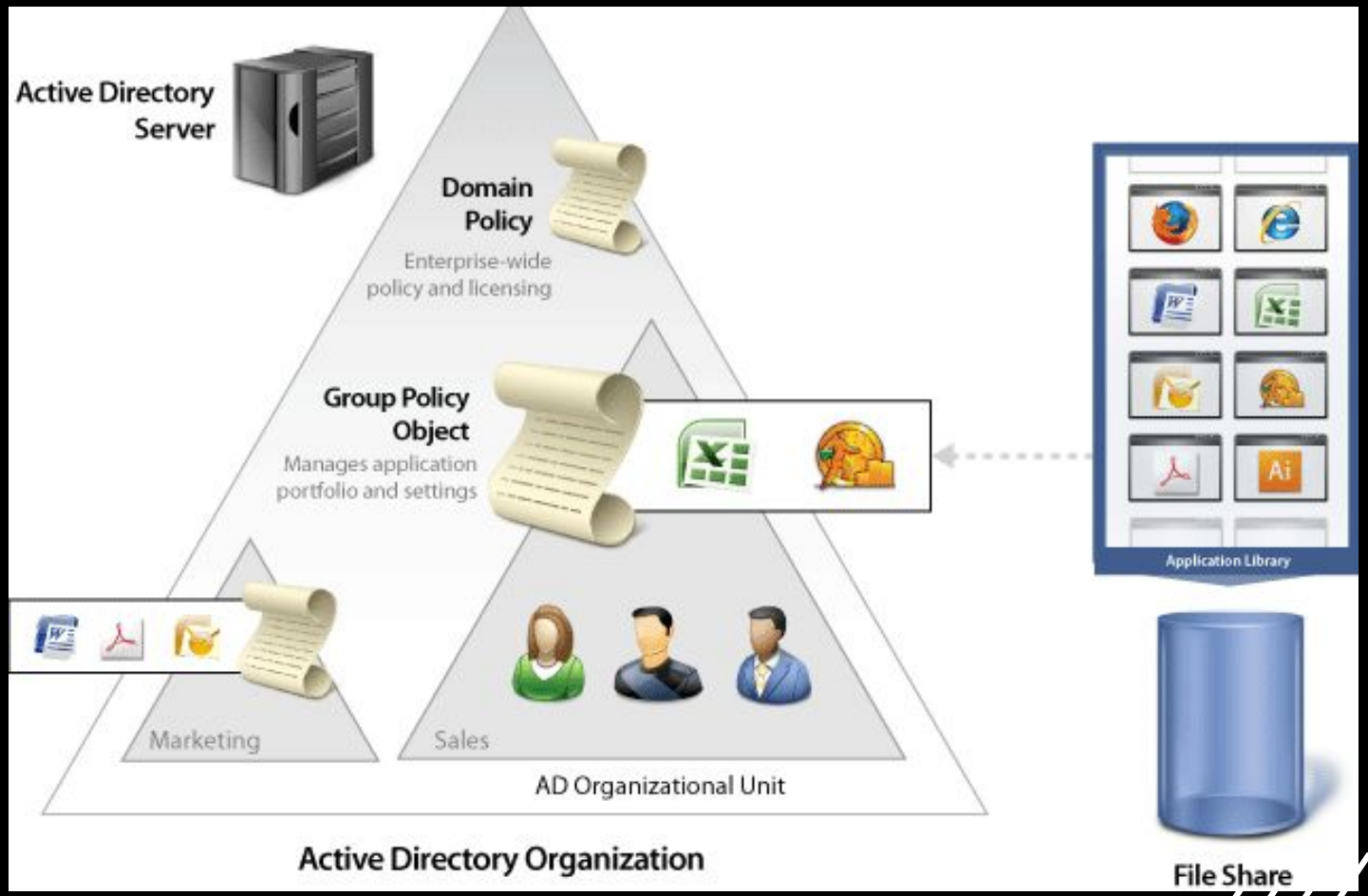
INTRODUCTION TO ACTIVE DIRECTORY

SJU ACM STUDENT CHAPTER

WHAT IS ACTIVE DIRECTORY?

- *"DISTRIBUTED, HIERARCHICAL STRUCTURE THAT ALLOWS FOR CENTRALIZED MANAGEMENT OF AN ORGANIZATION'S RESOURCES, INCLUDING USERS, COMPUTERS, GROUPS, NETWORK DEVICES, FILE SHARES, GROUP POLICIES, DEVICES, AND TRUSTS"*
- 95% OF FORTUNE 500 COMPANIES USE AD



