LAB 03 | Hardening e linha de base

Registre controles fundamentais de um host próprio com foco em atualizações, contas, serviços e evidências.

Uso exclusivo em ambiente próprio, isolado ou expressamente autorizado. Materiais e endereços de teste são fictícios.

Objetivos de aprendizagem

- Definir uma linha de base segura para sistema próprio
- Verificar presença de atualizações, firewall e registros
- Priorizar correções observadas sem automatizar alterações destrutivas

Procedimento passo a passo

01 Estabelecer escopo

Escolha um Windows ou Linux de teste, registre sistema, versão, função, data e responsável.

02 Verificar atualizações

Confirme o estado das atualizações por ferramentas administrativas nativas do sistema. Registre evidência sem expor informações sensíveis.

03 Revisar contas e privilégios

Liste contas e perfis administrativos de teste. Verifique contas desnecessárias e documente alternativas de menor privilégio.

04 Revisar serviços e firewall

Mapeie serviços em execução e políticas do firewall do sistema. Evite interromper serviços de produção.

05 Registrar plano de ação

Classifique os achados em alto, médio ou baixo impacto, com proposta de correção e evidência esperada.

Evidências esperadas

- Checklist de configuração
- Registro dos principais serviços ativos
- Tabela de recomendações por criticidade

Checklist de execução

[ ] Sistema de teste identificado

[ ] Atualizações verificadas

[ ] Contas administrativas revisadas

[ ] Serviços e firewall avaliados

[ ] Plano de ação documentado

Questões para discussão

1. Qual é a diferença entre hardening e aplicação de patches?

2. Que riscos existem ao desativar um serviço sem mapear dependências?

Registro final

Data: ____ / ____ / _____ Responsável: _____

Resultado, justificativa e limitações: