

Passo a Passo para Análise de Riscos

1. Configuração do Ambiente de Laboratório Virtual:

- Inicie o software de simulação de rede.
- Monte uma rede básica incluindo um servidor, um switch, um roteador e pelo menos dois computadores cliente.
- Configure IP estático ou DHCP para a atribuição de endereços IP.

2. Identificação de Ativos e Serviços:

- Identifique quais serviços estão rodando nos dispositivos da rede. Isso pode incluir servidores web, FTP, SSH, entre outros.
- Liste os ativos importantes que precisam ser protegidos. Isso inclui dados sensíveis armazenados no servidor ou informações de acesso.

3. Varredura da Rede com Nmap:

- Use o Nmap para realizar uma varredura na rede e identificar quais portas estão abertas e quais serviços estão rodando nesses dispositivos. Um comando básico para começar pode ser: **nmap -sV <endereço IP ou faixa de IP>**.
- Analise os resultados para identificar potenciais vulnerabilidades, como serviços desatualizados ou desnecessários expostos à rede.

4. Identificação de Vulnerabilidades:

- Com base nos serviços identificados na etapa anterior, discuta quais podem ser vulnerabilidades potenciais. Por exemplo, um servidor FTP sem autenticação forte pode ser uma vulnerabilidade.
- Use recursos online como o CVE (Common Vulnerabilities and Exposures) para pesquisar vulnerabilidades conhecidas nos serviços identificados.

5. Análise de Riscos:

- Para cada vulnerabilidade identificada, avalie o risco associado considerando a probabilidade de uma ameaça explorar essa vulnerabilidade e o impacto que isso teria sobre a rede. Use uma escala simples como baixo, médio e alto para classificar tanto a probabilidade quanto o impacto.
- Documente essa análise em uma tabela simples, incluindo a vulnerabilidade, a probabilidade, o impacto e o risco geral.

6. Proposta de Mitigação:

- Para as vulnerabilidades identificadas, proponha medidas de mitigação. Isso pode incluir atualizar software para a versão mais recente, desabilitar serviços desnecessários, implementar autenticação mais forte, entre outras medidas.

7. Conclusão:

- Conclua a análise discutindo como as medidas de mitigação propostas podem reduzir o risco para a rede.

- Prepare uma apresentação curta para compartilhar suas descobertas e recomendações com a turma.