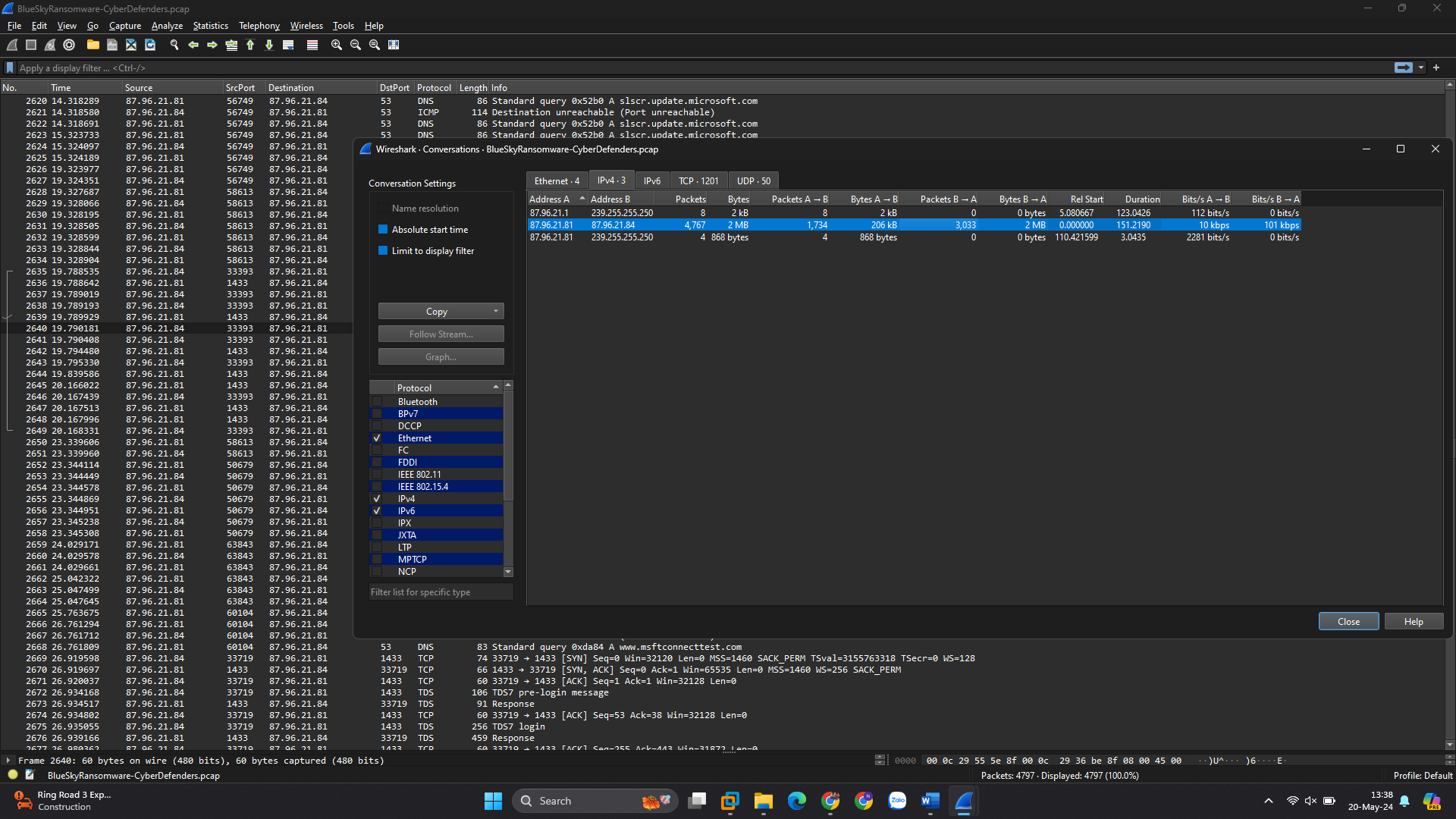
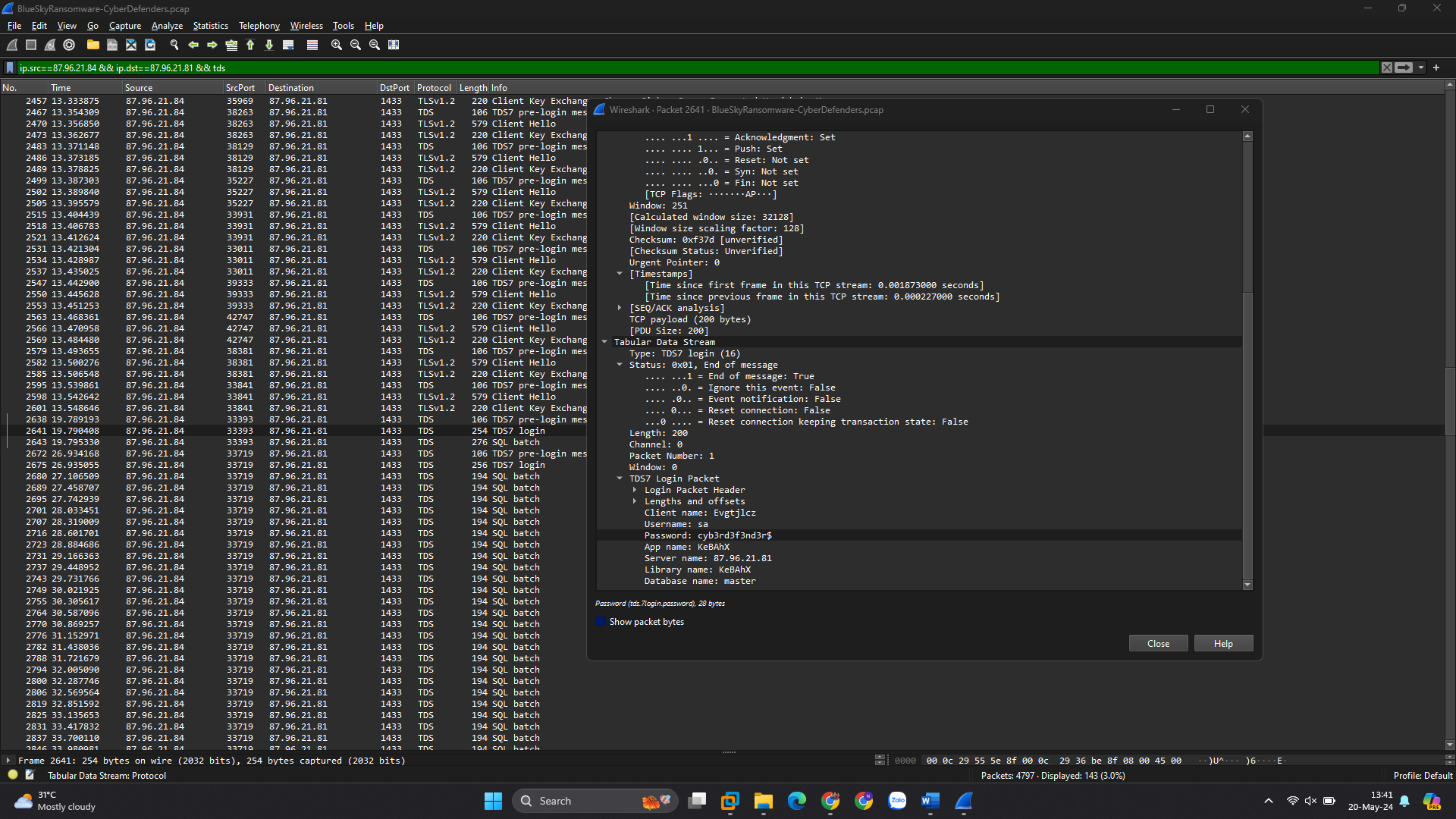
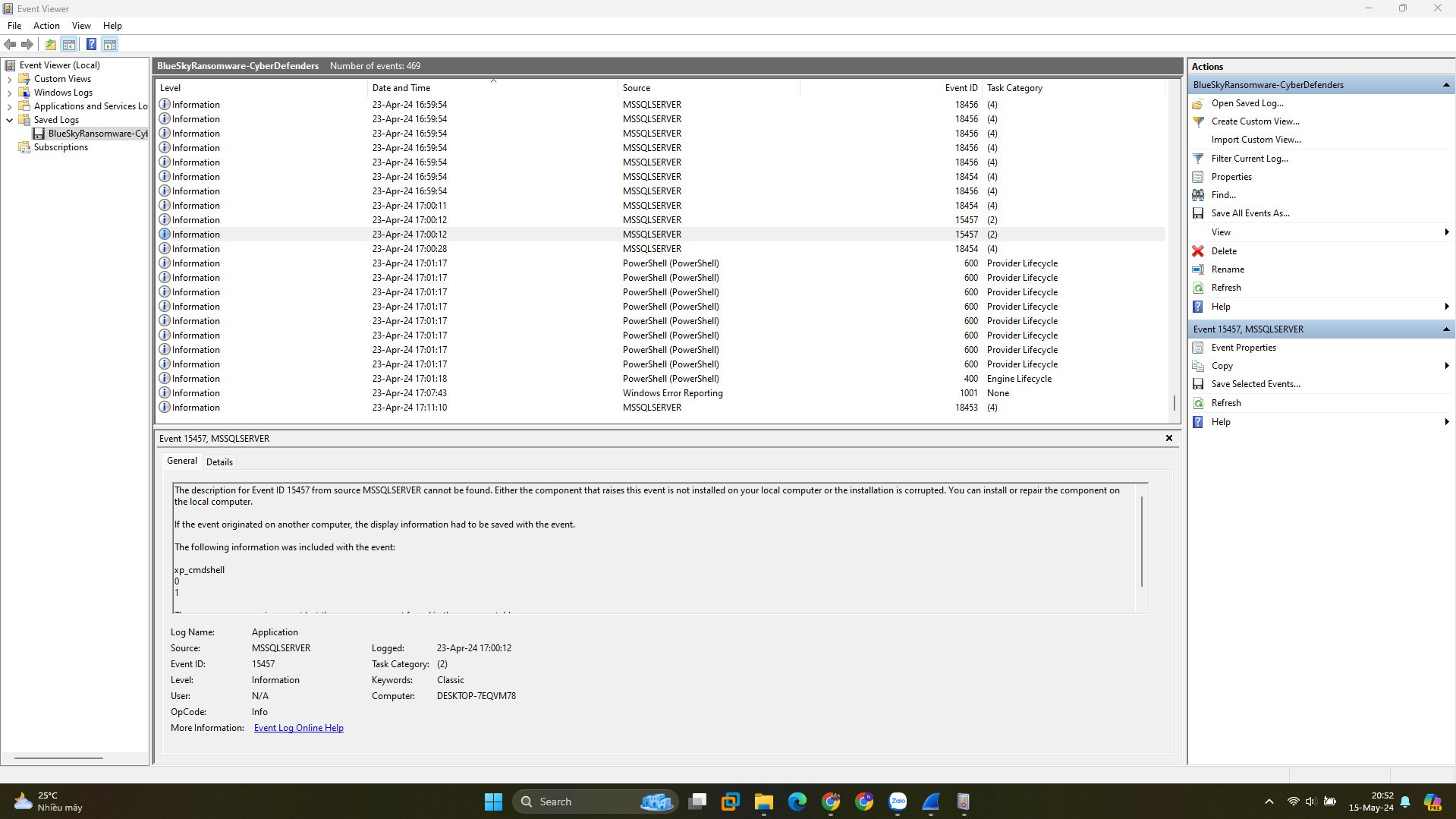
