O MAIOR FESTIVAL HACKER DA AMERICA LATINA

ROADSEC 2022

黑客文化

ROADSEC

Windows logon: dos logs aos processos

Marcus Oliveira

Especialista de Cyber Segurança

Disclaimer

Essa palestra é um estudo pessoal e não tem relação com a empresa a qual trabalho.

O intuito é divulgar conhecimento, não me responsabilizando pelo o que terceiros possam fazer com ele.

$whoami

Marcus Oliveira
Especialista em Cyber Segurança

- Twitter: @Marcus_mcs
- E-mail: marcus.oliveira5@fatec.sp.gov.br
- Telegram: @mvvamo
- Linkedin: https://www.linkedin.com/in/mvmoliveira/
- Não sou o CR7
- Tricolor Fanático
- Pratico natação e musculação
- Purple Team mindset
- 8 anos de experiência em TI/SI
- Tecnólogo em Segurança da Informação pela Fatec São Caetano do Sul
- Focos de estudo e pesquisa:
    - Segurança Ofensiva (Red Team)
    - Segurança Defensiva (Blue Team)
    - Buffer Overflow

Agenda

O que é um logon?

O que é uma sessão?

Windows Authentication Architecture

Logs/eventos de logon

Processo de logon

Cenários

Referências

Dúvidas?

O que é um logon?

O que é um logon?

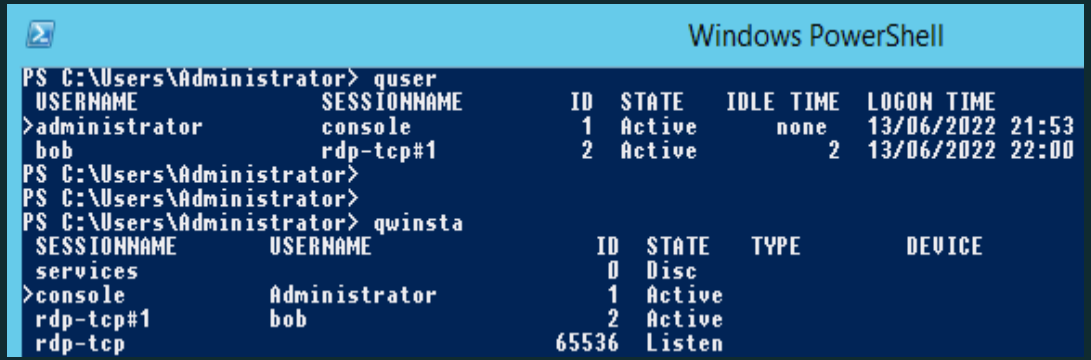
Segundo Chirag Savla, logon é:

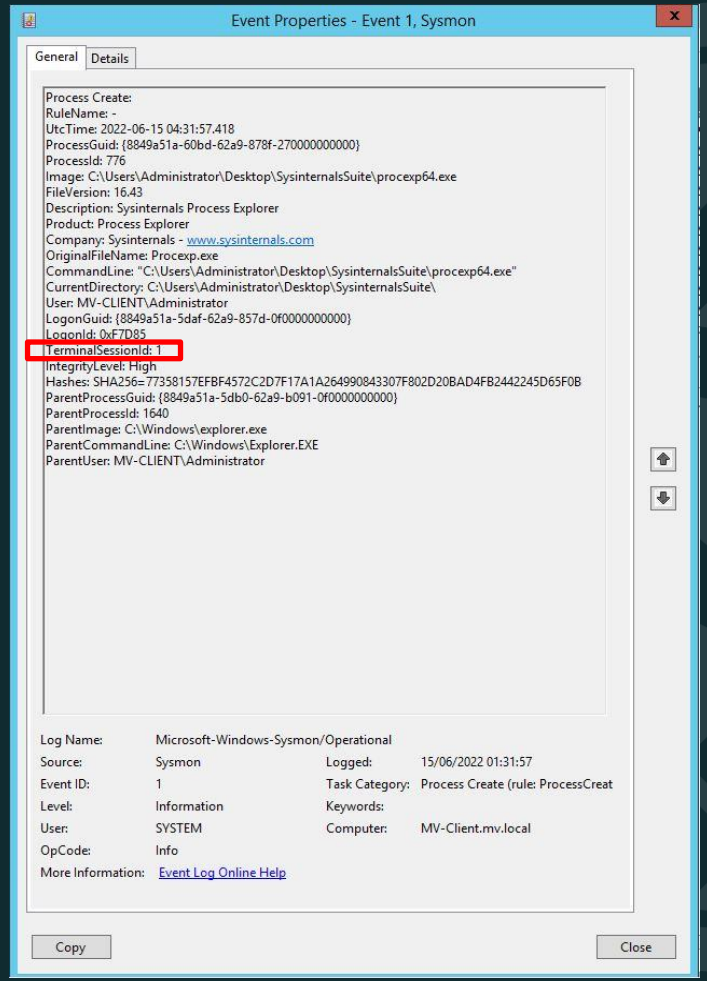
- “In simple words logon is a process of gaining access to local or remote systems using valid credentials. The user information is validated by Local Security Authority (LSA), incase of local account it will verify the information from Security Accounts Manager (SAM) database and incase of domain account it will verify the information from the Domain Controller.”

O que é uma sessão?

O que é uma sessão?

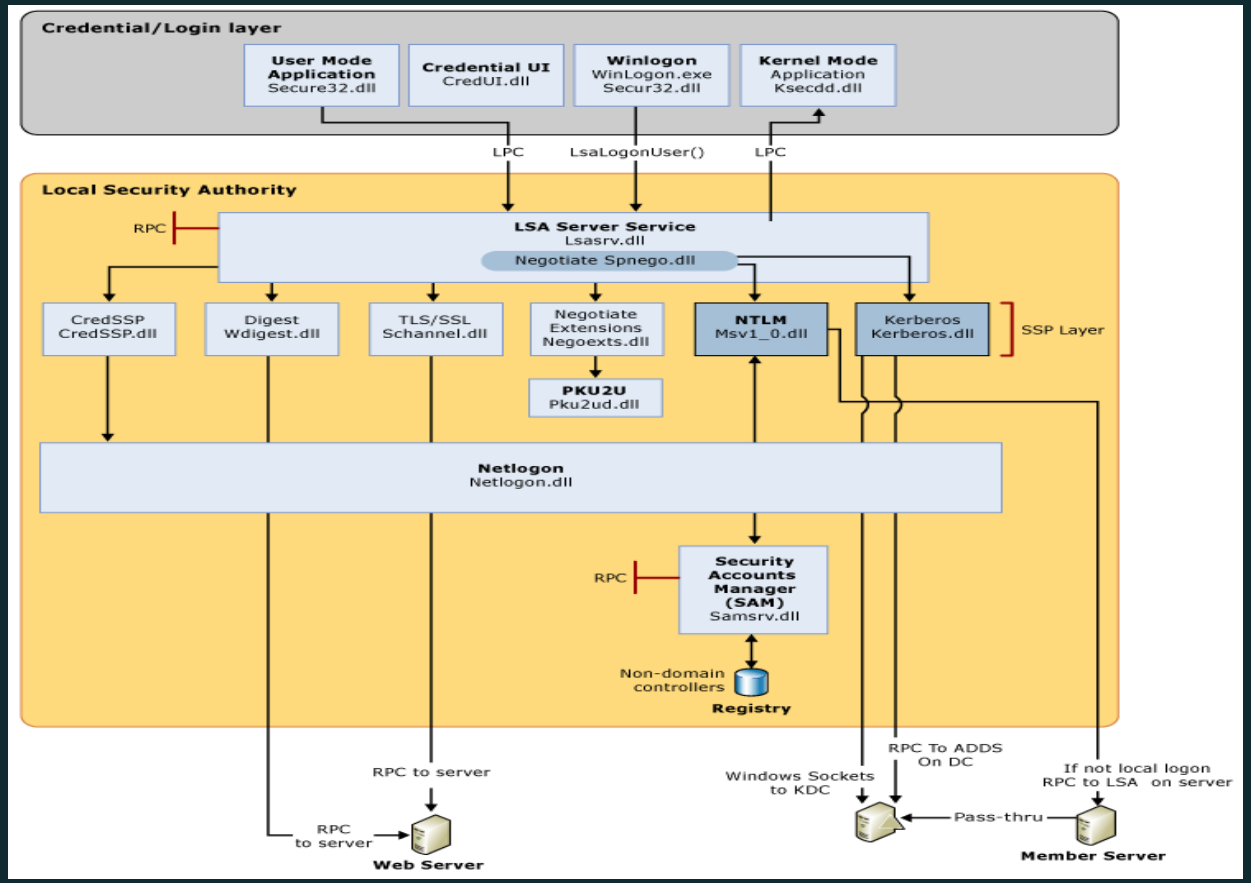
- Segundo Craig Marcho sessão é:
  - “A session consists of all of the processes and other system objects that represent a single user’s logon session.”
- Cada sessão recebe um número, sendo 0 sempre a do sistema operacional e cada logon de usuário vai recebendo n+1 como número de sessão.
- No Sysmon o campo TerminalSessionId no EventID 1, mostra a sessão do usuário que originou o processo.





Windows Authentication Architecture

Windows Authentication Architecture

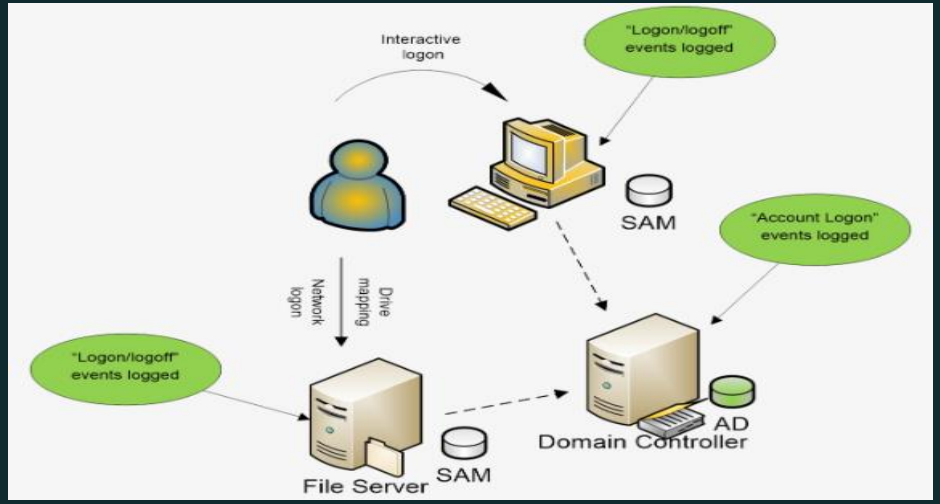


Account logon events VS Logon events

Account logon events VS Logon events

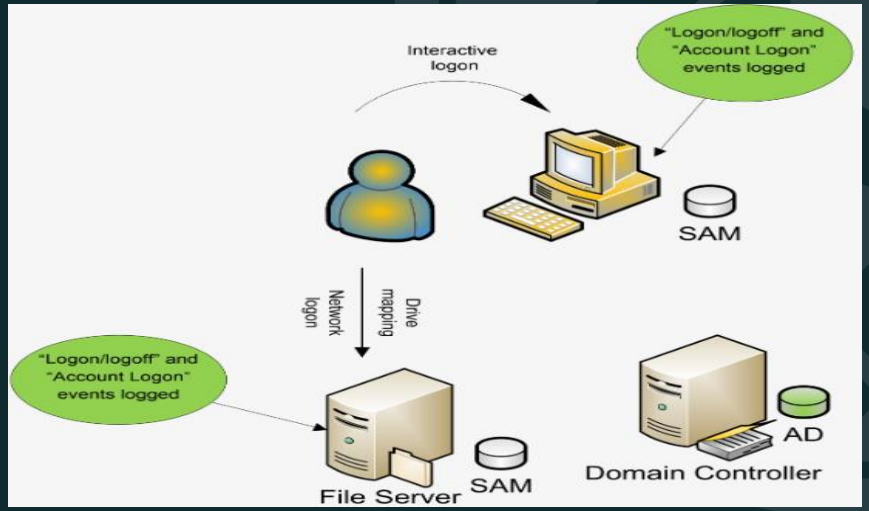
Account Logon Events:

- Corresponde a categoria Audit account logon events nas politicas de auditoria
- Autenticação (ocorre onde o usuário reside)



Logon Events:

- Corresponde a categoria Audit logon events nas politicas de auditoria
- Logon Sessions (ocorre onde o usuário está obtendo acesso ao sistema)



Logs/eventos de Account logon

Logs/eventos de Account logon

Windows 2000 Family	Windows XP & 2003 Family	Windows Vista, 7, 8 & 2008, 2012 Family	Description
672	672	4768	An authentication service (AS) ticket was successfully issued and validated (2000). An authentication service (AS) ticket was requested (2008). It is logged on DC Only.
673	673	4769	A ticket granting service (TGS) ticket was granted. Win2003 and Win2008 use this for both successful and failed service ticket requests with the proper Kerberos result/failure code.
674	674	4770	A security principal renewed an AS ticket or TGS ticket.
675	675	4771	Preauthentication failed. This event is generated on a Key Distribution Center (KDC) for the Kerberos errors during authentication.
676	672	4768	Authentication ticket request failed. See the Kerberos Error Code.
677	673	4769	A TGS ticket was not granted (failed). This event 677 in Windows 2000 is replaced with 673 in Windows XP/2003 family) and 4769 with later versions with audit type/codes for failures.
678	678	4774	An account was successfully mapped for logon to a domain account. Not common.
680	680	4776	Account used for logon by. Logged for local user (local SAM) authentication. DC logs this event for NTLM authentication.
681	680	4776	Logon failure on Windows 2000 for NTLM authentication. A domain account logon was attempted. This event is replaced with 680 in Windows XP/2003 family and 4776 with Windows 2008/Vista onwards with the audit type/codes for failures.
682	682	4778	A user has reconnected to a disconnected terminal session.
683	683	4779	A user disconnected a terminal session without logging off.

Logs/eventos de logon

Logs/eventos de logon

Windows 2000 Family	Windows XP & 2003 Family	Windows Vista, 7, 8 & 2008, 2012 Family	Description
528	528	4624	Successful logon: A user successfully logged on to a computer. For information about the type of logon, see the next section.
529	529	4625	Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password. For Windows 2008 and above, event ID 4625 logs every failed logon attempt with failure status code regardless of logon type or type of account.
530	530	4625	Logon failure for a logon attempt to log on outside of the allowed time.
531	531	4625	Logon failure for a logon attempt using a disabled account.
532	532	4625	Logon failure for a logon attempt using an expired account.
533	533	4625	Logon failure. A logon attempt was made by a user who is not allowed to log on at this computer.
534	534	4625	Logon failure. The user attempted to log on with a type that is not allowed.
535	535	4625	Logon failure. The password for the specified account has expired.
536	536	4625	Logon failure. The Net Logon service is not active.
537	537	4625	Logon failure. The logon attempt failed for other reasons. In some cases, the reason for the logon failure may not be known.
538	538	4634	The logoff process was completed for a user.
539	539	4625	Logon failure. The account was locked out at the logon.
540	540	4624	Successful network logon: A user successfully logged on over a network.
538	551	4647	A user initiated the logoff process. It is logged for Interactive and RemoteInteractive logons in place of logoff event 538/4634.
552	552	4648	A user successfully logged on to a computer using explicit credentials while already logged on as a different user.
682	682	4778	A user has reconnected to a disconnected terminal session.
683	683	4779	A user disconnected a terminal session without logging off.

Logon type:

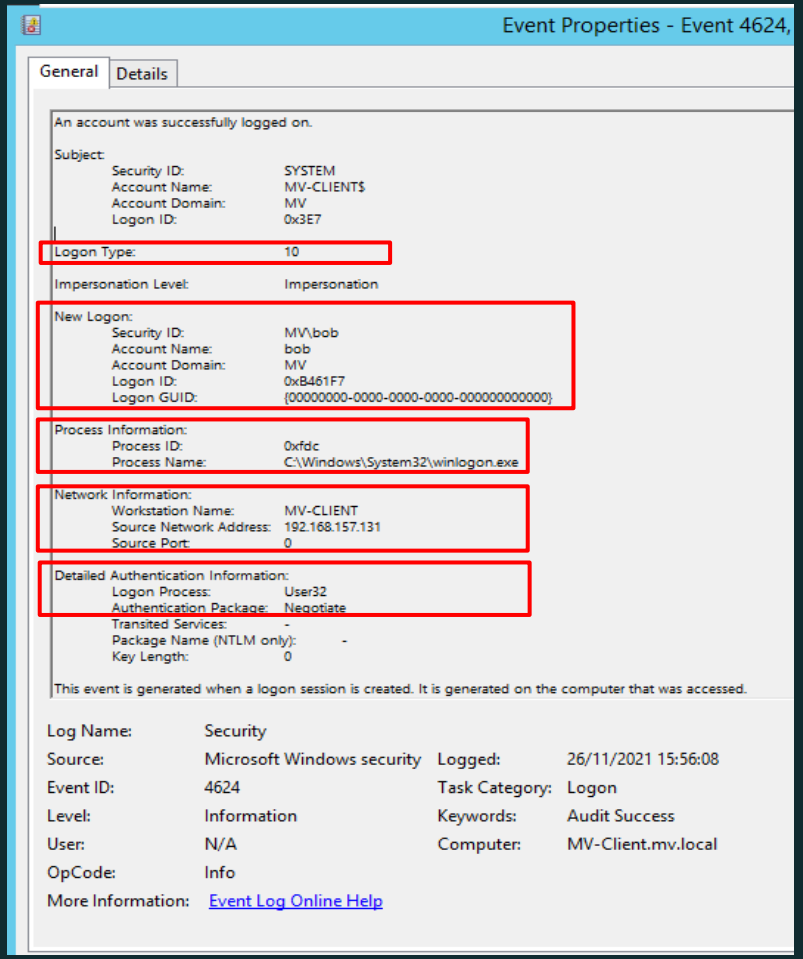
Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unnattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication") See this article for more information.
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials see 4648. MS says "A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections."
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	**CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)**

Cenários de logon

- Interactive Logon:
  - In an Interactive logon, user enters credentials into the Log On to Windows dialog box or user inserts a smart card into the smart card reader. User's authentication is then checked against the security database on the user's local computer or to an Active Directory domain. User can perform an interactive logon in two different ways:
    - Locally, when the user has direct access to the console.
    - Remotely, through Terminal Services.

- Network Logon:
  - Network logon are very common to Windows environment. They are only used after an account authentication such as user, computer, service has already taken place. For network logon, the process does not use the initial logon dialog box to enter the credentials. Instead, already established credentials for the account are used, or credentials are collected using in a different way. This is typically invisible to the user unless alternate credentials are used. Network logon confirms the users' identification to the network service such as mapped drive on another server that the user is attempting to access (Microsoft TechNet, 2003). Windows logs logon type 3 for network logons such as accessing shared folders, printers, GPOs, and most logons to IIS.

