

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**BÁO CÁO BÀI TẬP LỚN**

Đề tài: Kiểm thử dịch vụ Active Directory từ External

Môn: Kiểm Thử Xâm Nhập

Giảng Viên : Đinh Trường Duy

Nhóm Bài tập lớn: 7

**Sinh viên thực hiện:**

Vũ Ngọc Phương B20DCAT142

Ninh Chí Hướng B20DCAT094

Hoàng Trung Kiên B20DCAT098

Nguyễn Văn Khang B20DCAT102

Nguyễn Trần Minh B20DCAT126

Lê Đình Quân B20DCAT146

**Hà Nội – 2024**

**Mục lục**

[A. **Lý thuyết về Active Directory**. 4](#_Toc164007072)

[1. Active Directory là gì? 4](#_Toc164007073)

[2. Các giao thức. 5](#_Toc164007074)

[a) Cơ chế xác thực Kerberos. 5](#_Toc164007075)

[b) Giao thức truy nhập thư mục đơn giản – LDAP. 8](#_Toc164007076)

[3. Uỷ quyền trong Active Directory. 8](#_Toc164007077)

[B. **Printer Bug**. 11](#_Toc164007078)

[1. Khái niệm. 11](#_Toc164007079)

[2. SpoolSample.exe. 12](#_Toc164007080)

[C. **Các công cụ sử dụng và Quy trình**. 13](#_Toc164007081)

[1. Sharphound – Bloohound. 13](#_Toc164007082)

[2. Impacket. 14](#_Toc164007083)

[3. Mimikatz. 14](#_Toc164007084)

[4. Rubeus. 15](#_Toc164007085)

[5. Metasploit. 15](#_Toc164007086)

[6. Quy trình thực hiện. 17](#_Toc164007087)

[D. **Demo**. 17](#_Toc164007088)

[1. Tạo môi trường. 17](#_Toc164007089)

[2. Chiếm máy WEB01. 17](#_Toc164007090)

[3. Chiếm DC. 21](#_Toc164007091)

[E. **Quy trình kiểm thử Active Directory chung**. 23](#_Toc164007092)

[F. **Kết luận và biện pháp**. 23](#_Toc164007093)

[**Tài liệu tham khảo** 24](#_Toc164007094)

**Lời mở đầu**

Ngày nay, các hệ thống thông tin hiện đại trở nên ngày càng phức tạp với kiến trúc mạng đa lớp, chứa nhiều ứng dụng, dịch vụ và có môi trường máy chủ đa dạng. Sự phức tạp này cũng dẫn đến việc bảo vệ dữ liệu và các tài sản thông tin quan trọng ngày càng khó khăn hơn. Kèm theo đó, gần đây cũng xuất hiện nhiều nhóm tội phạm Internet được tổ chức rất bài bản, đã thực hiện nhiều cuộc tấn công quy mô lớn vào các hệ thống của doanh nghiệp, tổ chức. Phát hiện ra các cuộc tấn công này là một trong những vấn đề được quan tâm rất lớn của cộng đồng.

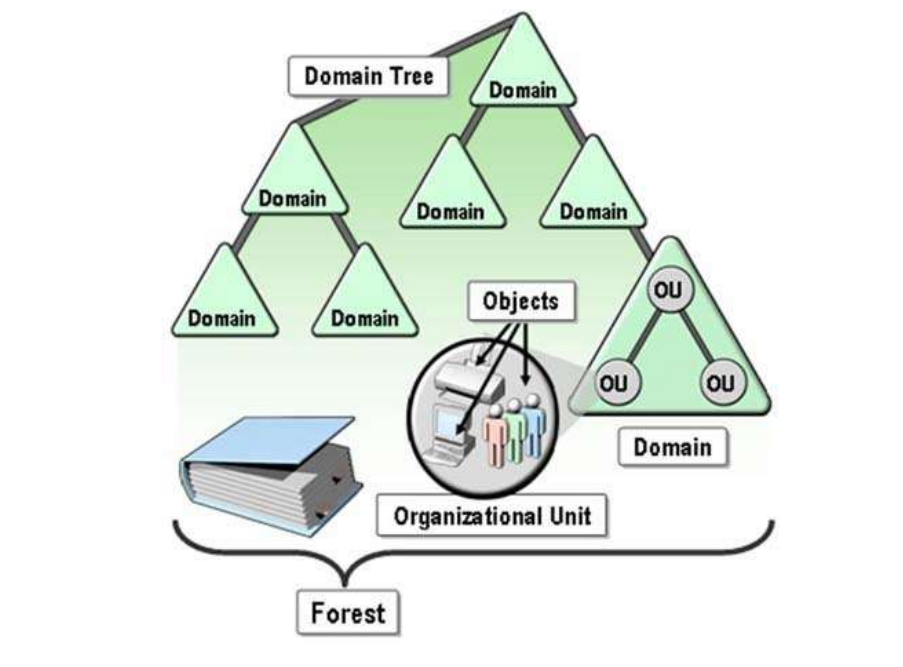
Mặc dù có nhiều hình thức đảm bảo an toàn cho các hệ thống thông tin nhưng một trong những phương pháp tin cậy nhất để biết mức độ an toàn là tự thực hiện việc kiểm tra đánh giá. Các hoạt động kiểm thử xâm nhập được thực hiện một cách đúng đắn sẽ có khả năng mô phỏng được các hành vi của kẻ tấn công, và từ đó cho biết được tình trạng an toàn của hệ thống trong tổ chức.

Trong quá trình thực hiện bài tập lớn, chúng ta sẽ xem xét các kỹ thuật phổ biến như kiểm thử xâm nhập ứng dụng web, mạng, hệ điều hành, cơ sở dữ liệu và các phương thức tấn công khác. Chúng ta cũng sẽ tìm hiểu về các công cụ và kỹ năng cần thiết để thực hiện kiểm thử xâm nhập một cách hiệu quả, giúp chúng ta hiểu rõ hơn về phương pháp và kỹ thuật kiểm thử xâm nhập, từ việc xác định mục tiêu, thu thập thông tin, tiến hành phân tích, thực hiện cuộc tấn công mô phỏng, đánh giá và báo cáo kết quả.

Bài tập lớn này không chỉ giúp chúng ta nắm vững kiến thức về kiểm thử xâm nhập, mà còn rèn luyện tư duy phân tích, sáng tạo và khả năng xử lý vấn đề trong môi trường thực tế. Ngoài ra, nó cũng giúp chúng ta nhận thức sâu sắc hơn về tầm quan trọng của an ninh mạng và bảo mật thông tin trong thế giới kỹ thuật số ngày nay.

1. **Lý thuyết về Active Directory**.
2. Active Directory là gì?

* Thư mục động (Active Directory) là công nghệ cung cấp dịch vụ thư mục của Microsoft. Về cơ bản, dịch vụ thư mục nhằm lưu trữ, tổ chức, và đảm bảo truy nhập các thông tin trong thư mục. Trong môi trường mạng, dịch vụ thư mục mạng được dùng để xác định, quản lý, quản trị và tổ chức các mục, tài nguyên mạng dùng chung như ổ đĩa, thư mục, máy in, người dùng…
* Các thành phần của thư mục động về mặt lô-gíc bao gồm:
  + Object: là các đối tượng được tạo ra trong Active Directory, ví dụ: user account, computer account, group account.
* Đơn vị tổ chức (Organisation Units): là các đối tượng bên trong một miền cho phép bố trí và nhóm các tài nguyên lại để làm thuận tiện cho công việc quản trị và cho phép ủy thác (delegate) các quyền quản trị.
* Miền (Domain): là đơn vị lô-gíc các máy tính và tài nguyên mạng xác định ranh giới an ninh. Miền sử dụng một cơ sở dữ liệu miền động đơn lẻ để chia sẻ thông tin chung về an ninh và người dùng cho phép quản lý tập trung toàn bộ người dùng, nhóm và tài nguyên mạng. Một cơ quan hay doanh nghiệp có thể có nhiều miền tương ứng với cơ cấu tổ chức.
* Cây (Tree): chứa một hay nhiều miền dùng chung không gian định danh gốc. Có thể hình dung cây tập hợp các miền chia sẻ không gian tên Internet như fit.ptit.edu.vn.
* Rừng (Forest): chứa một hay nhiều cây và không gian định danh có thể tách biệt. Miền đầu tiên trong rừng được gọi là miền gốc của rừng (forest root domain).
* Quan hệ tin cậy (Trust relationship): cho phép người dùng từ các miền khác nhau sử dụng tài nguyên mạng của các miền.
* Điểm (Site): Nhóm các máy tính cùng mạng con IP kết nối tốc độ cao với nhau.
  + Máy chủ miền (Domain controller): Trong mỗi miền của thư mục động có máy chủ đặc biệt gọi là máy chủ miền chịu trách nhiệm lưu bản sao thông tin tài khoản và an ninh của miền. Để chống lỗi có thể sử dụng nhiều máy chủ miền. Tất cả các máy chủ miền trong một miền nhận các thay đổi và sao chép các sửa đổi này vào phần miền được lưu trong toàn bộ các máy chủ còn lại. Kết quả, tất các các máy chủ miền đều ngang hàng với nhau và cùng quản lý việc sao lưu.



