LABORATÓRIO PESSOAL – 2
Análise de tráfego utilizando Wireshark e Zeek

Autor: Lucas Vieira Areal

Data: 12/01/2026

Repositório: https://github.com/sacullaera/Labs

Este laboratório prático foi desenvolvido para simular e analisar atividades de troubleshooting em sistema Windows e Linux, uma habilidade fundamental para profissionais de segurança da informação e Service desk. Para esse laboratório, utilizei scripts para simular problemas de lentidão, quedas no servidor SSH e scripts maliciosos (.bat e/ou .sh) em pastas compartilhadas para alteração do sistema.

As motivações do projeto foram:

- Construção de um laboratório local e isolado;
- Aperfeiçoar as habilidades de troubleshooting através de problemas cotidianos reais;
- Analisar e interpretar logs para rastreamento do problema;
- Desenvolver habilidades fundamentais para atuação em equipes de Segurança da Informação e Service Desk.

A ambientação do laboratório se dá conforme apresentado no quadro abaixo:

COMPONENTE	DETALHE
Máquina Host	**Windows 11**
Hypervisor	**VMware Workstation Pro**
VM Atacante	**Kali Linux 2025.3**
VM Vítima	**Ubuntu Server 24.04 LTS & Windows 10**
Rede	**Modo “Host-only” no VMware**
Ferramentas	**Explorador de processos, logs**

Tabela 1: Componentes do laboratório

Antes de iniciar todo o processo é importante criar um Snapshot da VM para que em qualquer situação anômala você consiga retornar antes do problema sem ter a necessidade da instalação completa da Máquina Virtual.

Troubleshooting 1 -
Lentidão do computador

Ambientação

Este laboratório simula uma situação comum em equipes de suporte de TI: um usuário relata que seu computador está apresentando lentidão significativa, sem saber a causa. Para reproduzir esse cenário de forma controlada e segura, foi criado um script PowerShell inofensivo, cujo único propósito é gerar carga artificial na CPU, sem realizar qualquer operação maliciosa ou acessar a rede. O código utilizado foi o seguinte:

```
# simulando lentidão do pc

Write-Host "Simulando alta carga de CPU... (pressione Ctrl+C para parar)"

while ($true) {

  # Cálculo inútil para consumir CPU

  $x = 1..10000 | ForEach-Object { [Math]::Pow($_, 2) }

  Start-Sleep -Milliseconds 100

}
```

O arquivo foi salvo como simulando-pc-lento.ps1 na área de trabalho do usuário. Em seguida, foi executado em segundo plano com o comando:

Start-Process powershell.exe -ArgumentList "-File C:\Users\lab3\Desktop\simulando-pc-lento.ps1" -WindowStyle Hidden

Essa abordagem simula um processo oculto consumindo recursos do sistema, replicando comportamentos que podem ocorrer tanto por erros de configuração quanto por atividades maliciosas.

Processo do troubleshooting

Ao acessar a máquina, foi possível observar sintomas claros de sobrecarga: lentidão no cursor do mouse, demora na abertura de aplicativos e até travamentos momentâneos do Windows Explorer.

A primeira etapa diagnóstica foi abrir o Gerenciador de Tarefas (Ctrl+Shift+Esc) e verificar o consumo de recursos. A CPU estava acima de 50% mesmo sem aplicativos visíveis em execução — um indicativo claro de processo anômalo.

Ao ordenar os processos por uso de CPU, identificou-se uma instância do powershell.exe consumindo mais de 30% do recurso. Isso levanta uma pergunta crítica:

“Um processo do PowerShell deveria estar rodando em segundo plano sem interação do usuário?”

A resposta, em ambientes corporativos, quase sempre é não — especialmente se não há automações legítimas configuradas.

Antes de encerrar o processo, foram coletadas informações técnicas para análise forense. Utilizando o PowerShell, executei o comando ***Get-WmiObject Win32_Process -Filter "Name='powershell.exe'" | Select-Object ProcessId, CommandLine, ExecutablePath*** e o resultado obtido foi:

ProcessId: 4156

CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -File C:\Users\lab3\Desktop\simulando-pc-lento.ps1

ExecutablePath: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Esses dados confirmam que:

- O binário é legítimo (localizado em System32);
- O script sendo executado está na área de trabalho (local incomum para scripts corporativos);
- O processo foi iniciado com um argumento específico, indicando execução automatizada.

Análise com perspectiva de segurança

Para aprofundar a investigação, foi utilizado o Process Explorer da suíte Sysinternals (Microsoft), uma ferramenta amplamente empregada por equipes de resposta a incidentes.

Com o Process Explorer executado como administrador, foram analisadas as seguintes abas:

- Image: Confirma o caminho completo do executável;
- Strings: Pode revelar comandos embutidos (útil em análise de malware);
- TCP/IP: Verifica conexões de rede ativas (nenhuma foi detectada, descartando comunicação externa).