THE FUNDAMENTALS

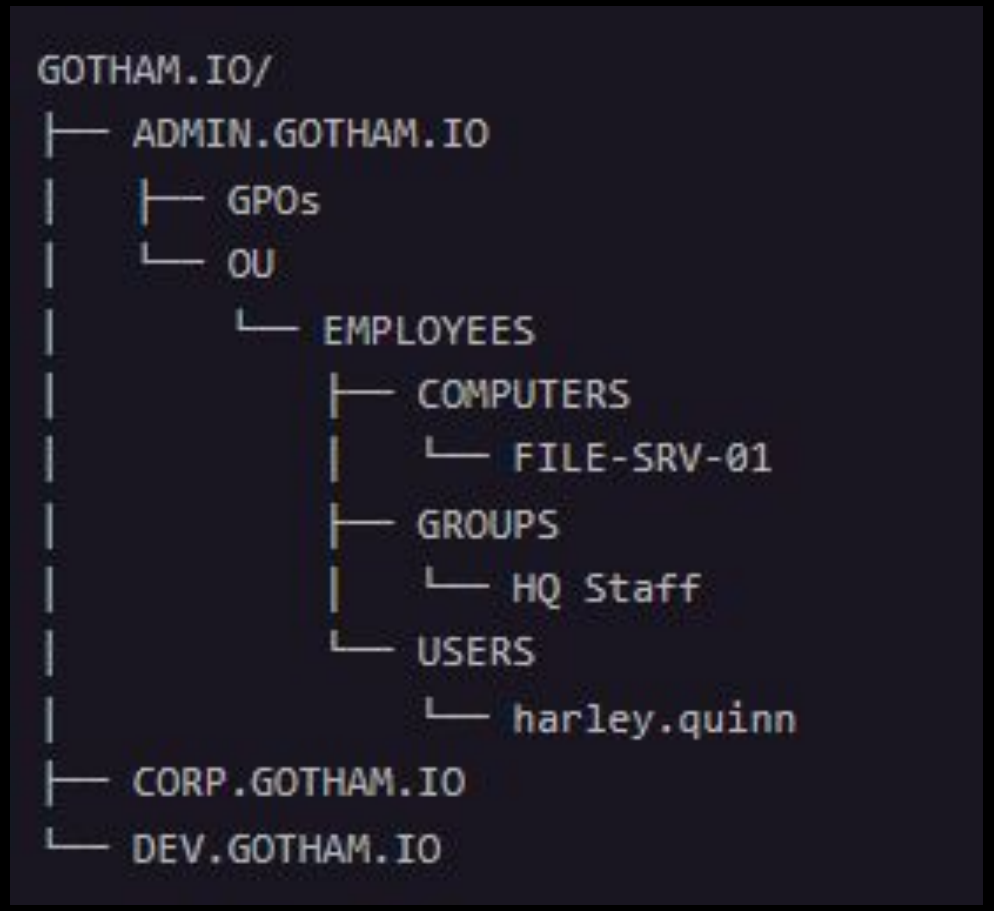
STRUCTURE AND AD OBJECTS

ACTIVE DIRECTORY STRUCTURE

- DIRECTORY SERVICE
  - GIVES AN ORGANIZATION WAYS TO STORE DIRECTORY DATA AND MAKE IT AVAILABLE TO BOTH STANDARD USERS AND ADMINISTRATORS ON THE SAME NETWORK.
    - ACTIVE DIRECTORY DOMAIN SERVICES (AD DS)
- ARRANGED IN A HIERARCHICAL TREE STRUCTURE
  - FORESTS AT THE TOP
    - FORESTS CONTAIN TREES (OR DOMAINS)
      - TREES CAN CONTAIN SUBDOMAINS
      - DOMAINS CAN CONTAIN ORGANIZATIONAL UNITS (OUS)
- DOMAINS
  - A DOMAIN IS A STRUCTURE WITHIN WHICH CONTAINED OBJECTS (USERS, COMPUTERS, AND GROUPS) ARE ACCESSIBLE. IT HAS MANY BUILT-IN ORGANIZATIONAL UNITS (OUS), SUCH AS DOMAIN CONTROLLERS, USERS, COMPUTERS, AND NEW OUS CAN BE CREATED AS REQUIRED.
    - OUS ARE WAYS OF GROUPING THINGS TOGETHER IN AD
      - OUS MAY CONTAIN OBJECTS AND SUB-OUS, ALLOWING FOR THE ASSIGNMENT OF DIFFERENT GROUP POLICIES.