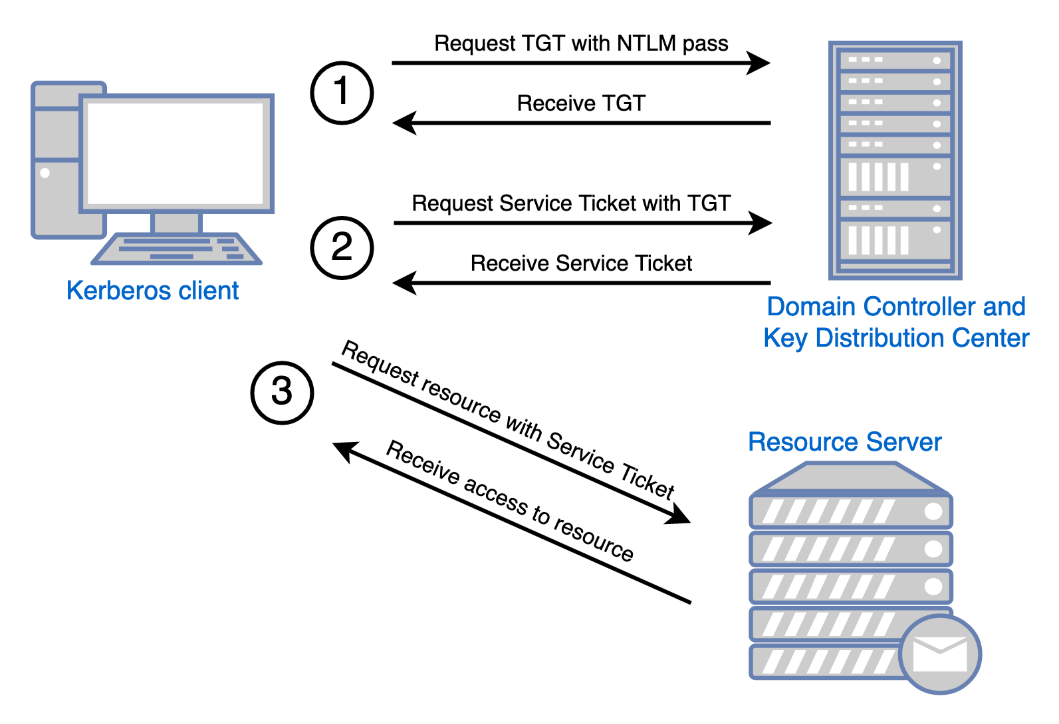
Hình 1. Các thành phần của Active Directory.

1. Các giao thức.

* Thư mục động là công nghệ do Microsoft đưa ra cung cấp một số dịch vụ:
* LDAP (Lightweight Directory Access Protocol),
* Xác thực một lần dựa trên Kerberos,
* Đặt tên dựa trên DNS,
* Quản trị mạng tập trung.

1. Cơ chế xác thực Kerberos.

* Cơ chế xác thực Kerberos sử dụng giao thức xác thực mạng máy tính cho phép các máy xác định định danh của mình qua mạng không an toàn một cách đảm bảo. Nó được phát triển bởi Massachusetts Institute of Technology (MIT) và đã trở thành một phần của các phiên bản Windows từ Windows 2000 trở đi.



Hình 2. Cơ chế xác thực Kerberos

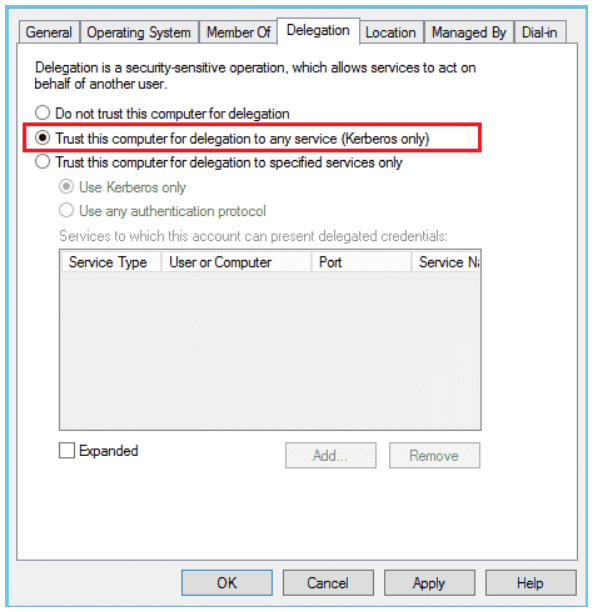
* Các thành phần trung tâm phân phối khóa (Key Distribution Centre – KDC):
  + Máy chủ xác thực (Authentication Server – AS);
  + Máy chủ cấp vé ((Ticket Granting Server – TGS);
  + Cơ sở dữ liệu (Database).
* Ban đầu, giao thức Kerberos được triển khai nhằm cho phép người dùng mạng có thể tự xác thực an toàn và cung cấp quyền truy cập vào các hệ thống. Tại thời điểm này, hầu hết các hệ thống trên mạng đều có phương thức xác thực truyền thống đó là sử dụng ID và [mật khẩu](https://bkhost.vn/blog/password/) không được [mã hóa](https://bkhost.vn/blog/ma-hoa/). Do đó, những kẻ tấn công thường lợi dụng lỗ hổng này để truy cập vào mạng và đánh cắp các thông tin cũng như [dữ liệu](https://bkhost.vn/blog/data-du-lieu/) quan trọng của người dùng.
* Để giải quyết được vấn đề này, các nhà phát triển đã triển khai giao thức xác thực mạng đáng tin cậy đó là Kerberos. Loại giao thức này giúp xác thực các máy chủ trên mạng không đáng tin cậy. Ngoài ra, các quản trị viên hệ thống còn được cung cấp cơ chế xác thực thông qua Internet.
* Cách hoạt động của giao thức Kerberos:
* Yêu cầu máy chủ xác thực: Trước khi bắt đầu quá trình xác thực máy khách Kerberos, máy khách đó sẽ tự tạo một yêu cầu xác thực để gửi đến máy chủ KDC Kerberos. Trong đó, yêu cầu xác thực này được gửi dưới dạng văn bản và đảm bảo rằng không có bất kỳ thông tin nhạy cảm nào được đưa vào yêu cầu đó. Sau đó, máy chủ xác thực sẽ tiến hành xác minh yêu cầu trong cơ sở dữ liệu KDC và truy xuất khóa cá nhân của máy khách đang khởi tạo.
* Máy chủ xác thực phản hồi: Sau khi xác thực yêu cầu được gửi đến, nếu như không tìm thấy tên của người dùng trên ứng dụng khách đang khởi tạo thì quá trình xác thực yêu cầu đó sẽ dừng lại. Nếu tìm thấy tên người dùng thì máy chủ xác thực sẽ gửi cho máy khách một TGT và một khóa phiên.
* Yêu cầu dịch vụ Ticket: Hoàn tất xác thực từ máy chủ, người dùng sẽ tiếp tục gửi đi một yêu cầu cấp dịch vụ Ticket từ TGS. Trong đó, yêu cầu này cần phải đi kèm với TGT được gửi từ máy chủ xác thực KDC.
* Phản hồi dịch vụ Ticket: Nếu như TGS xác thực khách hàng thành công thì nó sẽ gửi về thông tin đăng nhập và Ticket để người dùng có thể bắt đầu truy cập vào dịch vụ. Quá trình này sẽ được mã hóa tự động bằng khóa phiên dành riêng cho người dùng và dịch vụ hiện tại.
* Yêu cầu máy chủ ứng dụng: Máy khách sẽ gửi đến máy chủ ứng một một yêu cầu truy cập với Ticket được nhận từ trước. Máy khách được cấp quyền truy cập chỉ khi máy chủ ứng dụng đồng ý xác thực thành công yêu cầu này.
* Phản hồi của máy chủ ứng dụng: Nếu như máy khách yêu cầu máy chủ ứng dụng tự động xác thực thì đây gọi là phản hồi bắt buộc. Tức là máy khách đã tự xác thực và phản hồi của máy chủ ứng dụng sẽ bao gồm cả xác thực Kerberos.
* Ưu điểm của Kerberos:
* Bảo mật: Kerberos sử dụng mã hóa mạnh để bảo vệ thông tin đăng nhập của người dùng và dữ liệu truyền tải.
* Tính toàn vẹn dữ liệu: Kerberos đảm bảo rằng dữ liệu truyền tải không bị thay đổi.
* Khả năng chống lại việc phát lại: Kerberos ngăn chặn việc phát lại các yêu cầu xác thực đã được sử dụng trước đây.
* Ủy quyền: Kerberos cho phép người dùng được ủy quyền để thực hiện các hành động thay mặt cho người dùng khác.
* Nhược điểm của Kerberos:
* Độ phức tạp: Kerberos là một giao thức phức tạp có thể khó triển khai và quản lý.
* Tương thích: Kerberos không tương thích với tất cả các hệ điều hành và ứng dụng.
* Yêu cầu về cơ sở hạ tầng: Kerberos yêu cầu một cơ sở hạ tầng PKI để hoạt động.