Além disso, foi verificada a árvore de processos (quem iniciou o powershell.exe). Neste caso, o processo era filho de outro powershell.exe, sugerindo execução manual ou via script — e não um ataque clássico por macro (ex: winword.exe → powershell.exe).

Apesar disso, a execução oculta (-WindowStyle Hidden) e a localização do script na área de trabalho são indicadores de comportamento suspeito em ambientes corporativos, merecendo investigação adicional.

Resolução do problema

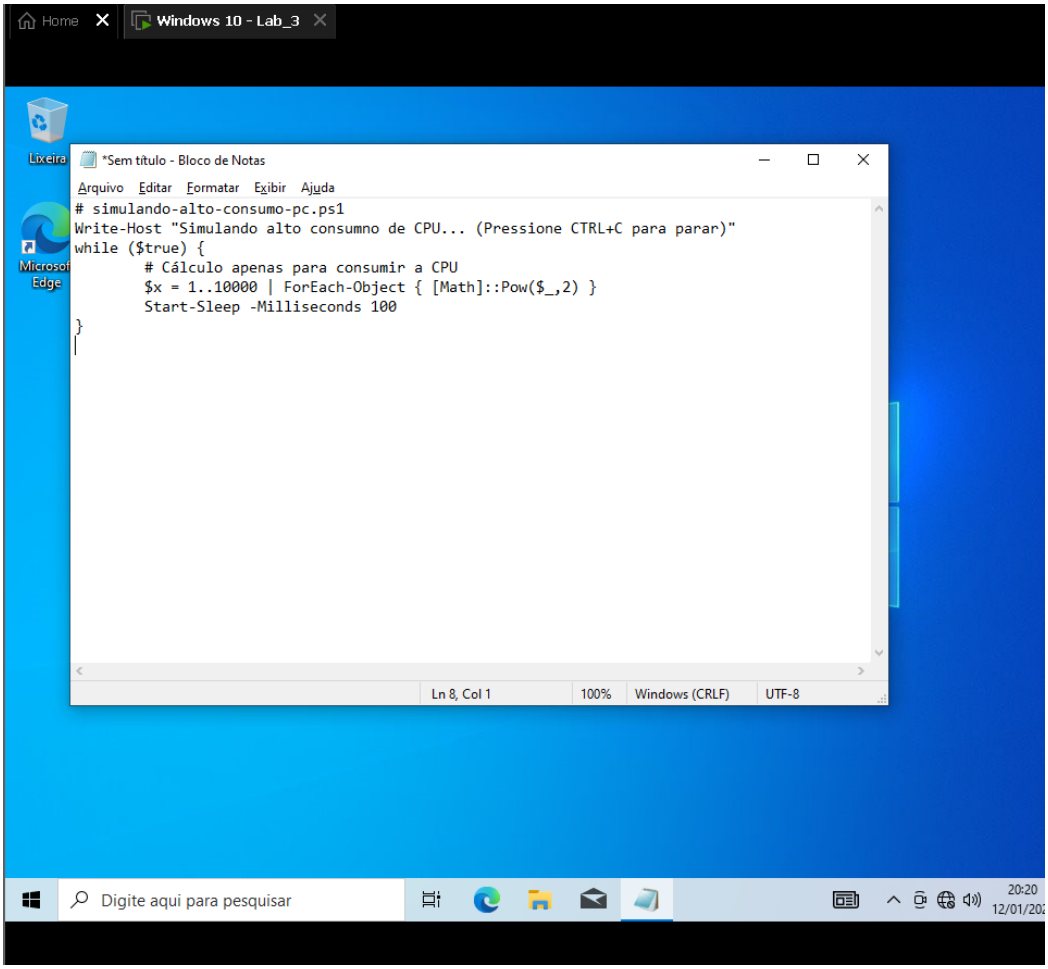
Após coleta e análise das evidências, o processo foi encerrado com segurança. Três métodos estavam disponíveis:

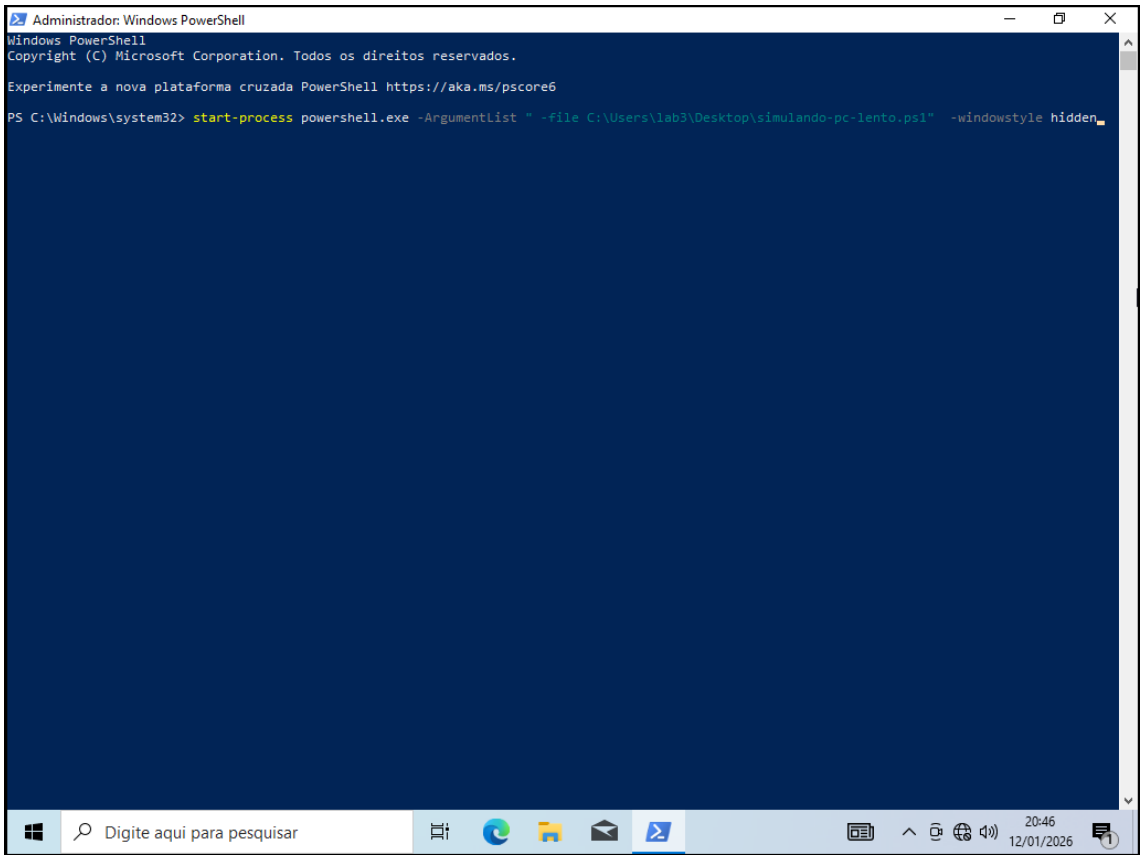
- Via PowerShell: Stop-Process -Id 4156;
- Via Gerenciador de Tarefas;
- Via Process Explorer (botão direito → Kill Process).

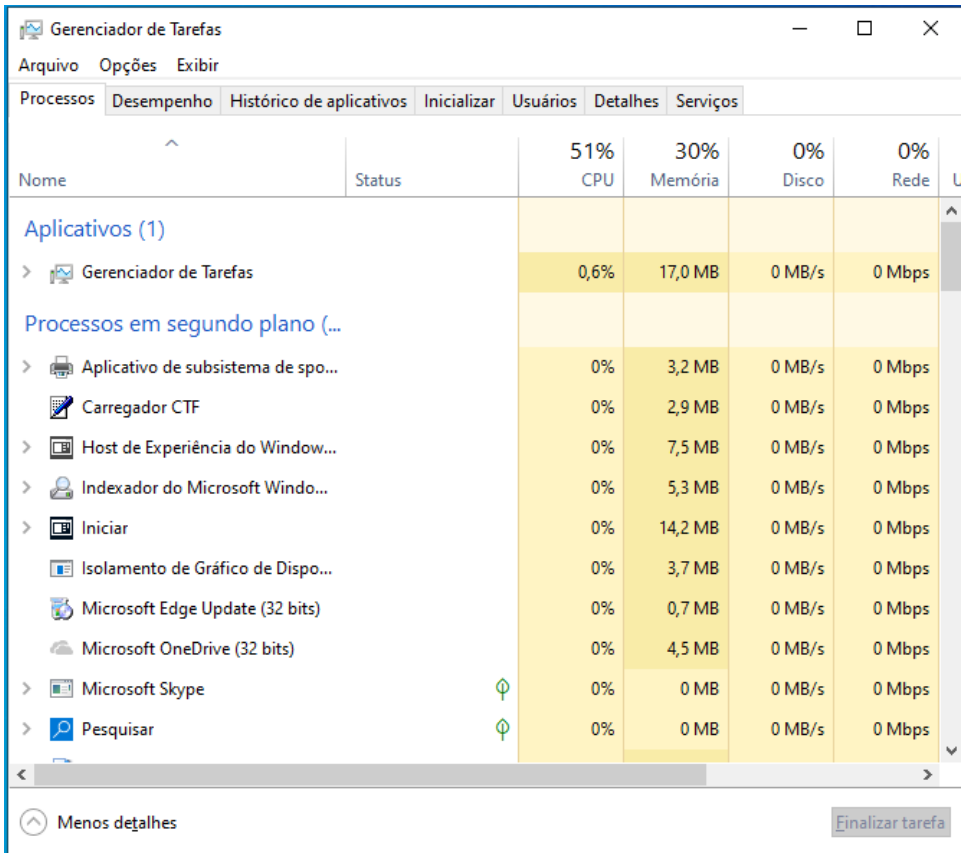
Optei pelo Process Explorer, já aberto para análise, garantindo que o processo fosse terminado de forma limpa.

