# Mục tiêu:

-Sử dụng Hydra cho

+cuộc tấn công đoán mật khẩu chống lại SMB trên máy windows

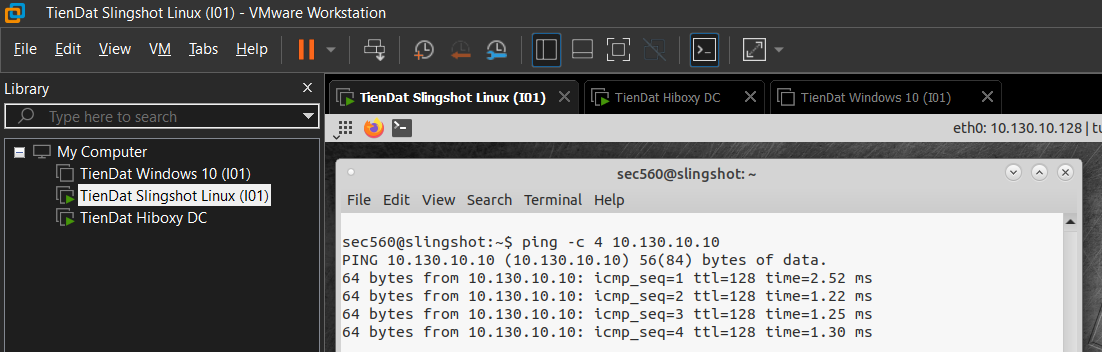
+Cuộc tấn công spray mật khẩu chống lại SMB trên máy windows

+Cuộc tấn công đoán mật khẩu chống lại SSH deamon

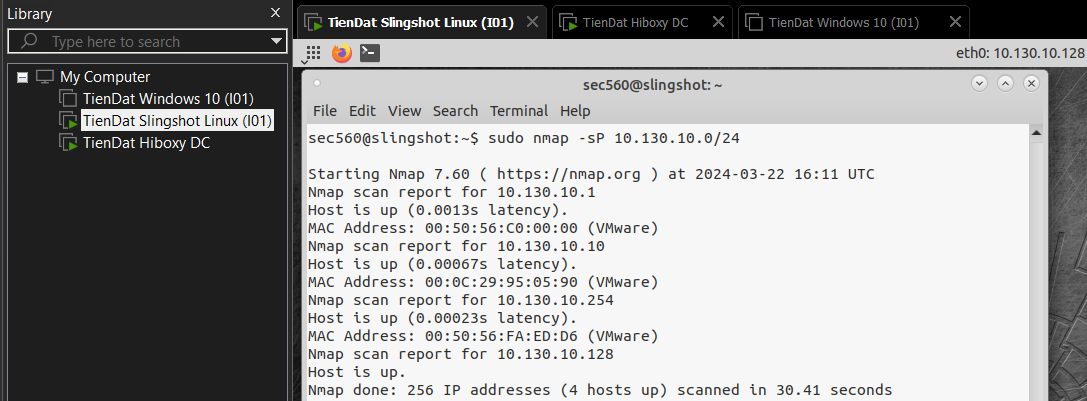
# 1.Password Spray (SMB)

Thực hiện một phương pháp phun mật khẩu, trong đó chúng ta chọn một mật khẩu và rất nhiều tên người dùng. Đây là một kỹ thuật tốt khi bạn có một danh sách tài khoản người dùng lớn và bạn phải cẩn thận với các chính sách đăng nhập khóa tài khoản sau quá nhiều lần đoán mật khẩu không thành công.