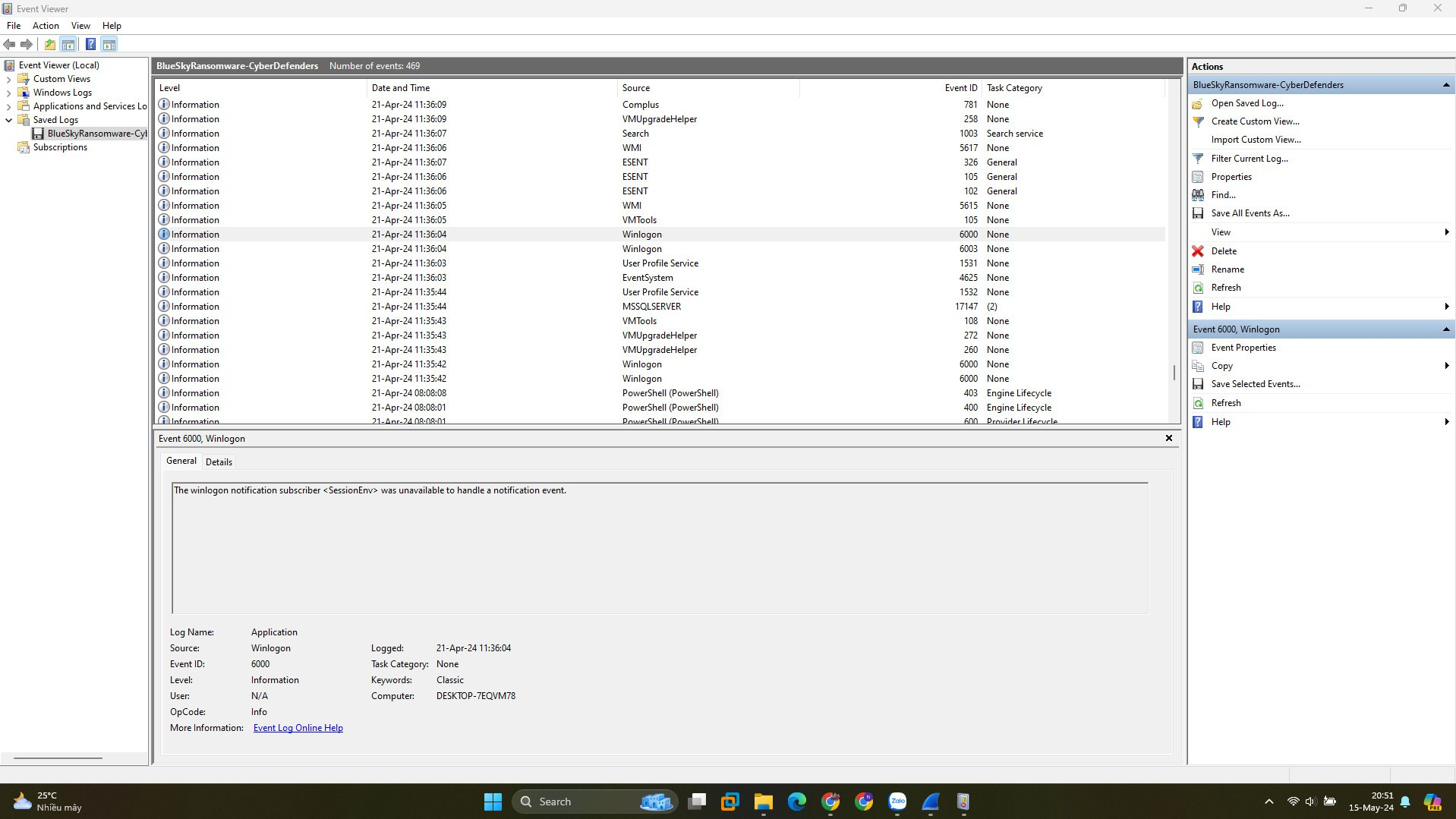
https://cyberdefenders.org/blueteam-ctf-challenges/bluesky-ransomware/

