NETWORK FORENSICS

Trình bày: Nguyễn Xuân Việt – FPT CIO

NỘI DUNG CHÍNH

01 Khái niệm của Điều tra mạng (Network Forensics)

02 Các bước điều tra mạng

03 Điều tra mạng tại vùng mạng nội bộ

04 Điều tra mạng tại vùng mạng VPN

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

Điều tra mạng (Network forensics)

- Là một nhánh của khoa học điều tra số liên quan đến việc giám sát và phân tích lưu lượng mạng máy tính nhằm phục vụ cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các xâm nhập vào hệ thống máy tính này.

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

- **Điều tra mạng** có thể được thực hiện như một cuộc điều tra độc lập hoặc kết hợp với việc điều tra máy tính (Computer Forensics) – thường được sử dụng để phát hiện mối liên kết giữa các thiết bị kỹ thuật số hay tái tạo lại quy trình phạm tội.

- **Điều tra mạng** bao gồm việc chặn bắt, ghi âm và phân tích các sự kiện mạng để khám phá nguồn gốc của các cuộc tấn công hoặc sự cố của một vấn đề nào đó. Không giống các loại hình điều tra số khác, điều tra mạng xử lý những thông tin dễ thay đổi và biến động. Lưu lượng mạng được truyền đi và không được lưu lại, do đó việc điều tra mạng thường phải rất linh hoạt, chủ động.

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

Các bước điều tra mạng:

Tại bước 3 sau khi đã phát hiện được các sự kiện bất thường có thể gây hậu quả nghiêm trọng cho hệ thống, tổ chức có thể thực hiện ngay bước 7 để có thể xử lý sự cố ngay lập tức. Đồng thời thực hiện các bước còn lại song song.

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

Các bước điều tra mạng:

01
Xác định nguồn lây

Xác định nguồn tấn công có ảnh hưởng rất lớn đến các bước tiếp theo.

Nhận biết và xác định sự cố dựa trên các thông số trên mạng như địa chỉ IP, địa chỉ MAC...

02
Thu thập các sự kiện

Lấy toàn bộ các Log liên quan đến network, các log từ các hệ thống như firewall, IDS/IPS, hệ thống VPN, hệ thống netflow… trong khoảng thời gian tổ chức bị tấn công mạng.

03
Dò tìm

Thực hiện việc dò tìm và xác định các sự kiện bất thường trong phần Log đã thu thập được từ bước 2

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

04 Cách ly và duy trì

Duy trì hoạt động của hệ thống mạng, đồng thời đảm bảo cách ly các dữ liệu của tổ chức không bị tấn công cũng như lưu trữ lại các bằng chứng số phục vụ việc điều tra

05 Kiểm tra và Phân tích

Dựa vào các bằng chứng số và các dữ liệu log thu thập được, tổng hợp và phân tích các sự kiện này bằng các công cụ quản lý sự kiện và thông tin bảo mật (SIEM)

06 Kết luận

Dựa trên quá trình phân tích điều tra viên đưa ra kết luận về cuộc tấn công mạng trong tổ chức

07 Ứng phó xử lý sự cố

Tổ chức thực hiện các biện pháp cần thiết để xử lý sự cố

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

Ví dụ cụ thể tại **Vùng mạng nội bộ**:

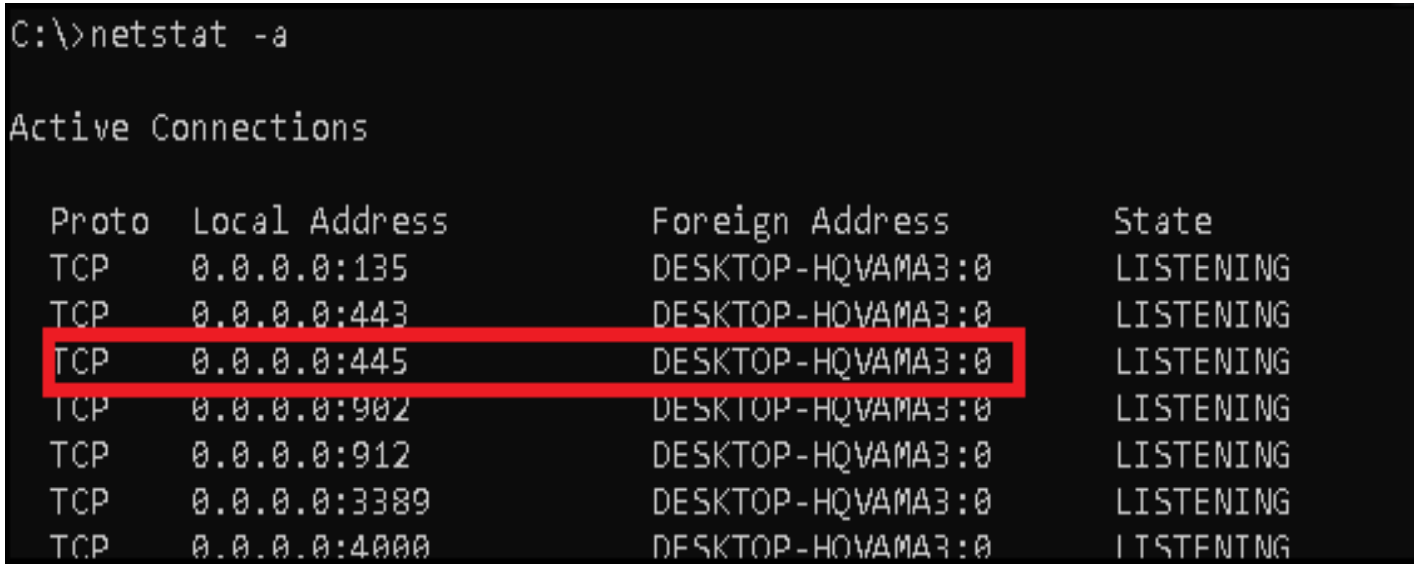
1 máy tính của người dùng hoặc 1 server nằm trong mạng nội bộ của tổ chức bị nhiễm mã độc và được điều khiển bởi attacker, từ máy tính hoặc server này attacker lấy làm bàn đạp để tấn công các hệ thống khác trong mạng nội bộ gây ra các ảnh hưởng nghiêm trọng cho tổ chức

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

Sau đây là cách thức lấy thông tin tại các vùng mạng trọng yếu hay bị attacker khai thác:

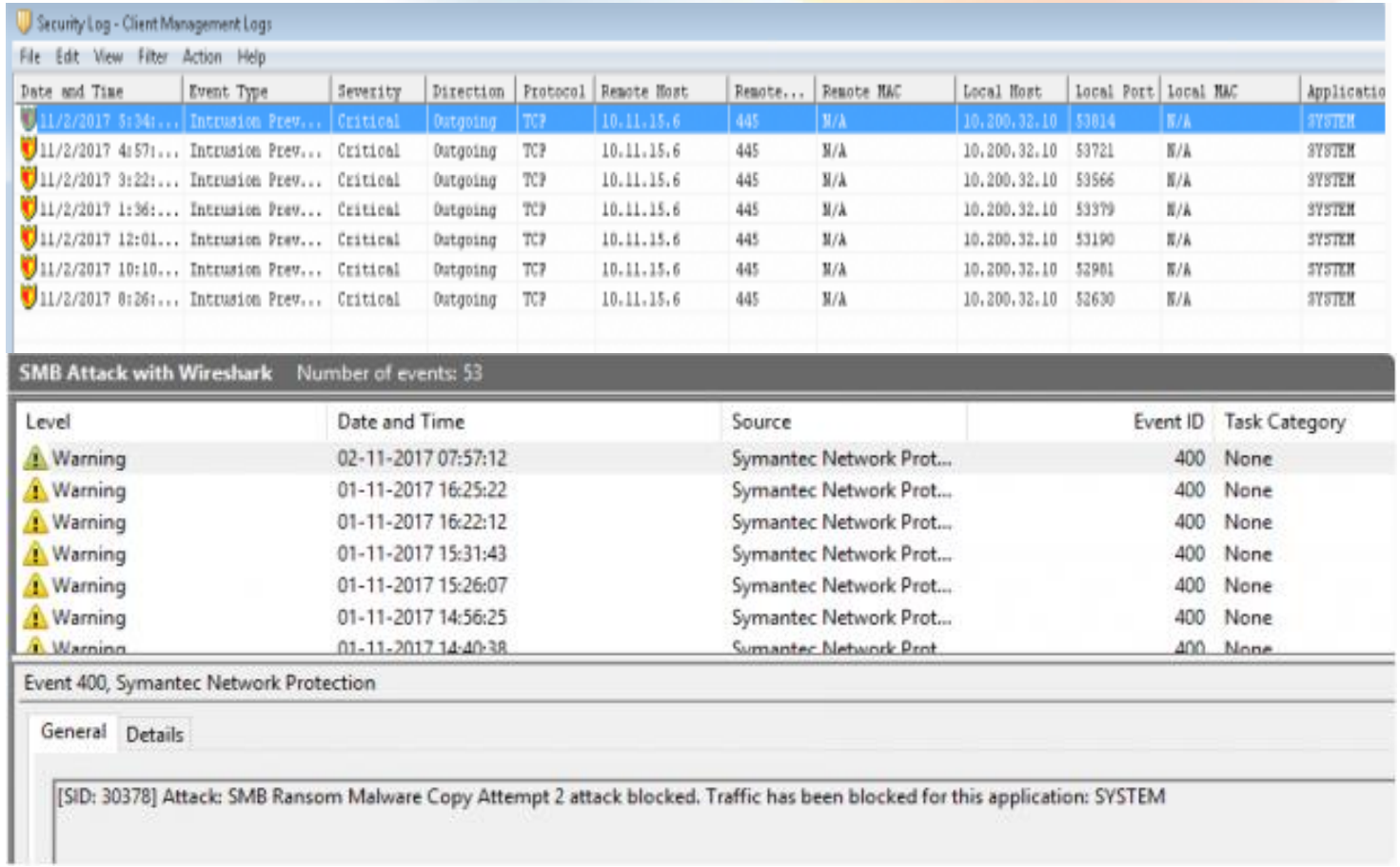
Cách 1: Kiểm tra log kết nối đến server bị tấn công, trên chính server bị tấn công ta có thể sử dụng câu lệnh trên cửa sổ cmd như sau “netstat -a”

Ở đây, server đang bị máy tính tên DESKTOP-HQVAMA3:0 quét port dịch vụ và tấn công SMB thông qua port 445 để lấy cắp, mã hóa các dữ liệu quan trọng của tổ chức.



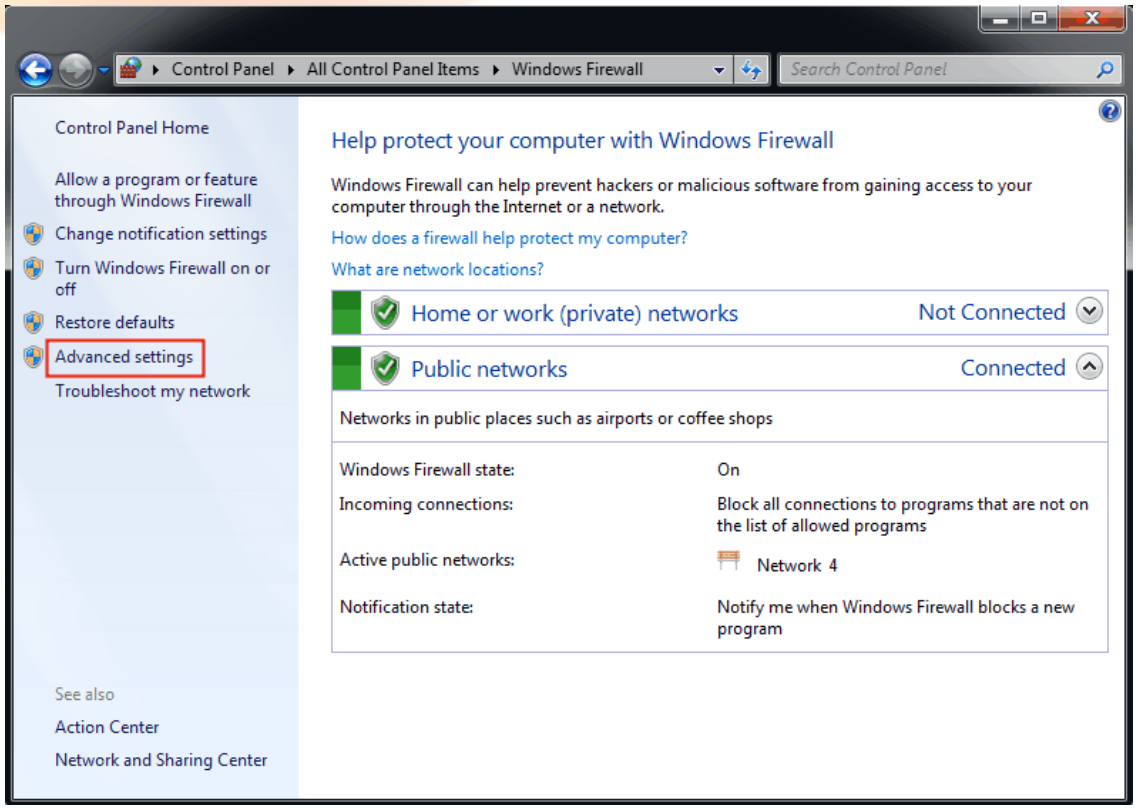
ĐIỀU TRA MẠNG (NETWORK FORENSICS)

