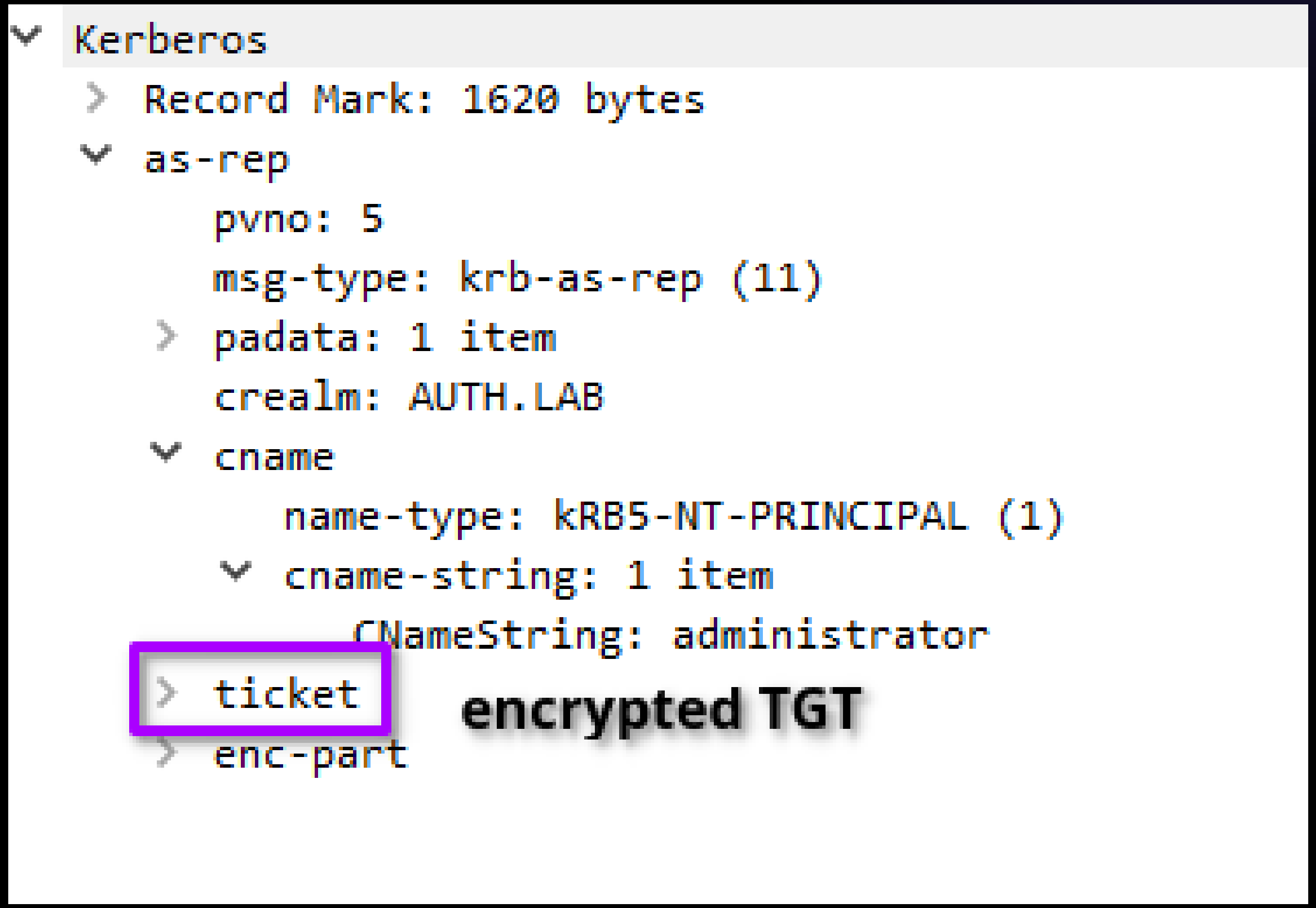


```
v Kerberos
  > Record Mark: 256 bytes
  v as-req
      pvno: 5
      msg-type: krb-as-req (10)
    > padata: 2 items
    v req-body
        Padding: 0
      > kdc-options: 50800000
      v cname
          name-type: kRB5-NT-PRINCIPAL (1)
        v cname-string: 1 item
            CNameString: administrator
        realm: AUTH.LAB
      v sname
          name-type: kRB5-NT-PRINCIPAL (1)
        v sname-string: 2 items
            SNameString: krbtgt
            SNameString: AUTH.LAB
        till: Apr 20, 2025 20:22:24.000000000 Pacific Daylight Time
        rtime: Apr 20, 2025 20:22:24.000000000 Pacific Daylight Time
        nonce: 26313077
      > etype: 1 item
```

username

authentication service

TGT REQUEST



```
v Kerberos
  > Record Mark: 1620 bytes
  v as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
    > padata: 1 item
      crealm: AUTH.LAB
    v cname
        name-type: kRB5-NT-PRINCIPAL (1)
      v cname-string: 1 item
          CNameString: administrator
    > ticket
    > enc-part
```

encrypted TGT

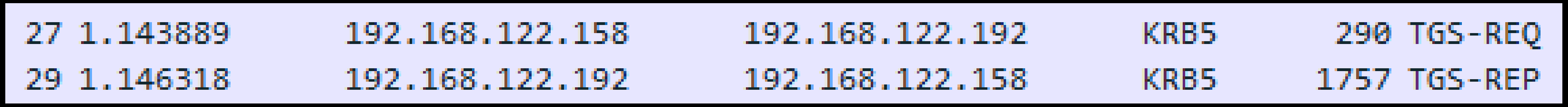
TGT REPLY

AUTHENTICATION COURSE

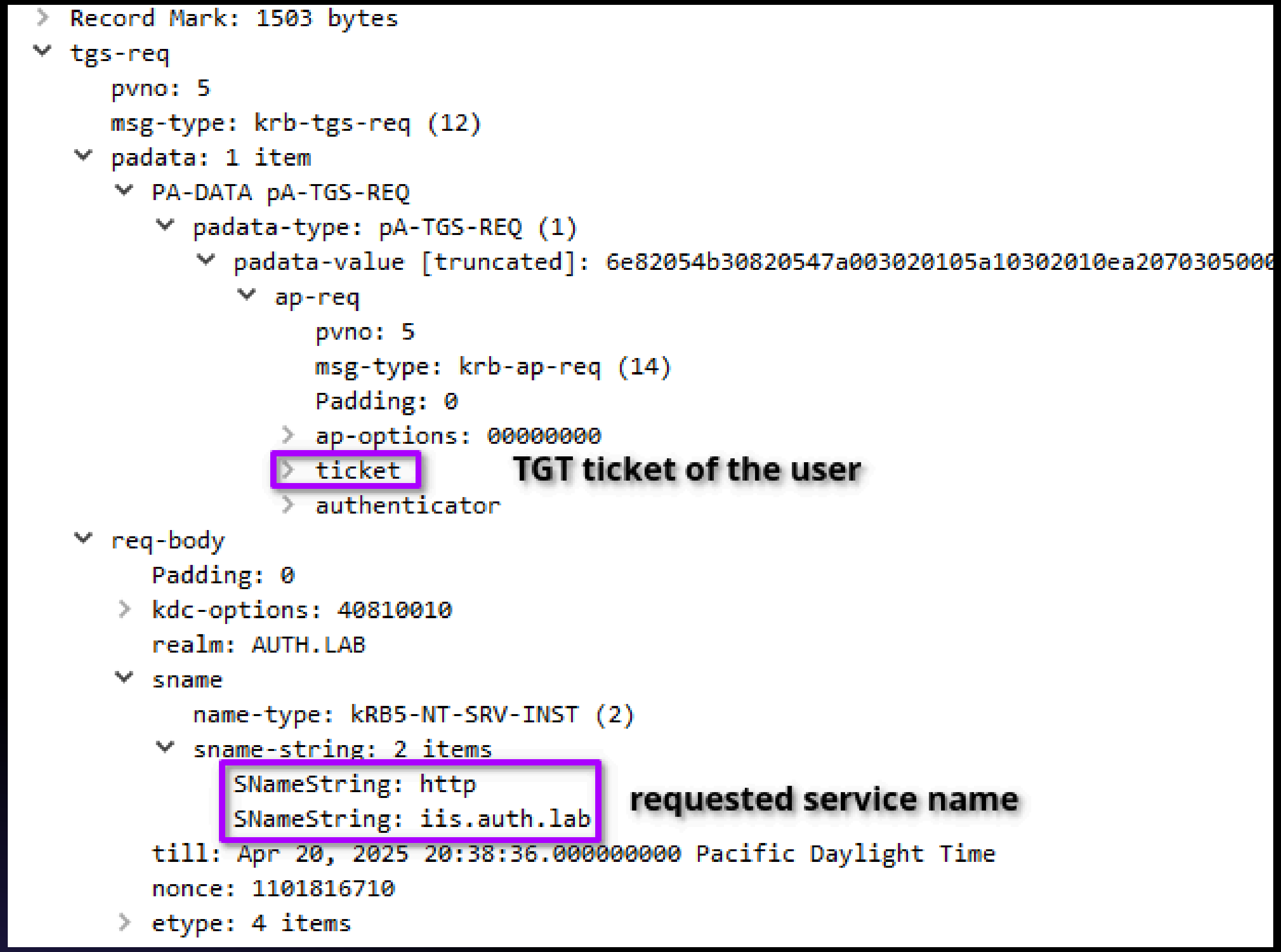
Kerberos Authentication Flow

USER ACCESSES THE SERVER (IIS SERVER)

