Exercícios de Revisão para AV1
Disciplina: 4SEG – 2021/2
Profa. Maria Cláudia

Tópicos que serão cobrados na AV1:

- Conceito de segurança da informação e sua importância no cenário atual

- Princípios Básicos de Segurança da Informação, principalmente CID / CIDA

- Ameaças, Vulnerabilidades, Ataques

- Soluções de proteção

- Noções de Criptografia, Chaves Simétricas e Assimétricas, Principais Algoritmos e Aplicações

Exercícios:

1) A sociedade vive atualmente um novo momento de transformação no mercado de trabalho. São exemplos de termos que representam esse movimento:

(a) 1ª Revolução Industrial, Web 2.0
(b) Industria 4.0, Transformação Digital
(c) Internet, Redes Sociais
(d) Redes Sociais, 2ª Revolução Industrial

2) No contexto atual, podemos definir Segurança da Informação como:

(a) É instalar soluções que utilizem os melhores equipamentos de segurança do mercado.
(b) É optar pelo uso de documentos digitais em relação aos documentos físicos.
(c) É implementar controle de acesso aos dados e confiar no cliente / usuário / prestador de serviço.
(d) É a proteção da informação contra vários tipos de ameaças para garantir a continuidade e minimizar riscos.

3) Consideramos o acrônimo CIDA como os pilares da Segurança da Informação. Esse acrônimo significa:

(a) Confidencialidade, Integridade, Disponibilidade e Autenticidade
(b) Confidencialidade, Indisponibilidade, Dedicação e Austeridade
(c) Confiabilidade, Integridade, Dinamismo e Austeridade
(d) Confiabilidade, Indisponibilidade, Dinamismo e Autenticidade

4) Estudamos que uma ameaça é um possível perigo que pode explorar uma vulnerabilidade. Os códigos maliciosos podem ser classificados como:

(a) Ameaças Naturais
(b) Ameaças Involuntárias
(c) Ameaças Voluntárias
(d) Ameaças Artificiais

5) (Prova de Concurso de Nível Técnico – 2020) Quais são os aplicativos ou dispositivos que ficam em execução em um determinado computador para monitorar todas as entradas do teclado?

(a) Ransomwares. (b) Keyloggers. (c) Spams.
(d) Jobs. (e) KeyParams.

Exercícios de Revisão para AV1
Disciplina: 4SEG – 2021/2
Profa. Maria Cláudia

6) Classifique as sentenças como Verdadeiras (V) ou Falsas (F). Corrija as sentenças falsas:

6.1) (F) A instalação e a execução de um ou mais sistemas antimalware em um computador garantem proteção contra softwares maliciosos, mesmo que o usuário execute frequentemente arquivos recebidos em mensagens e não atualize seus programas e o sistema operacional.

6.2) (F) Worm é um programa que aparenta ter uma finalidade atraente, mas que esconde alguma funcionalidade maliciosa.

6.3 (V / F) Backdoor é um programa que permite ao atacante contornar os controles de segurança de um sistema, proporcionando o acesso desautorizado com privilégios indevidos.

6.4 (F) A criptografia não é capaz de criptografar um documento de texto. Ela somente consegue utilizar seus algoritmos para criptografar textos puros, transformando-os em textos cifrados.

6.5 (F) Os honeypots (potes de mel), enquanto tecnologia de detecção de intrusão, podem ser utilizados para atingir os objetivos de atrair um atacante potencial e afastá-lo de sistemas críticos e de incentivar o atacante a ficar no sistema por período de tempo suficiente para que haja resposta dos administradores, mas não para coletar informações sobre a atividade do atacante, uma vez que não foram projetados para esse fim.

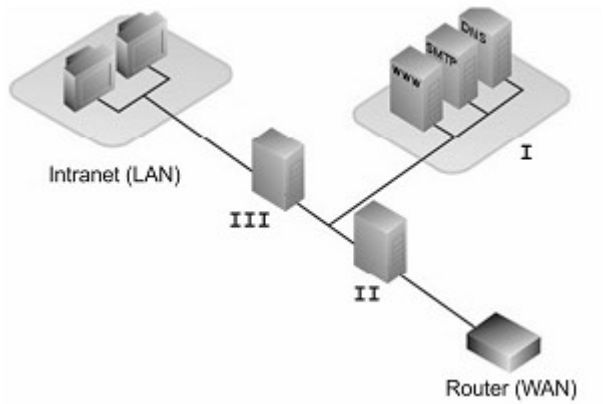
7) Em relação à arquitetura de firewall, a preocupação reside na disposição dos equipamentos que compõem uma rede de computadores e o próprio firewall. Considere a separação entre a rede interna da organização da rede externa, que pode ser a internet, por meio da utilização de uma máquina que contenha duas interfaces de rede. Essa disposição consiste em uma arquitetura de firewall do tipo:

(a) Screened Host
(b) Dual-Homed Host
(c) Screened Subnet
(d) Screened-Homed
(e) Dual-Homed Subnet

8) Referente à segurança da informação, a criptografia é a principal ferramenta de proteção dos dados. Assinale a alternativa que apresenta o tipo de criptografia descrito a seguir: “Qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que podem ser amplamente disseminadas, e chaves privadas que são conhecidas apenas pelo proprietário.”.

(a) Criptografia assimétrica.
(b) Criptografia simétrica.
(c) Criptografia quântica.
(d) Pretty Good Privacy.
(e) MD5.

9) (Prova: FCC - 2017 - ARTESP - Agente de Fiscalização à Regulação de Transporte - Tecnologia de Informação) A imagem abaixo mostra a utilização de uma arquitetura com mecanismos apropriados para proteger a rede interna de uma organização.



Na arquitetura mostrada na figura, I é

(a) um cluster, II é um firewall e III é uma DMZ.
(b) uma DMZ e II e III são firewalls.
(c) um Data Center, II é uma DMZ e III é um firewall.
(d) um cluster de servidores e II e III são DMZs.
(e) um firewall, II é um IPS e III é um IDS.