Có thể kiểm tra Log trên Event Viewer Log của server



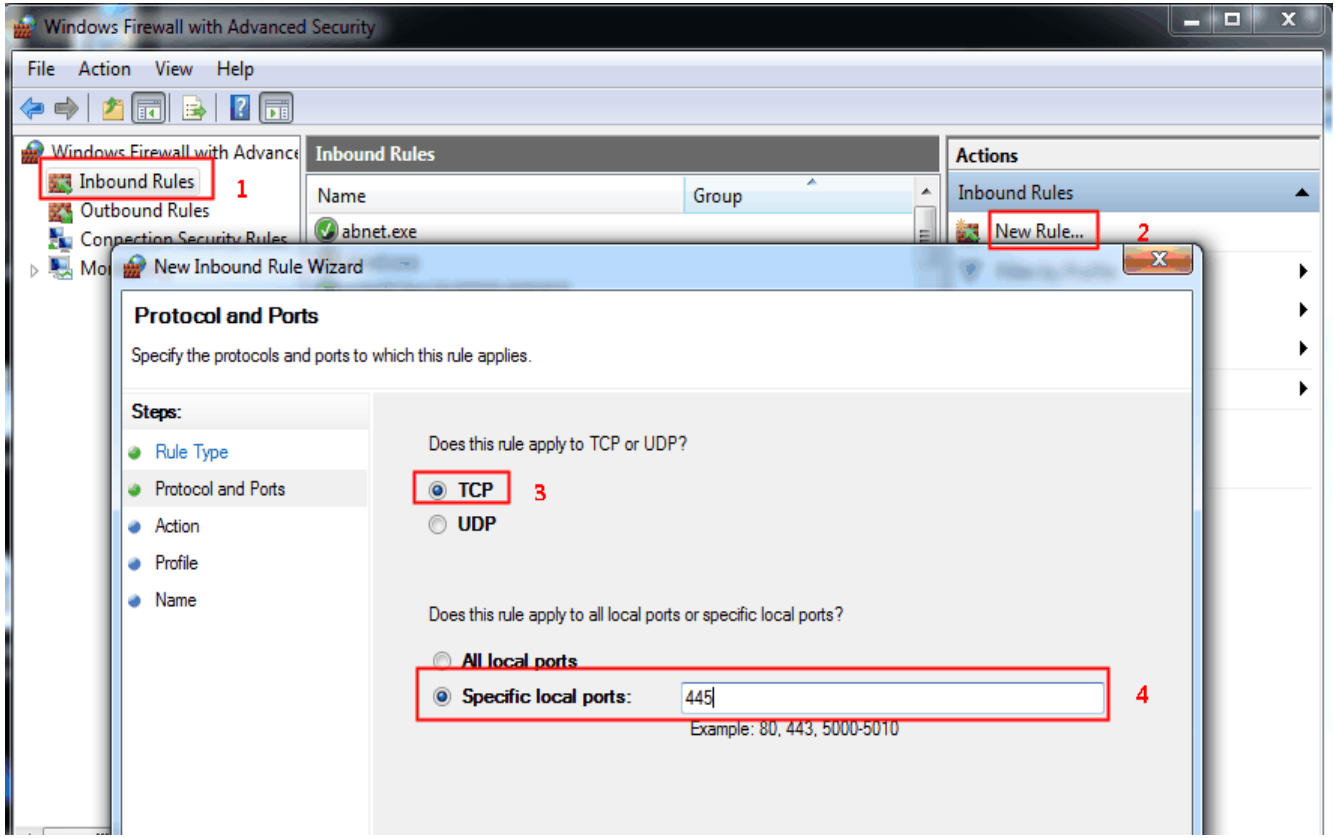
ĐIỀU TRA MẠNG (NETWORK FORENSICS)

- Sau khi phát hiện ra máy tính trong mạng nội bộ tấn công vào máy chủ, ta block máy tính này thông qua hệ thống firewall hoặc chặn trên firewall local của máy chủ như sau:
- **Start > Control Panel > Windows Firewall > Advanced settings**