The browser sends the user TGT to the DC and requests a Service Ticket (TGS) for the IIS web application. (Kerberos TGS-REQ / TGS-REP).



```
27 1.143889     192.168.122.158     192.168.122.192     KRB5      290 TGS-REQ
29 1.146318     192.168.122.192     192.168.122.158     KRB5     1757 TGS-REP
```

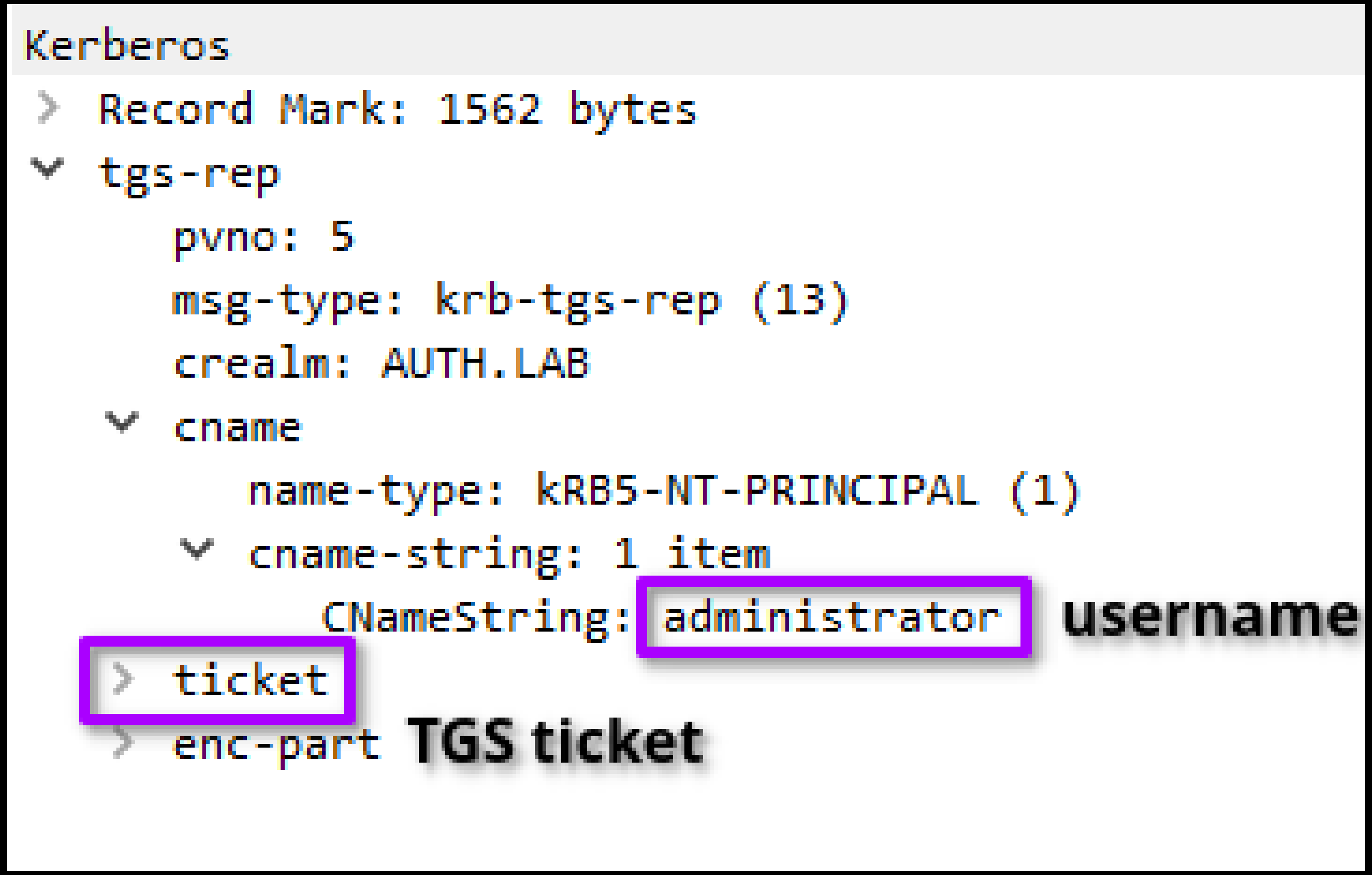


```
> Record Mark: 1503 bytes
v tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
  v padata: 1 item
    v PA-DATA pA-TGS-REQ
      v padata-type: pA-TGS-REQ (1)
        v padata-value [truncated]: 6e82054b30820547a003020105a10302010ea2070305000
          v ap-req
              pvno: 5
              msg-type: krb-ap-req (14)
              Padding: 0
            > ap-options: 00000000
            > ticket
            > authenticator
  v req-body
      Padding: 0
    > kdc-options: 40810010
      realm: AUTH.LAB
    v sname
        name-type: kRB5-NT-SRV-INST (2)
      v sname-string: 2 items
          SNameString: http
          SNameString: iis.auth.lab
      till: Apr 20, 2025 20:38:36.000000000 Pacific Daylight Time
      nonce: 1101816710
    > etype: 4 items
```

TGT ticket of the user

requested service name

TGS REQUEST



```
Kerberos
> Record Mark: 1562 bytes
v tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: AUTH.LAB
  v cname
      name-type: kRB5-NT-PRINCIPAL (1)
    v cname-string: 1 item
        CNameString: administrator
  > ticket
  > enc-part
```