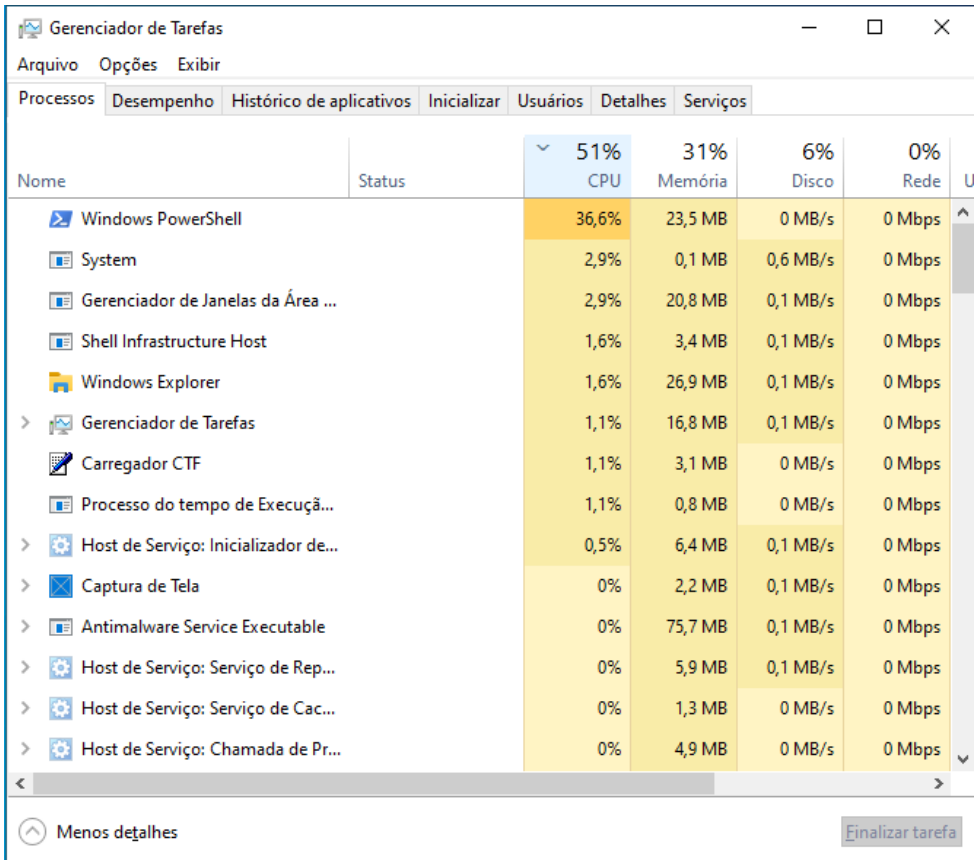
Após o encerramento, o consumo de CPU retornou ao normal e a performance do sistema foi totalmente restaurada. Por fim, o script foi removido da área de trabalho para evitar reexecução acidental.