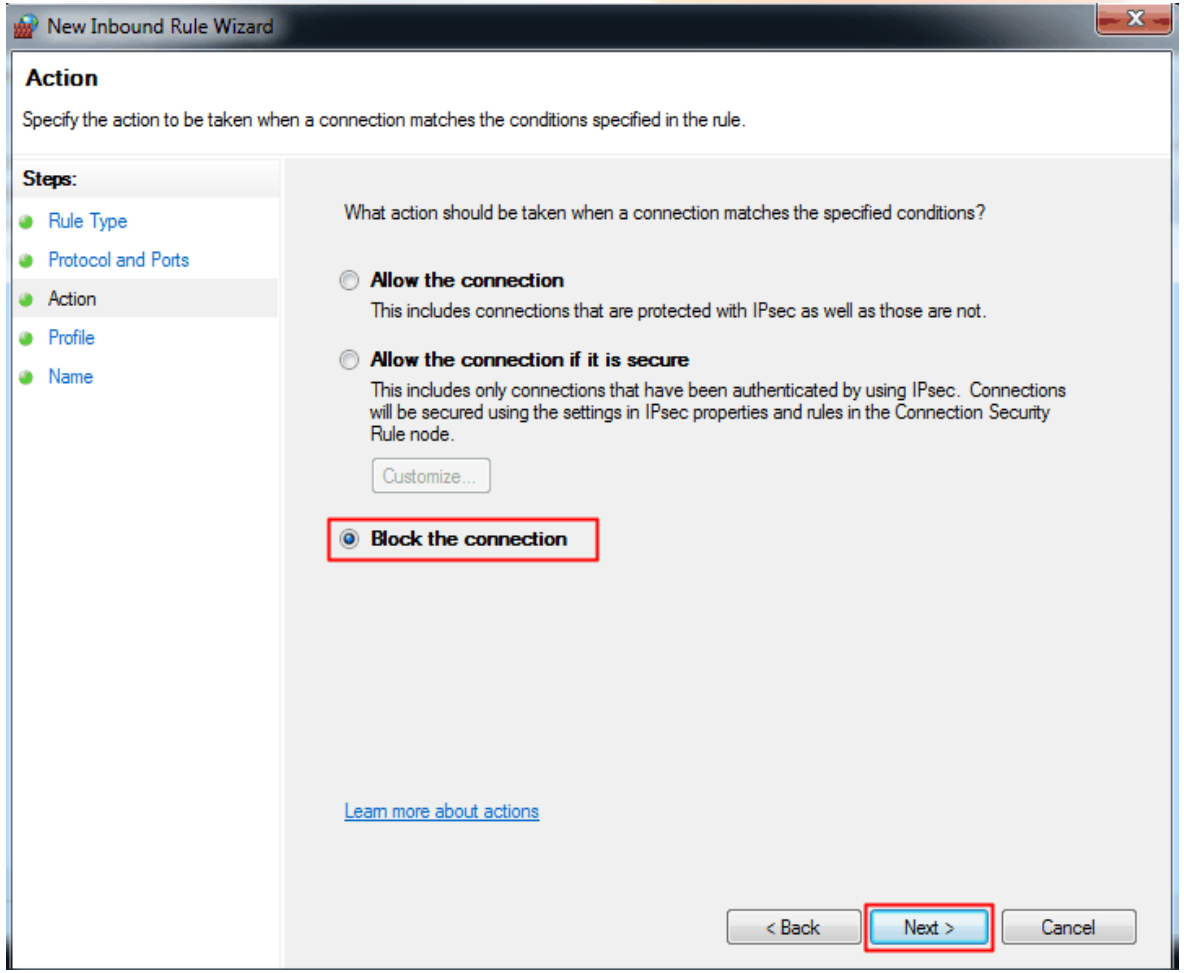


ĐIỀU TRA MẠNG (NETWORK FORENSICS)

- **Inbound Rules > New rule**. **Port > Next >TCP > Specific local ports** and type **445** and go **Next.**

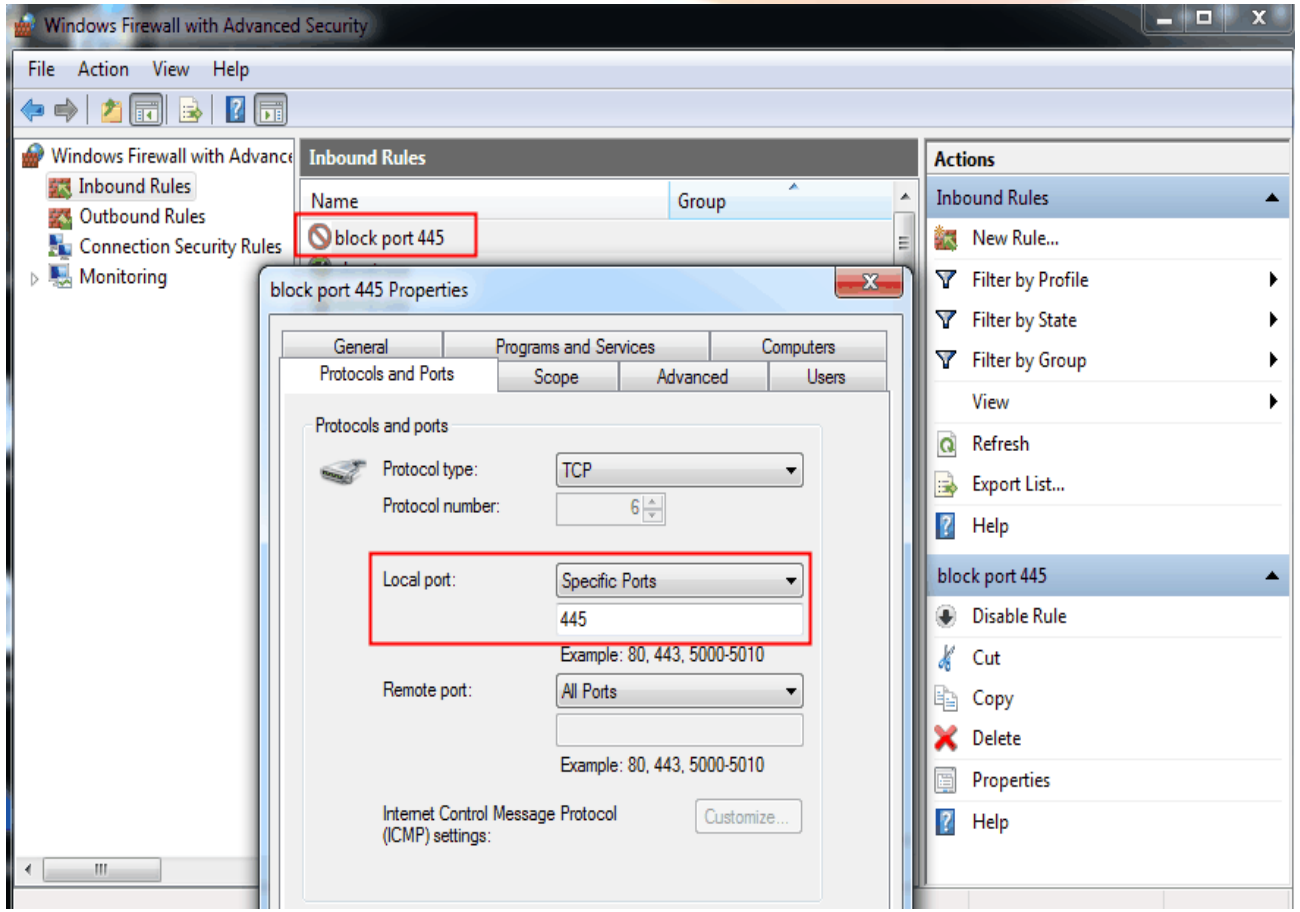


- **Block the connection > Next** >Finish.



ĐIỀU TRA MẠNG (NETWORK FORENSICS)