-Ping đến máy 10.130.10.10 để kiểm tra kết nối



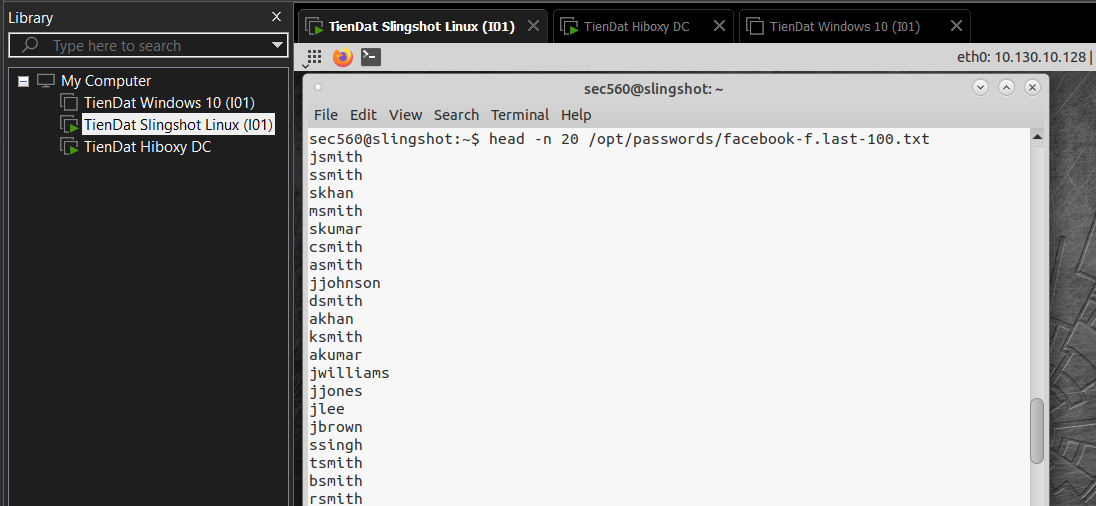
-Thực hiện quét ping (nmap quét mạng; -sP là tùy chọn của nmap – thực hiện quét Ping) để xác định xem các địa chỉ IP trong mạng con hoạt động và có thể truy cập đc hay ko



-Hiển thị 20 dòng đầu tiên của tệp tin "facebook-f.last-100.txt" trong thư mục "/opt/passwords"

**+"head"**: Là một lệnh dùng để hiển thị các dòng đầu tiên của một tệp tin

+tùy chọn "-n 20" cho biết rằng chúng ta muốn hiển thị 20 dòng đầu tiên của tệp tin.



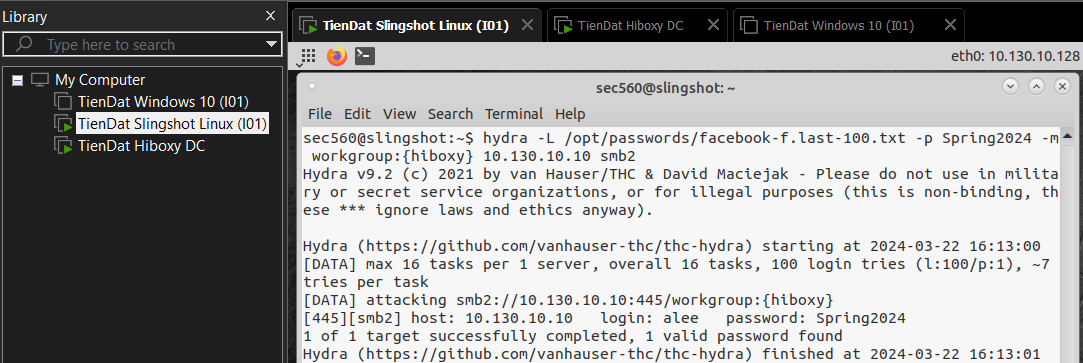
-Sử dụng lệnh để thực hiện tấn công brute-force (tấn công nguồn mở) trên giao thức SMB2 đối với địa chỉ IP 10.130.10.10

**+"hydra"**: Là một công cụ tấn công brute-force phổ biến được sử dụng để thử các mật khẩu khác nhau và tìm ra mật khẩu chính xác để truy cập vào hệ thống hoặc dịch vụ.

+"-L /opt/passwords/facebook-f.last-100.txt": Đây là tùy chọn của Hydra để chỉ định danh sách tên người dùng (username) từ tệp tin "/opt/passwords/facebook-f.last-100.txt". Hydra sẽ thử các tên người dùng từ danh sách này trong quá trình tấn công.