STRUCTURE CONT

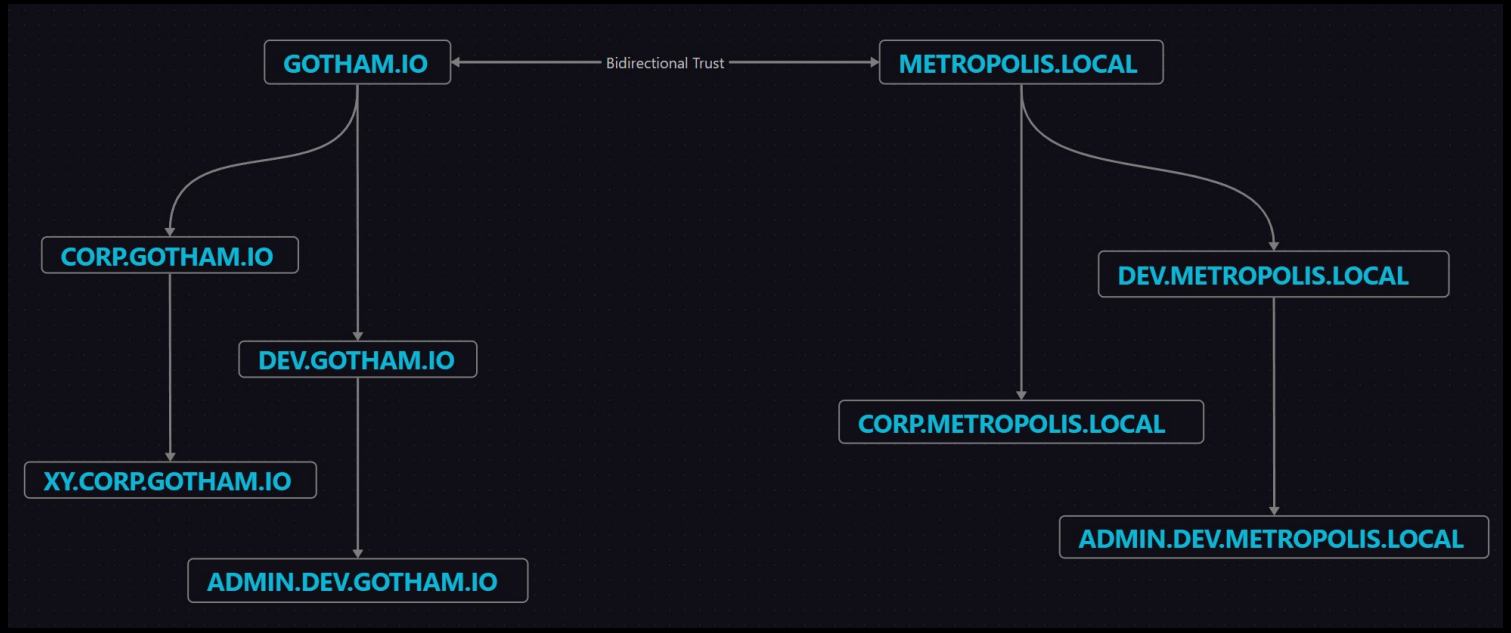
- THE TREE HERE IS GOTHAM.IO
  - THIS IS ALSO KNOWN AS THE ROOT DOMAIN
- THE GOTHAM.IO TREE CONTAINS 3 SUBDOMAINS:
  - ADMIN.GOTHAM.IO
  - CORP.GOTHAM.IO
  - DEV.GOTHAM.IO
- EACH DOMAIN CONTAINS VARIOUS OUS WHICH IN TURN CONTAIN THE OBJECTS FOR THE DOMAIN



STRUCTURE CONT

TRUSTS

- DOMAIN TRUSTS ARE A WAY OF LINKING TWO OR MORE EXISTING TREES/FORESTS TOGETHER
  - THIS IS VERY COMMON IN ORGS THAT PERFORM A LOT OF ACQUISITIONS
  - IT IS MUCH EASIER TO CREATE A DOMAIN TRUST THAN IT IS TO RECREATE AN ENTIRE DOMAIN AFTER PERFORMING AN ACQUISITION.



AD OBJECTS

- AN OBJECT CAN BE DEFINED AS ANY RESOURCE PRESENT WITHIN AN ACTIVE DIRECTORY ENVIRONMENT SUCH AS OUS, PRINTERS, USERS, DOMAIN CONTROLLERS.
- NOTABLE OBJECTS:
  - USERS
  - COMPUTERS
  - PRINTERS
  - DOMAINS
  - DOMAIN CONTROLLERS
  - GROUPS
  - OUS
  - BUILT-IN

ACTIVE DIRECTORY PROTOCOLS

KERBEROS, DNS, LDAP, MSRPC AND NTLM

KERBEROS

- DEFAULT AD AUTHENTICATION PROTOCOL
- OPEN STANDARD
- MUTUAL AUTHENTICATION
- TICKETS
  - KDC
- USERS PORT 88 (TCP AND UDP)

HOW DOES KERBEROS WORK?