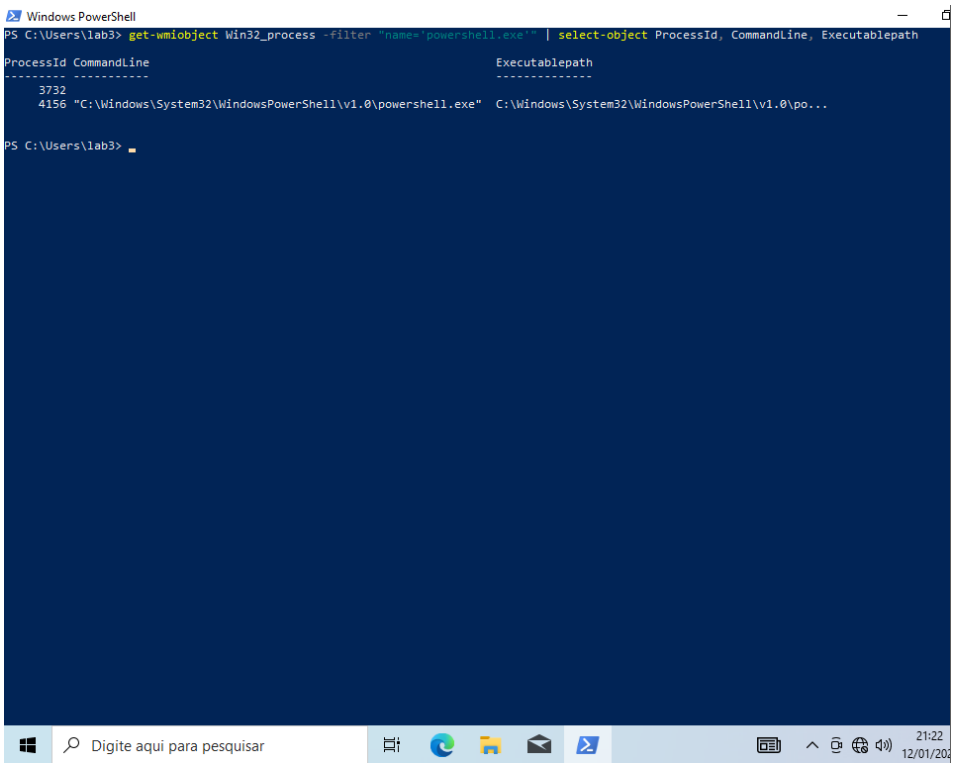
Prints do passo a passo

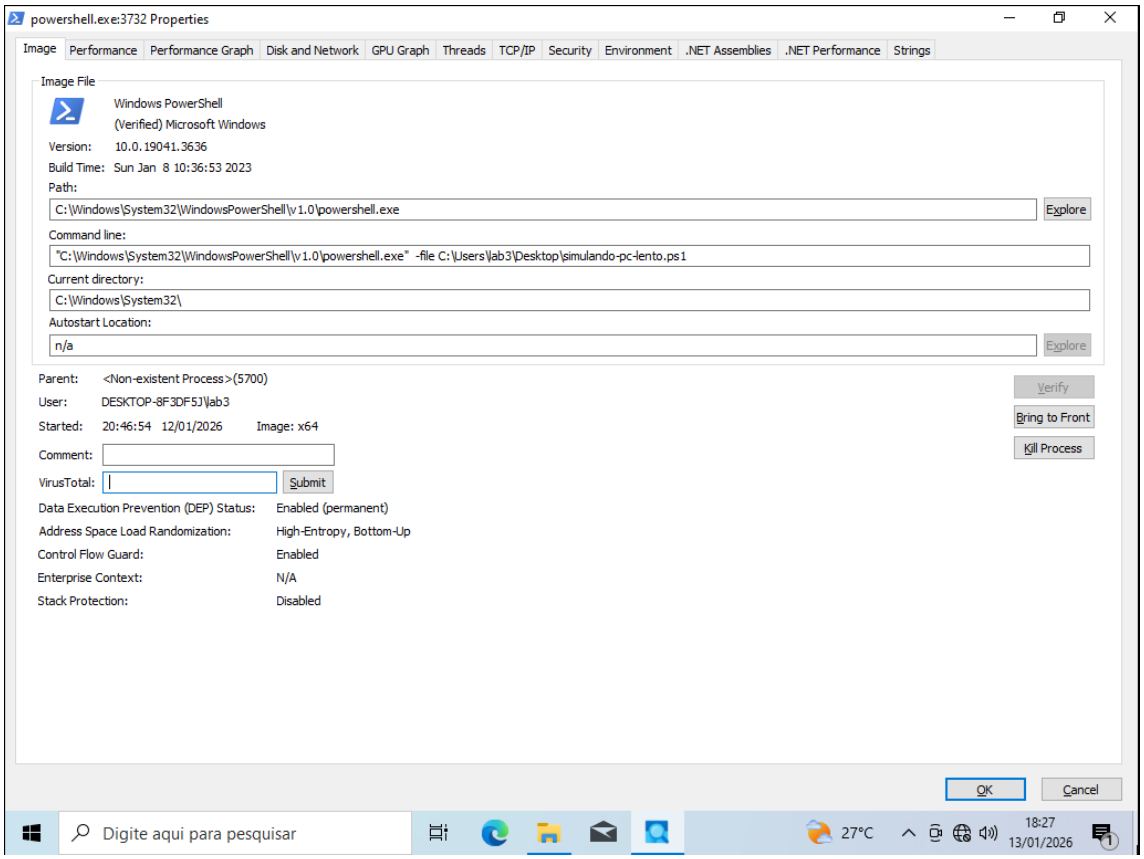


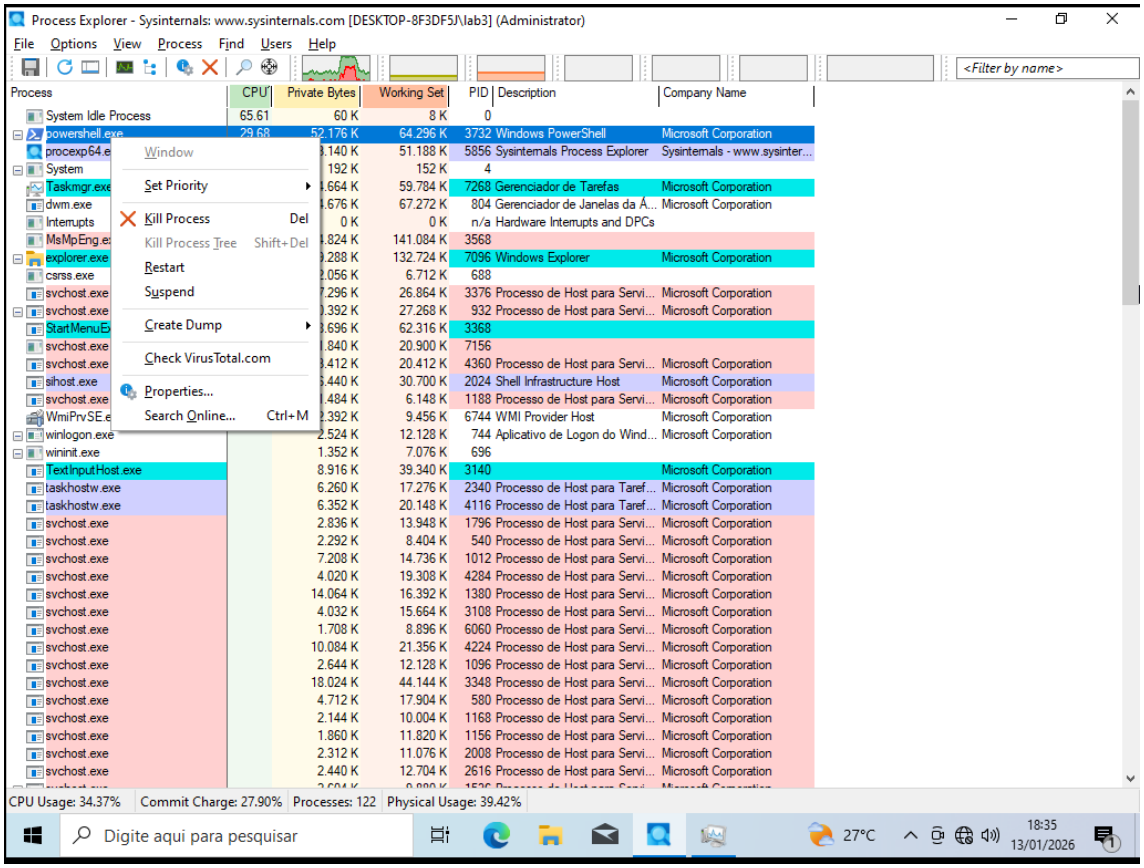

Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.
Experimente a nova plataforma cruzada PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> start-process powershell.exe -ArgumentList " -file C:\Users\lab3\Desktop\simulando-pc-lento.ps1" -windowstyle hidden
Digite aqui para pesquisar
20:46
12/01/2026

