## Audite as contas que foram adicionadas ao Windows usando scripts PowerShell e em lote

A segurança é uma preocupação fundamental para qualquer sistema operacional, e o Windows não é exceção. Uma das principais preocupações é garantir que apenas as contas autorizadas tenham acesso ao sistema. Neste artigo, exploraremos como auditar as contas que foram adicionadas ao Windows usando scripts PowerShell e em lote. Essas técnicas podem ajudar a identificar atividades suspeitas e manter a integridade do sistema.

Exemplos:

1. Script PowerShell para auditar contas adicionadas: O PowerShell é uma poderosa ferramenta de automação e gerenciamento de sistemas no Windows. Abaixo está um exemplo de um script PowerShell que pode ser usado para auditar as contas adicionadas ao sistema:

```
$eventLog = Get-WinEvent -FilterHashtable @{LogName='Security';Id=4720}
$eventLog | ForEach-Object {
    $timeCreated = $_.TimeCreated
    $accountName = $_.Properties[0].Value
    $accountDomain = $_.Properties[1].Value
    $accountType = $_.Properties[2].Value
    Write-Host "Conta adicionada: $accountDomain\$accountName ($accountTyp
e) em $timeCreated"
}
```

Este script usa o cmdlet Get-WinEvent para obter eventos de segurança com o ID 4720, que indica a criação de uma nova conta. Em seguida, ele itera sobre cada evento e exibe informações relevantes, como o nome da conta, o domínio e o tipo de conta.

2. Script em lote para auditar contas adicionadas: Embora o PowerShell seja uma opção poderosa, também é possível usar scripts em lote para auditar contas adicionadas. Abaixo está um exemplo de um script em lote que pode ser usado para esse fim:

```
@echo off
for /f "tokens=1,2,3,4,5,6,7,*" %%a in ('wevtutil qe Security /q:"*[System
[(EventID=4720)]]" /rd:true /f:text') do (
    echo Conta adicionada: %%d\%%e (%%f) em %%b %%c
)
```

Este script usa o utilitário wevtutil para consultar o log de eventos de segurança em busca de

eventos com o ID 4720. Em seguida, ele itera sobre cada linha de saída e exibe as informações relevantes, como o nome da conta, o domínio e a data/hora da criação.

Conclusão: Auditar as contas adicionadas ao Windows é uma prática importante para garantir a segurança do sistema. Neste artigo, exploramos exemplos de como realizar essa auditoria usando scripts PowerShell e em lote. Essas técnicas podem ser facilmente adaptadas e incorporadas a processos de monitoramento de segurança existentes, permitindo a detecção rápida de atividades suspeitas e a proteção do ambiente Windows.