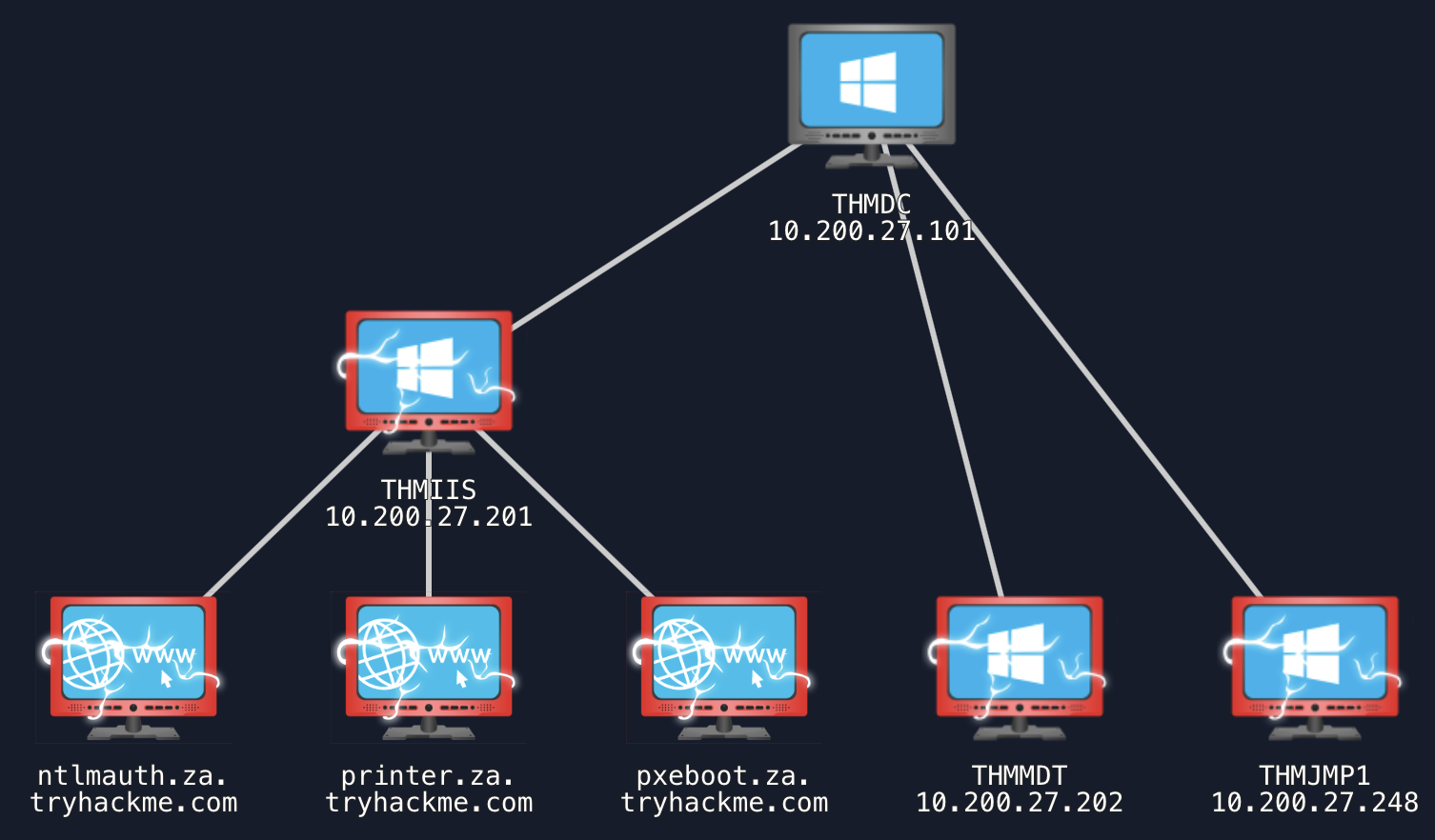
**Breaching Active Directory**



**Giới thiệu về AD Breaches**

Active Directory được dùng bởi 90% của 1000 công ty đa quốc gia. Nếu tổ chức đang dùng Microsoft Windows, bạn gần như chắc chắn sẽ tìm thấy AD. Microsoft AD là 1 ứng dụng nổi trội quản lý mạng của Windows domain. Vì AD được dùng để quản lý truy cập và thực thể, nó nắm giữ chìa khóa dẫn đến vương quốc, khiến nơi đây rất có thể trở thành mục tiêu ưa thích của kẻ tấn công.

**Breaching Active Directory**

Trước khi chúng ta có thể khai thác lỗi cấu hình AD để leo thang đặc quyền, lateral movement và thực thi, bạn cần truy cập đầu tiên. Bạn cần thông tin đăng nhập AD hợp lệ. Do số lượng dịch vụ và tính năng của AD, phạm vi tấn công để lấy được thông tin đăng nhập thường rất lớn. Trong phòng này, chúng ta sẽ thảo luận một số cách nhưng đây không phải là một danh sách đầy đủ.

Khi tìm kiếm thông tin đăng nhập, chúng ta không tập trung vào các đặc quyền của một tài khoản, một tài khoản có đặc quyền thấp là đủ. Chúng ta đang tìm kiếm cách để xác thực AD, cho phép chúng ta liệt kê nhiều hơn trên AD.

**Mục tiêu học:**

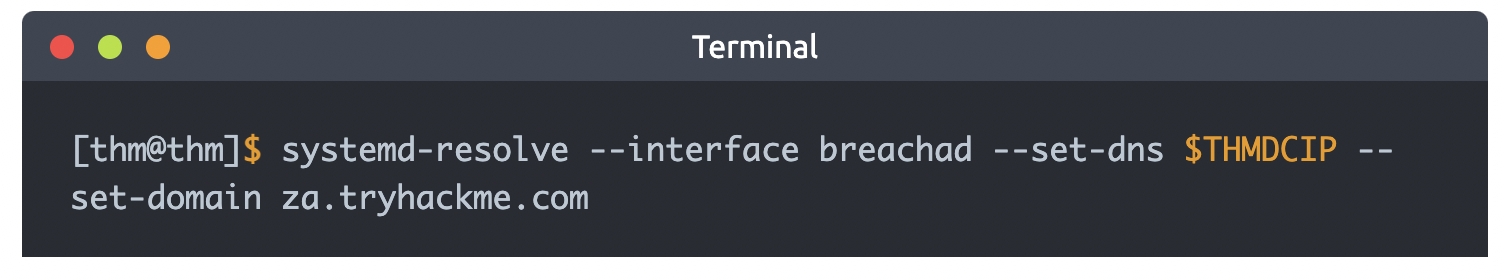
Trong mạng này, chúng ta sẽ đi qua một số phương pháp có thể breach AD:

* NTLM Authenticated Services
* LDAP Bind Credentials
* Authentication Relays
* Microsoft Deployment Toolkit
* Configuration Files

**Cách kết nối mạng:**

**AttackBox**

Nếu bạn dùng AttackBox, bạn sẽ được kết nối đến mạng tự động. Bạn có thể xác mình điều này bằng cách chạy lệnh ping đối với IP của máy chủ THMDC.za.tryhackme.com. Chúng ta vẫn cần cấu hình DNS. Windows Networks dùng DNS để phân giải tên máy chủ thành ip. Bạn phải cấu hình DNS trên máy chủ bạn đang chạy kết nối vpn. Để cấu hình DNS, chạy lệnh sau:



Nhớ thay $THMDCIP bằng ip của THMDC trong sơ đồ mạng. Bạn có thể kiểm tra DNS đang chạy bằng lệnh:

nslookup thmdc.za.tryhackme.com

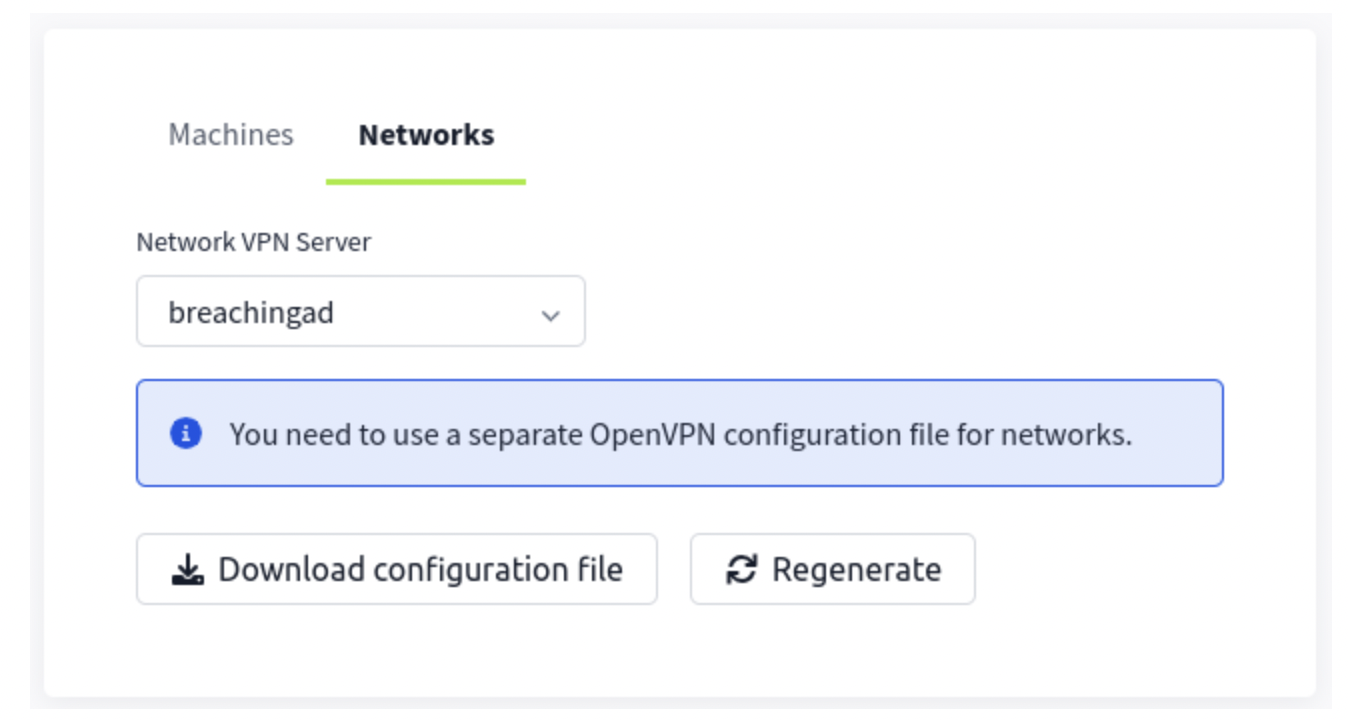
Nó sẽ phân giải ip của DC.

**Lưu ý:** DNS có thể reset trên AttackBox mỗi 3 giờ. Nếu điều này xảy ra, bạn sẽ phải chạy lại dịch vụ systemd-resolved. Nếu AttackBox bị chấm dửt và bạn tiếp tục sử dụng phòng ở giai đoạn sau, bạn sẽ phải làm lại các bước DNS.