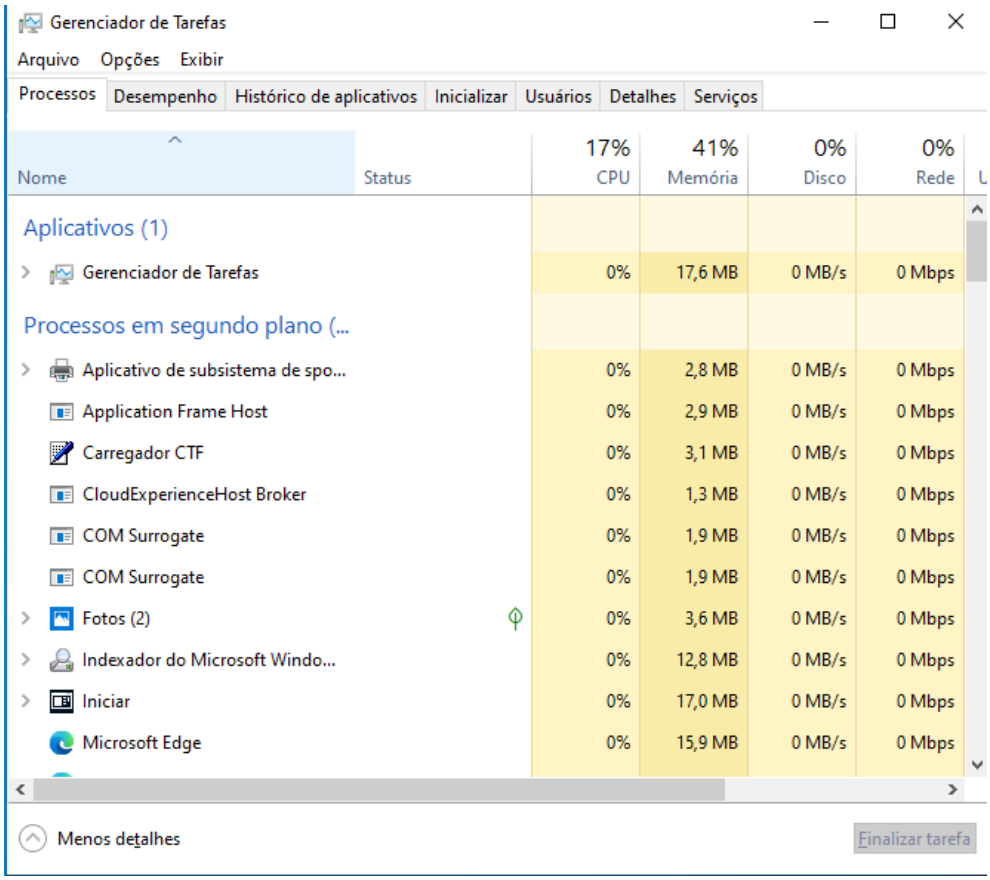

Gerenciador de Tarefas
Arquivo Opções Exibir
Processos Desempenho Histórico de aplicativos Inicializar Usuários Detalhes Serviços
Nome Status 51% CPU 30% Memória 0% Disco 0% Rede
Aplicativos (1)
Gerenciador de Tarefas 0,6% 17,0 MB 0 MB/s 0 Mbps
Processos em segundo plano (...
Aplicativo de subsistema de spo... 0% 3,2 MB 0 MB/s 0 Mbps
Carregador CTF 0% 2,9 MB 0 MB/s 0 Mbps
Host de Experiência do Window... 0% 7,5 MB 0 MB/s 0 Mbps
Indexador do Microsoft Windo... 0% 5,3 MB 0 MB/s 0 Mbps
Iniciar 0% 14,2 MB 0 MB/s 0 Mbps
Isolamento de Gráfico de Dispo... 0% 3,7 MB 0 MB/s 0 Mbps
Microsoft Edge Update (32 bits) 0% 0,7 MB 0 MB/s 0 Mbps
Microsoft OneDrive (32 bits) 0% 4,5 MB 0 MB/s 0 Mbps
Microsoft Skype 0% 0 MB 0 MB/s 0 Mbps
Pesquisar 0% 0 MB 0 MB/s 0 Mbps
Menos detalhes
Finalizar tarefa


Gerenciador de Tarefas
Arquivo Opções Exibir
Processos Desempenho Histórico de aplicativos Inicializar Usuários Detalhes Serviços
Nome Status 51% CPU 31% Memória 6% Disco 0% Rede
Windows PowerShell 36,6% 23,5 MB 0 MB/s 0 Mbps
System 2,9% 0,1 MB 0,6 MB/s 0 Mbps
Gerenciador de Janelas da Área ... 2,9% 20,8 MB 0,1 MB/s 0 Mbps
Shell Infrastructure Host 1,6% 3,4 MB 0,1 MB/s 0 Mbps
Windows Explorer 1,6% 26,9 MB 0,1 MB/s 0 Mbps
Gerenciador de Tarefas 1,1% 16,8 MB 0,1 MB/s 0 Mbps
Carregador CTF 1,1% 3,1 MB 0 MB/s 0 Mbps
Processo do tempo de Execuçã... 1,1% 0,8 MB 0 MB/s 0 Mbps
Host de Serviço: Inicializador de... 0,5% 6,4 MB 0,1 MB/s 0 Mbps
Captura de Tela 0% 2,2 MB 0,1 MB/s 0 Mbps
Antimalware Service Executable 0% 75,7 MB 0,1 MB/s 0 Mbps
Host de Serviço: Serviço de Rep... 0% 5,9 MB 0,1 MB/s 0 Mbps
Host de Serviço: Serviço de Cac... 0% 1,3 MB 0 MB/s 0 Mbps
Host de Serviço: Chamada de Pr... 0% 4,9 MB 0 MB/s 0 Mbps
Menos detalhes
Finalizar tarefa


Windows PowerShell
PS C:\Users\lab3> get-wmiobject Win32_process -filter "name='powershell.exe'" | select-object ProcessId, CommandLine, Executablepath
ProcessId CommandLine Executablepath
3732
4156 "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" C:\Windows\System32\WindowsPowerShell\v1.0\po...
PS C:\Users\lab3>
Digite aqui para pesquisar
21:22


powershell.exe:3732 Properties
Image
Performance
Performance Graph
Disk and Network
GPU Graph
Threads
TCP/IP
Security
Environment
.NET Assemblies
.NET Performance
Strings
Image File
Windows PowerShell
(Verified) Microsoft Windows
Version: 10.0.19041.3636
Build Time: Sun Jan 8 10:36:53 2023
Path:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Explore
Command line:
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -file C:\Users\lab3\Desktop\simulando-pc-lento.ps1
Current directory:
C:\Windows\System32\
Autostart Location:
n/a
Explore
Parent: <Non-existent Process>(5700)
User: DESKTOP-8F3DF5J\lab3
Started: 20:46:54 12/01/2026 Image: x64
Comment:
VirusTotal:
Submit
Verify
Bring to Front
Kill Process
Data Execution Prevention (DEP) Status: Enabled (permanent)
Address Space Load Randomization: High-Entropy, Bottom-Up
Control Flow Guard: Enabled
Enterprise Context: N/A
Stack Protection: Disabled
OK
Cancel
Digite aqui para pesquisar
27°C
18:27
13/01/2026