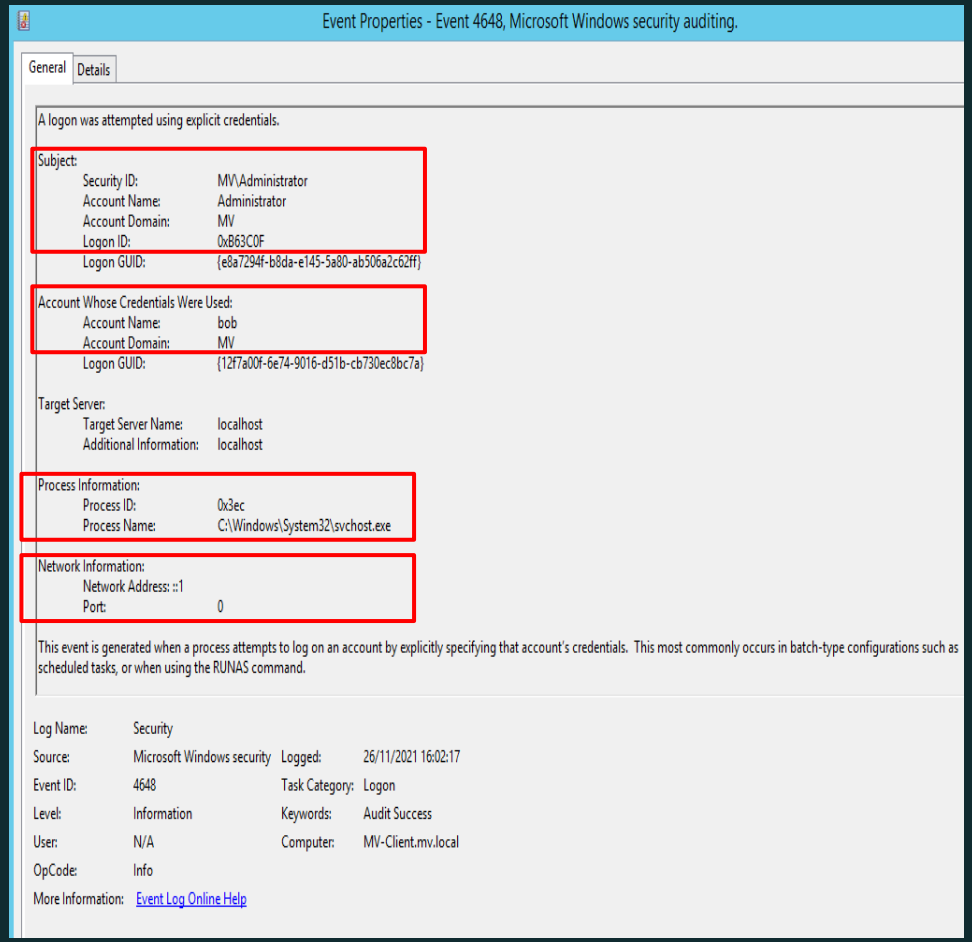
Logs/eventos de logon: 4624 - An account was successfully logged on



Campos úteis:

- Em subject:
  - Logon Type: Determina o tipo de logon;
- New Logon:
  - Security ID: Dominio + username
  - Logon ID: Identificador único dentro da sessão
- Process Information:
  - Process Name: Nome do processo que gerou o login;
- Network Information:
  - Workstation Name: Nome do computador que fez autenticação
  - Source Network Address: IP de origem;
  - Source Port: Porta de origem
- Detailed Authentication Information:
  - Logon Process: Nome do processo de logon que realizou o login;
  - Authentication Package: Nome do pacote usado para autenticação

Logs/eventos de logon: 4648 - A logon was attempted using explicit credentials



- Campos uteis:
- Subject:
  - Security ID: Dominio + username que gerou a autenticação;
- Account Whose Credentials...
  - Account Name: User impersonificado
  - Account Domain: Dominio do usuário impersonificado
- Process information:
  - Process ID: Id do processo criado;
  - Process Name: Nome do processo criado;
- Network Information:
  - Network Address: IP de origem que fez ação
  - Source Port: Porta de origem

Processo de logon

Processo de logon

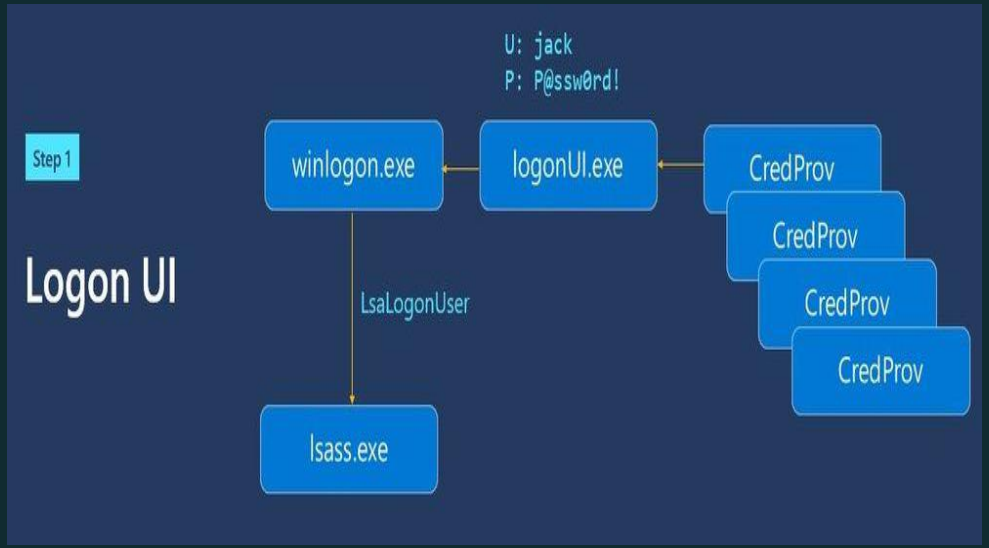
Processos importantes:

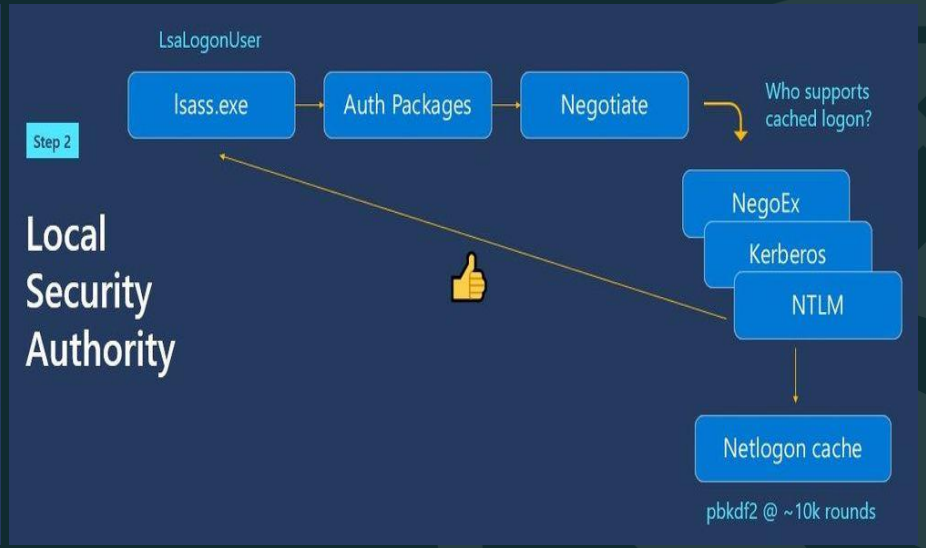
- Wininit.exe:
  - A principal função desse processo é lançar a maioria das aplicações que rodam em background (segundo plano) e estão constantemente em execução. O “wininit.exe” é também responsável por iniciar o Service Control Manager (services.exe), o Local Security Authority process (lsass.exe) e o Local Session Manager (lsm.exe). Também cria a windows station (Winsta0) interativa.

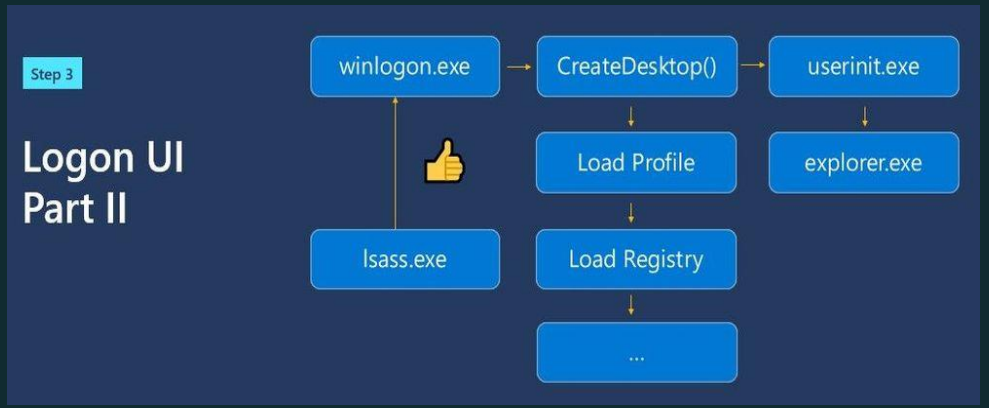
Login interativo

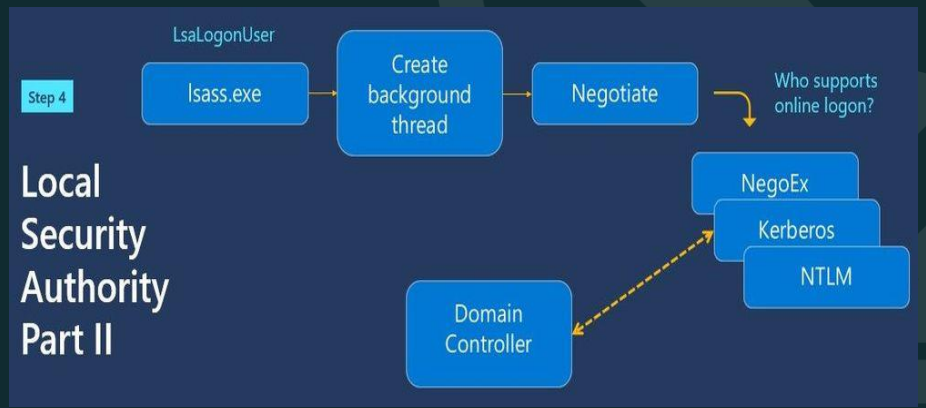
- Winlogon.exe:
  - Responsável pelo logon e logoff;
  - Carregar o perfil do usuário quando o usuário inicia a sessão;
  - Secure Attention Sequence (SAS): SAS é a combinação de chaves para que os usuários possam pressionar, antes do logon (Ctrl + alt + del). O winlogon.exe é responsável por assegurar que o usuário tenha uma tela segura para logar e previnir roubo de credenciais;
  - Travar o computador e executar um protetor de tela (screensaver): O winlogon.exe é responsavel por monitorar atividades do mouse e teclado, travar a tela e executar o protetor de tela (screensaver) no caso de um periodo de inatividade;
- LogonUI.exe:
  - Envia as credenciais para o lsass.exe;
  - Iniciado pelo winlogon.exe
- Userinit.exe :
  - Processo que inicia o shell do usuário;
- Explorer.exe:
  - Shell padrão do usuário;
  - É iniciado pelo userinit.exe.

