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) 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, furtar dados do computador infectado e enviar spam.

B) 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.

C) 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.

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

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.

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.

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

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

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

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

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

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) II

B) I e II

C) I

D) I e III

E) III

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) III

B) II e III

C) I e II

D) I

E) I e III

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

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 F F V

B V V F V

C F V V F

D V F F F

E F F V F

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 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.

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 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.

D 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.

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.

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 Negação de serviço.

B Vulnerabilidade.

C Ameaça.

D Resiliência.

E BYOD.

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.

A

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

B

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

C

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

D

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

E

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

Questão **1** de 10

1 2 3 4 5

6 7 8 9 10

○ Em branco **(10)**