Perguntas Sobre Segurança da Informação

Nível Médio

##### Segurança da Informação

1. *Tipos de Ataques*

O(A) representa um ataque que compromete diretamente a disponibilidade. Assinale a opção que completa corretamente a frase acima.

* 1. cavalo de tróia
  2. b) falsificação
  3. c) negação de serviço.

d) phishing

e) sniffing

1. Existe uma forma muito poderosa de ataque a um sistema denominada **DDoS**, cujo principal objetivo é:
2. inserir usuários não autorizados em um sistema.
3. executar aplicativos em um sistema com os privilégios de outro usuário.
4. enganar um servidor de um serviço de rede ao informá- lo um endereço falso durante o processo de autenticação ou solicitação de informações.
5. provocar uma sobrecarga com um número inesperado de acessos a um site, o que torna o carregamento de suas páginas mais demorado e sujeito a erros, provocando, em alguns casos, a interrupção dos seus serviços.
6. permitir acesso ao sistema pelo seu próprio projetista, utilizando uma porta introduzida por ele durante o processo de desenvolvimento, com a finalidade de furar a segurança normal implementada pela política de segurança.
7. Analise as seguintes afirmações relativas à segurança na Internet:

#### I - Engenharia Social é um termo utilizado para descrever um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

#### I I- Vulnerabilidade pode ser definida como uma falha no projeto ou implementação de um software que, quando explorada por um atacante,resulta na violação da segurança de um sistema.

1. **III** - Um **vírus de macro** normalmente é recebido como um arquivo executável anexado a uma mensagem de correio eletrônico. O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, fazendo com que o vírus seja executado.

**IV - Engenharia reversa** é uma das principais técnicas adotadas por hackers para ter acesso não autorizado a computadores ou informações.

Estão corretos os itens:

a) I e II b) II e III c) III e IV

d) I e III e) II e IV

1. *Malwares (Softwares Maliciosos)*
2. O código malicioso caracterizado por ser executado independentemente, consumindo recursos do hospedeiro para a sua própria manutenção, podendo propagar versões completas de si mesmo para outros hospedeiros, é denominado:

a) vírus.

b) backdoor.

c) cookie.

d) verme.

e) spyware.

1. Analise as seguintes afirmações relacionadas a vírus e antivírus.
2. Um **cookie** é

um vírus do tipo malware que pode ser armazenado pelo browser se um website requisitar. A informação não tem um tamanho muito grande e, quando acionados, alteram a configuração de segurança do browser.

1. Qualquer

malware que possua um **backdoor** permite que o computador infectado seja controlado totalmente ou parcialmente através de um canal de IRC ou via conexão com uma porta.

#### O Cavalo de

**Tróia** é um programa que, explorando deficiências de segurança de computadores, propaga-se de forma autônoma, contaminando diversos computadores geralmente conectados em rede. O Cavalo de Tróia mais conhecido atacou quantidades imensas de computadores na Internet durante os anos 90.

#### A Engenharia

**Reversa** é a arte de reverter códigos já compilados para uma forma que seja legível pelo ser humano. Técnicas de engenharia reversa são aplicadas na análise de vírus e também em atividades ilegais, como a quebra de proteção anticópia. A engenharia reversa é ilegal em diversos países, a não ser que seja por uma justa causa como a análise de um malware.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II b) II e III c) III e IV

d) I e III e) II e IV.