username

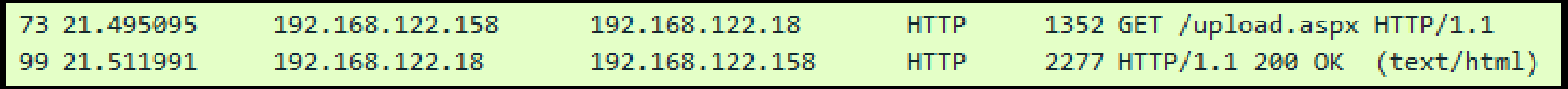
TGS ticket

TGS REPLY

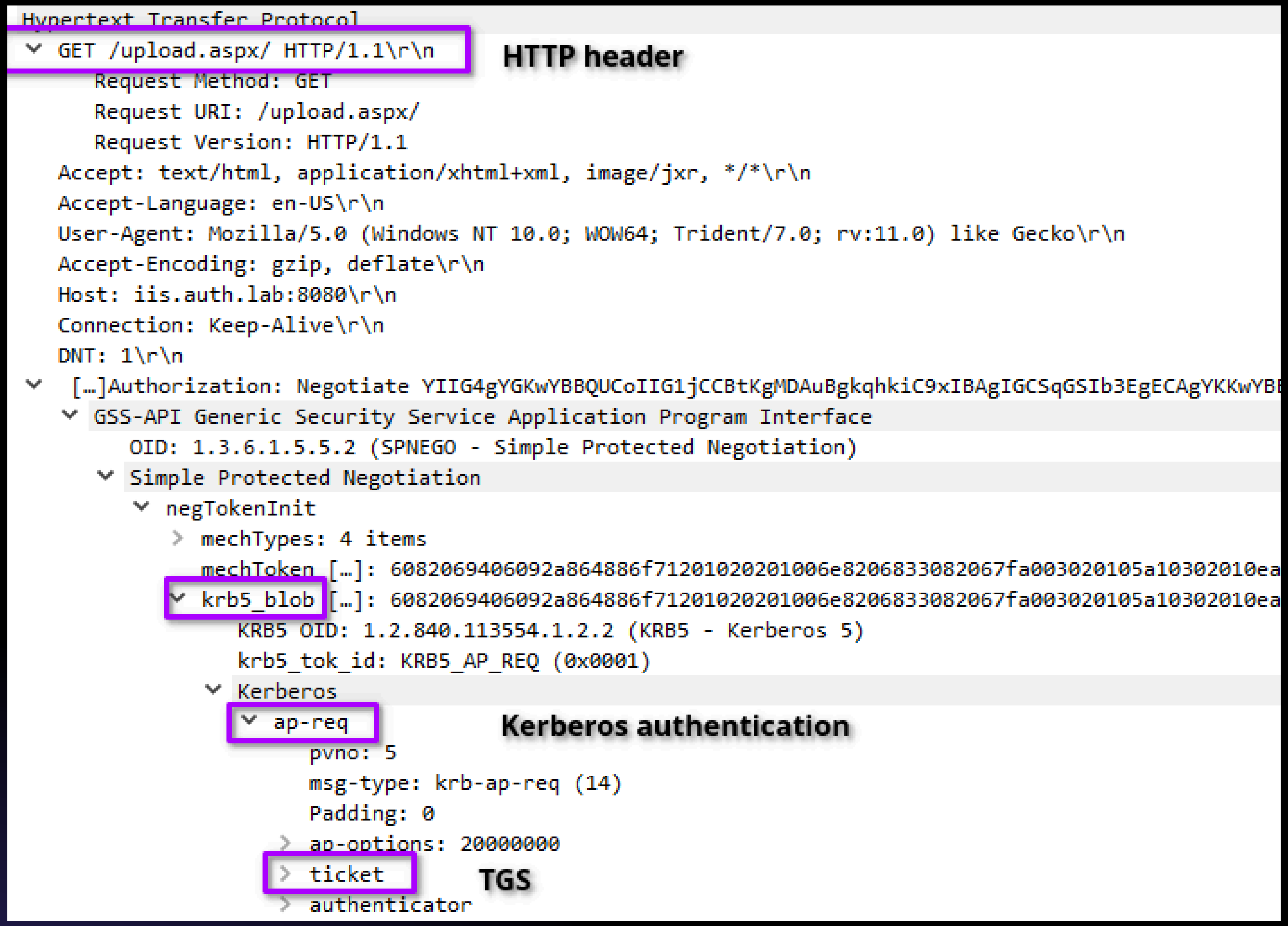
Kerberos Authentication Flow

USER ACCESSES THE SERVER (IIS SERVER)

The user presents the obtained Service Ticket (TGS) to the IIS server to authenticate and use the service. (Kerberos AP-REQ / AP-REP)

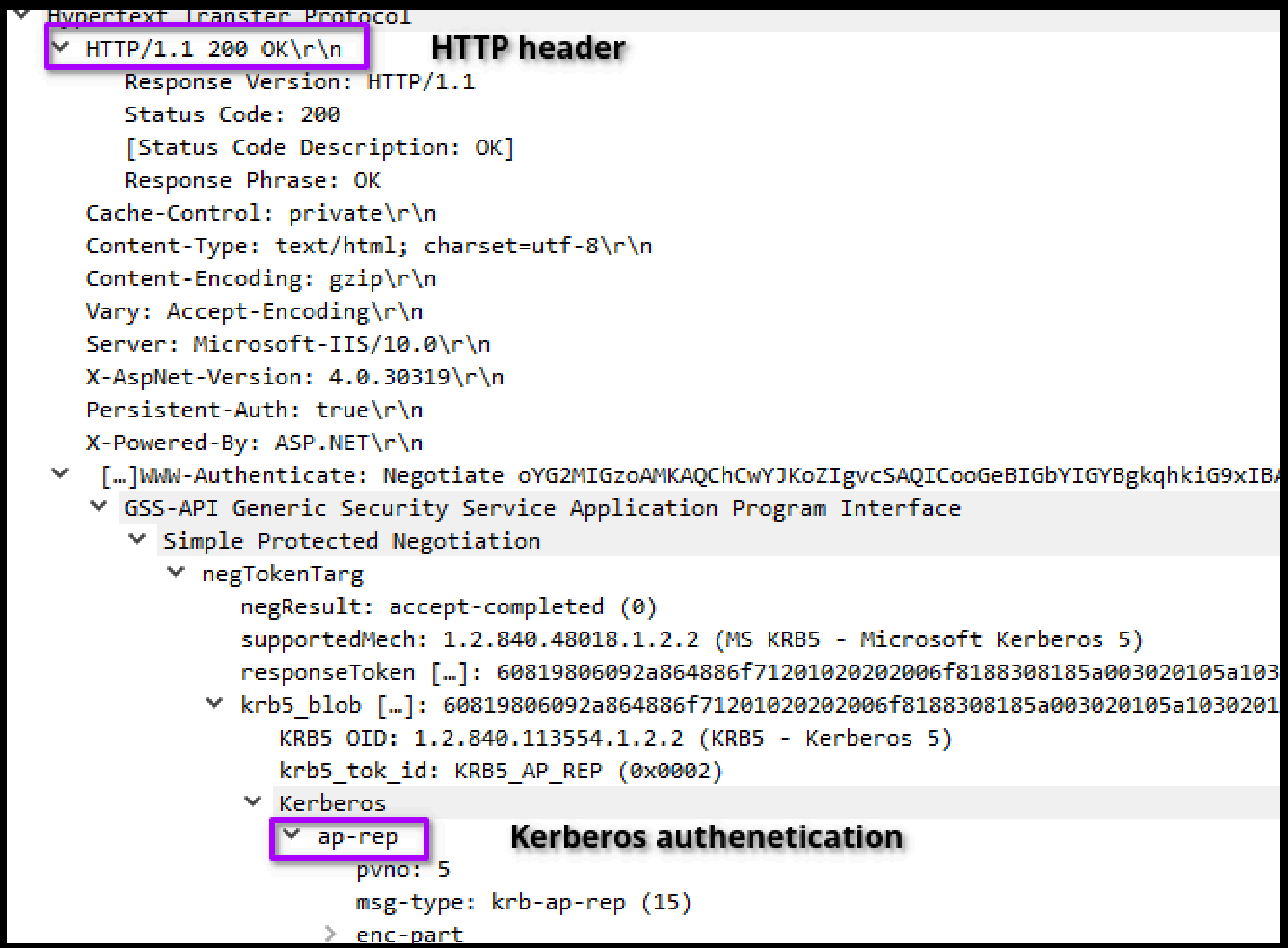


```
73 21.495095      192.168.122.158      192.168.122.18      HTTP      1352 GET /upload.aspx HTTP/1.1
99 21.511991      192.168.122.18       192.168.122.158     HTTP      2277 HTTP/1.1 200 OK  (text/html)
```



```
Hypertext Transfer Protocol
  GET /upload.aspx/ HTTP/1.1\r\n
      Request Method: GET
      Request URI: /upload.aspx/
      Request Version: HTTP/1.1
  Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: iis.auth.lab:8080\r\n
  Connection: Keep-Alive\r\n
  DNT: 1\r\n
   […]Authorization: Negotiate YIIG4gYGKwYBBQUCoIIG1jCCBtKgMDAuBgkqhkiC9xIBAgIGCSqGSIb3EgECAgYKKwYBE
    GSS-API Generic Security Service Application Program Interface
      OID: 1.3.6.1.5.5.2 (SPNEGO - Simple Protected Negotiation)
      Simple Protected Negotiation
        negTokenInit
          mechTypes: 4 items
          mechToken […]: 6082069406092a864886f71201020201006e8206833082067fa003020105a10302010ea
          krb5_blob […]: 6082069406092a864886f71201020201006e8206833082067fa003020105a10302010ea
            KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
            krb5_tok_id: KRB5_AP_REQ (0x0001)
            Kerberos
              ap-req
                pvno: 5
                msg-type: krb-ap-req (14)
                Padding: 0
                ap-options: 20000000
                ticket
                authenticator
```