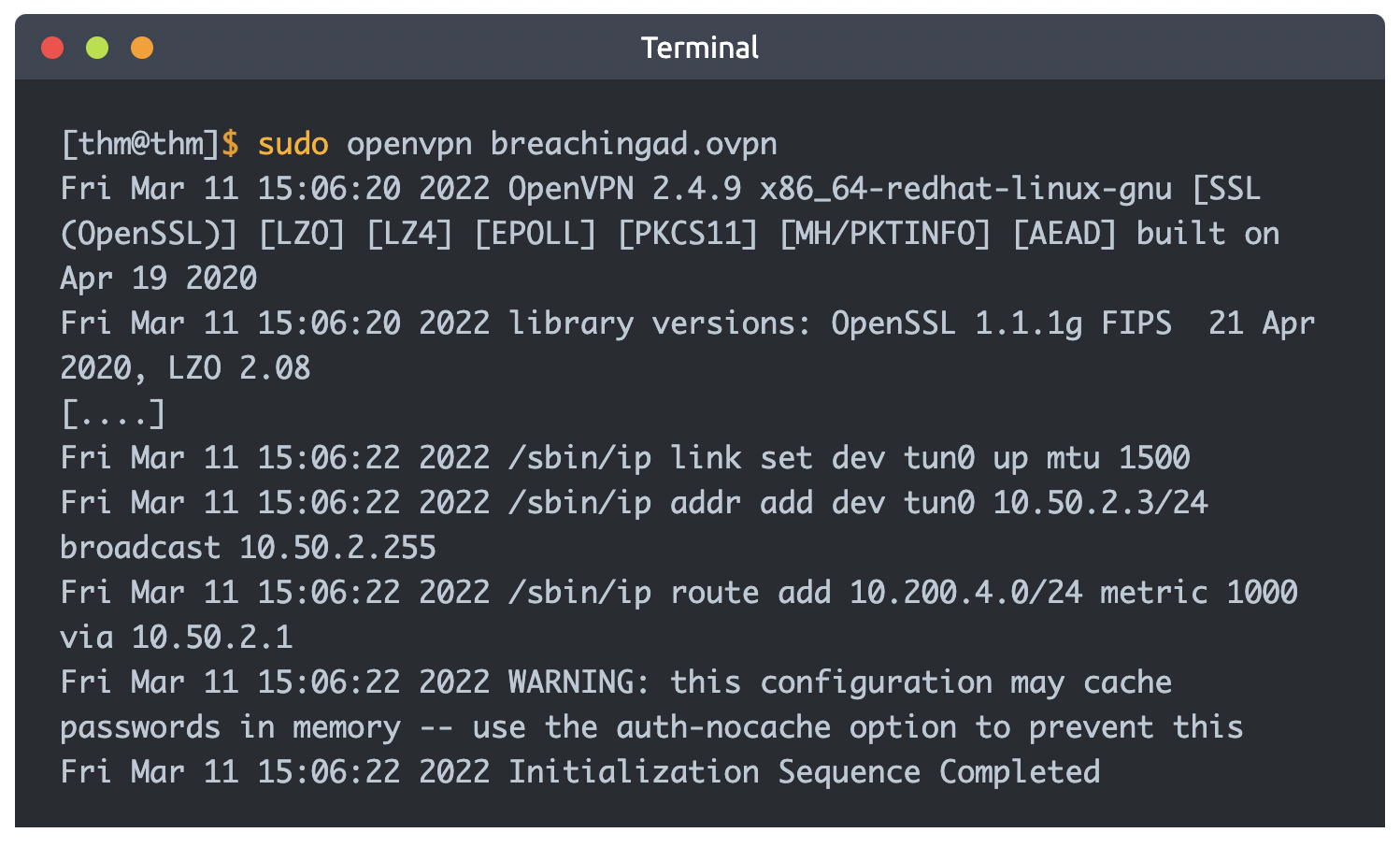
Bạn nên chú ý VPN IP của mình. Dùng lệnh ifconfig hoăc ip a, để ý IP của breached network adapter. Đó là ip của bạn và giao diện mà bạn sử dụng khi thực hiện tấn công trong bài học này.

**Other Hosts**

Nếu bạn dùng máy ảo của mình, 1 tệp cấu hình OpenVPN sẽ được tạo khi bạn tham gia phòng. Đến trang access. Chọn ‘BreachingAD’ từ các máy chủ VPN và tải tệp cấu hình.



Dùng OpenVPN client để kết nối.



**Lưu ý:** Bạn vẫn cấu hình DNS tương tự như những gì được trình bày ở trên.

Điều quan trọng cần lưu ý là mặc dù không được sử dụng nhưng DC vẫn ghi nhật ký các yêu cầu DNS. Nếu bạn dùng máy ảo của mình, các logs có thể chứa hostname của thiết bị. Ví dụ, nếu bạn chạy VPN trên máy ảo kali với hostname là kali, điều này sẽ được ghi lại.

Nếu bạn đang dùng máy ảo kali, Network Manager có thể quản lý DNS. Bạn có thể dùng GUI để cấu hình DNS:

* Network Manager -> Advanced Network Configuration -> Your Connection -> IPv4 Settings
* Đặt địa chỉ IP DNS của bạn ở đây thành IP của THMDC trong sơ đồ mạng ở trên.
* Thêm 1 DNS khác như 1.1.1.1 để đảm bảo bạn vẫn có quyền truy cập Internet.
* Chạy sudo systemctl restart NetworkManager và kiểm tra DNS tương tự như các bước ở trên

**Debugging DNS**

DNS là 1 phần kiểm thử Active Directory dù bạn có muốn hay là không. Đó là vì một trong hai giao thức chính để xác thực AD là Kerberos, dựa vào DNS để tạo tickets. Các tickets không thể liên kết với IPs nên DNS là bắt buộc. Nếu bạn muốn kiểm thử mạng AD, bạn sẽ phải trang bị cho mình những kĩ năng cần thiết để giải quyết các vấn đề liên quan đến DNS. Do đó, bạn thường có hai lựa chọn:

* Bạn có thể hardcode các điểm vào DNS trong tệp /etc/hosts. Mặc dù điều này có thể hoạt động tốt nhưng sẽ không khả thi khi bạn thử nghiệm các mạng có hơn 10000 máy chủ.
* Bạn có thể dành thời gian để debug các vấn đề của DNS để làm cho nó hoạt động. Mặc dù điều này có thể khó khăn hơn nhưng về lâu dài nó sẽ mang lại cho bạn kết quả tốt hơn.

Khi một trong những bài trong phòng này không hoạt động với bạn, điều đầu tiên bạn nên nghĩ là: DNS của mình có đang hoạt động? Từ kinh nghiệm, tôi, người tạo ra mạng này, có thể nói với bạn rằng tôi đã lãng phí vô số giờ đánh giá để tự hỏi tại sao công cụ của tôi không hoạt động, chỉ để nhận ra rằng DNS của tôi đã thay đổi.

Khi bạn nghĩ cấu hình DNS không hoạt động như mình mong đợi, hãy làm theo các bước sau để debug:

1. Làm theo các bước ở trên. Đảm bảo thực hiện theo các bước dành cho loại máy cụ thể của bạn. Nếu bạn dùng 1 hệ điều hành hoàn toàn khác, bạn sẽ phải tìm kiếm các cấu hình tương tự
2. Chạy ping DC IP> Điều này sẽ xác minh rằng mạng đang hoạt động. Nếu bạn không nhận được phản hồi từ ping, điều đó có nghĩa là mạng hiện không hoạt động. Nếu mạng của bạn nói nó đang chạy sau khi bạn làm mới phòng và bạn vẫn không nhận được phản hồi từ ping, liên hệ THM support nhưng chỉ cần đợi hết giờ mạng trước khi khởi động lại mạng sẽ khắc phục được sự cố.
3. Chạy nslookup tryhackme.com DC IP> Điều này sẽ xác minh rằng máy chủ DNS trong mạng đang hoạt động. Nếu ping hoạt động nhưng cái này không được, đã đến lúc liên hệ với bộ phận hỗ trợ vì đã xảy ra sự cố. Bạn cũng nên nhấn nút đặt lại mạng.
4. Cuối cùng, chạy nsloopup tryhackme.com Nếu bạn nhận 1 phản hồi khác với phản hồi trong bước 3, điều đó có nghĩa là đã xảy ra lỗi với cấu hình DNS. Quay lại các bước cấu hình ở đầu bài và làm theo chúng 1 lần nữa. Một vấn đề phổ biến thường nhìn thấy trong kali là mục DNS được đặt ở vị trí thứ hai trong tệp /etc/resolv.conf. Bằng cách đặt nó ở mục đầu tiên, nó sẽ giải quyết được vấn đề.

Các mạng AD được xếp hạng trung bình, có nghĩa là nếu bạn mới tham gia THM, đây có lẽ không phải là nơi bạn nên bắt đầu học. AD rất lớn và bạn sẽ cần áp dụng lối tư duy tìm hiểu một thứ gì đó nếu bạn muốn kiểm thử thành công. Tuy nhiên, nếu tất cả bước trên bị thất bại, vui lòng mô tả càng chi tiết càn tốt về những gì bạn đang cố gắng thực hiện khi liên hệ với bộ phận hỗ trợ để họ có thể giúp bạn hiệu quả nhất có thể.

**NTLM Authenticated Services**

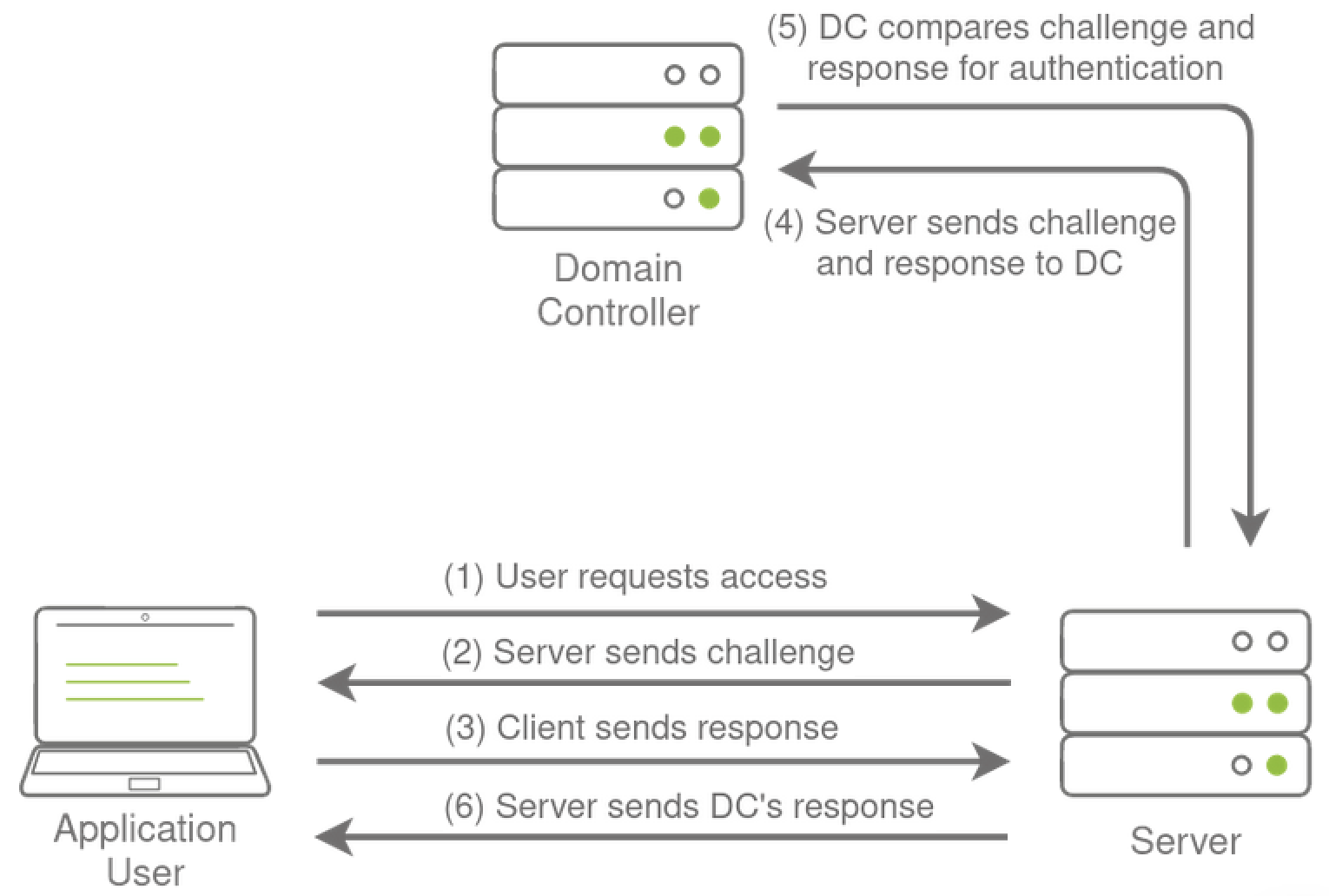
**NTLM and NetNTLM**

New Technology LAN Manager (NTLM) là bộ các giao thức bảo mật xác thực danh tính người dùng trong AD.