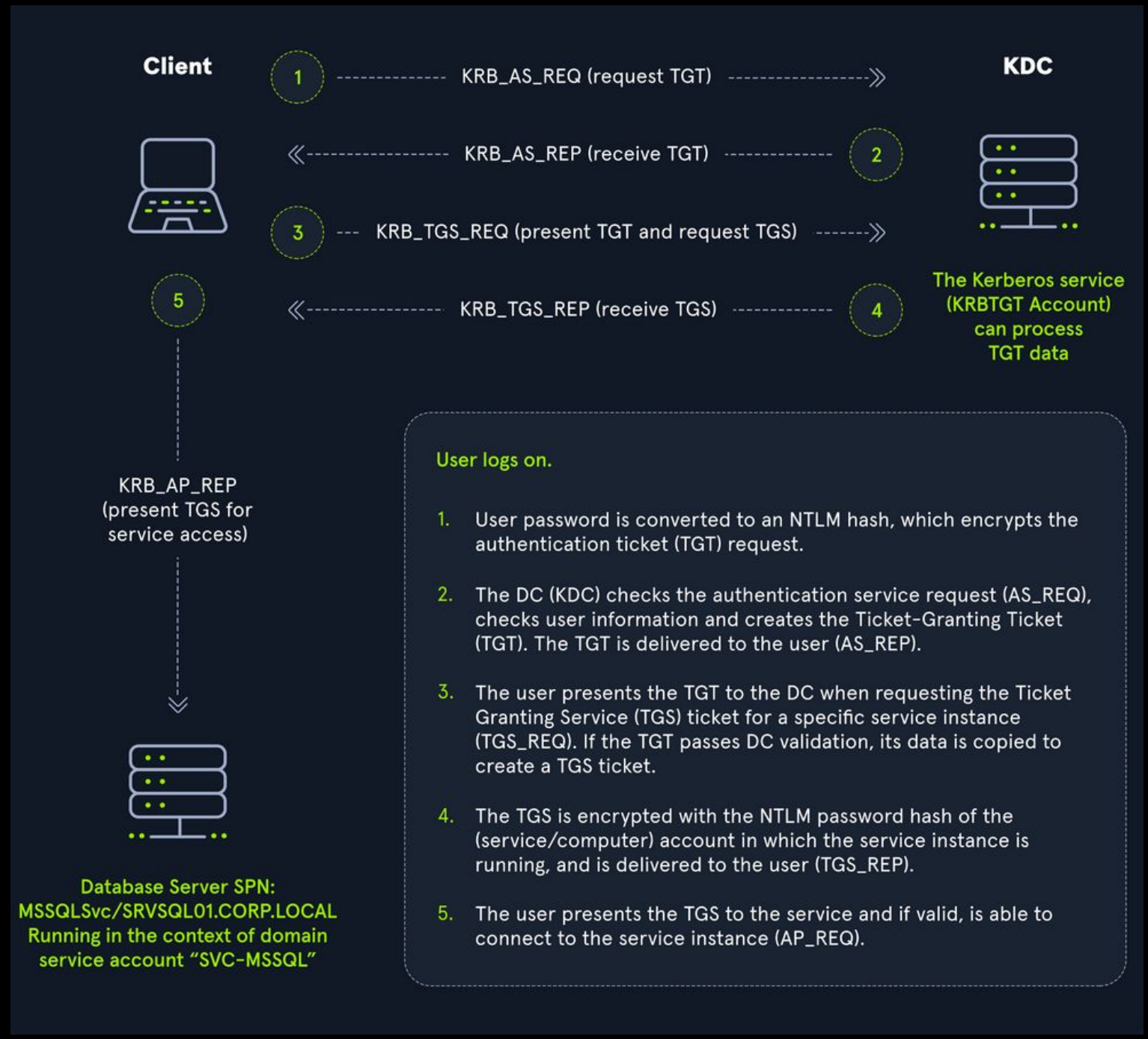
THE USER LOGS ON, AND THEIR PASSWORD IS CONVERTED INTO AN NTLM HASH, WHICH IS USED TO ENCRYPT THEIR TGT REQUEST.

- THIS MAKES IT SO THAT YOU DONT ACTUALLY HAVE TO SEND A PASSWORD OR PASSWORD HASH OVER THE NETWORK

THE KDC TRIES TO DECRYPT THE REQUEST (AS-REQ) USING THE USERS PASSWORD. IF SUCCESSFUL IT CREATES A TGT, ENCRYPTS IT WITH THE USERS PASSWORD HASH AND SENDS IT TO THE USER.

THE USER PRESENTS THE TGT TO THE DC, REQUESTING A TGS FOR A SPECIFIC SERVICE. IF THE DC CAN DECRYPT THE TGT USING THE USERS PASSWORD, IT WILL CREATE A TGS, ENCRYPT IT WITH THE SERVICES NTLM HASH, AND SEND IT TO THE USER.

