

1

Marcar para revisão

(FCC/2012 - Adaptada) Códigos maliciosos (malwares) são programas que objetivam executar ações danosas e atividades maliciosas em um computador. Neste contexto encontram-se bots e botnets, sobre os quais é correto afirmar:

A

Botnet é um software malicioso de monitoramento de rede que tem a função de furtrar dados que transitam pela rede e, normalmente, tornar a rede indisponível disparando uma grande carga de dados direcionados ao servidor da rede.

B

Bot é um programa que dispõe de mecanismos de comunicação com o invasor e possui um processo de infecção e propagação igual ao do vírus, ou seja, não é capaz de se propagar automaticamente.

C

Um computador infectado por um bot costuma ser chamado de attack base, pois serve de base para o atacante estabelecer suas ações maliciosas. Também pode ser chamado de spam host, pois o bot instalado tem o objetivo de enviar infinitamente spams para a caixa de e-mail de quem é vítima do ataque.

D

A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer exclusivamente via redes do tipo P2P. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtrar dados do computador infectado e enviar spam.

E

Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos, coleta de informações de um grande número de computadores, envio de spam e camuflagem da identidade do atacante.

✕

Resposta incorreta

Opa! A alternativa correta é a letra E. Confira o gabarito comentado!

Gabarito Comentado

Botnets, também conhecido como rede zumbi, é um conjunto de equipamentos que sofreu um ataque, resultando no controle do equipamento pelo hacker. Através de botnets é possível fazer ataques de negação de serviço, envios de e-mails em massa e vários outros.

2

Marcar para revisão

Ativos são recursos econômicos controlados por uma organização que possuem valor e podem gerar benefícios futuros. Eles são divididos em duas categorias principais: ativos tangíveis e ativos intangíveis. De maneira geral, qual exemplo pode ser considerado um ativo lógico tangível?

A

Informação.

B

Marca.

C

Colaboradores.

D

Humanos.

E

Imagem da organização.

✓

Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

Ativos tangíveis lógicos são aqueles que envolvem a informação e sua representação em algoritmos, por exemplo, uma fórmula química, os detalhes sobre a safra da laranja no mercado norte-americano, o algoritmo principal de busca do Google, os detalhes técnicos das baterias dos carros do Elon Musk.

3

Marcar para revisão

Considere que uma equipe esteja trabalhando num software web com severas restrições de segurança. Além dos desenvolvedores e analistas, essa equipe conta com profissionais especialistas em segurança que têm, entre outras atribuições, a responsabilidade de realizar a revisão dos códigos a fim de evitar vulnerabilidades. Se durante a etapa de desenvolvimento um revisor da equipe de segurança detectar uma vulnerabilidade, é sua responsabilidade:

A

Corrigir a vulnerabilidade, contatando os desenvolvedores que programaram o trecho de código vulnerável.

B

Separar a vulnerabilidade e alertar a equipe de segurança para que o problema seja resolvido.

C

Separar a vulnerabilidade, tratando o código com erro como mais um problema que requer correção.

D

Isolar o problema e solicitar que a equipe de desenvolvimento corrija a vulnerabilidade imediatamente.

E

Corrigir o problema e relatar a vulnerabilidade à equipe de segurança.

✓

Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

Na situação apresentada, a responsabilidade do revisor de segurança ao detectar uma vulnerabilidade é separá-la e alertar a equipe de segurança para que o problema seja resolvido. Isso ocorre porque o revisor de segurança não necessariamente tem a habilidade ou autoridade para corrigir a vulnerabilidade, mas sim para identificá-la e reportá-la à equipe responsável pela segurança do software. Portanto, a alternativa correta é: "Separar a vulnerabilidade e alertar a equipe de segurança para que o problema seja resolvido".

4

Marcar para revisão

Sobre os conceitos de segurança da informação, analise as afirmativas a seguir:

- I. Uma ameaça tem o poder de comprometer ativos vulneráveis.
- II. Risco é a combinação das consequências de um incidente de segurança com a sua probabilidade de ocorrência.
- III. Vulnerabilidades técnicas são mais críticas do que vulnerabilidades criadas por comportamento humano.

Está correto somente o que se afirma em:

A

I

B

II

C

III

D I e II

E I e III



Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

As afirmativas I e II estão corretas. A primeira afirmação é verdadeira porque uma ameaça, de fato, tem o poder de comprometer ativos que são vulneráveis. A segunda afirmação também é verdadeira, pois o risco é a combinação das consequências de um incidente de segurança com a sua probabilidade de ocorrência. No entanto, a terceira afirmação é falsa, pois não se pode afirmar categoricamente que vulnerabilidades técnicas são mais críticas do que as vulnerabilidades criadas por comportamento humano. Ambas podem ter impactos significativos na segurança da informação e dependem do contexto específico.

5

Marcar para revisão

(FCC/2010) Sobre segurança da informação, considere:

I. Ameaça: algo que possa provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade.

II. Vulnerabilidade: é medida pela probabilidade de uma ameaça acontecer e o dano potencial à empresa.

III. Risco: ponto pelo qual alguém pode ser atacado, molestado ou ter suas informações corrompidas.

Está correto o que consta APENAS em

A II e III

B I e II

C I e III

D I

E III



Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

Os itens II e III apresentam os conceitos invertidos, sendo correto afirmar:

Vulnerabilidade: ponto pelo qual alguém pode ser atacado, molestado ou ter suas informações corrompidas;

Risco: é medido pela probabilidade de uma ameaça acontecer e o dano potencial à empresa.

