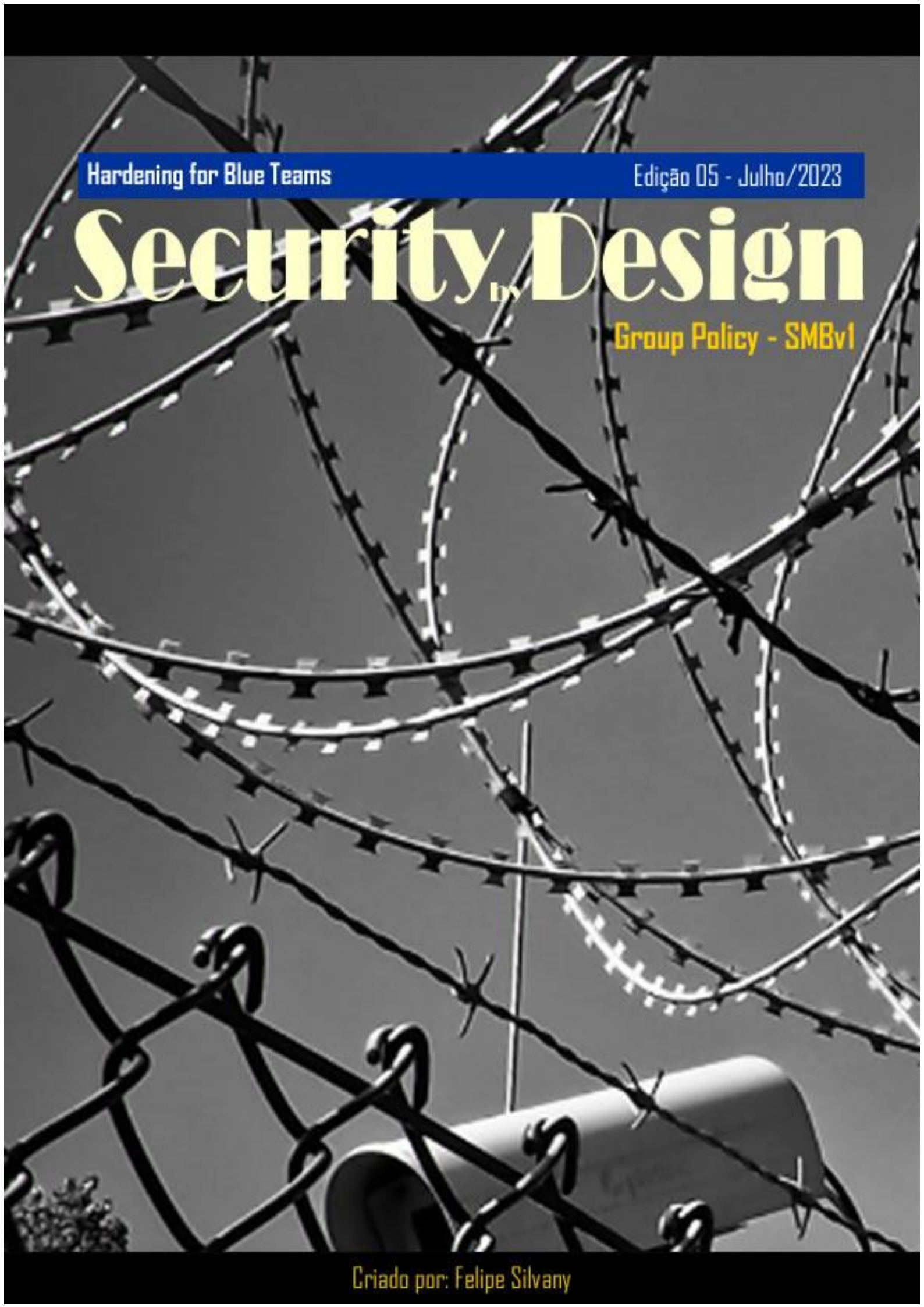


Hardening for Blue Teams

Edição 05 - Julho/2023

Security Design

Group Policy - SMBv1

Criado por: Felipe Silvany

SUMÁRIO

CONFIDENCIALIDADE

Este documento contém informações confidenciais ou privilegiadas, sendo seu sigilo protegido por lei, não sendo autorizado o uso, cópia ou divulgação das informações ou tomar qualquer ação baseada nessas informações.

