

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.

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

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

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 autenticuem 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 (excepto o endereço IP, ou o nome DNS)

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**

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

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.

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

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) Permite 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**

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

Numa base de dados, o mecanismo de atualização em duas fases:

- a) **NOT SURE** 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

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

Qual das seguintes afirmações é **falsa** tendo em conta o que é um registo CVE?

- a) Um registo CVE dá algumas indicações de como uma vulnerabilidade pode ser explorada
- b) Um registo CVE refere a potencial gravidade de um ataque face a uma vulnerabilidade
- c) Um registo CVE descreve uma vulnerabilidade num software
- d) Um registo CVE descreve como pode ser realizado um ataque a um software vulnerável

O processo de manipulação da cache ARP de um sistema remoto designa-se por:

- a) ARP Resolution
- b) ARP Spoofing - spoofing é so a criação do falso ARP certo?
- c) ARP Poisoning
- d) ARP Corruption

~~Qual é o objetivo dos Stack Canaries?~~

- a) Detetar quando algum código escreve dados para outras aplicações?
- b) Detetar quando algum código altera o registo EBP
- c) Detetar quando algum código altera o registo ESP
- d) Detetar quando algum código escreve dados para além das suas variáveis locais

Qual das seguintes respostas corresponde a uma vantagem introduzida pelos processos de randomização de chaves assimétricas? (OAEP)

- a) O mesmo valor, cifrado várias vezes com a mesma chave assimétrica, produz sempre o mesmo valor
- b) Permite fazer um controlo de integridade do criptograma, após a sua decifra
- c) Impede a criptanálise de valor conhecidos cifrados com chaves privadas
- d) Permite acelerar as cifras assimétricas

Qual dos seguintes modos de cifra não propaga erros do criptograma para outros bits que não os correspondentes do texto recuperado?

- a) GCM (Galois/Counter Mode)
- b) CFB
- c) ECB
- d) CBC

Qual dos seguintes modos de cifra não permite um acesso aleatório constante na decifra?

- a) CFB
- b) CTR
- c) GCM
- d) OFB

Qual das seguintes propriedades de uma função de síntese não é seguramente vital para assegurar a qualidade de uma assinatura digital?

- a) Resistência à colisão
- b) Resistência à procura de um texto original
- c) Resistência à procura de um segundo texto original
- d) Elevado desempenho

No cálculo de um MAC qual dos seguintes tipos de funções é normalmente usado?

- a) Cifra de Vernam
- b) Cifras simétricas por blocos
- c) Cifras assimétricas
- d) Cifras simétricas contínuas

Um dos objectivos das assinaturas digitais é o não-repúdio, que consiste em:

- a) Garantir que uma mensagem, no documento, não sofreu qualquer alteração
- b) Impedir o acesso não autorizado ao conteúdo das mensagens/documentos
- c) Forçar o uso de smartcards na geração de assinaturas
- d) Impedir que uma entidade que produziu uma mensagem/documento assinada(o) o possa negar

Para se verificar uma assinatura digital de um documento é preciso:

- a) A chave privada do assinante
- b) O certificado de chave pública do verificador
- c) O certificado de chave privada do assinante
- d) O certificado de chave publica do assinante

Uma Entidade Certificador raiz é confiável porque

- a) Confiamos na correção da sua chave pública
- b) Ninguém certifica o seu certificado
- c) Tem um certificado autoassinado
- d) Certifica muitas outras Entidades Certificadoras

Tendo em conta o periodo de validade de um certificado, qual destas afirmações é falsa?

- a) Serve para limitar, no tempo, o uso da correspondente chave privada
- b) Impede que a chave privada possa ser usada fora desse periodo
- c) Não pode ser usado para validar assinaturas feitas fora desse periodo
- d) Pode ser encurtado caso seja revogado