1. Giao thức truy nhập thư mục đơn giản – LDAP.

* Giao thức mức ứng dụng dùng cổng 389 cho truy vấn và thay đổi dữ liệu sử dụng dịch vụ thư mục mạng trên TCP/IP.
* Các đối tượng trong thư mục được tổ chức theo giới hạn của cơ quan hay địa lý.
* Thư mục LDAP được tổ chức theo một kiến trúc cây đơn giản gồm:
  + Thư mục gốc,
  + Country,
  + Organizations,
  + Organizational units,
  + Individuals

1. Uỷ quyền trong Active Directory.

* Unconstrained Delegation (ủy quyền) là sự cho phép 1 tài khoản hoặc một máy tính trong domain có thuộc tính Delegate được tùy chọn để ủy quyền máy tính khác truy cập tài nguyên trong mạ ng. Trong Active Directory, nếu một máy tính được tùy chọn “Trust This user/computer for delegation to any service”, nó có thể thay mặt các máy tính khác truy cập dịch vụ.

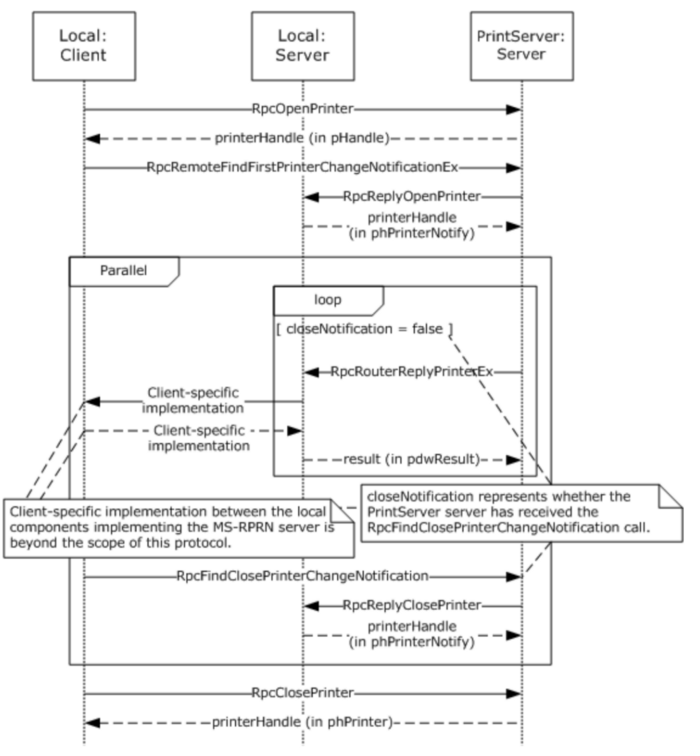


Hình 3. Unconstrained Delegation trong AD

* Nếu thuộc tính Delegation được tùy chọn, Web Server có thể mạo danh người dùng đã xác thực và chuyển thông tin xác thực của họ để yêu cầu dữ liệu từ database.
* Nếu 1 Attacker có thể dump TGT tickets của tất cả các tài khoản được xác thực từ Unconstrained Delegation Server và một trong những tài khoản này là Domain Admin, Attacker có thể mạo danh để truy cập bất kỳ dịch vụ nào trong Domain với quyền Domain Admin.

1. **Printer Bug**.
2. Khái niệm.

* Printer Bug được coi là một cấu hình bị lạm dụng bởi các đối thủ có trong Giao thức từ xa của hệ thống in Windows (MS-RPRN), trong đó kẻ tấn công có tài khoản người dùng miền có thể sử dụng phương pháp MS-RPRN RpcRemoteFindFirstPrinterChangeNotification để buộc bất kỳ máy nào đang chạy dịch vụ bộ đệm phải xác thực với máy do kẻ tấn công kiểm soát (có ủy quyền không bị ràng buộc) thông qua Kerberos hoặc NTLM. Như vậy chiếm được TGT của tài khoản máy. Nó dựa trên giao thức Gọi thủ tục từ xa (RPC) hỗ trợ các hoạt động in và lưu đệm đồng bộ giữa máy khách và máy chủ, bao gồm kiểm soát lệnh in và quản lý hệ thống in.



Hình 7. MS-RPRN

* Việc lạm dụng này chỉ thực thi 2 phương thức đầu tiên (RpcOpenPrinter và RpcRemoteFindFirstPrinterChangeNotificationEx) và dừng lại sau khi phương thức thông báo trả về mã lỗi cửa sổ khác 0. Kết nối ban đầu giữa mục tiêu (máy chủ máy in) và máy của kẻ tấn công (máy chủ không bị ràng buộc) chỉ cần thiết cho "Lỗi máy in". Khi phương thức RpcOpenPrinter được thực thi, nó cần trả về giá trị ERROR\_SUCCESS.

1. SpoolSample.exe.

* spoolsample.exe là một tệp thực thi được bao gồm trong Windows Server và Windows 10/11. Nó là một phần của công cụ Spoolsample được sử dụng để kiểm tra hoạt động của hệ thống in ấn và xác định các vấn đề tiềm ẩn.
* Spoolsample.exe cũng có thể được sử dụng để thực thi các lệnh Spoolsample cụ thể, chẳng hạn như:
* Gửi các công việc in thử nghiệm
* Kiểm tra trạng thái máy in
* Khắc phục sự cố in ấn
* Công cụ này có thể khai thác lỗi máy in (PrinterBug) để ép buộc các máy chủ Windows xác thực với các máy khác thông qua giao diện MS-RPRN RPC. Điều này cũng có thể thực hiện được thông qua các giao thức khác.

1. **Các công cụ sử dụng và Quy trình**.
2. Sharphound – Bloohound.

* SharpHound là công cụ thu thập dữ liệu chính thức cho BloodHound. Nó được viết bằng C# và sử dụng các hàm Windows API gốc cũng như các hàm không gian tên LDAP để thu thập dữ liệu từ bộ điều khiển miền và hệ thống Windows nối miền.
* SharpHound sẽ tự động xác định người dùng hiện tại của bạn thuộc miền nào, tìm bộ điều khiển miền cho miền đó và bắt đầu phương pháp thu thập “mặc định”. Phương pháp thu thập mặc định sẽ thu thập các thông tin sau từ bộ điều khiển miền:
* Thành viên nhóm bảo mật
* Ủy thác tên miền
* Quyền lạm dụng trên các đối tượng Active Directory
* Liên kết chính sách nhóm
* Cấu trúc cây OU
* Một số thuộc tính từ các đối tượng máy tính, nhóm và người dùng
* Liên kết quản trị SQL
* Ngoài ra, SharpHound sẽ cố gắng thu thập thông tin sau từ mỗi máy tính Windows đã tham gia miền:
* Các thành viên của quản trị viên cục bộ, máy tính để bàn từ xa, COM phân tán và nhóm quản lý từ xa
* Các phiên hoạt động mà SharpHound sẽ cố gắng tương quan với các hệ thống nơi người dùng đăng nhập tương tác
* Khi hoàn tất, SharpHound sẽ tạo một số tệp JSON và đặt chúng vào tệp zip. Kéo và thả tệp zip đó vào GUI BloodHound và giao diện sẽ đảm nhiệm việc hợp nhất dữ liệu vào cơ sở dữ liệu.