AP REQUEST



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
  Cache-Control: private\r\n
  Content-Type: text/html; charset=utf-8\r\n
  Content-Encoding: gzip\r\n
  Vary: Accept-Encoding\r\n
  Server: Microsoft-IIS/10.0\r\n
  X-AspNet-Version: 4.0.30319\r\n
  Persistent-Auth: true\r\n
  X-Powered-By: ASP.NET\r\n
   […]WWW-Authenticate: Negotiate oYG2MIGzoAMKAQChCwYJKoZIgvcSAQICooGeBIGbYIGYBgkqhkiG9xIBA
    GSS-API Generic Security Service Application Program Interface
      Simple Protected Negotiation
        negTokenTarg
          negResult: accept-completed (0)
          supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
          responseToken […]: 60819806092a864886f71201020202006f8188308185a003020105a103
          krb5_blob […]: 60819806092a864886f71201020202006f8188308185a003020105a1030201
            KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
            krb5_tok_id: KRB5_AP_REP (0x0002)
            Kerberos
              ap-rep
                pvno: 5
                msg-type: krb-ap-rep (15)
                enc-part
```

AP REPLY

AUTHENTICATION COURSE

Authentication from IIS to File Server

IIS TRIES TO FETCH THE FILES

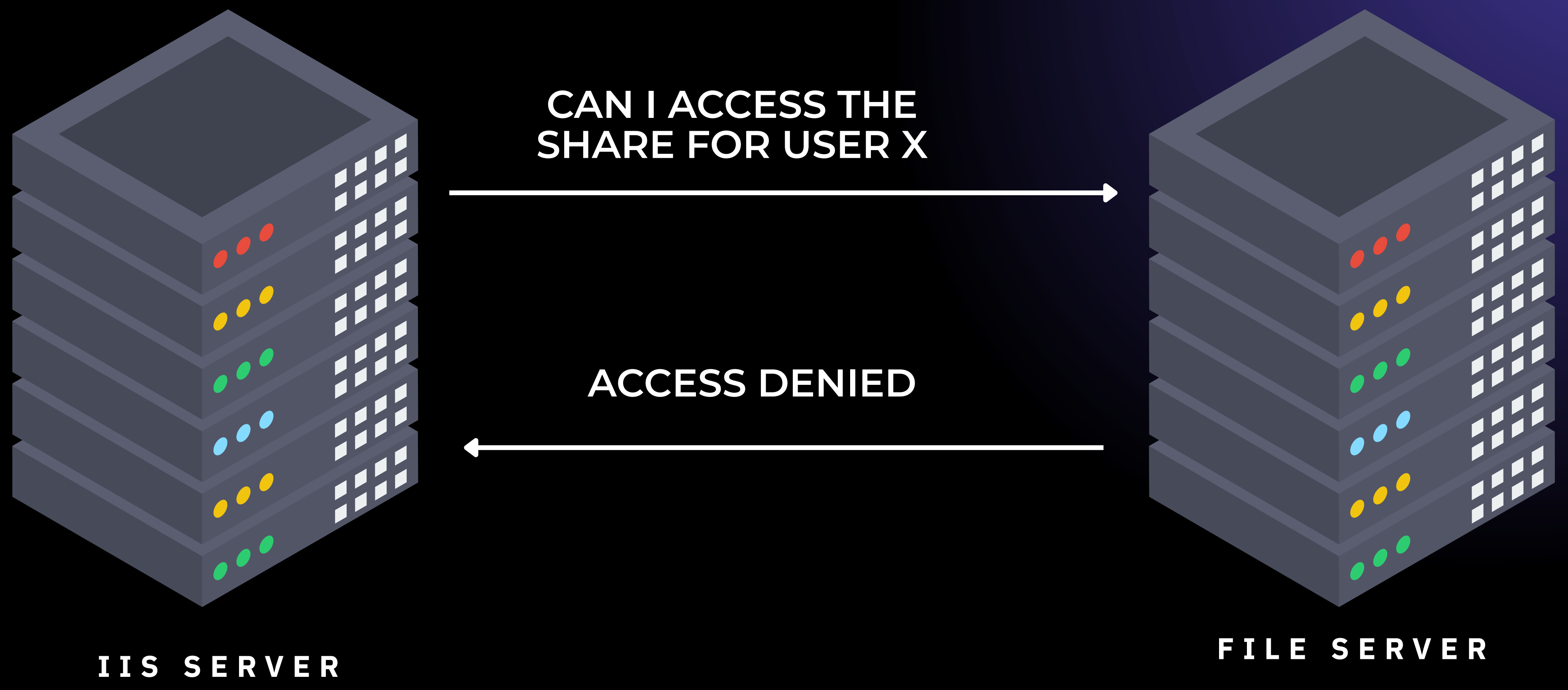
When the user accesses the portal, IIS tries to fetch their files from the File Server, it says:
“I am the IIS server, and I want User X's files.”

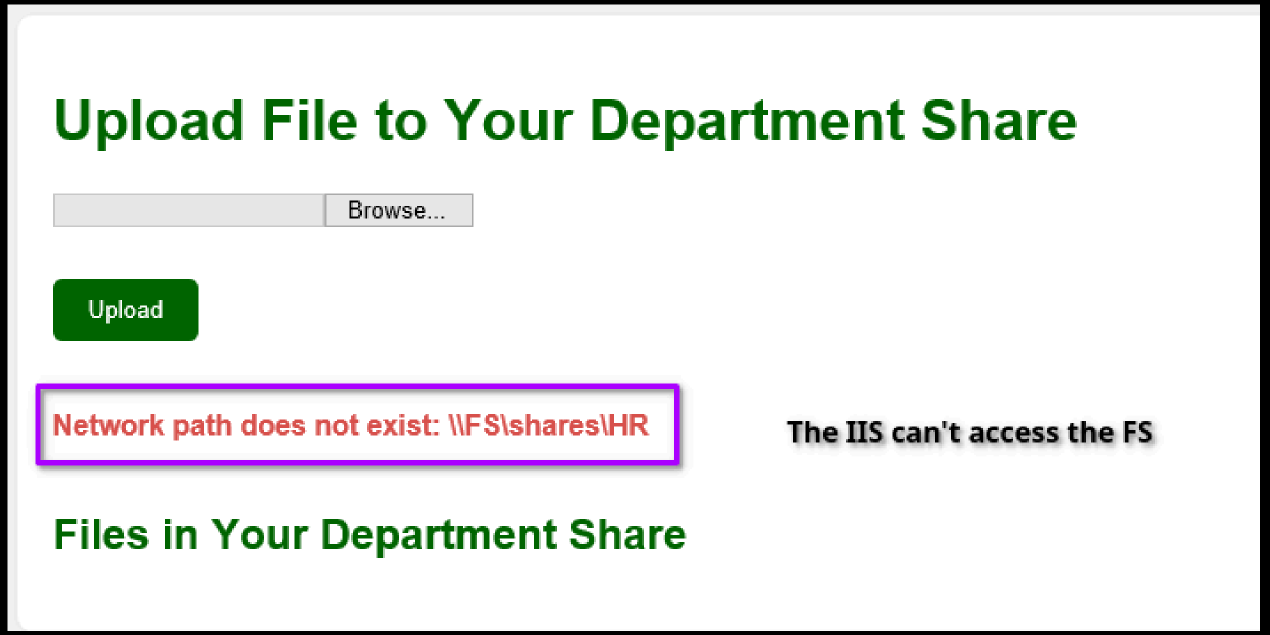
FILE SERVER REPLY

The File Server responds:
“Access Denied — you’re not User X.”

THIS HAPPENS BECAUSE

- The shares are protected by departmental ACLs.