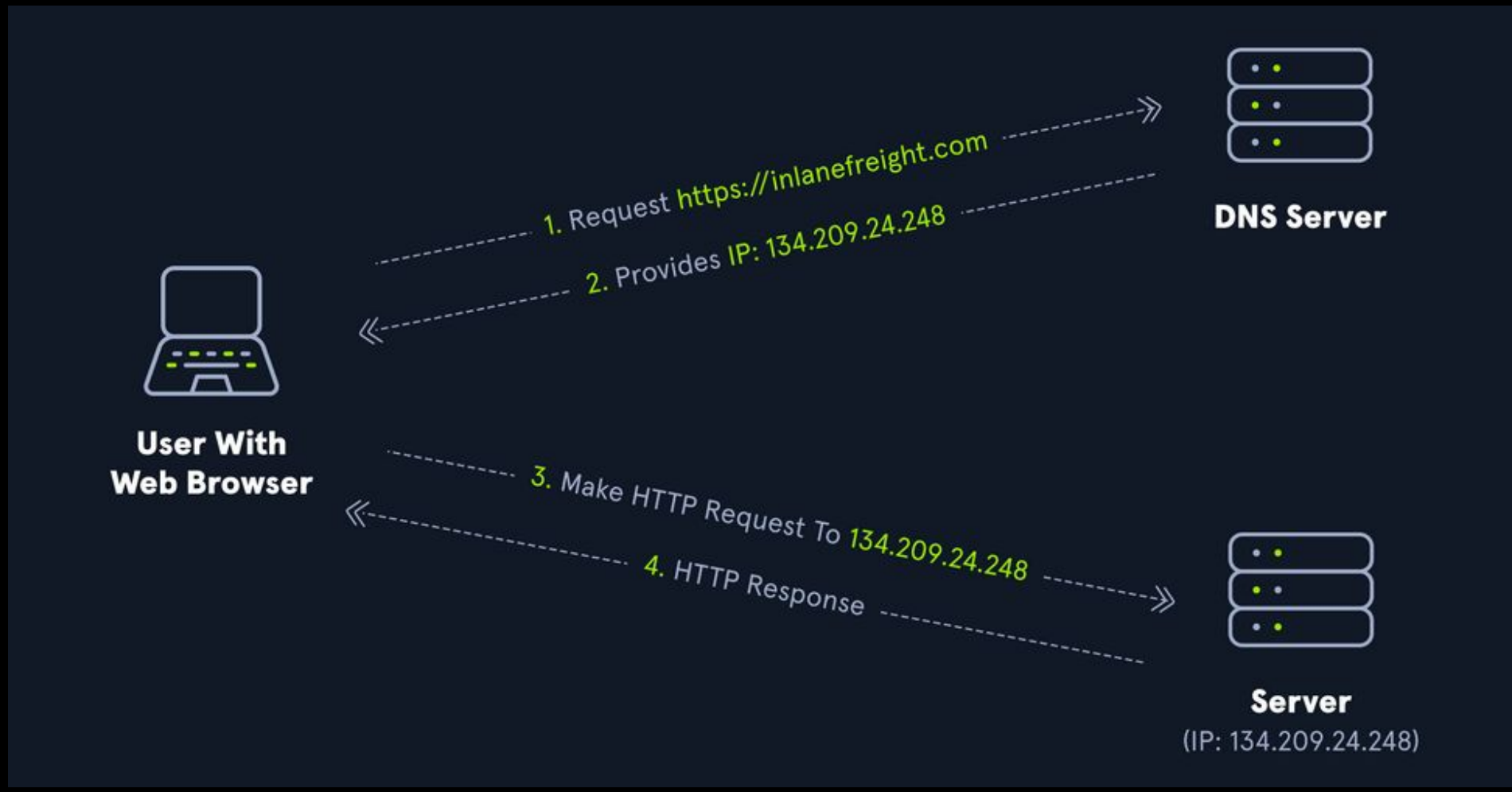
THE USER PRESENTS THE TGT TO THE SERVICE, AND IF THE SERVICE CAN DECRYPT IT USING ITS OWN PASSWORD, IT GRANTS THE USER ACCESS.


Client
KDC
1
KRB_AS_REQ (request TGT)
KRB_AS_REP (receive TGT)
2
3
KRB_TGS_REQ (present TGT and request TGS)
KRB_TGS_REP (receive TGS)
4
5
The Kerberos service (KRBTGT Account) can process TGT data
KRB_AP_REP (present TGS for service access)
Database Server SPN: MSSQLSvc/SRVSQL01.CORP.LOCAL Running in the context of domain service account "SVC-MSSQL"
User logs on.
1. User password is converted to an NTLM hash, which encrypts the authentication ticket (TGT) request.
2. The DC (KDC) checks the authentication service request (AS_REQ), checks user information and creates the Ticket-Granting Ticket (TGT). The TGT is delivered to the user (AS_REP).
3. The user presents the TGT to the DC when requesting the Ticket Granting Service (TGS) ticket for a specific service instance (TGS_REQ). If the TGT passes DC validation, its data is copied to create a TGS ticket.
4. The TGS is encrypted with the NTLM password hash of the (service/computer) account in which the service instance is running, and is delivered to the user (TGS_REP).
5. The user presents the TGS to the service and if valid, is able to connect to the service instance (AP_REQ).