1. Impacket.

* Impacket là tập hợp các lớp Python3 tập trung vào việc cung cấp quyền truy cập vào các gói mạng. Impacket cho phép các nhà phát triển Python3 tạo và giải mã các gói mạng một cách đơn giản và nhất quán. Nó bao gồm hỗ trợ cho các giao thức cấp thấp như IP, UDP và TCP, cũng như các giao thức cấp cao hơn như NMB và SMB.
* Impacket có hiệu quả cao khi được sử dụng cùng với tiện ích hoặc gói chụp gói như Pcapy. Các gói có thể được xây dựng từ đầu cũng như được phân tích cú pháp từ dữ liệu thô. Hơn nữa, API hướng đối tượng giúp làm việc với hệ thống phân cấp giao thức sâu trở nên đơn giản.
* Secretdump.py của Impacket sẽ thực hiện nhiều kỹ thuật khác nhau để chuyển các bí mật từ máy từ xa mà không cần thực thi bất kỳ tác nhân nào. Các kỹ thuật bao gồm đọc bí mật SAM và LSA từ các cơ quan đăng ký, loại bỏ hàm băm NTLM, thông tin xác thực văn bản gốc và khóa kerberos cũng như loại bỏ NTDS.dit. Lệnh sau sẽ cố gắng loại bỏ tất cả bí mật từ máy mục tiêu bằng các kỹ thuật đã đề cập trước đó.
* mssqlclient.py là tập lệnh từ bộ sưu tập Impacket có thể được sử dụng để thiết lập kết nối được xác thực đến Máy chủ MS SQL
* psexec.py là một trong nhiều ví dụ về tập lệnh kiểm tra thâm nhập mạnh mẽ cho phép bạn thực thi các lệnh từ xa trên một máy khác.

1. Mimikatz.

* Mimikatz là một công cụ thường được [tin tặc](https://www.sentinelone.com/cybersecurity-101/what-is-a-hacker/) và chuyên gia bảo mật sử dụng để trích xuất thông tin nhạy cảm, chẳng hạn như mật khẩu và thông tin đăng nhập, từ bộ nhớ của hệ thống. Công cụ mimikatz được phát triển lần đầu tiên vào năm 2007 bởi [Benjamin Delpy](https://twitter.com/gentilkiwi). Nó thường được sử dụng để có được quyền truy cập trái phép vào mạng, hệ thống hoặc ứng dụng hoặc để thực hiện các hoạt động độc hại khác, chẳng hạn như leo thang đặc quyền hoặc [di chuyển ngang](https://www.sentinelone.com/cybersecurity-101/lateral-movement/) trong mạng.
* Mimikatz có thể được sử dụng theo nhiều cách khác nhau, tùy thuộc vào mục đích và mục đích của kẻ tấn công. Ví dụ: nó có thể được sử dụng để:
* Trích xuất mật khẩu và thông tin xác thực từ bộ nhớ của hệ thống, cho phép kẻ tấn công truy cập vào mạng, hệ thống hoặc ứng dụng.
* Bỏ qua các cơ chế xác thực, chẳng hạn như [xác thực đa yếu tố](https://www.sentinelone.com/cybersecurity-101/what-is-multi-factor-authentication-mfa/) , bằng cách đánh cắp và sử dụng thông tin xác thực bị đánh cắp.
* Nâng cao đặc quyền trên hệ thống, cho phép kẻ tấn công giành quyền truy cập vào dữ liệu nhạy cảm hoặc thực hiện các hành động độc hại khác.
* Di chuyển ngang trong mạng, cho phép kẻ tấn công truy cập vào các hệ thống hoặc mạng bổ sung.

Nhìn chung, Mimikatz là một công cụ mạnh mẽ mà kẻ tấn công có thể sử dụng để truy cập trái phép vào mạng, hệ thống và ứng dụng cũng như thực hiện các hoạt động độc hại khác.

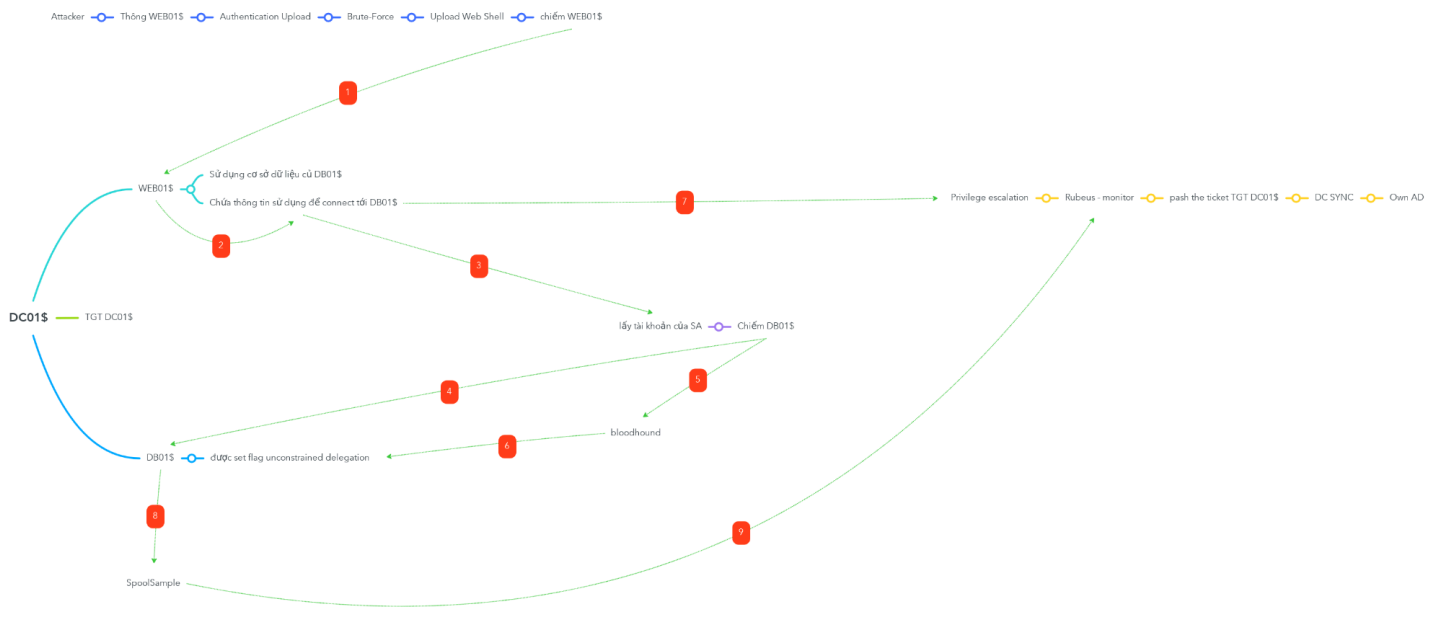
1. Rubeus.

* Rubeus là bộ công cụ C# dành cho tương tác và lạm dụng Kerberos thô. Nó là một công cụ linh hoạt được thiết kế đặc biệt để tương tác với vé Kerberos và hiểu quy trình xác thực.