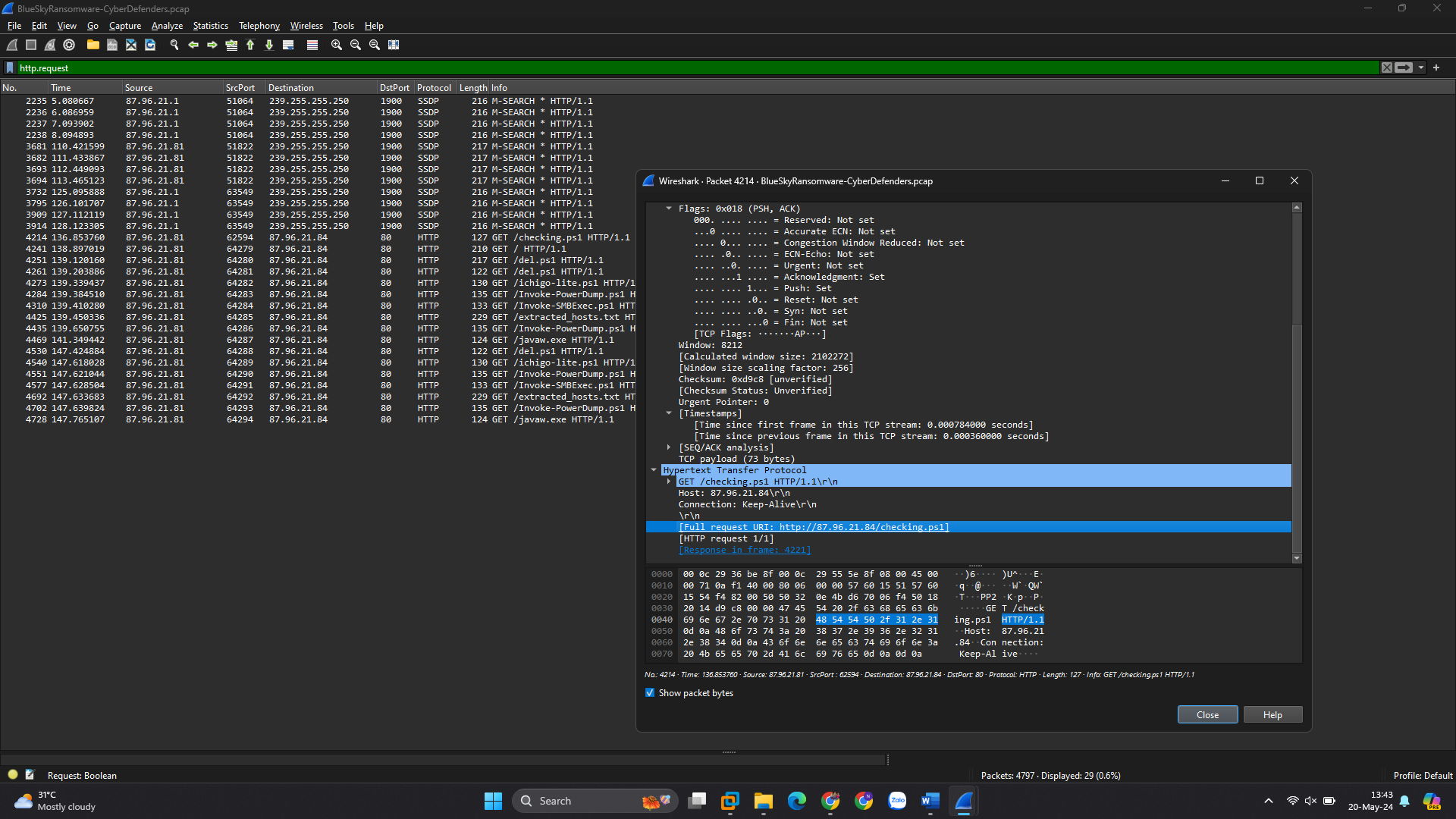
Q1. IP nguồn tấn công quét port: 87.96.21.84. Số packet mà 87.96.21.84 gửi đi cho 87.96.21.81 là 3.033 gói. Có nhiều gói tin đến từ 87.96.21.84 đang brute-force TDS Login vào 87.96.21.81.  