Processo de logon

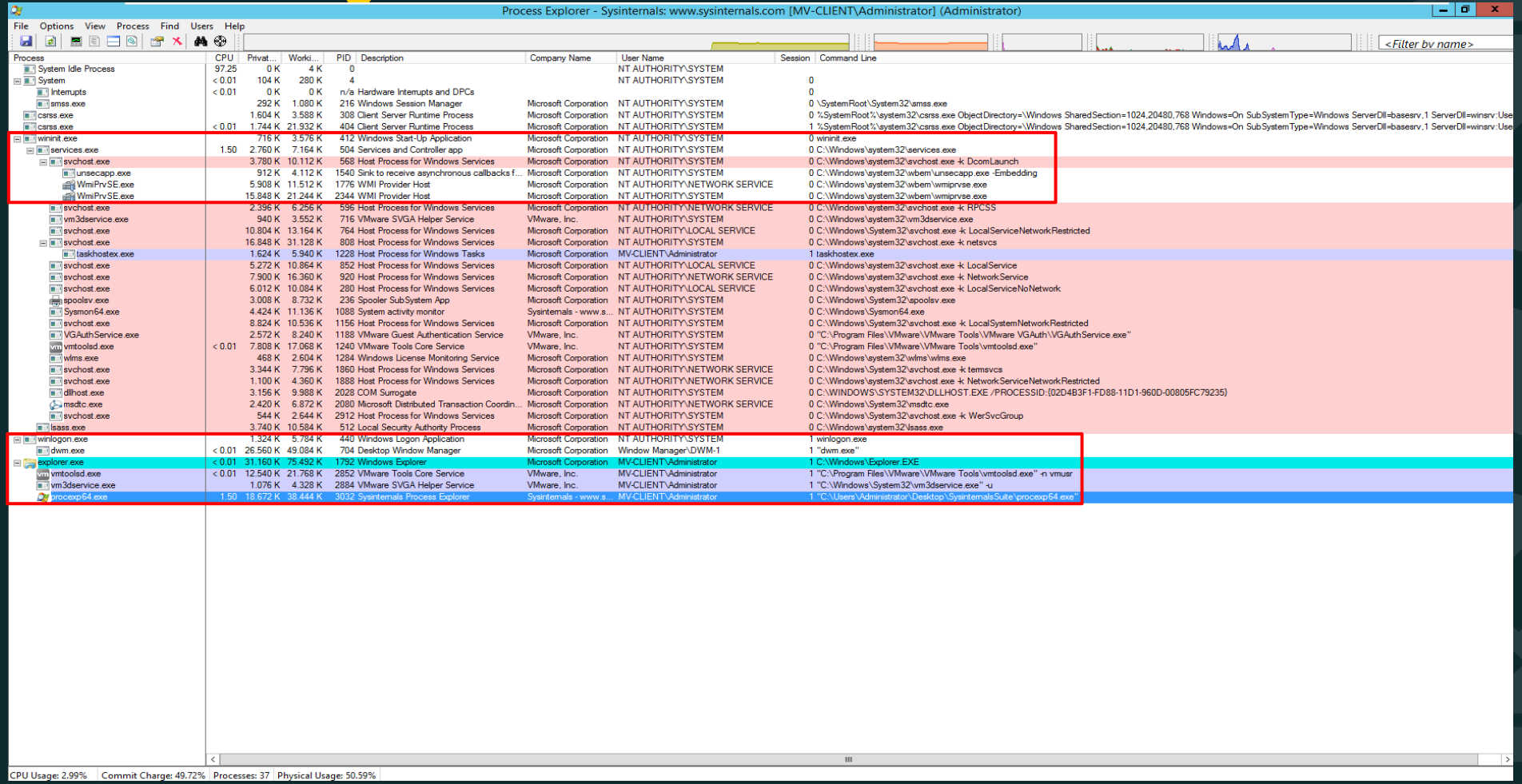




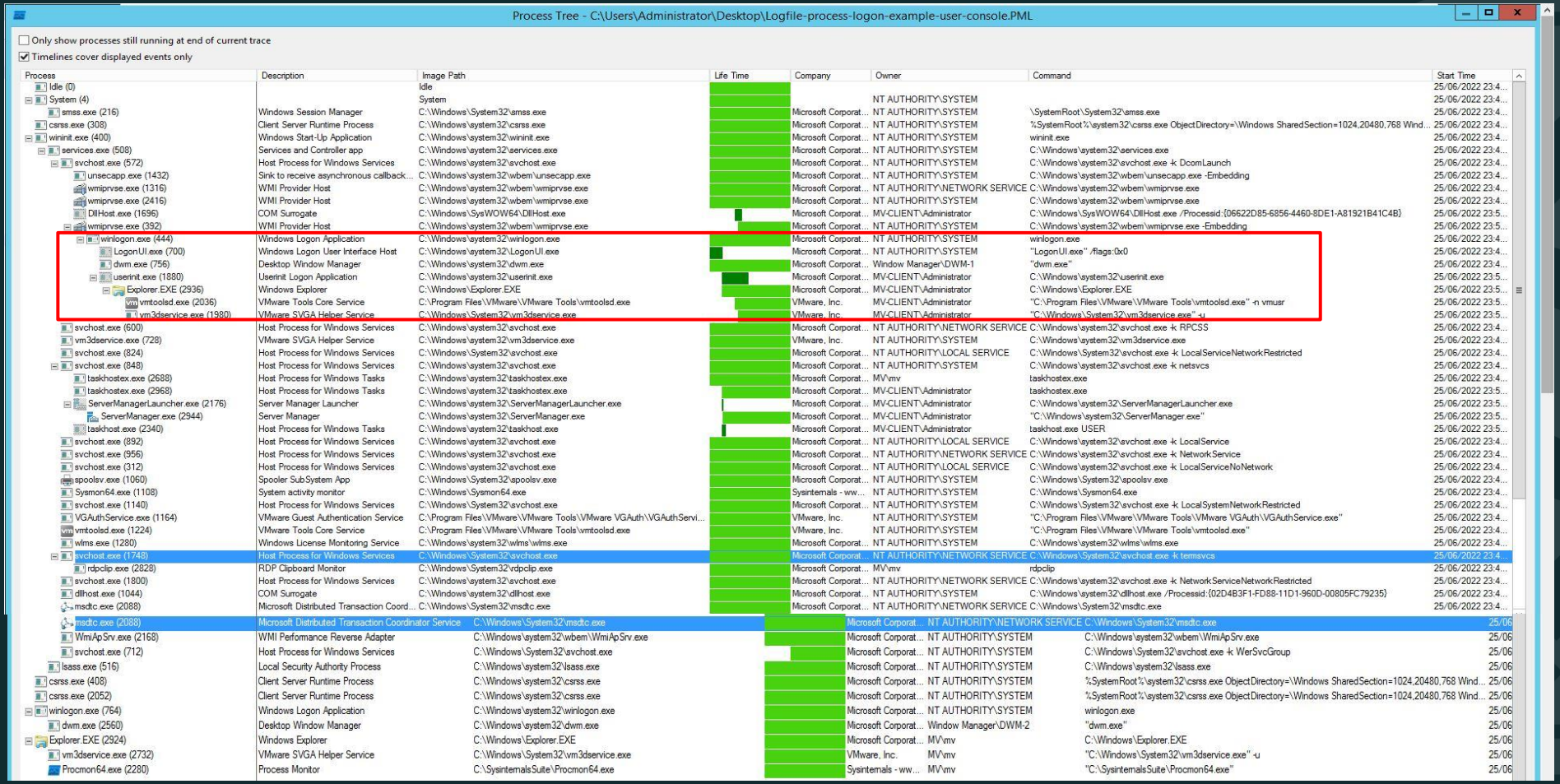




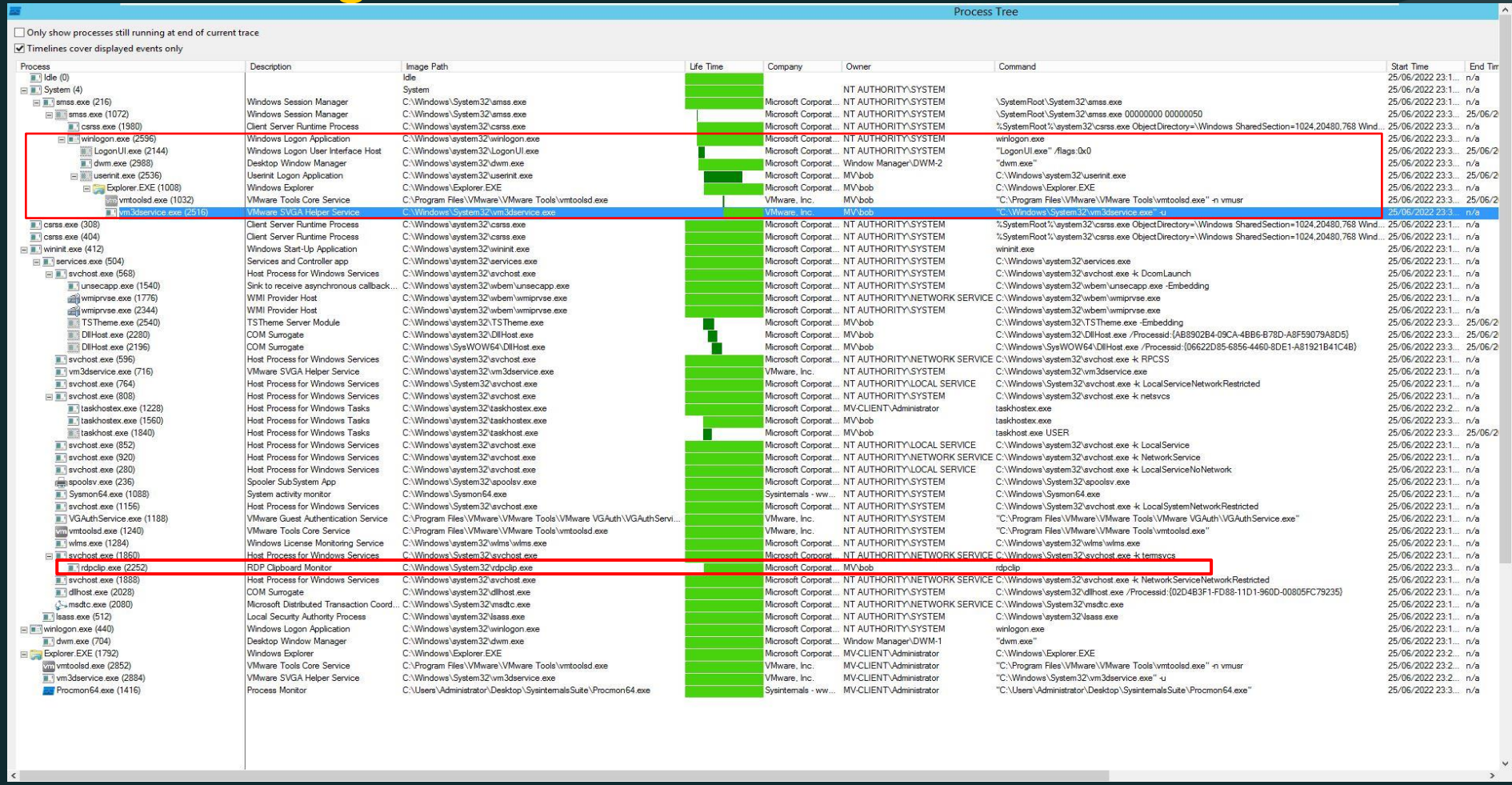
Processo de logon



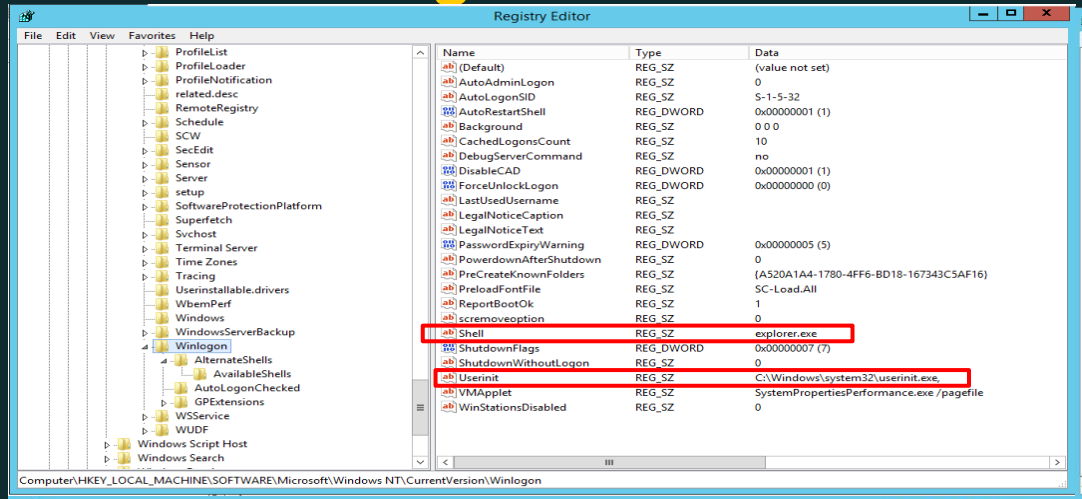
Processo de logon

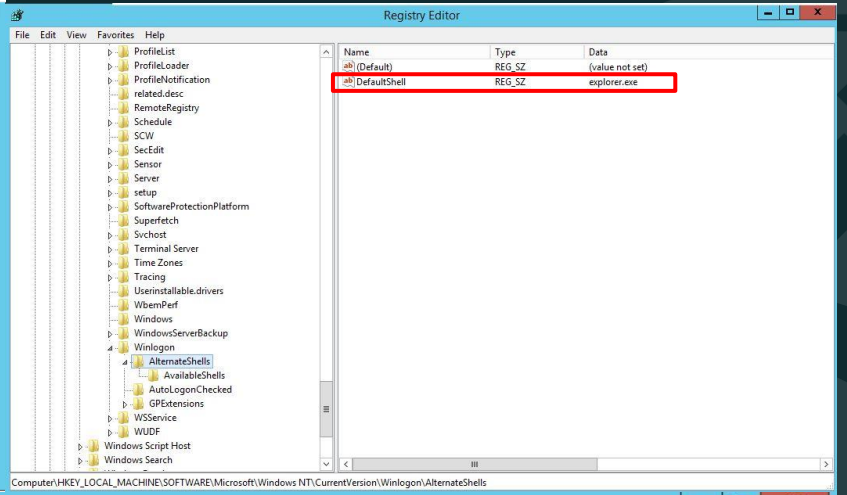


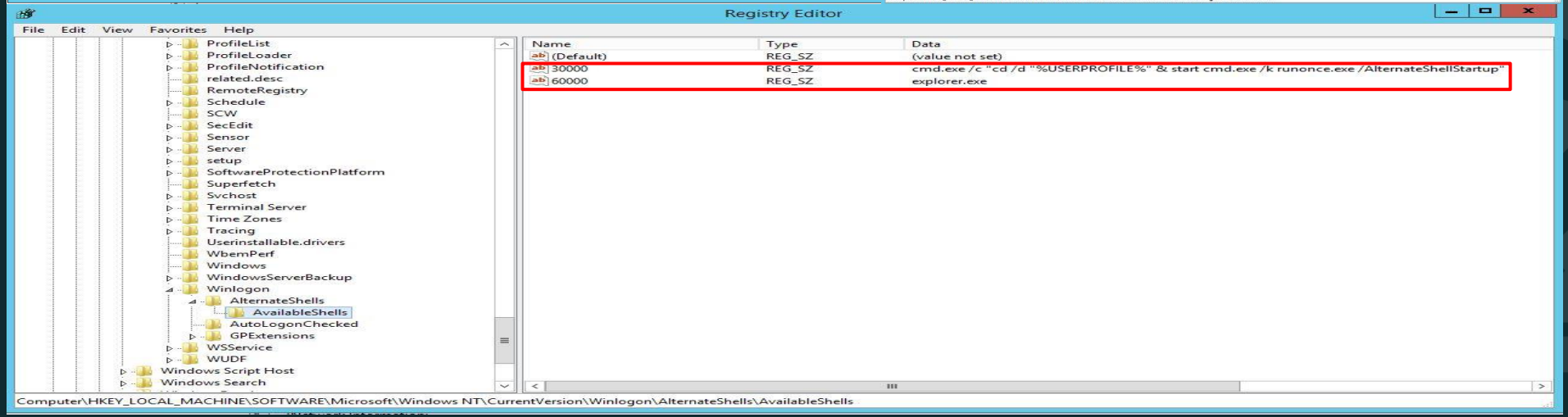
Processo de logon



Processo de logon

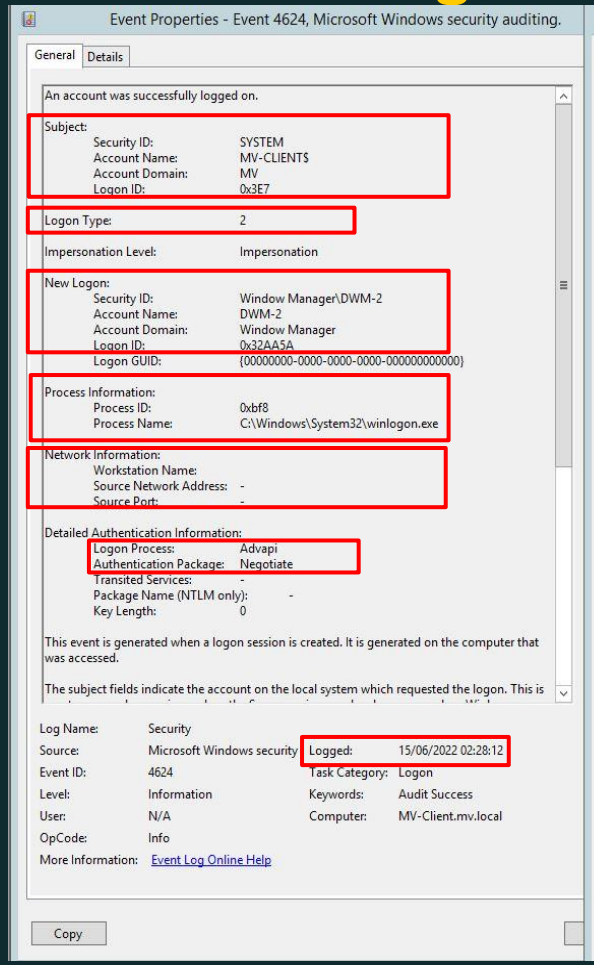


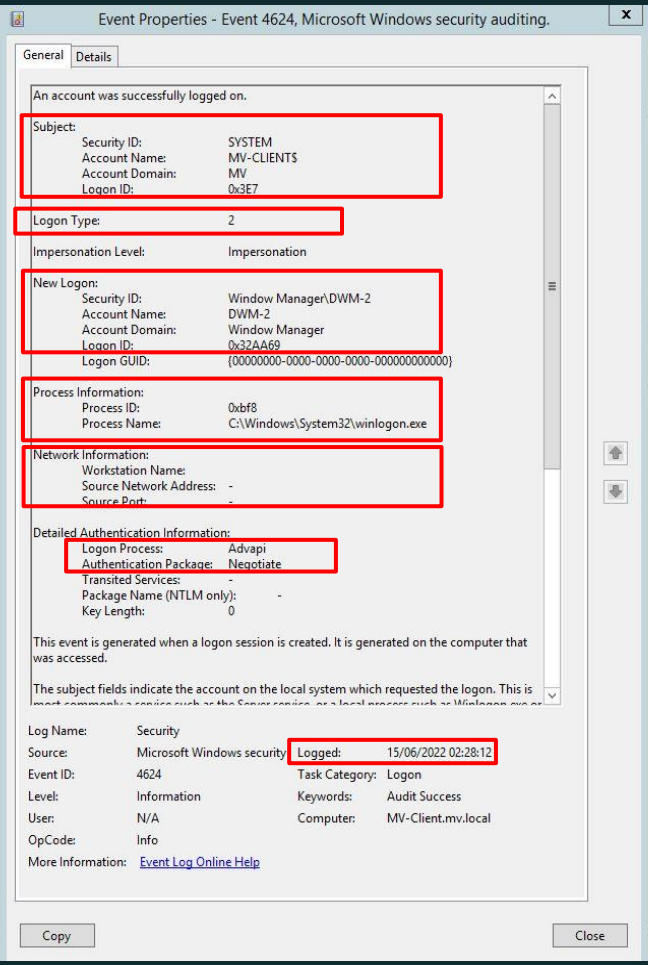


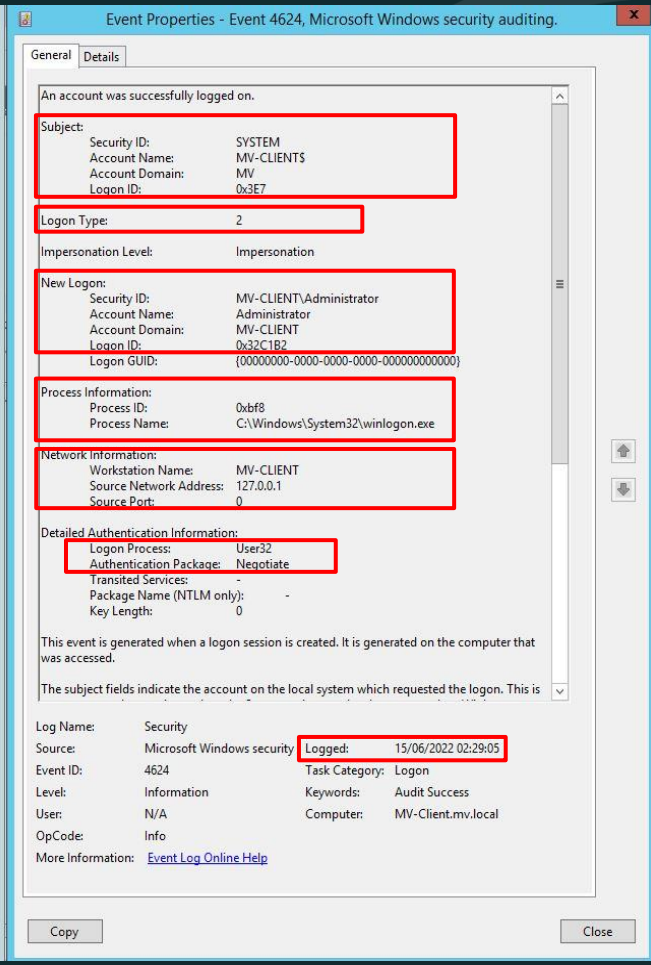


Cenários

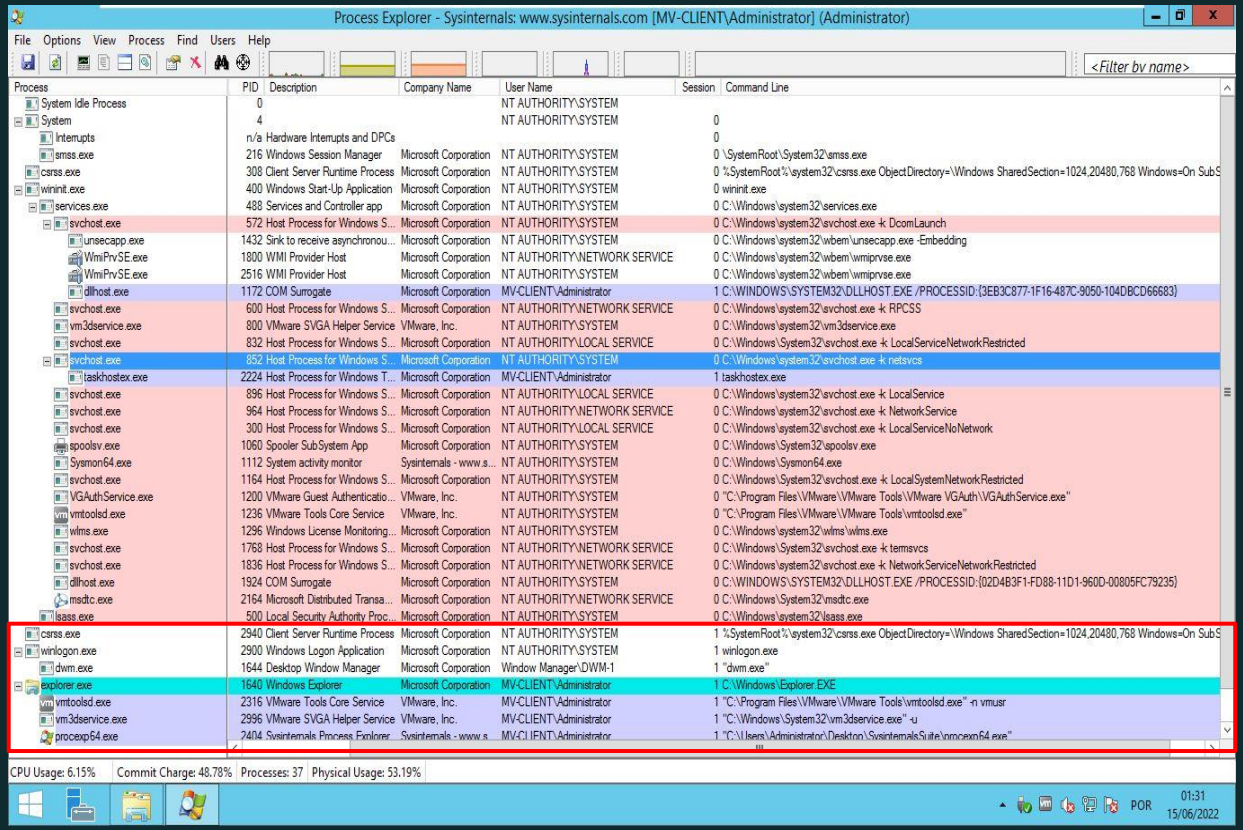
Cenário 1 – Logon comum – Console/interativo