Desta forma, os destinatários destes documentos comprometem-se em:

1. Não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros.
2. Não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso.
3. Não apropriar-se de material confidencial e/ou sigiloso da tecnologia que venha a ser disponível.
4. Não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

SOBRE O AUTOR

Felipe Silvany é coordenador de Cybersecurity, com 21 anos de experiência na área de tecnologia, com sólidos conhecimentos em resposta à incidentes de segurança, SOC, hardering, análise de vulnerabilidades, pentest e grandes projetos de cybersecurity em ambientes onpremises, Cloud e mobile (AppSec).
Sólida experiência na implementação de soluções técnicas e estruturação de equipes de segurança de alta performance.
Responsável pela implementação de serviços, ferramentas e processos como: SOC/CSIRT 24x7, playbooks, Plano de Resposta à Incidentes de Segurança (RI), SIEM com base no MITRE ATT&CK, hardening e baselines de segurança, exercícios de RedTeam como Pentest, análise de vulnerabilidades DAST e SAST na infraestrutura onpremises/cloud (OpSec), mobiles Android e IOS (AppSec) e definição de arquitetura segura com conceitos de Zero Trust. Implementação de ferramentas de BlueTeam como: NGAv/EDR, NGFw, MTLS, NAC, DLP, IDS, IPS, WAF, AppControl, Anti-DDoS e outras.
Graduado em "Sistema de Informação", Pós Graduado em "Projetos e Gerência de Redes" e com MBA em "Gestão Empresarial Estratégica". Membro da ISO/ABNT/CE-021 000.027 (Comissão Especial de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade de dados), membro da ANPPD (Associação Nacional dos Profissionais de Privacidade de Dados) e certificado nos mais conceituados frameworks internacionais, como: ISO27001, ISO20000, ITIL, COBIT, Scrum, Kanban e outros.

Linkedin: https://www.linkedin.com/in/felipe-silvany-69241365/
Github: https://github.com/FelipeSilvany

SOBRE ESTE DOCUMENTO

Este não é um e-book comum.
Você está prestes a obter um conhecimento privilegiado em segurança da informação e hardening.
Esta obra utiliza uma metodologia focada em *Security by Design* e implementação de boas práticas de segurança desde a concepção de projetos corporativos até sua passagem para produção.
A segurança deve ser sempre preventiva e pró ativa, nunca reativa.
Nesta edição veremos boas práticas de segurança da informação e hardening na estruturação de Group Policy (GPO) em ambientes corporativos.

Edição 05 – Criação do Documento
Julho/2023 – Felipe Silvany

AGRADECIMENTOS

“Ao meu filho, Thor, que me dá toda força para enfrentar todas as dificuldades e tribulações da vida com força e ânimo. À minha esposa, Fabiana, por sempre me apoia em todos os desafios profissionais e perde várias noites de sono comigo. À minha mãe e meu pai, Maria Aparecida e Adilton, por terem me dado a maior herança que um homem por ter, o estudo. À Deus, que por intermédio do meu Senhor Jesus Cristo conduz a minha vida, me guia e me guarda.” **– Felipe Silvany**

1 - INTRODUÇÃO

O SMBv1 (Server Message Block versão 1) é um protocolo antigo usado para compartilhar arquivos em rede.

Em 2017, o ransomware WannaCry usou o exploit "*EternalBlue SMB*" desenvolvido pela NSA para se propagar rapidamente em todo o mundo, explorando a versão 1 do SMB.

Embora a Microsoft afirme que os ataques de WannaCry, Petya e similares, não tenham influenciado a decisão, a Microsoft decidiu desativar o protocolo SMBv1 por padrão.