DNS

DNS IS USED TO ALLOW CLIENTS (WORKSTATION, SERVERS, ETC..) TO LOCATE DOMAIN CONTROLLERS, AND FOR THE DOMAIN CONTROLLERS THEMSELVES TO COMMUNICATE AMONGST EACHOTHER.

USES PORT 53 UDP BY DEFAULT BUT WILL FALLBACK TO 53 TCP IF IT CANT USE UDP FOR WHATEVER REASON (FOR MESSAGES LONGER THAN 512 BYTES FOR EXAMPLE)



LDAP

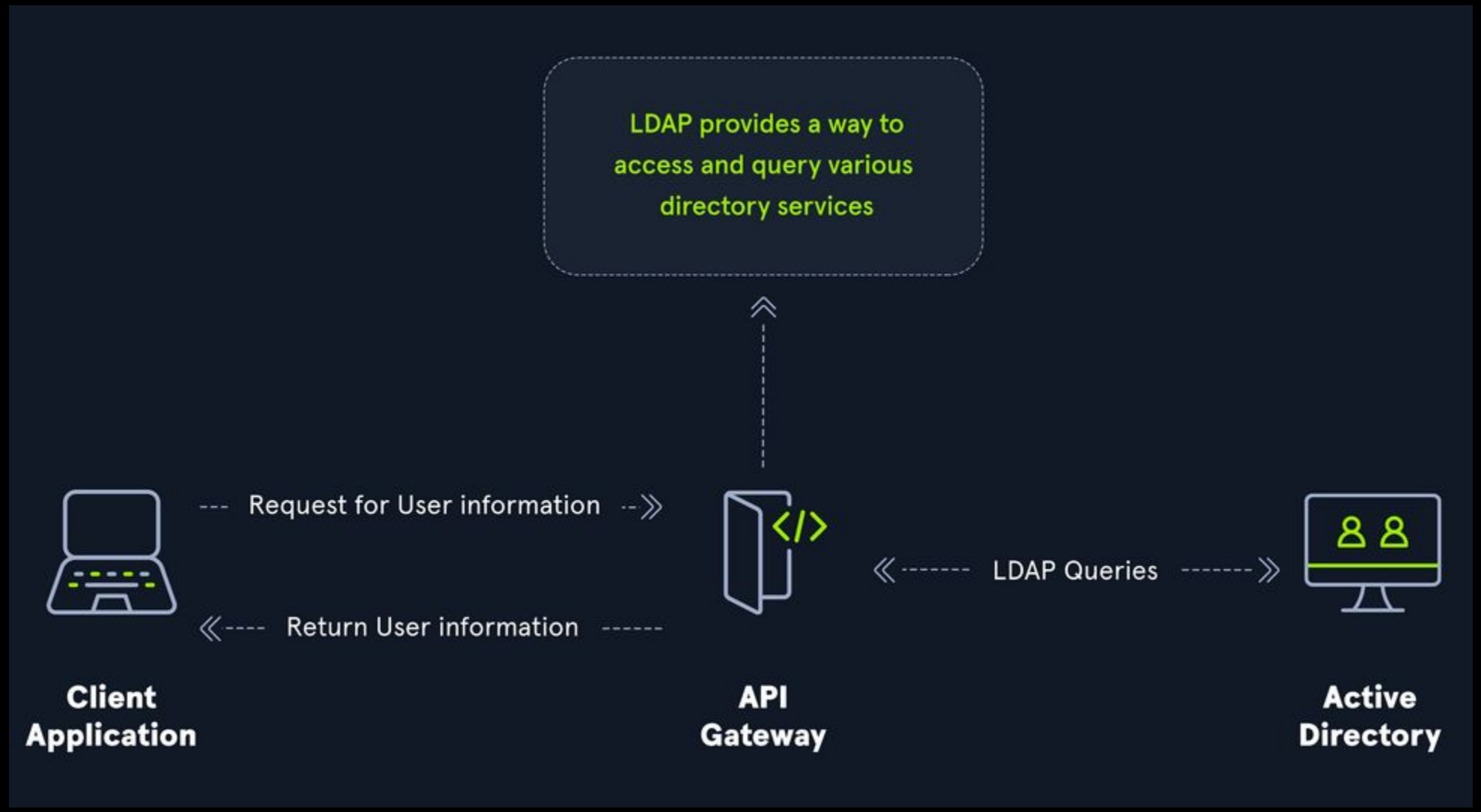
LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

OPEN-SOURCE AND CROSS-PLATFORM PROTOCOL USED FOR AUTHENTICATION AGAINST VARIOUS DIRECTORY SERVICES (SUCH AS AD)

USES PORT 389, AND LDAP OVER SSL (LDAPS) COMMUNICATES OVER PORT 636

LDAP IS THE LANGUAGE THAT APPLICATIONS USE TO COMMUNICATE WITH OTHER SERVERS THAT PROVIDE DIRECTORY SERVICES. IN OTHER WORDS, LDAP IS HOW SYSTEMS IN THE NETWORK ENVIRONMENT CAN "SPEAK" TO AD.