Q2. Username mục tiêu mà kẻ tấn công nhắm tới: sa.

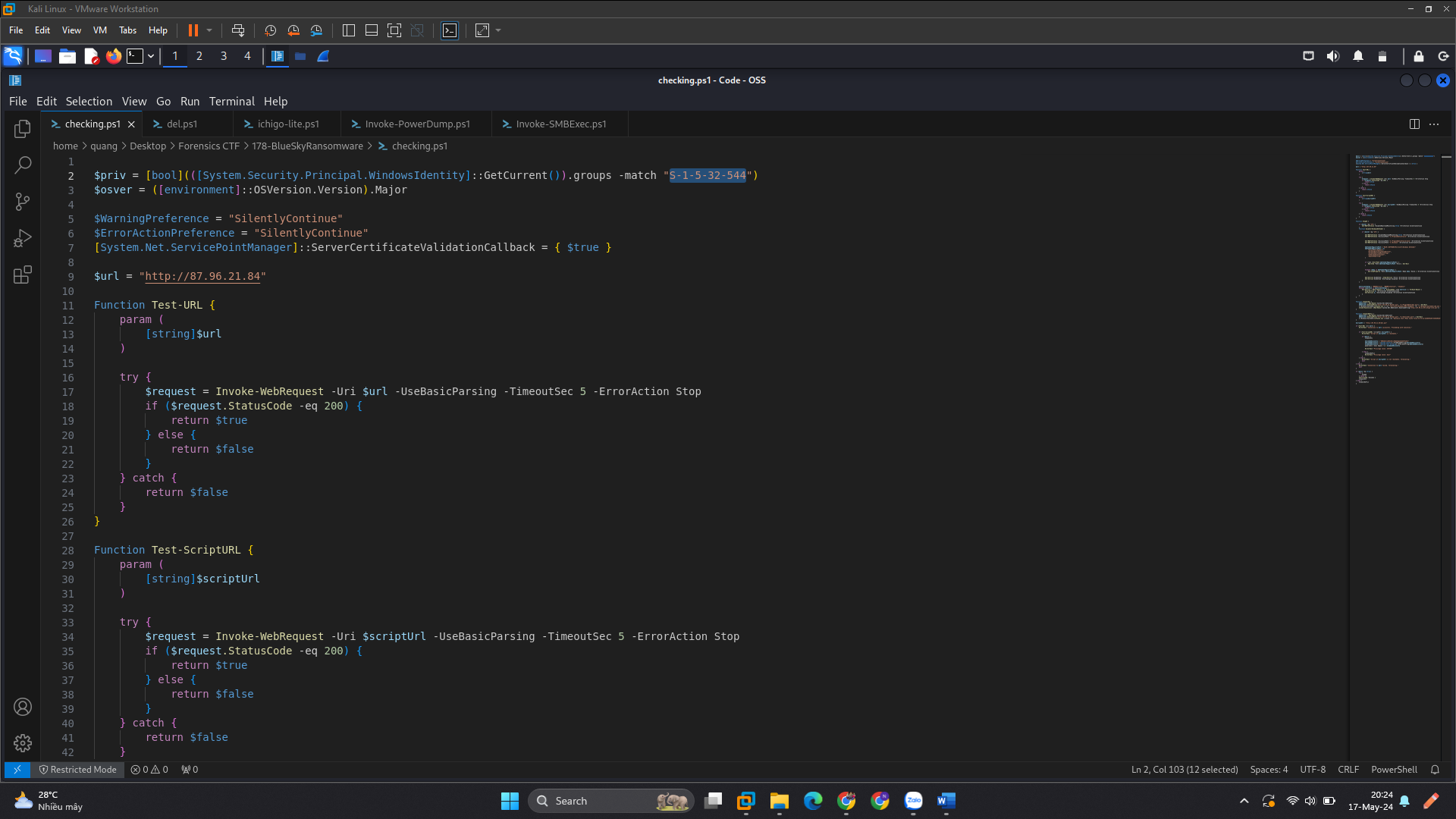
Q3. Password mục tiêu mà kẻ tấn công nhắm tới: cyb3rd3f3nd3r$.  


Q4. Những kẻ tấn công thường thay đổi một số cài đặt để tạo điều kiện thuận lợi cho việc di chuyển trong mạng. Kẻ tấn công đã kích hoạt xp\_cmdshell để kiểm soát máy chủ mục tiêu và thực thi các lệnh PowerShell.  