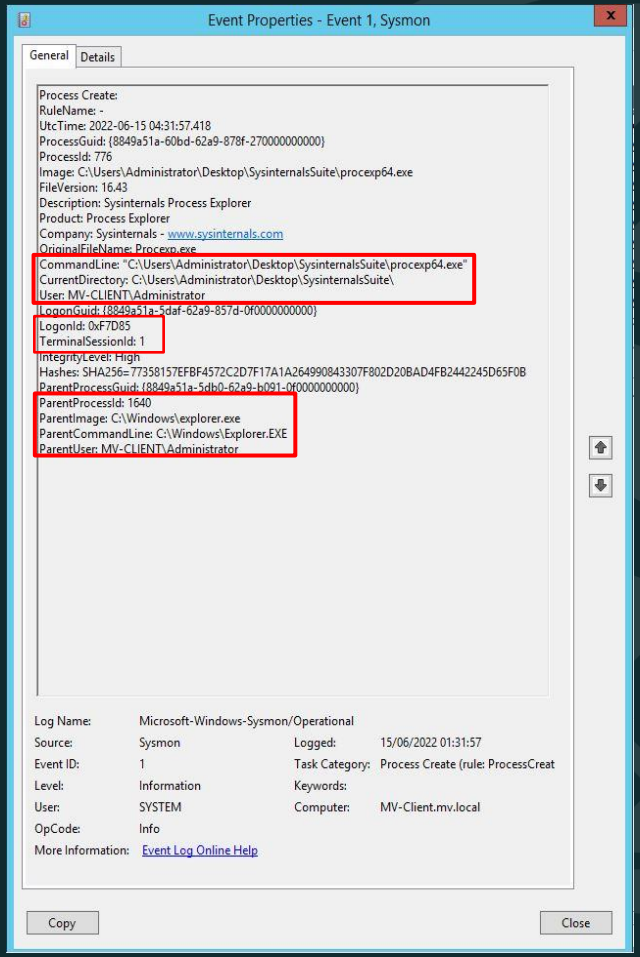




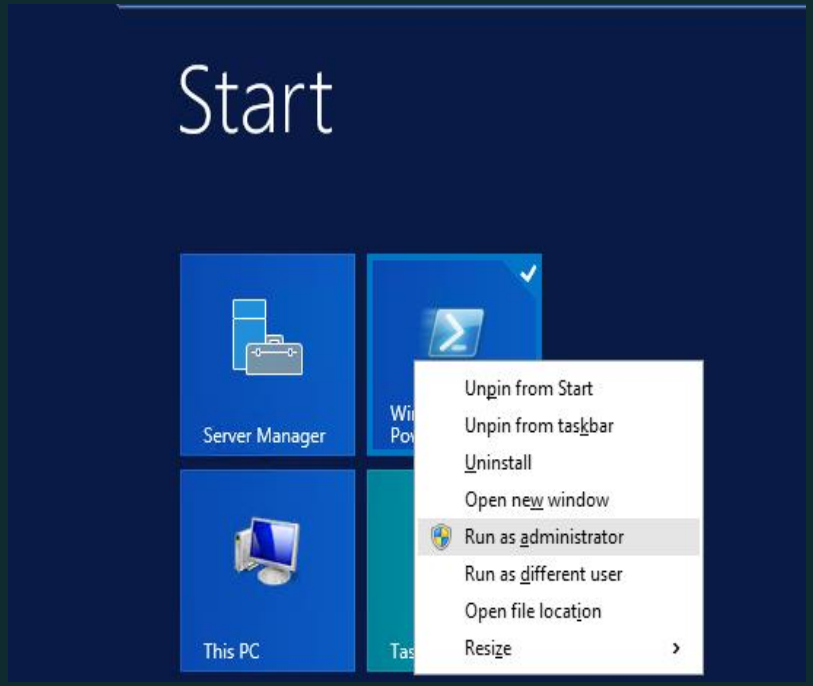


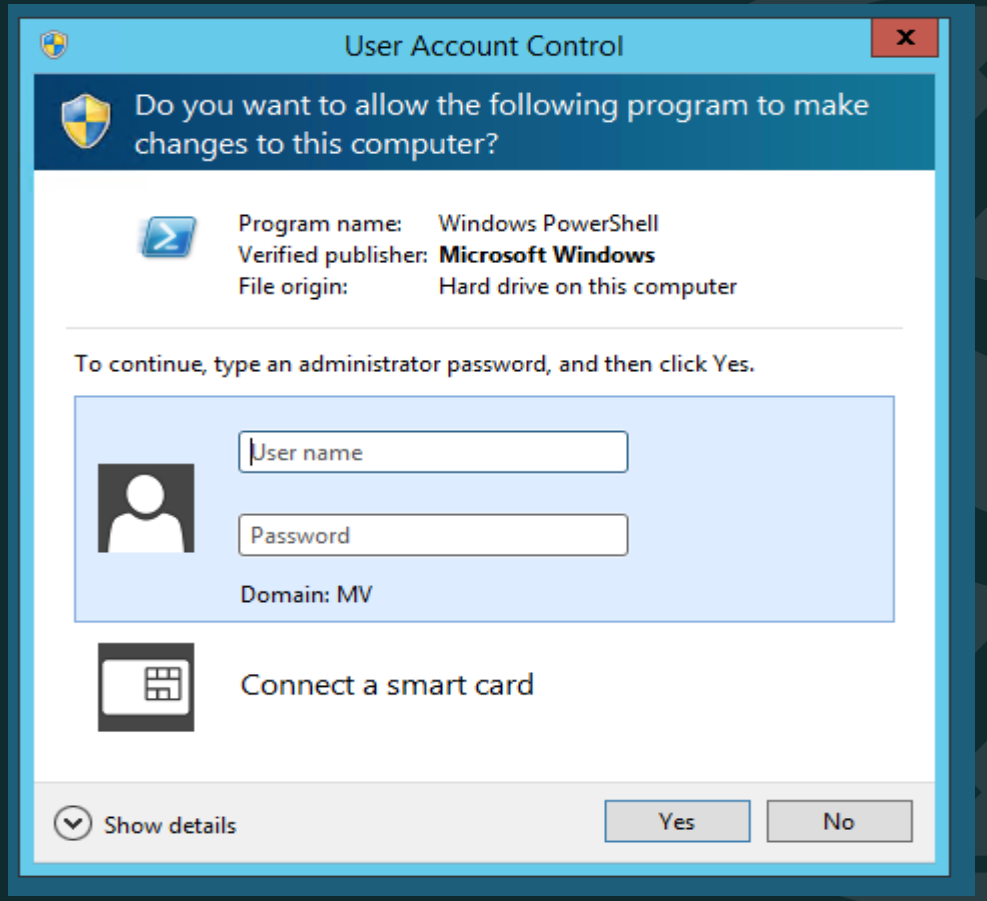
Cenário 1 – Logon comum – Console/interativo