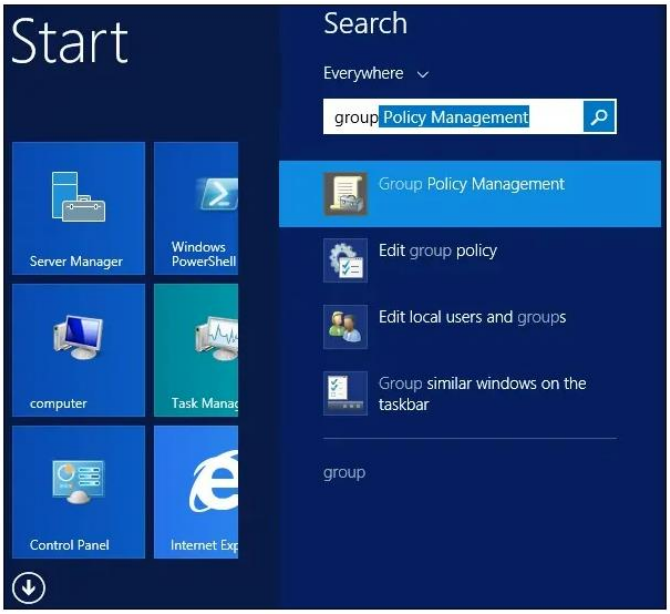
> ⓘ **Importante**
>
> É altamente recomendável que você não reinstale o SMBv1. Isso ocorre porque esse protocolo mais antigo tem problemas de segurança conhecidos relacionados a ransomware e outros malwares.

É importante que o protocolo SMBv1 esteja desativado mandatoriamente em todas as estações e servidores de sua Empresa, e a forma mais fácil de realizar ou replicar configurações mandatórias de segurança em um ambiente corporativo é através de Políticas de Grupo (Group Policy).

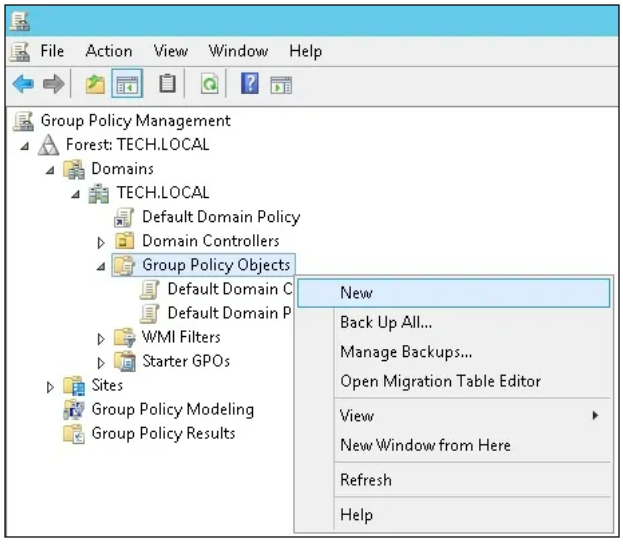
A seguir, veremos passo-a-passo como criar uma Política para desativar o SMBv1 em todo ambiente.

2 – CRIANDO A GPO

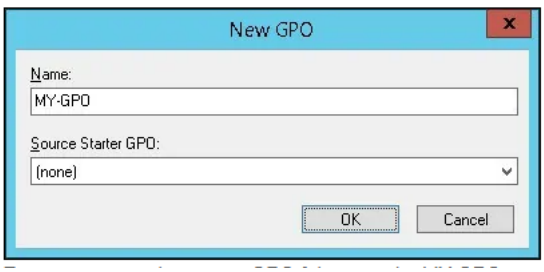
No controlador de domínio, abra a ferramenta de gerenciamento de políticas de grupo.



Crie uma nova política de grupo.



Digite um nome para a nova política do grupo.



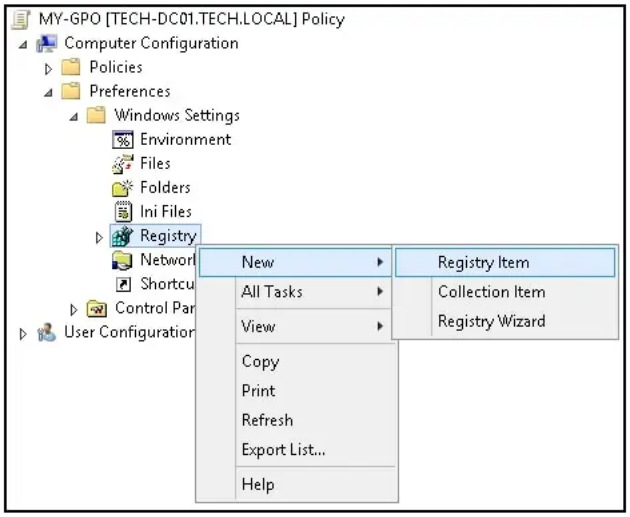
Neste exemplo, estamos chamado a GPO criada de: *MY-GPO.*