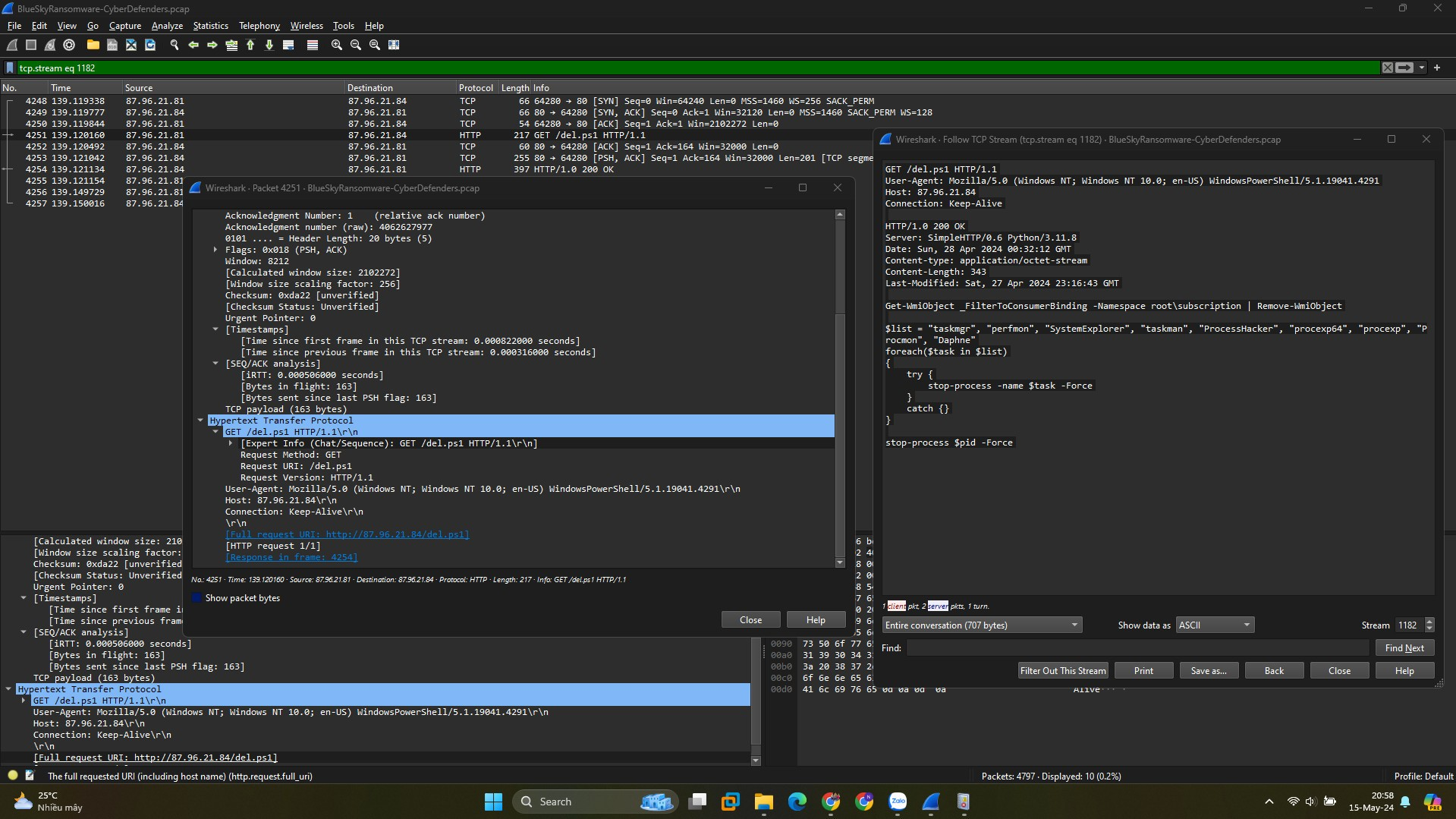
Q5. Việc chèn quy trình thường được những kẻ tấn công sử dụng để leo thang đặc quyền trong hệ thống. Kẻ tấn công đã đưa C2 (Command and Control) vào quy trình Winlogon.exe để leo quyền quản trị.  


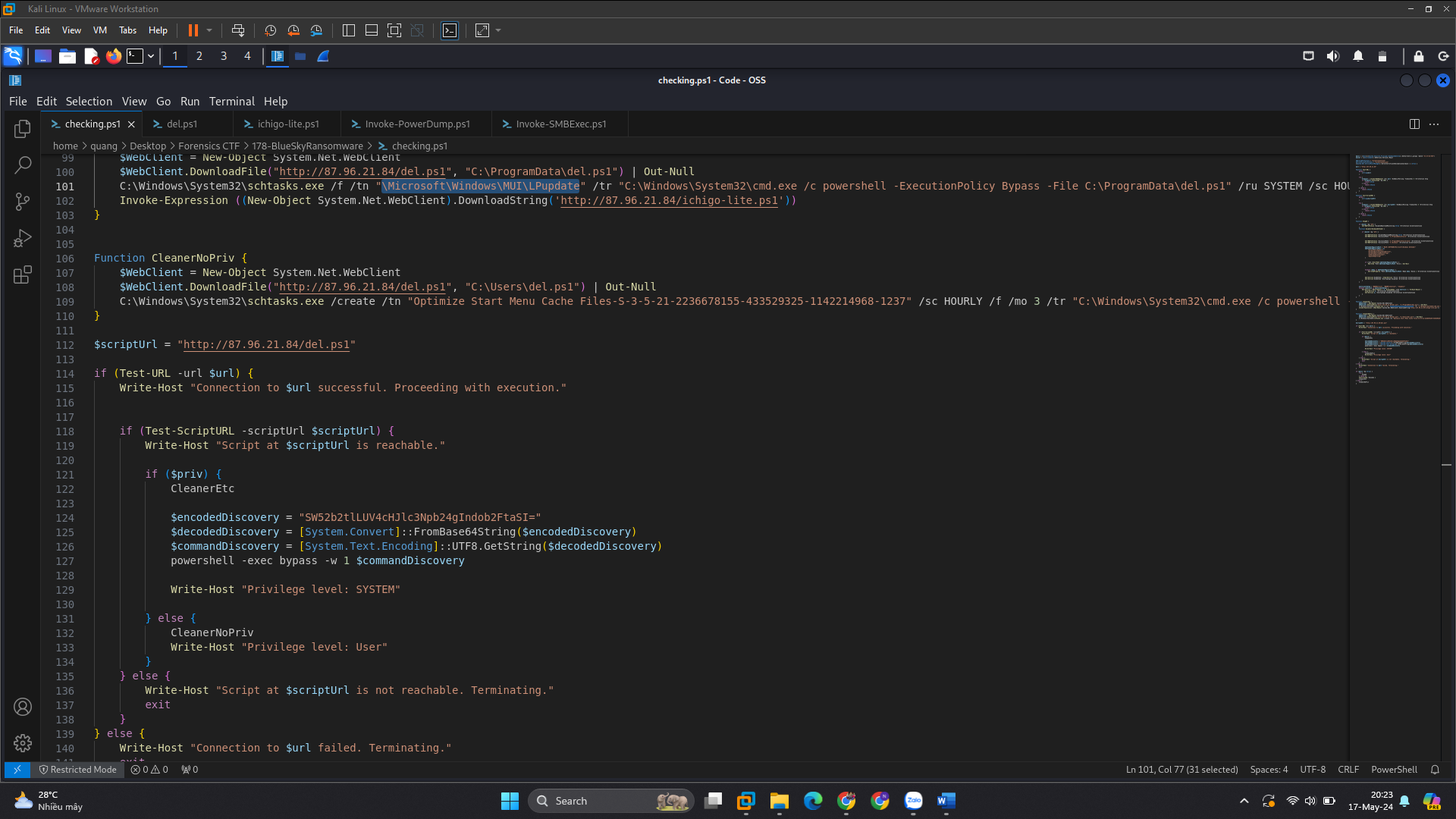
Q6. Sau khi leo quyền quản trị, kẻ tấn công đã cố tải xuống một tệp. URL được xác định để tải tệp là <http://87.96.21.84/checking.ps1>.  