- Only users from the correct department are allowed access.





Upload File to Your Department Share

Network path does not exist: \\FS\shares\HR

The IIS can't access the FS

Files in Your Department Share

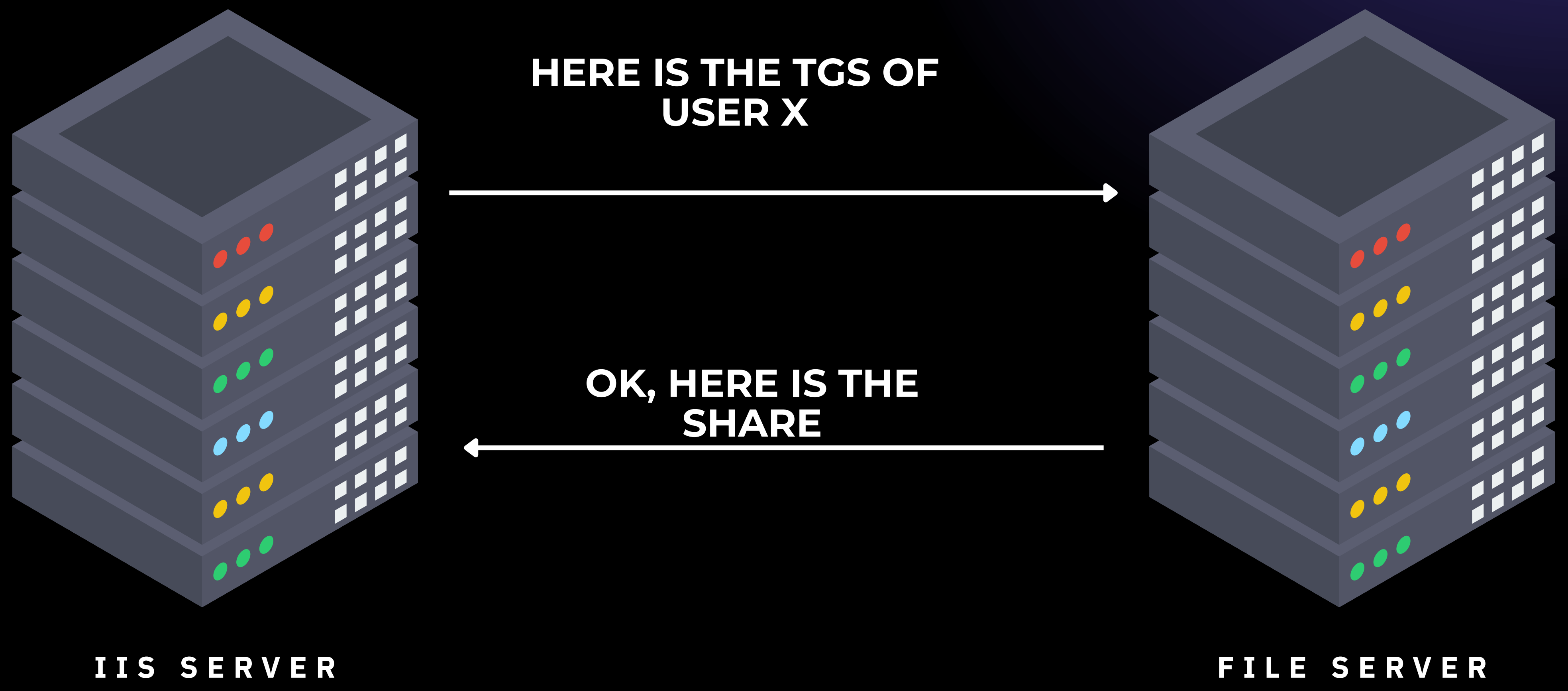
This is known as the Kerberos Double Hop Problem –

WHERE IS THE PROBLEM EXACTLY

A front-end service (IIS) tries to access a back-end service (File Server) on behalf of a user, but can't forward the user's identity.

THE SOLUTION

A Windows feature called delegation where it allows the IIS server to impersonate the user, enabling it to securely access backend resources as if it were the user.

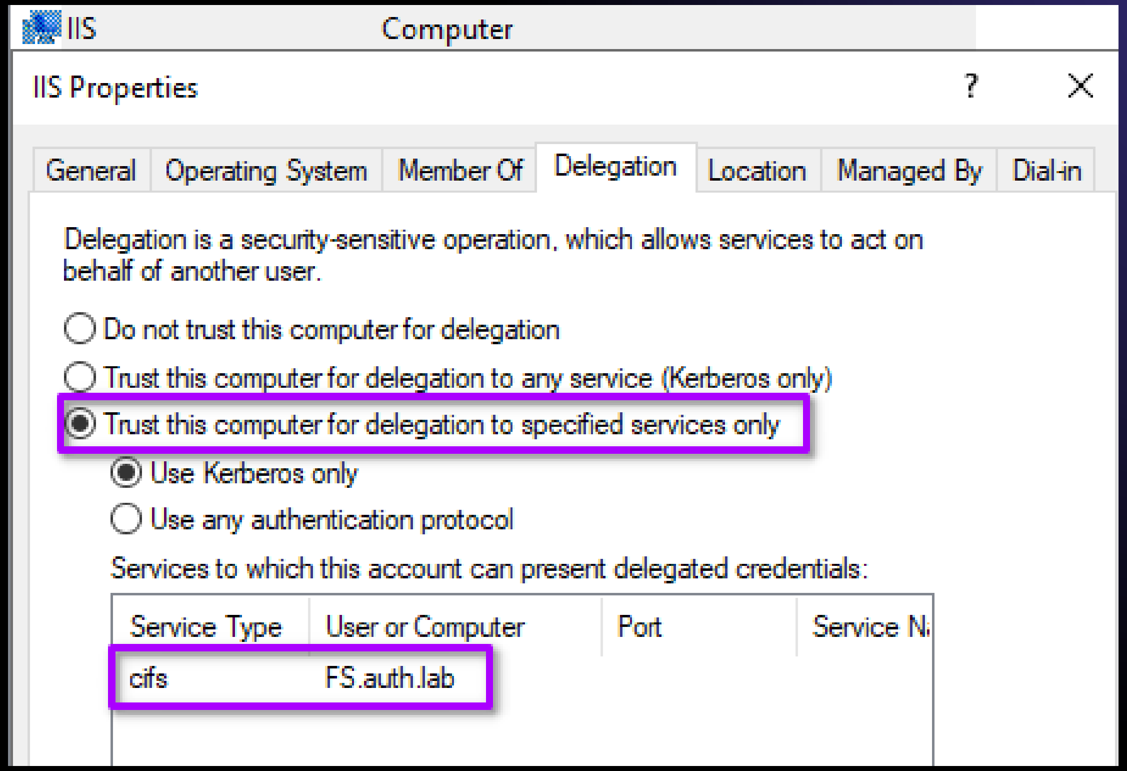


Delegation: under the hood

HOW ITS CONFIGURED

Delegation is configured by enabling it on the IIS server's computer account in Active Directory.

we specify the File Server's CIFS service in the Delegation tab, allowing the IIS server to request service tickets on behalf of users and access file shares using their identity.



IIS Computer
IIS Properties
? ✕
General | Operating System | Member Of | Delegation | Location | Managed By | Dial-in

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

● Use Kerberos only

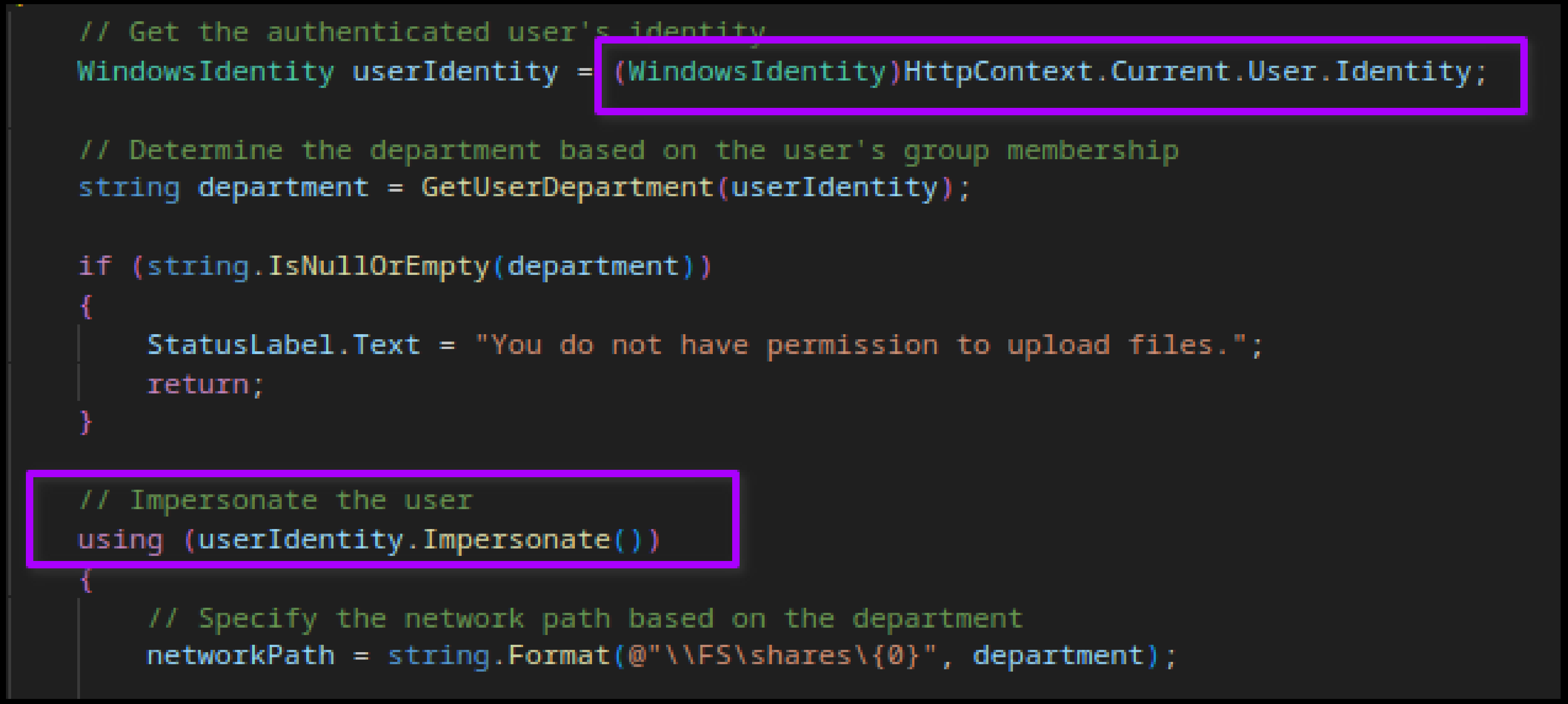
○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
cifs	FS.auth.lab		

HOW ITS CODED

The application retrieves the authenticated user's identity from the IIS context and uses impersonation to temporarily execute actions under that user's security context.

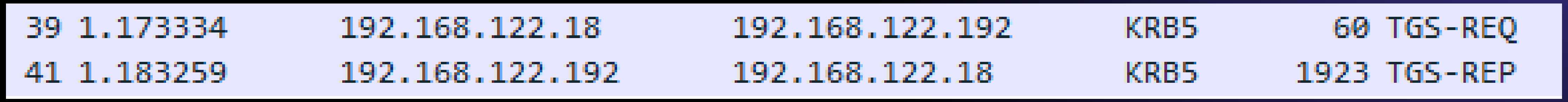


```
// Get the authenticated user's identity
WindowsIdentity userIdentity = (WindowsIdentity)HttpContext.Current.User.Identity;

// Determine the department based on the user's group membership
string department = GetUserDepartment(userIdentity);

if (string.IsNullOrEmpty(department))
{
    StatusLabel.Text = "You do not have permission to upload files.";
    return;
}

// Impersonate the user
using (userIdentity.Impersonate())
{
    // Specify the network path based on the department
    networkPath = string.Format(@"\\FS\shares\{0}", department);
```

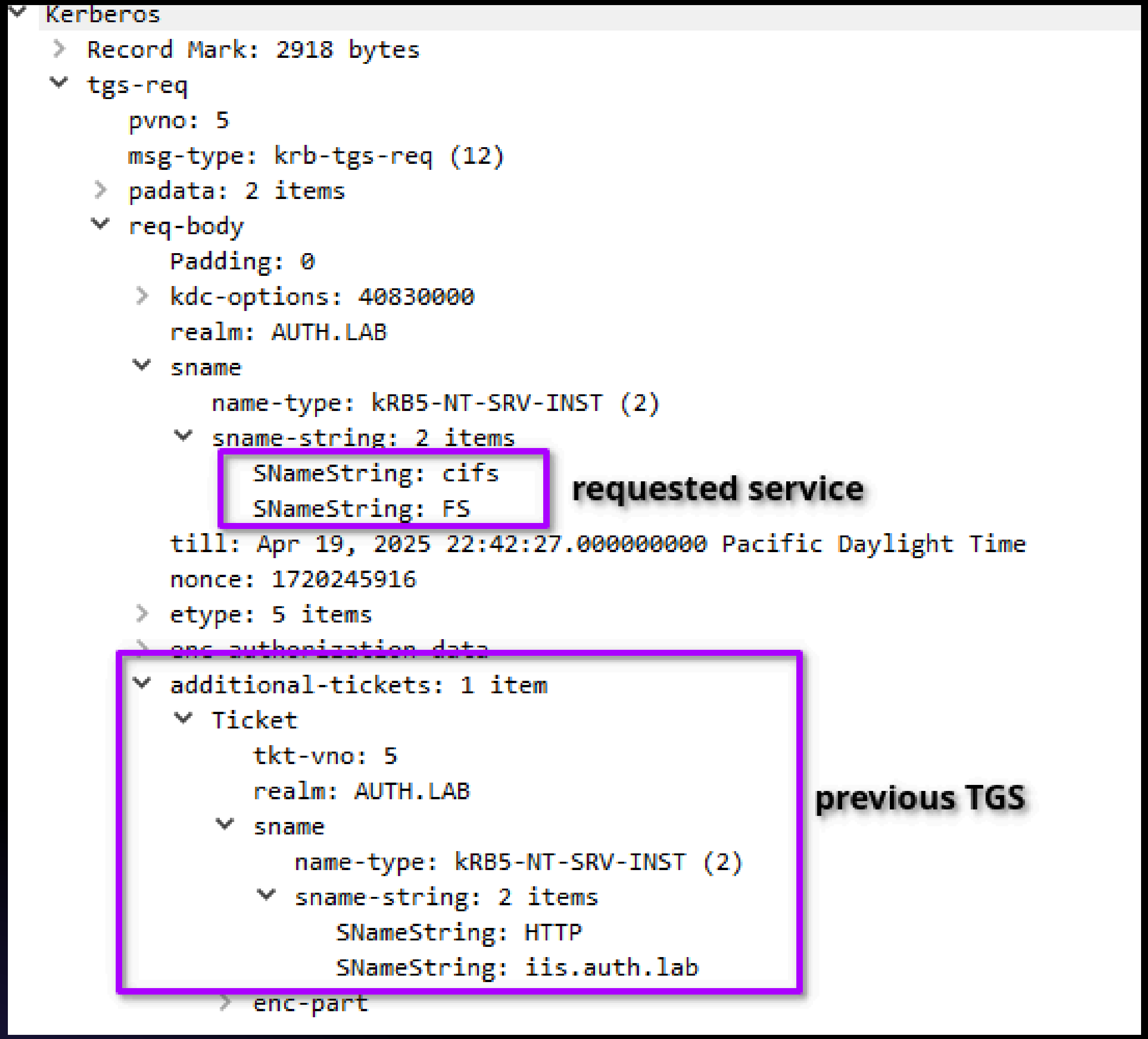
AUTHENTICATION COURSE

Delegation Traffic

we can see the IIS server is requesting a TGS for the user administrator for the fileserver service.

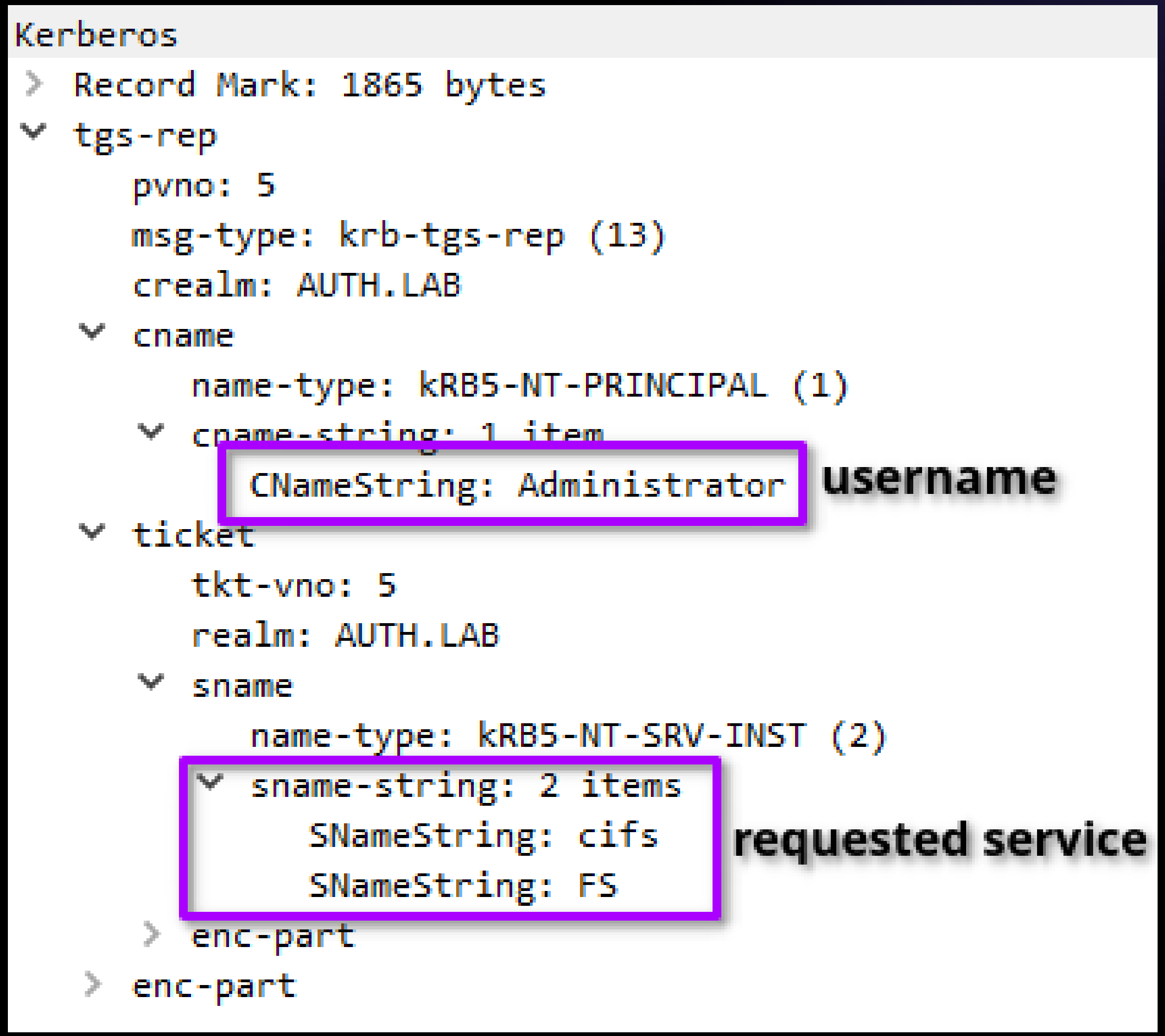


```
39 1.173334      192.168.122.18      192.168.122.192     KRB5       60 TGS-REQ
41 1.183259      192.168.122.192     192.168.122.18      KRB5     1923 TGS-REP
```