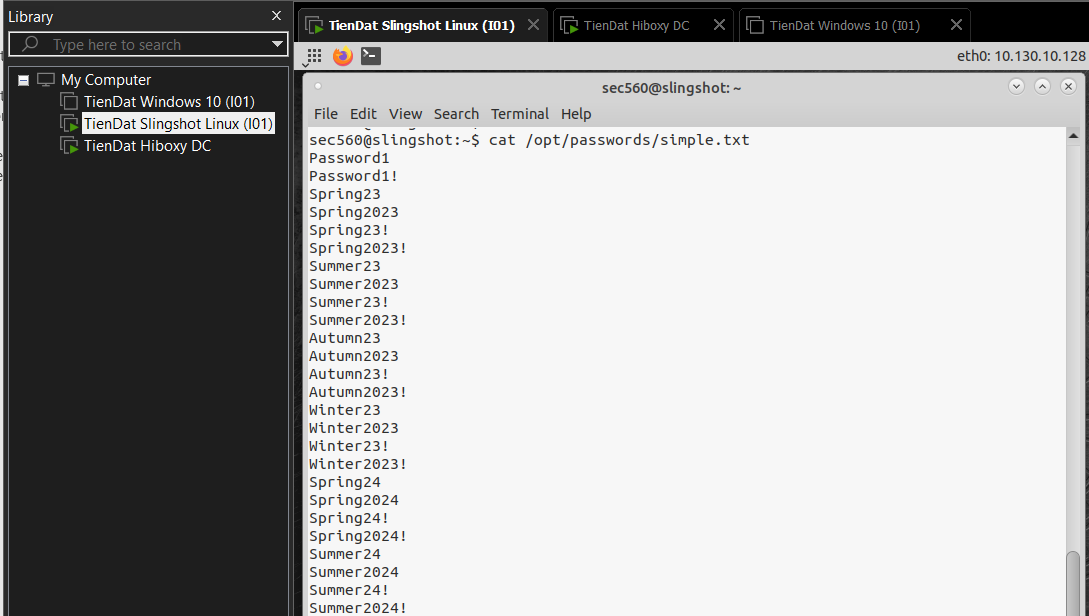
+"-p Spring2024": Đây là tùy chọn của Hydra để xác định mật khẩu (password) cần thử. Trong trường hợp này, mật khẩu được đặt là "Spring2024".

+"-m workgroup:{hiboxy}": Đây là tùy chọn của Hydra để xác định thông tin xác thực đối với giao thức SMB2. Trong trường hợp này, Hydra sẽ sử dụng tên người dùng "workgroup" và mật khẩu "{hiboxy}" để thử tấn công.

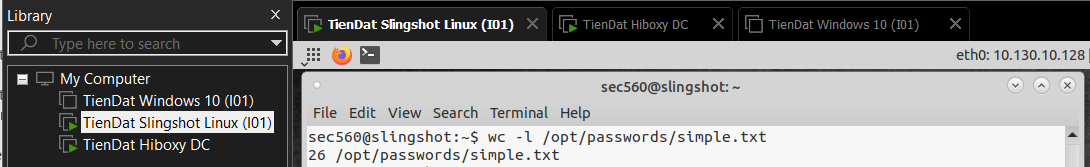


# 2. The dictionary

-Đọc file



-Lệnh đếm số dòng trong tệp tin simple.txt

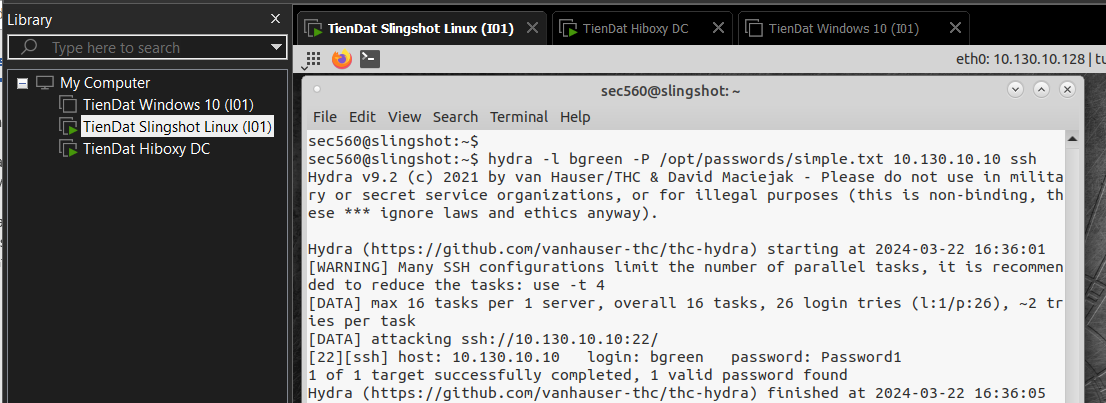


# 3.Password guessing (SSH)

-Lệnh "hydra -l bgreen -P /opt/passwords/simple.txt 10.130.10.10 ssh" được sử dụng để thực hiện tấn công brute-force (tấn công nguồn mở) trên giao thức SSH đối với địa chỉ IP 10.130.10.10

+"-l bgreen": Đây là tùy chọn của Hydra để xác định tên người dùng (username) cần thử. Trong trường hợp này, tên người dùng được đặt là "bgreen".