1. Metasploit.

* **Metasploit** là một nền tảng mã nguồn mở cho việc phát triển, thử nghiệm và sử dụng các kỹ thuật tấn công mạng. Được phát triển bởi Rapid7, Metasploit cung cấp cho các chuyên gia bảo mật, nhà nghiên cứu và haker đạo đức một tập các công cụ khai thác lỗ hổng để kiểm tra tính bảo mật của các hệ thống và ứng dụng. Với Metasploit, người dùng có thể tái hiện các cuộc tấn công mạng thực tế để xác định điểm yếu và cách bảo vệ hệ thống khỏi chúng.
* Quá trình hoạt động của Metasploit bao gồm các bước sau:
* Thu thập thông tin: Công cụ thu thập thông tin về mục tiêu, bao gồm [địa chỉ IP](https://bkhost.vn/blog/dia-chi-ip/), cổng mạng, và các dịch vụ đang hoạt động.
* Phát hiện lỗ hổng: Metasploit sử dụng các module để phát hiện lỗ hổng trong hệ thống và ứng dụng.
* Chọn module tấn công: Dựa trên lỗ hổng được phát hiện, bạn chọn một module tấn công thích hợp.
* Thực hiện cuộc tấn công: Metasploit tận dụng lỗ hổng để thực hiện cuộc tấn công, thường là việc gửi mã độc vào hệ thống mục tiêu.
* Kiểm tra kết quả: Công cụ đánh giá xem cuộc tấn công có thành công hay không và cung cấp thông tin chi tiết về lỗ hổng.
* **Msfvenom** là một công cụ dòng lệnh mạnh mẽ được bao gồm trong Metasploit Framework. Nó được sử dụng để **tạo các payload độc hại** có thể được sử dụng để khai thác lỗ hổng bảo mật và tấn công hệ thống máy tính.
* Chức năng chính của msfvenom:
* Tạo các payload tùy chỉnh: Msfvenom cho phép bạn tạo các payload tùy chỉnh để nhắm mục tiêu vào các hệ thống và ứng dụng cụ thể. Bạn có thể chọn từ nhiều loại payload khác nhau, bao gồm shellcode, backdoor, dropper và trojan.
* Mã hóa payload: Msfvenom có thể mã hóa payload của bạn để che giấu chúng khỏi phần mềm chống vi-rút và các công cụ bảo mật khác.
* Đóng gói payload: Msfvenom có thể đóng gói payload của bạn thành các định dạng tệp khác nhau, chẳng hạn như tệp EXE, tệp PDF hoặc tệp Office.
* Tùy chỉnh payload: Msfvenom cung cấp nhiều tùy chọn để tùy chỉnh payload của bạn, chẳng hạn như thêm các tùy chọn hành động sau khi khai thác thành công hoặc đặt các cờ tùy chỉnh.
* Meterpreter là một tải trọng tấn công Metasploit cung cấp lớp vỏ tương tác mà từ đó kẻ tấn công có thể khám phá máy mục tiêu và thực thi mã. Meterpreter được triển khai bằng cách sử dụng tính năng chèn DLL trong bộ nhớ. Kết quả là Meterpreter nằm hoàn toàn trong bộ nhớ và không ghi gì vào đĩa. Không có quy trình mới nào được tạo khi Meterpreter tự đưa chính nó vào quy trình bị xâm nhập, từ đó nó có thể di chuyển sang các quy trình đang chạy khác. Kết quả là, dấu vết pháp lý của một cuộc tấn công là rất hạn chế.

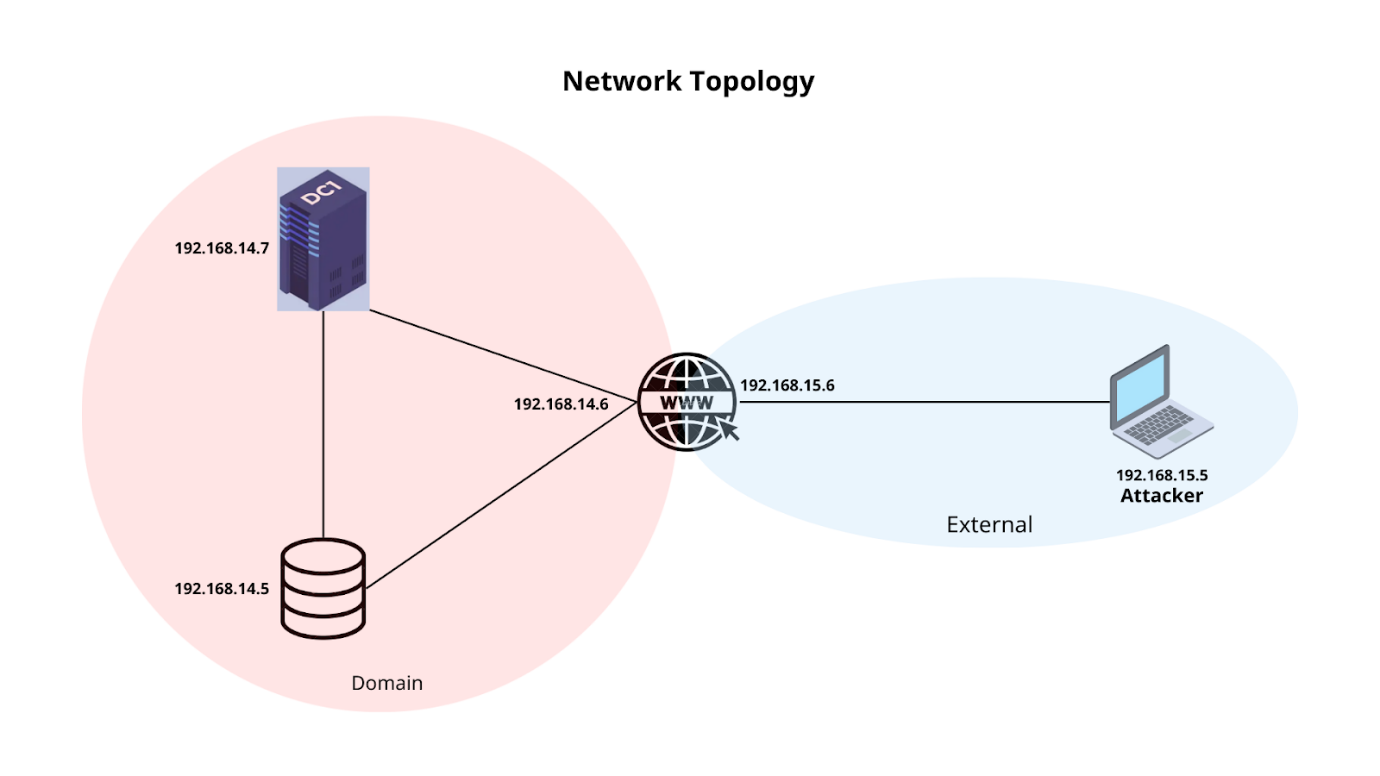
1. Quy trình thực hiện.



Hình 7. Quy trình thực hiện.

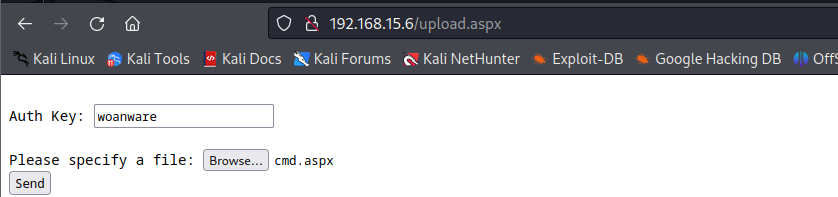
1. **Demo**.
2. Tạo môi trường.

