**TESTE 2021/2022 (FRENTE ONLY)**

1. **Relativamente à autenticação com desafio e resposta:**
2. **Não permite uma fácil implementação do protocolo de autenticação mútua.**
3. **Não pode ser utilizada em combinação com smart-cards.**
4. **Pode ser utilizada em autenticações unidirecionais.**
5. **É fundamental que os desafios apresentados a uma mesma credencial nunca se repitam.**
6. **Relativamente à autenticação por apresentação de senha direta memorável:**
   1. **O sal serve para aumentar o tamanho das senhas.**
   2. **É vulnerável a ataques por dicionário.**
   3. **Os utentes memorizam senhas complexas com facilidade.**
   4. **Se o administrador definir a (dnawdsin) de senhas de 256 bits aleatórias, o processo torna-se seguro.**
7. **Considerando a autenticação de utentes em Smartphones:**
8. **O Trusted Execution Environment é um (dainsd) seguro implementado pelo cartão SIM.**
9. **As chaves são fornecidas às aplicações pelas componentes do TEE para validação.**
10. **O reconhecimento facial é considerado robusto.**
11. **A exploração de (idinaisnd) paralelos pode ser um problema para autenticação com PIN.**
12. **Relativamente à autenticação de utentes com S/Key:**
13. **Permite que para o mesmo utente, a mesma senha produza senhas descartáveis diferentes para sistemas diferentes.**
14. **As senhas descartáveis são geradas (dinaiwds) a partir de uma senha.**
15. **Usa pares de chaves (daswmdawsmd nao sei o resto).**
16. **É um protocolo de autenticação mútua.**
17. **Relativamente à autenticação biométrica de utentes:**
18. **Facilita a transferência de credenciais entre utentes.**
19. **É um método de autenticação ideal quando se tem muitos utentes.**
20. **É um método de autenticação universal (não exclui pessoas).**
21. **Pode dar origem a falsos negativos, mas estes não são perigosos.**
22. **A segunda fase do 802.1X destina-se a:**
23. **Autenticar mutuamente o Suplicante e o Servidor de Autenticação.**
24. **Autenticar apenas o Servidor de Autenticação.**
25. **Autenticar mutuamente o Autenticador e o Servidor de Autenticação.**
26. **Autenticar apenas o Suplicante.**
27. **A proteção de tráfego Wi-Fi no meio sem fios com WEP permite qual das seguintes funcionalidades?**
28. **Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES.**
29. **Controlo de integridade do cabeçalho e da carga útil com Michel(wtf).**
30. **Cifra da cagar útil com o algoritmo RC4.**
31. **Cifra de carga útil com o algoritmo AES.**
32. **A autenticação WPA no acesso a um terminal móvel à rede:**
33. **Depende sempre de um serviço central de autenticação.**
34. **Mantém a autenticação SKA do WEP mas evita a sua insegurança.**
35. **Segue os princípios do padrão 802.1X.**
36. **Elimina apenas o modo OSA do WEP.**
37. **No UNIX/Linux caso um ficheiro tenha a proteção -u-rwx---x, qual dos seguintes acessos é negado?**
38. **Leitura por um processo com um GID igual ao do ficheiro.**
39. **Escrita/alteração por um processo com um GID igual ao do ficheiro.**
40. **Escrita/alteração pelo dono.**
41. **Leitura pelo dono.**
42. **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?**
    1. **O root UID terá o valor 0 e o effective UID terá o valor 0.**
    2. **O root UID terá o valor 0 e o root GID terá o valor 0.**
    3. **O real UID terá o valor 1000 e o root GID terá o valor 0.**
    4. **o effective UID terá o valor 0 e o effective GID terá o valor 0.**
43. **No UNIX/Linux, relativamente à chamada ao sistema chroot, qual das seguintes afirmações é verdadeira?**
    1. **(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):**
   1. **Não protege a integridade da informação.**
   2. **Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS).**
   3. **O cliente pode escolher livremente quais as credenciais que usa na sua autenticação.**
   4. **É vulnerável a ataques por dicionário.**
2. **Na autenticação de utentes do sistema Linux:**
   1. **O processo de autenticação não suporta múltiplos fatores.**
   2. **A senha é armazenada no disco, depois de validada pelo TPM.**
   3. **O administrador pode alterar o método de armazenamento das credenciais.**
   4. **O ficheiro /etc/shadow possui um backup do ficheiro /etc/passwd**
3. **Qual dos seguintes protocolos de autenticação é vulnerável a ataques com dicionário?**
   1. **TTLS.**
   2. **RSA SecurID.**
   3. **SSH.**
   4. **Linux (diz aqui qualquer merda unix mas eu não percebo).**
4. **Relativamente à autenticação no GSM (Global System for Mobile Communications):**
   1. **Baseia-se no conhecimento mútuo (utente e rede) de um PIN.**
   2. **O desafio enviado pela rede é baseado no PIN.**
   3. **A função de transformação do desafio apresentado pela rede é universal e realizada pelos terminais móveis.**
   4. **É imune a ataques com dicionário.**
5. **Na autenticação de utentes do sistema MS Windows:**
6. **O TPM fornece credenciais ao sistema após desbloqueio com um PIN.**
7. **O TEE executa um sistema seguro para armazenamento de credenciais.**
8. **O reconhecimento facial faz uso de um PIN para identificação do utilizador.**
9. **O método NTLM Password hash calcula uma síntese da senha com SALT.**
10. **O EAP (Extensible Authentication Protocol):**
    1. **É um protocolo de autenticação baseado em chaves assimétricas.**
    2. **É usado no 802.1X para autenticar um Suplicante perante um Autenticador.**
    3. **É um protocolo que permite entender outros protocolos de autenticação.**
    4. **É usado no 802.1X para autenticar um Suplicante perante um Servidor de Autenticação.**
11. **A proteção do tráfego Wi-Fi por meio sem fios com TKIP permite qual das seguintes funcionalidades?**
    1. **Controlo de integridade do cabeçalho e da carga útil com Michael(who the fk is Michael?).**
    2. **Controlo de integridade do cabeçalho e da carga útil com CRC-32.**
    3. **Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES.**
    4. **Controlo de integridade da carga útil com CBC-MAC e AES.**
12. **A autenticação do WPA no acesso a um terminal móvel à rede:**
    1. **Depende sempre de um serviço central de autenticação.**
    2. **Mantém a autenticação SKA do WEP mas evita a sua insegurança.**
    3. **Usa sempre EAP.**
    4. **Realiza sempre uma distribuição de chaves ao Suplicante e ao Autenticador.**
13. **Tendo em conta a existência de diferentes níveis de proteção na execução de um CPU (protection rings), indique a resposta certa:**
    1. **Sem esses níveis o núcleo de um sistema operativo estaria vulnerável a ataques feitos pelas aplicações.**
    2. **Os sistemas operativos podem definir as instruções que podem fazer parte de cada nível.**
    3. **Não é possível transitar de um nível menos privilegiado para outro mais privilegiado.**
    4. **Existe uma relação direta entre esses níveis e os privilégios de administração de um sistema operativo.**
14. **Relativamente ao mecanismo AppArmor, qual das seguintes afirmações é correta?**
    1. **Não é útil para vários programas interpretados quando chamados através do seu interpretador (ex python3 app.py).**
    2. **Implementa um mecanismo de armadura que protege as aplicações de atacantes externos.**
    3. **Uma aplicação pode escolher ignorar as regras do mecanismo.**
    4. **fodeu, está numa pagina que eu nao tenho :’).**
15. **Considerando o mecanismo Set-UID/Set-GID, qual é a afirmação verdadeira?**
16. **Um ficheiro com permissões Set-UID irá executar com as permissões de quem o executa.**
17. **O mecanismo de Set-UID afeta o effective UID de um processo mas mantém o seu real UID inalterado.**
18. **Um processo possui as permissões do utilizador com o real UID associado ao processo.**
19. **A permissão de Set-GID altera o GID associado a um ficheiro.**

**12. Considerando o UNIX/Linux, qual das seguintes afirmações é verdadeira?**

* 1. **Cabe exclusivamente ao seu núcleo a função de gerir um modelo computacional independente do hardware.**
  2. **A interação entre processos pode-se realizar sem qualquer pedido expresso ao núcleo.**
  3. **Os procedimentos de login de um utente são geridos pelo seu núcleo.**
  4. **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?**

1. **RAID 1.**
2. **RAID 0+1**
3. **RAID 6.**
4. **RAID 5.**

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

1. **Avaria de N-1 discos.**
2. **Avaria de apenas um disco (qualquer).**
3. **Avaria de 3 discos.**
4. **Avaria de 2 discos.**

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

* 1. **A avaria de qualquer disco implica sempre a perda de informação.**
  2. **Avaria de todos os N discos.**
  3. **Avaria de ambos os discos com as somas de controlo (paridade).**
  4. **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):**
   1. **Usa sempre segredos partilhados entre utentes e servidor.**
   2. **Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor.**
   3. **Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS).**
   4. **É da responsabilidade do servidor SSH forçar a utilização de segredos complexos.**
2. **Relativamente à autenticação usando TLS (Transport Layer Security):**
   1. **Não protege a integridade da informação.**
   2. **Serve para garantir a negociação de uma chave de sessão entre os interlocutores corretos.**
   3. **O cliente pode escolher livremente quais as credenciais que usa na sua autenticação.**
   4. **A autenticação dos clientes é uma opção dos mesmos.**
3. **Relativamente à autenticação GSM (Global System for Mobile Communications):**
   1. **A função de transformação do desafio apresentado pela rede é universal e realizada pelos terminais móveis.**
   2. **Baseia-se no conhecimento mútuo (utente e rede) de um PIN.**
   3. **A posse do módulo SIM onde está a chave secreta é normalmente suficiente para um terminal móvel se autenticar.**
   4. **Usa um protocolo de autenticação multimétodo.**
4. **Relativamente à autenticação de utentes com S/Key:**
   1. **São usadas senhas descartáveis memorizadas pelos utentes.**
   2. **Os autenticadores precisam de reinstalar as suas credenciais de autenticação após um determinado número de utilizações.**
   3. **É imune a ataques de dicionário.**
   4. **É um protocolo de autenticação mútua.**
5. **Relativamente à autenticação de utentes com desafio resposta e pares de chaves assimétricas:**
   1. **Quem se autentica deve cifrar a resposta com a chave pública do autenticador.**
   2. **Quem se autentica deve apresentar a sua chave privada.**
   3. **A utilização de certificados de chave pública pode fornecer os mecanismos de identificação de quem se autentica.**
   4. **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:**
   1. **Controlo de integridade da carga útil com CBC-MAC e AES.**
   2. **Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES.**
   3. **Controlo de integridade da carga útil com Michael.**
   4. **Controlo de integridade da carga útil com CRC-32.**
7. **A autenticação do WPA no acesso de um terminal móvel à rede:**
   1. **Usa sempre EAP**
   2. **Permite a utilização de SKA para sistemas mais antigos.**
   3. **Elimina apenas o modo OSA do WEP.**
   4. **Permite o modelo SOHO para redes de pequenas dimensão.**
8. **A fase four-way Handshake do 802.1X destina-se:**
   1. **Autenticar mutuamente o Suplicante e o Servidor de Autenticação.**
   2. **Distribuir chaves criptográficas entre o Suplicante e o Servidor de Autenticação.**
   3. **Distribuir chaves criptográficas entre o Autenticador e o Servidor de Autenticação.**
   4. **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?**
   1. **Escrita/alteração pelo dono.**
   2. **Execução por um processo com GID igual ao ficheiro.**
   3. **Leitura pelo dono.**
   4. **Leitura por um processo com um GID igual ao ficheiro.**
10. **Relativamente ao mecanismo AppArmor, qual das afirmações é correta?**
    1. **Não acrescenta nada face ao mecanismo (o resto está tapado).**
    2. **Apenas limita as comunicações na rede.**
    3. **Aplica regras genéricas, válidas para aplicações com o mesmo comportamento.**
    4. **Não se aplica a processos executados pelo root.**
11. **Considerando o mecanismo Set-UID/Set-GID, qual é a afirmação verdadeira?**
    1. **A permissão do Set-UID altera o UID associado a um ficheiro.**
    2. **A permissão do Set-UID altera o GID associado a um ficheiro.**
    3. **Um ficheiro com permissões Set-UID irá executar com as permissões de quem o executa.**
    4. **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?**
    1. **É equivalente ao mecanismo AppArmor.**
    2. **Os interfaces de rede não podem pertencer a um namespace pois não são processos.**
    3. **Os processos não podem pertencer a vários namespaces.**
    4. **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?**
    1. **Permitem utilizar mecanismos de duplicação de blocos.**
    2. **Garantem integridade do estado de cada ficheiro.**
    3. **Não garantem integridade do estado global dos ficheiros.**
    4. **Não garantem integridade do estado de cada ficheiro.**
14. **Relativamente ao método dos backups incrementais do sistema de ficheiros, qual das afirmações é verdadeira?**
    1. **A adição de novos dados é feita considerando o último backup completo.**
    2. **A longo prazo, o carácter incremental deste método irá resultar na utilização de mais espaço do que backups completos.**
    3. **A recuperação de dados é mais complexa que em outros métodos.**
    4. **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?**
    1. **Avaria de todos os N discos.**
    2. **Avaria do disco que contém as somas de controlo e um outro qualquer.**
    3. **Avaria de qualquer disco, excepto o que contém as somas de controlo (paridade).**
    4. **Avaria de 1 disco (qualquer).**
16. **Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?**
    1. **RAID 6**
    2. **RAID 0**
    3. **RAID 1**
    4. **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.**