1. ) Em relação a vírus de computador é correto afirmar que, entre as categorias de malware, o **Cavalo de Tróia** é um programa que:
2. usa um código desenvolvido com a expressa intenção de se replicar. Um Cavalo de Tróia tenta se alastrar de computador para computador incorporando-se a um programa hospedeiro. Ele pode danificar o hardware, o software ou os dados. Quando o hospedeiro é executado, o código do Cavalo de Tróia também é executado, infectando outros hospedeiros e, às vezes, entregando uma carga adicional.
3. parece útil ou inofensivo, mas que contém códigos ocultos desenvolvidos para explorar ou danificar o sistema no qual é executado. Os cavalos de tróia geralmente chegam aos usuários através de mensagens de e-mail que disfarçam a finalidade e a função do programa. Um Cavalo de Tróia faz isso entregando uma carga ou executando uma tarefa mal- intencionada quando é executado.
4. usa um código mal-intencionado auto-propagável que pode se distribuir automaticamente de um computador para outro através das conexões de rede. Um Cavalo de Tróia pode desempenhar ações nocivas, como consumir recursos da rede ou do sistema local, possivelmente causando um ataque de negação de serviço.
5. pode ser executado e pode se alastrar sem a intervenção do usuário, enquanto alguns variantes desta categoria de malware exigem que os usuários executem diretamente o código do Cavalo de Tróia para que eles se alastrem. Os Cavalos de Tróia também podem entregar uma carga além de se replicarem.
6. não pode ser considerado um vírus ou um verme de computador porque tem a característica especial de se propagar. Entretanto, um Cavalo de Tróia pode ser usado para copiar um vírus ou um verme em um sistema-alvo como parte da carga do ataque, um processo conhecido como descarga. A intenção típica de um Cavalo de Tróia é interromper o trabalho do usuário ou as operações normais do sistema. Por exemplo, o Cavalo de Tróia pode fornecer uma porta dos fundos no sistema para que um hacker roube dados ou altere as definições da configuração.
7. É crescente o número de incidentes de segurança causados por **vírus de computador e suas variações**. Com isso, as organizações estão enfrentando o problema com o rigor e cuidados merecidos. Nesse contexto, é correto afirmar que:
8. cavalos de tróia são variações de vírus que se propagam e possuem um mecanismo de ativação (evento ou data) e uma missão.
9. Vírus polimórficos suprimem as mensagens de erro que normalmente aparecem nas tentativas de execução da atividade não- autorizada, utilizando, muitas vezes, criptografia para não serem detectados por anti-vírus.
10. os vírus de macro utilizam arquivos executáveis como hospedeiros, inserindo macros com as mesmas funções de um vírus em tais arquivos.
11. vírus geram cópias de si mesmo a fim de sobrecarregarem um sistema, podendo consumir toda a capacidade do processador, memória ou espaço em disco, eventualmente.
12. Com relação à segurança e a ataques em redes de computadores, pode-se observar que, depois que um malware alcança uma máquina hospedeira, geralmente executará uma ação conhecida como carga. O tipo de carga conhecido como “**Porta dos fundos**” é um tipo de carga de malware particularmente preocupante porque é normalmente desenvolvida para roubar informações. Se uma carga puder comprometer a segurança de um computador hospedeiro, é possível que ele desenvolva um mecanismo para passar informações para os responsáveis pelo malware.
13. é um dos tipos de carga mais destrutivos, normalmente um código mal-intencionado que altera ou exclui dados, tornando as informações no computador do usuário inúteis.
14. é um do tipo DoS, isto é, uma investida computadorizada feita por um invasor para sobrecarregar ou parar os serviços de uma rede, como um servidor da WEB ou um servidor de arquivos.
15. é um ataque DDoS que visa a simplesmente tornar um serviço específico temporariamente indisponível.
16. *Agentes de Segurança*
17. Um **Firewall** pode ser definido como uma coleção de componentes, colocada entre duas redes, que coletivamente possua propriedades que:
18. independentemente da política de segurança adotada, tem como objetivo principal impedir a entrada de vírus em um computador, via arquivos anexados a e-mails.
19. garantem que todo o tráfego de dentro para fora da rede, e vice-versa, deve ser bloqueado, independentemente da política de segurança adotada. Todo firewall deve ser à prova de violação.
20. garantem que todo o tráfego de dentro para fora da rede, e vice-versa, passe por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o firewall e, finalmente, ele deve ser à prova de violação.
21. garantem que apenas o tráfego de dentro para fora da rede deve passar por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o firewall e, fi nalmente, ele deve ser à prova de violação.
22. garantem que apenas o tráfego de fora para dentro da rede deve passar por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o firewall e, fi nalmente, ele deve ser à prova de violação.
23. *Princípios da Segurança da Informação*
24. A segurança da informação tem como objetivo a preservação da:
    1. confi dencialidade, interatividade e acessibilidade das informações.
    2. complexidade, integridade e disponibilidade das informações.
    3. confidencialidade, integridade e acessibilidade das informações.
    4. universalidade, interatividade e disponibilidade das informações.
    5. confidencialidade, integridade e disponibilidade das informações.
25. informação, para ser considerada segura, precisa manter seus aspectos de confidenciabilidade, integridade e disponibilidade. A confidenciabilidade é a
    1. propriedade de evitar a negativa de autoria de transações por parte do usuário, garantindo ao destinatário o dado sobre a autoria da informação recebida.
    2. garantia de que o sistema se comporta como esperado, em geral após atualizações e retificações de erro.
    3. análise e responsabilização de erros de usuários autorizados do sistema.
    4. garantia de que as informações não poderão ser acessadas por pessoas não autorizadas.
    5. propriedade que garante o acesso às informações através dos sistemas oferecidos.
26. Nos sistemas de Segurança da Informação, existe um método que . Este método visa garantir a integridade da informação. Escolha a opção que preenche corretamente a lacuna acima.
27. valida a autoria da mensagem
28. verifica se uma mensagem em trânsito foi alterada
29. verifica se uma mensagemem trânsito foi lida por pessoas não autorizadas
30. cria um backup diferencial da mensagem a ser transmitida
31. passa um antivírus na mensagem a ser transmitida
32. Analise as seguintes afirmações relacionadas a conceitos básicos de Segurança da Informação.
33. Um **firewall**, instalado entre uma rede LAN e a Internet, também é utilizado para evitar ataques a qualquer máquina desta rede LAN partindo de máquinas da própria rede LAN.
34. A **confidenciabilidade** é a propriedade de evitar a negativa de autoria de transações por parte do usuário, garantindo ao destinatário o dado sobre a autoria da informação recebida.