* Cấu hình các máy theo sơ đồ mạng như sau :

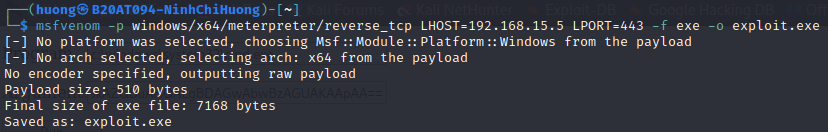


1. Chiếm máy WEB01.

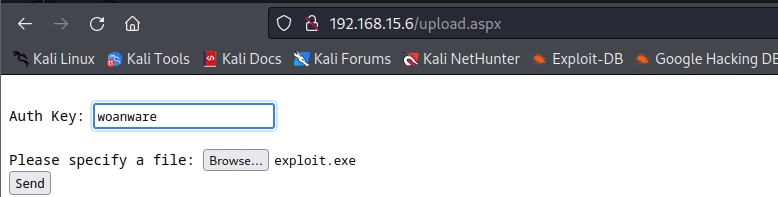
* Upload shell



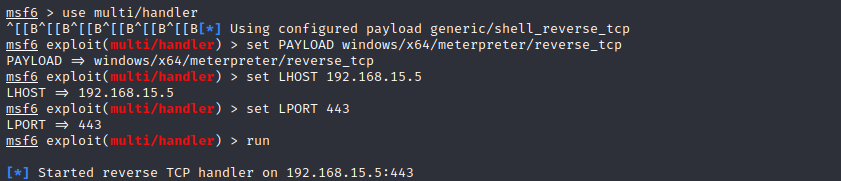
* Tạo file thực thi để lấy về phiên meterpreter



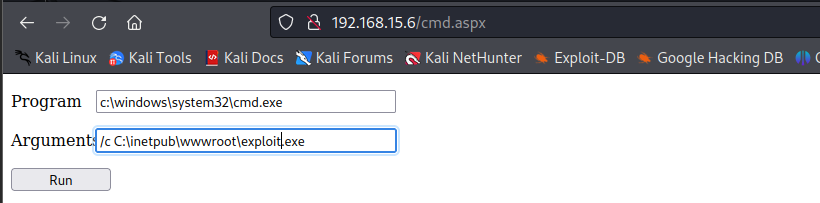
* Upload exploit.exe



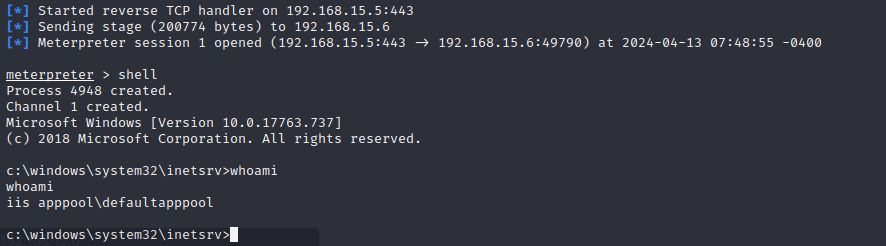
* Tạo trình lắng nghe trên metasploit:



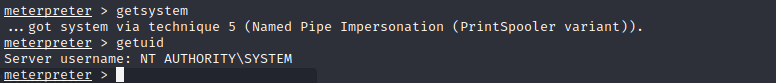
* Thực thi “exploit.exe” thông qua “cmd.aspx” đã upload trước đó:



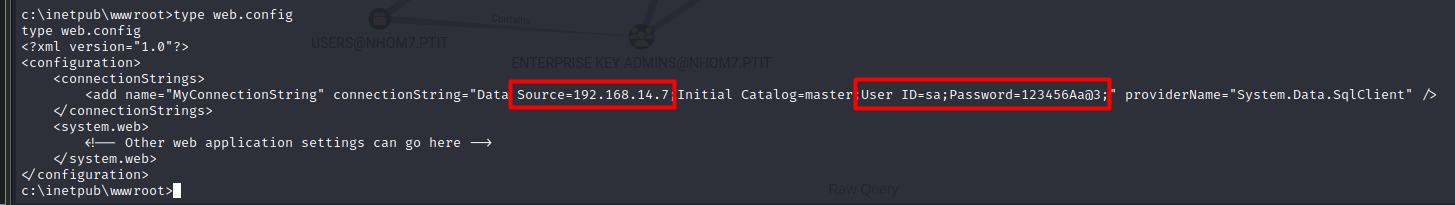
* Lấy được session của máy WEB01



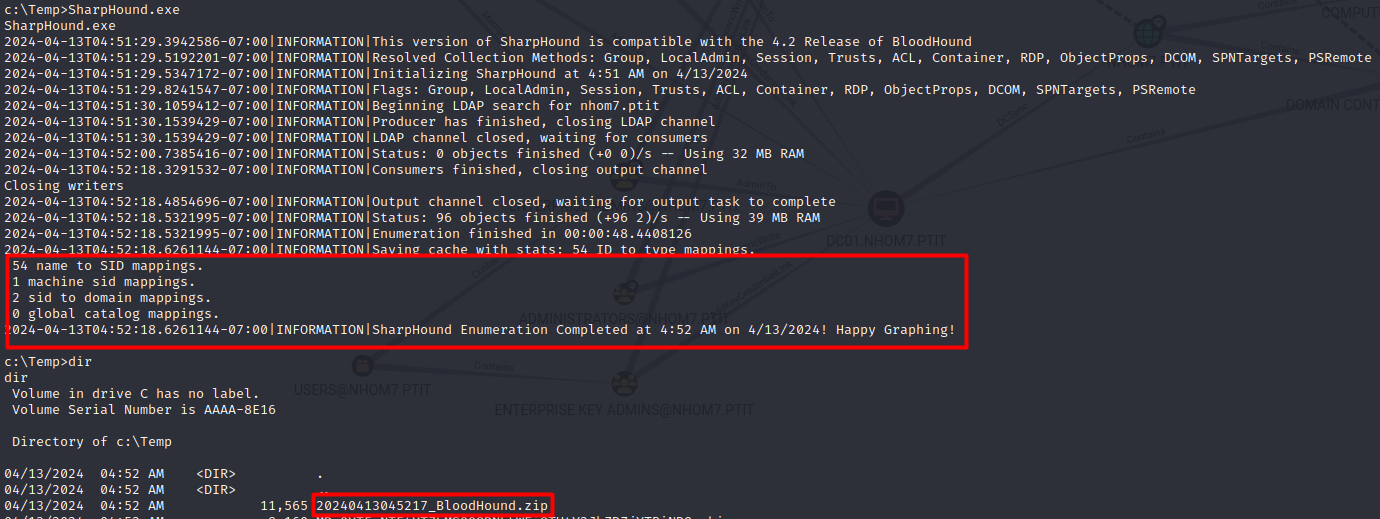
* Thực hiện leo quyền tự động trên WEB01 -> lấy về quyền của SYSTEM



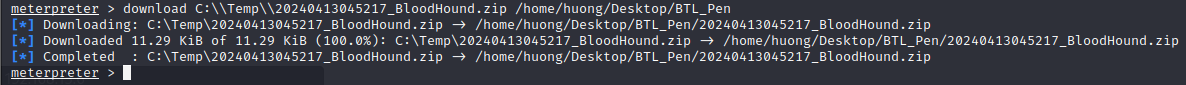
* Thực hiện thu thập tài khoản user trong các file config -> thu được tài khoản quản trị cơ sở dữ liệu của máy DB01:



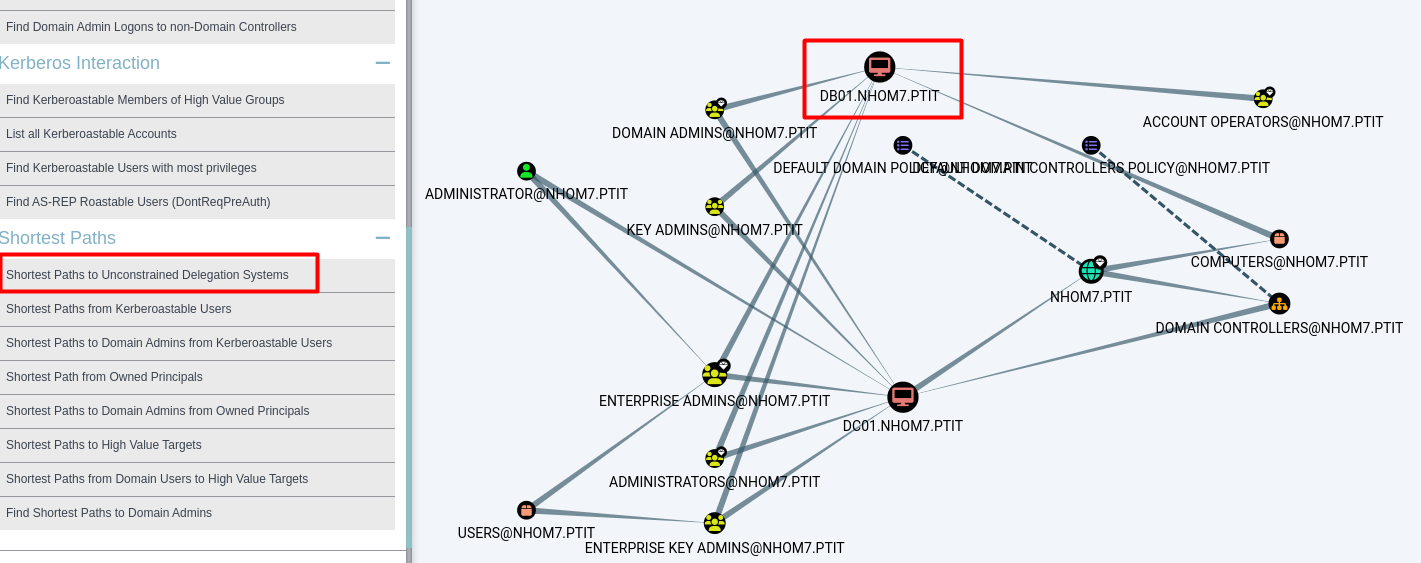
* Thực hiện dump bloodhound trên máy WEB01 để lấy thông tin về toàn bộ domain dưới dạng file zip



