Xây dựng và Khai thác Hệ thống Active Directory Phức tạp

Setup Bổ sung/Điều chỉnh:

1. **DC01:**
   - Giữ `vdt.local`.
   - Giữ `dev01` (AS-REP Roasting, mật khẩu yếu).
   - Tạo user `admin_service`.
   - **Cấu hình NULL Session RID Cycling** (Như yêu cầu trước của bạn).
   - **Cấu hình ACL:** Cấp cho `dev01` quyền `GenericWrite` (hoặc ít nhất là `WriteProperty` + `ResetPassword`) trên `admin_service`.
   - **Cấu hình RBCD:** Cấp cho `admin_service` quyền sửa thuộc tính `msDS-AllowedToActOnBehalfOfOtherIdentity` của **chính nó** (hoặc của một máy tính, ví dụ `WS01`). Cách dễ nhất là cấp `GenericWrite` cho `admin_service` trên `WS01`.
2. **WS01:**
   - Join domain.
   - Bật WinRM (cho phép `Domain Users`).
   - Tạo một máy tính `WS01`.
3. **Kali:**
   - Đầy đủ tools.

Luồng Tấn công Mới :

1. **Giai đoạn 1: Recon**
   - `Nmap`: Tìm DC, WinRM.
   - `Netexec`: RID Cycling qua NULL session -> Lấy `userlist.txt`.
2. **Giai đoạn 2: Initial Access
   - `GetNPUsers.py`: Dùng `userlist.txt` -> Tìm `dev01` -> Lấy hash AS-REP.
   - `Hashcat`: Crack hash -> Có pass `dev01`.
3. **Giai đoạn 3: Recon Nội bộ & Lập kế hoạch**
   - `Evil-WinRM`: Dùng `dev01` vào WS01.
   - `SharpHound`: Chạy từ WS01 -> Phân tích bằng BloodHound.
   - **Kết quả:** BloodHound sẽ chỉ ra đường `dev01` -> `GenericWrite` -> `admin_service`. Nó cũng có thể chỉ ra `admin_service` -> `GenericWrite` -> `WS01` (Nếu setup như trên).
4. **Giai đoạn 4: Leo thang qua ACL & RBCD**
   - **Chiếm `admin_service`:**
     - Từ WS01 (quyền `dev01`), dùng PowerShell `Set-ADAccountPassword` hoặc `net user` để đổi pass `admin_service`.
   - **Thiết lập RBCD:**
     - Dùng `evil-winrm` vào WS01 *với tư cách* `admin_service`.
     - Dùng `BloodyAD` hoặc PowerShell AD module (cài trên WS01) để sửa thuộc tính `msDS-AllowedToActOnBehalfOfOtherIdentity` của `WS01`, thêm `admin_service` vào đó. Lệnh tương tự: `rbcd.py 'vdt.local/admin_service:NewPass' -delegate-to WS01$ -action write ...` (Chạy từ Kali).
   - **S4U Abuse:**
     - Dùng `getST.py` với `admin_service` để yêu cầu ticket mạo danh `Administrator` *đến* `WS01$`.
     - Lệnh: `getST.py -spn cifs/ws01.vdt.local -impersonate Administrator 'vdt.local/admin_service:NewPass'`.
   - **Kết quả:** Có được ticket (TGS) của `Administrator` để truy cập `WS01`.
5. **Giai đoạn 5: Chiếm Domain**
   - **Truy cập WS01 (Admin):**
     - Dùng ticket vừa lấy với `impacket-psexec` hoặc `evil-winrm -k` để có shell *Admin* trên `WS01`.
     - Lệnh: `KRB5CCNAME=Administrator.ccache impacket-psexec -k -no-pass ws01.vdt.local`.
   - **Dump LSASS:**
     - Khi đã là Admin/System trên WS01, dùng `Mimikatz` (tải lên) để dump bộ nhớ LSASS: `sekurlsa::logonpasswords`.
   - **Phân tích:** Tìm kiếm hash NTLM của Domain Admin (nếu có ai đó đã đăng nhập vào WS01, hoặc có thể tìm hash máy tính DC). *Nếu không có DA, đây là điểm dừng.*
   - **Hướng Tin cậy hơn:** Nếu `admin_service` (hoặc user nó có thể chiếm được) có quyền **DCSync**, thì dùng `secretsdump.py` ngay từ bước có ticket RBCD (nếu ticket có thể dùng cho `ldap/dc01`) hoặc sau khi lên Admin trên WS01 (nếu WS01 có thể kết nối DC). *Để đơn giản, có thể cấp quyền DCSync cho `admin_service` trong setup lab.*