Xuất ra các file đã sử dụng trong giao tiếp giữa 2 IP: File > Export Objects > Chọn folder > Save All.

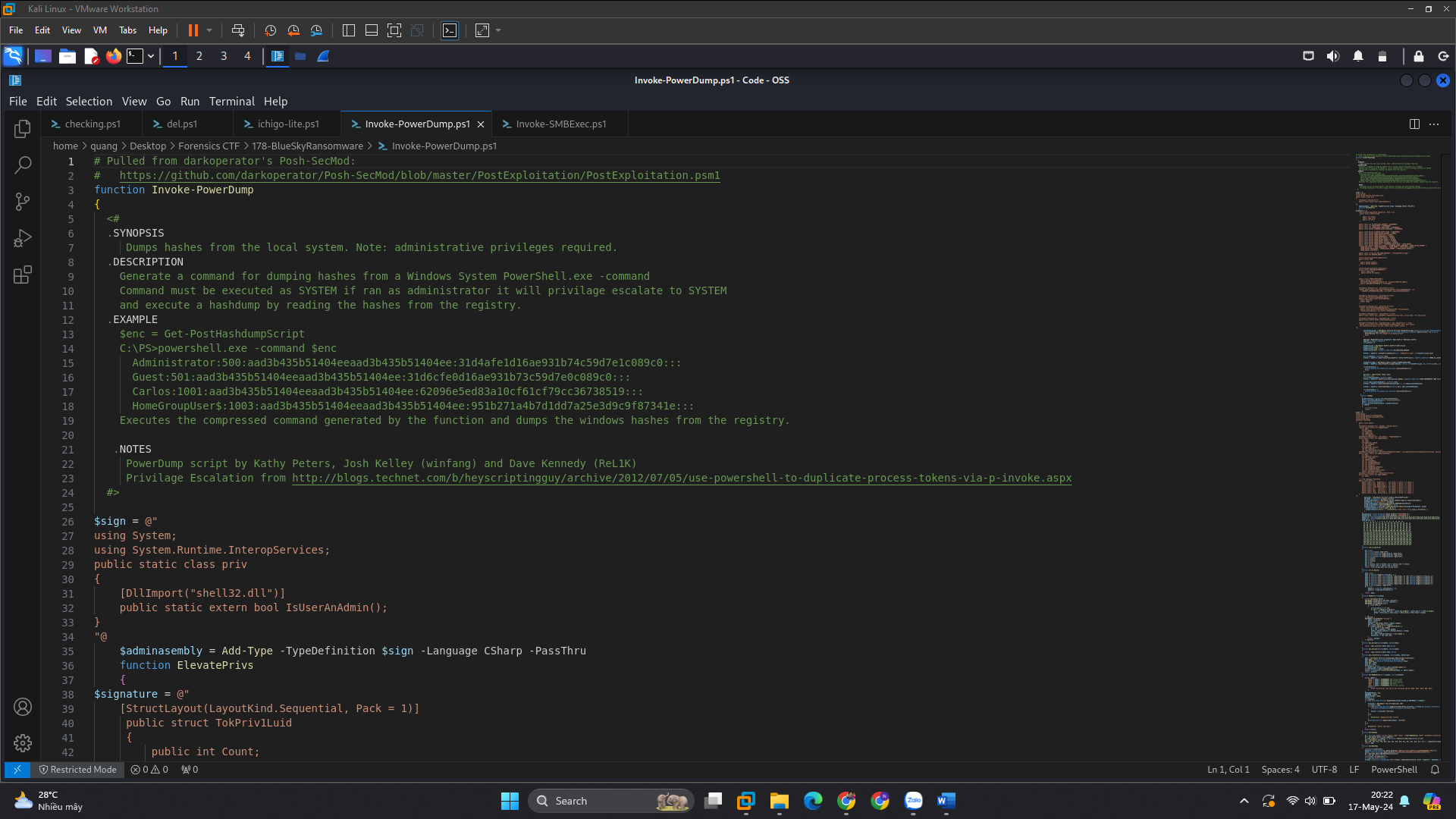
Q7. Việc hiểu Tập lệnh độc hại (SID) thuộc nhóm nào sẽ kiểm tra để xác minh các đặc quyền của người dùng hiện tại có thể cung cấp thông tin chi tiết về ý định của kẻ tấn công. SID cụ thể trong trường hợp này là S-1-5-32-544.  