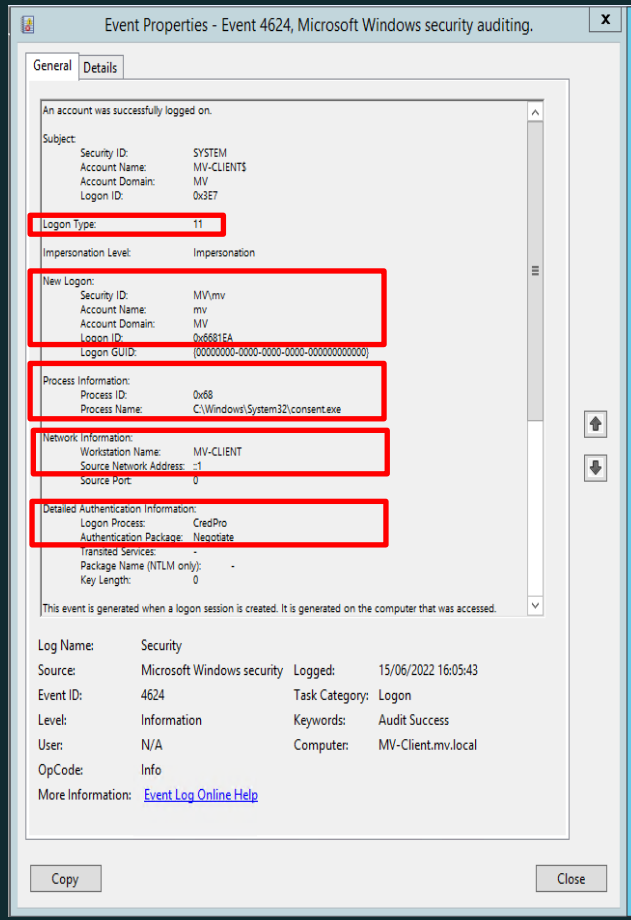


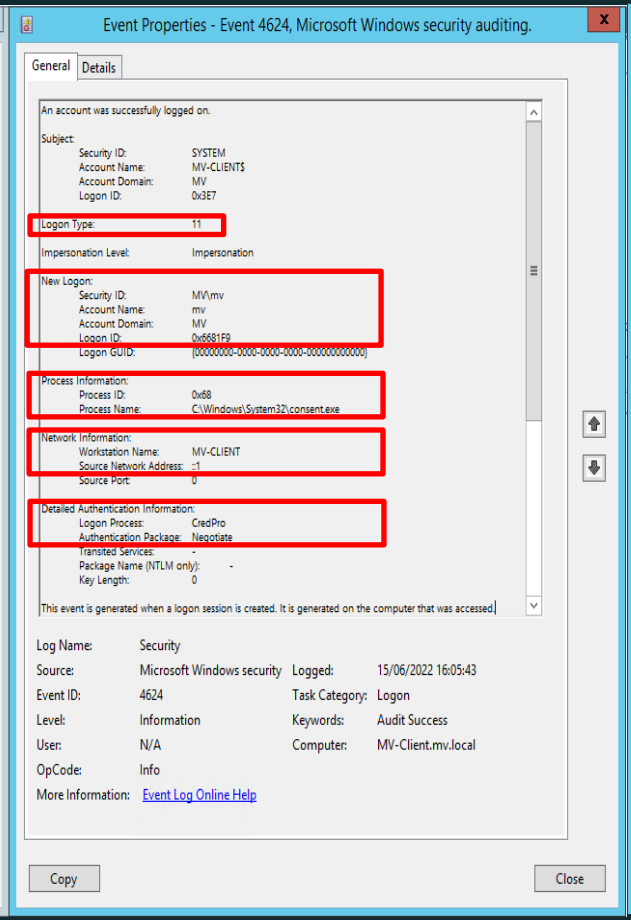
Cenário 2 – Consent.exe

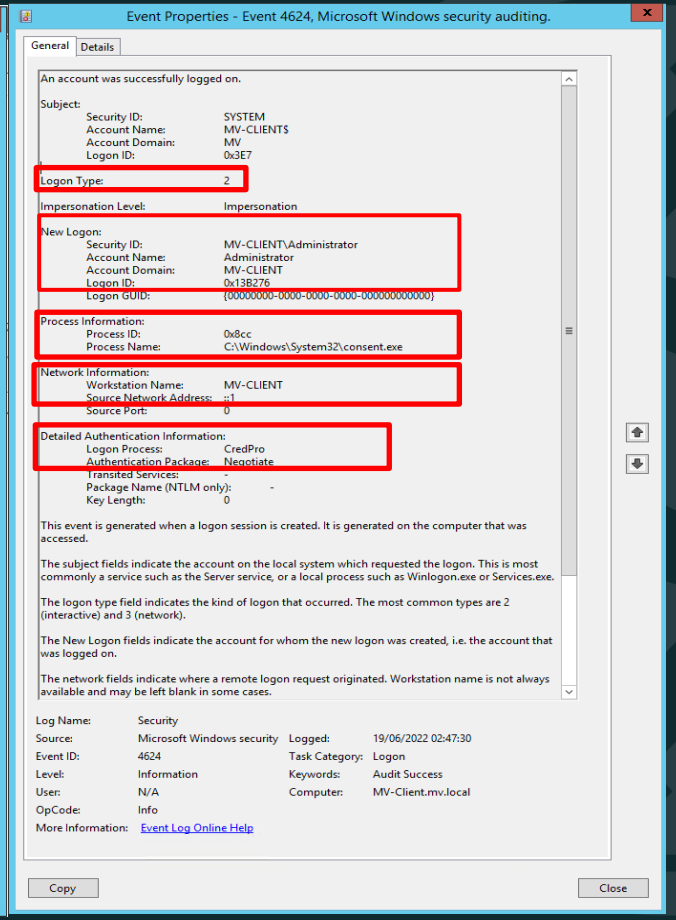




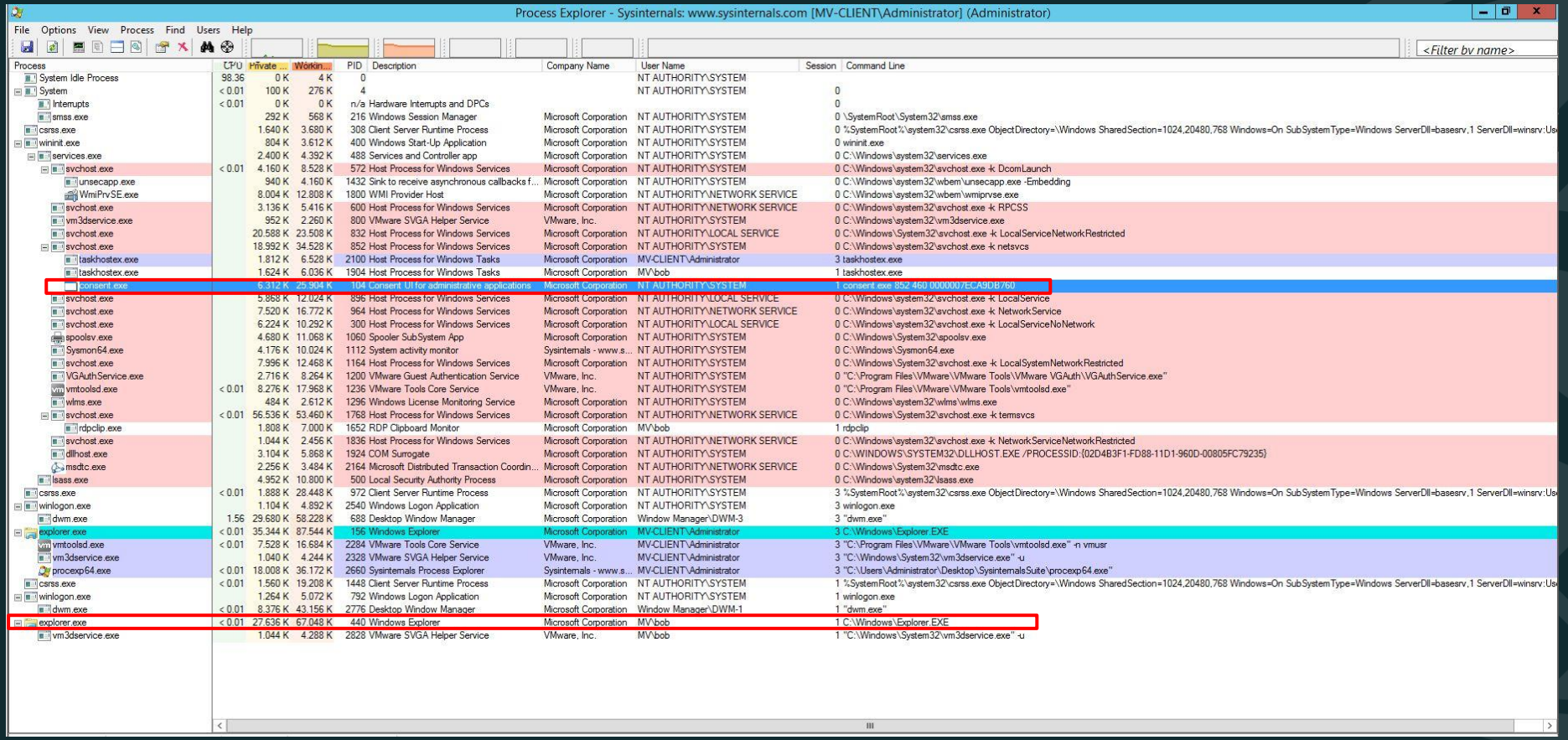
Cenário 2 – Consent.exe



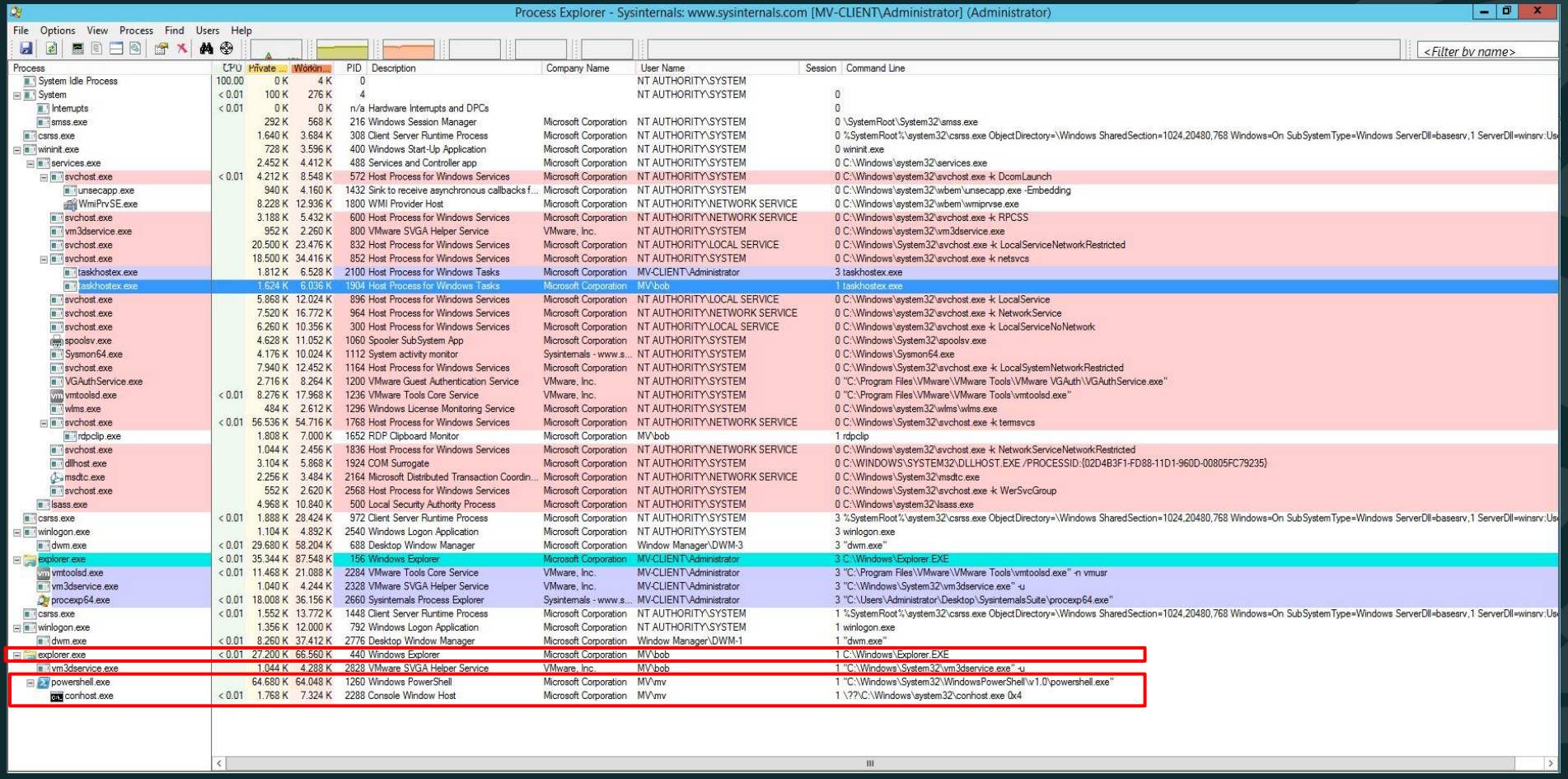




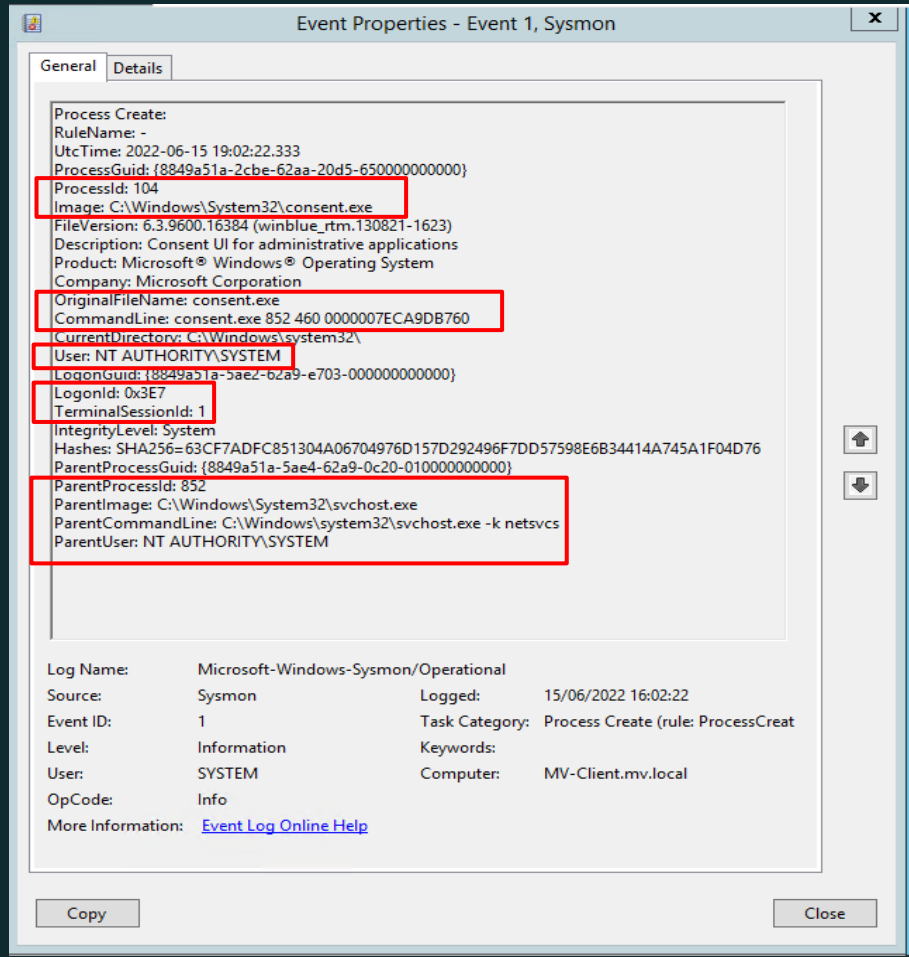
Cenário 2 – Consent.exe

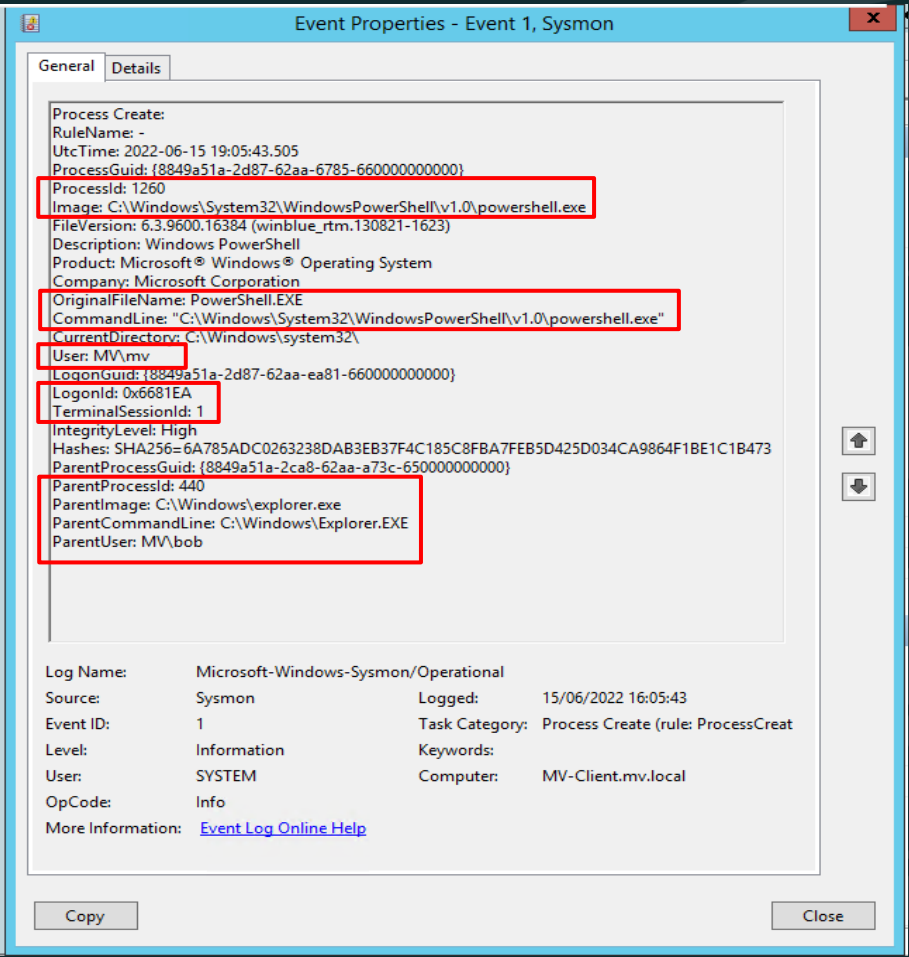


Cenário 2 – Consent.exe

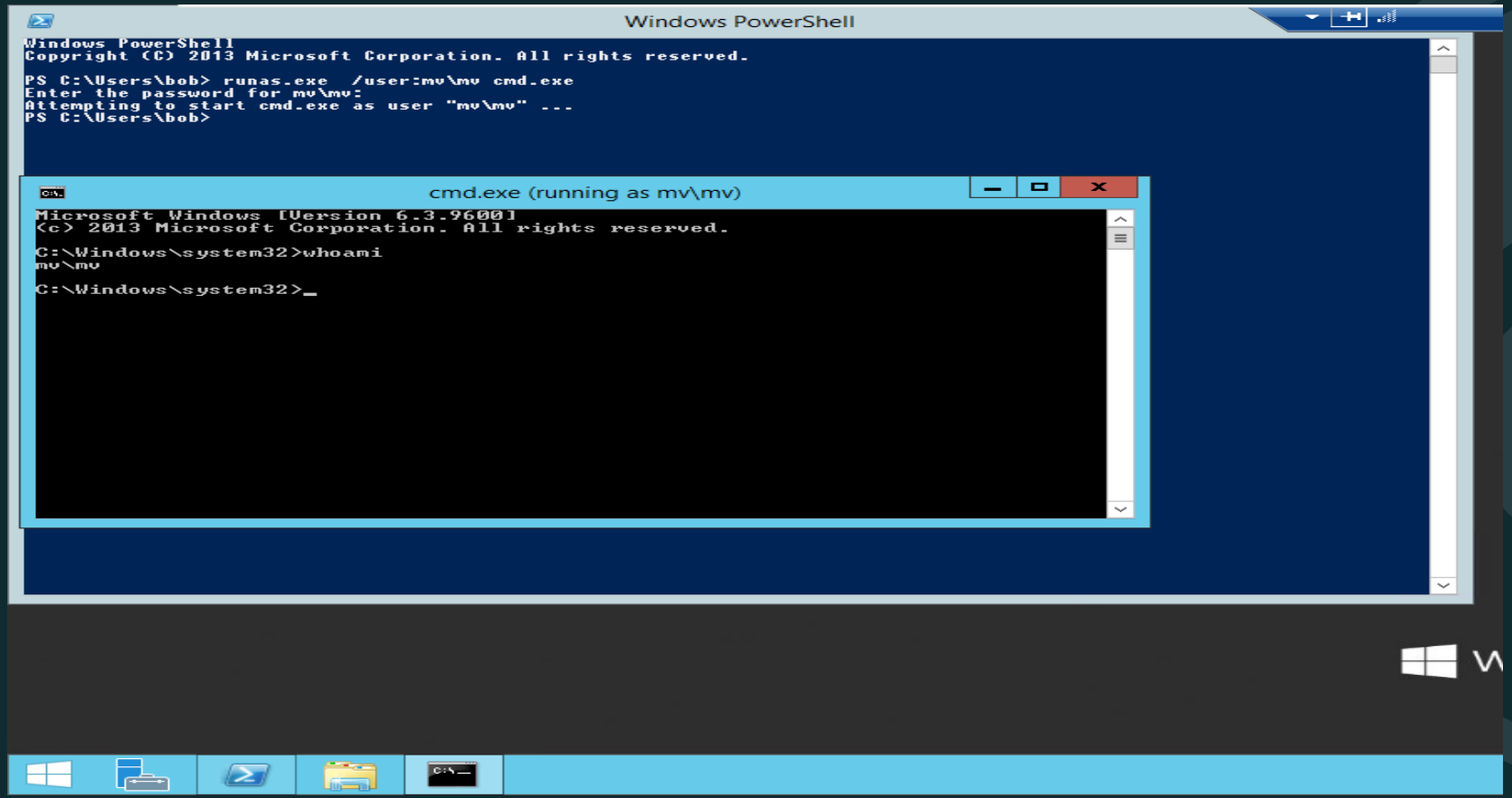


Cenário 2 – Consent.exe

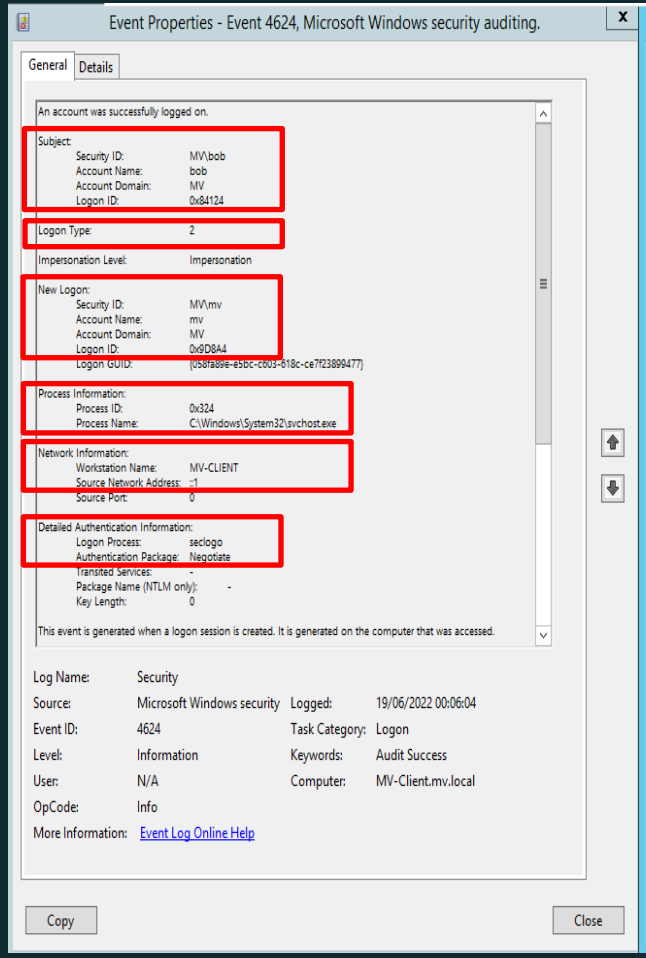


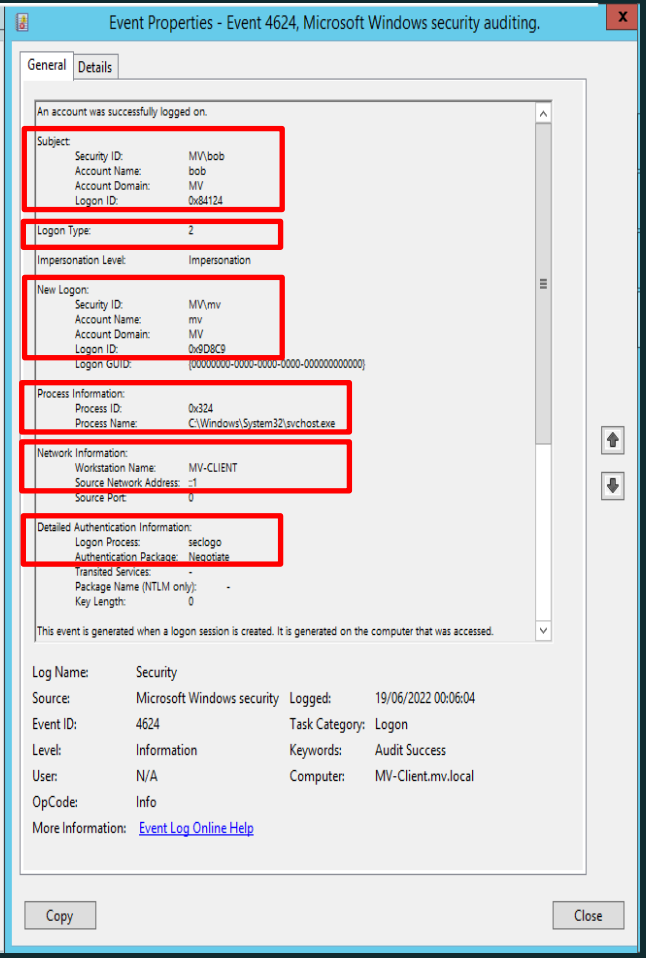


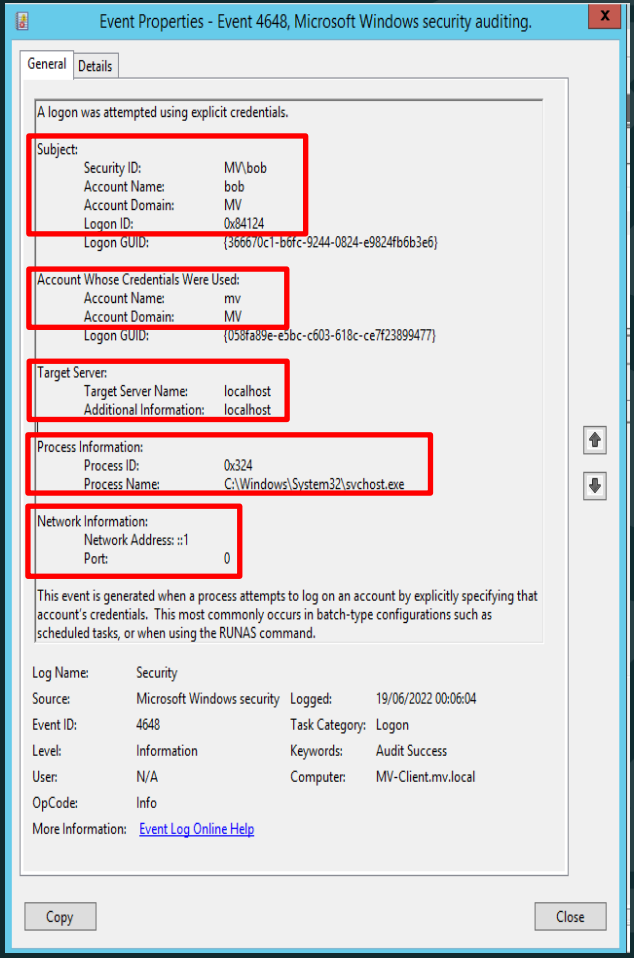
Cenário 3 - Runas



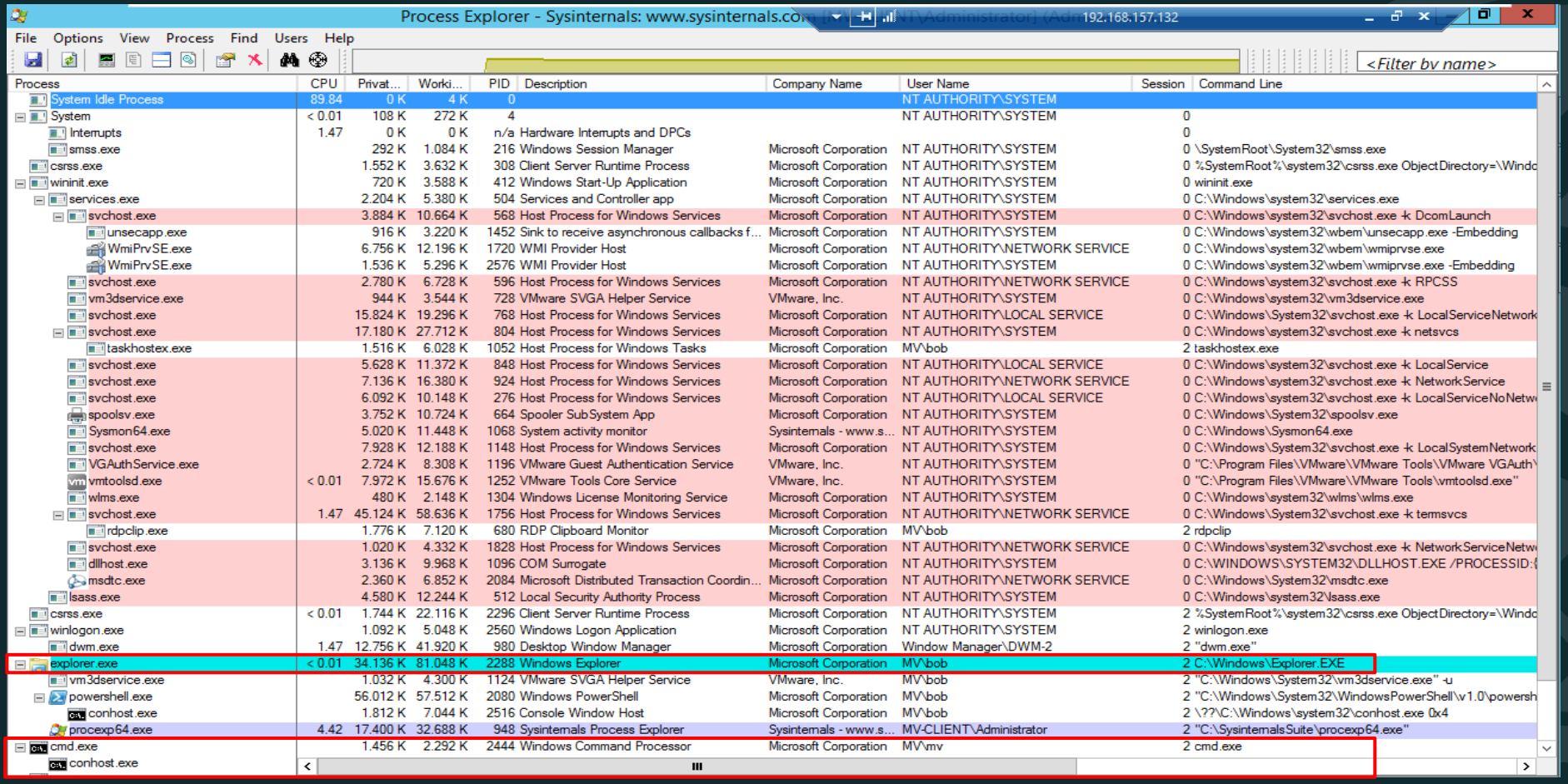
Cenário 3 - Runas



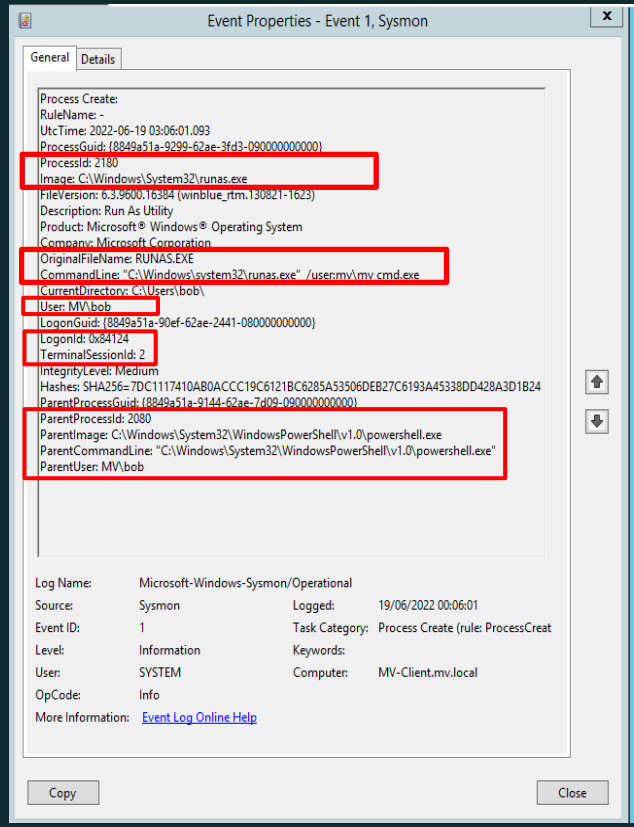


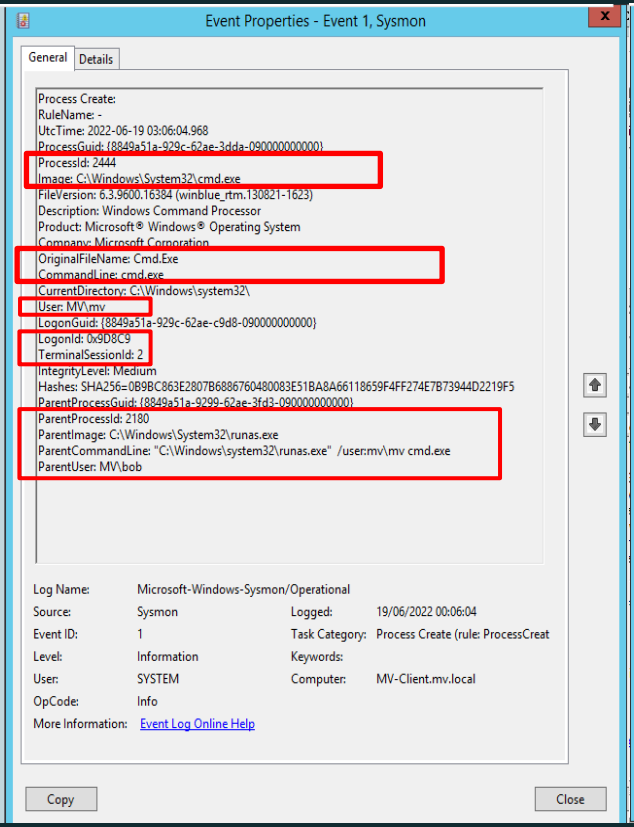


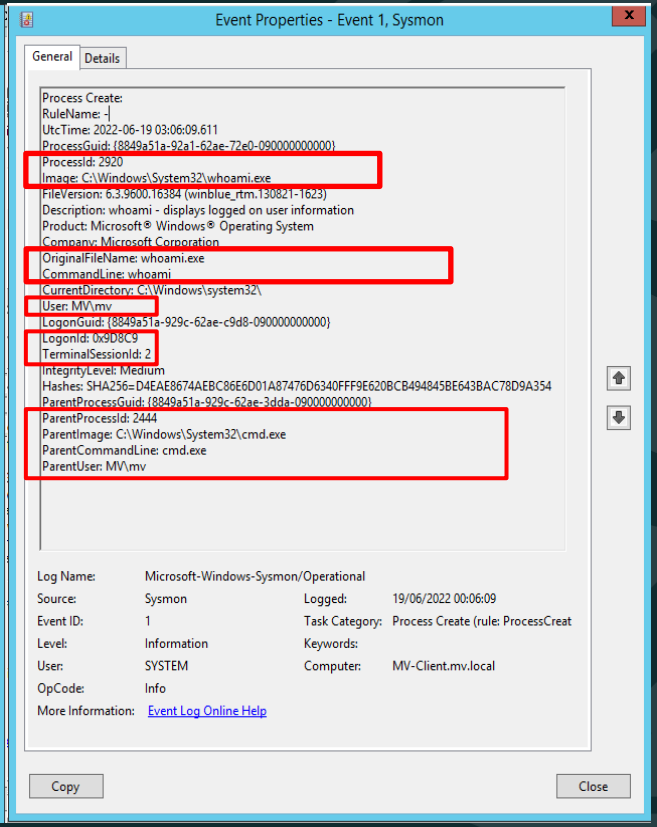
Cenário 3 - Runas



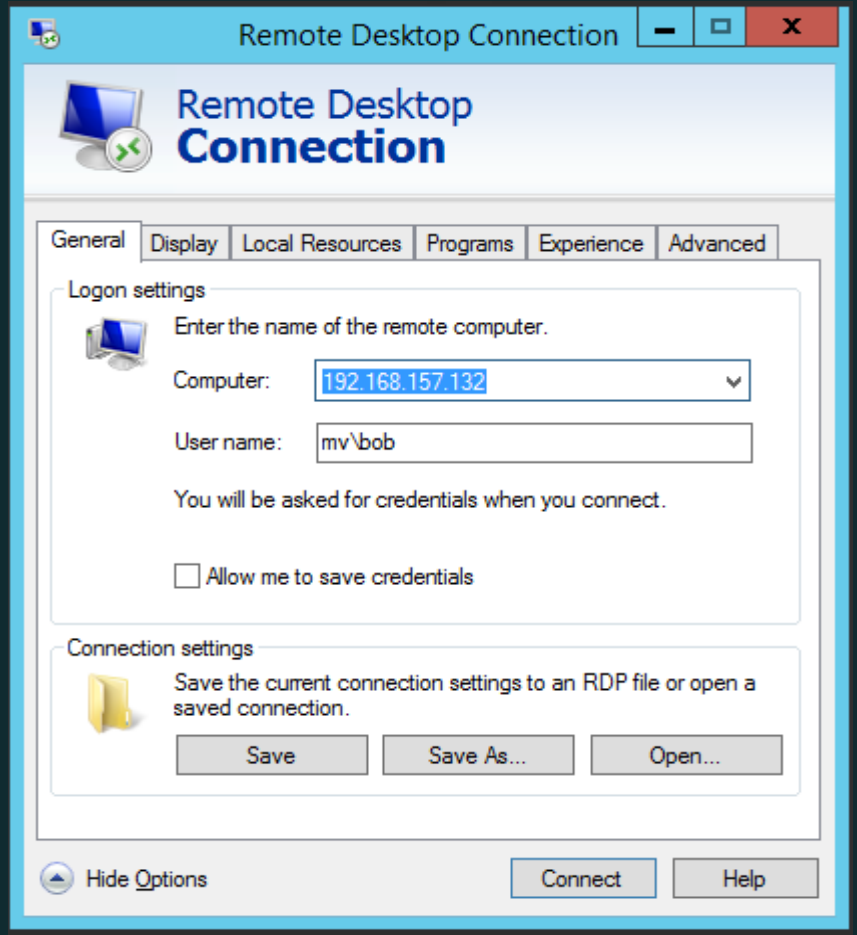
Cenário 3 - Runas

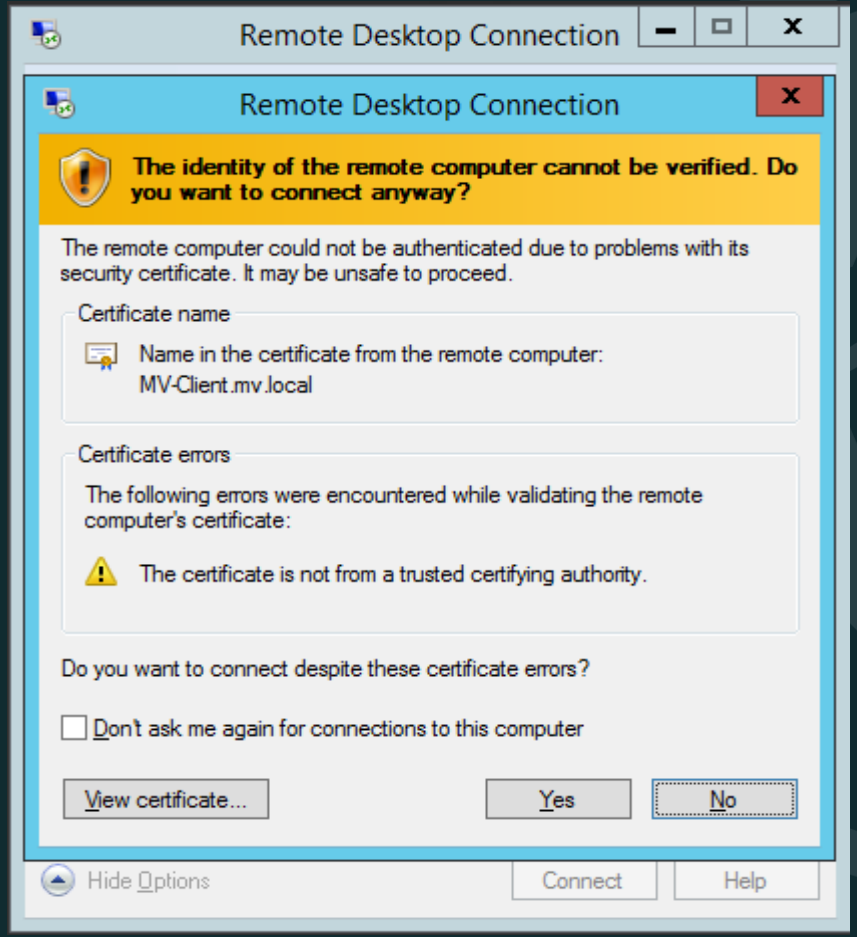




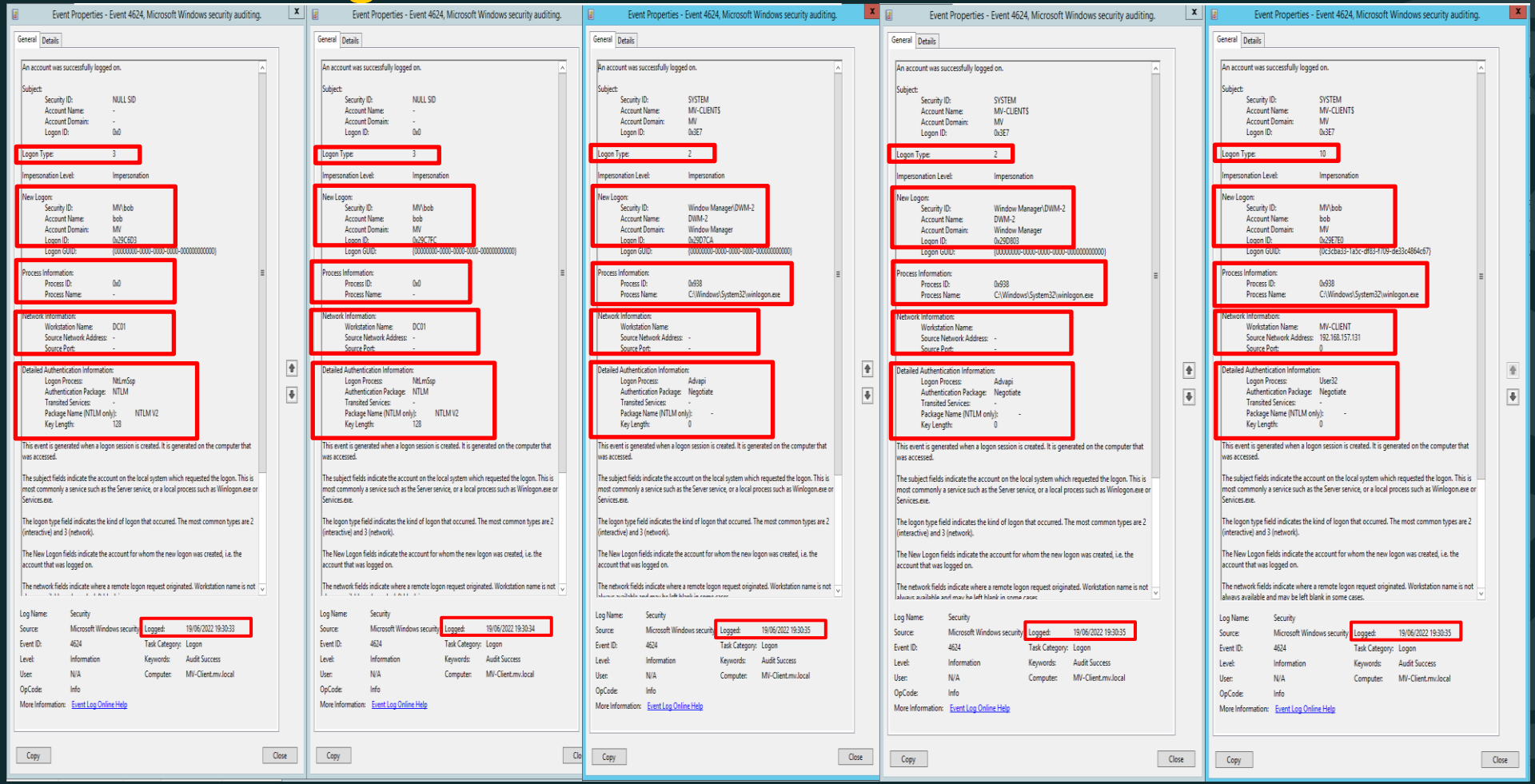


Cenário 4 – Logon TS/RDP

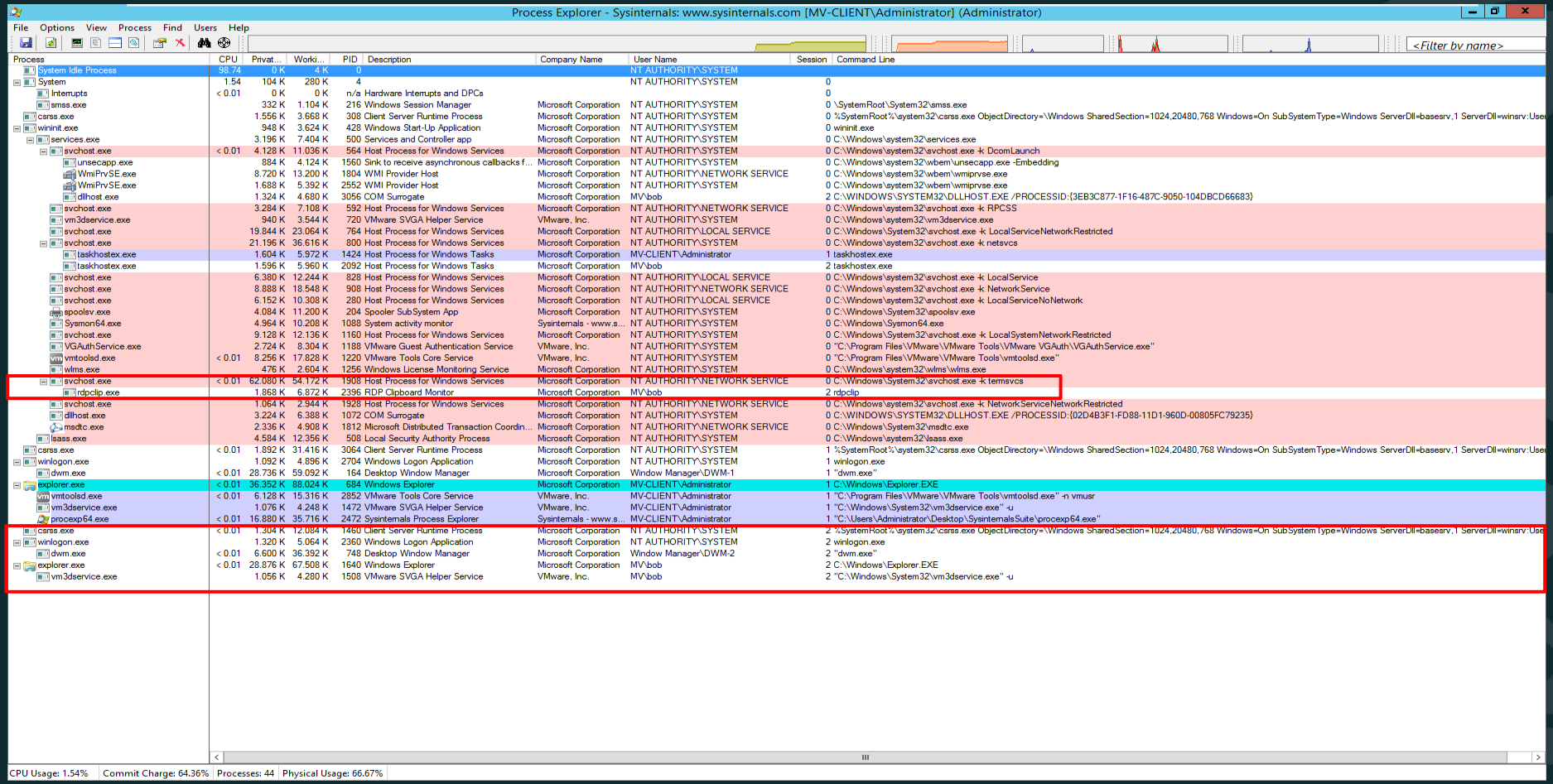




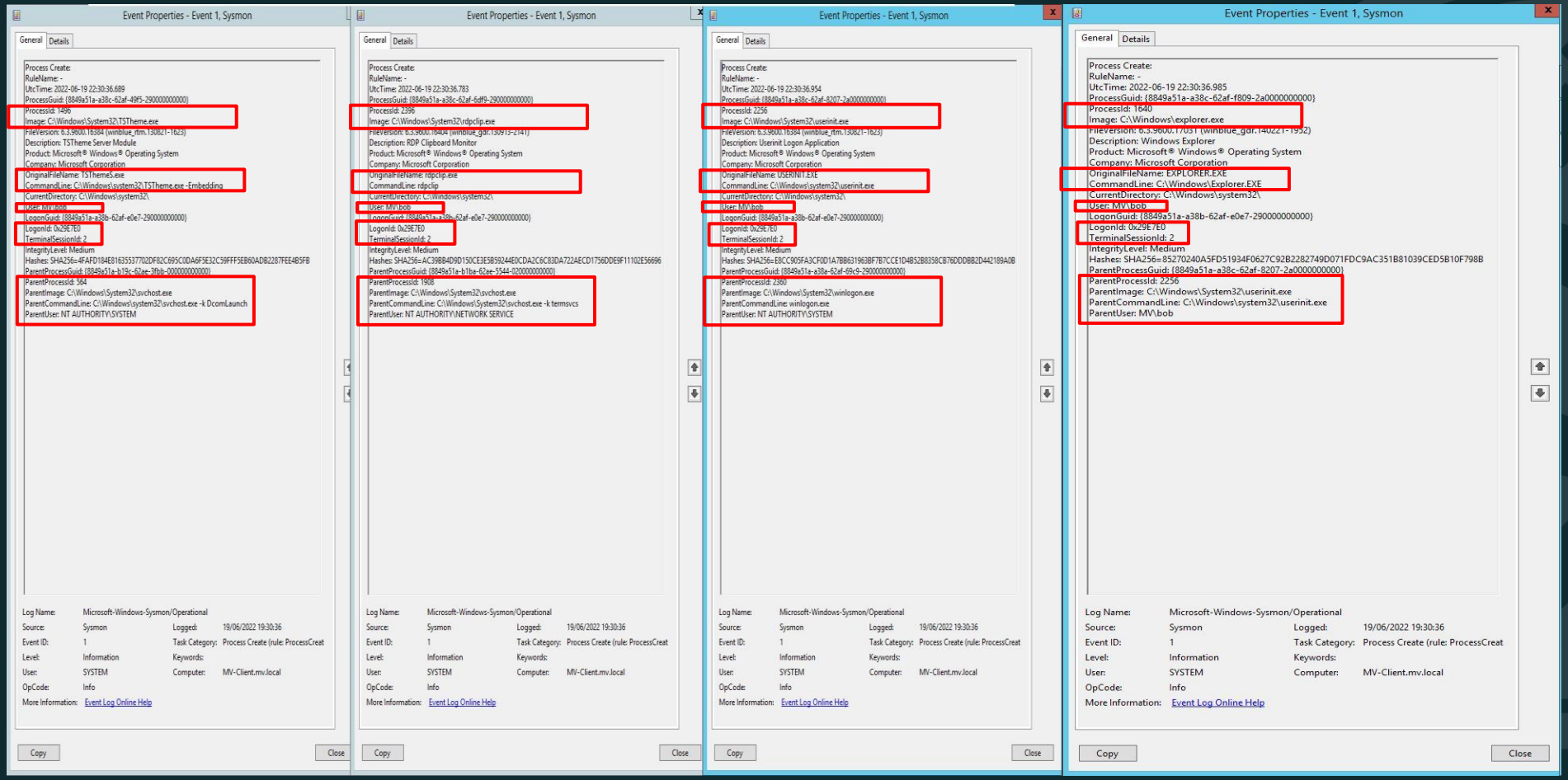
Cenário 4 – Logon TS/RDP



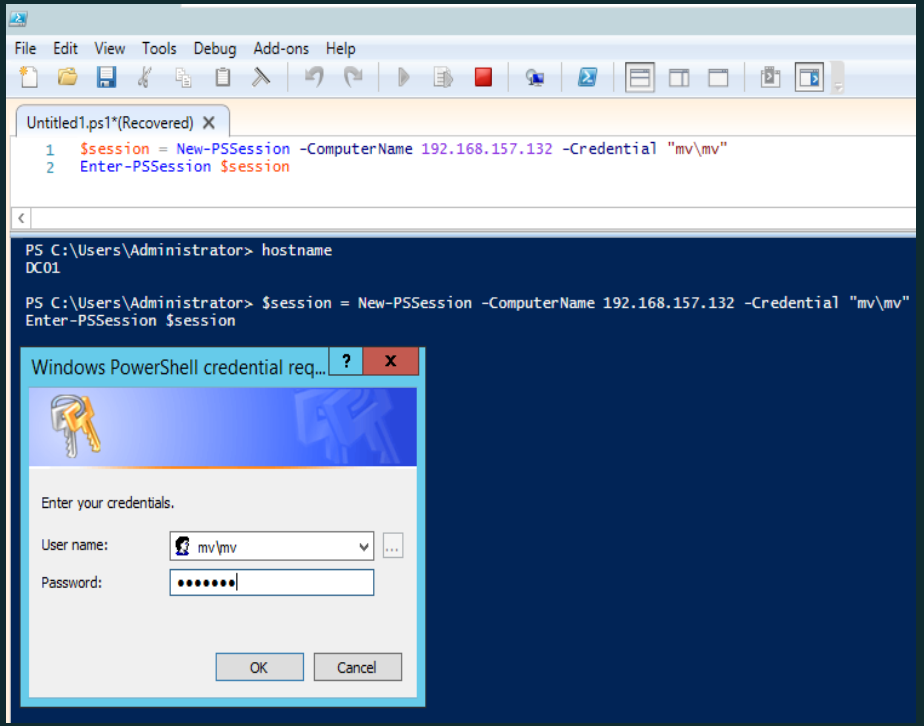
Cenário 4 – Logon TS/RDP

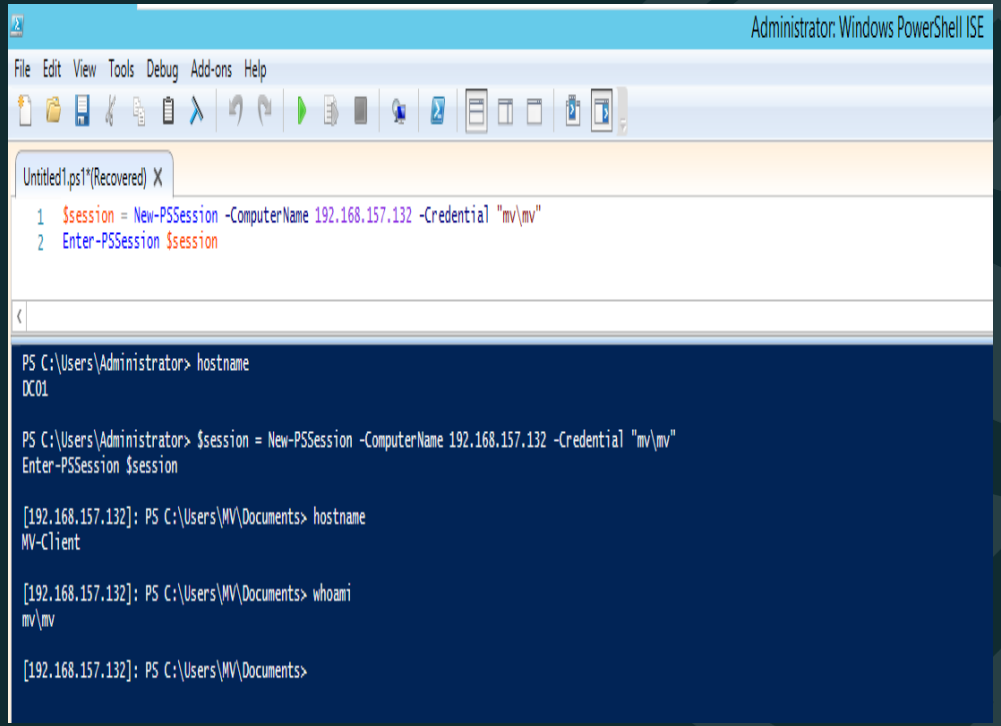


Cenário 4 – Logon TS/RDP

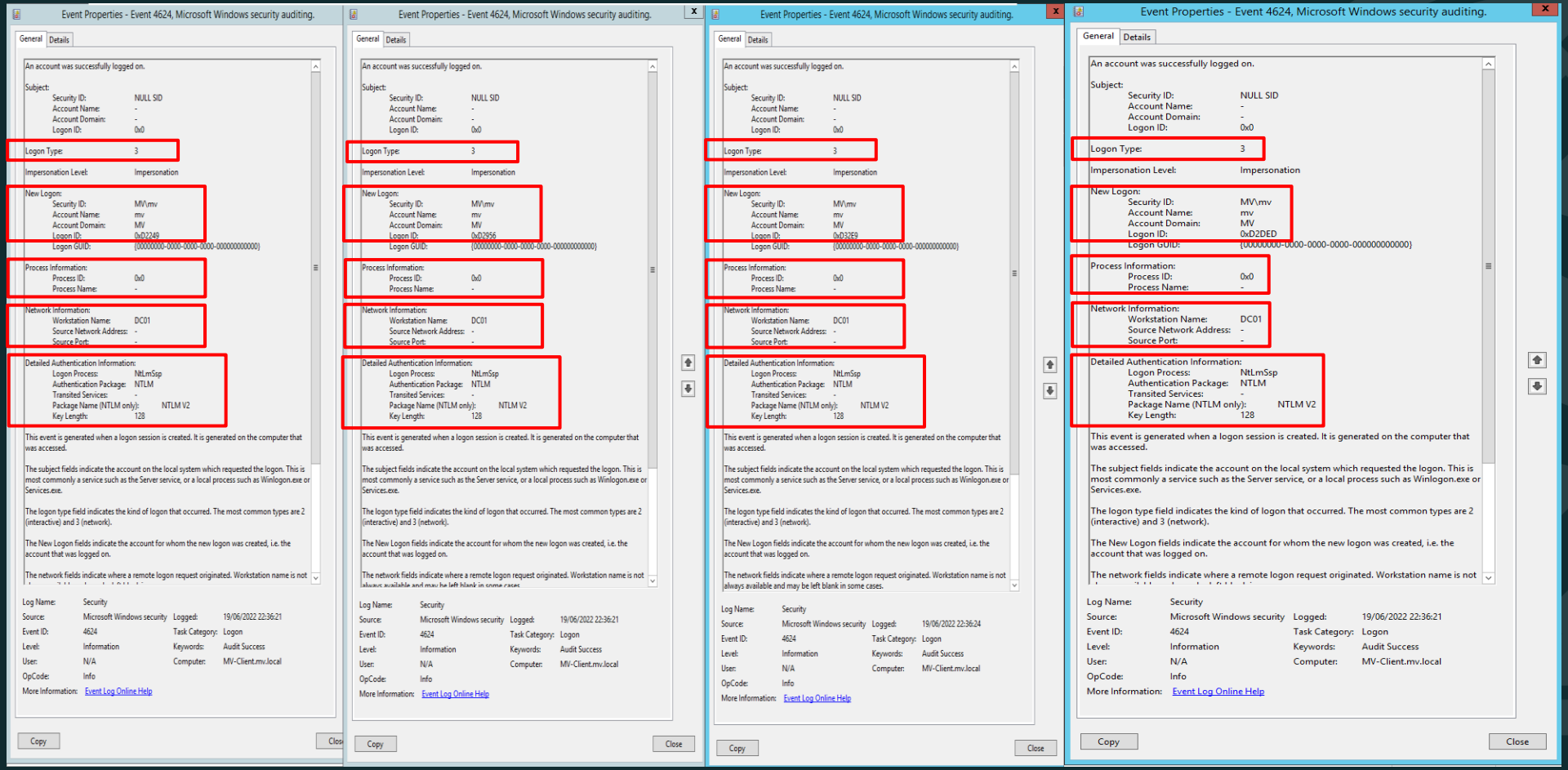


Cenário 5 – Logon powershell session

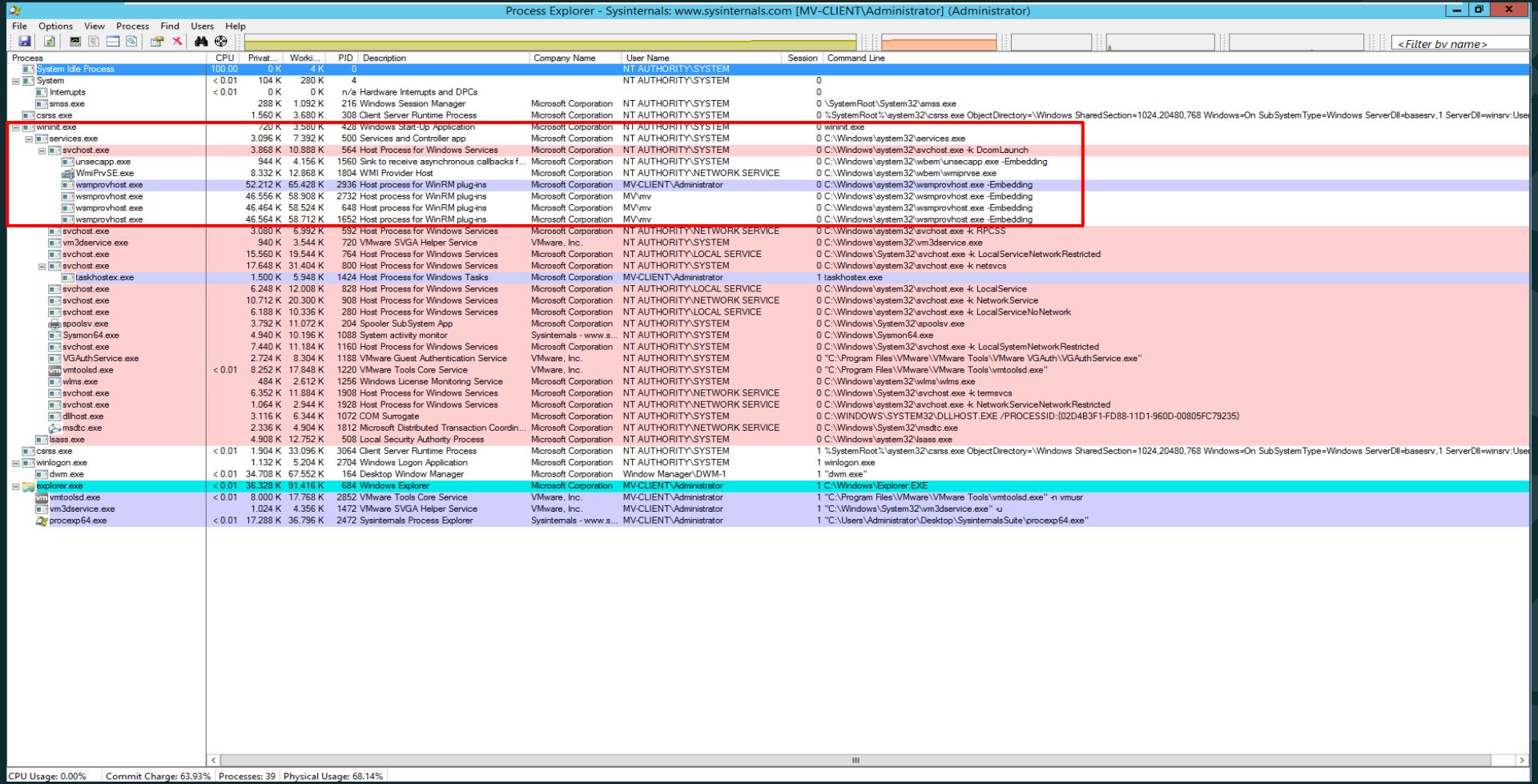




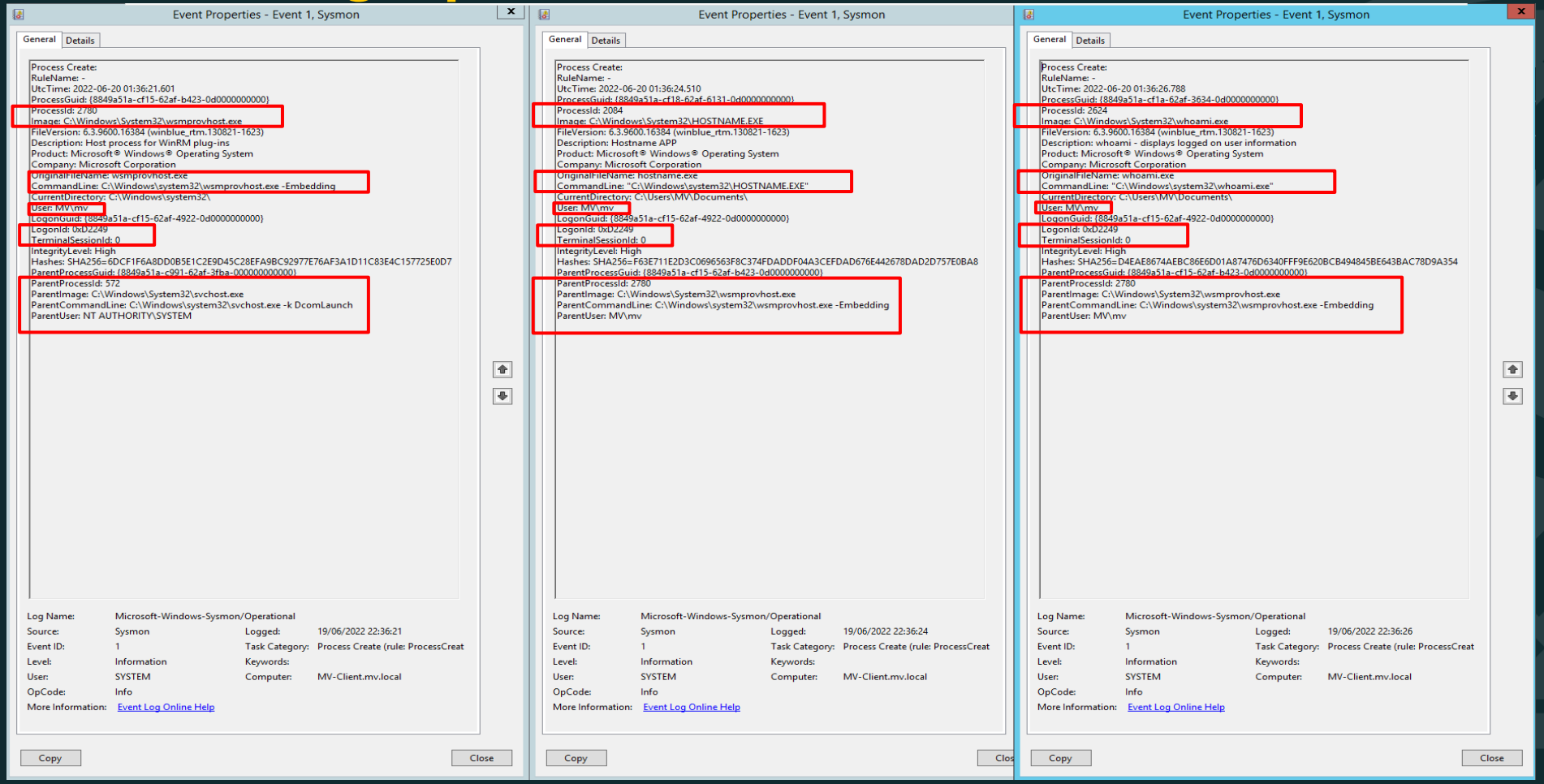
Cenário 5 – Logon powershell session



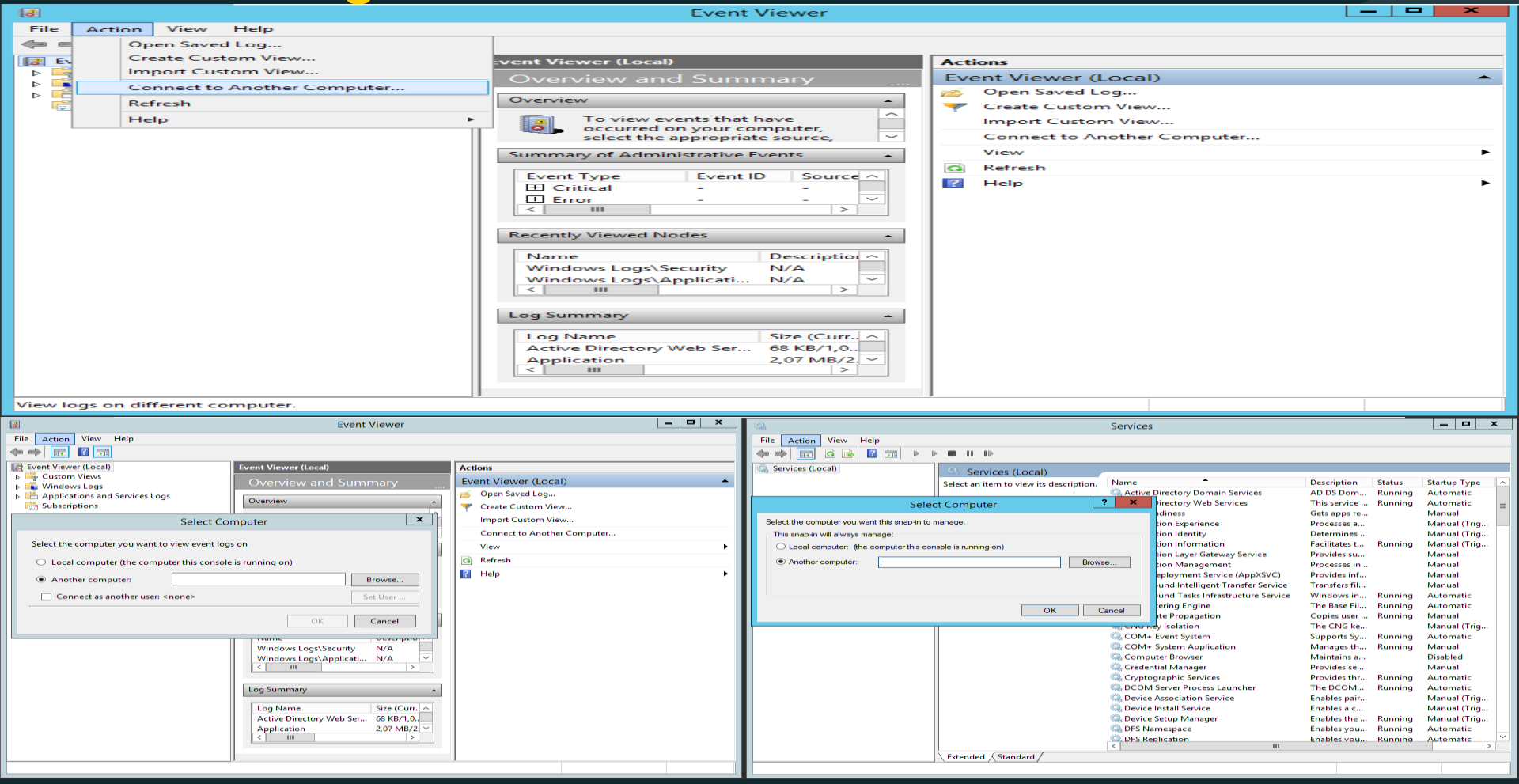
Cenário 5 – Logon powershell session



