Laboratório - Ameaças à segurança da rede de pesquisa

# Objetivos

Parte 1: Explorar o Site do SANS

Parte 2: Identificar as Ameaças à Segurança de Redes Recentes

Parte 3: Detalhar uma Ameaça à Segurança de Redes Específica

# Histórico/cenário

Para proteger uma rede contra ataques, um administrador deve identificar ameaças externas que representem um perigo para a rede. Sites de segurança podem ser utilizados para identificar ameaças emergentes e fornecer opções de mitigação para defender uma rede.

Um dos sites mais populares e confiáveis para oferecer proteção contra ameaças para computadores e redes é o SysAdmin, Audit, Network, Security (SANS). O site do SANS fornece vários recursos, incluindo uma lista dos 20 principais controles de segurança essenciais para a defesa digital eficiente e o informativo semanal @Risk: The Consensus Security Alert. Este informativo detalha novos ataques e vulnerabilidades da rede.

Neste laboratório, você vai navegar e explorar o site do SANS, vai usá-lo para identificar ameaças recentes de segurança de redes, pesquisar outros sites que identifiquem ameaças, e pesquisar e apresentar os detalhes sobre um ataque específico à rede.

# Recursos necessários

* Dispositivo com acesso à Internet
* Computador para apresentação com PowerPoint ou software de apresentação instalado

# Instruções

## Explorar o Site do SANS

Na Parte 1, acesse o site do SANS e explore os recursos disponíveis.

### Encontrar recursos do SANS.

Pesquise SANS na Internet. Na home page SANS, clique em **Recursos**GRÁTIS.

#### Pergunta:

Relacione três recursos disponíveis.

Digite suas respostas aqui.

### Localize o link para os controles críticos de segurança do CIS.

Os **Controles Críticos de Segurança da CIS** vinculados no site da SANS são o culminar de uma parceria público-privada envolvendo o Departamento de Defesa (DoD), a Associação Nacional de Segurança, o Centro de Segurança na Internet (CIS) e o Instituto SANS. A lista foi desenvolvida para priorizar os controles de segurança digital e os gastos do DoD. Tornou-se a peça central para programas eficazes de segurança para o governo dos Estados Unidos. No menu **Resources** (Recursos), selecione **Critical Security Controls** (Controles de segurança críticos) ou atividade similar. O documento CIS Críticos Security Controls está hospedado no site do Center for Internet Security (CIS) e requer registro gratuito para acessar. Há um link na página de controles de segurança CIS no SANS para baixar o pôster de controles críticos de segurança SANS 2014, que fornece uma breve descrição de cada controle.

#### Pergunta:

Selecione um dos controles e liste as sugestões de implementação para esse controle.

Digite suas respostas aqui.

### Localizar o menu Newsletters (Informativos).

#### Pergunta:

Destaque o menu **Resources**, selecione **Newsletters**. Descreva brevemente cada um dos três boletins informativos disponíveis.

Digite suas respostas aqui.

## Identificar as Ameaças à Segurança de Redes Recentes

Na Parte 2, você pesquisará ameaças à segurança de rede recentes usando o site do SANS para identificar outros sites que contenham informações sobre as ameaças de segurança.

### Localizar o @Risk: Consensus Security Alert Newsletter Archive.

Na página **Newsletters**, selecione **Archive** no @RISK: The Consensus Security Alert. Role para baixo até **Archives Volumes** e selecione um boletim informativo semanal recente. Analise as seções **Notable Recent Security Issues e Most Popular Malware Files**.

#### Pergunta:

Liste algumas vulnerabilidades recentes. Consulte vários boletins informativos recentes, se necessário.

Digite suas respostas aqui.

### Identificar sites que fornecem informações recentes sobre ameaças à segurança.

#### Perguntas:

Além do site do SANS, identifique outros sites que forneçam informações recentes sobre ameaças à segurança.

Digite suas respostas aqui.

Relacione algumas ameaças à segurança recentes detalhadas nesses sites.

Digite suas respostas aqui.

## Detalhar uma Ameaça à Segurança de Redes Específica

Na Parte 3, você pesquisará um ataque específico à rede que tenha ocorrido e criará uma apresentação com base em suas constatações. Preencha o formulário abaixo com base em suas constatações.

### Preencher o formulário a seguir para o ataque à rede selecionado.

|  |  |
| --- | --- |
| **Nome do ataque:** |  |
| **Tipo do ataque:** |  |
| **Data dos ataques:** |  |
| **Computadores/organizações afetados:** |  |
| **Como funciona e o que fez:** | |
|  | |
| **Opções de mitigação:** | |
|  | |
| **Links para referências e informações:** | |
|  | |

### Seguir as diretrizes do instrutor para finalizar a apresentação.

# Perguntas para reflexão

* 1. Que etapas você pode adotar para proteger seu computador?

Digite suas respostas aqui.

* 1. Quais são algumas etapas importantes que as organizações podem adotar para proteger seus recursos?

Fim do documento