#### Na criptografia de chaves públicas, também chamada de criptografia assimétrica, uma chave é utilizada para criptografar e uma chave diferente é utilizada para decriptografar um arquivo.

1. Uma das finalidades da **assinatura digital** é evitar que alterações feitas em um documento passem sem ser percebidas. Nesse tipo de procedimento, o documento original não precisa estar criptografado.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II b) II e III c) III e IV

d) I e III e) II e IV

1. Analise as seguintes afirmações relativas à segurança da informação.
2. **disponibilidade** assegura que a informação será acessível somente por quem tem autorização de acesso.
3. Para garantir a **segurança da informação**, é necessário que os princípios básicos de confidencialidade, integridade e risco sejam respeitados.
4. A **integridade** assegura que a informação não foi alterada durante o processo de transporte.
5. **Vírus de macro** infectam a área do sistema de um disco, ou seja, o registro de inicialização em disquetes e discos rígidos.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II b) II e III c) III e IV

d) II e IV e) I e III

1. Alguns tipos de malware tentam atingir um objeto portador, também conhecido como hospedeiro, para infectá-lo. O número e tipo de objetos portadores que são alvos variam com as características dos malwares. Entre os portadores-alvo mais comuns, **as macros**:
2. são arquivos localizados em áreas específicas dos discos do computador (discos rígidos e mídias removíveis inicializáveis), como o registro mestre de inicialização (MBR).
3. são arquivos que suportam linguagens como Microsoft Visual Basic® Script, JavaScript, AppleScript ou PerlScript. As extensões dos arquivos desse tipo são:

.vbs, .js, .wsh e .prl.

1. são o alvo do vírus “clássico” que é replicado anexando-se a um programa hospedeiro. Além dos arquivos típicos que usam a extensão das macros, arquivos com as seguintes extensões também podem ser usados com essa finalidade: .com, .sys, .dll, .ovl,

.ocx e .prg.