THE RELATIONSHIP BETWEEN AD AND LDAP CAN BE COMPARED TO APACHE AND HTTP. THE SAME WAY APACHE IS A WEB SERVER THAT USES THE HTTP PROTOCOL, ACTIVE DIRECTORY IS A DIRECTORY SERVER THAT USES THE LDAP PROTOCOL.


LDAP provides a way to access and query various directory services
Request for User information
Return User information
LDAP Queries
Client Application
API Gateway
Active Directory

AD LDAP AUTHENTICATION

THERE ARE TWO TYPES OF LDAP AUTHENTICATION.

1. SIMPLE AUTHENTICATION:
   A. THIS INCLUDES ANONYMOUS AUTHENTICATION, UNAUTHENTICATED AUTHENTICATION, AND USERNAME/PASSWORD AUTHENTICATION. SIMPLE AUTHENTICATION MEANS THAT A USERNAME AND PASSWORD CREATE A BIND REQUEST TO AUTHENTICATE TO THE LDAP SERVER.
2. SASL AUTHENTICATION:
   A. THE SIMPLE AUTHENTICATION AND SECURITY LAYER (SASL) FRAMEWORK USES OTHER AUTHENTICATION SERVICES, SUCH AS KERBEROS, TO BIND TO THE LDAP SERVER AND THEN USES THIS AUTHENTICATION SERVICE (KERBEROS IN THIS EXAMPLE) TO AUTHENTICATE TO LDAP. THE LDAP SERVER USES THE LDAP PROTOCOL TO SEND AN LDAP MESSAGE TO THE AUTHORIZATION SERVICE, WHICH INITIATES A SERIES OF CHALLENGE/RESPONSE MESSAGES RESULTING IN EITHER SUCCESSFUL OR UNSUCCESSFUL AUTHENTICATION. SASL CAN PROVIDE ADDITIONAL SECURITY DUE TO THE SEPARATION OF AUTHENTICATION METHODS FROM APPLICATION PROTOCOLS.

MSRPC

Microsoft's implementation of Remote Procedure Call (RPC), an interprocess communication technique used for client-server model-based applications.

Windows systems use MSRPC to access systems in Active Directory using four key RPC interfaces.

- LSARPC
  - A set of RPC calls to the Local Security Authority (LSA) system which manages the local security policy on a computer, controls the audit policy, and provides interactive authentication services. LSARPC is used to perform management on domain security policies.
- NETLOGON
  - NETLOGON is a Windows process used to authenticate users and other services in the domain environment. It is a service that continuously runs in the background.

- SAMR
  - PROVIDES MANAGEMENT FUNCTIONALITY FOR THE DOMAIN ACCOUNT DATABASE, STORING INFORMATION ABOUT USERS AND GROUPS
- DRSUAPI
  - THE MICROSOFT API THAT IMPLEMENTS THE DIRECTORY REPLICATION SERVICE (DRS) REMOTE PROTOCOL WHICH IS USED TO PERFORM REPLICATION-RELATED TASKS ACROSS DOMAIN CONTROLLERS IN A MULTI-DC ENVIRONMENT.

NTLM AUTHENTICATION

ASIDE FROM KERBEROS AND LDAP, ACTIVE DIRECTORY USES SEVERAL OTHER AUTHENTICATION METHODS WHICH CAN BE USED (AND ABUSED) BY APPLICATIONS AND SERVICES IN AD. THESE INCLUDE LM, NTLM, NTLMV1, AND NTLMV2. LM AND NTLM HERE ARE THE HASH NAMES, AND NTLMV1 AND NTLMV2 ARE AUTHENTICATION PROTOCOLS THAT UTILIZE THE LM OR NT HASH.

MANAGING USERS

USERS, GROUPS, RIGHTS AND PRIVILEGES

USERS

USER ACCOUNTS ARE CREATED ON BOTH LOCAL SYSTEMS (NOT JOINED TO AD) AND IN ACTIVE DIRECTORY TO GIVE A PERSON OR A PROGRAM (SUCH AS A SYSTEM SERVICE) THE ABILITY TO LOG ON TO A COMPUTER AND ACCESS RESOURCES BASED ON THEIR RIGHTS.

WHEN A USER LOGS IN THEY ARE GIVEN AN ACCESS TOKEN. THIS TOKEN SPECIFIES WHAT THEY CAN AND CANNOT ACCESS.

USERS CAN BE ASSIGNED TO GROUPS THAT CAN CONTAIN ONE OR MORE MEMBERS. THESE GROUPS CAN ALSO BE USED TO CONTROL ACCESS TO RESOURCES.