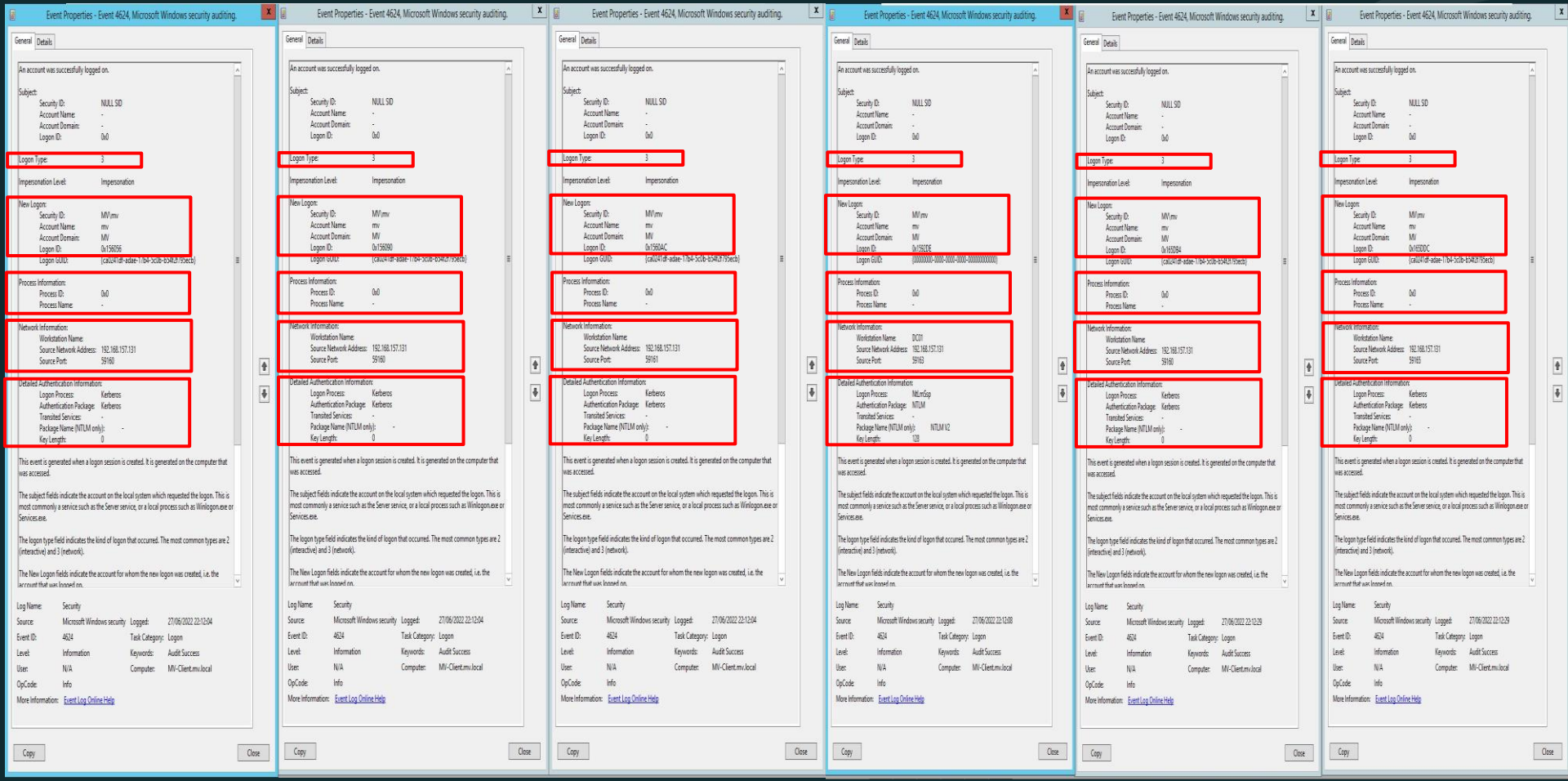
Cenário 5 – Logon powershell session



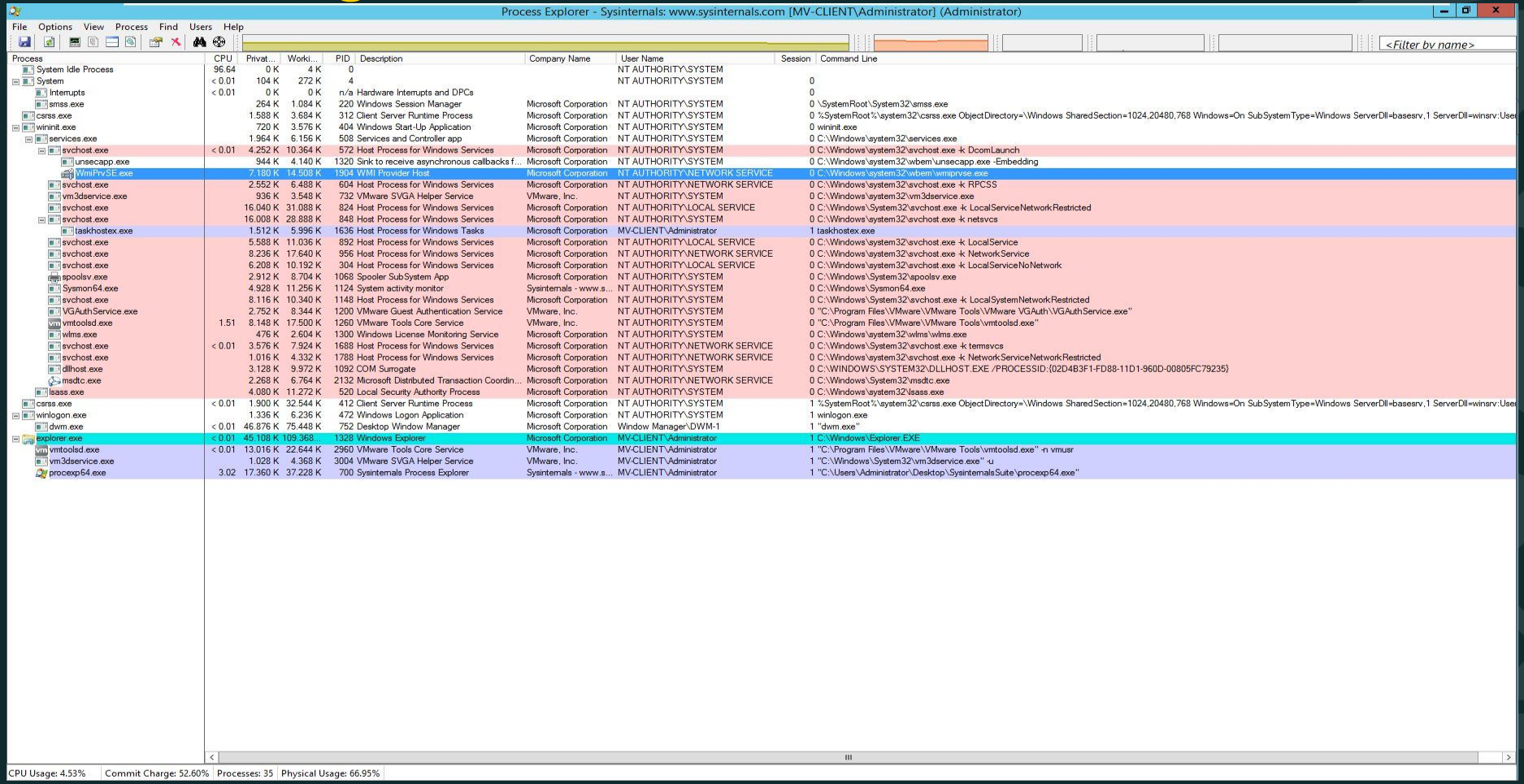
Cenário 6 – Logon services ou eventviewer



Cenário 6 – Logon services ou eventviewer



Cenário 6 – Logon services ou eventviewer

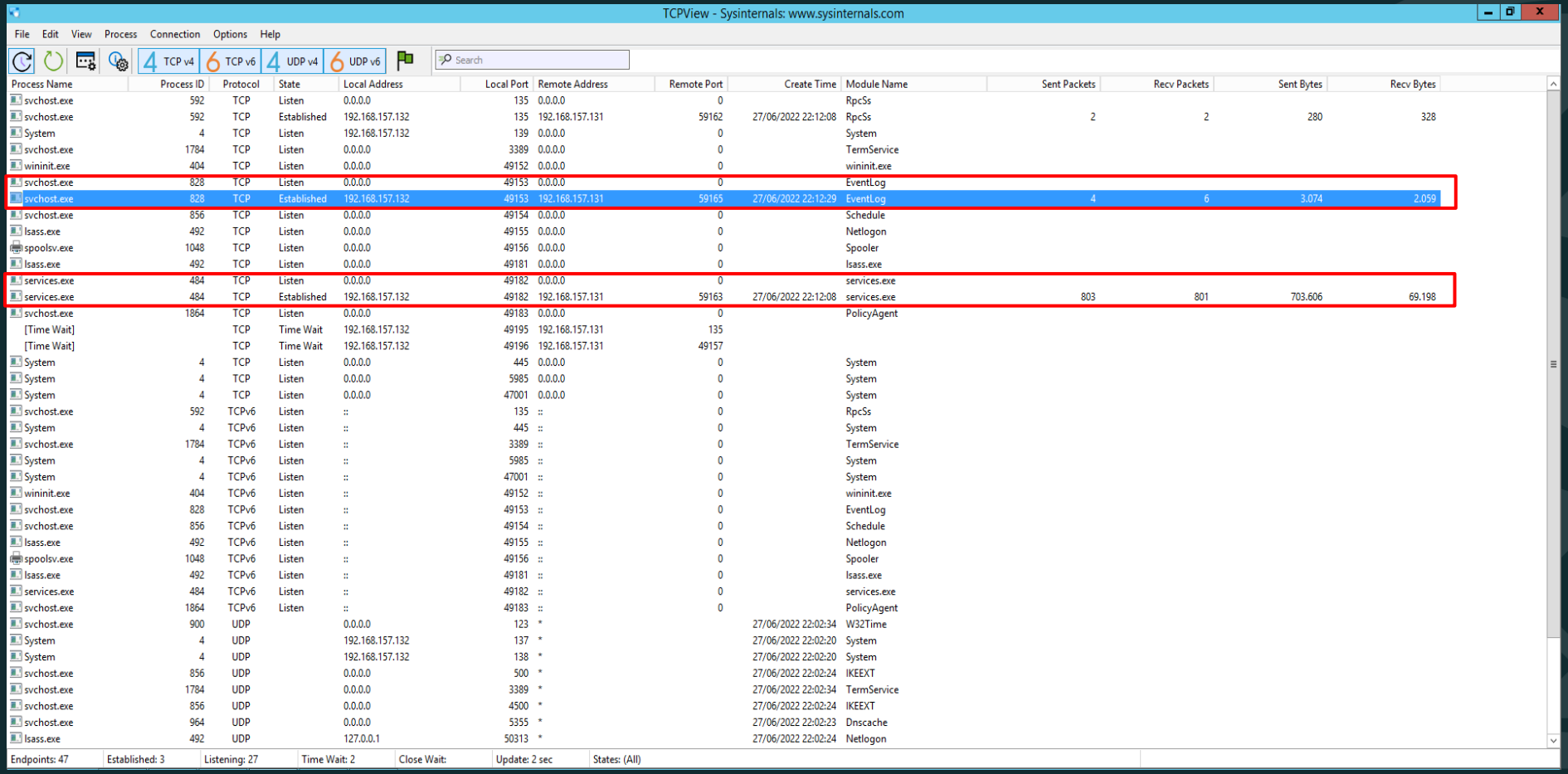


Cenário 6 – Logon services ou eventviewer

E agora o que fazer?

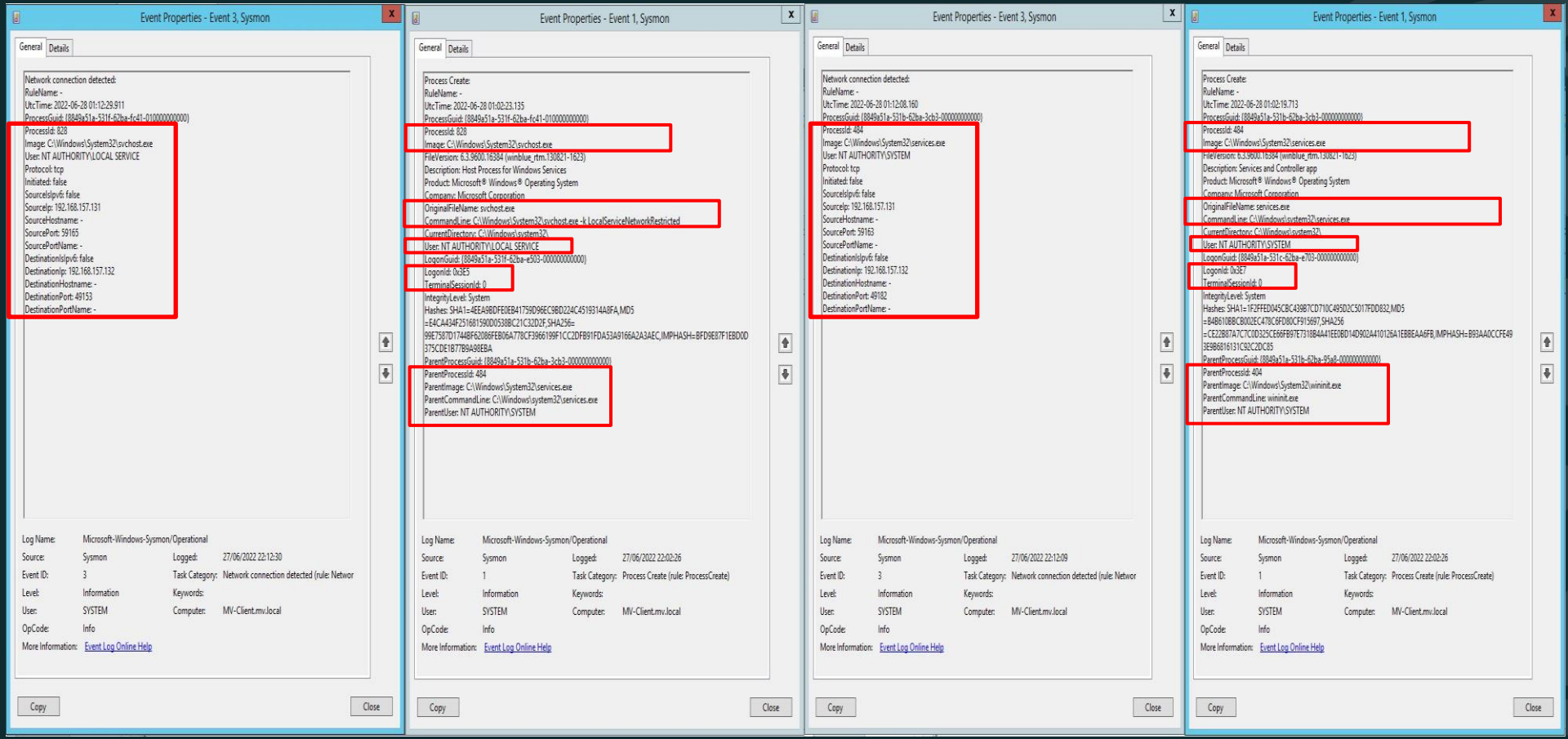
Os processos não mudaram e o log de logon não diz que recurso foi acessado

Cenário 6 – Logon services ou eventviewer



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets	Sent Bytes	Recv Bytes
svchost.exe	592	TCP	Listen	0.0.0.0	135	0.0.0.0	0		RpcSs				
svchost.exe	592	TCP	Established	192.168.157.132	135	192.168.157.131	59162	27/06/2022 22:12:08	RpcSs	2	2	280	328
System	4	TCP	Listen	192.168.157.132	139	0.0.0.0	0		System				
svchost.exe	1784	TCP	Listen	0.0.0.0	3389	0.0.0.0	0		TermService				
wininit.exe	404	TCP	Listen	0.0.0.0	49152	0.0.0.0	0		wininit.exe				
svchost.exe	828	TCP	Listen	0.0.0.0	49153	0.0.0.0	0		EventLog				
svchost.exe	828	TCP	Established	192.168.157.132	49153	192.168.157.131	59165	27/06/2022 22:12:29	EventLog	4	6	3.074	2.059
svchost.exe	856	TCP	Listen	0.0.0.0	49154	0.0.0.0	0		Schedule				
lsass.exe	492	TCP	Listen	0.0.0.0	49155	0.0.0.0	0		Netlogon				
spoolsv.exe	1048	TCP	Listen	0.0.0.0	49156	0.0.0.0	0		Spooler				
lsass.exe	492	TCP	Listen	0.0.0.0	49181	0.0.0.0	0		lsass.exe				
services.exe	484	TCP	Listen	0.0.0.0	49182	0.0.0.0	0		services.exe				
services.exe	484	TCP	Established	192.168.157.132	49182	192.168.157.131	59163	27/06/2022 22:12:08	services.exe	803	801	703.606	69.198