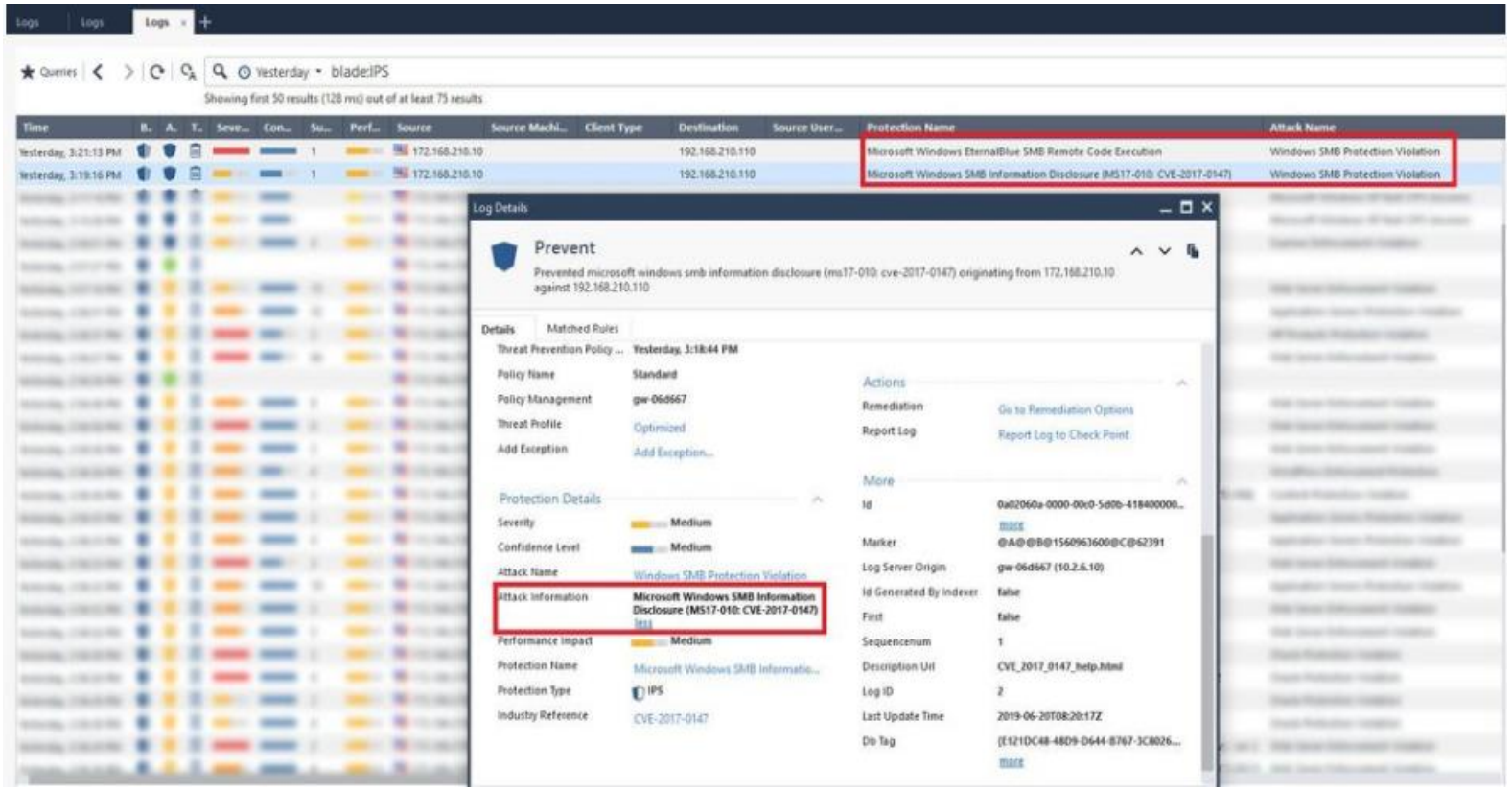
- **Properties > Protocols and Ports > Local Port**



ĐIỀU TRA MẠNG (NETWORK FORENSICS)

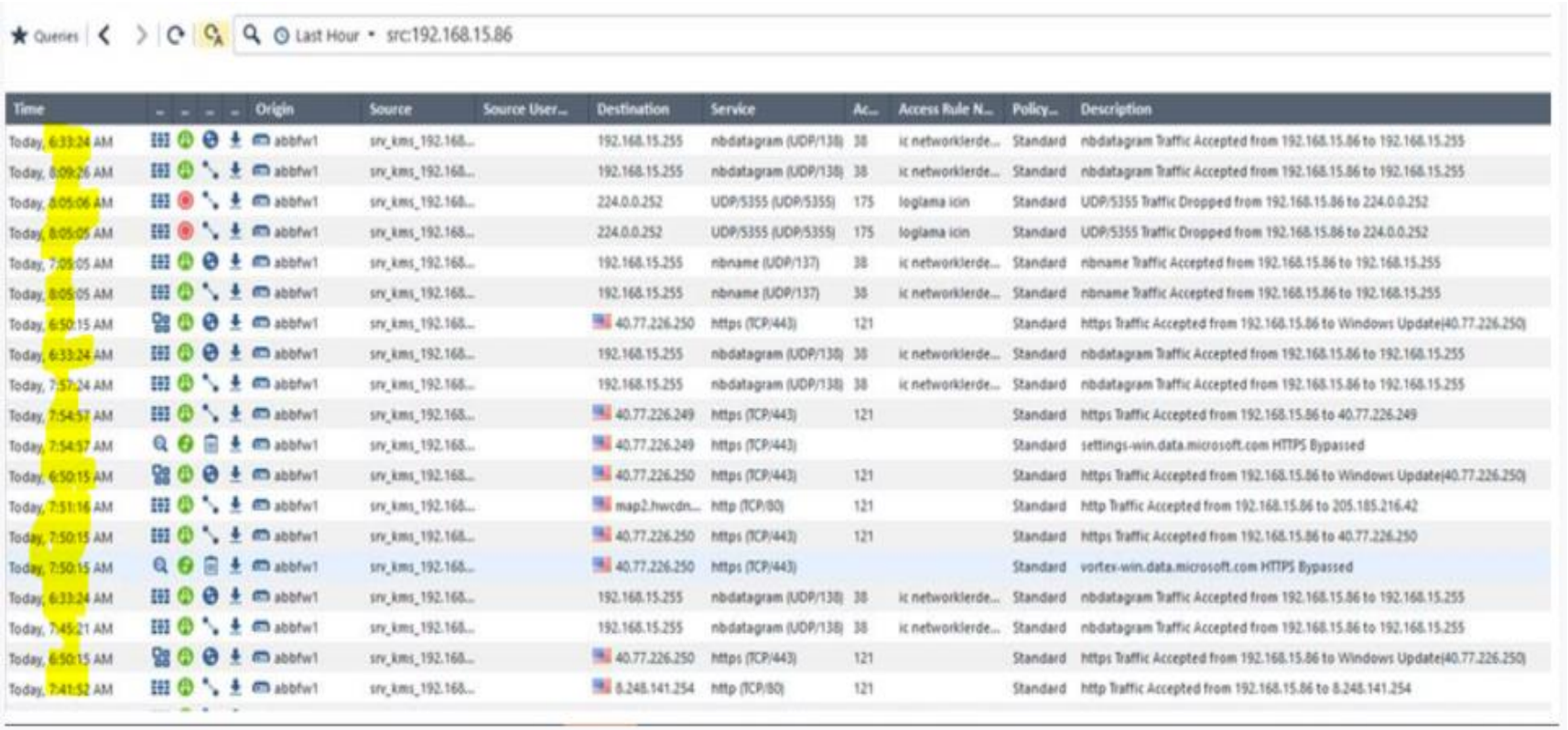
- **Cách 2: Kiểm tra log trên hệ thống IDS/IPS,** trong trường hợp người quản trị mạng không có quyền truy cập vào server bị tấn công để kiểm tra.

Tại dây ta có thể thấy máy chủ trong mạng đang bị tấn công qua giao thức SMB từ máy tính có IP 172.168.210.10 được hệ thống IPS phát hiện ra và ngăn chặn kịp thời.



ĐIỀU TRA MẠNG (NETWORK FORENSICS)

- **Cách 3: Kiểm tra log trên hệ thống Firewall**, ta có thể xác định các gói tin truyền qua mạng đến server bị tấn công và đưa ra cách thực xử lý.