6

Marcar para revisão

É um tipo de malware feito para extorquir dinheiro de sua vítima. Esse tipo de ciberataque irá criptografar os arquivos do usuário e exigir um pagamento para que seja enviada a solução de descriptografia dos dados da vítima. O scareware é seu tipo mais comum e usa táticas ameaçadoras ou intimidadoras para induzir as vítimas a pagar.

O texto se refere ao:

A Spyware

B Botnet

C Spam

D DDoS

E Ransomware



Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

O enunciado descreve um tipo de malware que criptografa os arquivos do usuário e exige um pagamento para descriptografá-los. Este é o comportamento característico do Ransomware. O Ransomware é um tipo de software malicioso que restringe o acesso ao sistema infectado e cobra um resgate para que o acesso possa ser restabelecido. Portanto, a alternativa correta é o Ransomware.

7

Marcar para revisão

(FEPESE/2017) Identifique abaixo as afirmativas verdadeiras (V) e as falsas (F) sobre Negação de Serviço (DoS e DDoS):

() Negação de serviço, ou DoS (Denial of Service) é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

() Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDos (Distributed Denial of Service).

() O principal objetivo dos ataques de Negação de Serviço (DoS e DDos) é invadir e coletar informações do alvo.

() Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques. A grande maioria dos computadores, porém, participa dos ataques sem o conhecimento de seu dono, por estar infectado e fazendo parte de botnets.

Assinale a alternativa que indica a sequência correta, de cima para baixo.

A V V F V

B V F F V

C V F F F

D F V V F

E F F V F



Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

Podemos assumir que o principal objetivo dos ataques de Negação de Serviço (DoS e DDos) é paralisar as operações do alvo.

8

Marcar para revisão

(UFES/2014) O termo "Engenharia Social" é comumente utilizado para se referir a técnicas utilizadas por pessoas mal-intencionadas que abusam de relações sociais para conseguir informações sigilosas ou acesso a sistemas. Dos cenários abaixo, NÃO caracteriza um caso de Engenharia Social o que está descrito em

A Em um ambiente de trabalho, uma pessoa liga, identifica-se como administrador dos sistemas da empresa e solicita que você siga uma série de passos, incluindo acesso a sites na internet e instalação de softwares, para melhorar o desempenho da sua máquina.

B Você recebe um e-mail indicando que acaba de ser sorteado com um prêmio e instruindo-o a acessar um determinado site e preencher o cadastro para coletar o seu prêmio.

C Você recebe um e-mail alertando sobre um novo vírus muito perigoso e orientando-o a procurar por determinado arquivo em seu sistema e, caso ele exista, excluí-lo imediatamente e repassar a mensagem a todos os seus conhecidos.

D Uma pessoa liga para você, identifica-se como sendo de uma empresa prestadora de serviços (ex.: de telefonia), explica que há um problema no seu cadastro e pede que você informe vários dados pessoais, como nome completo, endereço, etc.

E Após fornecer seu endereço de e-mail em um site para se cadastrar, você recebe uma mensagem de e-mail desse site pedindo que você clique em um link para confirmar o seu cadastro.

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A Engenharia Social é um método de ataque que utiliza a persuasão para obter dados sigilosos do usuário, seja por meios eletrônicos ou não. Normalmente, o atacante se passa por alguém confiável, como uma instituição conhecida, como um banco ou empresa. A opção correta mencionada refere-se apenas a um procedimento de confirmação, comum quando você se cadastra em um site e recebe uma mensagem para confirmar a validade do seu endereço de e-mail.

9

Marcar para revisão

O link de acesso à internet de uma instituição encontra-se muito instável porque o seu provedor não cumpre o SLA. Do ponto de vista de segurança e análise de risco, isso deve ser considerado como evidência de:

A BYOD.

B Ameaça.

C Resiliência.

D Negação de serviço.

E Vulnerabilidade.

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

Na situação descrita no enunciado, a instabilidade do link de acesso à internet, devido ao não cumprimento do SLA pelo provedor, é uma evidência de vulnerabilidade. Vulnerabilidade, no contexto de segurança da informação, refere-se a uma fraqueza que pode ser explorada por ameaças para causar danos a um ativo. Neste caso, a vulnerabilidade é a instabilidade do link de acesso à internet, que pode ser explorada para interromper ou degradar o serviço, afetando a disponibilidade da informação.

10

Marcar para revisão

Indique a alternativa que pode conter um relacionamento mais apropriado entre os conceitos de AMEAÇA, IMPACTO, INCIDENTE e VULNERABILIDADE tratados pela Gestão de Riscos na Tecnologia da Informação.

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor de aplicação	Falta de atualizações do sistema operacional	Exploração de vulnerabilidades conhecidas	Perda de Confidencialidade, Integridade e Disponibilidade

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor Web	Servidor de aplicação acessível pela internet	Ataque Hacker DDoS	Integridade

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Firewall da rede	Sem controle de manutenção periódica	Defeito no firmware	Perda da confidencialidade nos acessos a internet

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor Web	Ataque Hacker DDoS	Falta de atualizações do sistema operacional	Indisponibilidade

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Firewall da rede	Falta de atualizações do IOS	Perda de desempenho	Não suporta atualizações de hardware

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A resposta correta é:

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor de aplicação	Falta de atualizações do sistema operacional	Exploração de vulnerabilidades conhecidas	Perda de Confidencialidade, Integridade e Disponibilidade

Questão 1 de 10

1	2	3	4	5
6	7	8	9	10

○ Corretas (9)
○ Incorretas (1)
○ Em branco (0)