 **Scan SMB Port (445) từ nhiều địa chỉ IP**:

* Địa chỉ IP đơn lẻ hoặc một nhóm IP có nhiều yêu cầu kết nối đến nhiều IP đích qua port 445 trong thời gian ngắn. Đây là dấu hiệu của một đợt port scan để tìm máy có dịch vụ SMB mở.

 **Dos/DDoS thông qua SMB**:

* Một hoặc nhiều địa chỉ IP gửi lượng lớn gói tin đến một IP đích trên port 445 trong thời gian ngắn, dẫn đến tình trạng ngập lụt tài nguyên (flooding).
* Các kết nối từ nhiều IP đến cùng một dịch vụ SMB với tần suất cao và kéo dài có thể là hành vi tấn công DoS hoặc DDoS.

 **Brute Force hoặc Dictionary Attack qua SMB**:

* Nhiều yêu cầu đăng nhập không thành công vào dịch vụ SMB từ một IP đến một hoặc nhiều IP đích trong thời gian ngắn. Hành vi này cho thấy có thể đang cố gắng brute force tài khoản.
* Cần chú ý số lượng và tần suất các yêu cầu xác thực SMB thất bại, từ đó có thể cảnh báo nếu vượt ngưỡng cho phép.

 **Tạo nhiều kết nối đồng thời qua SMB**:

* Nhiều kết nối đồng thời từ một IP đến nhiều máy đích qua port 445 có thể là dấu hiệu của việc lây nhiễm malware hoặc ransomware qua SMB.
* Các hành vi sao chép hoặc sửa đổi file qua SMB trên nhiều thiết bị cũng là dấu hiệu đáng lưu ý cho các hành vi lây nhiễm.
* **Sử dụng SMBv1 một phiên bản cũ không an toàn và dễ bị khai thác**
* Thiết kế ban đầu, không có cơ chế mã hóa dữ liệu hoặc bảo vệ các gói tin. Các kết nối không được mã hóa và không an toàn.
* **CVE-2020-0796 (SMBGhost):**

Là một lỗ hổng nghiêm trọng trong giao thức SMBv3. Lỗ hổng này cho phép thực hiện mã từ xa (Remote Code Execution). Lỗ hổng này liên quan đến việc xử lý dữ liệu nén không đúng cách trong giao thức SMBv3. Khi SMBv3 nhận một yêu cầu chứa dữ liệu nén lớn, nếu kích thước của dữ liệu nén không khớp với kích thước dữ liệu thực tế, điều này có thể dẫn đến lỗi xử lý bộ nhớ.

* Dấu hiệu:

Gói tin yêu cầu SMB kích thước lớn

Lỗi nén dữ liệu

Phiên làm việc SMB bị ngắt đột ngột

* Ví dụ về Rule:

if event\_type="SMBv3" and (message\_size > 16384 or (decompressed\_data\_size != actual\_data\_size))

* **CVE-2017-0144 và CVE-2017-0145 (EternalBlue và EternalRomance):**

Cả 2 đều khai thác lỗ hổng qua SMBv1 và gửi các gói tin SMB có thiết kế đặc biệt cho phép kẻ tấn công thực thi mã từ xa mà không cần xác thực

* Dấu hiệu:

Lưu lượng SMB không mã hoá trên cổng 445

Gói tin Trans2 kích thước lớn, cờ không hợp lệ

Kết nối SMB mà không cần xác thực

* Ví dụ về Rule:

if event\_type="SMBv1" and src\_port=445 and (message\_type="Trans2" and message\_size > 4096)