Análise de Vulnerabilidades

Toda organização necessita de uma infra-estrutura de redes muito bem elaborada. O objetivo da Análise de vulnerabilidade é reduzir o risco em relação aos incidentes de segurança, seja tanto na rede interna quanto na externa, é necessário detectar essas possíveis falhas e corrigí-las para garantir que a rede esteja em um nível de segurança adequada.

A análise de vulnerabilidade visa detectar falhas em diversos componentes como: aplicações, softwares, equipamentos, sistemas operacionais, dentre outros. Deve-se fazer continuamente o processo de verificação e análise da rede, para que a mesma fique sempre atualizada e livre de acessos não permitidos e indesejáveis.

Essa análise pode ser feita local e/ou remota.

Após tal análise são oferecidos relatórios com as respectivas soluções propostas.

Nestes relatórios podem constar também itens dos quais objetiva-se melhorar a segurança do ambiente, não necessariamente relacionados às falhas encontradas.

Divide-se em dois tipos:

Ativa - Encontra-se e corrigi-se as falhas, emitindo relatórios apenas do que foi feito.

Passiva - Encontra-se as falhas e emite-se relatórios para que o cliente se encarregue de corrigir

Objetivo: compreender as vulnerabilidades: quais são, o que as causa e quais seus efeitos.

Existem vulnerabilidades de S.O.(Windows, Linux, OS X, etc), de aplicativos (browsers, instant messengers, media players, ...), humanas (por exemplo, aquele admininstrador de redes é suscetível a ataques de engenharia social!)

Testes de invasão só fazem sentido se você souber o quê vai testar e analisar o resultado.

É importante também saber como corrigir as vulnerabilidades detectadas.

Existem dezenas de *sites* que reportam vulnerabilidades diversas, mas para aprender os detalhes temos:

- Carnegie-Mellon CERT Coordination Center (http://www.cert.org/)
- Security Focus (http://www.securityfocus.com/)
- Microsoft TechNet (http://www.microsoft.com/technet/security/current.aspx)

Outros Links:
http://www.nic.br
http://www.cais.rnp.br
http://www.sysinternals.com
http://www.packetstormsecurity.org
http://www.ask.com

ISTF > Segurança da Informação > Penetration Tests
Análise de vulnerabilidades, teste de invasão
http://www.istf.com.br/vb/penetration-tests/7420-analise-de-vulnerabilidades-teste-de-invasao-etc.html

ISTF > Segurança da Informação > Penetration Tests
Métodos e processos para Auditoria/Análise de vulnerabilidades em redes
http://www.istf.com.br/vb/penetration-tests/8336-metodos-e-processos-para-auditoria-analise-de-vulnerabilidades-em-redes.html

---

A importância da análise de vulnerabilidade no gerenciamento de riscos de segurança

Todo sistema computadorizado possui diversas entradas e saídas lógicas disponíveis para a comunicação entre seus próprios componentes ou aplicações externas.

As *vulnerabilidades e exposições*, de modo geral podem ser as que:

- Permitem que um atacante execute comandos;
- Alcance os dados privados e
- Se comporte como uma entidade reconhecida.

A análise de vulnerabilidade é um dos itens fundamentais no gerenciamento de risco, pois de forma freqüente são verificadas as vulnerabilidades ou exposições existentes.

As principais vantagens nas atividades da análise de vulnerabilidade são:

- Identificação das vulnerabilidades;
- Correção das vulnerabilidades reduzindo os riscos;
- Mapeamento proativo das ameaças existentes;
- Redução no tempo de paradas;
- Economia de recursos e
- Maior controle sobre os potenciais de riscos.

Tarefa 1 **Scanner de Portas:** **Nmap** (pode ser outro scanner)
Tarefa 2 **Scanner de Vulnerabilidades:** **Nessus** (pode ser outro scanner)