svchost.exe	1864	TCP	Listen	0.0.0.0	49183	0.0.0.0	0		PolicyAgent				
[Time Wait]		TCP	Time Wait	192.168.157.132	49195	192.168.157.131	135						
[Time Wait]		TCP	Time Wait	192.168.157.132	49196	192.168.157.131	49157						
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0		System				
System	4	TCP	Listen	0.0.0.0	5985	0.0.0.0	0		System				
System	4	TCP	Listen	0.0.0.0	47001	0.0.0.0	0		System				
svchost.exe	592	TCPv6	Listen	::	135	::	0		RpcSs				
System	4	TCPv6	Listen	::	445	::	0		System				
svchost.exe	1784	TCPv6	Listen	::	3389	::	0		TermService				
System	4	TCPv6	Listen	::	5985	::	0		System				
System	4	TCPv6	Listen	::	47001	::	0		System				
wininit.exe	404	TCPv6	Listen	::	49152	::	0		wininit.exe				
svchost.exe	828	TCPv6	Listen	::	49153	::	0		EventLog				
svchost.exe	856	TCPv6	Listen	::	49154	::	0		Schedule				
lsass.exe	492	TCPv6	Listen	::	49155	::	0		Netlogon				
spoolsv.exe	1048	TCPv6	Listen	::	49156	::	0		Spooler				
lsass.exe	492	TCPv6	Listen	::	49181	::	0		lsass.exe				
services.exe	484	TCPv6	Listen	::	49182	::	0		services.exe				
svchost.exe	1864	TCPv6	Listen	::	49183	::	0		PolicyAgent				
svchost.exe	900	UDP		0.0.0.0	123	*		27/06/2022 22:02:34	W32Time				
System	4	UDP		192.168.157.132	137	*		27/06/2022 22:02:20	System				
System	4	UDP		192.168.157.132	138	*		27/06/2022 22:02:20	System				
svchost.exe	856	UDP		0.0.0.0	500	*		27/06/2022 22:02:24	IKEEXT				
svchost.exe	1784	UDP		0.0.0.0	3389	*		27/06/2022 22:02:34	TermService				
svchost.exe	856	UDP		0.0.0.0	4500	*		27/06/2022 22:02:24	IKEEXT				
