1. **Relativamente à autenticação no GSM, indique a resposta errada:**
    a. Permite autêntica os terminais móveis mas não permite autenticar a rede
    b. Usa um protocolo de autenticação multimétodo
    c. Baseia-se no conhecimento mútuo de uma chave secreta
    d. Não é imune a ataques com dicionários

2. **Relativamente à autenticação de utentes com S/Key, indique a resposta errada:**
    a. O autenticador tem acesso à senha original dos clientes
    b. Os autenticados precisam de reinstalar as suas credenciais de autenticação após um determinado número de utilizações
    c. As senhas descartáveis são geradas a partir de uma senha
    d. Permite que, para o mesmo utente, a mesma senha produza senhas descartáveis diferentes para sistemas diferentes

3. **Relativamente à autenticação com desafio-resposta, indique a resposta errada:**
    a. Não é tipicamente aplicável a autenticações biométricas
    b. É fundamental que os desafios apresentados a uma mesma credencial nunca se repitam
    c. Visa proteger as credenciais usadas no processo de autenticação
    d. Não permite uma fácil implantação de protocolos de autenticação mútua

4. **Relativamente à autenticação de utentes com RSA Secure ID, indique a resposta errada:**
    a. É imune a ataques com dicionários
    b. As senhas descartáveis são geradas a partir de uma chave secreta
    c. Obriga a que os que utentes usem um equipamento próprio (ou uma aplicação)
    d. A chave secreta de cada utente é gerada a partir de uma senha

5. **A arquitetura PAM (escolha a resposta errada):**
    a. Permite adicionar novos mecanismos de autenticação sem alterar as aplicações
    b. Permite customizar mecanismos de autenticação
    c. É uma forma de separar a forma de autenticar da necessidade que as aplicações têm que ela ocorra
    d. Permite que as aplicações programaticamente orquestrem a forma como querem concluir os seus processos de autenticação

6. **Qual dos seguintes modelos de controlo de acesso controla a integridade em fluxos de informação?**
    a. Clark-Wilson
    b. Bell-LaPadula (confidencialidade dos dados)
    c. Biba (políticas de segurança)
    d. RBAC

7. **A não observância do princípio do Privilégio Mínimo (escolha a resposta errada):**
    a. Permite que os utentes se possam exceder nas suas actividades
    b. Permite abusos
    c. Abre caminho a problemas causados involuntariamente
    d. É perfeitamente aceitável caso haja um sistema robusto de auditoria

8. **Relativamente à autenticação de utentes baseados em senhas descartáveis, indique a resposta errada.**
    a. Pode envolver a troca de um desafio para indicar a senha descartável a ser usada.
    b. Exige que o utente tenha de ter algo para memorizar ou gerar as senhas descartáveis.
    c. É imune a ataques com dicionários
    d. Tipicamente não permite autenticação mútua.

9. **Relativamente à autenticação no GSM, indique a resposta errada:**
    a. Permite autenticar os terminais móveis mas não permite autenticar a rede.
    b. A posse do módulo SIM onde está a chave secreta é normalmente suficiente para um terminal móvel se autenticar
    c. Permite delegar a autenticação dos terminais móveis noutras redes
    d. Baseia-se no conhecimento mútuo de uma chave secreta

10. **Relativamente à autenticação de utentes do UNIX/Linux indique a resposta errada:**
    a. Usa senhas memorizadas
    b. Usa valores guardados em ficheiros inacessíveis aos utentes comuns.
    c. Não deverá ser usada para criar sessões remotas sobre comunicações não seguras
    d. Usa uma aproximação desafio-resposta

11. **Relativamente à autenticação no SSH indique a resposta errada:**
    a. Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor
    b. Permite que os utentes se autentiquem de forma flexível
    c. Protege a autenticação dos clientes realizando-a no âmbito de uma comunicação segura
    d. Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou o nome DNS)

12. **Considerando um mecanismo de Set-UID / Set-GID, qual é a afirmação verdadeira:**
    a. Um processo possui as permissões do grupo com o real GID associado ao processo
    b. A permissão do Set-GID altera o GID associado a um ficheiro
    c. O mecanismo Set-UID não permite que um utilizador obtenha mais permissões do que as que já possui.
    d. Um ficheiro com permissão Set-UID irá executar com as permissões do UID do dono do ficheiro

13. **No UNIX/Linux, caso um ficheiro tenha a proteção - wxrwx--x, qual dos seguintes acessos é negado?**
    a. Execução por um processo com um GID igual ao do ficheiro
    b. Execução pelo dono
    c. Leitura pelo dono
    d. Alteração do bit Set-UID pelo dono

14. **No UNIX/Linux relativamente ao comando sudo, qual das seguintes afirmações é falsa?**
    a. Permite realizar uma elevação de privilégios por comando
    b. É um comando especial que é reconhecido como tal pelo núcleo do sistema operativo.
    c. É um comando que serve para concretizar elevações de privilégios pontuais, logo é útil para concretizar políticas de privilégio mínimo.
    d. Permite que os comandos realizados para fins de administração sejam registados em nome de quem os executou.

15. **No UNIX/Linux qual dos seguintes direitos está sempre vedado ao dono de um ficheiro (excepto se for root)?**
    - **a.** Alterar o seu dono
    - **b.** Alterar a proteção relativa ao seu dono
    - **c.** Eliminar o nome de um ficheiro
    - **d.** Alterar o seu grupo

16. **A técnica de K-anonimato aplicada a uma base de dados destina-se a:**
    - **a.** Nunca dar menos do que K linhas em qualquer pergunta
    - **b.** Não fornecer mais do que K valores diferentes em cada linha em qualquer pergunta
    - **c.** Não fornecer mais do que K colunas em qualquer pergunta
    - **d.** Não fornecer mais do que K valores diferentes em cada coluna em qualquer pergunta

17. **Numa base de dados, o mecanismo de atualização em duas fases:**
    - **a.** Garante uma evolução global da base de dados de acordo com as alterações requeridas
    - **b.** Cria uma réplica da base de dados em cada transação, podendo reverter para a anterior em caso de necessidade
    - **c.** Valida primeiro os dados fornecidos numa transação e atualiza só se forem válidos
    - **d.** Assegura a correção dos valores guardados na base de dados

18. **No Java, uma política de segurança(secure policy) (escolhe a resposta errada):**
    - **a.** É um conjunto de autorizações dadas e negadas
    - **b.** Possui um conjunto de valores iniciais especializados? em ficheiros de configuração
    - **c.** é algo que existe sempre em qualquer execução de uma jvm
    - **d.** Não pode ser programaticamente alterado a partir de uma aplicação

Respostas:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
d	a	d	a	d	a	d	c	b	d	a	d	c	b	a	a	a	d

Qual das seguintes afirmações é falsa relativamente à cifra de ficheiros usando aplicações?

a) Não existe um método padrão de identificar se um ficheiro está cifrado
b) Permitem cifras diferentes em cada ficheiro
c) Permite que os ficheiros partilhados em rede circulem de forma cifrada
d) A partilha de utentes por vários utentes é simples