Na tela Gerenciamento de Políticas de Grupo, expanda a pasta chamada *Group Policy Objects.*

Clique com o botão direito do mouse no novo Objeto de Política de Grupo e selecione a opção *Edit*.

Na tela do editor de política do grupo, expanda a pasta de configuração do computador e localize o seguinte item: *Computer Configuration > Preferences > Windows Settings > Registry*

Clique com o botão direito do mouse na opção *Registry* e crie uma entrada de registro.



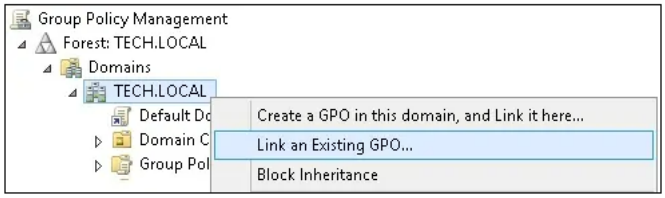
Na janela de registro, execute a seguinte configuração:

- *Action: Create*
- *Hive: HKEY_LOCAL_MACHINE*
- *Key Path: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters*
- *Value name: SMB1*
- *Value type: REG_DWORD*
- *Value data: 0*
- *Clique no botão OK.*

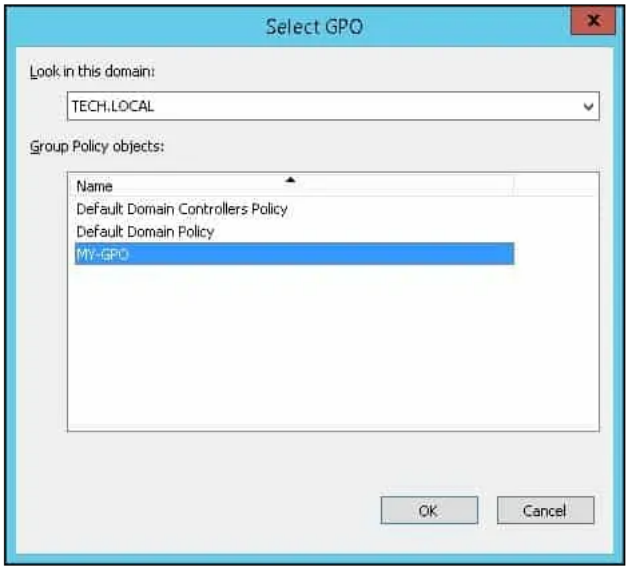
Para salvar a configuração da política de grupo, você precisa clicar em *Apply* e fechar o editor de Política de Grupo.

3 – APLICANDO A GPO NO DOMÍNIO

Na tela de gerenciamento de políticas do Grupo, clique com o botão direito do mouse na Unidade Organizacional desejada e selecionar a opção *Link na Existing GPO*.



Em nosso exemplo, vamos vincular a política de grupo chamada *MY-GPO* à raiz do domínio.



Após vinculação da política, clique em *OK* e aguarde o tempo de replicação entre dos demais controladores de domínio que pode durar aproximadamente 20 minutos.

4 – LEITURA COMPLEMENTAR

- https://www.gov.br/ctir/pt-br/centrais-de-conteudo/publicacoes/alertas/2017/alerta_2017_02_ransomwarewncry.pdf
- https://learn.microsoft.com/pt-br/security-updates/securityadvisories/2009/973811
- https://support.microsoft.com/pt-br/topic/ms16-114-atualiza%C3%A7%C3%A3o-de-seguran%C3%A7a-para-windows-smbv1-server-ter%C3%A7a-feira-13-de-setembro-de-2016-c10c1af1-5992-1e4a-264e-4c0ed082a3a4