- **Giả sử có DCSync:** Dùng `secretsdump.py` với creds `admin_service` (nếu có quyền) hoặc ticket RBCD (nếu có thể) để dump hash `krbtgt`.
- **Golden Ticket:** Tạo và sử dụng Golden Ticket để vào DC01.

Bước 0: Cấu hình Mạng 🌐

- **(Như cũ):** Tạo mạng ảo riêng (VMnet/Host-only) `192.168.198.0/24`, **tắt DHCP**. Kết nối tất cả các VM vào mạng này.

Bước 1: Cài đặt và Cấu hình DC01 👑

1. **Cài đặt & Nâng cấp DC:**
   - **(Như cũ):** Tạo VM `DC01`, cài Win Server, đặt IP `192.168.198.10`, DNS `127.0.0.1`. Cài AD DS & DNS, nâng cấp lên DC với domain `vdt.local`.
2. **Tạo Users:**
   - **(Như cũ, nhưng chỉ 2 user):** Mở ADUC, tạo:
     - `dev01`: Mật khẩu yếu (`Password123!`), không đổi mk, không hết hạn.
     - `admin_service`: Mật khẩu mạnh.
3. **Cấu hình AS-REP Roasting (`dev01`):**
   - **Hành động:** Trong ADUC, tìm `dev01`, vào `Properties` -> `Account` -> Tick ô `Do not require Kerberos preauthentication`.
   - **Giải thích:** Tạo lỗ hổng AS-REP Roasting cho `dev01`.
   - *(Cấu hình đúng: Ô được tick).*
4. **Cấu hình ACL Abuse (`dev01` -> `admin_service`):**
   - **Hành động:** Trong ADUC, bật `Advanced Features`. Tìm `admin_service`, `Properties` -> `Security` -> `Advanced` -> `Add`. Chọn `dev01`, cấp quyền `Allow` cho `Write all properties` và `Reset password`.
   - **Giải thích:** Cấp cho `dev01` quyền chiếm `admin_service`.
   - *(Cấu hình đúng: `dev01` xuất hiện trong ACL của `admin_service` với quyền đã cấp).*
5. **Cấu hình Cho phép NULL Session RID Cycling (Qua GPO):**
   - **Hành động:** Mở GPMC, edit `Default Domain Controllers Policy`. Đi đến `Computer Configuration` -> `Policies` -> `Windows Settings` -> `Security Settings` -> `Local Policies` -> `Security Options`. Thay đổi các chính sách sau:
     - `Network access: Allow anonymous SID/Name translation`: `Enabled`.
     - `Network access: Do not allow anonymous enumeration of SAM accounts`: `Disabled`.
     - `Network access: Do not allow anonymous enumeration of SAM accounts and shares`: `Disabled`.
     - `Network access: Let Everyone permissions apply to anonymous users`: `Enabled`.
   - Chạy `gpupdate /force`.
   - **Giải thích:** Nới lỏng các hạn chế mặc định để cho phép `nxc` thực hiện RID Cycling bằng NULL session.
   - *(Cấu hình đúng: Các chính sách được áp dụng).*
6. **Cấu hình WinRM (Qua GPO):**
   - **Hành động:** Tạo GPO mới (`Enable_WinRM_ForAllUsers`), link vào `vdt.local`. Edit GPO:
     - **Bật Dịch vụ:** `Computer Configuration` -> `Policies` -> `Windows Settings` -> `Security Settings` -> `System Services` -> `Windows Remote Management (WS-Management)` -> `Automatic`.
     - **Bật Listener:** `Computer Configuration` -> `Policies` -> `Administrative Templates` -> `Windows Components` -> `Windows Remote Management (WinRM)` -> `WinRM Service` -> `Allow remote server management through WinRM` -> `Enabled`, IP Filters: `*`.
     - **Cấp Quyền:** `Computer Configuration` -> `Policies` -> `Windows Settings` -> `Security Settings` -> `Restricted Groups`. Click chuột phải -> `Add Group...`. Group: `Remote Management Users`. Trong cửa sổ mới, dưới `Members of this group:`, click `Add...`. Gõ `VDT\Domain Users`. Click `OK`.
   - Chạy `gpupdate /force` trên DC01 (và lát nữa trên WS01).
   - **Giải thích:** Bật WinRM, mở firewall và cho phép tất cả `Domain Users` có quyền kết nối từ xa.
   - *(Cấu hình đúng: Dịch vụ WinRM chạy, cổng 5985 mở, Domain Users là thành viên nhóm Remote Management Users).*