svchost.exe	964	UDP		0.0.0.0	5355	*		27/06/2022 22:02:23	Dnscache				
lsass.exe	492	UDP		127.0.0.1	50313	*		27/06/2022 22:02:24	Netlogon				

Cenário 6 – Logon services ou eventviewer



Conclusão

Conclusão

- **TENHA LOGS;**
- Os logs se complementam;
- Dependendo do cenário a telemetria de processos pode substituir o log de acesso;
- Os logs de telemetria de rede são úteis, desde que tenha os logs de telemetria de processos para correlacionar;
- Sempre consulte/correlacione/use mais de uma fonte de logs;
- Entender o **“porque das coisas”** pode te salvar da dependência de um log especifico e ajuda a extrair o máximo de informações;
- Façam testes e laboratórios para entender o **“porque das coisas”**.

Referências

Referências

- https://www.alteredsecurity.com/post/fantastic-windows-logon-types-and-where-to-find-credentials-in-them#viewer-f74bo
- https://techcommunity.microsoft.com/t5/itops-talk-blog/deep-dive-logging-on-to-windows/ba-p/2420705
- https://techcommunity.microsoft.com/t5/ask-the-performance-team/sessions-desktops-and-windows-stations/ba-p/372473
- https://www.ultimatewindowssecurity.com/securitylog/book/default.aspx
- https://www.sans.org/posters/hunt-evil/
- Mais referências estarão no github, junto com essa apresentação.

Dúvidas?

Dúvidas?

- Não tenham medo de mim haha
- Vejo vocês no QA

Obrigado!

telegram/mvvamo
linkedin/mvmoliveira

twitter/Marcus_mcs
github/mvvamo

MAIS UM EVENTO:
Flipside
SECURITY BEYOND TECHNOLOGY

REALIZAÇÃO:
Green Helmet

roadsec.com.br | @roadsec | *#dontstophacking*