NTLM xác thực bằng cơ chế challenge-response gọi là NetNTLM. Cơ chế xác thực này được dùng rất nhiều bởi các dịch vụ trên mạng. Các dịch vụ xác thực bằng NetNTLM có thể được kết nối bằng Internet: máy chủ mail, dịch vụ kết nối từ xa (RDP), ứng dụng web,..

NetNTLM thường được nhắc đến là Windows Authentication hoặc chỉ là xác thực NTLM, cho phép ứng dụng đóng vai trò trung gian giữa máy khách và AD. Thông tin xác thực sẽ được chuyển đến Domain Controller dưới dạng challenge, nếu thành công, người dùng có thể truy cập ứng dụng.

Điều này có nghĩa là ứng dụng đang xác thực thay cho người dùng và không xác thực trực tiếp với ứng dụng. Điều này ngăn chặn ứng dụng lưu trữ thông tin đăng nhập AD vốn chỉ nên lưu trữ trong DC.



**Brute-force Login Attacks**

Các dịch vụ mà bạn có thể kết nối bằng Internet: máy chủ mail, RDP, VPN, ứng dụng web,… là 1 nơi rất tốt để bạn kiểm tra thông tin đăng nhập.

Vì môi trường AD được cấu hình khóa tài khoản, chúng ta không thể tấn công dồn dập được. Thay vào đó, chúng ta cần thực hiện tấn công rải mật khẩu. Thay vì thử nhiều mật khẩu khác nhau, có thể thực thi tính năng khóa tài khoản, chúng ta chọn và dùng một mật khẩu và cố gắng xác thực bằng nhiều username. Các tấn công này có thể bị phát hiện vì số lần đăng nhập thất bại chúng ta tạo ra.

Bạn được cung cấp 1 danh sách username khám phá trong quá trình red team OSINT. OSINT cũng chỉ ra mật khẩu đăng nhập ban đầu của tổ chức là “Changeme123”. Mặc dù người dùng luôn thay đổi mật khẩu ban đầu, nhưng chúng ta biết có người vẫn quên. Chúng ta sẽ sử dụng 1 tập lệnh được phát triển tùy chỉnh để tiến hành dò tìm mật khẩu đối với ứng dụng web: http://ntlmauth.za.tryhackme.com

Chuyển hướng đến URL, chúng ta thấy nó nhắc chúng ta về thông tin đăng nhập Windows:



Chúng ta có thể dùng công cụ như Hydra để tấn công rải mật khẩu. Tuy nhiên, tốt hơn hết bạn nên tự viết 1 tập lệnh cho những kiểu tấn công này, cho phép bạn kiểm soát toàn bộ quá trình.



Hàm password\_spray nhận mật khẩu và url chúng ta nhắm đến làm đầu vào và cố gắng xác thực URL với mỗi tên người dùng trong tệp văn bản. Bằng cách theo dõi sự khác nhau trong trạng thái code của HTTP, chúng ta có thể xác định thông tin đăng nhập hợp lệ hay là không.

**Password Spraying**

Chúng ta có thể chạy script bằng lệnh sau:

python ntlm\_passwordspray.py -u <userfile> -f <fqdn> -p <password> -a <attackurl>

<fqdn>: tên miền đầy đủ liên kết với tổ chức mà chúng ta đang tấn công - “za.tryhackme.com”



**LDAP Bind Credentials**

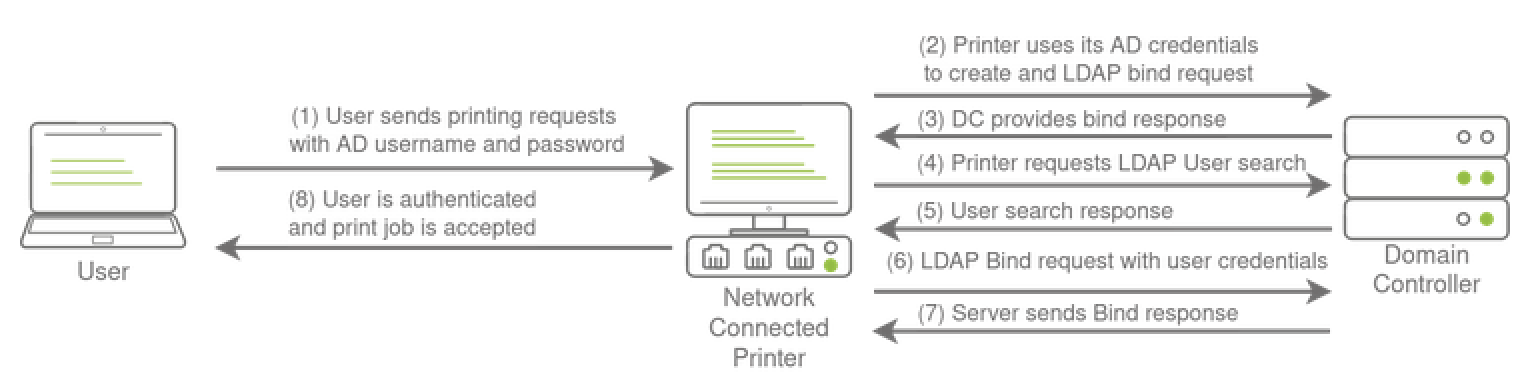
**LDAP**

Một phương pháp xác thực AD khác mà ứng dụng có thể dùng là Lightweight Directory Access Protocol (LDAP). Xác thực LDAP rất giống với xác thực NTLM. Tuy nhiên, với xác thực LDAP, ứng dụng trực tiếp xác minh thông tin đăng nhập của người dùng. Ứng dụng có thông tin đăng nhập AD mà trước tiên nó có thể sử dụng để truy vấn LDAP, sau đó xác minh thông tin đăng nhập của người dùng.

Xác thực LDAP là 1 cơ chế phổ biến với ứng dụng ở bên thứ ba (không phải là Microsoft) tích hợp với AD. Chúng bao gồm các ứng dụng và hệ thống như:

* Gitlab
* Jenkins
* Custom-developed web applications
* Printers
* VPNs

Nếu bất cứ ứng dụng hay dịch vụ nào có thể kết nối bằng Internet, có thể sử dụng kiểu tấn công giống như NTLM nhằm vào các hệ thống được xác thực. Vì ứng dụng xác thực bằng LDAP yêu cầu thông tin đăng nhập của AD, nó mở thêm phạm vi tấn công. Về bản chất, chúng ta có thể khôi phục thông tin đăng nhập AD được dịch vụ sử dụng để có quyền truy cập xác thực vào AD. Quá trình xác thực thông qua LDAP được thực hiện như sau:



Nếu bạn có thể truy cập ban đầu vào đúng máy chủ như Gitlab, nó có thể đơn giản như việc đọc các tệp cấu hình để khôi phục các thông tin đăng nhập AD này. Thông tin đăng nhập thường được lưu dưới dạng văn bản thô trong các tệp cấu hình vì mô hình bảo mật dựa vào việc giữ an toàn cho vị trí và tệp cấu hình hơn là nội dung của nó.

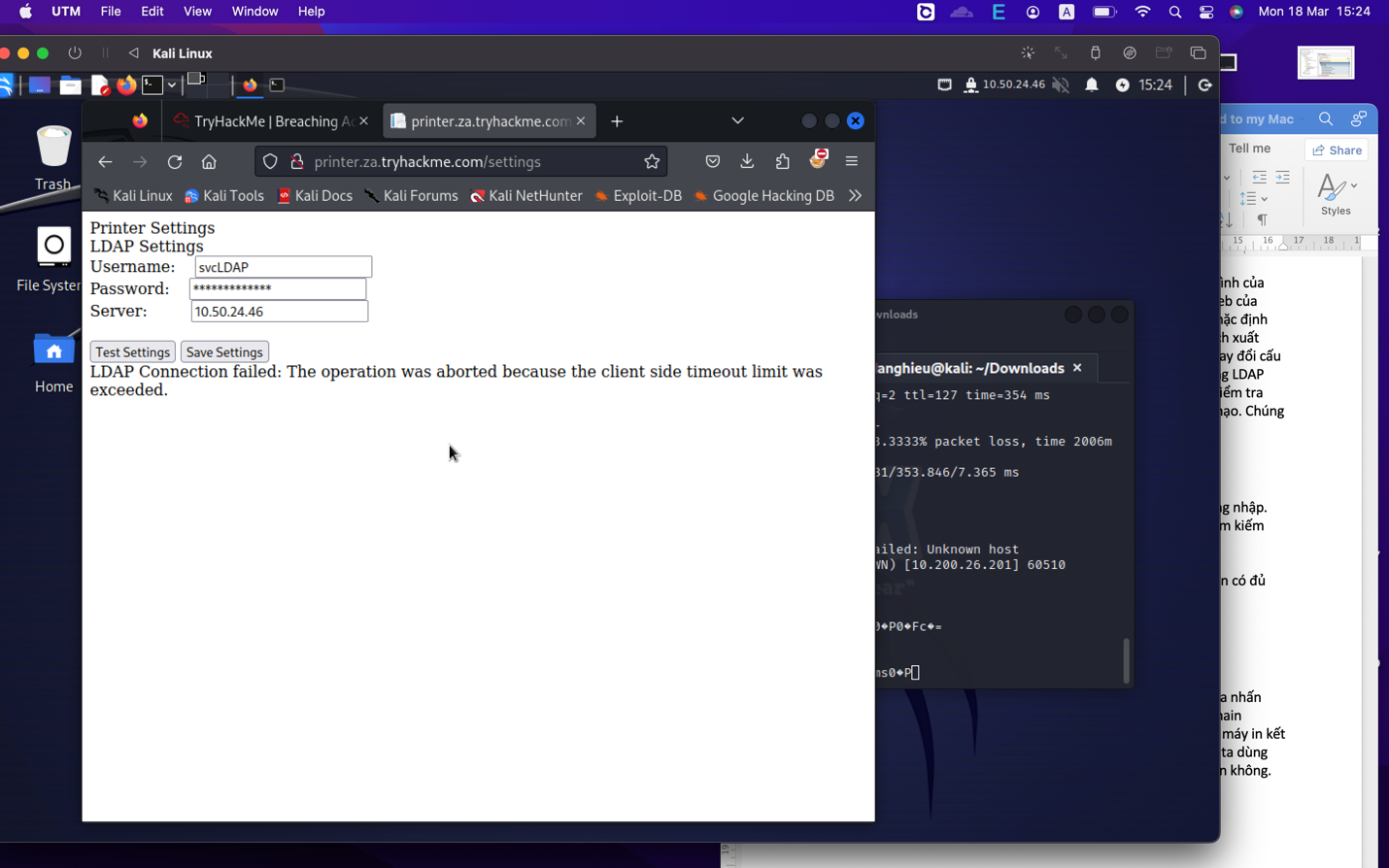
**LDAP Pass-back Attacks**

Tuy nhiên, một tấn công rất thú vị có thể thực hiện đối với xác thực LDAP gọi là LDAP Pass-back. Đây là một kiểu tấn công phổ biến chống lại các thiết bị mạng, như máy in, khi bạn truy cập ban đầu vào mạng nội bộ, chẳng hạn như cắm một thiết bị giả mạo trong phòng họp.

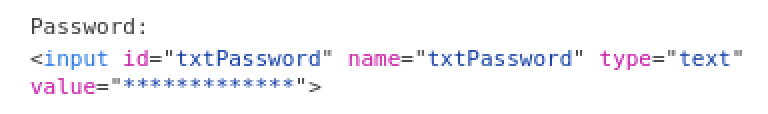
LDAP Pass-back có thể được thực hiện khi chúng ta truy cập được cấu hình của thiết bị có tham số LDAP được chỉ định. Ví dụ, đây có thể là giao diện web của máy in trong mạng, thông tin đăng nhập cho các giao diện được giữ ở mặc định như admin:admin hoặc admin:password. Ở đây, chúng ta không thể trích xuất thông tin đăng nhập LDAP vì mật khẩu bị ẩn. Thường chúng ta có thể thay đổi cấu hình LDAP như ip hoặc hostname của máy chủ LDAP. Trong một tấn công LDAP Pass-back, chúng ta có thể điều chỉnh ip thành ip của chúng ta, sau đó kiểm tra cấu hình LDAP, sẽ buộc thiết bị cố gắng xác thực LDAP đến thiết bị giả mạo. Chúng ta có thể chặn nỗ lực xác thực để khôi phục thông tin đăng nhập LDAP.