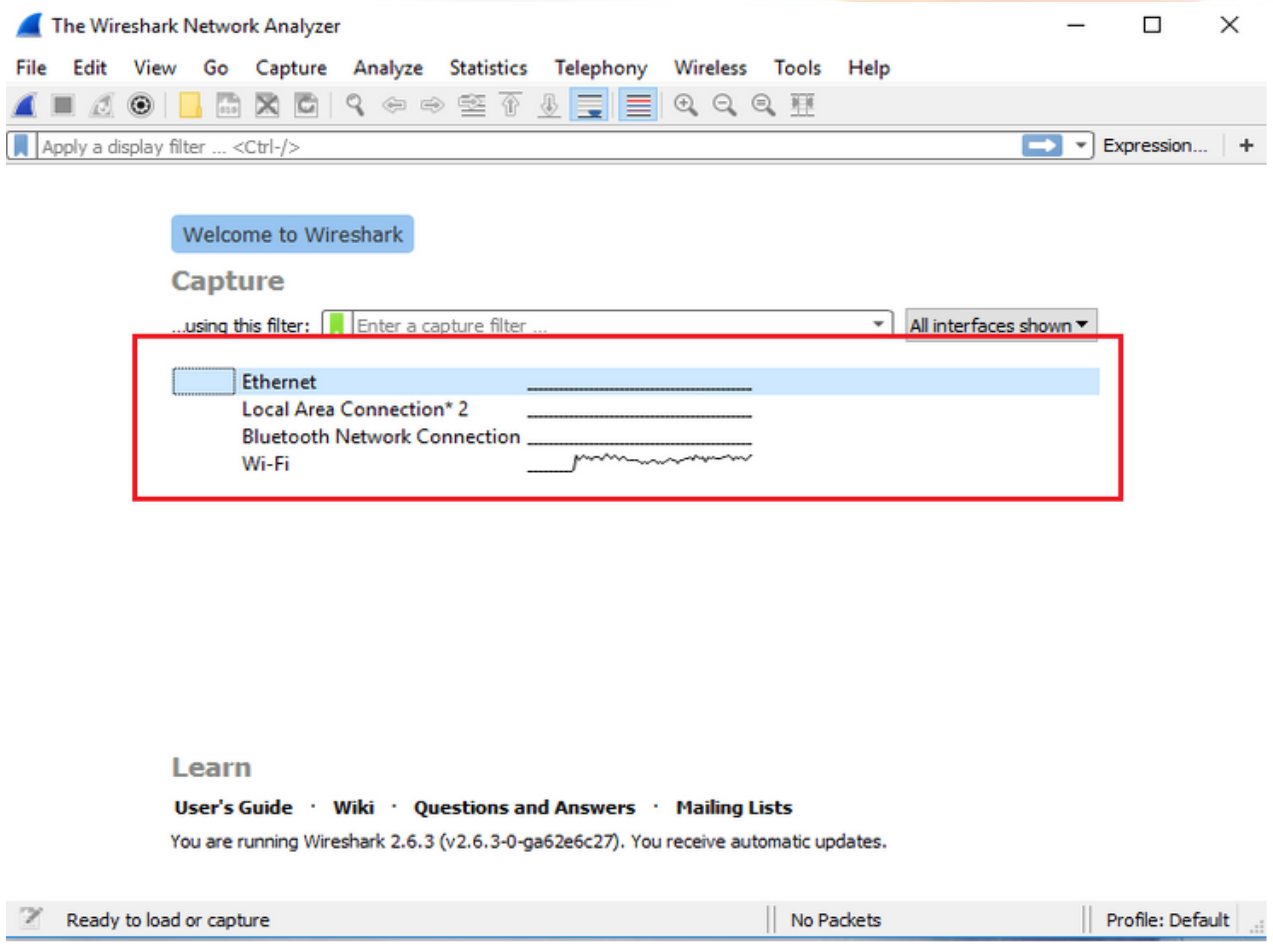
Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 6:33:24 AM	abbfw1	srv_kms_192.168...		192.168.15.255	nbdatagram (UDP/138)	38	ic networklerde...	Standard	nbdatagram Traffic Accepted from 192.168.15.86 to 192.168.15.255
Today, 8:09:26 AM	abbfw1	srv_kms_192.168...		192.168.15.255	nbdatagram (UDP/138)	38	ic networklerde...	Standard	nbdatagram Traffic Accepted from 192.168.15.86 to 192.168.15.255
Today, 8:05:06 AM	abbfw1	srv_kms_192.168...		224.0.0.252	UDP/5355 (UDP/5355)	175	loglama icin	Standard	UDP/5355 Traffic Dropped from 192.168.15.86 to 224.0.0.252
Today, 8:05:05 AM	abbfw1	srv_kms_192.168...		224.0.0.252	UDP/5355 (UDP/5355)	175	loglama icin	Standard	UDP/5355 Traffic Dropped from 192.168.15.86 to 224.0.0.252
Today, 7:05:05 AM	abbfw1	srv_kms_192.168...		192.168.15.255	nbname (UDP/137)	38	ic networklerde...	Standard	nbname Traffic Accepted from 192.168.15.86 to 192.168.15.255
Today, 8:05:05 AM	abbfw1	srv_kms_192.168...		192.168.15.255	nbname (UDP/137)	38	ic networklerde...	Standard	nbname Traffic Accepted from 192.168.15.86 to 192.168.15.255
Today, 6:50:15 AM	abbfw1	srv_kms_192.168...		40.77.226.250	https (TCP/443)	121		Standard	https Traffic Accepted from 192.168.15.86 to Windows Update(40.77.226.250)
Today, 6:33:24 AM	abbfw1	srv_kms_192.168...		192.168.15.255	nbdatagram (UDP/138)	38	ic networklerde...	Standard	nbdatagram Traffic Accepted from 192.168.15.86 to 192.168.15.255
Today, 7:57:24 AM	abbfw1	srv_kms_192.168...		192.168.15.255	nbdatagram (UDP/138)	38	ic networklerde...	Standard	nbdatagram Traffic Accepted from 192.168.15.86 to 192.168.15.255
Today, 7:54:57 AM	abbfw1	srv_kms_192.168...		40.77.226.249	https (TCP/443)	121		Standard	https Traffic Accepted from 192.168.15.86 to 40.77.226.249
Today, 7:54:57 AM	abbfw1	srv_kms_192.168...		40.77.226.249	https (TCP/443)			Standard	settings-win.data.microsoft.com HTTPS Bypassed
Today, 6:50:15 AM	abbfw1	srv_kms_192.168...		40.77.226.250	https (TCP/443)	121		Standard	https Traffic Accepted from 192.168.15.86 to Windows Update(40.77.226.250)
Today, 7:51:16 AM	abbfw1	srv_kms_192.168...		map2.hwcdn...	http (TCP/80)	121		Standard	http Traffic Accepted from 192.168.15.86 to 205.185.216.42
Today, 7:50:15 AM	abbfw1	srv_kms_192.168...		40.77.226.250	https (TCP/443)	121		Standard	https Traffic Accepted from 192.168.15.86 to 40.77.226.250
Today, 7:50:15 AM	abbfw1	srv_kms_192.168...		40.77.226.250	https (TCP/443)			Standard	vortex-win.data.microsoft.com HTTPS Bypassed
Today, 6:33:24 AM	abbfw1	srv_kms_192.168...		192.168.15.255	nbdatagram (UDP/138)	38	ic networklerde...	Standard	nbdatagram Traffic Accepted from 192.168.15.86 to 192.168.15.255
Today, 7:45:21 AM	abbfw1	srv_kms_192.168...		192.168.15.255	nbdatagram (UDP/138)	38	ic networklerde...	Standard	nbdatagram Traffic Accepted from 192.168.15.86 to 192.168.15.255
Today, 6:50:15 AM	abbfw1	srv_kms_192.168...		40.77.226.250	https (TCP/443)	121		Standard	https Traffic Accepted from 192.168.15.86 to Windows Update(40.77.226.250)
Today, 7:41:52 AM	abbfw1	srv_kms_192.168...		8.248.141.254	http (TCP/80)	121		Standard	http Traffic Accepted from 192.168.15.86 to 8.248.141.254