Bước 2: Cài đặt và Cấu hình WS01 💻

1. **Cài đặt & Join Domain:**
   - **(Như cũ):** Tạo VM `WS01`, cài Win 10/11, đặt IP `192.168.198.13`, DNS `192.168.198.10`. Join domain `vdt.local`.

2. **Cập nhật GPO:**
   - **Hành động:** Khởi động lại WS01 hoặc chạy `gpupdate /force`.
   - **Giải thích:** Đảm bảo WS01 nhận GPO `Enable_WinRM_ForAllUsers`.
   - *(Cấu hình đúng: WinRM chạy trên WS01, có thể kết nối từ Kali bằng `dev01`).*
3. **Cấu hình RBCD (`admin_service` -> `WS01`):**
   - **Hành động:** Quay lại **DC01**. Mở **ADUC**. Tìm máy tính `WS01` (trong OU `Computers` hoặc OU bạn đã chuyển vào). Click chuột phải -> `Properties`.
   - Chuyển sang tab `Security`. Click `Advanced`.
   - Click `Add`. Chọn Principal `admin_service`.
   - Cấp quyền `Allow` cho `GenericWrite`. Click `OK` 3 lần.
   - **Giải thích:** Cấp cho `admin_service` quyền ghi *tất cả* thuộc tính của đối tượng máy tính `WS01`. Quyền này đủ mạnh để `admin_service` có thể tự cấu hình RBCD, cho phép nó mạo danh người dùng khác *đến* WS01.
   - *(Cấu hình đúng: `admin_service` có quyền `GenericWrite` trên `WS01`).*

Bước 3: Cài đặt Kali Linux ⚔️

- **(Như cũ):** Đặt IP `192.168.198.100`, DNS `192.168.198.10`. Cập nhật và cài `nmap`, `impacket`, `hashcat`, `evil-winrm`, `bloodhound-python`, `neo4j`.

Tóm tắt Luồng Tấn công với Setup Này:

1. **Kali -> Nmap:** Quét mạng.
2. **Kali -> `nxc` (NULL Session):** RID Cycle DC01 -> Lấy `userlist.txt`.
3. **Kali -> `GetNPUsers.py`:** Dùng `userlist.txt` -> Tìm `dev01` -> Lấy hash AS-REP.
4. **Kali -> `hashcat`:** Crack hash -> Có pass `dev01`.
5. **Kali -> `evil-winrm`:** Dùng `dev01` vào WS01.
6. **WS01 -> `SharpHound`:** Chạy thu thập dữ liệu -> Tải về Kali -> Phân tích bằng BloodHound. (Sẽ thấy `dev01` -> `admin_service` qua ACL).
7. **WS01 -> PowerShell:** Dùng `Set-ADAccountPassword` (với quyền `dev01`) để đổi pass `admin_service`.
8. **Kali -> `rbcd.py`:** Dùng `admin_service` (với pass mới) để cấu hình RBCD, cho phép `admin_service` mạo danh người dùng *đến* `WS01`.
9. **Kali -> `getST.py`:** Dùng `admin_service` (với pass mới) + RBCD để lấy ticket mạo danh `Administrator` *đến* `cifs/ws01.vdt.local`.
10. **Kali -> `impacket-psexec -k`:** Dùng ticket mạo danh để có shell System trên WS01.
11. **WS01 (System Shell) -> Mimikatz:** Tải Mimikatz lên -> Chạy `sekurlsa::logonpasswords` -> Dump hash Domain Admin (nếu có ai đăng nhập) hoặc các hash khác.
12. **Kali -> `impacket-psexec` (PtH):** Dùng hash DA tìm được để vào DC01. **-> Domain Admin!**

Thiết lập này đã loại bỏ các phần phức tạp như KCD đa tầng, GPO Linux, GMSA, Cross-Session Relay nhưng vẫn giữ được một chuỗi tấn công đa bước, logic và bao gồm các kỹ thuật AD quan trọng như AS-REP, ACL Abuse và RBCD Abuse, làm cho nó khả thi hơn để học và thực hiện trong một tháng.

Máy WS01

để đánh giá xem kỹ thuật Dump LSASS hay Dump DPAPI có khả năng thành công cao hay không. Trong môi trường doanh nghiệp thực tế, các loại tài khoản sau đây có thể đăng nhập vào một máy trạm như WS01:

1. Người dùng Chính (Primary User):

- **Là ai:** Đây là nhân viên được cấp máy WS01 để làm việc hàng ngày (trong lab của chúng ta, vai trò này có thể coi là `dev01` hoặc một người dùng tương tự).
- **Tần suất đăng nhập: Rất thường xuyên**, hàng ngày.
- **Khả năng lưu mật khẩu (DPAPI): Rất cao**. Họ thường lưu mật khẩu cho:
  - Trình duyệt web (tài khoản cá nhân, công việc).
  - Ứng dụng email (Outlook).
  - Ứng dụng chat (Teams, Zalo...).
  - Kết nối RDP đến các máy khác (nếu họ có nhu cầu).

    - Mật khẩu Wi-Fi.
    - Mật khẩu Windows Vault / Credential Manager cho các ổ đĩa mạng (mapped drives).
- **Khả năng có trong LSASS: Chắc chắn có** khi họ đang đăng nhập. Tuy nhiên, credential của họ thường có đặc quyền thấp.

2. Bộ phận Hỗ trợ Kỹ thuật (Help Desk / IT Support):

- **Là ai:** Nhân viên IT chịu trách nhiệm khắc phục sự cố cho người dùng.
- **Tần suất đăng nhập: Thỉnh thoảng**, khi có sự cố cần xử lý. Họ có thể đăng nhập trực tiếp, qua RDP, hoặc dùng các công cụ điều khiển từ xa (có thể không tạo session đầy đủ).
- **Loại tài khoản sử dụng:**
    - Tài khoản cá nhân của họ (thường có quyền admin cục bộ trên máy trạm).
    - Tài khoản hỗ trợ dùng chung (có thể có quyền admin cục bộ).
    - *Hiếm khi* (và là thực hành rất tệ) dùng tài khoản Domain Admin.
- **Khả năng lưu mật khẩu (DPAPI): Thấp**. Họ thường không lưu mật khẩu khi RDP hoặc dùng tool.
- **Khả năng có trong LSASS: Có thể có** nếu họ đăng nhập gần đây. Hash của tài khoản admin cục bộ (nếu họ dùng) có thể hữu ích cho việc di chuyển ngang nếu mật khẩu đó được dùng lại ở nơi khác.