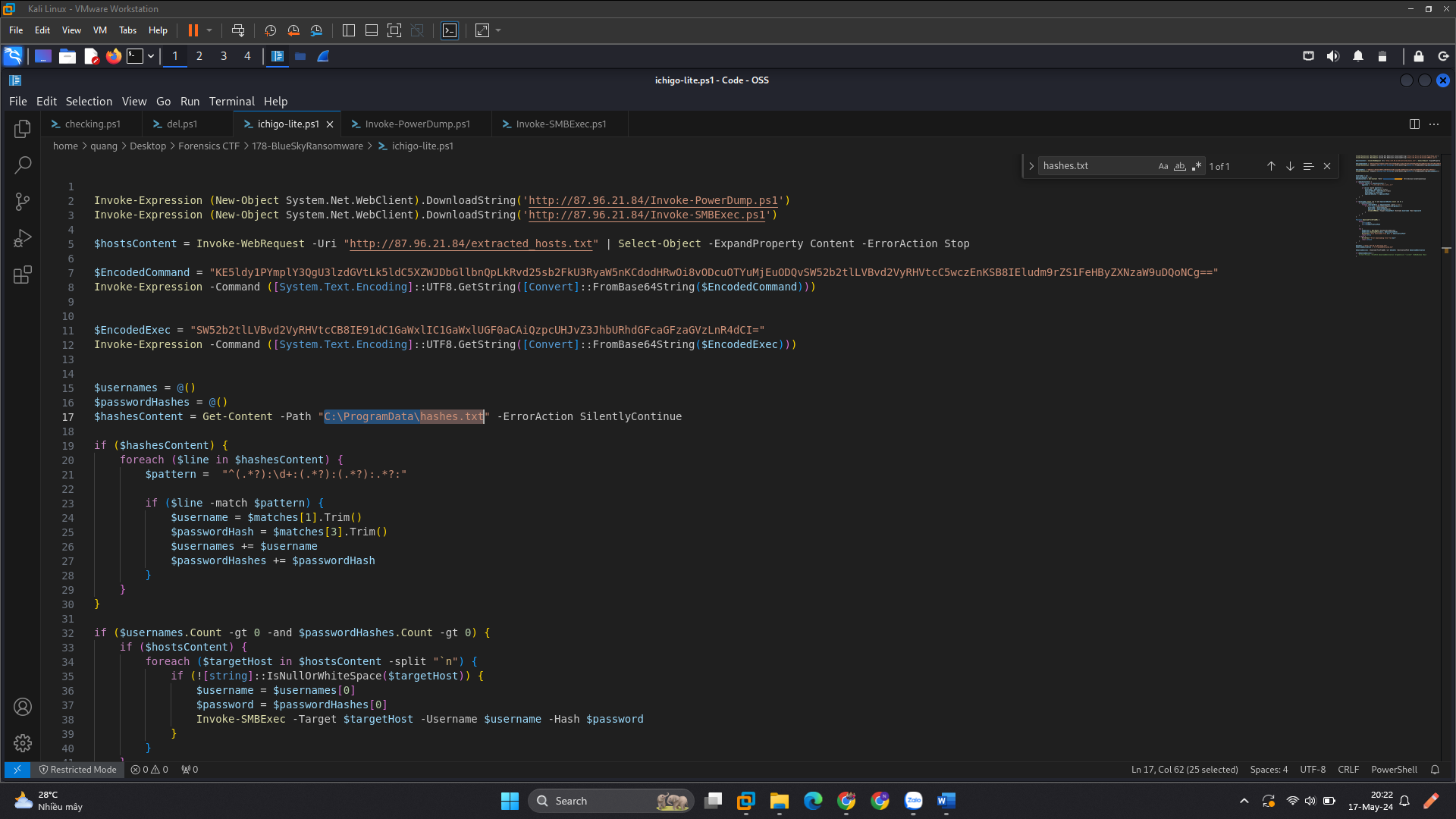
Q8. Windows Security đóng vai trò quan trọng trong việc bảo vệ chống lại các mối đe dọa trên mạng. Nếu kẻ tấn công vô hiệu hóa nó, hệ thống sẽ trở nên dễ bị tấn công hơn. Kẻ tấn công sử dụng và thực thi các lệnh regedit vô hiệu hóa các chức năng của Windows Security.  
DisableAntiSpyware,DisableRoutinelyTakingAction,DisableRealtimeMonitoring,SubmitSamplesConsent,SpynetReporting  


Q9. URL của tệp thứ hai được kẻ tấn công tải xuống máy nạn nhân là http://87.96.21.84/del.ps1.  


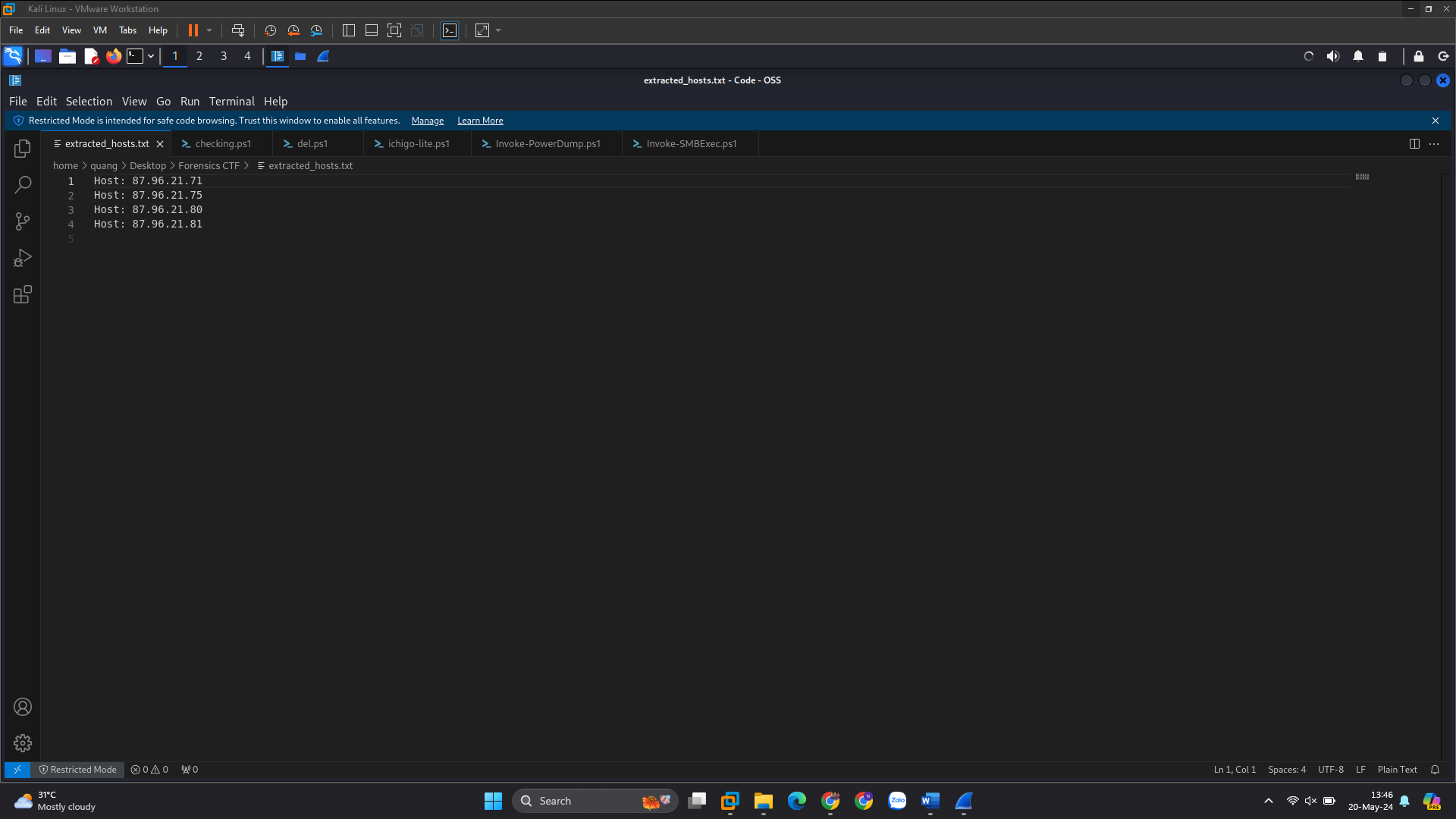
Q10. Việc xác định các tác vụ độc hại và hiểu cách chúng được sử dụng để duy trì liên tục sẽ giúp củng cố khả năng phòng thủ trước các cuộc tấn công trong tương lai. Tên đầy đủ của nhiệm vụ do kẻ tấn công tạo ra để duy trì tấn công là \Microsoft\Windows\MUI\LPupdate.  