1. são arquivos que suportam uma linguagem script de macro de um aplicativo específico, como um processador de texto, uma planilha eletrônica ou um aplicativo de banco de dados. Por exemplo, os vírus podem usar as linguagens de macro no Microsoft Word para causar vários efeitos, que podem variar de prejudiciais, como trocar palavras ou mudar as cores em um documento, a mal-intencionados, como formatar o disco rígido do computador.
2. são arquivos localizados no registro de inicialização do DOS e são capazes de executar códigos mal- intencionados. Quando o registro de um disco de inicialização é infectado, a replicação será efetivada se ele for usado para iniciar os sistemas de outros computadores.
3. Analise as seguintes afirmações relativas aos conceitos de Segurança da Informação:

#### Cofidencialida

**de** é a propriedade de manutenção do sigilo das informações. É uma garantia de que as informações não poderão ser acessadas por pessoas não autorizadas.

#### Irretratabilidad

**e** é a propriedade de evitar a negativa de autoria de transações por parte de usuários, garantindo ao destinatário o dado sobre a autoria da informação recebida.

#### Autenticidade

é a proteção da informação contra acessos não autorizados.

#### Isolamento ou

**modularidade** é a garantia de que o sistema se comporta como esperado, em especial após atualizações ou correções de erro.

|  |  |  |
| --- | --- | --- |
| Estão corretos os itens: |  | |
| a) I e II | b) II e III | c) III e IV |
| d) I e III | e) II e IV |  |

1. Considere um sistema no qual existe um conjunto de informações disponível para um determinado grupo de usuários denominados “auditores”. Após várias consultas com respostas corretas, em um determinado momento, um usuário pertencente ao grupo “auditores” acessa o sistema em busca de uma informação e recebe, como resposta à sua consulta, uma informação completamente diferente da desejada. Neste caso houve uma falha na segurança da informação para este sistema na propriedade relacionada à:

a) Confidencialidade b)

Integridade c) Auditoria

d) Disponibilidade e) Privacidade

1. Considere um sistema no qual existe um conjunto de informações disponível para um determinado grupo de usuários denominados “auditores”. Após várias consultas com respostas corretas e imediatas, em um determinado momento, um usuário pertencente ao grupo “auditores” acessa o sistema em busca de uma informação já acessada anteriormente e não consegue mais acessá-la. Neste caso houve uma falha na segurança da informação para este sistema na propriedade relacionada à
2. Privacidade b) Integridade
   1. Consistência
   2. Irretratabilidade e) Disponibilidade
3. *Criptografia, Assinatura Digital, Hash*
4. Sendo E (o Emissor) que envia uma mensagem sigilosa e criptografada, com chaves pública e privada, para R (o Receptor), pode-se dizer que E codifica com a chave
5. pública de R e R decodifica com a chave pública de E.
6. pública de R e R decodifica com a chave privada de R.
7. pública de E e R decodifica com a chave privada de R.
8. privada de E e R decodifica com a chave pública de R.
9. privada de E e R decodifica com a chave pública de E.
10. Analise as seguintes afirmações relativas a conceitos de proteção e segurança da informação. Um **ataque** é qualquer tentativa de penetrar em um sistema sem autorização. Os ataques podem ser classificados como ativos, quando alteram o conteúdo de uma mensagem, ou passivos, quando somente copiam seu conteúdo.

#### A autenticação

é o processo destinado a verificar a validade de determinada mensagem.