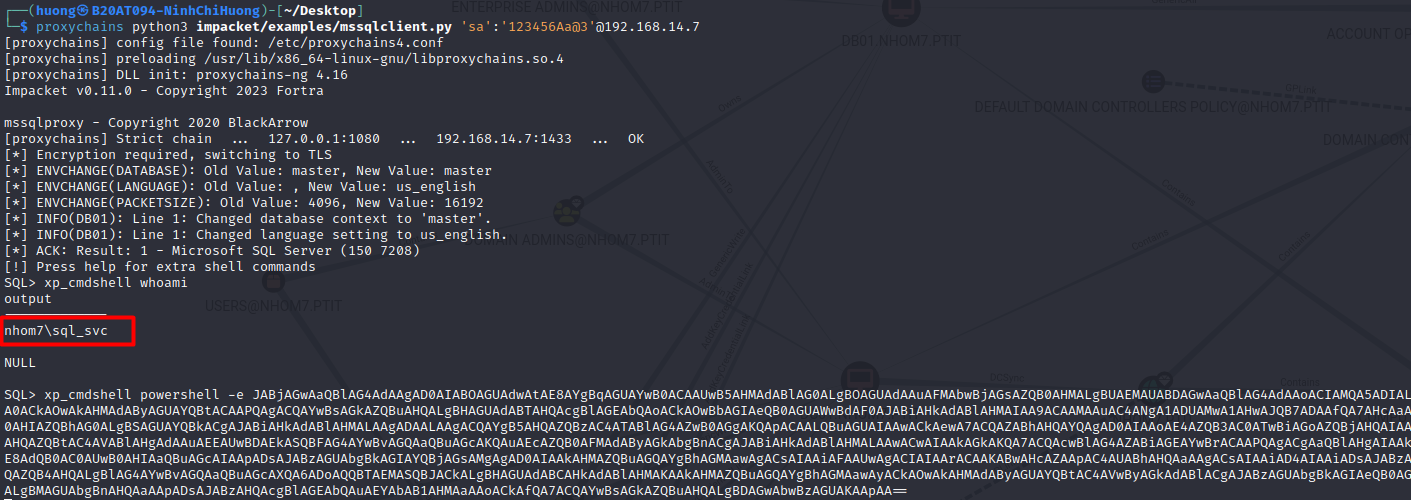
* Sử dụng lệnh tích hợp của meterpreter để download file zip về:



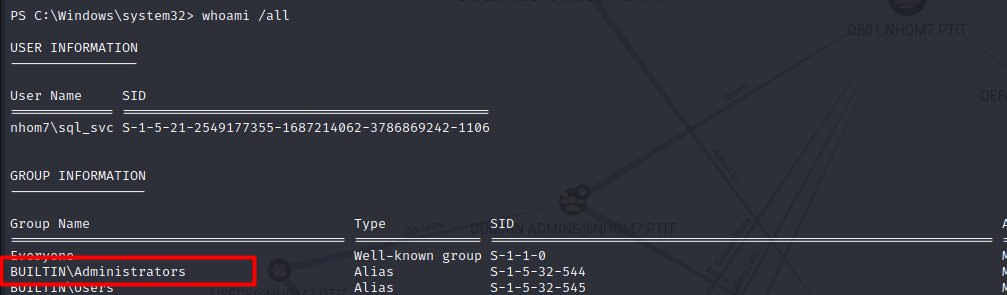
* Upload file zip lên công cụ Bloodhound , sử dụng chức năng tìm kiếm các máy chủ “Uncontrained Delegation System” -> biết được máy “DB01” có tài khoản ip là 192.168.14.7 là máy chủ “Uncontrained” -> ưu tiên thực hiện chiếm quyền điều khiển máy chủ này:



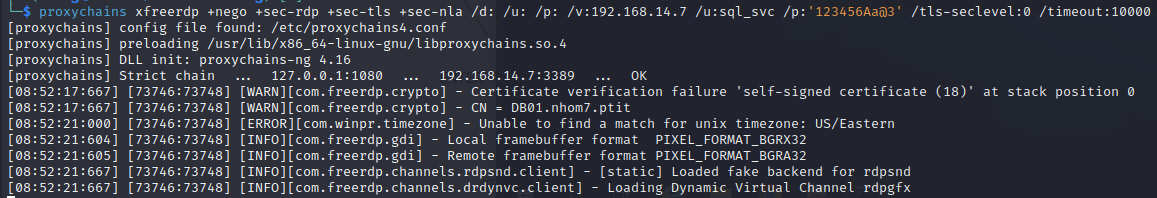
* Do ta có tài khoản quản trị viên cơ sở dữ liệu của máy chủ DB01 -> thực hiện chiếm quyền điều khuyển máy chủ này
* Sử dụng mssqlclient.py để lấy về shell của DB01:

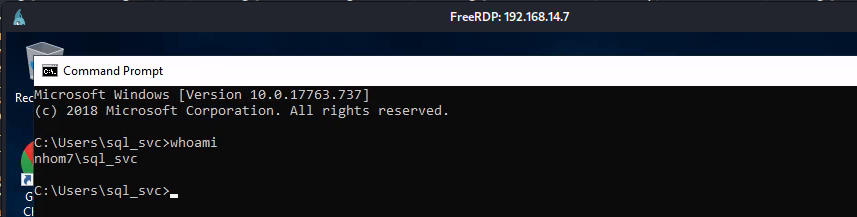


* Theo như shell hiện tại của máy DB01 , ta đang có quyền của người dùng “sql\_svc” trên máy chủ này.Kiểm tra quyền của user ‘sql\_svc’ , ta thấy được user này thuộc group quản trị viên “Administrators”



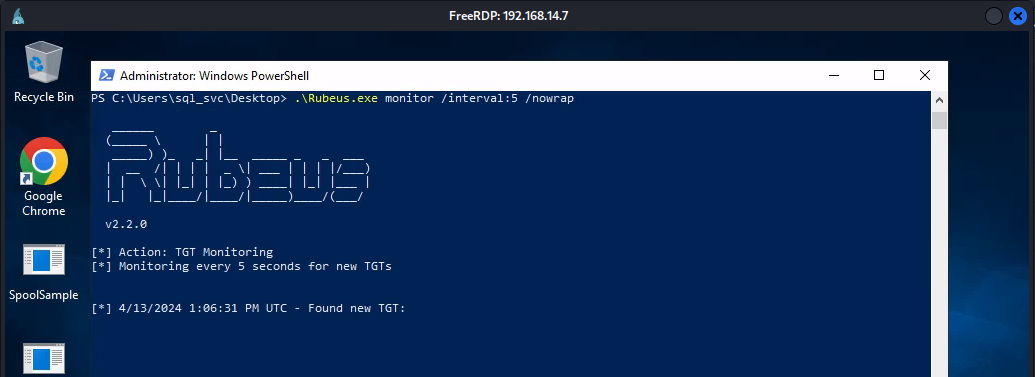
* Bỏ qua bước leo quyền , sử dụng tài khoản của “sql\_svc” để rdp tới máy chủ:



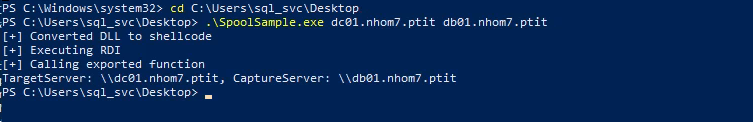


1. Chiếm DC.

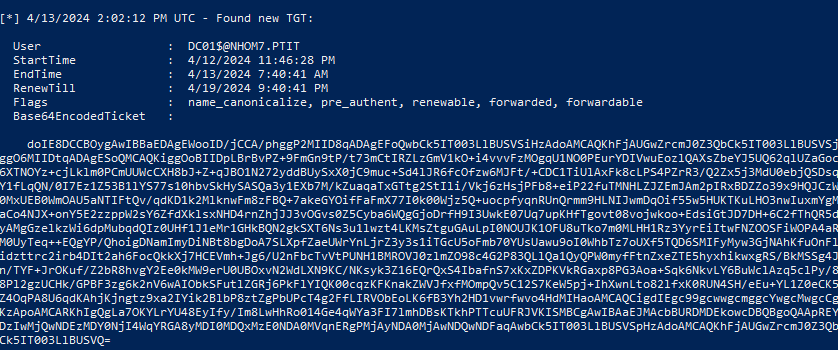
* Trên máy chủ DB01 , tạo trình lắng nghe để bắt ticket của DC01$ trả về sau khi khai thác lỗi máy in:



* Chạy công cụ khai thác lỗi máy in



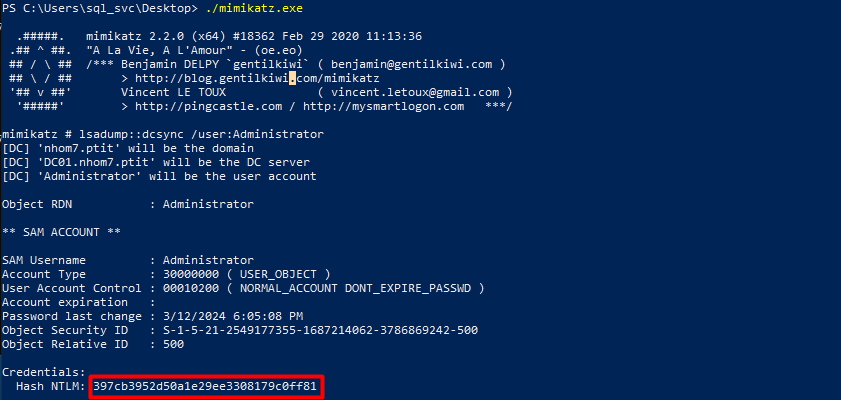
* Lấy về TGT của DC01$



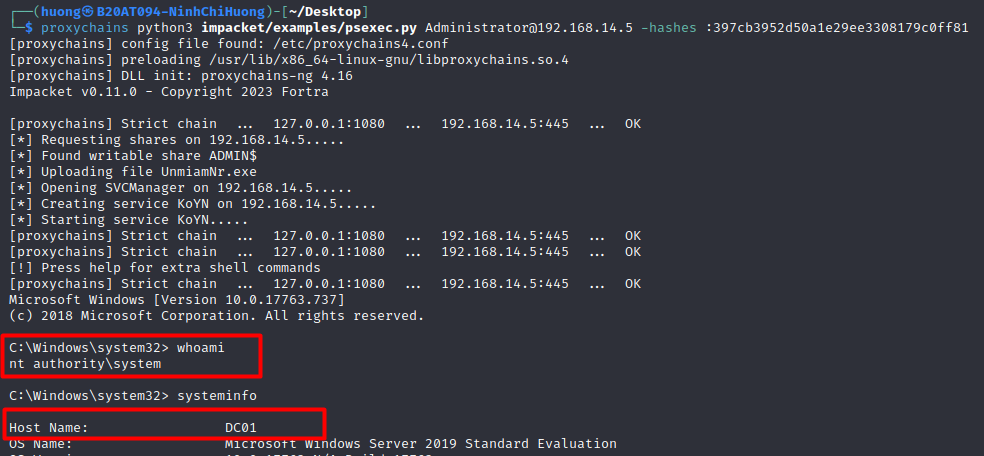
* Yêu cầu cấp vé mới và thực hiện pash-the-ticket để import vé của DC01$ vào phiên powershell hiện tại



* Từ phiên powershell có ticket của DC01$ , sử dụng mimikatz để thực hiện DCSync , lấy về hash của Domain Admin

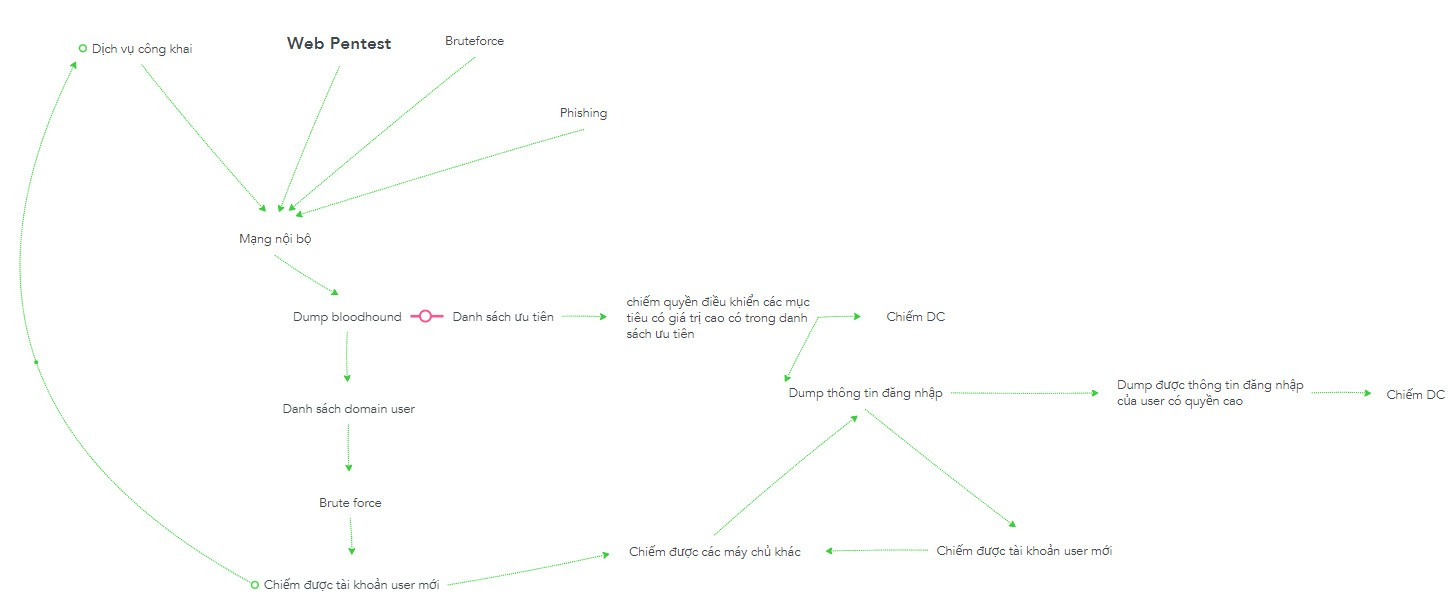


* Sử dụng công cụ impacket và hash của Admin vừa lấy được , tiến hành chiếm DC01:



=> *kết quả, chiếm DC thành công*

1. **Quy trình kiểm thử Active Directory chung**.



1. **Kết luận và biện pháp**.

* Bảo vệ các trang web, dịch vụ công khai thuộc máy chủ nằm trong dịch vụ Active Directory
* Thường xuyên cập nhật các lỗ hổng bảo mật mới từ các máy chủ dịch vụ
* Hạn chế việc sử dụng ủy quyền không cần thiết
* Sử dụng chính sách mật khẩu mạnh đối với người dùng trong domain
* Sử dụng các biện pháp để ngăn chặn phishing
* Giám sát và đưa ra cảnh báo sớm đối với các cuộc tấn công vét cạn.

**Tài liệu tham khảo**

<https://bkhost.vn/blog/giao-thuc-kerberos/>

<https://cloudviet.com.vn/active-directory-la-gi-tong-quan-ve-active-directory/>

<https://sec.vnpt.vn/2023/02/kerberos-unconstrained-delegation-attack/>

<https://www.thehackersprint.com/kerberos-delegation-and-abuse-cases/unconstrained-delegation/printer-bug>

<https://github.com/tennc/webshell/blob/master/fuzzdb-webshell/asp/cmd.aspx>

<https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound.html>