DOMAIN-JOINED VS NON-DOMAIN-JOINED MACHINES

- DOMAIN JOINED
  - A HOST JOINED TO A DOMAIN WILL ACQUIRE ANY CONFIGURATIONS OR CHANGES NECESSARY THROUGH THE DOMAIN'S GROUP POLICY.
  - THE BENEFIT HERE IS THAT A USER IN THE DOMAIN CAN LOG IN AND ACCESS RESOURCES FROM ANY HOST JOINED TO THE DOMAIN, NOT JUST THE ONE THEY WORK ON. THIS IS THE TYPICAL SETUP YOU WILL SEE IN ENTERPRISE ENVIRONMENTS.
- NON-DOMAIN-JOINED
  - NON-DOMAIN JOINED COMPUTERS OR COMPUTERS IN A WORKGROUP ARE NOT MANAGED BY DOMAIN POLICY.
  - SHARING RESOURCES OUTSIDE YOUR LOCAL NETWORK IS MUCH MORE COMPLICATED THAN IT WOULD BE ON A DOMAIN
  - THE ADVANTAGE OF THIS SETUP IS THAT THE INDIVIDUAL USERS ARE IN CHARGE OF ANY CHANGES THEY WISH TO MAKE TO THEIR HOST. ANY USER ACCOUNTS ON A WORKGROUP COMPUTER ONLY EXIST ON THAT HOST, AND PROFILES ARE NOT MIGRATED TO OTHER HOSTS WITHIN THE WORKGROUP.

GROUPS

- CAN PLACE SIMILAR USERS TOGETHER AND MASS ASSIGN RIGHTS AND ACCESS
- KEY TARGET FOR ATTACKERS
- THERE ARE MANY BUILT-IN GROUPS IN ACTIVE DIRECTORY, AND MOST ORGANIZATIONS ALSO CREATE THEIR OWN GROUPS TO DEFINE RIGHTS AND PRIVILEGES, FURTHER MANAGING ACCESS WITHIN THE DOMAIN.

BUILT-IN VS. CUSTOM GROUPS

- SEVERAL BUILT-IN SECURITY GROUPS ARE CREATED WITH A DOMAIN LOCAL GROUP SCOPE WHEN A DOMAIN IS CREATED
  - ONLY USER ACCOUNTS CAN BE ADDED TO THESE BUILT-IN GROUPS AS THEY DO NOT ALLOW FOR GROUP NESTING (GROUPS WITHIN GROUPS).
  - DOMAIN ADMINS
- IT IS COMMON FOR MOST ORGANIZATIONS TO CREATE ADDITIONAL GROUPS (BOTH SECURITY AND DISTRIBUTION) FOR THEIR OWN PURPOSES.
- CHANGES/ADDITIONS TO AN AD ENVIRONMENT CAN ALSO TRIGGER THE CREATION OF ADDITIONAL GROUPS.
  - FOR EXAMPLE, WHEN MICROSOFT EXCHANGE IS ADDED TO A DOMAIN, IT ADDS VARIOUS DIFFERENT SECURITY GROUPS TO THE DOMAIN

RIGHTS AND PRIVILEGES

- CORNERSTONES OF AD MANAGEMENT
- ACCESS RIGHTS AND PRIVILEGES ARE TWO IMPORTANT TOPICS IN AD (AND INFOSEC IN GENERAL), AND WE MUST UNDERSTAND THE DIFFERENCE.
  - RIGHTS ARE TYPICALLY ASSIGNED TO USERS OR GROUPS AND DEAL WITH PERMISSIONS TO ACCESS AN OBJECT SUCH AS A FILE
    -
  - PRIVILEGES GRANT A USER PERMISSION TO PERFORM AN ACTION SUCH AS RUN A PROGRAM, SHUT DOWN A SYSTEM, RESET PASSWORDS, ETC.
    - CAN BE ASSIGNED INDIVIDUALLY TO USERS OR CONFERRED UPON THEM VIA BUILT-IN OR CUSTOM GROUP MEMBERSHIP.
    - WINDOWS COMPUTERS HAVE A CONCEPT CALLED USER RIGHTS ASSIGNMENT, WHICH, WHILE REFERRED TO AS RIGHTS, ARE ACTUALLY TYPES OF PRIVILEGES GRANTED TO A USER

RESOURCES

GENERAL RESOURCES:

- https://academy.hackthebox.com/module/details/74
- https://tryhackme.com/room/winadbasics
- https://learn.microsoft.com/en-us/shows/introtoad/
- https://www.comparitech.com/net-admin/active-directory-step-by-step-tutorial/

ATTACKING ACTIVE DIRECTORY

- https://tryhackme.com/room/attacktivedirectory
- https://tryhackme.com/room/adenumeration
- https://academy.hackthebox.com/module/details/143
- https://academy.hackthebox.com/module/details/22