```
Kerberos
  Record Mark: 2918 bytes
  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 2 items
    req-body
      Padding: 0
      kdc-options: 40830000
      realm: AUTH.LAB
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: cifs
          SNameString: FS
      till: Apr 19, 2025 22:42:27.000000000 Pacific Daylight Time
      nonce: 1720245916
      etype: 5 items
      enc-authorization-data
      additional-tickets: 1 item
        Ticket
          tkt-vno: 5
          realm: AUTH.LAB
          sname
            name-type: kRB5-NT-SRV-INST (2)
            sname-string: 2 items
              SNameString: HTTP
              SNameString: iis.auth.lab
          enc-part
```

because the IIS doesn't have the user's TGT. it sends the users TGS

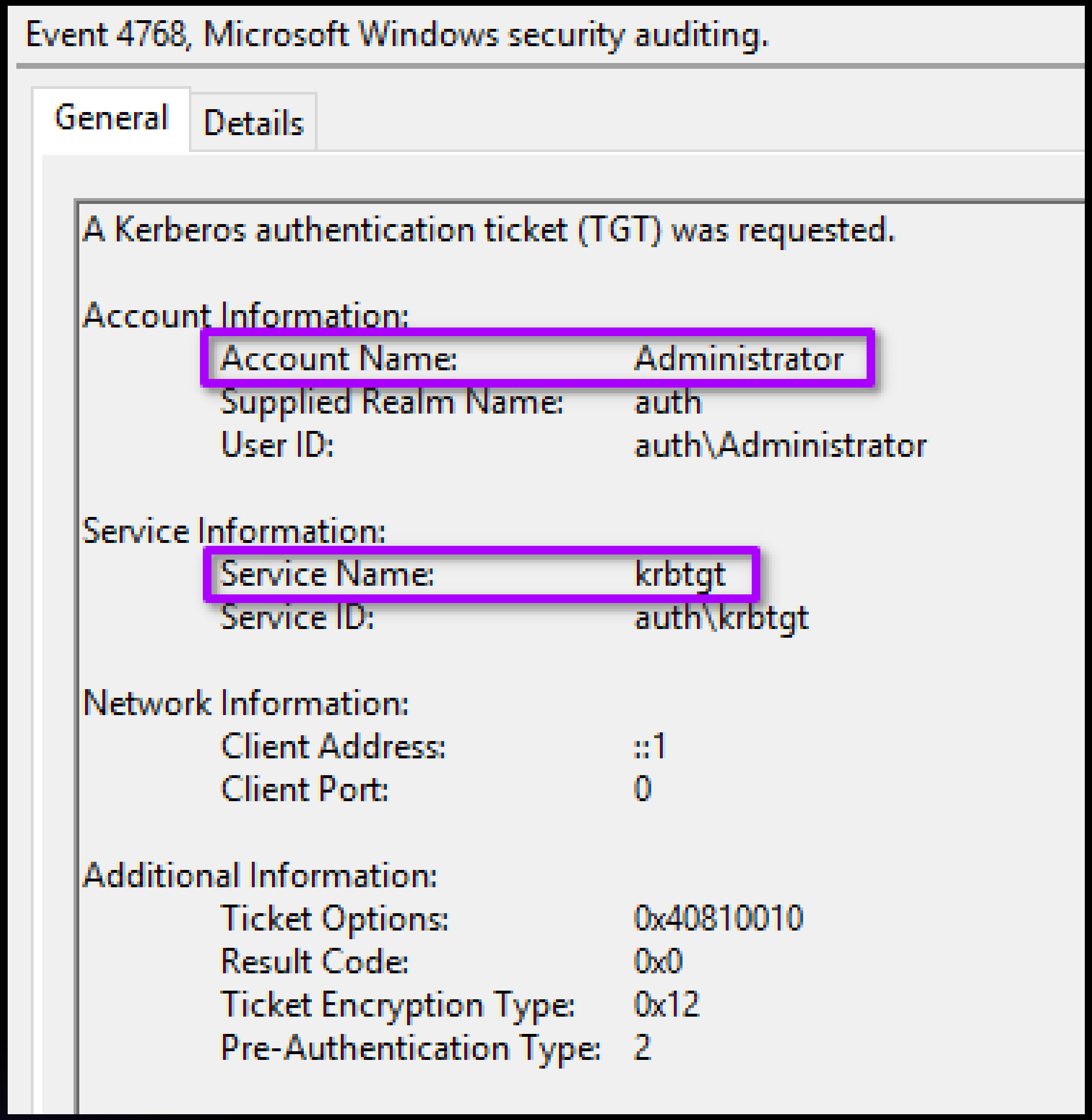


```
Kerberos
  Record Mark: 1865 bytes
  tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: AUTH.LAB
    cname
      name-type: kRB5-NT-PRINCIPAL (1)
      cname-string: 1 item
        CNameString: Administrator
    ticket
      tkt-vno: 5
      realm: AUTH.LAB
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: cifs
          SNameString: FS
      enc-part
    enc-part
```

here the DC replies with the users TGS

Logging

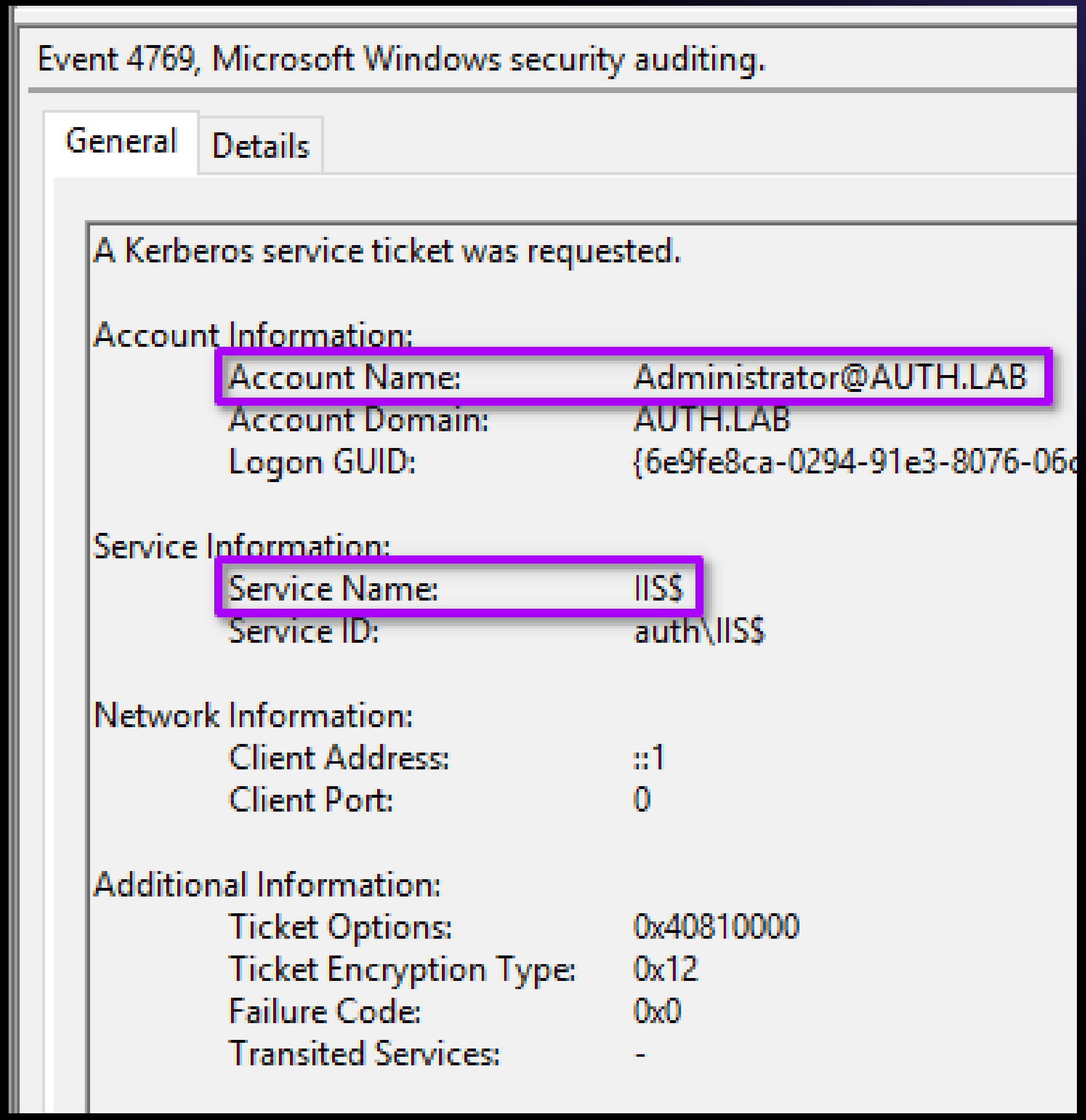
All the ticket events can be found in the DC security channel.



```
Event 4768, Microsoft Windows security auditing.

