

Laboratório – Identificação de ameaça

Objetivos

Pesquise as funcionalidades de segurança usadas pelas empresas para proteger os dados.

Parte 1: Como investigar a ameaça de ataques cibernéticos

Parte 2: Tríade CIA

Histórico/Cenário

As ameaças impostas pelo mundo virtual são reais. Essas ameaças têm o potencial para prejudicar a vida do mundo computadorizado. É importante compreender essas ameaças e, visando combatê-las, o mundo precisa de pessoas comprometidas que possam reconhecer as ameaças e frustrar os planos dos criminosos virtuais. Para desenvolver os talentos necessários, empresas como a CompTIA, Cisco Systems e ISC2 criaram programas para formar e qualificar profissionais virtuais.

Recursos necessários

- Computador ou dispositivo móvel com acesso à Internet

Parte 1: Como investigar a ameaça de ataques cibernéticos

Os ataques cibernéticos estão no topo da lista de ameaças aos países ao redor do mundo. Ao pensar nas ameaças à segurança nacional ou mundial, a maioria das pessoas se refere a ataques físicos ou armas de destruição em massa. O fato é que as ameaças virtuais estão no topo da lista de mais de vinte países no mundo inteiro. A classificação dos ataques cibernéticos como o primeiro lugar revela alguns fatores sobre como a sociedade mudou. Os computadores e as redes de computadores afetam nossa maneira de aprender, comprar, comunicar, viajar e viver. Os sistemas computadorizados controlam quase todos os aspectos de nossas vidas. Uma interrupção nos sistemas computadorizados e redes de computadores pode ter um impacto devastador na vida atual. Sistemas de geração e distribuição de energia elétrica, sistemas de tratamento e abastecimento de água, sistemas de transporte e sistemas financeiros são alvos de ataques cibernéticos. Cada um desses sistemas vem sendo vítima de ataques cibernéticos. Assista ao vídeo abaixo. Divida em grupos de 3-4 pessoas. Após assistir ao vídeo, responda as perguntas abaixo.

Passo 1: Pesquise as ameaças.

No passo 1, você pesquisará as ameaças.

- a. Clique [aqui](#) para assistir ao vídeo. De acordo com o vídeo, qual é a arma mais perigosa do mundo? Por quê? Você concorda?

- b. Indique cinco maneiras pelas quais um criminoso virtual pode usar computadores para infringir a lei. Algum dos crimes que indicou pode afetar você no nível pessoal? Você ou seus familiares foram afetados por esses crimes?

- c. Alguma das possíveis ameaças retratadas no vídeo realmente ocorreu? Clique [aqui](#) para saber mais sobre esses ataques.

Passo 2: Pesquise os últimos ataques.

- a. O impacto e o alcance dos últimos ataques cibernéticos têm muitas empresas e funcionários públicos interessados. Clique [aqui](#) para rever as 10 invasões virtuais mais importantes e mais devastadoras de 2015.

Quantas pessoas a violação de dados do US Office of Personnel Management afetou?

- b. Descreva o ataque de TalkTalk de 2015. Quem foi o responsável e o que os criminosos virtuais roubaram?

Parte 2: Tríade CIA

Confidencialidade, integridade e disponibilidade são os três princípios fundamentais da segurança digital. Esses três princípios formam a tríade CIA. Os elementos da tríade são os componentes mais críticos da segurança. Todos os profissionais de segurança digital devem se familiarizar com esses princípios fundamentais.

Passo 1: Pesquise a tríade CIA.

- a. Clique [aqui](#) para assistir ao vídeo. O que é sigilo dos dados? Por que o sigilo dos dados é tão importante para as pessoas e empresas?

- b. O que é integridade de dados? Indique três maneiras em que a integridade ou credibilidade de dados é afetada.

- c. O que é disponibilidade do sistema? O que pode acontecer se um sistema computadorizado crucial deixar de estar disponível?

Passo 2: Pesquise os ataques cibernéticos.

Clique [aqui](#) para assistir a um vídeo. O que os criminosos virtuais estavam tentando fazer? Em que hora do dia o ataque ocorreu? Ataques à rede podem ocorrer após o expediente? Por quê?