+"-P": Đây là tùy chọn của Hydra để chỉ định đường dẫn đến tệp tin chứa danh sách mật khẩu (password list).



# 4.Verifying access

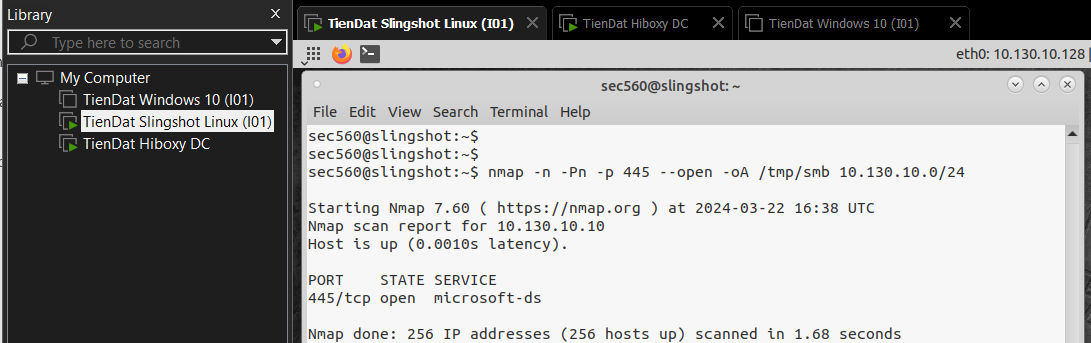
-Lệnh "nmap -n -Pn -p 445 --open -oA /tmp/smb 10.130.10.0/24" được sử dụng để quét các cổng mạng trên mạng con 10.130.10.0/24 và tìm các máy chủ có cổng 445 (cổng SMB) mở.

+"-n": Đây là tùy chọn của Nmap để vô hiệu hóa việc giải quyết tên miền (DNS resolution). Bằng cách sử dụng tùy chọn này, Nmap sẽ không thử giải quyết tên miền của các địa chỉ IP.

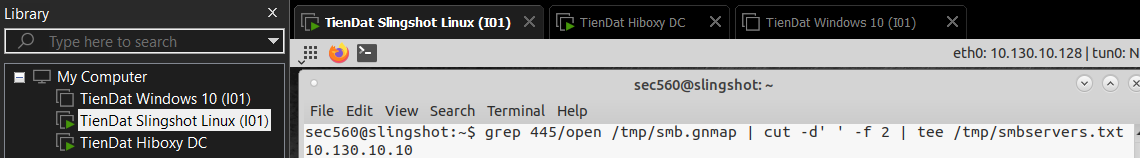
+"-Pn": Đây là tùy chọn của Nmap để bỏ qua việc kiểm tra tính khả dụng (ping sweep). Bằng cách sử dụng tùy chọn này, Nmap sẽ không thử ping các máy chủ để xác định xem chúng có phản hồi hay không.

+"-p 445": Đây là tùy chọn của Nmap để chỉ định cổng mạng mà chúng ta muốn quét. Trong trường hợp này, cổng 445 (cổng SMB) được chỉ định để tìm các máy chủ có cổng này mở.

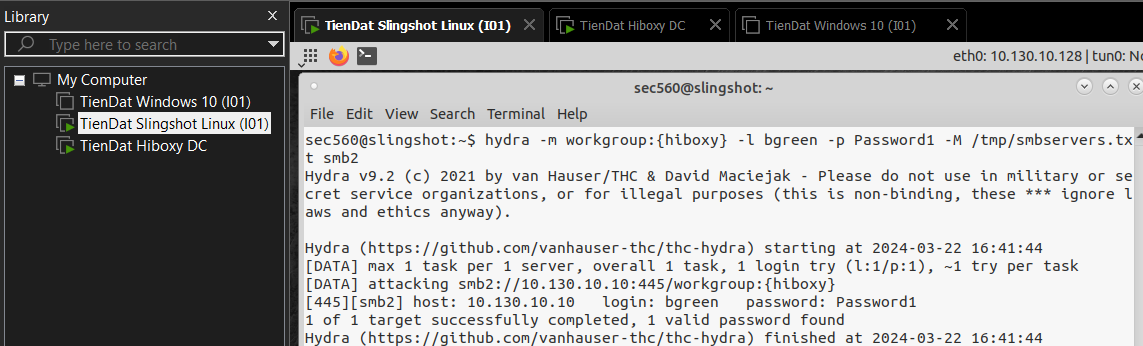
+"-oA /tmp/smb": Đây là tùy chọn của Nmap để lưu kết quả quét vào các tệp tin đầu ra. Trong trường hợp này, Nmap sẽ tạo các tệp tin đầu ra với tiền tố "/tmp/smb" (bao gồm tệp tin văn bản, tệp tin XML và tệp tin nén) để lưu trữ thông tin về quét.