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-8F3DF5J\lab3] (Administrator)
File Options View Process Find Users Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name
System Idle Process 65.61 60 K 8 K 0
powershell.exe 29.68 52.176 K 64.296 K 3732 Windows PowerShell Microsoft Corporation
procexp64.e 3.140 K 51.188 K 5856 Sysinternals Process Explorer Sysinternals - www.sysinter...
System 192 K 152 K 4
Taskmgr.exe 4.664 K 59.784 K 7268 Gerenciador de Tarefas Microsoft Corporation
dwm.exe 4.676 K 67.272 K 804 Gerenciador de Janelas da Á... Microsoft Corporation
Interrupts 0 K 0 K n/a Hardware Interrupts and DPCs
MsMpEng.e 4.824 K 141.084 K 3568
explorer.exe 9.288 K 132.724 K 7096 Windows Explorer Microsoft Corporation
csrss.exe 2.056 K 6.712 K 688
svchost.exe 7.296 K 26.864 K 3376 Processo de Host para Servi... Microsoft Corporation
svchost.exe 0.392 K 27.268 K 932 Processo de Host para Servi... Microsoft Corporation
StartMenuEx 3.696 K 62.316 K 3368
svchost.exe 1.840 K 20.900 K 7156
svchost.exe 3.412 K 20.412 K 4360 Processo de Host para Servi... Microsoft Corporation
sihost.exe 5.440 K 30.700 K 2024 Shell Infrastructure Host Microsoft Corporation
svchost.exe 1.484 K 6.148 K 1188 Processo de Host para Servi... Microsoft Corporation
WmiPrvSE.e 2.392 K 9.456 K 6744 WMI Provider Host Microsoft Corporation
winlogon.exe 2.524 K 12.128 K 744 Aplicativo de Logon do Wind... Microsoft Corporation
wininit.exe 1.352 K 7.076 K 696
TextInputHost.exe 8.916 K 39.340 K 3140 Microsoft Corporation
taskhostw.exe 6.260 K 17.276 K 2340 Processo de Host para Taref... Microsoft Corporation
taskhostw.exe 6.352 K 20.148 K 4116 Processo de Host para Taref... Microsoft Corporation
svchost.exe 2.836 K 13.948 K 1796 Processo de Host para Servi... Microsoft Corporation
svchost.exe 2.292 K 8.404 K 540 Processo de Host para Servi... Microsoft Corporation
svchost.exe 7.208 K 14.736 K 1012 Processo de Host para Servi... Microsoft Corporation
svchost.exe 4.020 K 19.308 K 4284 Processo de Host para Servi... Microsoft Corporation
svchost.exe 14.064 K 16.392 K 1380 Processo de Host para Servi... Microsoft Corporation
svchost.exe 4.032 K 15.664 K 3108 Processo de Host para Servi... Microsoft Corporation
svchost.exe 1.708 K 8.896 K 6060 Processo de Host para Servi... Microsoft Corporation
svchost.exe 10.084 K 21.356 K 4224 Processo de Host para Servi... Microsoft Corporation
svchost.exe 2.644 K 12.128 K 1096 Processo de Host para Servi... Microsoft Corporation
svchost.exe 18.024 K 44.144 K 3348 Processo de Host para Servi... Microsoft Corporation
svchost.exe 4.712 K 17.904 K 580 Processo de Host para Servi... Microsoft Corporation
svchost.exe 2.144 K 10.004 K 1168 Processo de Host para Servi... Microsoft Corporation
svchost.exe 1.860 K 11.820 K 1156 Processo de Host para Servi... Microsoft Corporation
svchost.exe 2.312 K 11.076 K 2008 Processo de Host para Servi... Microsoft Corporation
svchost.exe 2.440 K 12.704 K 2616 Processo de Host para Servi... Microsoft Corporation
Window
Set Priority
Kill Process Del
Kill Process Tree Shift+Del
Restart
Suspend
Create Dump
Check VirusTotal.com
Properties...
Search Online... Ctrl+M
CPU Usage: 34.37% Commit Charge: 27.90% Processes: 122 Physical Usage: 39.42%
Digite aqui para pesquisar
27°C
18:35
13/01/2026


Gerenciador de Tarefas
Arquivo Opções Exibir
Processos Desempenho Histórico de aplicativos Inicializar Usuários Detalhes Serviços
Nome Status 17% CPU 41% Memória 0% Disco 0% Rede
Aplicativos (1)
Gerenciador de Tarefas 0% 17,6 MB 0 MB/s 0 Mbps
Processos em segundo plano (...
Aplicativo de subsistema de spo... 0% 2,8 MB 0 MB/s 0 Mbps
Application Frame Host 0% 2,9 MB 0 MB/s 0 Mbps
Carregador CTF 0% 3,1 MB 0 MB/s 0 Mbps
CloudExperienceHost Broker 0% 1,3 MB 0 MB/s 0 Mbps
COM Surrogate 0% 1,9 MB 0 MB/s 0 Mbps
COM Surrogate 0% 1,9 MB 0 MB/s 0 Mbps
Fotos (2) 0% 3,6 MB 0 MB/s 0 Mbps
Indexador do Microsoft Windo... 0% 12,8 MB 0 MB/s 0 Mbps
Iniciar 0% 17,0 MB 0 MB/s 0 Mbps
Microsoft Edge 0% 15,9 MB 0 MB/s 0 Mbps
Menos detalhes
Finalizar tarefa