3. Quản trị viên Hệ thống / Desktop (System / Desktop Administrators):

- **Là ai:** Người chịu trách nhiệm triển khai phần mềm, vá lỗi, cấu hình máy trạm hàng loạt.
- **Tần suất đăng nhập: Ít khi đăng nhập trực tiếp/RDP**. Họ thường dùng các công cụ quản lý tập trung (SCCM, Intune), PowerShell Remoting (WinRM), hoặc script GPO để thực thi tác vụ. Các tác vụ này có thể chạy dưới ngữ cảnh của tài khoản quản trị.
- **Loại tài khoản sử dụng:** Tài khoản quản trị có đặc quyền cao, có thể là Domain Admin hoặc tài khoản quản trị cấp cao khác.
- **Khả năng lưu mật khẩu (DPAPI): Rất thấp**.
- **Khả năng có trong LSASS: Có thể có**, đặc biệt là nếu họ chạy script hoặc dùng WinRM/Psexec bằng tài khoản đặc quyền. Đây là một mục tiêu rất giá trị.

4. Quản trị viên Domain (Domain Administrators - DA):

- **Là ai:** Tài khoản có quyền cao nhất trong domain.
- **Tần suất đăng nhập: Cực kỳ hiếm (lý tưởng là KHÔNG BAO GIỜ)**. Theo các khuyến nghị bảo mật tốt nhất (như mô hình Tier/PAW), DA **không bao giờ** nên đăng nhập vào các máy trạm hoặc máy chủ thành viên thông thường.
- **Tại sao vẫn có thể xảy ra?** Trong thực tế, vì sự tiện lợi hoặc trong trường hợp khẩn cấp, đôi khi DA vẫn đăng nhập vào máy trạm. Đây là một **thực hành cực kỳ tồi tệ** vì nó đặt credential quý giá nhất vào một môi trường có rủi ro cao.
- **Khả năng lưu mật khẩu (DPAPI): Gần như bằng không** (nếu admin có ý thức bảo mật).
- **Khả năng có trong LSASS: Thấp nhưng là mục tiêu "vàng"**. Nếu một DA vừa đăng nhập vào WS01, việc dump LSASS vào thời điểm đó gần như chắc chắn sẽ mang lại quyền kiểm soát toàn bộ domain.

5. Tài khoản Dịch vụ (Service Accounts):

- **Là ai:** Các tài khoản được dùng để chạy các dịch vụ/ứng dụng trên máy trạm (ví dụ: agent của phần mềm diệt virus, agent backup...).
- **Tần suất đăng nhập:** Liên tục (dưới dạng Logon Type 5 - Service).
- **Khả năng lưu mật khẩu:** Mật khẩu được lưu trong cấu hình dịch vụ hoặc LSA, có thể dump được bằng các kỹ thuật khác nhau (không hẳn là DPAPI/LSASS theo nghĩa thông thường).
- **Khả năng có trong LSASS: Có**. Hash của chúng thường có trong LSASS. Nếu tài khoản dịch vụ có đặc quyền cao, đây cũng là mục tiêu tốt.

Kết luận cho bài lab của bạn:

- Khi bạn dump LSASS trên WS01, bạn **chắc chắn** sẽ thấy `dev01` (nếu bạn đăng nhập bằng nó qua WinRM). Bạn cũng có thể thấy `admin_service` (nếu bạn dùng nó để WinRM).
- Việc tìm thấy `Administrator` trong LSASS trên WS01 là **khó xảy ra trong thực tế**, nhưng trong lab, bạn **có thể cố tình RDP từ WS01 đến DC01 bằng tài khoản Administrator** (hoặc ngược lại, RDP từ DC01 đến WS01) *ngay trước khi* dump LSASS để đảm bảo rằng bạn sẽ tìm thấy hash của nó. Điều này giúp bạn hoàn thành kịch bản học tập, dù nó không phản ánh 100% thực tế bảo mật tốt nhất.
- Dump DPAPI trên WS01 có thể tìm thấy mật khẩu web/ứng dụng của `dev01`, nhưng khả năng tìm thấy mật khẩu DA là rất thấp.

