Tuần 1 - Nghiên cứu và mô phỏng các kỹ thuật tấn công hệ thống Active Directory

Lý thuyết:

Tổng quan về Active Directory

Active Directory (AD) là một dịch vụ thư mục được phát triển bởi Microsoft, cung cấp một phương pháp tập trung để quản lý các tài nguyên mạng trong một môi trường Windows Domain. Nó giống như một "danh bạ" khổng lồ lưu trữ thông tin về tất cả các **đối tượng** (objects) trong mạng của tổ chức, bao gồm người dùng (users), máy tính (computers), nhóm (groups), máy in (printers), ứng dụng và các thiết bị khác

Vai trò của Active Directory

- **Quản lý tập trung:** Giúp quản trị viên dễ dàng quản lý hàng ngàn hoặc hàng triệu đối tượng từ một vị trí duy nhất.
- **Xác thực và Ủy quyền:** Cung cấp cơ chế xác thực mạnh mẽ (Kerberos, NTLM) để xác minh danh tính người dùng và máy tính, sau đó cấp quyền truy cập phù hợp vào các tài nguyên.
- **Kiểm soát truy cập:** Cho phép áp dụng các chính sách bảo mật chi tiết (Group Policy Objects - GPO) để kiểm soát quyền truy cập, cấu hình hệ thống và hành vi người dùng.
- **Khả năng mở rộng:** Thiết kế để hỗ trợ các mạng từ nhỏ đến rất lớn, với khả năng mở rộng linh hoạt.
- **Giảm chi phí quản lý:** Tự động hóa nhiều tác vụ quản trị, giảm gánh nặng cho đội ngũ IT.
- **Tăng cường bảo mật:** Bằng cách cung cấp một mô hình bảo mật thống nhất và các công cụ giám sát.

Các Thành phần Chính của Active Directory

Mặc dù có nhiều dịch vụ dưới tên gọi Active Directory (AD CS, AD FS, AD RMS, AD LDS), trong ngữ cảnh của quản lý danh tính và bảo mật mạng, chúng ta thường đề cập đến **Active Directory Domain Services (AD DS)**
Các thành phần cốt lõi của AD DS bao gồm:

- **Database (Cơ sở dữ liệu):** Là nơi lưu trữ tất cả thông tin về các đối tượng và cấu hình của AD. Nó được lưu trữ dưới dạng một file `NTDS.DIT` trên mỗi Domain Controller
- **Schema:** Là bản thiết kế (blueprint) của cơ sở dữ liệu AD. Nó định nghĩa tất cả các loại đối tượng có thể tồn tại trong AD (ví dụ: User, Computer, Group) và các thuộc tính mà mỗi loại đối tượng đó có thể có (ví dụ: tên, địa chỉ email, mật khẩu)
- **Global Catalog (GC):** Là một bản sao một phần của tất cả các đối tượng trong Forest. Nó chứa một tập hợp con các thuộc tính của mỗi đối tượng, cho phép người dùng và ứng dụng tìm kiếm đối tượng một cách nhanh chóng trên toàn bộ Forest mà không cần phải biết đối tượng đó nằm ở miền nào
- **Query Processor:** Xử lý các yêu cầu tìm kiếm và truy vấn thông tin từ cơ sở dữ liệu AD
- **Replication Engine:** Đảm bảo dữ liệu được đồng bộ giữa các Domain Controller để duy trì tính nhất quán và khả năng sẵn sàng cao

Kiến trúc Logic của Active Directory

Kiến trúc logic của Active Directory được thiết kế theo một mô hình phân cấp để quản lý các tài nguyên một cách hiệu quả và linh hoạt:

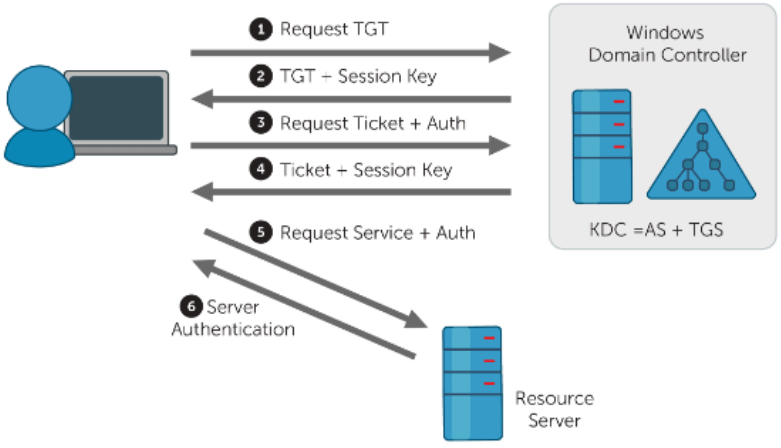
- **Forest (Rừng):**
  - Là cấp độ cao nhất trong cấu trúc logic của Active Directory.
  - Một Forest là một tập hợp của một hoặc nhiều **Tree** (cây miền) có mối quan hệ tin cậy hai chiều (two-way transitive trust) với nhau một cách tự động.
  - Tất cả các Domains trong cùng một Forest chia sẻ chung **Schema**, **Global Catalog** và cấu hình.
  - **Forest là ranh giới bảo mật cao nhất:** Quyền quản trị ở cấp độ Forest (Enterprise Admins, Schema Admins) có thể ảnh hưởng đến toàn bộ các miền trong Forest.
- **Tree (Cây miền):**
  - Là một tập hợp của một hoặc nhiều **Domain** có mối quan hệ cha-con phân cấp và chia sẻ một không gian tên (namespace) DNS liền kề duy nhất. Ví dụ: `sales.contoso.com` là một Domain con của `contoso.com`.
  - Các Domains trong cùng một Tree tự động thiết lập mối quan hệ tin cậy hai chiều, cho phép người dùng từ một Domain truy cập tài nguyên ở Domain khác trong cùng Tree.
- **Domain (Miền):**

    - Là đơn vị quản lý cốt lõi trong Active Directory.
    - Mỗi Domain là một **ranh giới bảo mật và quản lý** riêng biệt. Nó chứa các đối tượng như người dùng, máy tính, nhóm và các tài nguyên khác.
    - Mỗi Domain có cơ sở dữ liệu AD riêng, được lưu trữ và quản lý bởi các **Domain Controller** thuộc Domain đó.
- **Organizational Unit (OU):**
    - Là một container (thùng chứa) trong một Domain, được sử dụng để tổ chức các đối tượng (người dùng, máy tính, nhóm, hoặc các OUs khác) một cách logic theo cấu trúc của tổ chức (ví dụ: theo phòng ban, vị trí địa lý, chức năng).
    - OUs giúp đơn giản hóa việc quản lý và là nơi lý tưởng để áp dụng **Group Policy Objects (GPO)** một cách chi tiết đến các nhóm đối tượng cụ thể mà không ảnh hưởng đến toàn bộ Domain.
- **Objects (Đối tượng):**
    - Là các thực thể riêng lẻ được lưu trữ trong Active Directory. Mỗi đối tượng có một tập hợp các thuộc tính riêng.
    - Các loại đối tượng phổ biến bao gồm:
        - **User Accounts (Tài khoản người dùng):** Đại diện cho một cá nhân hoặc một dịch vụ để đăng nhập và truy cập tài nguyên.
        - **Computer Accounts (Tài khoản máy tính):** Đại diện cho các máy trạm và máy chủ tham gia vào Domain.
        - **Groups (Nhóm):** Là tập hợp các người dùng hoặc máy tính được nhóm lại để đơn giản hóa việc quản lý quyền truy cập. Khi gán quyền cho một nhóm, tất cả thành viên của nhóm đó sẽ kế thừa quyền tương ứng.
        - **Service Accounts (Tài khoản dịch vụ):** Các tài khoản đặc biệt được sử dụng bởi các ứng dụng và dịch vụ để chạy với các quyền hạn cụ thể.

