

Disciplina: Segurança de Informação

Professor: Prof. Esp. Paulo Henrique S. Barbosa

Data: 04/05/2021

Nome do aluno WALLAS VIEIRA LIMA

ATIVIDADE AVALIATIVA SOBRE MALWARES

INSTRUÇÕES:

Marque a opção correta ou certo / errado.

Questões

1. Os vírus de macro que danificam documentos do Word podem ser eliminados com a instalação do aplicativo Visual Basic for Applications, do Windows.

Resposta: FALSO

2. Os worms são pouco ofensivos, pois referem-se ao envio automático de mensagens indesejadas de correio eletrônico a um grande número de destinatários, que não as solicitaram ou que tiveram seus endereços eletrônicos copiados de um sítio pirata. **FALSO**

Resposta: FALSO

3. Os worms podem se propagar rapidamente para outros computadores por meio da Internet.

Resposta: CORRETA

4. Cavalos de troia (trojan) e worms são programas maliciosos, geralmente enviados por e-mail, que, instalados inadvertidamente pelo próprio usuário, causam impactos às vezes irreversíveis aos computadores e seus dados. **CORRETO**

5. Dadas as seguintes declarações: I. Programas que se replicam e se espalham de um computador a outro, atacando outros programas, áreas ou arquivos em disco. II. Programas que se propagam em uma rede sem necessariamente modificar programas nas máquinas de destino. III. Programas que parecem ter uma função inofensiva, porém, têm outras funções sub-reptícias.

Os itens I, II e III correspondem, respectivamente, a ameaças programadas do tipo:

a. cavalo de tróia, vírus e worms.

- b. worms, vírus e cavalo de tróia.
 - c. worms, cavalo de tróia e vírus.
 - d. vírus, worms e cavalo de tróia. **CORRETA**
 - e. vírus, cavalo de tróia e worms.
6. Spywares são programas que agem na rede, checando pacotes de dados, na tentativa de encontrar informações confidenciais como senhas de acesso e nome de usuário.

Resposta: **FALSO**

7. Arquivos de dados produzidos por suíte de aplicativos para escritório, por ex. Microsoft Office, costumam ser alvo predileto de contaminação por:

- a. trojans.
- b. worms.
- c. hijackers
- d. vírus de boot.
- e. vírus de macro **CORRETO**

8. Programa que a partir da execução em determinado computador vítima passa a monitorar informações digitadas e visualizadas e, em seguida, envia e-mail para o seu criador encaminhando informações capturadas denomina-se:

- a. cavalo de tróia.
- b. spyware. **CORRETO**
- c. phishing scan.
- d. hijackers.

9. Os keyloggers são aplicativos destinados a capturar o que é digitado no teclado. **CORRETO**

10. Mensagem não solicitada e mascarada sob comunicação de alguma instituição conhecida e que pode induzir o internauta ao acesso a páginas fraudulentas, projetadas para o furto de dados pessoais ou financeiros do usuário. Trata-se especificamente de:

- a. keylogger.
- b. scanning.
- c. botnet.
- d. phishing. **CORRETO**
- e. rootkit.

11. Backdoor são sistemas simuladores de servidores que se destinam a enganar um invasor, deixando-o pensar que está invadindo a rede de uma empresa.

Resposta: **CORRETA**

12. Cavalos-de-tróia ou trojans são malwares, que basicamente, permitem acesso remoto ao computador após a infecção. Os cavalos-de-tróia podem ter outras funcionalidades, como captura de dados do usuário e execução de funções não autorizadas no sistema. **FALSO**

13. Cavalo-de-troia é um programa que se instala a partir de um arquivo aparentemente inofensivo, sem conhecimento do usuário que o recebeu, e que pode oferecer acesso de outros usuários à máquina infectada. **CORRETA**

14. Entre os princípios básicos de segurança da informação, destacam-se a confidencialidade, a integridade e a disponibilidade. **CORRETA**

15. Os programas de antivírus são indicados para fazer controle e eliminação de pragas virtuais. São exemplos típicos de pragas virtuais: spyware, worm, firewall e boot. **FALSO**

16. O firewall atua como barreira por meio de regras estabelecidas, mas não cumpre a função de controlar os acessos. **CORRETO**

17. A criptografia é uma solução indicada para evitar que um arquivo seja decifrado, no caso de ele ser interceptado indevidamente, garantindo-se, assim, o sigilo das informações nele contidas. **CORRETA**

18. Redes virtuais privadas são canais fechados utilizados, por exemplo, para trafegar dados entre divisões de uma mesma empresa. **FALSO**

19. Phishing scam são e-mails não solicitados que tentam convencer o destinatário a acessar páginas fraudulentas na Internet com o objetivo de capturar informações, como senhas de contas bancárias e números de cartões de crédito. **CORRETO**

20. A disponibilidade e a integridade são itens que caracterizam a segurança da informação. A primeira representa a garantia de que usuários autorizados tenham acesso a informações e ativos associados quando necessário, e a segunda corresponde à garantia de que sistemas de informações sejam acessíveis apenas àqueles autorizados a acessá-los. **CORRETO**

21. Firewall e anti-spyware são nomes diferentes para software com os mesmos objetivos, ambos implementam o bloqueio a determinadas páginas web. **FALSO**

22. A realização de cópias de segurança (backup) e armazenamento de arquivos em mídias e locais diferentes são procedimentos que contribuem para a disponibilidade da informação no ambiente computacional. **CORRETA**

23.A criptografia é um processo de segurança de dados que faz com que eles fiquem inacessíveis, sendo possível acessar o conteúdo apenas a partir de uma chave de criptografia equivalente.

CORRETO

24.Hacker é um programa inteligente de computador que, após detectar falhas em um ambiente computacional, causa danos irreparáveis e a proliferação de outros programas maliciosos. **FALSO**

25.Programas de antivírus fazem varreduras no computador para procurar arquivos maliciosos disseminados pela transferência de arquivos. **CORRETA**

26.Ativado quando o disco rígido é ligado e o sistema operacional é carregado; é um dos primeiros tipos de vírus conhecido e que infecta a partição de inicialização do sistema operacional. Trata-se de

- a) vírus de boot. **CORRETA**
- b) cavalo de Troia. **FALSA**
- c) verme. **FALSA**
- d) vírus de macro. **FALSA**
- e) spam. **FALSA**

27.Programa que a partir da execução em determinado computador vítima passa a monitorar informações digitadas e visualizadas e, em seguida, envia e-mail para o seu criador encaminhando informações capturadas denomina-se:

- a) cavalodetróia. **FALSA**
- b) spyware. **CORRETA**
- c) phishingscan. **FALSA**
- d) hijackers. **FALSA**