1- Para realizar a autenticação com um SmartCard, o que deve ser enviado entre as entidades para realizar uma autenticação unidirecional?

(a) O autenticador envia um NONCE e o autenticado envia uma assinatura do valor usando a sua chave pública.

(b) O autenticador envia um NONCE e o autenticado envia uma assinatura do valor usando a sua chave privada

(c) O autenticador envia um NONCE e o autenticado envia uma assinatura do valor usando o PIN

(d) O autenticador espera pelo autenticado, que envia a sua chave publica

2- Um processo de autenticação serve essencialmente para:

1. Permitir a execução de cifras mais robustas

(b) Controlar o acesso de indivíduos

(c) Obter um atributo, objeto ou conhecimento

(d) Facilitar a exploração de outros protocolos

3- Considerando a autenticação de utentes em Smartphones:

(a) Armazena os modelos biométricos e senhas no cartão SIM

(b) A exploração de canais paralelos pode ser problema para autenticação com PIN

(c) O gatekeeperd reconhece as impressões digitais

(d) O reconhecimento facial é considerado robusto

4- Relativamente à autenticação de utentes com desafio resposta e pares de chaves assimétricas:

(a) Implica que os autenticadores protejam as credenciais de autenticação dos seus clientes

(b) É fundamental assegurar a randomização das cifras dos desafios (e.g. com Optimal Assym Enc Padding)

(c) Não requer dispositivos adc para calculo da resposta

(d) A utilização de certificados de chave publica pode fornecer os mecanismos de identificação de quem se autentica

5- Na autenticação de utentes do sistema Linux:

1. A utilização de um sal reduz a segurança do sistema
2. O acesso às credenciais de vários utentes permite rapidamente verificar quais são semelhantes
3. As informações sobre a shell de um utente são armazenadas no ficheiro /etc/passwd
4. O file /etc/shadow é uma cópia de segurança do ficheiro /etc/passwd

6- Qual dos seguintes de autenticação é vulnerável a ataques com dicionários?

1. TTLS
2. TLS
3. RSA securID
4. MS-CHAP v2

7- Relativamente à autenticação com desafio e resposta:

1. Implica sempre a troca de mais do que uma mensagem
2. Pode ser utilizado em comunicações unidirecionais
3. Requer a utilização de canais seguros
4. Obriga a que o autenticador armazene respostas a vários desafios

8- Qual das seguintes opções representa um tipo de prova de autenticação?

1. Algo que temos
2. Algo que testamos
3. Algo que compramos
4. Algo que propagamos

9- No Linux, relativamente ao comando sudo, qual das seguintes afirmações é falsa?

1. Permite realizar uma elevação de privilégios por comando
2. É um comando cujo ficheiro possui o bit Set-UID ativo e cujo dono é root.
3. É um comando especial que é reconhecido como tal pelo núcleo do sistema operativo.
4. É um comando que serve para concretizar elevações de privilégios pontuais, logo útil para concretizar políticas de privilégio mínimo.

10- Uma MV é importante para a segurança de um sistema, devido a mecanismos como:

1. Integridade da informação
2. Duplicação dos dados do utilizador
3. Execução de Anti Virus
4. Prioritização de acesso a recursos

11- Para alterar os controlos de acesso discricionários do kernel Linux é necessário:

1. Alterar o ficheiro /etc/controls.conf de forma adequada
2. Adicionar o argumento CONTROLS = custom ao início do kernel
3. Definir as Access Control Lists de forma adequada, usando um user com essas permissões
4. Alterar o código do kernel e recompilar

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

1. Alteração do bit Set-UID pelo dono
2. Execução pelo dono
3. Escrita/Alteração por um processo com um GID igual ao do ficheiro
4. Execução por um processo com um GID igual ao do ficheiro

13- Que formato será melhor escolha para cifrar a fotografias a nível aplicacional?

1. EncApp
2. WAV
3. TIFF
4. ZIP

14- Considerando a cifra a nível do sistema de ficheiros:

1. É efetuada pelas aplicações antes de cada operação de fwrite.
2. Em algumas situações, permite a exploração segura de sistemas de armazenamento em Cloud (ex: Dropbox)
3. É considerado inseguro pois o sistema de ficheiros não é confiável.
4. Tem de ser usado da mesma forma por tds os users de um sistema

15- Relativamente à utilização de sistemas de armazenamento em fornecedores remotos:

1. Aumenta o nº de sujeitos com acesso à informação
2. Se o fornecedor for de confiança, pode ser realizada pela internet sem cifra dos dados
3. Utilização de cifra de informação aumenta a disponibilidade por um nº alargado de sujeitos
4. Não aumenta o risco de acesso à informação por sujeitos indevidos

16- Num sistema RAID 4 com N discos, qual a situação limite, apos o qual existirá perda de informação?

1. Avaria de qualquer disco, exceto o que contém as somas de controlo (paridade)
2. Avaria de 1 disco (qualquer)
3. Avaria de 5 discos
4. Avaria de todos os N discos

17- Descreva um cenário com autenticação Multifatorial onde não seja desejável usar biometria. Justifique a sa resposta.

18- Em Linux, como é q um binário executado do sistema de ficheiros é associado a um contexto de permissões para acesso a ficheiros?