Authentication: Kerberos

- Là giao thức xác thực chính và mặc định trong Active Directory
- Nó dựa trên các vé (tickets) được mã hóa để xác minh danh tính người dùng và cấp quyền truy cập dịch vụ
- Các thành phần chính: **Key Distribution Center (KDC)** (do DC thực hiện), **Ticket Granting Ticket (TGT)** và **Service Ticket**
- Vai trò của **Service Principal Name (SPN)** là rất quan trọng, nó là định danh duy nhất cho một dịch vụ chạy dưới một tài khoản cụ thể trong AD

Kerberos authentication flow:



Giống như đi chơi công viên, vé TGT (encrypt từ master key) sẽ được dùng để vào cổng, và TGT sẽ được dùng để đổi lấy vé Service Ticket tại quầy trò chơi. Vé Service Ticket chỉ được dùng để chơi trò chơi tương ứng

SPN (Service Principle Name):

- Một máy chủ có thể có nhiều service chạy cùng lúc -> SPN ra đời để định danh chính xác
- SPN được lưu trữ như thuộc tính của một đối tượng trong AD
- Kerberos sử dụng SPNs để cấp đúng ticket cho đúng dịch vụ

LDAP (Lightweight Directory Access Protocol)

là một giao thức ứng dụng được sử dụng để truy cập và duy trì các dịch vụ thông tin thư mục phân tán.

- Active Directory sử dụng LDAP làm giao thức để cho phép các ứng dụng và người dùng truy cập, tìm kiếm, và quản lý dữ liệu bên trong nó.
- Các đối tượng trong AD (bao gồm người dùng, máy tính, nhóm) được lưu trữ dưới dạng các mục LDAP
- Các SPN được lưu trữ dưới dạng thuộc tính `servicePrincipalName` của các đối tượng user hoặc computer trong AD. Do đó, bất kỳ người dùng nào có quyền đọc thông tin trong AD (người dùng thông thường cũng có quyền này theo mặc định) đều có thể thực hiện truy vấn LDAP để liệt kê tất cả các tài khoản có SPN được đăng ký -> Đây là một lỗ hổng thiết kế của Kerberos, cho phép kẻ tấn công thu thập thông tin về các mục tiêu tiềm năng mà không cần đặc quyền cao

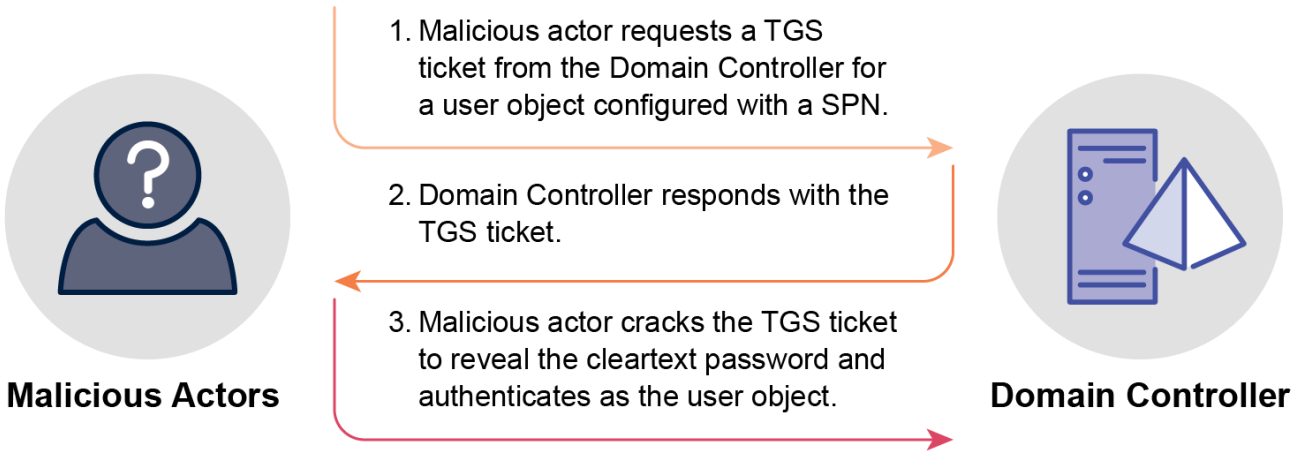
Mô hình Lab:

- **Domain:** `vdt.local` với một **Domain Controller (VDT-DC01)** chạy Windows Server (IP: `192.168.198.10`)
- **Máy tấn công:** Một máy ảo **Kali Linux (KALI)** (IP: `192.168.198.20`)
- **Cấu hình mạng:** Cả hai máy ảo đều sử dụng chế độ **NAT** trên subnet `192.168.198.0/24`, đảm bảo kết nối nội bộ và truy cập Internet cho Kali
- **Đối tượng trong AD:**
  - Tài khoản `Administrator` (quản trị viên miền)
  - Tài khoản người dùng thông thường `analyst` (dùng để khởi tạo tấn công)
  - Tài khoản dịch vụ `svc_webapp` (mục tiêu Kerberoasting): Được cấu hình với một **Service Principal Name (SPN)** `HTTP/webapp.vdt.local` và mật khẩu yếu (`password123`)

Cách tiếp cận tấn công:

1. **Tấn công Xác thực (Kerberoasting):** Từ máy Kali, lợi dụng một tài khoản người dùng bình thường (`analyst`) để tìm kiếm SPN và trích xuất Kerberos Service Ticket (TGS ticket) của tài khoản dịch vụ `svc_webapp`. Sau đó, bẻ khóa offline để lấy mật khẩu plaintext của `svc_webapp`
2. **Tấn công Ủy quyền (Abuse ACL - GenericAll):** Sử dụng tài khoản `svc_webapp` đã bị chiếm đoạt để tìm kiếm và khai thác các lỗ hổng cấu hình quyền hạn (ACLs) trong AD. Cụ thể, lợi dụng quyền `WriteDACL` được gán cho `svc_webapp` trên đối tượng Domain để tự cấp quyền `GenericAll` trên Domain. Quyền `GenericAll` là một quyền rất mạnh, cho phép `svc_webapp` có toàn quyền kiểm soát đối tượng Domain, bao gồm cả việc thêm mình vào nhóm `Domain Admins`
3. **Chiếm quyền và Duy trì quyền kiểm soát (Golden Ticket):** Với quyền `Domain Admins` (có được nhờ `GenericAll`), trích xuất hash của tài khoản `krbtgt` (khóa vàng của Kerberos). Từ hash `krbtgt`, tạo "Golden Ticket" để thiết lập quyền kiểm soát vĩnh viễn trên Domain.

Kerberoasting (Tấn công Xác thực)



- **Nguyên lý:** Kẻ tấn công (từ máy Kali với tư cách `analyst`) yêu cầu KDC (trên VDT-DC01) cấp Service Ticket cho SPN (`HTTP/webapp.vdt.local`) của `svc_webapp`. KDC trả về vé được mã hóa bằng NT hash của `svc_webapp`. Kẻ tấn công trích xuất hash từ vé và dùng công cụ như `Hashcat` để bẻ khóa mật khẩu `password123` của `svc_webapp` offline
- **Công cụ chính:** `Impacket's GetUserSPNs.py`, `Hashcat`

Leo quyền lên DC qua abuse ACLs (GenericAll)

- **Nguyên lý:** Sau khi có mật khẩu của `svc_webapp`, kẻ tấn công sẽ dùng tài khoản này để phân tích các quyền hạn trong AD. Cụ thể, lợi dụng việc `svc_webapp` đã được cấu hình sai với quyền `WriteDACL` trên đối tượng Domain `vdt.local`. Quyền này cho

phép `svc_webapp` tự sửa đổi DACL của đối tượng Domain, từ đó tự cấp cho mình quyền `GenericAll` trên Domain. Khi có quyền `GenericAll` trên Domain, tài khoản `svc_webapp` có thể thêm mình vào nhóm `Domain Admins`, từ đó chiếm quyền quản trị miền.

- **Công cụ chính:** `BloodHound` (để phân tích các đường tấn công từ `svc_webapp` đến `Domain Admins`), Impacket's `addacl.py` (hoặc `PowerView` nếu có shell PowerShell trên DC) để sửa đổi ACL và tự cấp quyền.

Chiếm quyền và Duy trì quyền kiểm soát (Golden Ticket)

- **Golden Ticket (Authentication Attack - Duy trì quyền):** Sau khi `svc_webapp` đã được thêm vào nhóm `Domain Admins` (nhờ quyền `GenericAll`), kẻ tấn công có quyền quản trị miền. Lúc này, kẻ tấn công sẽ trích xuất NT hash của tài khoản `krbtgt` (khóa vàng của Kerberos) từ DC (thông qua `secretsdump.py`). Từ hash `krbtgt`, kẻ tấn công sử dụng `Mimikatz` để tạo ra một Kerberos Ticket-Granting Ticket (TGT) giả mạo. TGT này có thể được tạo cho bất kỳ người dùng nào (thường là một tài khoản giả mạo hoặc `Administrator`) với quyền hạn cao nhất trong miền và thời gian sống tùy ý, cho phép duy trì quyền kiểm soát ngay cả khi mật khẩu gốc bị thay đổi
- **Công cụ chính:** `Impacket's secretsdump.py`, `Mimikatz`

Khuyến nghị và cách phòng chống

- Sử dụng mật khẩu mạnh và phức tạp cho tài khoản dịch vụ
- Triển khai Managed Service Accounts (MSAs) và Group Managed Service Accounts (gMSAs):
  - MSAs và gMSAs là các tài khoản dịch vụ được quản lý tự động bởi Active Directory. Chúng có mật khẩu dài, ngẫu nhiên và tự động thay đổi thường xuyên mà không cần quản trị viên can thiệp. Điều này giúp loại bỏ rủi ro mật khẩu yếu và lỗi cấu hình SPN do con người.
- Hạn chế quyền hạn của tài khoản dịch vụ
- Giám sát và phát hiện:
  - Giám sát Event 4769 (Kerberos Service Ticket Operations): Giám sát các sự kiện yêu cầu Service Ticket
  - Giám sát Event ID 4732/4733 (thay đổi thành viên nhóm bảo mật): Phát hiện khi các tài khoản được thêm hoặc xóa khỏi các nhóm quan trọng như Domain Admins.
  - Giám sát Event ID 4767 (thay đổi ACL trên đối tượng): Phát hiện các thay đổi bất thường về quyền truy cập trên các đối tượng AD quan trọng
  - Sử dụng các giải pháp SIEM/EDR: Triển khai các hệ thống Security Information and Event Management (SIEM) và Endpoint Detection and Response (EDR) để phát hiện các hoạt động đáng ngờ như việc yêu cầu Service Ticket hàng loạt, hoặc các công cụ tấn công được sử dụng
- Định kỳ kiểm tra các SPN đã đăng ký trong AD để đảm bảo rằng chúng hợp lệ
- Thường xuyên chạy các công cụ như `BloodHound` hoặc `PowerView` để kiểm tra các mối quan hệ ủy quyền trong AD
- Tách biệt tài khoản quản trị:
  - Tiered Administration Model: Triển khai mô hình quản trị phân cấp (Tiered Administration Model) để tách biệt các tài khoản quản trị viên theo cấp độ rủi ro (ví dụ: Tier 0 cho Domain Admins, Tier 1 cho quản trị viên ứng dụng/server, Tier 2 cho quản trị viên máy trạm
  - Sử dụng Workstation được bảo vệ (PAWs - Privileged Access Workstations): Buộc các tài khoản quản trị cấp cao chỉ đăng nhập từ các máy trạm chuyên dụng, được bảo vệ nghiêm ngặt.