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

- **Cách 4:** Ta có thể bắt các gói tin thông qua mạng bằng cách **sử dụng phần mềm Wireshark** và tìm lọc các gói tin bất thường trong mạng, đây là 1 cách khó cần người quản trị có am hiểu về các giao thức mạng và cách thức tấn công của attacker

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

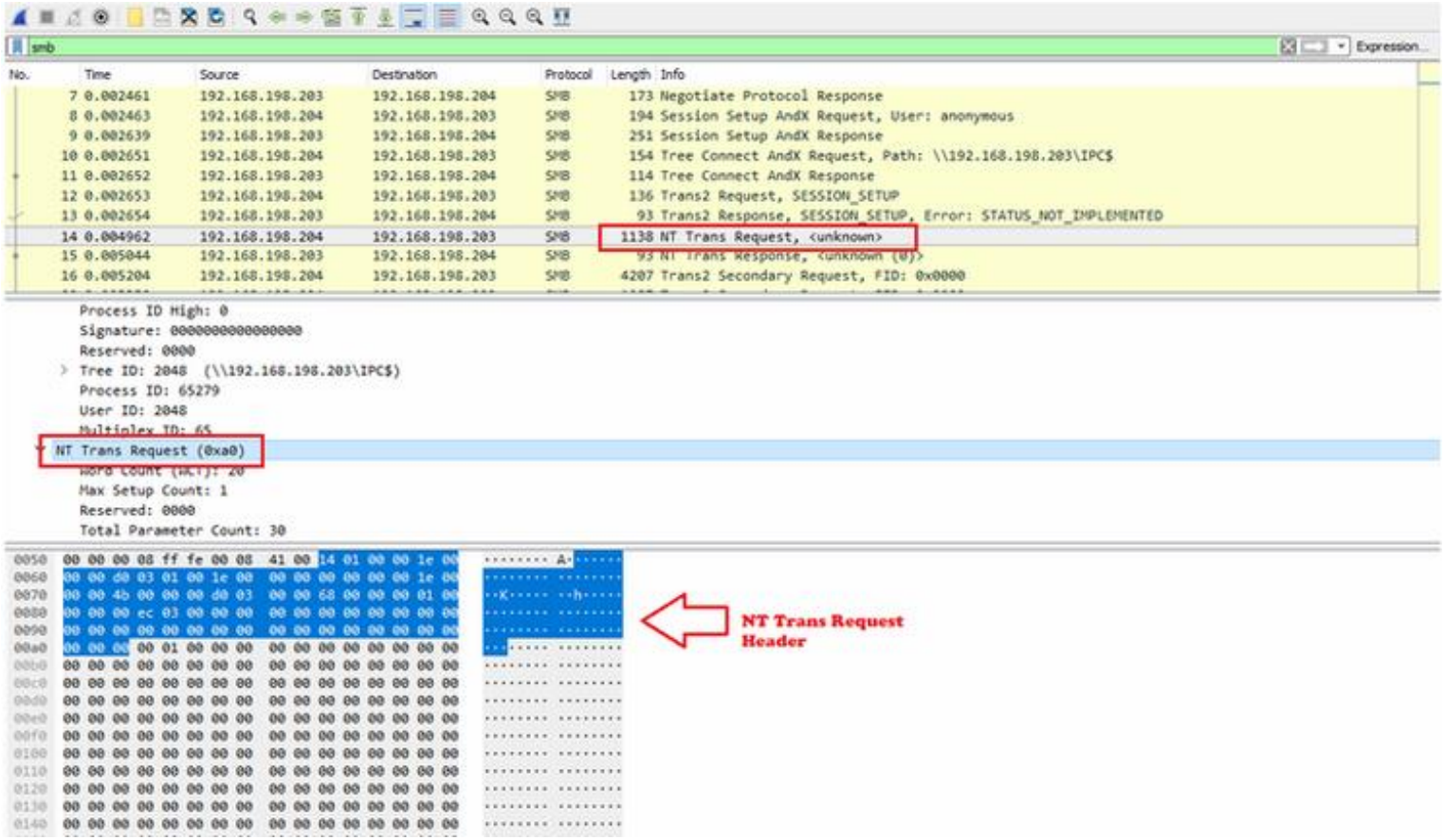
- Mở phần mềm Wireshark chọn card mạng cần theo dõi gói tin



ĐIỀU TRA MẠNG (NETWORK FORENSICS)

- Filter giao thức cần theo dõi, trong ví dụ cụ thể này ta cần theo dõi giao thức SMB

- Sau khi filter ta có thể xác định được máy tính tấn công đến máy chủ từ đó tiến hành quy trình xử lý và lưu thông tin các gói tin tấn công làm bằng chứng.