**Thực hiện tấn công LDAP Pass-back**

Có 1 máy in trong mạng trang web quản trị không yêu cầu thông tin đăng nhập. Chuyển hướng đến http://printer.za.tryhackme.com/settings.aspx để tìm kiếm trang cài đặt của máy in:

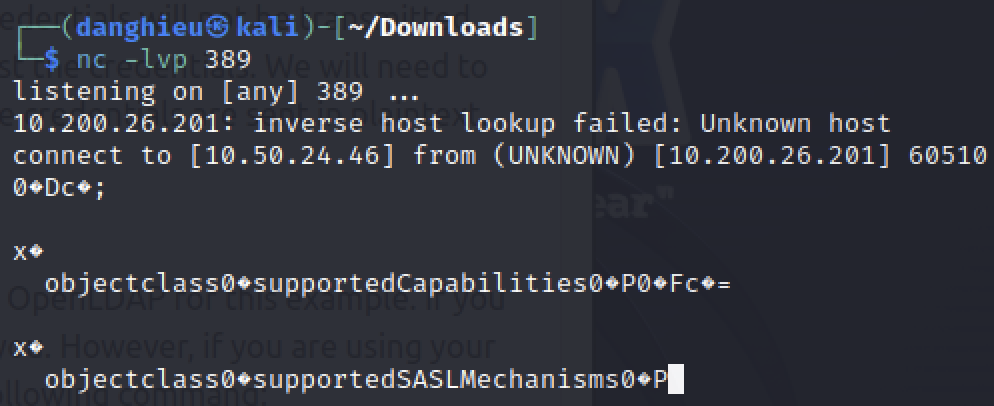


Điều tra trình duyệt, chúng ta có thể xác minh rằng trang web của máy in có đủ bảo mật để không gửi lại mật khẩu cho trình duyệt.



Vì vậy chúng ta có username không có password. Tuy nhiên, khi chúng ta nhấn test settings, chúng ta có thể thấy 1 yêu cầu xác thực được gửi đến domain controller để kiểm tra thông tin đăng nhập ldap. Hãy cố khai thác nó để máy in kết nối với chúng ta, sẽ tiết lộ thông tin đăng nhập. Để làm điều này, chúng ta dùng Netcat listener để kiểm tra xem chúng ta có nhận được kết nối từ máy in không. Vì cổng mặc định của ldap là 389, chúng ta dùng lệnh sau:

nc -lvp 389



Phản hồi supportedCapabilities thông báo cho chúng ta biết có vấn đề. Trước khi máy in gửi thông tin xác thực, nó sẽ cố gắng đàm phán chi tiết về phương thức xác thực LDAP. Nó sẽ sử dụng quá trình đàm phán này để chọn phương thức xác thực an toàn nhất mà cả máy in và máy chủ LDAP đều hỗ trợ. Nếu phương thức xác thực quá an toàn, thông tin đăng nhập sẽ không được truyền đi ở dạng văn bản thô. Với một số phương thức xác thực, thông tin đăng nhập sẽ không được truyền qua mạng! Vì vậy chúng ta không thể dùng Netcat để thu thập thông tin đăng nhập. Chúng ta cần tạo 1 máy chủ LDAP giả và cấu hình nó để đảm bảo thông tin đăng nhập được gửi đi ở dạng văn bản thô.

**Tạo 1 máy chủ LDAP giả**

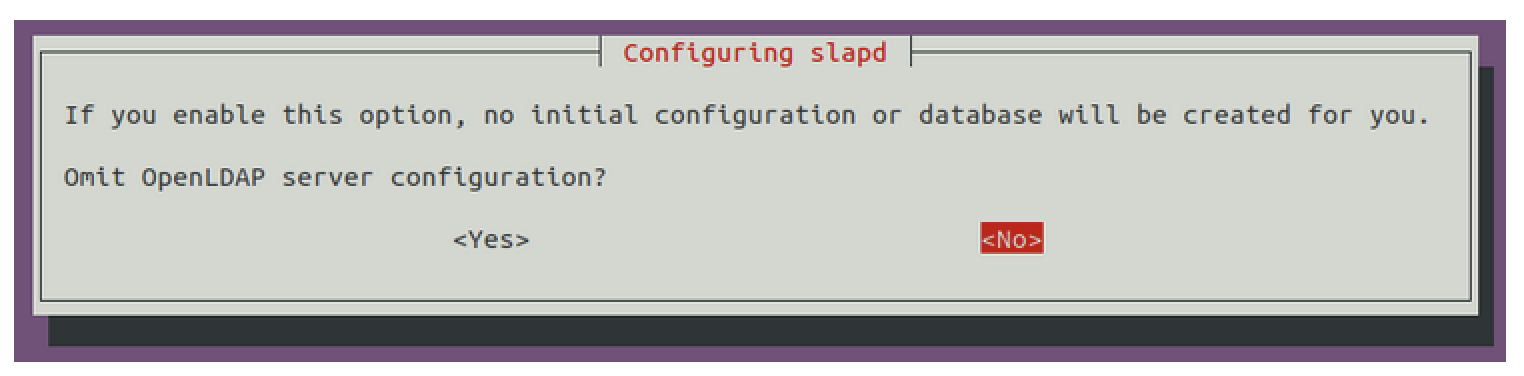
Có một số cách để lưu trữ máy chủ LDAP giả, nhưng chúng ta sẽ dùng OpenLDAP làm ví dụ. Nếu bạn dùng Attackbox, OpenLDAP đã được cài đặt cho bạn. Nếu bạn dùng máy ảo của riêng mình, bạn sẽ cần cài đặt OpenLDAP bằng lệnh sau:

sudo apt-get update && sudo apt-get -y install slapd ldap-utils && sudo systemctl enable slapd

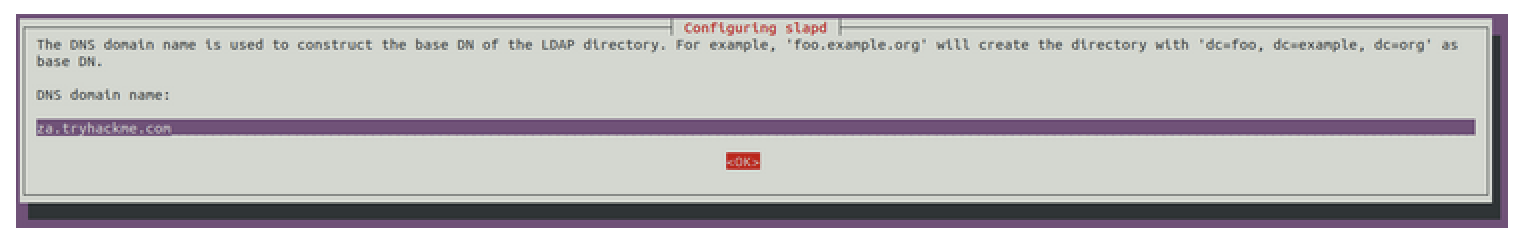
Bạn phải cấu hình máy chủ LDAP trên AttackBox luôn. Chúng ta sẽ bắt đầu cấu hình lại máy chủ LDAP bằng lệnh sau:

sudo dpkg-reconfigure -p low slapd

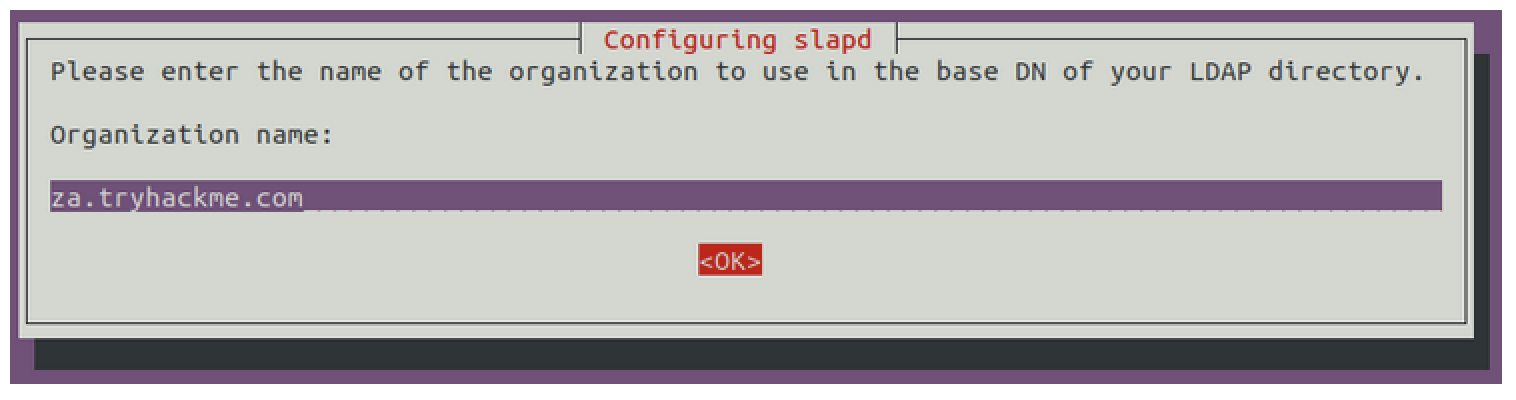
Đảm bảo chọn <No> khi được yêu cầu nếu bạn muốn bỏ qua cấu hình máy chủ:



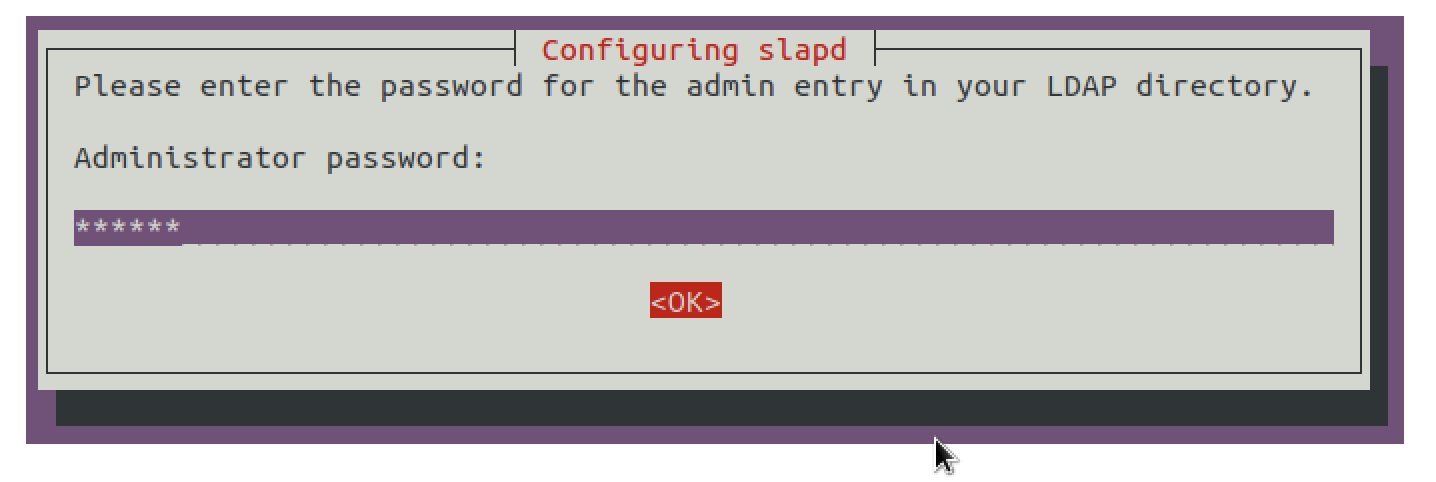
Đối với tên miền DNS, bạn muốn cung cấp tên miền mình muốn nhắm đến là za.tryhackme.com:



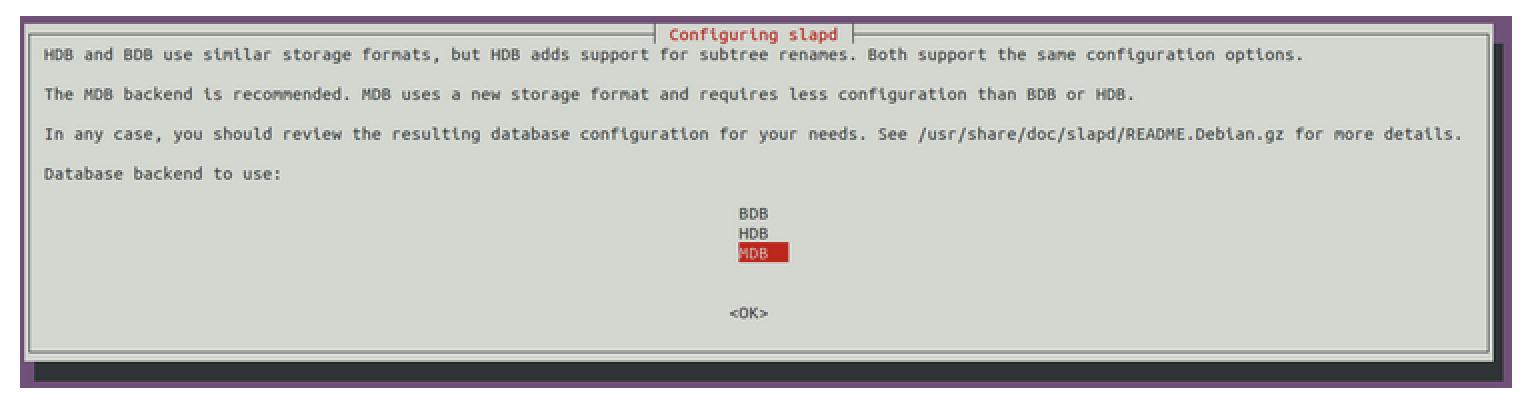
Dùng tên tương tự với Organisation name:



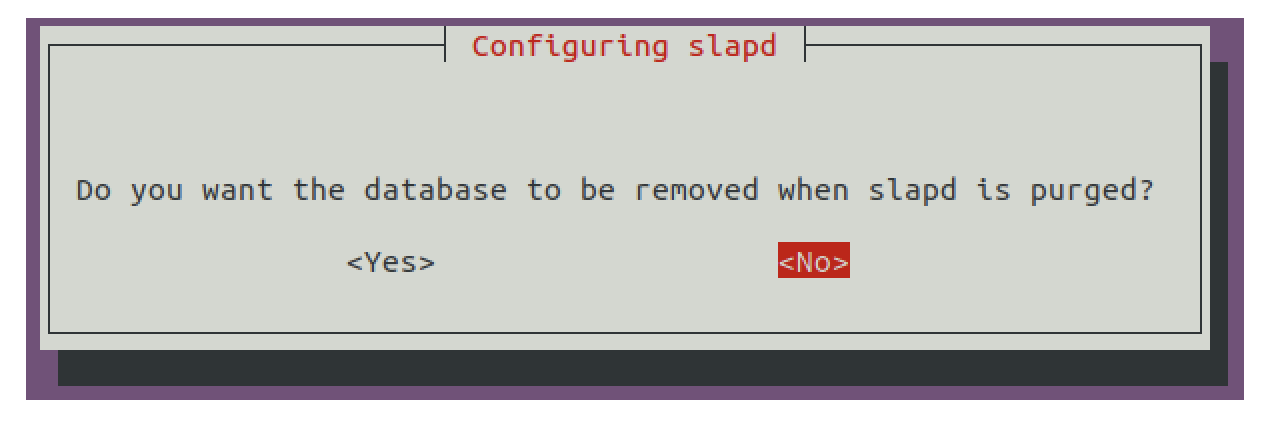
Cung cấp mật khẩu của quản trị viên:



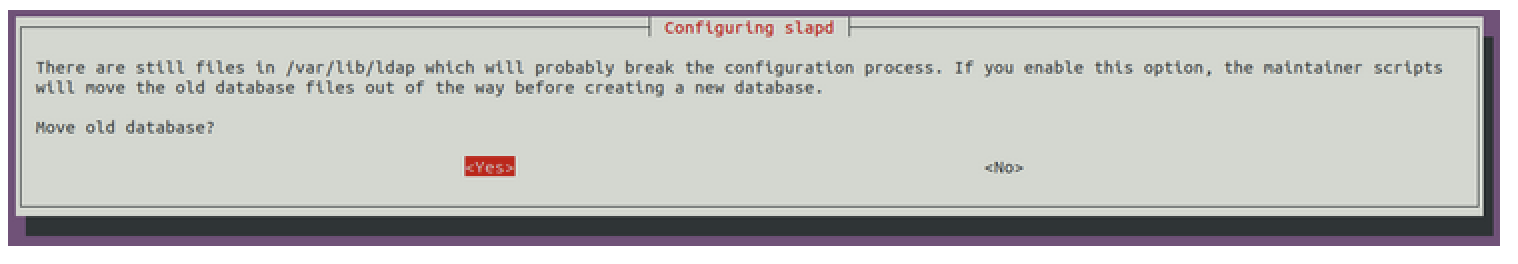
Chọn MDB là cơ sở dữ liệu LDAP để dùng:



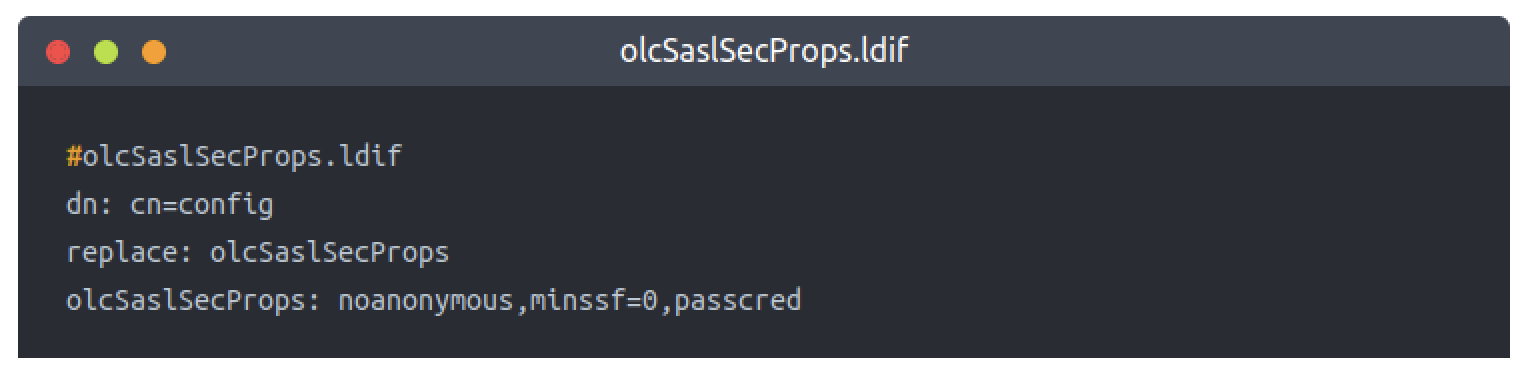
Với hai lựa chọn cuối, đảm bảo cơ sở dữ liệu không bị xóa khi slapd bị xóa:



Di chuyển tập tin csdl cũ trước khi tập tin mới được tạo:



Trước khi dùng máy chủ LDAP giả, chúng ta cần làm cho nó dễ bị tấn công bằng cách giảm các cơ chế xác thực được hỗ trợ. Chúng ta muốn đảm bảo máy chủ LDAP chỉ hỗ trợ phương thức xác thực PLAIN và LOGIN. Để làm điều đó, chúng ta cần tạo 1 tệp mới ldif với nội dung sau:



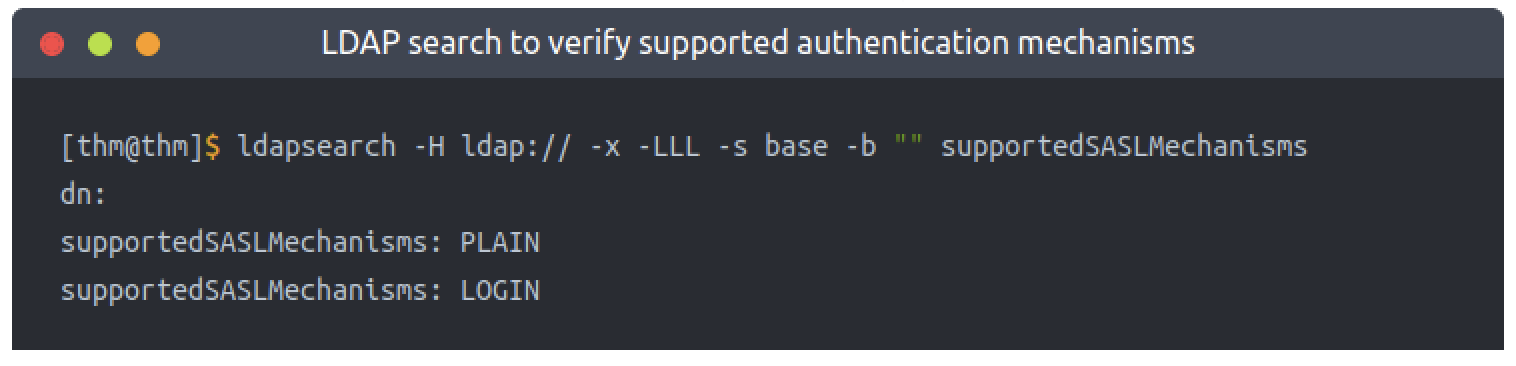
Tập tin có các thuộc tính sau:

* olcSaslSecProps: chỉ định các thuộc tính bảo mật SASL
* noanonymous: vô hiệu hóa truy cập anonymous
* minssf: chỉ định mức độ bảo mật là 0, nghĩa là không có biện pháp bảo vệ.

Bây giờ chúng ta có thể dùng tệp ldif để vá máy chủ LDAP bằng lệnh sau:

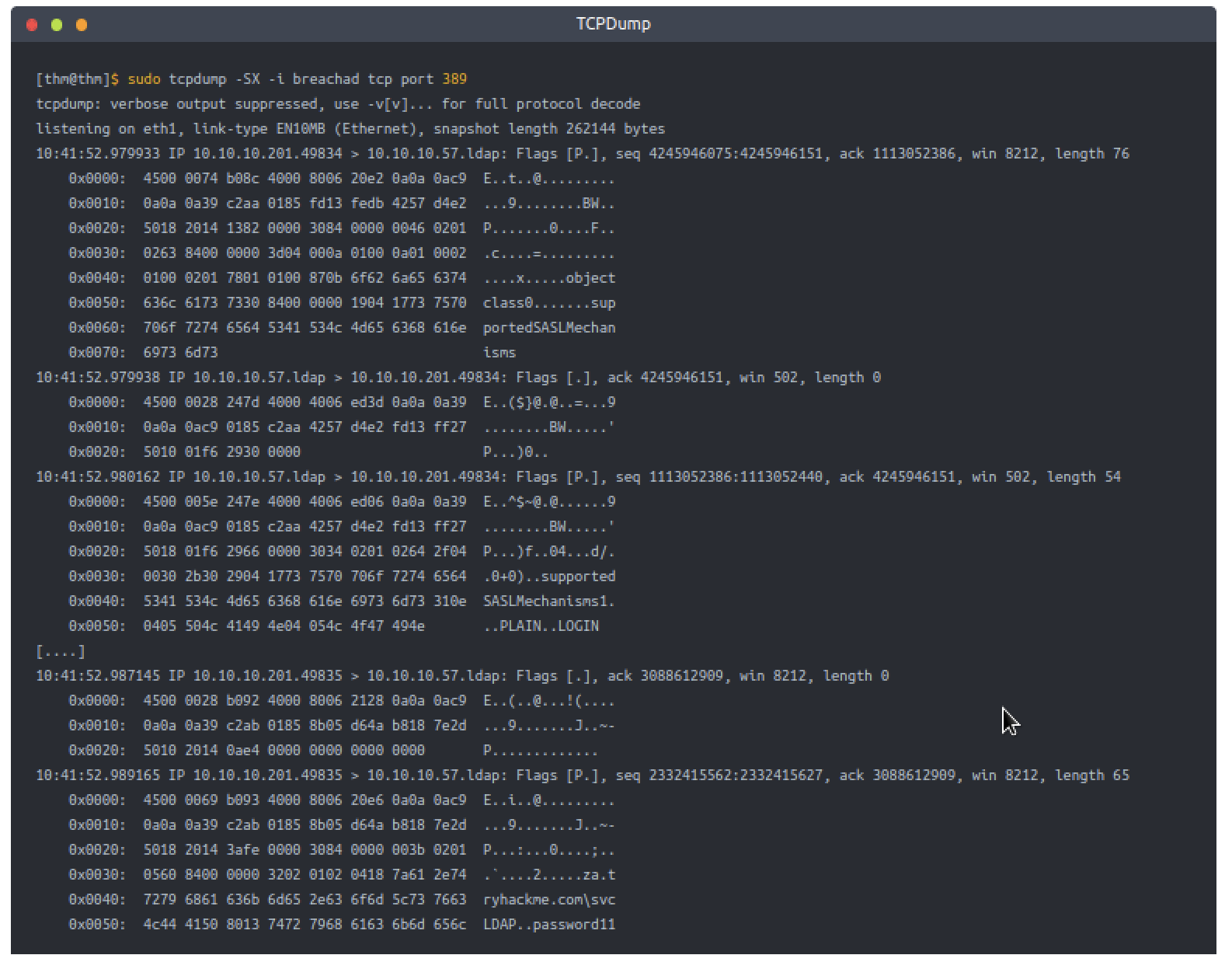
sudo ldapmodify -Y EXTERNAL -H ldapi:// -f ./olcSaslSecProps.ldif && sudo service slapd restart

