Atividade 1.4.5: Identificar Principais Vulnerabilidades de Segurança

Objetivos

Ao concluir esta atividade, você poderá:

- Utilizar o site SANS para identificar rapidamente ameaças à segurança da Internet.
- Explicar como as ameaças são organizadas.
- Listar diversas vulnerabilidades de segurança recentes.
- Utilizar os links SANS para acessar outras informações relativas à segurança.

Contexto

Um dos websites mais populares e confiáveis relativos à defesa contra ameaças à segurança de redes e computadores é o SANS. SANS é a sigla para SysAdmin, Audit, Network, Security (Administração de Sistemas, Auditoria, Rede, Segurança). O SANS contém vários componentes, cada um deles um grande contribuinte para a segurança de informações. Para mais informações sobre o website do SANS, visite http://www.sans.org/ e selecione itens no menu Recursos.

Como um administrador de segurança corporativa pode identificar rapidamente ameaças à segurança? O SANS e o FBI compilaram sua lista dos 20 principais Alvos de Ataques à Segurança da Internet no site http://www.sans.org/top20/. A lista é atualizada regularmente com informações formatadas por:

- Sistemas Operacionais —Windows, Unix/Linux, MAC
- Aplicativos — Plataformas cruzadas, incluindo Web, bancos de dados, Ponto-a-Ponto, mensagens instantâneas, reprodutores de mídia, servidores DNS, software de backup e servidores de gerenciamento
- Dispositivos de Rede — Dispositivos de infra-estrutura de rede (roteadores, switches, etc.), dispositivos VoIP
- Elementos Humanos — Políticas de segurança, comportamento humano, problemas pessoais
- Seção Especial — Questões de segurança não listadas em nenhuma das categorias acima

Cenário

Este laboratório apresentará os alunos a vulnerabilidades de questões de segurança dos computadores. O website do SANS será utilizado como uma ferramenta para identificação de vulnerabilidade de ameaças, compreensão e defesa.

Este laboratório deve ser concluído fora do laboratório da Cisco em um computador com acesso à Internet.

O tempo estimado para conclusão é de uma hora.

Tarefa 1: Localizar os Recursos SANS

Passo 1: Abrir a Lista Top 20 do SANS.

Utilizando um navegador Web, vá para a URL http://www.sans.org. No menu **recursos**, selecione **lista top 20**, exibida na Figura 1.

Figura 1. Menu SANS

A lista **20 Principais Alvos de Ataque à Segurança na Internet do SANS** é organizada por categoria. Uma letra de identificação indica o tipo de categoria e números separam tópicos da categoria. Tópicos de roteador e switch caem na categoria Network Devices (dispositivos de rede), **N**. Há dois tópicos de hyperlink principais:

N1. Servidores e Telefones VoIP
N2. Pontos Fracos Comuns de Configuração de Dispositivos de Rede e Outros

Passo 2: Clicar no hyperlink N2. Pontos Fracos Comuns de Configuração de Dispositivos de Rede e Outros para pular para este tópico.

Tarefa 2: Revisar os Recursos SANS

Passo 1: Revisar o conteúdo de N2.2 Problemas Comuns de Configuração-padrão.

Por exemplo, N.2.2.2 (em janeiro de 2007) contém informações sobre ameaças associadas a contas e valores-padrão. Uma busca no Google sobre "**senhas de roteador wireless" retorna links para diversos sites que publicam uma lista de nomes de conta de administrador e senhas padrão de roteadores sem fio**. **A falha ao alterar a senha-padrão nesses dispositivos pode levar a comprometimento e vulnerabilidade a ataques.**

Passo 2: Observar as referências de CVE.

A última linha sob vários tópicos menciona a Common Vulnerability Exposure (CVE – Exposição Comum a Vulnerabilidade). O nome CVE está vinculado ao National Vulnerability Database (NVD) do National Institute of Standards and Technology (NIST), patrocinado pela Divisão de Segurança Cibernética Nacional do Department of Homeland Security (DHS) e US-CERT, que contém informações sobre a vulnerabilidade.

Tarefa 3: Coletar Dados

O restante deste laboratório o leva a uma investigação e solução de vulnerabilidade.

Passo 1: Escolher um tópico para investigar e clicar em um exemplo de hyperlink CVE.

Nota: Como a lista CVE muda, a lista atual pode não conter as mesmas vulnerabilidades de janeiro de 2007.

O link deve abrir uma nova janela de navegador conectada ao site http://nvd.nist.gov/ e à página de resumo de vulnerabilidades para CVE.

Passo 2: Preencher informações sobre a vulnerabilidade:

Data original de lançamento: _____

Última revisão: _____

Origem:

Panorama:

_____

_____

_____

_____

_____

Sob Impacto, há diversos valores. A gravidade Common Vulnerability Scoring System (CVSS – Sistema de Pontuação de Vulnerabilidade Comum) é exibida e contém um valor entre 1 e 10.

Passo 3: Preencher informações sobre o impacto da vulnerabilidade:

Gravidade CVSS: _____

Faixa: _____

Autenticação: _____

Tipo de Impacto: _____

O próximo cabeçalho contém links com informações sobre vulnerabilidade e possíveis soluções.

Passo 4: Utilizando os hyperlinks, dê uma breve descrição da solução encontrada nestas páginas.

_____

_____

_____

_____

_____

_____

_____

Tarefa 4: Reflexão

O número de vulnerabilidades a computadores, redes e dados continua aumentando. Governos vêm dedicando recursos significativos para coordenar e disseminar informações sobre a vulnerabilidade e possíveis soluções. Ainda é responsabilidade do usuário final implementar a solução. Pense em formas de como usuários podem ajudar a fortalecer a segurança. Pense em hábitos do usuário que criam riscos à segurança.

Tarefa 5: Desafio

Tente identificar uma organização que fará uma reunião conosco para explicar como vulnerabilidades são rastreadas e soluções são aplicadas. Encontrar uma organização disposta a fazer isso pode ser difícil, por motivos de segurança, mas beneficiará os alunos, que aprenderão como a diminuição de vulnerabilidades é realizada no mundo. Isso também dará aos representantes da organização uma oportunidade de reunião com a classe e realização de entrevistas informais internas.