Cấu hình và Hành động Mô phỏng trên WS01

Mục tiêu: Đảm bảo credential của Domain Admin (`VDT\Administrator`) tồn tại trong bộ nhớ LSASS hoặc được lưu trong DPAPI/Windows Vault trên WS01.

1. User Đăng nhập Chính

- **Hành động:** Khởi động máy ảo `WS01`. Khi màn hình đăng nhập hiện ra, hãy **đăng nhập bằng tài khoản** `VDT\Administrator` (sử dụng mật khẩu bạn đã đặt khi cài đặt DC01).
- **Giải thích:** Đây là bước **quan trọng nhất**. Việc đăng nhập tương tác (Interactive Logon) bằng tài khoản Domain Admin sẽ nạp hash NTLM và có thể cả Kerberos ticket của tài khoản này vào bộ nhớ của tiến trình LSASS.
- **Trạng thái:** Bạn có thể **để nguyên session này đang chạy** (không log off, chỉ có thể khóa màn hình - Lock Screen) hoặc log off. Việc để session chạy (hoặc mới log off) sẽ tăng khả năng credential còn tồn tại trong LSASS khi kẻ tấn công vào được.

2. Setting Lưu Mật khẩu (Tùy chọn, để tăng khả năng thành công DPAPI)

- **Hành động:** Khi đang đăng nhập bằng `VDT\Administrator` trên `WS01`:
  1. Mở **Remote Desktop Connection** (`mstsc.exe`).
  2. Nhập `DC01` (hoặc `192.168.198.10`) vào ô `Computer`.
  3. Click `Show Options`.
  4. Trong tab `General`, nhập `VDT\Administrator` vào ô `User name`.
  5. **Quan trọng:** Tick vào ô `Allow me to save credentials`.
  6. Click `Connect`. Khi được hỏi mật khẩu, nhập mật khẩu `Administrator` và **tick vào ô** `Remember me`.
  7. Hoàn thành việc kết nối RDP (bạn có thể đóng ngay sau đó).
- **Giải thích:** Hành động này mô phỏng việc Admin RDP đến DC và *lưu lại* thông tin đăng nhập. Windows sẽ lưu credential này vào **Windows Vault / Credential Manager**, và nó được bảo vệ bởi DPAPI. Điều này tạo cơ hội cho kẻ tấn công (nếu có quyền) dump DPAPI và lấy được mật khẩu.

3. Đảm bảo Trạng thái Hoạt động

- **Hành động:** Để máy `WS01` **luôn bật** trong suốt quá trình bạn thực hiện tấn công từ Kali. Không cần user nào khác (như `dev01`) phải đăng nhập sẵn, vì kẻ tấn công sẽ tự đăng nhập bằng `dev01` qua WinRM.
- **Giải thích:** Máy phải hoạt động để có thể bị tấn công và để session/credential của Administrator còn tồn tại.

Tóm tắt các Hành động Cần Làm trên WS01:

1. Khởi động `WS01`.
2. Đăng nhập bằng `VDT\Administrator`.
3. (Tùy chọn) RDP đến `DC01` và **lưu mật khẩu** `Administrator`.
4. Để `WS01` chạy (có thể khóa màn hình hoặc log off, nhưng tốt nhất là để session chạy hoặc vừa log off).
5. Bắt đầu tấn công từ Kali.

Bằng cách thực hiện các bước này, bạn đã "dọn đường" sẵn cho giai đoạn cuối của cuộc tấn công. Khi kẻ tấn công có được quyền System trên `WS01`, việc chạy `Mimikatz` để dump LSASS gần như chắc chắn sẽ thu được NTLM hash của `VDT\Administrator`, cho phép thực hiện Pass-the-Hash và chiếm quyền DC01 thành công.