Redes de Computadores II

C.T. Informática para Internet
Prof. Vinícius Alves Hax

Antes

- Análise de tráfego

Hoje

- Auditoria (de Redes)

O que é auditoria?

- “Auditoria é um exame cuidadoso e sistemático das atividades desenvolvidas em determinada organização, cujo objetivo é averiguar se elas estão de acordo com as **planejadas e/ou estabelecidas previamente**, se foram implementadas com eficácia e adequadas (em conformidade) à consecução dos objetivos.
  As auditorias podem ser classificadas em: **auditoria externa** e **auditoria interna**.“ Wikipédia, grifos meus.

Auditoria externa

- Contratada:
  - Para reduzir custos
  - Por não ter o “*know how*”
  - Para dar mais confiabilidade: muito comum em auditoria fiscal. Ex: Padrões ISO
- Órgãos de controle
  - Entre órgãos públicos. Ex: Controladoria Geral da União (CGU)
  - Para agentes privados. Ex: fiscalização sanitária

Tipos de auditoria

- Financeira
- Ambiental
- De qualidade
- De segurança do trabalho
- De segurança da informação
- ???
- ???
- Etc

Em TI, auditoria está muito ligada à segurança da informação.

- Por que isso acontece?

Auditoria

- Padrões:
  - Internos (desenvolvidos pela própria organização)
  - Normas e leis: NBR 27001/27002; Lei Geral de Proteção de Dados (LGPD); etc.

Auditoria de Segurança da Informação

- “Podemos definir auditoria como a medição de algo contra um padrão. Apesar de estarmos tratando de Segurança da Informação, o conceito de auditoria pode ser aplicado em qualquer área, como qualidade, ambiental, financeira, de conformidade etc.”

PEIXINHO, Ivo de Carvalho; FONSECA, Francisco M.; LIMA, Franscisco M. Segurança de Redes e Sistemas. Escola Superior de Redes RNP", Rio de Janeiro/RJ, 2013.

Auditoria de Segurança da Informação (2)

"Quando tratamos especificamente de auditoria de SI, podemos estar auditando o cumprimento de uma política de segurança, a eficácia de um novo sistema de segurança (como um firewall), se um sistema está com todas as correções conhecidas aplicadas, entre outros. [...] Entre as técnicas utilizadas em auditorias, as mais comuns são a análise de vulnerabilidades e os testes de penetração (penetration testing ou pentest)."

Peixinho et al

Técnicas comuns

- Análise de vulnerabilidade: mais específica; geralmente contra um “alvo” único: hardware ou software; informações internas;
- Pentest: mais abrangente, geralmente contra uma rede ou um sistema; teste “black box”;

Análise de vulnerabilidade

- Podemos averiguar:
  - Senhas e configurações padrão
    - Exemplo: cofre
  - Ataques de negação de serviço
  - Controle de acesso
  - Falhas comuns (especialmente recentes)
    - Geralmente com uso de ferramentas automatizadas
  - Código-fonte (backdoors e/ou erros de programação)

Etapas de um Pentest

- 1. Mapeamento de hosts da rede/portas abertas
- 2. Exploração de vulnerabilidades contra host/sistema
- 3. Escalada de privilégios

Teoricamente poderia incluir também tentativa de acesso físico

Exercício em aula

- Elaborando um checklist para uma auditoria de redes/segurança da informação

Exercício em aula

- Elaborando um checklist para uma auditoria de redes/segurança da informação
  - Se a rede tem senha
  - Verificar as regras do firewall
  - Saber se existe VPN, e se existir testar segurança
  - Verificar se as senhas são “fortes”
  - Verificar velocidade da Internet
  - Verificar validade dos backups
  - Equipamentos desatualizados

Exercício (continuação)

- Verificar se dados dentro da rede são criptografados
- Acessos site
- Verificar se dados sensíveis estão expostos
- Verificar quem tem acesso físico aos equipamentos
-

Dúvidas?