TESTE 2021/2022 (FRENTE ONLY)

1. **Relativamente à autenticação com desafio e resposta:**
    a. **Não permite uma fácil implementação do protocolo de autenticação mútua.**
    b. **Não pode ser utilizada em combinação com smart-cards.**
    c. **Pode ser utilizada em autenticações unidirecionais.**
    d. **É fundamental que os desafios apresentados a uma mesma credencial nunca se repitam.**

2. **Relativamente à autenticação por apresentação de senha direta memorável:**
    a. **O sal serve para aumentar o tamanho das senhas.**
    b. **É vulnerável a ataques por dicionário.**
    c. **Os utentes memorizam senhas complexas com facilidade.**
    d. **Se o administrador definir a (dnawdsin) de senhas de 256 bits aleatórias, o processo torna-se seguro.**

3. **Considerando a autenticação de utentes em Smartphones:**
    a. **O Trusted Execution Environment é um (dainsd) seguro implementado pelo cartão SIM.**
    b. **As chaves são fornecidas às aplicações pelas componentes do TEE para validação.**
    c. **O reconhecimento facial é considerado robusto.**
    d. **A exploração de (idinaisnd) paralelos pode ser um problema para autenticação com PIN.**

4. **Relativamente à autenticação de utentes com S/Key:**
    a. **Permite que para o mesmo utente, a mesma senha produza senhas descartáveis diferentes para sistemas diferentes.**
    b. **As senhas descartáveis são geradas (dinaiwds) a partir de uma senha.**
    c. **Usa pares de chaves (daswmdawsmd nao sei o resto).**
    d. **É um protocolo de autenticação mútua.**

5. **Relativamente à autenticação biométrica de utentes:**
    a. **Facilita a transferência de credenciais entre utentes.**
    b. **É um método de autenticação ideal quando se tem muitos utentes.**
    c. **É um método de autenticação universal (não exclui pessoas).**
    d. **Pode dar origem a falsos negativos, mas estes não são perigosos.**

6. **A segunda fase do 802.1X destina-se a:**

    a. **Autenticar mutuamente o Suplicante e o Servidor de Autenticação.**
    b. **Autenticar apenas o Servidor de Autenticação.**
    c. **Autenticar mutuamente o Autenticador e o Servidor de Autenticação.**
    d. **Autenticar apenas o Suplicante.**

7. **A proteção de tráfego Wi-Fi no meio sem fios com WEP permite qual das seguintes funcionalidades?**
    a. **Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES.**
    b. **Controlo de integridade do cabeçalho e da carga útil com Michel(wtf).**
    c. **Cifra da cagar útil com o algoritmo RC4.**
    d. **Cifra de carga útil com o algoritmo AES.**

8. **A autenticação WPA no acesso a um terminal móvel à rede:**
    a. **Depende sempre de um serviço central de autenticação.**
    b. **Mantém a autenticação SKA do WEP mas evita a sua insegurança.**
    c. **Segue os princípios do padrão 802.1X.**
    d. **Elimina apenas o modo OSA do WEP.**

9. **No UNIX/Linux caso um ficheiro tenha a proteção -u-rwx---x, qual dos seguintes acessos é negado?**
    a. **Leitura por um processo com um GID igual ao do ficheiro.**
    b. **Escrita/alteração por um processo com um GID igual ao do ficheiro.**
    c. **Escrita/alteração pelo dono.**
    d. **Leitura pelo dono.**

10. **Considerando que um ficheiro pertence ao utilizador root (uid=0) e grupo root (gid=0), tendo as permissões rwxrwxrwx-x (not sure if that is whats written xd), se este for executado pelo utilizador com uid=1000 e gid=1000, qual é a informação correta do processo?**
    a. **O root UID terá o valor 0 e o effective UID terá o valor 0.**
    b. **O root UID terá o valor 0 e o root GID terá o valor 0.**
    c. **O real UID terá o valor 1000 e o root GID terá o valor 0.**
    d. **o effective UID terá o valor 0 e o effective GID terá o valor 0.**

11. **No UNIX/Linux, relativamente à chamada ao sistema chroot, qual das seguintes afirmações é verdadeira?**
    a. **(i can't read this one, um gajo não é de ferro)**

---------- FIM DE UM DOS TESTES (SÓ TEM PARTE DA FRENTE)----------

OUTRO TESTE 2021/2022 (FRENTE ONLY)

1. **Relativamente à autenticação usando TLS (Transport Layer Security):**
    a. **Não protege a integridade da informação.**
    b. **Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS).**
    c. **O cliente pode escolher livremente quais as credenciais que usa na sua autenticação.**
    d. **É vulnerável a ataques por dicionário.**

2. **Na autenticação de utentes do sistema Linux:**
    a. **O processo de autenticação não suporta múltiplos fatores.**
    b. **A senha é armazenada no disco, depois de validada pelo TPM.**
    c. **O administrador pode alterar o método de armazenamento das credenciais.**
    d. **O ficheiro /etc/shadow possui um backup do ficheiro /etc/passwd**

3. **Qual dos seguintes protocolos de autenticação é vulnerável a ataques com dicionário?**
    a. **TTLS.**
    b. **RSA SecurID.**
    c. **SSH.**
    d. **Linux (diz aqui qualquer merda unix mas eu não percebo).**

4. **Relativamente à autenticação no GSM (Global System for Mobile Communications):**
    a. **Baseia-se no conhecimento mútuo (utente e rede) de um PIN.**
    b. **O desafio enviado pela rede é baseado no PIN.**
    c. **A função de transformação do desafio apresentado pela rede é universal e realizada pelos terminais móveis.**
    d. **É imune a ataques com dicionário.**

5. **Na autenticação de utentes do sistema MS Windows:**
    a. **O TPM fornece credenciais ao sistema após desbloqueio com um PIN.**
    b. **O TEE executa um sistema seguro para armazenamento de credenciais.**
    c. **O reconhecimento facial faz uso de um PIN para identificação do utilizador.**
    d. **O método NTLM Password hash calcula uma síntese da senha com SALT.**

6. **O EAP (Extensible Authentication Protocol):**
    a. **É um protocolo de autenticação baseado em chaves assimétricas.**
    b. **É usado no 802.1X para autenticar um Suplicante perante um Autenticador.**
    c. **É um protocolo que permite entender outros protocolos de autenticação.**
    d. **É usado no 802.1X para autenticar um Suplicante perante um Servidor de Autenticação.**

7. **A proteção do tráfego Wi-Fi por meio sem fios com TKIP permite qual das seguintes funcionalidades?**
    a. **Controlo de integridade do cabeçalho e da carga útil com Michael(who the fk is Michael?).**
    b. **Controlo de integridade do cabeçalho e da carga útil com CRC-32.**
    c. **Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES.**
    d. **Controlo de integridade da carga útil com CBC-MAC e AES.**

8. **A autenticação do WPA no acesso a um terminal móvel à rede:**
    a. **Depende sempre de um serviço central de autenticação.**
    b. **Mantém a autenticação SKA do WEP mas evita a sua insegurança.**
    c. **Usa sempre EAP.**
    d. **Realiza sempre uma distribuição de chaves ao Suplicante e ao Autenticador.**

9. **Tendo em conta a existência de diferentes níveis de proteção na execução de um CPU (protection rings), indique a resposta certa:**
    a. **Sem esses níveis o núcleo de um sistema operativo estaria vulnerável a ataques feitos pelas aplicações.**
    b. **Os sistemas operativos podem definir as instruções que podem fazer parte de cada nível.**
    c. **Não é possível transitar de um nível menos privilegiado para outro mais privilegiado.**
    d. **Existe uma relação direta entre esses níveis e os privilégios de administração de um sistema operativo.**

10. **Relativamente ao mecanismo AppArmor, qual das seguintes afirmações é correta?**
    a. **Não é útil para vários programas interpretados quando chamados através do seu interpretador (ex python3 app.py).**
    b. **Implementa um mecanismo de armadura que protege as aplicações de atacantes externos.**
    c. **Uma aplicação pode escolher ignorar as regras do mecanismo.**
    d. **fodeu, está numa pagina que eu nao tenho :').**

11. **Considerando o mecanismo Set-UID/Set-GID, qual é a afirmação verdadeira?**
    a. **Um ficheiro com permissões Set-UID irá executar com as permissões de quem o executa.**
    b. **O mecanismo de Set-UID afeta o effective UID de um processo mas mantém o seu real UID inalterado.**
    c. **Um processo possui as permissões do utilizador com o real UID associado ao processo.**
    d. **A permissão de Set-GID altera o GID associado a um ficheiro.**

12. **Considerando o UNIX/Linux, qual das seguintes afirmações é verdadeira?**
    a. **Cabe exclusivamente ao seu núcleo a função de gerir um modelo computacional independente do hardware.**
    b. **A interação entre processos pode-se realizar sem qualquer pedido expresso ao núcleo.**
    c. **Os procedimentos de login de um utente são geridos pelo seu núcleo.**
    d. **Um processo com privilégios de administração tem acesso irrestrito a todas as instruções do CPU.**

13. Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?

a. **RAID 1.**
b. **RAID 0+1**
c. **RAID 6.**
d. **RAID 5.**

14. Num sistema RAID 1 com N discos, qual a situação limite, após o qual existirá perda de informação?

a. **Avaria de N-1 discos.**
b. **Avaria de apenas um disco (qualquer).**
c. **Avaria de 3 discos.**
d. **Avaria de 2 discos.**

15. Num sistema RAID 0 com N discos, qual a situação limite, após o qual existirá perda de informação?

e. **A avaria de qualquer disco implica sempre a perda de informação.**
f. **Avaria de todos os N discos.**
g. **Avaria de ambos os discos com as somas de controlo (paridade).**
h. **Avaria de N-1 discos.**

16. No protocolo TLS, qual é o objetivo e conteúdo de uma definição de uma CipherSuite?

17. Num sistema de backups, devem existir cópias em vários níveis, ou deve-se escolher um nível em particular? Justifique.

---------- FIM DO TESTE (FRENTE E VERSO)----------

EXAME 2021/2022 (FRENTE E VERSO)

1. **Relativamente à autenticação no SSH (Secure Shell):**
   a. **Usa sempre segredos partilhados entre utentes e servidor.**
   b. **Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor.**
   c. **Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS).**
   d. **É da responsabilidade do servidor SSH forçar a utilização de segredos complexos.**

2. **Relativamente à autenticação usando TLS (Transport Layer Security):**
    a. **Não protege a integridade da informação.**
    b. **Serve para garantir a negociação de uma chave de sessão entre os interlocutores corretos.**
    c. **O cliente pode escolher livremente quais as credenciais que usa na sua autenticação.**
    d. **A autenticação dos clientes é uma opção dos mesmos.**

3. **Relativamente à autenticação GSM (Global System for Mobile Communications):**
    a. **A função de transformação do desafio apresentado pela rede é universal e realizada pelos terminais móveis.**
    b. **Baseia-se no conhecimento mútuo (utente e rede) de um PIN.**
    c. **A posse do módulo SIM onde está a chave secreta é normalmente suficiente para um terminal móvel se autenticar.**
    d. **Usa um protocolo de autenticação multimétodo.**

4. **Relativamente à autenticação de utentes com S/Key:**
    a. **São usadas senhas descartáveis memorizadas pelos utentes.**
    b. **Os autenticadores precisam de reinstalar as suas credenciais de autenticação após um determinado número de utilizações.**
    c. **É imune a ataques de dicionário.**
    d. **É um protocolo de autenticação mútua.**

5. **Relativamente à autenticação de utentes com desafio resposta e pares de chaves assimétricas:**
    a. **Quem se autentica deve cifrar a resposta com a chave pública do autenticador.**
    b. **Quem se autentica deve apresentar a sua chave privada.**
    c. **A utilização de certificados de chave pública pode fornecer os mecanismos de identificação de quem se autentica.**
    d. **A validação das credenciais obriga à pré-partilha da chave pública do autenticador.**

6. **A proteção do tráfego Wi-Fi no meio sem fios com WEP permite qual das seguintes funcionalidades:**
    a. **Controlo de integridade da carga útil com CBC-MAC e AES.**
    b. **Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES.**
    c. **Controlo de integridade da carga útil com Michael.**
    d. **Controlo de integridade da carga útil com CRC-32.**

7. **A autenticação do WPA no acesso de um terminal móvel à rede:**
    a. **Usa sempre EAP**
    b. **Permite a utilização de SKA para sistemas mais antigos.**
    c. **Elimina apenas o modo OSA do WEP.**
    d. **Permite o modelo SOHO para redes de pequenas dimensão.**

8. **A fase four-way Handshake do 802.1X destina-se:**
    a. **Autenticar mutuamente o Suplicante e o Servidor de Autenticação.**
    b. **Distribuir chaves criptográficas entre o Suplicante e o Servidor de Autenticação.**
    c. **Distribuir chaves criptográficas entre o Autenticador e o Servidor de Autenticação.**
    d. **Autenticar mutuamente o Suplicante e o Autenticador.**

9. **No UNIX/Linux, caso um ficheiro tenha a proteção -w-rwx--x, qual dos seguintes acessos é negado?**
    a. **Escrita/alteração pelo dono.**
    b. **Execução por um processo com GID igual ao ficheiro.**
    c. **Leitura pelo dono.**
    d. **Leitura por um processo com um GID igual ao ficheiro.**

10. **Relativamente ao mecanismo AppArmor, qual das afirmações é correta?**
    a. **Não acrescenta nada face ao mecanismo (o resto está tapado).**
    b. **Apenas limita as comunicações na rede.**
    c. **Aplica regras genéricas, válidas para aplicações com o mesmo comportamento.**
    d. **Não se aplica a processos executados pelo root.**

11. **Considerando o mecanismo Set-UID/Set-GID, qual é a afirmação verdadeira?**
    a. **A permissão do Set-UID altera o UID associado a um ficheiro.**
    b. **A permissão do Set-UID altera o GID associado a um ficheiro.**
    c. **Um ficheiro com permissões Set-UID irá executar com as permissões de quem o executa.**
    d. **Um ficheiro com permissão Set-UID irá executar com as permissões do UID do dono do ficheiro.**

12. **Relativamente ao mecanismo de namespaces qual das afirmações é correta?**
    a. **É equivalente ao mecanismo AppArmor.**
    b. **Os interfaces de rede não podem pertencer a um namespace pois não são processos.**
    c. **Os processos não podem pertencer a vários namespaces.**
    d. **Os processos podem pertencer a vários namespaces de tipos diferentes.**

13. **Em relação às cópias de segurança ao nível do sistema de ficheiros, que afirmação é correta?**
    a. **Permitem utilizar mecanismos de duplicação de blocos.**
    b. **Garantem integridade do estado de cada ficheiro.**
    c. **Não garantem integridade do estado global dos ficheiros.**
    d. **Não garantem integridade do estado de cada ficheiro.**

14. **Relativamente ao método dos backups incrementais do sistema de ficheiros, qual das afirmações é verdadeira?**

a. **A adição de novos dados é feita considerando o último backup completo.**
b. **A longo prazo, o carácter incremental deste método irá resultar na utilização de mais espaço do que backups completos.**
c. **A recuperação de dados é mais complexa que em outros métodos.**
d. **Permite salvaguardar versões incrementais e globalmente consistentes de bases de dados.**

15. **Num sistema RAID 4 com N discos, qual a situação limite, após o qual existirá perda de informação?**
    a. **Avaria de todos os N discos.**
    b. **Avaria do disco que contém as somas de controlo e um outro qualquer.**
    c. **Avaria de qualquer disco, excepto o que contém as somas de controlo (paridade).**
    d. **Avaria de 1 disco (qualquer).**

16. **Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?**
    a. **RAID 6**
    b. **RAID 0**
    c. **RAID 1**
    d. **RAID 0+1**

17. **No protocolo TLS, qual é o objetivo e conteúdo de uma definição de uma CipherSuite?**

18. **Num sistema de backups, devem existir cópias em vários níveis, ou deve-se escolher um nível em particular? Justifique.**