#### A assinatura

**digital** é uma técnica para converter um texto claro em texto criptografado.

#### A criptografia

gera um valor associado a uma determinada mensagem, que a garante contra falsificação. Um exemplo de criptografia são os dígitos de controle usados em conjunto com os números de conta corrente dos bancos.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e III b) II e III c) III e IV

d) I e II e) II e IV

1. Uma **assinatura digital** é um meio pelo qual
2. o gerador de uma mensagem, de um arquivo ou de outras informações codificadas digitalmente vincula sua identidade às informações.
3. os servidores de e-mail substituem uma mensagem pelo equivalente codificado.
4. os servidores de páginas da Web identificam o endereço IP do site de destino.
5. os servidores de páginas da Web identificam o endereço IP do site de origem.
6. os Firewalls utilizam para garantir o repúdio da informação.
7. Quanto aos conceitos básicos de Segurança da Informação é correto afirmar que a criptografia simétrica:
8. usa um algoritmo de criptografia que requer que a mesma chave secreta seja usada na criptografia e na decriptografia.
9. é um método de criptografia no qual duas chaves diferentes são usadas: uma chave pública para criptografar dados e uma chave particular para decriptografá-los.
10. é um método de criptografia no qual duas chaves diferentes são usadas: uma chave particular para criptografar dados e uma chave pública para decriptografá-los.
11. é o processo de regravação de partes de um arquivo em setores contíguos de um disco rígido a fim de aumentar a segurança da informação.
12. é o resultado de tamanho fixo, também chamado de síntese da mensagem, obtido pela aplicação de uma função matemática unidirecional a uma quantidade de dados arbitrária.
13. *Extra*
14. O método de criptografia por chave assimétrica, entre dois pontos em comunicação, baseia-se somente na utilização de
15. uma chave secreta única para as duas pontas.
16. uma chave pública única para as duas pontas.
17. duas chaves secretas, uma para cada ponta.
18. duas chaves públicas, uma para cada ponta.
19. uma chave secreta individual e uma chave pública comum para cada uma das pontas.
20. Segundo a NBR ISO/IEC 17799:2001, o conceito de segurança da informação é caracterizado pela preservação de:
21. que é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
22. que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
23. que é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Preenchem correta e respectivamente as lacunas I, II e III:

1. disponibilidade − integridade – confidencialidade.
2. confidencialidade − integridade – disponibilidade.
3. integridade − confidencialidade − disponibilidade
4. confidencialidade − disponibilidade − integridade
5. disponibilidade − confidencialidade − integridade
6. Os antivírus são programas que NÃO têm capacidade de
7. identificar e eliminar a maior quantidade de vírus possível.
8. analisar os arquivos obtidos pela Internet.
9. evitar o acesso não autorizado a um backdoor instalado.
10. verificar continuamente os discos rígidos e disquetes.
11. procurar vírus em arquivos anexados aos e-mails. Técnico Legislativo – Agente de Polícia – Câmara dos Deputados (07-2007) Um programa capaz de se auto- propagar automaticamente através de redes, enviando cópias de si mesmo, de computador para computador, denomina-se

a) cavalo de tróia. b) macro. c) backup.

d) backdoor. e) worm.

1. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador é o

a) Worm. b) Spyware. c) Backdoor.

d) Keylogger. e) Cavalo de Tróia.

1. As ferramentas antivírus:
2. são recomendadas apenas para redes com mais de 100 estações.
3. dependem de um firewall para funcionarem.
4. podem ser utilizadas independentes do uso de um firewall.
5. e um firewall significam a mesma coisa e têm as mesmas funções.
6. devem ser instaladas somente nos servidores de rede e não nas estações de trabalho.
7. Uma pessoa mal intencionada tenta obter informações como números de cartões de crédito, senhas, dados de contas ou outras informações pessoais convencendo-o a fornecê-las sob pretextos enganosos em um ataque via WEB do tipo

a) phishing scam. b) adware.

c) slice and dice. d) spyware. e) hijack.

Gabarito

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1.C | 2.D | 3.A | 4.D | 5.E | 6.B | 7.D | 8.A | 9.C | 10.E |
| 11.D | 12.B | 13.C | 14.B | 15.D | 16.A | 17.B | 18.E | 19.B | 20.D |
| 21.A | 22.A | 23.E | 24.B | 25.C | 26.E | 27.D | 28.C | 29.A |  |