-Lệnh "grep 445/open /tmp/smb.gnmap | cut -d' ' -f 2 | tee /tmp/smbservers.txt" được sử dụng để trích xuất địa chỉ IP của các máy chủ có cổng 445 mở từ tệp tin "/tmp/smb.gnmap" và lưu chúng vào tệp tin "/tmp/smbservers.txt"

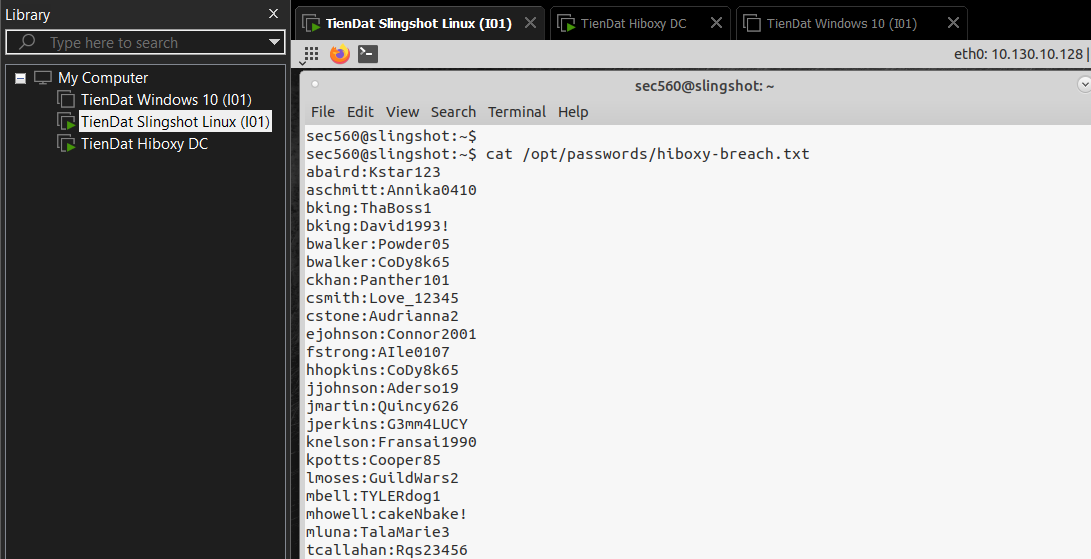


-Lệnh "hydra -m workgroup:{hiboxy} -l bgreen -p Password1 -M /tmp/smbservers.txt smb2" được sử dụng để thực hiện tấn công brute-force trên giao thức SMB2 (Server Message Block) đối với danh sách các máy chủ SMB được lưu trữ trong tệp tin "/tmp/smbservers.txt".