General  Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:
        Account Name:           Administrator
        Supplied Realm Name:    auth
        User ID:                auth\Administrator

Service Information:
        Service Name:           krbtgt
        Service ID:             auth\krbtgt

Network Information:
        Client Address:         ::1
        Client Port:            0

Additional Information:
        Ticket Options:         0x40810010
        Result Code:            0x0
        Ticket Encryption Type: 0x12
        Pre-Authentication Type: 2
```

TGT ISSUE EVENT

Event Code 4768, which is a security event found on the DC.



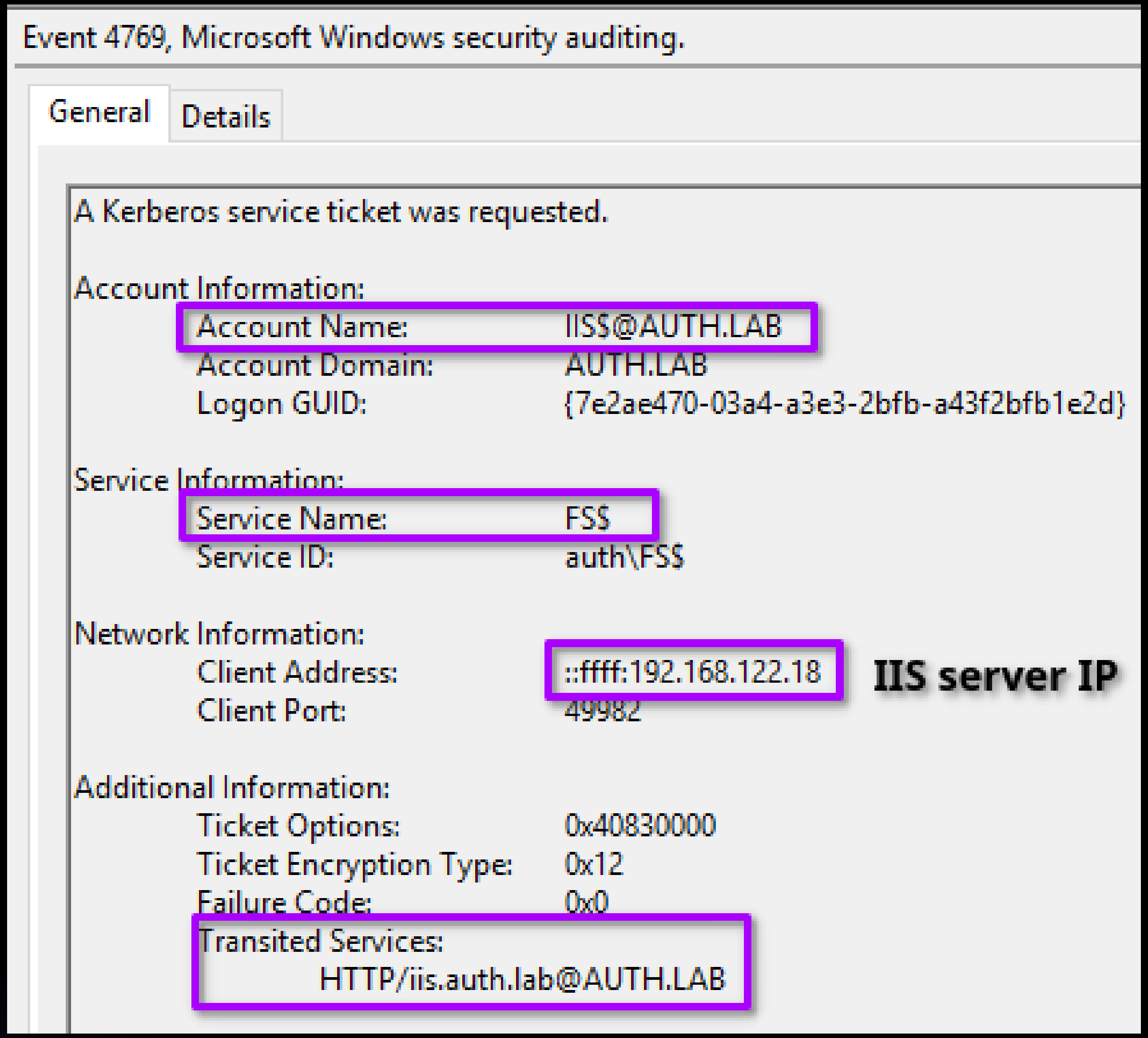
```
Event 4769, Microsoft Windows security auditing.

General  Details

A Kerberos service ticket was requested.

Account Information:
        Account Name:           Administrator@AUTH.LAB
        Account Domain:         AUTH.LAB
        Logon GUID:             {6e9fe8ca-0294-91e3-8076-06c

Service Information:
        Service Name:           IIS$
        Service ID:             auth\IIS$

Network Information:
        Client Address:         ::1
        Client Port:            0

Additional Information:
        Ticket Options:         0x40810000
        Ticket Encryption Type: 0x12
        Failure Code:           0x0
        Transited Services:     -
```

TGS ISSUE EVENT

Event Code 4769, which is a security event found on the DC.

Logging

All the ticket events can be found in the DC security channel.

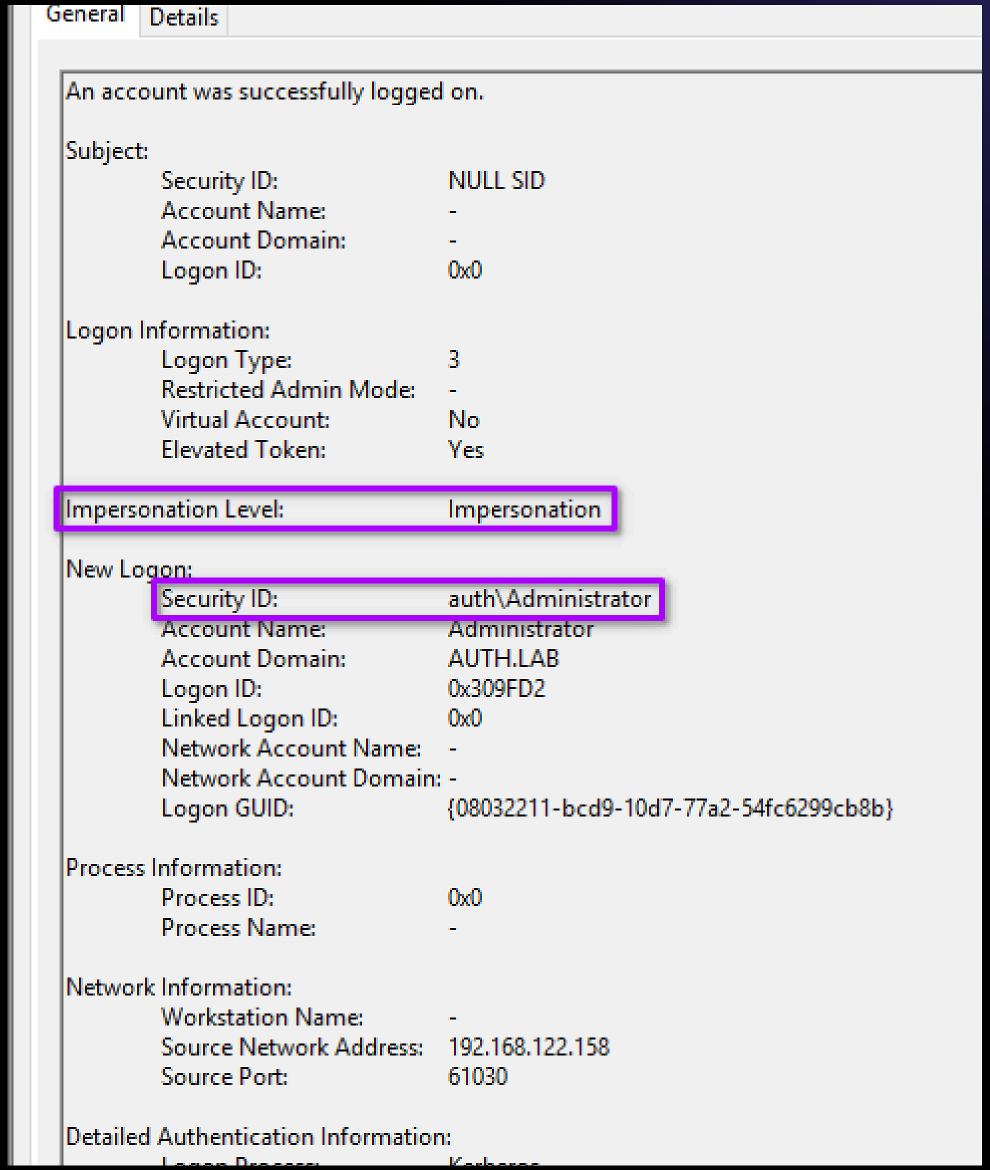


```
Event 4769, Microsoft Windows security auditing.

General  Details

A Kerberos service ticket was requested.

Account Information:
        Account Name:           IIS$@AUTH.LAB
        Account Domain:         AUTH.LAB
        Logon GUID:             {7e2ae470-03a4-a3e3-2bfb-a43f2bfb1e2d}

Service Information:
        Service Name:           FS$
        Service ID:             auth\FS$

Network Information:
        Client Address:         ::ffff:192.168.122.18
        Client Port:            49982

Additional Information:
        Ticket Options:         0x40830000
        Ticket Encryption Type: 0x12
        Failure Code:           0x0
        Transited Services:
                HTTP/iis.auth.lab@AUTH.LAB
```

IIS server IP

DELEGATION TGS

Event Code 4769, which is a security event found on the DC that shows Transited services.



```
General  Details

An account was successfully logged on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Information:
        Logon Type:             3
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            auth\Administrator
        Account Name:           Administrator
        Account Domain:         AUTH.LAB
        Logon ID:               0x309FD2
        Linked Logon ID:        0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {08032211-bcd9-10d7-77a2-54fc6299cb8b}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:       -
        Source Network Address: 192.168.122.158
        Source Port:            61030

Detailed Authentication Information:
        Logon Process:          Kerberos
```

LOGON EVENT

Event Code 4624, which is found on the IIS and FS indicating that a user has accessed them.

اسمع وانت
ساكت