1. As políticas de segurança de informação:

(a) São as tecnologias que permitem implementar um determinado objetivo de segurança

(b) São normas, regulamentos e orientações que definem o modelo de proteção num determinado domínio de segurança

(c)São processos e mecanismos específicos a utilizar de forma a obter segurança

(d) Definem-se para as pessoas da organização mas não obrigatóriamente para os processos

2. Em que consiste a Integridade da informação?

(a) Garantia que a informação não foi lida por terceiros

(b) Garantia que a informação não é convertida para outro formato

(c) Garantia que a informação é armazenada de forma integral

(d) Garantia que a informação não é alterada

3. Em relação à faceta ofensiva da segurança, assinale a cor-reta.

(a) É ilegal

(b) Diz respeito ao software, mas não aos processos

(c) Foca-se em diminuir o custo de um sistema

(d) É útil para validar a segurança de uma solução

4. Tendo em conta o que é um registo CVE (Common Vul-nerabilities and Erposures), é verdade que:

(a) Um registo CVE estima o valor monetário da exploração da vulnerabilidade

(b) Um registo CVE descreve virus e outras aplicações maliciosas

(c) Um registo CVE identifica formas de proteção de uma vulnerabilidade

(d) Um registo CVE descreve como pode ser realizado um ataque a um software vulnerável

5. O OWASP Top 10 consiste:

(2) Na lista das 10 empresas mais relevantes na área da segurança

(b) Nas 10 vulnerabilidades mais populares em sistemas atuais

(c) Nas 10 fontes de vulnerabilidades mais popslares em sistemas atuais/recentes

(d) Nos 10 mecanismos mais relevantes a implementar

~~6. O mecanismo de tegociação de chaves Dife-Hellman~~

~~(n) É, rolato contra atacantes ativos~~

~~(b) Faz uso de valotes públicos e privados~~

~~(c) Obriga a que on intervenientes dutribuam chaves abr teriormente à merciação~~

~~(d) Implementa um mecanismo de cifra híbrida~~

7. As técnicas de branqueamento em cifras

(a) Aplicara-se a aminataras de forma a esconder o mal-nante

(b) Aplicam chaves ao texto e jou criptograma com XOR

(e) Anonimizam os dados depois de decifradon

(d) Aumentam a difusão de uma cifra

8. Qual das seguintes cifras não existe.

(a) Cifras por blocos recorrendo a cifras contínuas

(b) Cifras por blocos assimétricas

(с) Cifras por blocos simétricas

(d) Cifras contínuas simétricas

9. Quando se diz que uma cifra é realizada em N-bit OFB(Output FeedBack), tal significa que:

(a) Requer um minino de N bits de memoria pars o gerador

(b) Por cada cifra por blocos do seu gerador só são usados N bits do resultado

(c) A cifra por blocos do gerador possui N bits nos blocos de entrada e saída

(d) Evita a propagação de ertos até N bits

10. Tendo em conta apenas a resistência à descoberta de colisoes em funcoes de sintese, qual destas expressoes é verdadeira?

(a) Será tanto menor quanto menor for a dimensão do resultado da função

(b) Se for reduzida, representa um risco caso a função seja usada num MIC (Message Integrily Code)

(c) Tem um limite superior que depende da dimensi da entrada da função

(d) Essa propriedade nao e relevante para a robus

dos processos de criacao e validacao de assinat

digitais

11. Os mecanismos de derivação de chaves (PBKDF2, são importantes para:

(a) Aumentar o universo de pesquisa da palavra

(b) Reduzir o universo de pesquisa da passe

(c) Evitar ataques por dicionário, sem imy ataques for força bruta

(d) Aumentar o custo de ataques por diciona

12. Um MIC (Message Integrity Code)

(a) É robusto contra modificações aleatórias de transmissao

(b) É implementado através de cifras assimétricas

(e) É implementado através de cifras c...

(d) Faz uso de uma chave conhecida a… locutores

8. Na autenticação de utentes do sistema Linux:

(a) Apenas o utilizador root pode aceder ao armazenamento de credenciais dos utentes

(b) A utilização de um sal reduz a segurança do sistema

(c) O acesso às credenciais de vários utentes permite rapidamente verificar quais são semelhantes

(d) O administrador pode alterar o método de armazenamento das credenciais

9. Relativamente ao mecanismo apparmor, qual das afirmações é correta?

(a) Uma aplicação pode escolher ignorar as regras do mecanismo

(b) Apenas limita as comunicações na rede

(c) As regras aplicam-se a aplicações com um nome es-pecífico, em qualquer local do sistema de ficheiros

(d) Apenas controla chamadas ao núcleo do sistema

10. Tendo em conta a existência de diferentes níveis de proteção na execução de um CPU (protection rings), indique a resposta certa:

(a) Os níveis podem ser definidos pelos sistemas opera-

tivos

(b) Não é possível transitar de um nível menos privile giado para outro mais privilegiado

(e) Os sistemas operativos podem definir as instrugdes

que podem fazer parte de cada nível

(d) Os sistemas operativos usam esses níveis para separar ações do seu núcleo das demais ações realizadas por aplicações

11. No Linux, relativamente ao comando sudo, qual das seguintes afirmações é **falsa**?

a) É um comando que serve para concretizar elevaçoes de privilégios pontuais, logo útil para concretizar políticas de privilégio mínimo

(b) Permite que os comandos realizados para fins de administração sejam registados em nome de quem os executou

(c) É um comando cujo ficheiro possui o bit Set-UID ativo e cujo dono é **root**  
(d)Pode ser utilizado por qualquer utilizador para o fim a que o mesmo se destina

12. No UNIX/Linux, caso um ficheiro tenha a proteção -w- rwx --x, qual dos seguintes acessos é negado?

(a) Escrita/alteração por um processo com um GID igual ao do ficheiro

(b) Leitura por um processo com um GID igual ao do ficheiro

(c) Escrita/alteração pelo dono

(d) Leitura por um processo que não possua o seu GID

13. Relativamente à utilização de sistemas de armazenamento em fornecedores remotos:

(a) Se o fornecedor for de confiança, os dados devem ser armazenados em claro para maximizar a performance

(b) Implica confiança em vários administradores

(c) As chaves de cifra da informação devem ser tendencialmente armazenadas pelo fornecedor de serviço

(d) Utilização de cifra de informação aumenta a disponibilidade por um número alargado de sujeitos