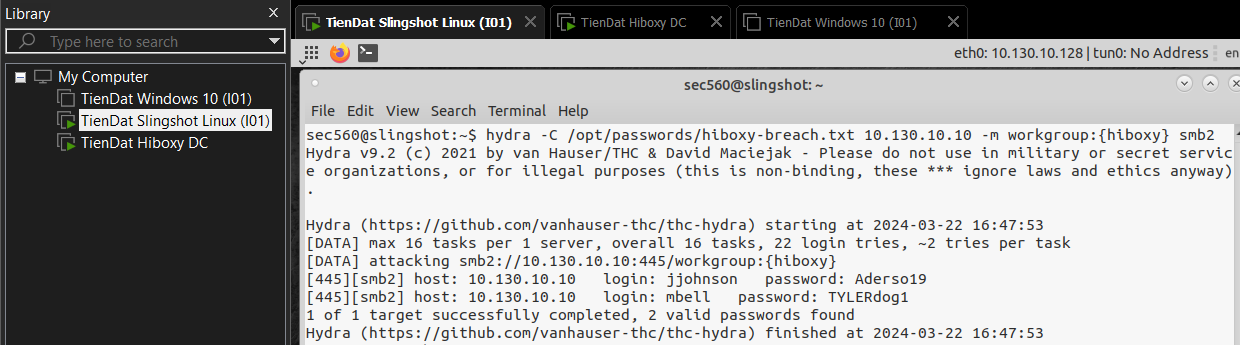


# 5. Breached Credentials

-Đọc file

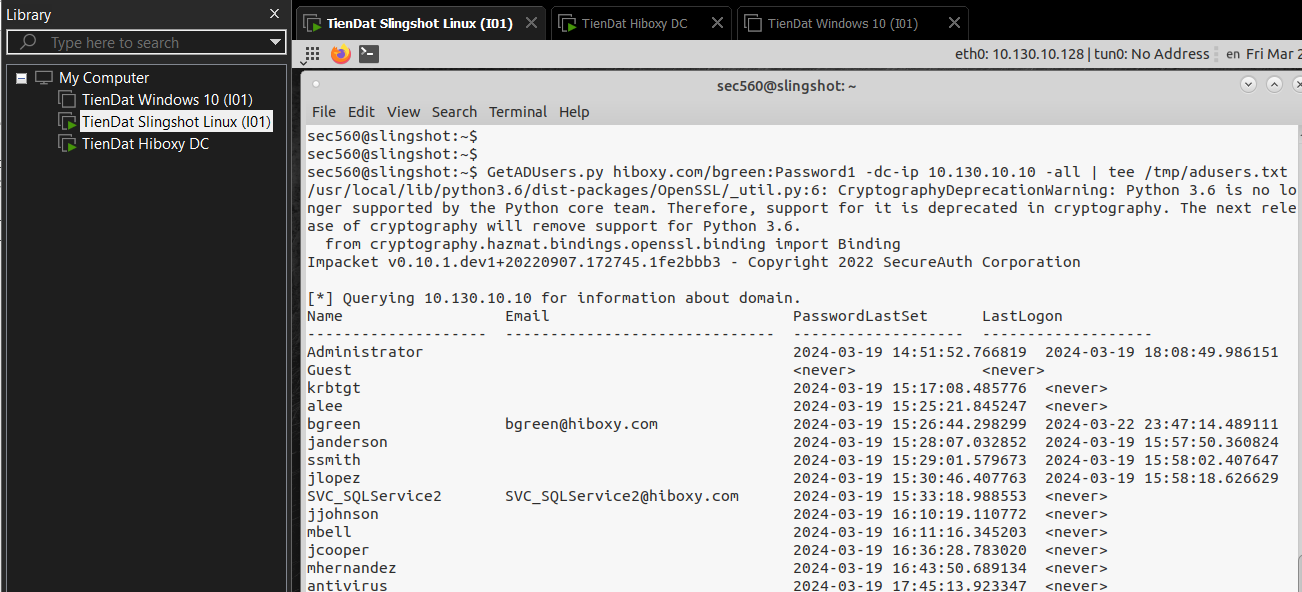


-Lệnh "hydra -C /opt/passwords/hiboxy-breach.txt 10.130.10.10 -m workgroup:{hiboxy} smb2" được sử dụng để thực hiện tấn công brute-force trên giao thức SMB2 đối với địa chỉ IP 10.130.10.10, sử dụng danh sách mật khẩu từ tệp tin "/opt/passwords/hiboxy-breach.txt" và thông tin tên miền là "workgroup" và tên người dùng bổ sung là "{hiboxy}".



# 6. Password Spraying all domain users

-Lệnh "GetADUsers.py hiboxy.com/bgreen:Password1 -dc-ip 10.130.10.10 -all | tee /tmp/adusers.txt" được sử dụng để lấy danh sách người dùng Active Directory (AD) từ miền hiboxy.com bằng cách sử dụng tên người dùng "bgreen" và mật khẩu "Password1". Kết quả sẽ được ghi vào tệp tin "/tmp/adusers.txt" và hiển thị trên màn hình



-Lệnh "tail -n +6 /tmp/adusers.txt | cut -d ' ' -f 1 | tee /tmp/domainusers.txt" được sử dụng để xử lý tệp tin "/tmp/adusers.txt" chứa danh sách người dùng Active Directory (AD) và tạo một tệp tin mới "/tmp/domainusers.txt" chứa chỉ danh sách tên người dùng.

-Lệnh "hydra -L /tmp/domainusers.txt -p Password1 -m workgroup:{hiboxy} 10.130.10.10 smb2" được sử dụng để thực hiện tấn công brute-force trên giao thức SMB2 đối với địa chỉ IP 10.130.10.10, sử dụng danh sách tên người dùng từ tệp tin "/tmp/domainusers.txt" và mật khẩu là "Password1". Thông tin tên miền được đặt là "workgroup" và tên người dùng bổ sung là "{hiboxy}".