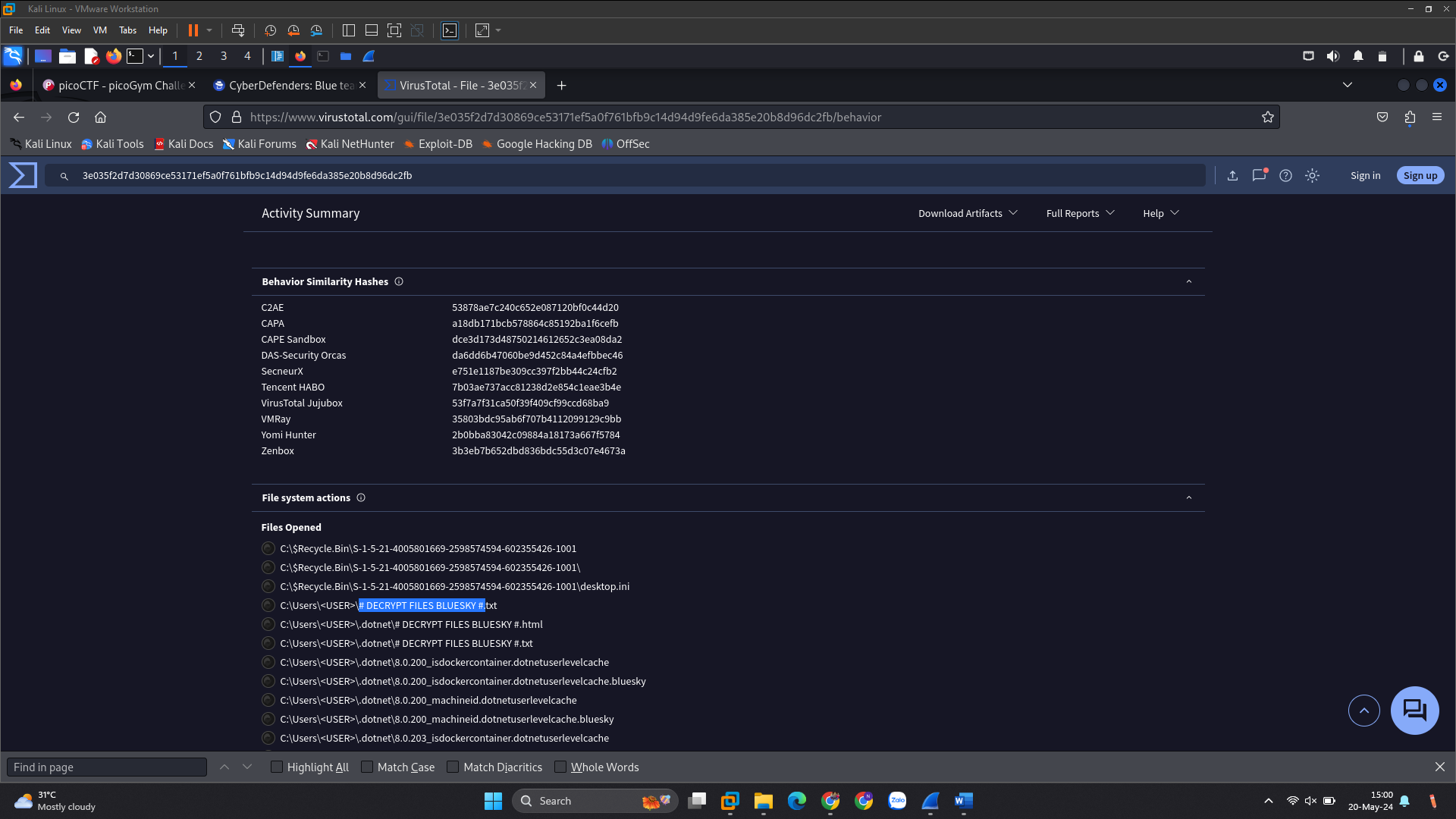
Q11. Theo phân tích về tệp del.ps1, MITRE ID mà nó hướng tới là TA0005. Các kỹ thuật được dùng trong tệp bao gồm vô hiệu hóa phần mềm bảo mật và ẩn giấu trong quy trình đáng tin cậy.

Q12. Tập lệnh PowerShell được gọi mà kẻ tấn công sử dụng để lấy cắp thông tin đăng nhập là Invoke-PowerDump.ps1.  


Q13. Hiểu được thông tin xác thực nào đã bị truy cập là điều cần thiết để đánh giá mức độ vi phạm dữ liệu. Tên của tệp văn bản đã lưu chứa thông tin xác thực bị kết xuất là C:\ProgramData\hashes.txt.  


Q14. Biết được các máy được nhắm mục tiêu trong giai đoạn trinh sát của kẻ tấn công, nhóm bảo mật có thể ưu tiên các nỗ lực khắc phục trên các máy chủ cụ thể này. Tên của tệp văn bản chứa các địa chỉ IP có liên quan được phát hiện: extracted\_hosts.txt.



Q15. Kẻ tấn công đã cố gắng triển khai ransomware trên máy chủ bị xâm nhập, lây lan nó sang phần còn lại của mạng cục bộ và mã hóa dữ liệu bằng cách sử dụng SMB. Bằng cách thực hiện phân tích hành vi, tên của tệp ghi chú để đòi tiền chuộc với mục đích giải mã dữ liệu là # DECRYPT FILES BLUESKY #.  


Q16. Trong một số trường hợp, các công cụ giải mã có sẵn cho các dòng ransomware cụ thể. Việc xác định họ có thể dẫn đến một giải pháp giải mã tiềm năng. Tên của họ ransomware trong javaw.exe này là conti.  