Chúng ta có thể kiểm tra cấu hình của máy chủ LDAP bằng lệnh sau (Nếu bạn dùng Kali, bạn có thể không nhận được đầu ra, tuy nhiên cấu hình vẫn hoạt động và bạn có thể làm bước tiếp theo) :



**Thu thập thông tin đăng nhập LDAP:**

Máy chủ LDAP của bạn đã cấu hình xong. Khi bạn chọn Test Settings, xác thực sẽ xảy ra ở dạng văn bản thô. Nếu bạn cấu hình máy chủ LDAP đúng cách, bạn sẽ nhận được lỗi sau: “This distinguished name contains invalid syntax”. Nếu bạn nhận được lỗi đó, bạn có thể dùng tcpdump để lấy thông tin đăng nhập bằng lệnh sau:



Lưu ý password11 chỉ là một ví dụ. Mật khẩu trên dịch vụ của bạn sẽ khác nhau. Bạn có thể nhấn Test Settings nhiều lần trước khi tcpdump trả về dữ liệu vì chúng ta đang thực hiện tấn công qua VPN.

Bây giờ chúng ta đã có thông tin đăng nhập AD hợp lệ.

**Authentication Relays**

Tiếp tục với các cuộc tấn công có thể được dàn dựng từ thiết bị giả mạo, bây giờ chúng ta sẽ xem xét các cuộc tấn công chống lại các giao thức xác thực mạng rộng hơn. Trong mạng Windows, có một lượng lớn các dịch vụ trao đổi với nhau, cho phép người dùng sử dụng các dịch vụ do mạng cung cấp.

Các dịch vụ phải dùng phương thức xác thực được dựng sẵn để xác minh danh tính của kết nối đang đến. Trong Task 2, chúng ta đã khám phá giao thức NTLM được dùng trong ứng dụng web. Trong bài này, chúng ta sẽ đi sâu hơn cách giao thức hoạt động theo góc nhìn của mạng. Tuy nhiên, chúng ta sẽ tập trung giao thức xác thực NetNTLM được dùng bởi SMB.

**Server Message Block**

Giao thức SMB cho phép máy khách (giống như workstations) giao tiếp với máy chủ (giống như file share). Trong mạng dùng Microsoft AD, SMB quản lý mọi thứ từ chia sẻ tệp liên mạng đến quản trị từ xa. Ngay cả cảnh báo “hết giấy” mà máy tính bạn nhận được khi bạn cố in tài liệu cũng là công việc của giao thức SMB.

Tuy nhiên, tính bảo mật của giao thức SMB các phiên bản trước được coi là chưa tốt. Một số lỗ hổng và khai thác có thể được lợi dụng để khôi phục thông tin đăng nhập hoặc thực thi lệnh từ xa trên thiết bị. Mặc dù một số lỗ hổng đã được xử lí trong các phiên bản mới của giao thức, thông thường các tổ chức không bắt buộc sử dụng các phiên bản mới hơn vì hệ thống cũ không hỗ trợ chúng. Chúng ta sẽ xem xét hai khai thác NetNTLM khác nhau của giao thức SMB:

* Vì NTLM challenges có thể bị chặn, chúng ta có thể dùng kĩ thuật bẻ khóa để khôi phục mật khẩu liên quan đến thử thách NTLM. Tuy nhiên, quá trình bẻ khóa này chậm hơn đáng kể so với việc bẻ khóa NTLM trực tiếp.
* Chúng ta có thể dùng thiết bị giả mạo để dàn dựng tấn công MITM, chuyển xác thực SMB giữa máy khách và máy chủ, điều này sẽ cung cấp cho chúng ta phiên xác thực đang hoạt động và quyền truy cập vào máy chủ mục tiêu.

**LLMNR, NBT-NS, và WPAD**

Trong bài này, chúng ta sẽ tìm hiểu một chút về xác thực xảy ra trong quá trình dùng SMB. Chúng ta sẽ dùng Responder để cố gắng chặn challenge NetNTLM để bẻ khóa nó. Thường có nhiều thử thách kiểu này xuất hiện trên mạng. Một số giải pháp bảo mật thậm chí còn thực hiện quét toàn bộ dải IP để khôi phục thông tin từ máy chủ. Đôi khi do bản ghi DNS cũ, những challenge xác thực có thể tấn công vào thiết bị giả mạo của bạn thay vì máy chủ dự định.

Responder cho phép chúng ta tấn công MITM bằng cách đầu độc các phản hồi trong quá trình xác thực NetNTLM, lừa máy khách nói chuyện với bạn thay vì máy chủ thực sự họ muốn kết nối. Trong mạng LAN thực tế, Responder sẽ đầu độc Link-Local Multicast Name Resolution (LLMNR), NetBIOS Name Service (NBT-NS) và các yêu cầu Web Proxy Auto-Discovery (WPAD) được phát hiện. Trong mạng lớn Windows, các giao thức cho phép các máy chủ phân giải DNS của chúng cho tất cả máy chủ trong mạng cục bộ. Thay vì làm quá tải các tài nguyên mạng như máy chủ DNS, trước tiên các máy chủ cố gắng xác định máy chủ mà chúng đang tìm kiếm có nằm trên cùng một mạng cục bộ hay không bằng cách gửi yêu cầu LLMNR và xem có máy chủ nào phản hồi không. NBT-NS là giao thức tiền thân của LLMNR và các yêu cầu WPAD được thực hiện để tìm proxy cho các kết nối HTTP(s) trong tương lai.

Vì các giao thức này dựa vào các yêu cầu được phát trên mạng cục bộ, thiết bị giả mạo của chúng ta cũng nhận được những yêu cầu này. Thông thường, những yêu cầu này sẽ bị loại bỏ vì chúng không dành cho máy chủ của chúng ta. Tuy nhiên, Responder sẽ tích cực lắng nghe các yêu cầu và gửi phản hồi độc hại cho máy chủ đang yêu cầu biết rằng IP của chúng ta được liên kết với máy chủ được yêu cầu. Bằng cách đầu độc những yêu cầu này, Responder buộc máy khách kết nối đến AttackBox của chúng ta. Nó bắt đầu lưu trữ một số máy chủ như SMB, HTTP, SQL và các máy chủ khác để bắt được các yêu cầu và buộc xác thực.

**Chặn NetNTLM Challenge**

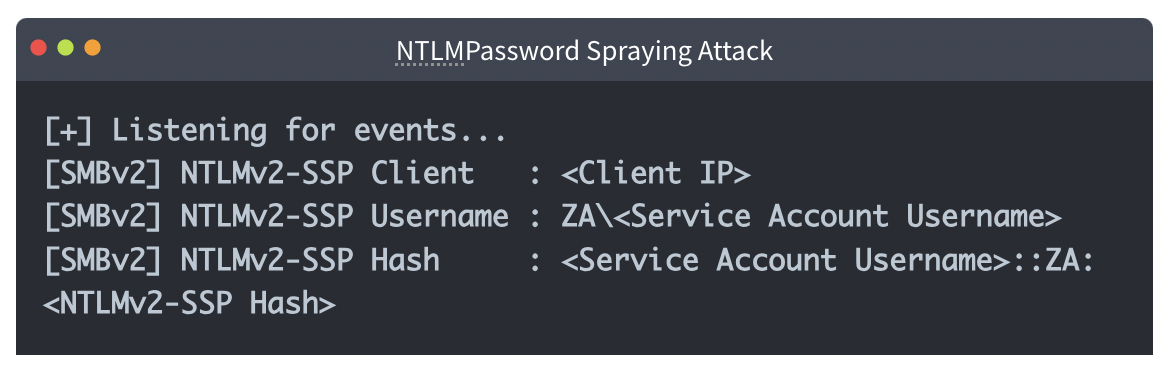
Một điều phải lưu ý là Responder cần chạy đua với thời gian bằng cách đầu độc các kết nối để đảm bảo bạn chặn được kết nối. Điều đó có nghĩa là Responder thường bị giới hạn trong việc đầu độc các challenges xác thực trên mạng cục bộ. Vì chúng ta đang kết nối mạng qua VPN, chúng ta chỉ có thể đầu độc các challenges của xác thực xảy ra trên mạng VPN. Vì lý do này, chúng tôi đã mô phỏng một yêu cầu xác thực có thể bị đầu độc chạy 30 phút một lần. Điều đó có nghĩa là bạn phải đợi một chút trước khi chặn được challenge của NetNTLM và phản hồi.

Mặc dù Responder có thể chặn và đầu độc nhiều yêu cầu xác thực khi được thực thi từ thiết bị giả mạo kết nối đến mạng LAN của tổ chức, điều quan trọng phải hiểu là hành vi này có thể gây rối và bị phát hiện. Bằng cách đầu độc các yêu cầu xác thực, nỗ lực xác thực mạng thông thường sẽ bị thất bại, có nghĩa là người dùng và dịch vụ sẽ không kết nối được máy chủ và chia sẻ chúng mong muốn. Hãy ghi nhớ điều này khi dùng Responder để đánh giá bảo mật.

Chúng ta sẽ thiết lập Responder chạy trên giao diện kết nối với VPN.

sudo responder -I breachad

Nếu bạn đang dùng AttackBox, không phải tất cả các dịch vụ của Responder có thể khởi động vì các dịch vụ khác đang chạy cổng đó. Tuy nhiên, nó sẽ không ảnh hưởng đến quá trình này. Responder sẽ lắng nghe các yêu cầu LLMNR, NBT-NS và WPAD đang gửi đến. Chúng ta sẽ để Responder chạy một chút trên mạng LAN thực. Trong trường hợp này, chúng ta phải mô phỏng đầu độc bằng cách yêu cầu 1 trong các máy chủ xác thực đến máy ảo trong VPN. Để Responder chạy một chút (10 phút) và bạn sẽ nhận được kết nối SMBv2 có thể lôi kéo và trích xuất được phản hồi NTLMv2-SSP.



Nếu chúng ta đang dùng thiết bị giả mạo, chúng ta có thể chạy Responder trong một thời gian khá lâu và nhận được một số phản hồi. Chúng ta có thể bẻ khóa các phản hồi với hy vọng khôi phục lại mật khẩu NTLM. Sao chép NTLMv2-SSP Hash vào 1 tệp văn bản, bẻ khóa hàm băm bằng lệnh sau:

hashcat -m 5600 <hash file> <password file> --force

**Relaying the Challenge**

Trong một số trường hợp, chúng ta cần làm thêm 1 bước nữa bằng cách lặp lại challenge thay vì lấy nó trực tiếp. Chúng ta cần thỏa một số điều kiện mới làm được:

* SMB Signing tắt hoặc bật nhưng không được thực thi. Khi chúng ta lặp lại, chúng ta thực hiện những thay đổi nhỏ đối với yêu cầu chuyển nó đi. Nếu SMB Signing được bật, chúng ta không thể giả mạo chữ ký tin nhắn, máy chủ sẽ từ chối nó.
* Người dùng cần có các quyền cần thiết trên máy chủ để truy cập tài nguyên. Lý tưởng nhất là chúng ta lặp lại challenge và response của một tài khoản có đặc quyền admin trên máy chủ.
* Vì chúng ta chưa có chỗ đứng trong AD, tài khoản nào sẽ có quyền trên máy chủ nào chỉ là phỏng đoán.