ĐIỀU TRA MẠNG (NETWORK FORENSICS)

Ví dụ tại **Vùng mạng VPN**:

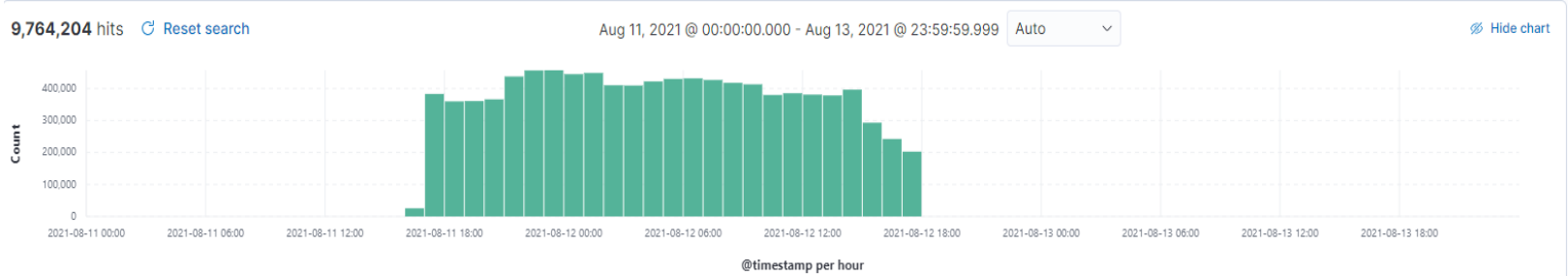
- Vùng mạng VPN là vùng mạng rất nhạy cảm khi mở kết nối từ bên ngoài có thể kết nối được đến các hệ thống nội bộ của tổ chức. Attacker lợi dụng việc này và tấn công vào mạng lấy cắp thông tin của chức hoặc gây ra các ảnh hưởng khác.

- 1 máy tính của người dùng được cấp quyền VPN bị nhiễm mã độc và bị điều khiển bởi attacker, máy tính này VPN vào mạng nội bộ và bắt đầu rà quét các ứng dụng, dịch vụ nội bộ để tìm đối tượng tấn công trong hệ thống.

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

- Ta có thể dựa vào Log trên hệ thống VPN để xác định máy tính này

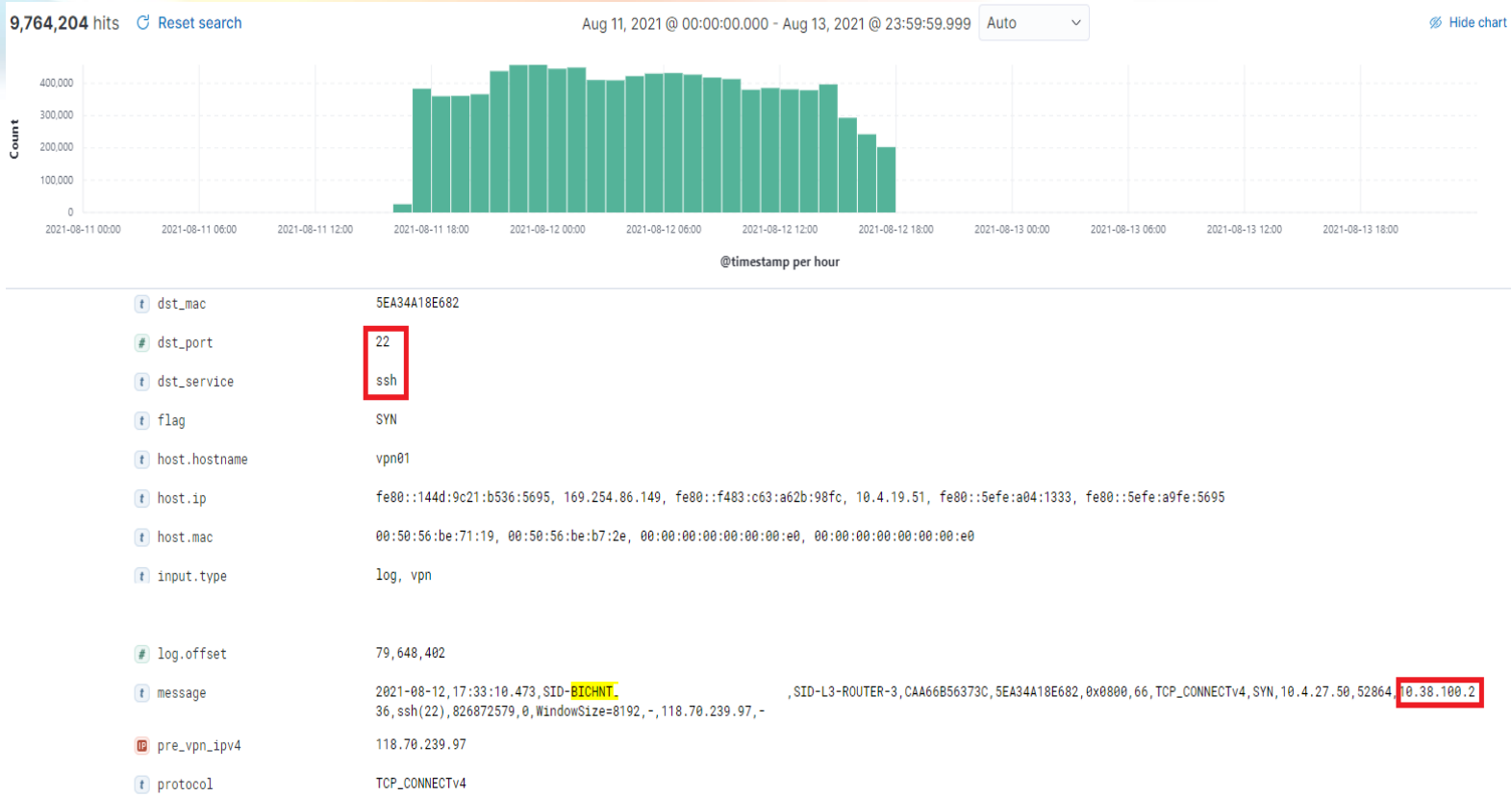
Ta có thể thấy máy tính VPN có ip 10.4.27.50 đang có hành vi dò quét các port dịch vụ trong dải mạng nội bộ



Time	src_ipv4	src_port	dst_ipv4	dst_port
Aug 12, 2021 @ 17:33:14.909	-	-	-	-
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	53,458	10.38.100.233	8,728
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	52,859	10.38.100.147	8,728
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	53,460	10.38.101.146	8,291
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	53,466	10.38.100.234	8,728
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	52,864	10.38.100.236	22
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	53,469	10.38.101.149	8,291
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	53,472	10.38.101.47	22
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	53,475	10.38.100.237	8,728
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	52,860	10.38.101.46	8,291
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	52,861	10.38.100.146	8,728
Aug 12, 2021 @ 17:33:11.262	10.4.27.50	53,470	10.38.100.236	8,728

ĐIỀU TRA MẠNG (NETWORK FORENSICS)

Phân tích sâu hơn trong từng mảnh log ta có thể thấy User có tên là BICHNT đang kết nối vào VPN và đang cố thử SSH và server 10.38.100.2.



Sau khi phân tích xong ta có thể lưu trữ lại đoạn log này làm bằng chứng đồng thời xử lý sự cố.

Thank You !