Đó là lý do tại sao blind relay không phổ biến. Lý tưởng nhất là bạn phải có được chỗ đứng trong AD bằng một phương pháp khác, sau đó liệt kê đặc quyền của tài khoản mà bạn xâm nhập. Từ đó, bạn có thể di chuyển ngang để leo thang đặc quyền trên domain. Tuy nhiên vẫn nên hiểu cách thức hoạt động của tấn công phát lại:



**Microsoft Deployment Toolkit**

Các tổ chức lớn cần các công cụ để triển khai và quản lý cơ sở hạ tầng bất động sản. Trong các tổ chức lớn, bạn không thể yêu cầu nhân viên IT sử dụng đĩa DVD hoặc thậm chí ổ USB Flash để cài đặt phần mềm trên từng máy. May mắn thay, Microsoft đã cung cấp các công cụ cần thiết để quản lý tài sản. Tuy nhiên, chúng ta có thể khai thác lỗi cấu hình trong các công cụ đó để breach được AD.

**MDT và SCCM**

Microsoft Deployment Toolkit (MDT) là **1 dịch vụ Microsoft tự động triển khai hệ điều hành Windows.** Các tổ chức lớn sử dụng các dịch vụ như MDT để giúp triển khai các images mới trong cơ sở của họ hiệu quả hơn vì các images cũ có thể được bảo trì và cập nhật ở vị trí trung tâm.

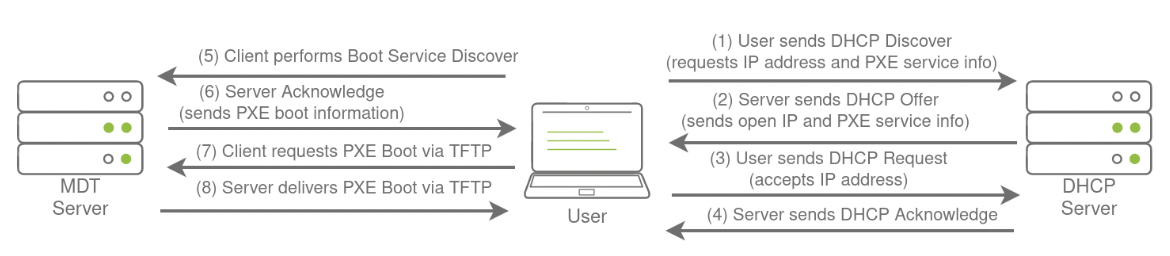
Thông thường, MDT được tích hợp với System Center Configuration Manager (SCCM) của Microsoft, quản lý tất cả các bản cập nhật cho tất cả ứng dụng, dịch vụ và hệ điều hành của Microsoft. Nó cho phép nhóm iT cấu hình trước và quản lý các images khởi động. Nếu họ cần cấu hình cho 1 máy ảo mới, họ chỉ cần cắm vào cáp mạng và mọi thứ sẽ diễn ra tự động. Họ có thể thực hiện nhiều thay đổi khác nhau cho các images như cài đặt trước các phần mềm mặc định như Office365 và anti-virus. Nó cũng đảm bảo bản mới dựng được cập nhật trong lần cài đặt đầu tiên.

SCCM có thể xem là một bản mở rộng và là người anh lớn của MDT. Phần mềm sẽ xảy ra chuyện gì sau khi nó được cài đặt? SCCM giống như quản lý bản vá cho các phần mềm. Nó cho phép đội IT xem lại các bản cập nhật mà phần mềm đã cài đặt. Họ có thể kiểm tra các bản vá trong môi trường sàng lọc để đảm bảo chúng được ổn định trước khi triển khai trên tất cả máy ảo. Điều này làm cho cuộc sống của nhóm IT trở nên dễ dàng hơn.

Tuy nhiên, bất cứ thứ gì quản lý tập trung như MDT và SCCM cũng có thể trở thành mục tiêu của kẻ tấn công. Mặc dù MDT có thể được cấu hình bằng nhiều cách khác nhau, nhưng trong bài này chúng ta sẽ tập trung hoàn toàn vào cấu hình Preboot Execution Environment (PXE) boot.

**PXE Boot**

Các tổ chức lớn sử dụng PXE boot, cho phép các thiết bị mới tải và cài đặt phần mềm trực tiếp trên mạng. **MDT có thể tạo, quản lý và lưu trữ các images PXE boot**. PXE boot thường tích hợp với DHCP, DHCP cấp mới IP, máy chủ được phép yêu cầu PXE boot image, bắt đầu quá trình cài đặt hệ điều hành trên mạng.



Khi tiến trình được thực hiện, máy khách dùng kết nối TFTP để tải PXE boot image. Chúng ta có thể khai thác PXE boot image cho hai mục đích khác nhau:

* Đưa vào 1 vector leo thang đặc quyền, chẳng hạn như một tài khoản Local Administrator để giành quyền truy cập quản trị viên trong hệ điều hành khi PXE boot được hoàn tất.
* Thực hiện tấn công quét mật khẩu để khôi phục thông tin đăng nhập AD trong quá trình cài đặt

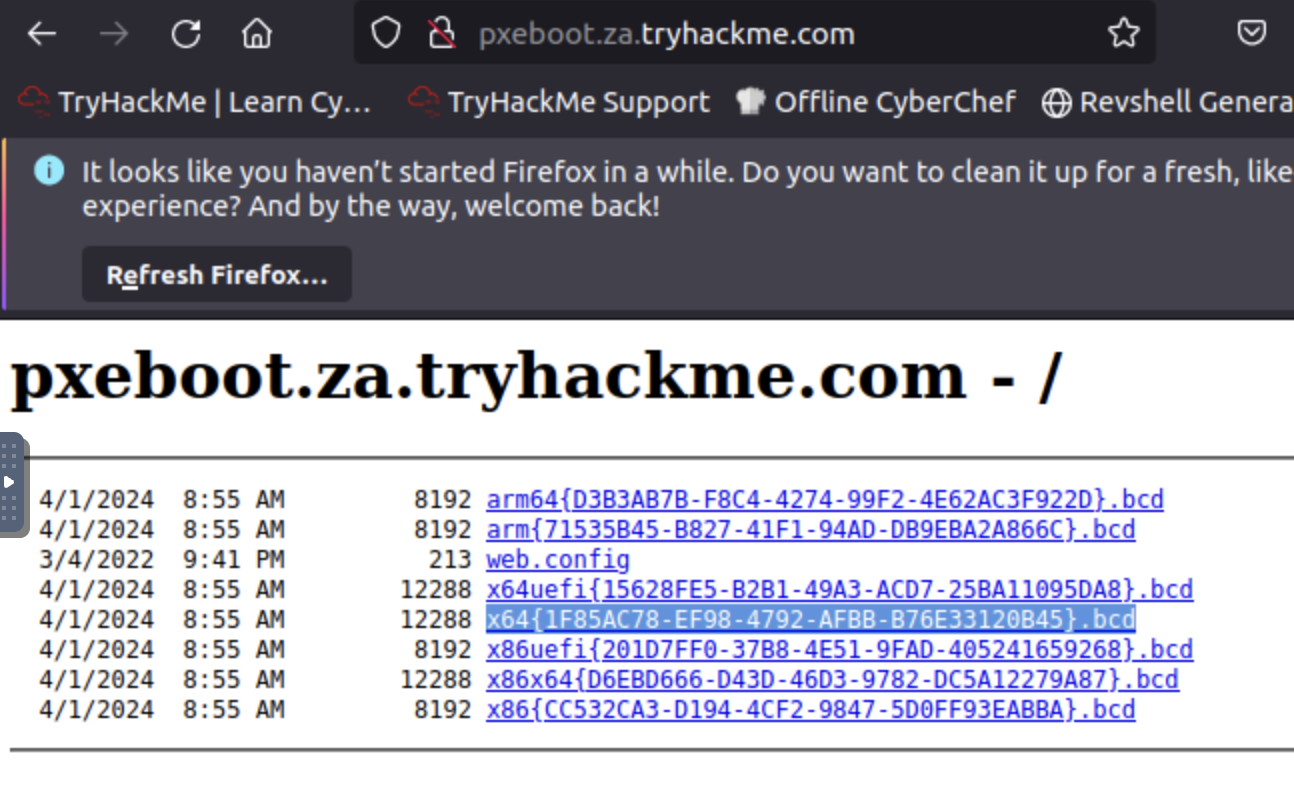
Trong bài này, chúng ta sẽ tập trung vào phần sau. Chúng ta sẽ cố gắng khôi phục tài khoản triển khai dịch vụ được liên kết với dịch vụ MDT bằng tấn công quét mật khẩu.

**PXE Boot Image Retrieval**

Vì DHCP hơi phức tạp nên chúng ta sẽ bỏ qua các bước đầu tiên của cuộc tấn công này. Chúng ta sẽ bỏ qua phần chúng ta cố gắng yêu cầu IP và cấu hình sẵn PXE boot từ DHCP. Chúng ta sẽ làm phần còn lại của tấn công bằng tay.

Thông tin đầu tiên liên quan đến cấu hình sẵn trong PXE boot mà bạn nhận được qua DHCP là **IP của máy chủ MDT** (sơ đồ mạng của Tryhackme).

Thông tin thứ hai mà bạn nhận được là **tên của tập tin BCD**. Các tập tin lưu trữ thông tin liên quan đến PXE Boots cho nhiều loại kiến trúc khác nhau. Để lấy được thông tin trên, bạn cần kết nối đến trang web: http://pxeboot.za.tryhackme.com



x64{1F85AC78-EF98-4792-AFBB-B76E33120B45}.bcd

Thông thường, bạn sẽ sử dụng TFTP để yêu cầu từng tệp BCD và liệt kê cấu hình cho tất cả chúng. Tuy nhiên, để tiết kiệm thời gian, chúng ta sẽ tập trung vào tập tin BCD của cấu trúc x64.

Với thông tin ban đầu chúng ta khôi phục từ DHCP, chúng ta có thể liệt kê và truy suất PXE Boot image.

ssh thm@THMJMP1.za.tryhackme.com

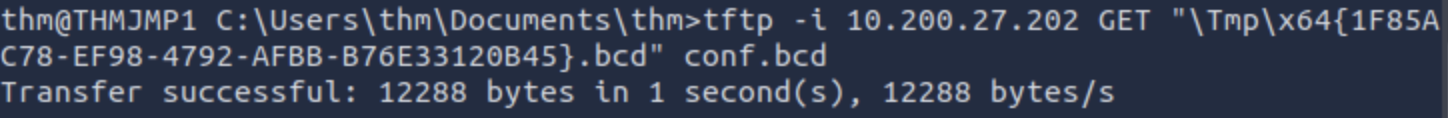
password: Password1@

Để đảm bảo tất cả người dùng trên mạng có thể dùng SSH, bắt đầu tạo 1 thư mục với tên của bạn và sao chép powerpxe đến thư mục đó:

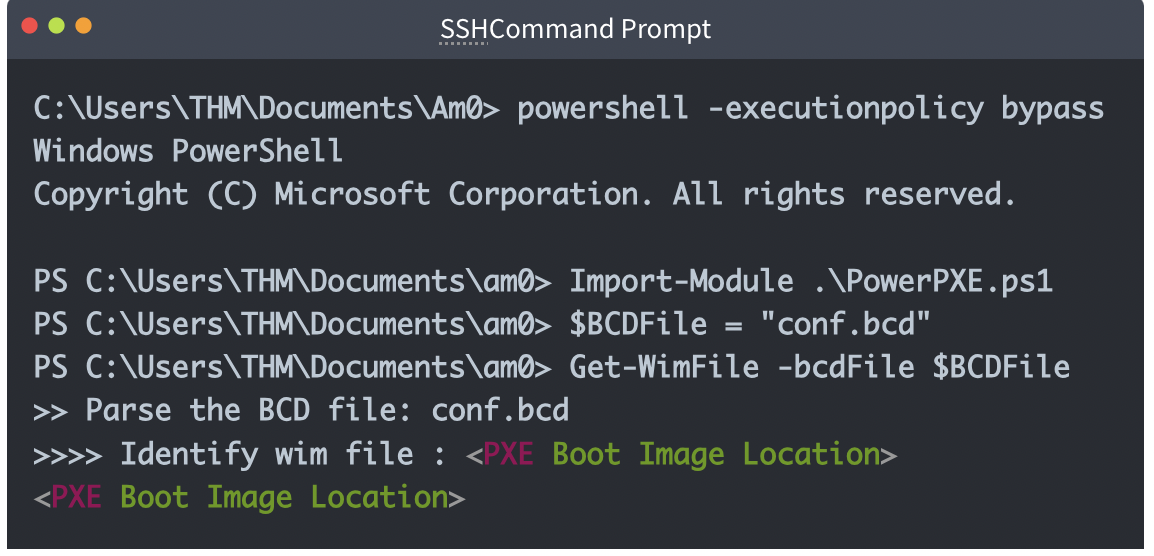


Bước đầu tiên chúng ta cần thực hiện là dùng TFTP và tải tập tin BCD để đọc tệp cấu hình của máy chủ MDT. TFTP phức tạp hơn FTP một chút vì chúng ta không thể liệt kê các tập tin. Thay vào đó, chúng ta gửi yêu cầu tệp và máy chủ sẽ kết nối lại với chúng ta qua UDP để vận chuyển tập tin. Do đó, chúng ta cần phải chính xác khi chỉ định tệp và đường dẫn tệp. Tập tin BCD luôn nằm trong thư mục /Tmp trên máy chủ MDT. Chúng ta có thể vận chuyển TFTP bằng lệnh sau:

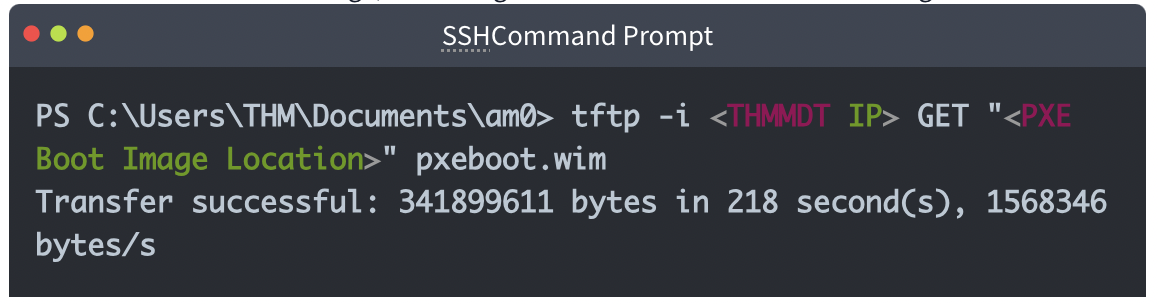
tftp -i <THMDT IP> GET "\Tmp\x64{1F85AC78-EF98-4792-AFBB-B76E33120B45}.bcd" conf.bcd



Chúng ta sẽ **dùng Powerpxe để đọc nội dung của tập tin BCD**. Powerpxe là 1 powershell script tự động thực hiện loại tấn công này nhưng thường trả về nhiều kết quả khác nhau, vì vậy tốt nhất bạn nên thực hiện thủ công. Chúng ta sẽ dùng hàm Get-WimFile để **khôi phục các vị trí của PXE Boot images từ tập tin BCD:**



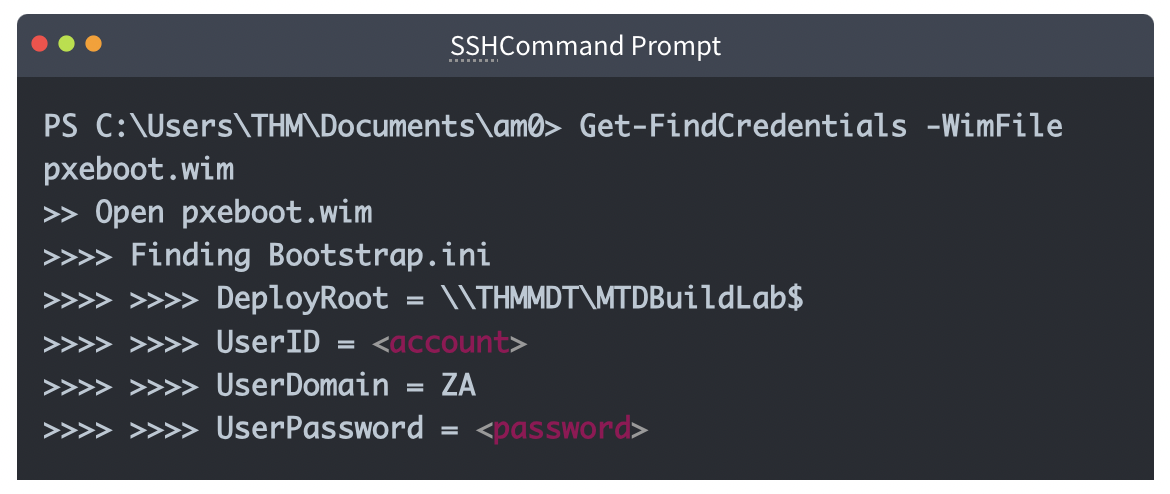
Tập tin WIM là image có thể khởi động trong Windows Imaging Format (WIM). Bây giờ chúng ta có vị trí của PXE Boot image, chúng ta có thể dùng tftp một lần nữa để tải image:



**Khôi phục thông tin đăng nhập từ PXE Boot Image**

Chúng ta đã khôi phục được PXE Boot image, chúng ta có thể trích xuất thông tin đăng nhập. Cần lưu ý rằng có nhiều cuộc tấn công khác nhau mà chúng ta có thể thực hiện. Chúng ta có thể thêm người dùng local administrater, vì vậy chúng ta có đặc quyền quản trị viên ngay khi image khởi động, chúng ta có thể cài đặt image để có 1 máy tính tham gia domain. Trong bài này chúng ta chỉ tập trung vào 1 cuộc tấn công đơn giản là cố gắng trích xuất thông tin đăng nhập.

Chúng ta sẽ dùng powerpxe để khôi phục thông tin đăng nhập.



**Các tệp cấu hình**

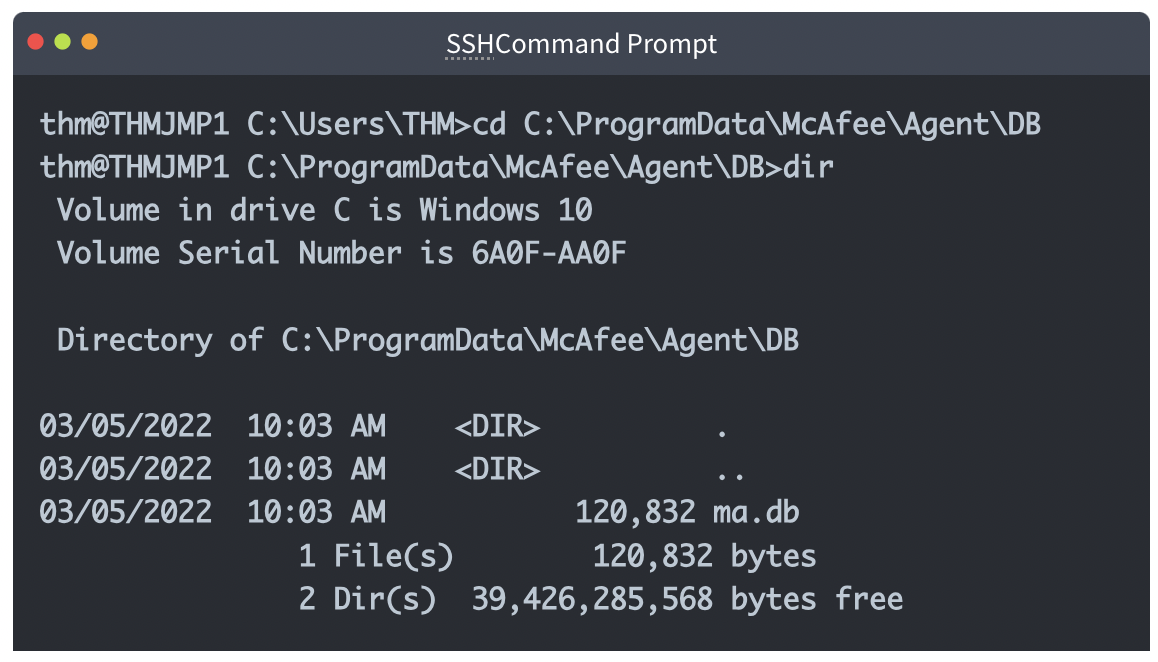
Manh mối cuối cùng chúng ta sẽ khám phá trên mạng là các tệp cấu hình.

**Các tệp cấu hình chứa thông tin đăng nhập**

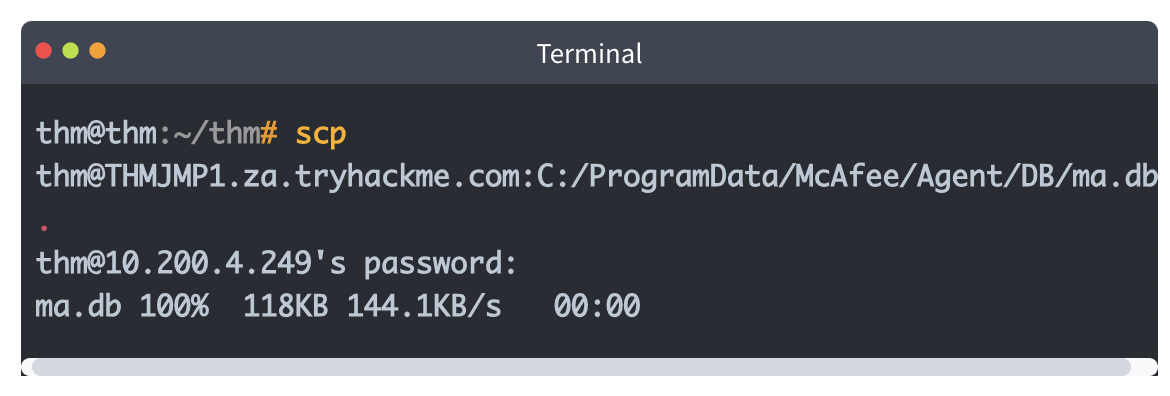
Trong bài này, chúng ta sẽ tập trung khôi phục thông tin đăng nhập từ 1 ứng dụng được triển khai tập trung. Thông thường, các ứng dụng này cần 1 phương thức để xác thực với domain trong cả giai đoạn cài đặt và thực thi. Một ví dụ về ứng dụng như vậy là McAfee Enterprise Endpoint Security, các tổ chức có thể sử dụng làm công cụ phản hồi và phát hiện điểm cuối để bảo mật.

McAfee nhúng thông tin đăng nhập được sử dụng trong quá trình cài đặt để kết nối lại với bộ điều hướng trong tập tin ma.db. Bạn có thể truy cập cục bộ để đọc tập tin cơ sở dữ liệu, khôi phục tài khoản AD.

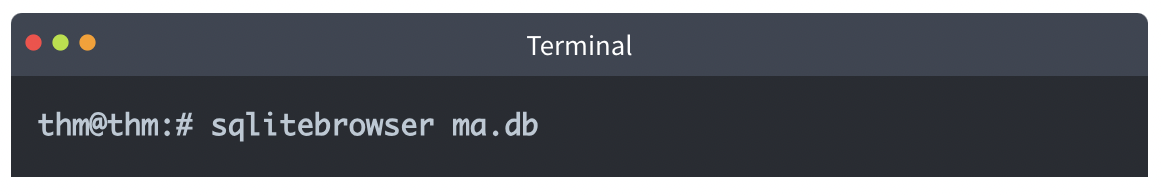
Tập tin ma.db được lưu ở vị trí cố định:



Chúng ta có thể dùng scp để sao chép tập tin ma.db đến attackbox:



Để đọc tập tin csdl, chúng ta có thể dùng sqlitebrowser.



Chọn Browse Data và tập trung vào bảng AGENT\_REPOSITORIES

